Oracle® Fusion Middleware

Upgrade Guide for Oracle Identity Management

11*g* Release 1 (11.1.1)

E10129-10

November 2011

ORACLE®

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

E10129-10

Primary Author: Showvik Roy Chowdhuri

Contributors: Ajay Keni , Bharath Reddy, Brad Donison, Elan Elango, Mark Wilcox, Michael Rubino, Olaf Stullich, Paul Dickson, Pramodini Gattu, Reza Shafii, Robert Donat, Semyon Shulman, Stuart Duggan, Summet Agarwal , Sanjeev Sharma , Simon Kissane , Sophia Maler, Sitaraman Swaminathan, William Norcott

Contents

Part I   Understanding Oracle Identity Management and Oracle Identity and Access Management

1   Overview

Part II   Upgrading Your Oracle Identity Management Environments

2   Summary of the Upgrade Process for Oracle Identity Management

3   Supported Starting Points for Upgrading Oracle Identity Management

4   Types of Environments for Oracle Identity Management

5   Upgrading Your Oracle Internet Directory Environment

6 Upgrading Your Oracle Virtual Directory Environment

7 Upgrading Your Oracle Identity Federation Environment

Part III   Upgrading Your Oracle Single Sign-On and Oracle Identity and Access Management Environments

8   Summary of Upgrade Process for Oracle Single Sign-On and Oracle Identity and Access Management

9   Supported Starting Points for Upgrading Oracle Single Sign-On and Oracle Identity and Access Management

10   Types of Environments for Oracle Single Sign-On and Oracle Identity and Access Management

11   Upgrading Oracle Single Sign-On Environment

12 Upgrading Oracle Adaptive Access Manager Environment

13 Upgrading Oracle Identity Manager Environment

Part IV   Upgrading Oracle Identity Management High Availability Environments

14   Upgrading Oracle Internet Directory High Availability Environments

15　Upgrading an Oracle Identity Management Cold Failover Cluster Environment

16　Performing an Oracle Identity Management Multimaster and Fan-Out Replication Upgrade

17　Upgrading an Oracle Virtual Directory High Availability Environment

18   Upgrading an Oracle Identity Federation High Availability Environment

Index

Preface

This preface contains the following sections:

- Audience
- Documentation Accessibility
- Related Documents
- Conventions

Audience

This manual is intended for Oracle Fusion Middleware system administrators who are responsible for installing and upgrading Oracle Fusion Middleware instances. It is assumed that the readers of this manual have knowledge of the following:

- Oracle Application Server 10*g* system administration and configuration
- The configuration and expected behavior of the system being upgraded

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit `http://www.oracle.com/support/contact.html` or visit `http://www.oracle.com/accessibility/support.html` if you are hearing impaired.

Related Documents

For more information, see the following documents:

- *Oracle Fusion Middleware Upgrade Planning Guide*
- *Oracle Fusion Middleware Installation Planning Guide*
- *Oracle Fusion Middleware Integration Guide for Oracle Identity Management*
- *Oracle Fusion Middleware Administrator'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.

Part I

Understanding Oracle Identity Management and Oracle Identity and Access Management

Part I contains the following chapter:

- Chapter 1, "Overview"

1

Overview

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

- What is Oracle Identity Management and Oracle Identity and Access Management?
- What is Upgraded to Oracle Identity Management 11g Release 1 (11.1.1)
- What is Upgraded to Oracle Identity and Access Management 11g Release 1 (11.1.1)

1.1 What is Oracle Identity Management and Oracle Identity and Access Management?

Oracle Identity Management and Oracle Identity and Access 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 and Oracle Identity and Access 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
- Authorization Policy 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

For Oracle Identity Management 11*g* Release 1 (11.1.1), there are two separate installers:

- Oracle Identity Management 11g Release 1 (11.1.1.6.0)
- Oracle Identity and Access Management 11g Release 1 (11.1.1.5.0)

Oracle Identity Management 11*g* Release 1 (11.1.1.6.0)

This installer includes the following components:

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

Oracle Identity and Access Management 11*g* Release 1 (11.1.1.5.0)

This installer includes the following components:

- Oracle Access Manager
- Oracle Adaptive Access Manager
- Oracle Identity Manager
- Oracle Entitlements Server
- Oracle Identity Navigator

1.2 What is Upgraded to Oracle Identity Management 11*g* Release 1 (11.1.1)

You can upgrade the following Oracle Identity Management 10*g* components to Oracle Identity Management 11*g*:

- Oracle Internet Directory
- Oracle Virtual Directory
- Oracle Identity Federation

For upgrading to Oracle Identity Management 11*g*, you must follow the procedures described in Part II, "Upgrading Your Oracle Identity Management Environments".

> **Note:** You can also upgrade your High Availability (HA) configurations for Oracle Identity Management 10*g* Release 2 (10.1.2) and 10*g* (10.1.4.0.1) to Oracle Identity Management 11*g* Release 1 (11.1.1). For more information, see Part IV, "Upgrading Oracle Identity Management High Availability Environments".

1.3 What is Upgraded to Oracle Identity and Access Management 11*g* Release 1 (11.1.1)

You can upgrade the following Oracle Identity Management 10*g* components to Oracle Identity and Access Management 11*g*:

- Oracle Adaptive Access Manager

■ Oracle Identity Manager

> **Note:**   Oracle Single Sign-On and Oracle Delegated Administration Services Release 10*g* are required components for Oracle Portal, Forms, Reports, and Discoverer in 10*g* Release and 11*g* Release.
>
> There are no 11*g* Release 1 (11.1.1) versions of Oracle Single Sign-On and Oracle Delegated Administration Services.
>
> If you are running Oracle Single Sign-On or Oracle Delegated Administration Services Release 10*g*, you can upgrade to Oracle Access Manager 11*g*, as described in Chapter 11, "Upgrading Oracle Single Sign-On Environment".

For upgrading to Oracle Identity and Access Management 11*g*, you must follow the procedures described in Part III, "Upgrading Your Oracle Single Sign-On and Oracle Identity and Access Management Environments".

Part II

Upgrading Your Oracle Identity Management Environments

Part II contains the following chapters:

2

Summary of the Upgrade Process for Oracle Identity Management

This chapter provides a high-level overview of the Oracle Internet Directory, Oracle Virtual Directory, and Oracle Identity Federation upgrade processes. Refer to the following sections for more information:

- Flow Chart of the Oracle Identity Management Upgrade Process
- Steps in the Oracle Identity Management Upgrade Process

2.1 Flow Chart of the Oracle Identity Management Upgrade Process

Figure 2–1 provides a flow chart of the Oracle Identity Management upgrade process. Review this chart to get familiar with the steps you will be required to take, based on your existing version of Oracle Identity Management.

Figure 2–1   Flow Chart of the Oracle Identity Management Upgrade Process
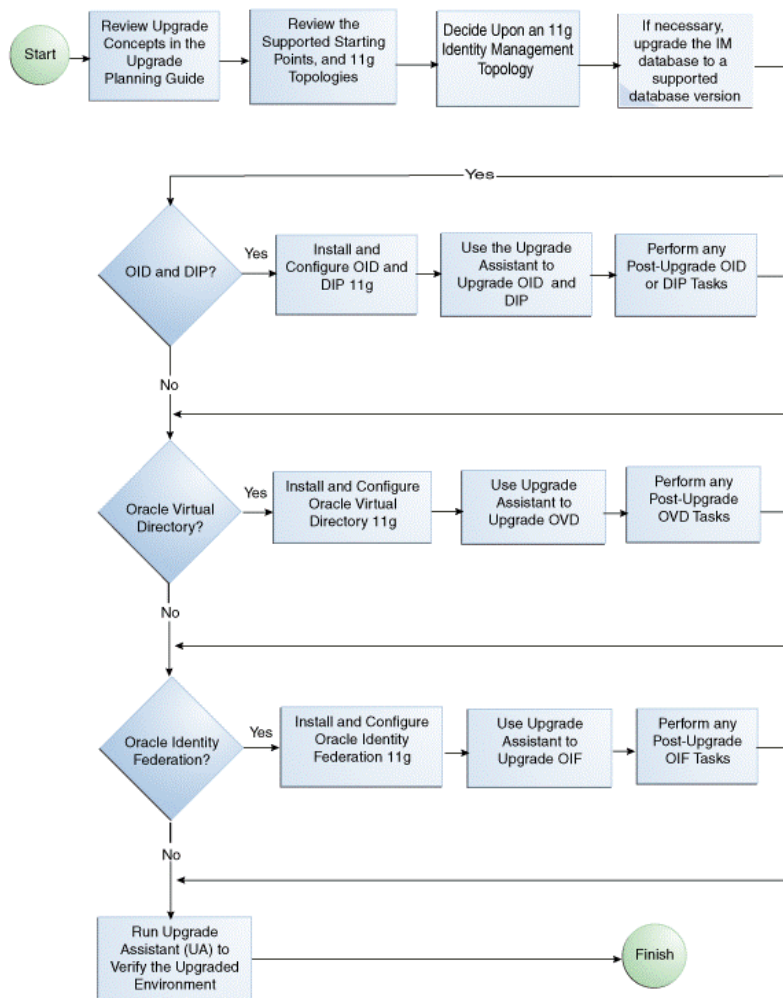
2.2 Steps in the Oracle Identity Management Upgrade Process

Table 2–1 describes each of the steps in the upgrade process flow chart, which is shown in Figure 2–1. The table also provides information on where to get more information on each step in the process.

Table 2–1   Steps in the Oracle Identity Management Upgrade Process

Step	Description	More Information
Review Upgrade Concepts in the Upgrade Planning Guide	The *Oracle Fusion Middleware Upgrade Planning Guide* provides a high-level overview of how to upgrade your entire Oracle Application Server environment to Oracle Fusion Middleware. It includes compatibility information and instructions for upgrading any databases that support your middleware components.	*Oracle Fusion Middleware Upgrade Planning Guide*
Understand the upgrade Starting Points and 11*g* Topologies	Before starting your upgrade, you should be familiar with the new features, supported started points, and recommended topologies for Oracle Fusion Middleware 11*g*. Based this knowledge, you can later decide upon an 11*g* topology.	Chapter 3, "Supported Starting Points for Upgrading Oracle Identity Management" Chapter 4, "Types of Environments for Oracle Identity Management"
Decide Upon an 11*g* Identity Management Topology	Oracle Fusion Middleware 11*g* introduces a new architecture based on Oracle WebLogic Server. As a result, you should review your current Oracle Application Server topology and decide upon an equivalent Oracle Fusion Middleware topology before you begin the upgrade process.	Chapter 4, "Types of Environments for Oracle Identity Management"
If necessary, upgrade the Oracle Identity Management database to a supported database version	When you upgrade to Oracle Fusion Middleware 11*g*, the OracleAS Identity Management schemas are upgraded to 11*g*. As a result, before you upgrade, ensure that the database that hosts the schemas is a supported version.	*Oracle Fusion Middleware Upgrade Planning Guide*
Oracle Internet Directory and Oracle Directory Integration Platform?	If you are upgrading Oracle Internet Directory or the Oracle Directory Integration Platform, then be sure to follow the appropriate instructions in this guide.	Chapter 5, "Upgrading Your Oracle Internet Directory Environment"
Install and Configure Oracle Internet Directory and Oracle Directory Integration Platform 11*g*	Install and configure an instance of Oracle Internet Directory 11*g* and Oracle Directory Integration Platform 11*g* on the same host as the Oracle Application Server 10*g* installation. Note that in preparation for upgrade, Oracle Universal Installer provides some specific installation screens when it detects that your database contains the 10*g* version of your OracleAS Identity Management schemas.	Section 5.3, "Task 3: Install and Configure the Oracle Internet Directory and Oracle Directory Integration Platform 11g Components"

Table 2–1   (Cont.) Steps in the Oracle Identity Management Upgrade Process

Step	Description	More Information
Use the Upgrade Assistant to Upgrade Oracle Internet Directory and Oracle Directory Integration Platform	Run the Upgrade Assistant from your new 11*g* Oracle home and upgrade the Oracle Internet Directory schemas and middle tiers.	Section 5.4, "Task 4: Use Upgrade Assistant to Upgrade Oracle Internet Directory"
Perform any Post-Upgrade Oracle Internet Directory or Oracle Directory Integration Platform Tasks	The Upgrade Assistant automates many of the upgrade procedures, but in some cases there are additional tasks that you might have to perform manually.	Section 5.5, "Task 5: Complete Any Required Oracle Internet Directory and Oracle Directory Integration Platform Post-Upgrade Tasks"
Oracle Virtual Directory?	If you are upgrading Oracle Virtual Directory, then ensure to follow the appropriate instructions in this guide.	Chapter 6, "Upgrading Your Oracle Virtual Directory Environment"
Install and Configure Oracle Virtual Directory 11*g*	Install and configure an instance of Oracle Virtual Directory 11*g* on the same host as the Oracle Application Server 10*g* installation. Note that in preparation for upgrade, Oracle Universal Installer provides some specific installation screens when it detects that your database contains the 10*g* version of your OracleAS Identity Management schemas.	Section 6.2, "Task 2: Install and Configure Oracle Fusion Middleware 11g"
Use the Upgrade Assistant to Upgrade Oracle Virtual Directory	Run the Upgrade Assistant from your new 11*g* Oracle home and upgrade the Oracle Virtual Directory schema and middle tier.	Section 6.3, "Task 3: Use Upgrade Assistant to Upgrade Oracle Virtual Directory"
Perform any Post-Upgrade Oracle Virtual Directory Tasks	The Upgrade Assistant automates many of the upgrade procedures, but in some cases there are additional tasks that you might have to perform manuall.	Section 6.4, "Task 4: Complete Any Required Oracle Virtual Directory Post-Upgrade Tasks"
Oracle Identity Federation?	If you are upgrading Oracle Identity Federation, then be sure to follow the appropriate instructions in this guide.	Chapter 7, "Upgrading Your Oracle Identity Federation Environment"
Install and Configure Oracle Identity Federation 11*g*	Install and configure an instance of Oracle Identity Federation 11*g* on the same host as the Oracle Application Server 10*g* installation. Note that in preparation for upgrade, Oracle Universal Installer provides some specific installation screens when it detects that your database contains the 10*g* version of your OracleAS Identity Management schemas.	Section 7.3, "Task 3: Install and Configure Oracle Fusion Middleware 11g"

Table 2–1   (Cont.) Steps in the Oracle Identity Management Upgrade Process

Step	Description	More Information
Use Upgrade Assistant to Upgrade Oracle Identity Federation	Run the Upgrade Assistant from your new 11*g* Oracle home and upgrade the Oracle Identity Federation schemas and middle tiers.	Section 7.4, "Task 4: Use the Upgrade Assistant to Upgrade Oracle Identity Federation"
Perform any Post-Upgrade Oracle Identity Federation tasks	The Upgrade Assistant automates many of the upgrade procedures, but in some cases there are additional tasks that you might have to perform manually.	Section 7.5, "Task 5: Complete Any Required Oracle Identity Federation Post-Upgrade Tasks"
Run Upgrade Assistant to verify the Upgraded Environment	You can use the Upgrade Assistant, as well other techniques to validate the upgrade and verify that the upgraded environment is up and running successfully.	Section 5.6, "Task 6: Verify the Oracle Internet Directory and Oracle Directory Integration Platform Upgrade" Section 6.5, "Task 5: Verify the Oracle Virtual Directory Upgrade" Section 7.6, "Task 6: Verify the Oracle Identity Federation Upgrade"

3

Supported Starting Points for Upgrading Oracle Identity Management

This chapter describes the supported starting points for Oracle Internet Directory, Oracle Virtual Directory, and Oracle Identity Federation upgrade processes. This chapter contains the following sections:

- Supported Starting Points for Oracle Internet Directory and Oracle Directory Integration Platform Upgrade
- Supported Starting Points for Oracle Virtual Directory Upgrade
- Supported Starting Points for Oracle Identity Federation Upgrade

---

Note: The starting point patchsets listed in this chapter were the latest patchsets available at the time this guide was published.

For a list of the latest patchsets available for your installation, refer to *My Oracle Support*.

3.1 Supported Starting Points for Oracle Internet Directory and Oracle Directory Integration Platform Upgrade

This guide provides instructions for upgrading from Oracle Internet Directory and Oracle Directory Integration Platform that is installed as part of the Oracle Application Server 10*g* releases and installation types described in Table 3–1.

Note: Note that there is no upgrade path supported for Oracle Single Sign-On or Oracle Delegated Administration Services 10*g*.

For more information, see Section 5.1, "Task 1: Understand Your Upgrade Options for SSO and Oracle Delegated Administration Services".

Table 3–1 Oracle Internet Directory and Oracle Directory Integration Platform Releases Supported By This Guide

Release	Installation Type	Description or Notes	Latest Patchset
10*g* Release 2 (10.1.2)	Oracle Identity Management and OracleAS Metadata Repository	This installation type includes the Identity Management software, as well as a database populated with the required Oracle Application Server Identity Management schemas.	10*g* Release 2 (10.1.2.3.0)
10*g* Release 2 (10.1.2)	Oracle Identity Management	This installation type installed only the Oracle Internet Directory software. It is assumed that you installed the required Identity Management schemas in an existing database by using the Repository Creation Utility (RCU).	10*g* Release 2 (10.1.2.3.0)
10*g* (10.1.4.0.1)	Oracle Identity Management and OracleAS Metadata Repository	This installation type includes the Identity Management software, as well as a database populated with the required Oracle Application Server Identity Management schemas.	10*g* (10.1.4.3)
10*g* (10.1.4.0.1)	Oracle Identity Management	This installation type installed only the Oracle Internet Directory software. It is assumed that you installed the required Identity Management schemas in an existing database by using the Repository Creation Utility (RCU).	10*g* (10.1.4.3)

3.2 Supported Starting Points for Oracle Virtual Directory Upgrade

This guide provides instructions for upgrading from the Oracle Virtual Directory releases described in Table 3–2.

Table 3–2 Oracle Virtual Directory Releases Supported By This Guide

Release	Description or Notes	Latest Patchset
10*g* (10.1.4.0.1)	This version of Oracle Virtual Directory was available as part of Oracle Application Server 10*g* (10.1.4.0.1). It was installed using a separate installation procedure and installation guide.	10*g* (10.1.4.3)

3.3 Supported Starting Points for Oracle Identity Federation Upgrade

This guide provides instructions for upgrading from the Oracle Identity Federation releases described in Table 3–3.

Table 3–3   Oracle Identity Federation Releases Supported By This Guide

Release	Description or Notes	Latest Patchset
10*g* (10.1.4.0.1)	This version of Oracle Identity Federation was available as part of Oracle Application Server 10*g* (10.1.4.0.1).	10*g* (10.1.4.3)

4

Types of Environments for Oracle Identity Management

This chapter describes the most common topologies for Oracle Identity Management 10*g* and how they compare with equivalent topologies in Oracle Fusion Middleware 11*g*.

This chapter contains the following sections:

- Oracle Internet Directory and Oracle Directory Integration Platform Topology
- Oracle Virtual Directory Topologies
- Oracle Identity Federation Topologies

4.1 Summary of the Oracle Identity Management 10*g* and 11*g* Components

The following sections describe the Oracle Identity Management components that were included in the Oracle Application Server 10*g* Release 2 (10.1.2) and Oracle Identity Management 10*g* (10.1.4.0.1) releases:

- Identity Management Components Available in Oracle Application Server 10g Release 2 (10.1.2)
- Identity Management Components Available in Oracle Identity Management 10g (10.1.4.0.1)
- Identity Management Components Available in Oracle Fusion Middleware 11g

4.1.1 Identity Management Components Available in Oracle Application Server 10*g* Release 2 (10.1.2)

In Oracle Application Server 10*g* Release 2 (10.1.2), the Oracle Identity Management components consists of the following:

- Oracle Internet Directory
- Oracle Directory Integration Platform
- Oracle Single Sign-On
- Oracle Delegated Administration Services

When you install and configure these 10*g* Release 2 (10.1.2) components, you can install them all into the same Oracle home (a colocated environment), or you can distribute them in separate Oracle homes (a distributed environment).

For the distributed environment, users typically install the Oracle Internet Directory and Oracle Directory Integration Platform components into one Oracle home and the Oracle Single Sign-On and Oracle Delegated Administration Services components into a second Oracle home.

4.1.2 Identity Management Components Available in Oracle Identity Management 10*g* (10.1.4.0.1)

Oracle Identity Management 10*g* (10.1.4.0.1) provided the following Oracle Identity Management components:

- Oracle Internet Directory

- Oracle Directory Integration Platform

- Oracle Single Sign-On

- Oracle Delegated Administration Services

- Oracle Virtual Directory

- Oracle Identity Federation

- Oracle Access Manager

As shown in the previous list, Oracle Identity Management 10*g* (10.1.4.0.1) introduced the Oracle Virtual Directory, Oracle Identity Federation, and Oracle Access Manager components.

In a typical environment, Oracle Virtual Directory and Oracle Identity Federation are separately from the colocated or distributed installations of the other Oracle Identity Management components.

4.1.3 Identity Management Components Available in Oracle Fusion Middleware 11*g*

Oracle Fusion Middleware 11*g* provides new versions of the following Oracle Identity Management 10*g* components:

- Oracle Internet Directory

- Oracle Directory Integration Platform

- Oracle Virtual Directory

- Oracle Identity Federation

Note that Oracle Fusion Middleware 11*g* does not include Oracle Single Sign-On or Oracle Delegated Administration Services.

For more information about the Oracle Identity Management components available with 11*g*, refer to the *Oracle Fusion Middleware Integration Guide for Oracle Identity Management*.

4.2 Oracle Internet Directory and Oracle Directory Integration Platform Topology

Oracle Identity Management 10*g* Release 2 (10.1.2) and 10*g* (10.1.4.0.1) supported two main types of Oracle Identity Management environments. The following sections describe these environments and compare them with an equivalent environment in Oracle Fusion Middleware 11*g*:

- Upgrading a Colocated Identity Management Environment

■ Upgrading a Non-Colocated Identity Management Environment

4.2.1 Upgrading a Colocated Identity Management Environment

Figure 4–1 compares a typical colocated Oracle Identity Management environment in 10*g* Release 2 (10.1.2) or 10*g* (10.1.4.0.1) with a similar topology in Oracle Fusion Middleware 11*g*.

Figure 4–1   Upgrading an Oracle Identity Management 10g Colocated Installation to Oracle Fusion Middleware 11g
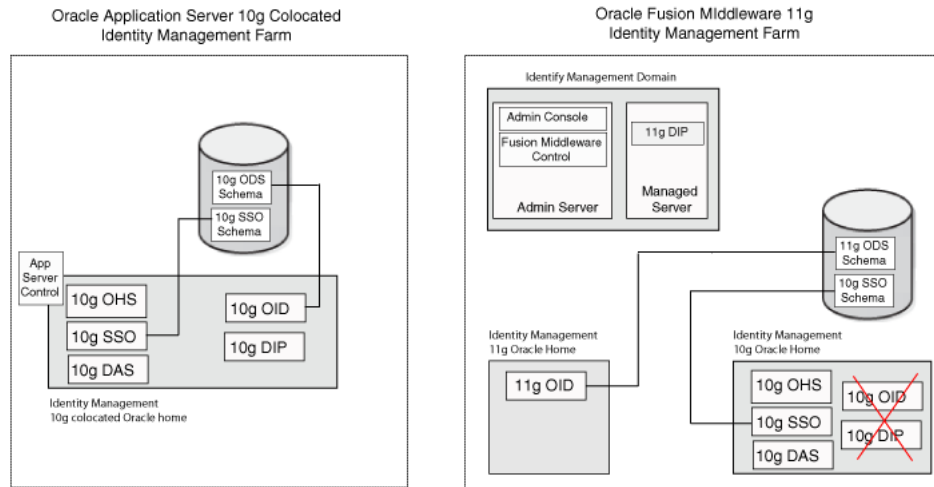
4.2.2 Upgrading a Non-Colocated Identity Management Environment

Figure 4–2 compares a typical non-colocated Oracle Identity Management environment in Oracle Application Server 10*g* Release 2 (10.1.2) or 10*g* (10.1.4.0.1) with a similar topology in 11*g*.

Figure 4–2   Upgrading an Oracle Identity Management 10g Non-Colocated Installation to Oracle Fusion Middleware 11g
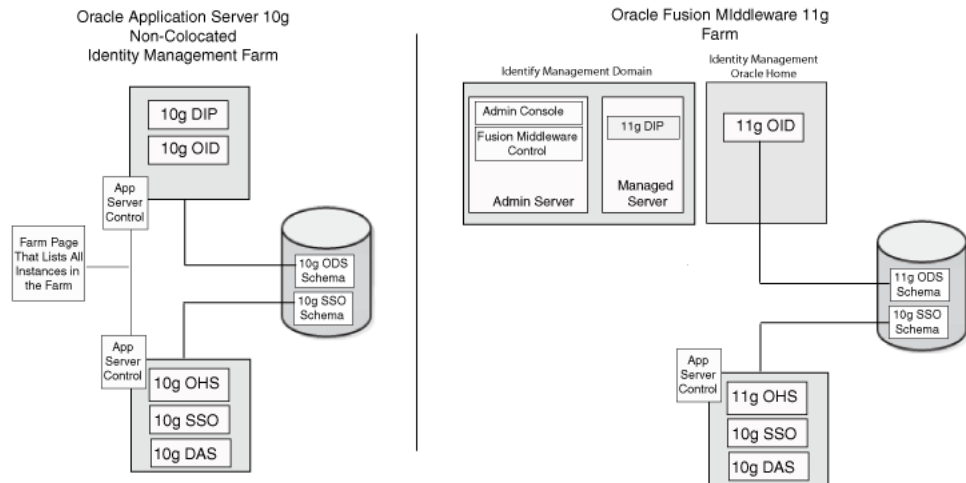
4.3 Oracle Virtual Directory Topologies

Oracle Virtual Directory 10*g* could be installed and configured with Oracle Internet Directory 10*g* or without Oracle Internet Directory 10*g*.

Figure 4–3 compares the Oracle Virtual Directory 10*g* and Oracle Virtual Directory 11*g* topologies when you are not using Oracle Internet Directory.

Figure 4–3 Upgrading Oracle Virtual Directory
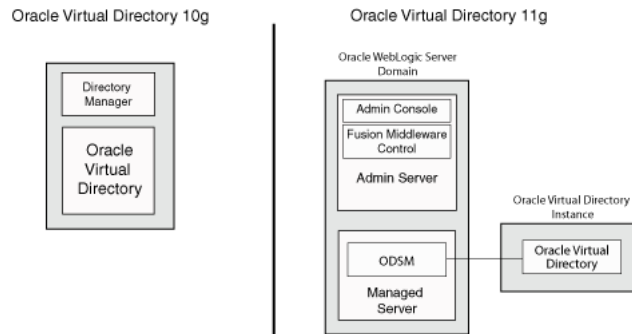
4.4 Oracle Identity Federation Topologies

Figure 4–4 compares a typical Oracle Identity Federation topology in Oracle Application Server 10*g* (10.1.4.0.1) with a similar topology in Oracle Fusion Middleware 11*g*.

Figure 4–4 Comparison of Typical Oracle Identity Federation Topologies in Oracle Application Server 10g (10.1.4.0.1) and Oracle Fusion Middleware 11g
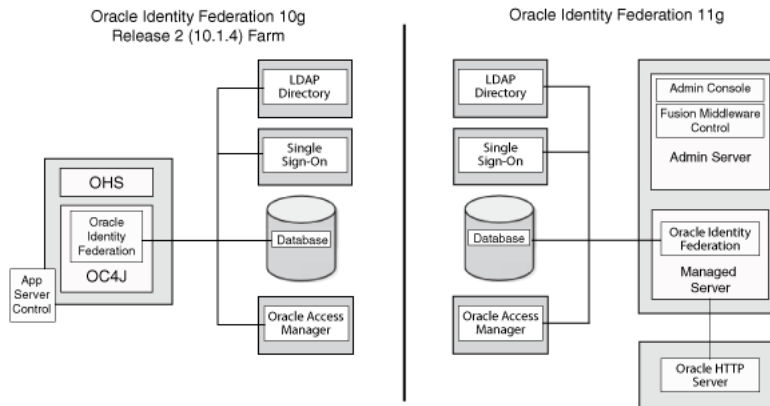
5

Upgrading Your Oracle Internet Directory Environment

This chapter describes how to upgrade your existing 10*g* Release 2 (10.1.2) or 10*g* (10.1.4.0.1) Oracle Internet Directory to Oracle Internet Directory Release 11*g*.

This chapter contains the following sections:

- Task 1: Understand Your Upgrade Options for SSO and Oracle Delegated Administration Services
- Task 2: If Necessary, Upgrade the Database that Contains the 10g Identity Management Schemas
- Task 3: Install and Configure the Oracle Internet Directory and Oracle Directory Integration Platform 11g Components
- Task 4: Use Upgrade Assistant to Upgrade Oracle Internet Directory
- Task 5: Complete Any Required Oracle Internet Directory and Oracle Directory Integration Platform Post-Upgrade Tasks
- Task 6: Verify the Oracle Internet Directory and Oracle Directory Integration Platform Upgrade

5.1 Task 1: Understand Your Upgrade Options for SSO and Oracle Delegated Administration Services

If you are using Oracle Single Sign-On or Oracle Delegated Administration Services, then you should be aware that there is no upgrade path to Oracle Fusion Middleware 11*g* for these components.

Instead, if you are using Oracle Single Sign-On with Oracle Portal, Forms, Reports, and Discoverer, then you upgrade your existing 10*g* Release 2 (10.1.2) or 10*g* (10.1.4.0.1) Oracle Single Sign-On instance to Oracle Access Manager, for more information see Chapter 11, "Upgrading Oracle Single Sign-On Environment".

> **See Also:** Section 4.1, "Summary of the Oracle Identity Management 10g and 11g Components".

Oracle Fusion Middleware offers a new version of Oracle Internet Directory and the Oracle Directory Integration Platform. Oracle recommends that you upgrade your Oracle Internet Directory and Oracle Directory Integration Platform instances to Oracle Fusion Middleware 11*g*.

5.2 Task 2: If Necessary, Upgrade the Database that Contains the 10*g* Identity Management Schemas

When you upgrade your Oracle Identity Management components, the Oracle Identity Management schemas in the metadata repository are upgraded "in-place." This means that you do not install the Oracle Fusion Middleware 11*g* schemas; instead, you upgrade the existing 10*g* schemas to 11*g*, using the Upgrade Assistant.

However, you must ensure that the version of the database that will contain the upgraded Oracle Identity Management schemas is supported by Oracle Fusion Middleware 11*g*.

For instructions on verifying that your database meets the requirements of Oracle Fusion Middleware 11*g*, as well as instructions for upgrading the database, see "Upgrading and Preparing Your Databases" in the *Oracle Fusion Middleware Upgrade Planning Guide*.

5.3 Task 3: Install and Configure the Oracle Internet Directory and Oracle Directory Integration Platform 11*g* Components

The following sections describe how to install and configure your new Oracle Fusion Middleware 11*g* environment in preparation for upgrading from Oracle Application Server 10*g*:

- Understanding the Implications of Installing Oracle Internet Directory 11g Against the Oracle Internet Directory 10g Schema

- Install the Oracle WebLogic Server Software and Creating the Middleware Home

- Install and Configure Oracle Internet Directory and Oracle Directory Integration Platform 11g in Preparation for Upgrade

---

Note: If you are upgrading your Oracle Application Server 10*g* Oracle Internet Directory and Oracle Directory Integration Platform components to 11*g*, then you must install the new 11*g* software on the same host as the Oracle Application Server 10*g* components.

5.3.1 Understanding the Implications of Installing Oracle Internet Directory 11*g* Against the Oracle Internet Directory 10*g* Schema

To upgrade Oracle Internet Directory to 11*g*, you must install the new Oracle Internet Directory 11*g* instance against the existing Oracle Internet Directory 10*g* (ODS) schema. Then, you can you run the Upgrade Assistant to upgrade the Oracle Internet Directory 10*g* schema to 11*g*.

Note, however, that until you upgrade the Oracle Internet Directory 10*g* schema to 11*g*, the new Oracle Internet Directory instance will be in read-only mode. As a result, be sure you have planned for enough time to not only install the new Oracle Internet Directory instance, but to upgrade the ODS schema, as described in "Task 4: Use Upgrade Assistant to Upgrade Oracle Internet Directory".

Ensure that you do not run the Oracle Internet Directory 10*g* and Oracle Internet Directory 11*g* at the same time, this will avoid port conflicts.

5.3.2 Install the Oracle WebLogic Server Software and Creating the Middleware Home

The following sections provide information about installing Oracle WebLogic Server and creating the Middleware home in preparation for an Oracle Identity Management upgrade:

- When is Oracle WebLogic Server Required?

- Install Oracle WebLogic Server Software and Create the Middleware Home

5.3.2.1 When is Oracle WebLogic Server Required?

Before you install Oracle Internet Directory and Oracle Directory Integration Platform 11*g*, note the following:

- Oracle Directory Integration Platform 11*g* requires an existing Oracle WebLogic Server domain.

- Oracle Internet Directory does not require a domain. However, if you install Oracle Internet Directory without specifying a domain, then you will not be able to manage the Oracle Internet Directory instance with Fusion Middleware Control or Oracle Directory Services Manager.

  Note that you can later use an OPMN command to register the standalone Oracle Internet Directory instance with a domain where Oracle Directory Services Manager is configured. For more information, see "Registering an Oracle Instance or Component with the WebLogic Server" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

When you install the Oracle WebLogic Server software on disk, you create a directory called the Middleware home, which contains the Oracle WebLogic Server software files. Later, you also install an Oracle Identity Management Oracle home inside the Middleware home.

5.3.2.2 Install Oracle WebLogic Server Software and Create the Middleware Home

For information on installing the Oracle WebLogic Server, see "Preparing for Installation" and "Running the Installation Program in Graphical Mode" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

5.3.3 Install and Configure Oracle Internet Directory and Oracle Directory Integration Platform 11*g* in Preparation for Upgrade

The following sections provide information about installing Oracle Internet Directory and Oracle Directory Integration Platform in preparation for upgrade:

- Before You Begin Installing Oracle Internet Directory and Oracle Directory Integration Platform

- Install Oracle Internet Directory and Oracle Directory Integration Platform 11g Release 1 (11.1.1.6.0)

5.3.3.1 Before You Begin Installing Oracle Internet Directory and Oracle Directory Integration Platform

Before you begin installing and configuring Oracle Internet Directory and Oracle Directory Integration Platform in preparation for an upgrade, consider the following:

- When you install Oracle Internet Directory and Oracle Directory Integration Platform in preparation for upgrade, the installation is similar to any other 11*g*

installation, except that in this case, you install the Oracle Internet Directory 11*g* instance against the existing Oracle Internet Directory 10*g* (ODS) schema.

Immediately after the installation, you then use the Oracle Fusion Middleware Upgrade Assistant to upgrade the ODS schema to 11*g*. During the time between the installation and running the Upgrade Assistant, the new Oracle Internet Directory instance is in read-only mode. As a result, it is not fully operational until after you run the Upgrade Assistant.

■ When you make your selections while installing Oracle Internet Directory and Oracle Directory Integration Platform, you should configure the new 11*g* environment so it matches the topology you configured for Oracle Application Server 10*g*.

For example, if you were running both Oracle Internet Directory and Oracle Directory Integration Platform out of the same 10*g* Oracle home, you should install and configure both components in the same Oracle Fusion Middleware 11*g* Oracle home.

■ When you install Oracle Internet Directory 11*g* ensure that you enter the same user credentials as used in the Oracle Application Server 10g components.

■ If you recently upgraded the database that contains your Oracle Identity Management schemas, be sure to check for invalid objects in the database before proceeding with the upgrade.

For more information, see "Upgrading and Preparing Your Databases" in the *Oracle Fusion Middleware Upgrade Planning Guide*.

5.3.3.2 Install Oracle Internet Directory and Oracle Directory Integration Platform 11*g* Release 1 (11.1.1.6.0)

For installing Oracle Identity Management, refer to the chapter "Installing and Configuring Oracle Identity Management (11.1.1.6.0)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

5.4 Task 4: Use Upgrade Assistant to Upgrade Oracle Internet Directory

After you install Oracle Internet Directory and Oracle Directory Integration Platform and point the installation to the existing Oracle Identity Management 10*g* schemas, you can then run the Oracle Fusion Middleware Upgrade Assistant.

The Upgrade Assistant automates the upgrade of the Oracle Internet Directory schema and your Oracle Identity Management 10*g* middle tier.

The Upgrade Assistant is installed into the `bin` directory of your Oracle Fusion Middleware Oracle home.

The following sections provide more information:

■ Task 4a: Perform Required Pre-Upgrade Tasks

■ Task 4b: Start the Upgrade Assistant for an Oracle Identity Management Upgrade

■ Task 4c: Upgrade the Oracle Internet Directory and Oracle Directory Integration Platform Instance

5.4.1 Task 4a: Perform Required Pre-Upgrade Tasks

Before you start the Upgrade Assistant, perform the following pre-Upgrade tasks that apply to your installation:

- Verifying the Status of Oracle Identity Management 10g Schemas
- Backing Up the Database Where the Oracle Identity Management 10g Schema Resides
- Modifying the SSL Port Configuration When Using SSL Authentication Mode on the Windows Operating System

5.4.1.1 Verifying the Status of Oracle Identity Management 10*g* Schemas

Before you start the Upgrade Assistant to upgrade your Oracle Identity Management components to Oracle Identity Management 11*g*, verify that the existing Oracle Identity Management 10*g* schemas in the database are valid:

> **Note:** This procedure is especially important to perform after you apply the 10*g* Release 2 (10.1.2.3) patch set to your 10*g* Release 2 (10.1.2) environment and before you upgrade our 10*g* Release 2 (10.1.2.3) components to 11*g*.

1. Connect to the database that contains the Oracle Internet Directory 10*g* schemas using SQLPlus.

2. Use the following SQL SELECT statement to view the status of the Oracle Internet Directory schemas:

   ```
   SELECT comp_id,version,status FROM app_registry where COMP_ID = 'OID';
   ```

3. Verify that the status of the schemas is set to VALID.

   If the output from the SELECT command identifies the Oracle Internet Directory schema as INVALID, perform the following steps to fix the issue:

   a. Use a text editor to open the following file in the Oracle Internet Directory 10*g* Oracle home:

      ```
      ORACLE_HOME/ldap/admin/oidi10121.sql
      ```

   b. Insert the following at the top of the oidi10121.sql file so that it is run as the ODS schema user:

      ```
      alter session set current_schema = ODS;
      ```

   c. Run patchcfg.sql as the SYS user.

      For example:

      ```
      cd ORACLE_HOME/ldap/admin/
      sqlplus "connect / as sysdba"
      SQL> @patchcfg.sql
      ```

   d. Identify the objects in the database that are owned by SYS and are also owned by ODS.

      patchcfg.sql displays a list of objects from the database, as shown in Example 5–1.

   e. For each of the objects, enter a DROP PACKAGE statement.

      For example:

      ```
      drop package OIDMETRICINFO;
      ```

Example 5–1   Invalid Objects to Drop from the Oracle Identity Management Schema Database

```
select owner, object_name, object_type from dba_objects
      where status = 'INVALID' order by owner, object_name;

OWNER      OBJECT_NAME        OBJECT_TYPE
---------- ------------------ ------------
SYS        LDAPBLKMOD         PACKAGE BODY
SYS        LDAPUPGUTLS        PACKAGE BODY
SYS        MODIFYDN           PACKAGE
SYS        MODIFYDN           PACKAGE BODY
SYS        ODIGETDIPINFO      PACKAGE BODY
SYS        OIDCONFIGINFO      PACKAGE BODY
SYS        OIDMETRICINFO      PACKAGE BODY
SYS        OIDPORTINFO        PACKAGE BODY
SYS        OIDREPLSTATUSINFO  PACKAGE BODY
SYS        OIDSTATUSINFO      PACKAGE BODY
SYS        OID_STATS          PACKAGE
SYS        OID_STATS          PACKAGE BODY
SYS        OLADD              PACKAGE BODY
SYS        PURGEADMIN         PACKAGE BODY
SYS        TSPURGE            PACKAGE BODY
```

5.4.1.2 Backing Up the Database Where the Oracle Identity Management 10*g* Schema Resides

Before you upgrade the Oracle Identity Management 10*g* schema to 11*g*, back up your database, in case you need to restore the database to its pre-upgrade state.

For more information, see "Backup Strategies for Upgrade" in the *Oracle Fusion Middleware Upgrade Planning Guide*.

5.4.1.3 Modifying the SSL Port Configuration When Using SSL Authentication Mode on the Windows Operating System

If you are running Oracle Identity Management components on the Windows operating system, and you have configured Authentication Mode for the SSL port for Oracle Internet Directory 10*g*, then you must change this configuration to SSL No Authentication Mode prior to the upgrade to 11*g*.

Similarly, if Oracle Directory Integration Platform 10*g* is connected to the Oracle Internet Directory SSL port using SSL Server Authentication Mode, then you must also reconfigure Oracle Directory Integration Platform to connect to Oracle Internet Directory using SSL No Authentication Mode mode prior to the upgrade to 11*g*.

For more information, see *Oracle Internet Directory Administrator's Guide* and *Oracle Identity Management Integration Guide* in the 10*g* (10.1.4.0.1) documentation library:

http://download.oracle.com/docs/cd/B28196_01/index.htm

After the upgrade, reconfigure both Oracle Internet Directory and Oracle Directory Integration Platform for SSL Server Authentication Mode mode using wallets.

For more information, see the following:

■   "Configuring Secure Sockets Layer (SSL)" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*

■   "Managing the Oracle Directory Integration Platform" in the *Oracle Fusion Middleware Integration Guide for Oracle Identity Management*

These changes are not required on Linux or UNIX-based operating systems.

5.4.2 Task 4b: Start the Upgrade Assistant for an Oracle Identity Management Upgrade

To start the Upgrade Assistant using the graphical user interface:

> **Note:** You can also use the Upgrade Assistant command-line interface to upgrade your Oracle Application Server 10*g* Oracle homes. For more information, see "Using the Upgrade Assistant Command-Line Interface" in the *Oracle Fusion Middleware Upgrade Planning Guide*.

1. Change directory the `ORACLE_HOME`/bin directory of the Oracle Fusion Middleware installation.

2. Enter the following command to start the Upgrade Assistant.

   On UNIX system:

   `./ua`

   On Windows systems:

   `ua.bat`

   The Upgrade Assistant displays the Welcome screen as shown in Figure 5–1

   Figure 5–1   Upgrade Assistant Welcome Screen

3. Click **Next** to display the Specify Operation screen (Figure 5–1).

   The options available in the Upgrade Assistant are specific to the Oracle home from which it started. When you start Upgrade Assistant from an Oracle Identity Management Oracle home, the options shown on the Specify Operation screen are the valid options for an Oracle Identity Management Oracle home.

Figure 5–2   Upgrade Assistant Specify Operation Screen for an Oracle Identity Management Upgrade
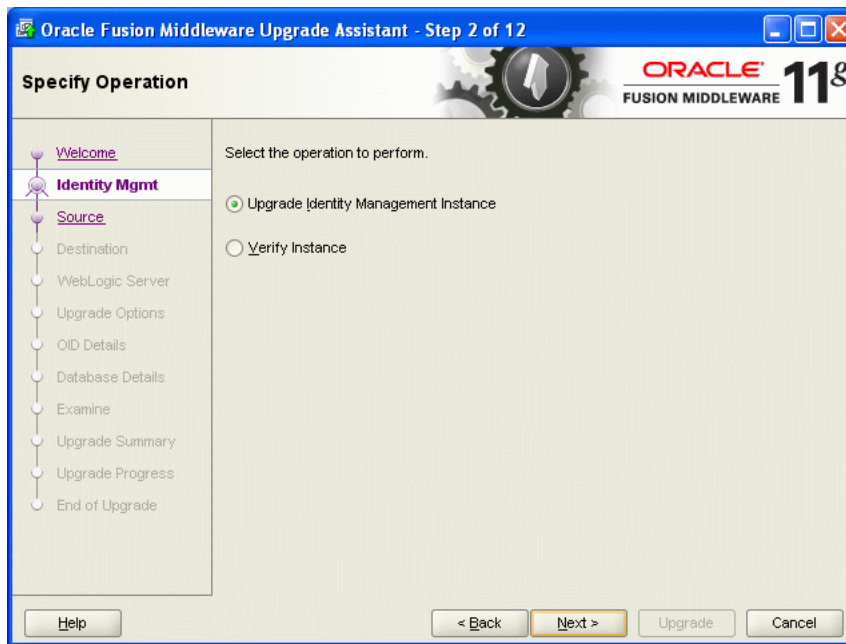
5.4.3 Task 4c: Upgrade the Oracle Internet Directory and Oracle Directory Integration Platform Instance

When you upgrade Oracle Internet Directory and Oracle Directory Integration Platform, the Upgrade Assistant upgrades the Oracle Identity Management schemas in the Metadata Repository and the configuration files in the Oracle Internet Directory and Oracle Directory Integration Platform middle tier.

Refer to the following sections for more information:

- Using the Upgrade Assistant to Upgrade Oracle Internet Directory and Oracle Directory Integration Platform

- About Specifying Real Application Clusters (RAC) Database Details on the Specify Database Details Screen

- Recovering From an Oracle Internet Directory Error During the Upgrade Assistant Examine Phase

5.4.3.1 Using the Upgrade Assistant to Upgrade Oracle Internet Directory and Oracle Directory Integration Platform

---

Note: This example assumes you have installed Oracle Internet Directory and Oracle Directory Integration Platform in the same Oracle Fusion Middleware 11*g* Oracle instance. You can also install Oracle Internet Directory and Oracle Directory Integration Platform in separate Oracle instances.

For more information, see Section 4.2, "Oracle Internet Directory and Oracle Directory Integration Platform Topology".

To upgrade Oracle Internet Directory and Oracle Directory Integration Platform when they reside in the same Oracle instance:

1. Backup the database that contains the Oracle Identity Management schemas.

   For more information, see "Backup Strategies for Upgrade" in the *Oracle Fusion Middleware Upgrade Planning Guide*.

2. Make sure that both the Oracle Internet Directory 10*g* instance and the new 11*g* instance are up and running before you start the Upgrade Assistant.

3. Start the Upgrade Assistant as described in Task 4b: Start the Upgrade Assistant for an Oracle Identity Management Upgrade.

4. Select **Upgrade Identity Management Instance** on the Specify Operation screen (Figure 5–2).

5. Refer to Table 5–1 for a description of the Upgrade Assistant screens that require input from you during an Oracle Internet Directory and Oracle Directory Integration Platform upgrade.

6. After the Target Database Details screen, the Upgrade Assistant performs the following tasks and provides the progress on each task:

   - Examines the components and schemas to be upgraded and verifies that they can be upgraded successfully.

   - Provides a summary of the components to be upgraded so you can verify that Upgrade Assistant is upgrading the components and schemas you expect.

   - Provides a progress screen so you can see the status of the upgrade as it proceeds.

   - Alerts you of any errors or problems that occur during the upgrade.

     See Also: "Troubleshooting Your Upgrade" in the *Oracle Fusion Middleware Upgrade Planning Guide* for specific instructions for troubleshooting problems that occur while running the Upgrade Assistant

   - Displays the End of Upgrade screen, which confirms that the upgrade was complete.

   - Sets the ODSSM schema password to match the existing ODS schema password.

7. Exit the Upgrade Assistant.

Table 5–1   Upgrade Assistant Screens That Require Input During an Oracle Internet Directory and Oracle Directory Integration Platform Upgrade

Upgrade Assistant Screen	Description
Specify Source Home	Select the 10*g* Release 2 (10.1.2) or 10*g* (10.1.4.0.1) source Oracle home.
	If the Oracle home you want to upgrade does not appear in the drop-down lists, see "Source Oracle Home Not Listed by OracleAS Upgrade Assistant" in the *Oracle Fusion Middleware Upgrade Planning Guide*.
Specify Destination Instance	Enter the complete path to the 11*g* Oracle instance, or click **Browse** to locate the instance directory.

Table 5–1 (Cont.) Upgrade Assistant Screens That Require Input During an Oracle Internet Directory and Oracle Directory Integration Platform Upgrade

Upgrade Assistant Screen	Description
Specify WebLogic Server	Enter the host and Administration Server port for the Oracle WebLogic Server you configured in Section 5.3.2, "Install the Oracle WebLogic Server Software and Creating the Middleware Home".
	Note this information is required if you are upgrading Oracle Directory Integration Platform. It is also required if you associated your Oracle Internet Directory 11*g* installation with Oracle WebLogic Server.
	For more information, see Section 5.3.2.1, "When is Oracle WebLogic Server Required?".
Warning Dialog Box	The Upgrade Assistant displays this warning dialog box if the source Oracle home contains Oracle Application Server components that are not installed and configured in the destination Oracle instance.
	This warning appears, for example, if the source Oracle home contains an instance of Oracle HTTP Server, which is not available in the 11*g* Oracle home. In addition, the 11*g* upgrade of Oracle Identity Management is for Oracle Internet Directory and Directory Integration Platform. Oracle HTTP Server and WebCache are required for Single Sign-On, so they are not necessary when you are migrating only Oracle Internet Directory and Directory Integration Platform.
	If the information in the dialog box is accurate and you understand which components will be upgraded, click **Yes** to continue. Otherwise, click **No** and verify which components are installed and configured in each 11*g* Oracle instance.
Specify Upgrade Options	Select the upgrade options you want to apply to the Oracle Identity Management upgrade:
	■ **Use source Oracle home ports in destination:** If you want to migrate the port assignments used by your Oracle Application Server 10g Oracle home to your new Oracle Fusion Middleware Oracle instance. Note if you select this option, you will not be able to run both the 10*g* and 11*g* middle tiers at the same time; otherwise, port conflicts will occur.
	■ **Start destination components after successful upgrade:** if you want the Upgrade Assistant to automatically start the components in the destination Oracle home after the upgrade is complete. If you do not select this option, then you will have to manually start the destination instance after the upgrade.
	Click **Help** to display more information about the upgrade options on this screen.
Specify Oracle Internet Directory Details	Use this screen to enter the details required to connect to the Oracle Internet Directory 10*g* instance, including the password to the Oracle Internet Directory super user account (`cn=orcladmin`).
	For more information, click **Help**.

Table 5–1   (Cont.) Upgrade Assistant Screens That Require Input During an Oracle Internet Directory and Oracle Directory Integration Platform Upgrade

Upgrade Assistant Screen	Description
Specify Database Details	Use this screen to enter the details required to connect to the database where the Oracle Identity Management schemas reside, including the host, service name, port, and SYS password for the database.
	Note the following important information about this screen:
	■ You must enter the password for the ODS schema password. The default ODS password is the same as the Oracle Application Server administrator password, but this password can be changed after installation, using the Oracle Internet Directory Database Password Utility.
	■ The instructions for identifying a Real Application Clusters (RAC) database are different, depending upon whether you are identifying the RAC database that contains the Oracle Internet Directory (ODS) schema or a RAC database that is being used for Oracle Directory Integration Platform.
	For more information, see Section 5.4.3.2, "About Specifying Real Application Clusters (RAC) Database Details on the Specify Database Details Screen".

5.4.3.2 About Specifying Real Application Clusters (RAC) Database Details on the Specify Database Details Screen

If you are upgrading the Oracle Internet Directory or Oracle Directory Integration Platform schemas that are stored in a RAC database, then you must consider the following important steps when entering the database connection details in the Specify Database Details screen in the Upgrade Assistant:

■ If you are upgrading the Oracle Internet Directory (ODS) schema in a RAC database, enter the details about only one node of the RAC database in the **Database Host**, **Database Port**, and **Database Service** fields. Do not enter any information about the Oracle Internet Directory schema database in the **Clustered Database Specification** field.

■ If you are upgrading Oracle Directory Integration Platform in a RAC database, then you must select the **Clustered Database** check box and enter the database connection details for each and every node in the cluster in the **Database Cluster Specification** field, using the syntax shown in Example 5–2.

Be sure to use the caret character (^) as a separator between each RAC node in the list.

Example 5–3 shows an example of how you would use the syntax to connect to a RAC database.

Example 5–2   Syntax for the Database Connection Details for a RAC Database

host_name:*port*:*first_instance_name*^*host_name*:*port*:*second_instance_name*@*db_service_name*

Example 5–3   Example of the Database Connection Details for a RAC Database

host1.example.com:1521:inst1^host3.example.com:1522:inst2@db_service.example.com

5.4.3.3 Recovering From an Oracle Internet Directory Error During the Upgrade Assistant Examine Phase

The Upgrade Assistant always examines the components in your source and target environments before performing an upgrade to Oracle Fusion Middleware 11g. After this examination phase, you can then proceed with the upgrade of the selected components.

However, if an error occurs while the Upgrade Assistant is examining an Oracle Internet Directory instance, you might have a problem using Upgrade Assistant to examine the Oracle Internet Directory instance again later.

Specifically, during the examine phase, the Upgrade Assistant checks to see if the Oracle Internet Directory instance is up and running. If the instance is not running, then the examine phase reports the problem. You must start the instance before proceeding to the upgrade phase.

After starting the instance, if you then click the **Back** button or restart the Upgrade Assistant, then the Upgrade Assistant skips the Oracle Internet Directory instance during the examination phase and does not report on its state.

To remedy this problem and to re-examine the Oracle Internet Directory instance after a previous examination error, do the following:

1. Stop the Upgrade Assistant.

2. Locate and delete the following temporary file:

   ORACLE_INSTANCE/OID/temp/oidretry.dat

3. Restart the Upgrade Assistant and re-examine the components you want to upgrade.

5.5 Task 5: Complete Any Required Oracle Internet Directory and Oracle Directory Integration Platform Post-Upgrade Tasks

After you upgrade Oracle Internet Directory and Oracle Directory Integration Platform, perform the following post-upgrade tasks:

- Recreating Any Non-Default Oracle Internet Directory Instances

- Disabling the Oracle Internet Directory and Oracle Directory Integration Platform 10g Components

- Configuring OPMN in the 10g Oracle Home After Upgrading Oracle Internet Directory to 11g

- Enabling Oracle Internet Directory Referential Integrity After Upgrade

- Reviewing Configuration Attributes that are not Upgraded to Oracle Internet Directory 11g

- Removing Oracle Internet Directory and Oracle Directory Integration Platform 10g from Application Server Control

- Removing Unneeded Oracle Directory Integration Platform Template Profiles After Upgrade

- Deleting Oracle Internet Directory 10g Audit Log Container

- Updating Oracle Internet Directory 10g Port Number in Oracle Enterprise Manager

- Configuring Oracle Single Sign-On 10g for Oracle Internet Directory 11g

5.5.1 Recreating Any Non-Default Oracle Internet Directory Instances

When you upgrade Oracle Internet Directory, only the default Oracle Internet Directory instance is upgraded.

If you have additional, non-default Oracle Internet Directory instances in your 10*g* environment, you must create those manually in the 11*g* environment, as follows:

1. Perform the following `ldapsearch` command to locate the additional Oracle Internet Directory instances:

```
ldapsearch
    -p oidPort
    -h oidHost
    -D cn=orcladmin
    -w adminPasswd
    -b "cn=osdldapd, cn=subconfigsubentry"
    -s one "cn=config*" dn orclsslport orclnonsslport orclmaxcc orclserverprocs
```

2. Verify the following before you create the additional Oracle Internet Directory instances:

   - That the following files, which are created during the installation, exist in the *ORACLE_INSTANCE*/config directory:

     ```
     tnsnames.ora
     tnsnames_copy.ora
     ```

   - Verify that OIDDB appears as an entry in the tnsnames.ora file.

3. Create each additional Oracle Internet Directory instance with the following command:

```
opmnctl createcomponent
    -adminRegistration OFF
    -componentType OID
    -componentName componentName
    -Db_info "DBHostName:Port:DBSvcName"
      [-Ods_Password_File 'File_with_DB_ODS_USER_PASSWORD']
      [-Sm_Password_File 'File_with_DB_ODSSM_USER_PASSWD']
      [-Admin_Password_File 'File_with_OID_Admin_Passwd']
    -Namespace "dc=domain_component1,dc=domain_component2..."
    [-Port nonSSLPortFromAboveSearchCommand]
    [-Sport SSLPortFromAboveSearchCommand]
```

4. After the new instance of Oracle Internet Directory is created, update the `orclmaxcc` and `orclserverprocs` using either Fusion Middleware Control or, as follows, using `ldapmodify` command:

```
ldapmodify -p <oidPort> -D cn=orcladmin -w <adminPaswd> << eof
dn: cn=<componentName>,cn=osdldapd,cn=subconfigsubentry
changetype: modify
replace: orclmaxcc
orclmaxcc: <orclMaxxCCValueFrom#1>
-
replace: orclserverprocs
orclserverProcs: <orclServerProcsValueFrom#1>
eof
```

5. Start new instances:

```
opmnctl startproc ias-component=componentName
```

5.5.2 Disabling the Oracle Internet Directory and Oracle Directory Integration Platform 10*g* Components

If you are using Oracle Single Sign-On and Oracle Delegated Administration Services, and then you upgrade the Oracle Internet Directory and Oracle Directory Integration Platform components in that environment, then you must disable the Oracle Internet Directory and Oracle Directory Integration Platform components in the Oracle Application Server 10*g* Oracle home.

This step is necessary because in most cases, you will want to maintain your Oracle Single Sign-On and Oracle Delegated Administration Services 10*g* components, but not the Oracle Internet Directory and Oracle Directory Integration Platform 10*g* components. For more information, see Section 4.2, "Oracle Internet Directory and Oracle Directory Integration Platform Topology".

To de-associate the existing 10*g* Oracle Single Sign-On from Oracle Internet Directory:

1. Modify the Oracle Internet Directory entry in the OPMN configuration file:

    a. Locate the following file in the Oracle Application Server 10*g* Oracle home:

       ```
       $ORACLE_HOME/opmn/conf/opmn.xml
       ```

    b. Make a backup copy of the file so you can easily revert to the original version if necessary.

    c. Locate the following entry in the opmn.xml file:

       ```
       <ias-component id="OID" status="enabled">
       ```

    d. Modify the entry so that the Oracle Internet Directory component is disabled:

       ```
       <ias-component id="OID" status="disabled">
       ```

2. Modify the Oracle Internet Directory and Oracle Directory Integration Platform settings in the ias.properties file:

    a. Locate the following file in the Oracle Application Server 10*g* Oracle home:

       ```
       ORACLE_HOME/config/ias.properties
       ```

    b. Make a backup copy of the file so you can easily revert to the original version if necessary.

    c. Locate the following entries in the ias.properties file and change them from true to false:

       ```
       OID.LaunchSuccess=false
       DIP.LaunchSuccess=false
       ```

3. Restart Oracle Single Sign-On in the Oracle Application Server 10*g* Oracle home.

> **Note:** Do not start any Oracle Internet Directory 10*g* and Oracle Directory Integration Platform 10*g* processes after the upgrade.

5.5.3 Configuring OPMN in the 10*g* Oracle Home After Upgrading Oracle Internet Directory to 11*g*

Use the information in this section if you are upgrading a distributed Oracle Identity Management environment, where the Oracle Internet Directory instance is on a different host from the Oracle Single Sign-On 10*g* instance.

In such a distributed environment, after you upgrade Oracle Internet Directory to 11*g*, you must reconfigure the `oc4j_security` OC4J instance so it does not continue to attempt to connect to OPMN on the Oracle Internet Directory 10*g* host. Otherwise, errors will appear in the `ons.log` file and the `oc4j_security` instance on the Oracle Single Sign-On host will fail to start.

To reconfigure the `oc4j_security` instance on the Oracle Single Sign-On host:

1. Locate the following configuration file in the Oracle Identity Management 10*g* Oracle home on the Oracle Single Sign-On host:

   ```
   ORACLE_HOME/opmn/conf/ons.conf
   ```

2. Edit the `ons.conf` file and remove any references to the Oracle Internet Directory host.

   In the following example, OPMN is using the information in the `ons.conf` file to communicate with OPMN on both SSOHOST1 and OIDHOST1. To stop OPMN from attempting to connect to the OIDHOST1, remove the OIDHOST1 and post from the file:

   ```
   nodes=SSOHOST1.example.com:6200,OIDHOST1.example.com:6200
   ```

5.5.4 Enabling Oracle Internet Directory Referential Integrity After Upgrade

When you upgrade Oracle Internet Directory to 11*g*, the referential integrity feature of Oracle Internet Directory is not enabled by default. As a result, if you were using referential integrity in Oracle Internet Directory 10*g*, perform the following steps after the upgrade to 11*g*:

1. Use the Oracle Internet Directory Server Diagnostic command-line tool (oiddiag) to identify and fix any referential integrity violations.

   For more information, see "oiddiag" in the *Oracle Fusion Middleware User Reference for Oracle Identity Management*.

2. Enable referential integrity for the upgraded Oracle Internet Directory 11*g*.

   For more information, see "Configuring Referential Integrity" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

5.5.5 Reviewing Configuration Attributes that are not Upgraded to Oracle Internet Directory 11*g*

When you upgrade your Oracle Internet Directory 11*g* instance to Oracle Internet Directory 11*g*, the following configuration parameter values are not upgraded to the 11*g* instance.

- `MinConnectionsInPool`: The value of this attribute will not be saved if it is zero.

- `PluginName`: This attribute identifies the authentication plug-in name; after upgrade, the 11*g* default values will be used for a particular authentication level.

- `ConnectionIdleTimeout`: This parameter is obsolete for Oracle Identity Management 11*g*.

For more information about the configuration parameters supported in Oracle Internet Directory 11*g*, see "Attribute Reference" in the *Oracle Fusion Middleware User Reference for Oracle Identity Management*.

5.5.6 Removing Oracle Internet Directory and Oracle Directory Integration Platform 10*g* from Application Server Control

After you upgrade to Oracle Internet Directory 11*g* and Oracle Directory Integration Platform 11*g*, the 10*g* versions of these components will still appear in the Oracle Enterprise Manager Application Server Control that is running out of the Oracle Single Sign-On 10*g* Oracle home.

To remove the Oracle Internet Directory and Oracle Directory Integration Platform targets from 10*g* Application Server Control:

1. Locate the following file in the Oracle Single Sign-On 10*g* Oracle home:

   `ORACLE_HOME`/sysman/emd/targets.xml

2. Delete the entry that represents the Oracle Internet Directory 10*g* instance from the `targets.xml` file.

   Note that the target element is formatted differently in the targets.xml file, depending on whether you are upgrading a 10*g* Release 2 (10.1.2) or 10*g* (10.1.4.0.1) Identity Management environment:

   - If you are upgrading from Oracle Identity Management 10*g* Release 2 (10.1.2), refer to Example 5–4 for an example of an entry in the `targets.xml` file that defines an Oracle Internet Directory target called `oid10g`.

   - If you are upgrading from Oracle Identity Management 10*g* (10.1.4.0.1), refer to Example 5–5 for an example of an entry in the targets.xml file that defines an Oracle Internet Directory target called `oid10g`.

   Note that Oracle Directory Integration Platform could not be managed by Oracle Enterprise Manager in 10*g* Release 2 (10.1.2), so you will not see a Oracle Directory Integration Platform entry in the 10*g* Release 2 (10.1.2) entry.

3. If necessary, do the same for the Oracle Directory Integration Platform target in the Oracle Single Sign-On 10*g* Oracle home.

   Refer to Example 5–6 for an example of any entry in targets.xml that defines an Oracle Directory Integration Platform target. When searching for the target, search for the target type, `"oracle_eps_server"`.

4. Start Application Server Control.

   Refer to the Oracle Application Server 10*g* documentation for instructions on stopping and starting Application Server Control.

   Note that these changes require a restart of Application Server Control before they take affect. However, in this case, the Oracle Application Server 10*g* environment will be down immediately after the upgraded, so there is no need to stop Application Server before starting it in this case.

Example 5–4   Oracle Internet Directory Target Entry in a 10g Release 2 (10.1.2) targets.xml File

```
<Target TYPE="oracle_ldap" NAME="oid10g.myhost.example.com_LDAP"
        DISPLAY_NAME="Internet Directory" VERSION="2.5"
        ON_HOST="myhost.example.com">
        <Property NAME="OracleHome" VALUE="/oracle/product/inst/ias10g"/>
                        .
                        .
                        .
</Target>
```

Example 5–5   Oracle Internet Directory Target Entry in a 10g (10.1.4.0.1) targets.xml File

```
<Target TYPE="oracle_ldap" NAME="oid10g.myhost.example.com_LDAP"
              DISPLAY_NAME="OID" VERSION="3.0" ON_HOST="myhost.example.com">
    <Property NAME="OracleHome"
              VALUE="/oracle/product/inst/ias10g"/>
                     .
                     .
                     .
    <CompositeMembership>
             <MemberOf TYPE="oracle_ias"
                   NAME="ias10g.myhost.example.com" ASSOCIATION=" "/>
    </CompositeMembership>
</Target>
```

Example 5–6   Oracle Directory Integration Platform Entry in a 10g (10.1.4.0.1)

```
<Target TYPE="oracle_eps_server"
       NAME="dip1014.myhost.example.com_DIP"
       DISPLAY_NAME="dip1014.myhost.example.com_DIP">
  <Property NAME="OracleHome" VALUE="C:\oracle\products\oim1014"/>
  <Property NAME="UserName" VALUE="013549bf4bf5c73c" ENCRYPTED="TRUE"/>
  <Property NAME="password" VALUE="fdfd90d00d859820" ENCRYPTED="TRUE"/>
  <Property NAME="host" VALUE="myhost"/>
  <Property NAME="ConnectDescriptor"
     VALUE="(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)
     (HOST=bigip41.example.com)
     (PORT=1251))(ADDRESS=(PROTOCOL=TCP)
     (HOST=bigip42.example.com)(PORT=1251))
     (LOAD_BALANCE=yes))(CONNECT_DATA=(SERVICE_NAME=newdb.example.com)))"/>
  <Property NAME="version" VALUE="10.1.4.0.1"/>
  <AssocTargetInstance ASSOC_TARGET="epsldap"
                    TYPE="oracle_ldap"
                    NAME="oid10g.myhost.example.com_LDAP"/>
  <CompositeMembership>
     <MemberOf TYPE="oracle_ias" NAME="ias10g.myhost.example.com"/>
  </CompositeMembership>
</Target>
```

5.5.7 Removing Unneeded Oracle Directory Integration Platform Template Profiles After Upgrade

All Oracle Directory Integration Platform 10*g* template profiles are upgraded to 11*g* during the upgrade process. These profiles can be deleted using Fusion Middleware Control, depending upon the needs of your environment.

Deleting these profiles is an optional step. Be sure not to delete any profiles that were actively being used in the 10g topology.

5.5.8 Deleting Oracle Internet Directory 10*g* Audit Log Container

The audit log container is obsolete for Oracle Identity Management 11g. You can delete the audit log container by running `bulkdelete` on the command-line as follows:

```
ORACLE_HOME/ldap/bin/bulkdelete connect="connect_string"
basedn="cn=auditlog"
```

5.5.9 Updating Oracle Internet Directory 10*g* Port Number in Oracle Enterprise Manager

You must update the Oracle Internet Directory 10*g* port numbers in the Oracle Enterprise, by running the following `opmnctl` command:

```
opmnctl updatecomponentregistration
```

For example:

```
ORACLE_INSTANCE/bin/opmnctl updatecomponentregistration -componentType OID
-componentName oid1 -adminHost myoidhostname -adminPort 7001 -adminUsername
weblogic -Port 389 -Sport 636
```

5.5.10 Configuring Oracle Single Sign-On 10*g* for Oracle Internet Directory 11*g*

After upgrading to Oracle Internet Directory 11*g*, if you want to use the Oracle Single Sign-On 10*g* then you must open the `ias.properties` file (Located at Oracle Single Sign-On 10*g* ORACLE_HOME) in a text editor and update the following parameters:

- `OIDport=` Enter the Oracle Internet Directory 11*g* port number.

- `OIDsslport=` Enter the Oracle Internet Directory 11*g* SSL port number.

5.6 Task 6: Verify the Oracle Internet Directory and Oracle Directory Integration Platform Upgrade

To verify that your Oracle Internet Directory and Oracle Directory Integration Platform upgrade was successful:

1. Run the Upgrade Assistant again and select **Verify Instance** on the Specify Operation page.

   Follow the instructions on the screen for information on how to verify that specific Oracle Fusion Middleware components are up and running.

   > **Note:** If the Oracle Internet Directory is configured only for SSL, then you cannot verify the Oracle Internet Directory using the Upgrade Assistant. You must manually verify by running the `ldapbind` command.

2. Use the Fusion Middleware Control to verify that the Oracle Internet Directory and Oracle Directory Integration Platform components are up and running.

   For more information, see "Getting Started Using Oracle Enterprise Manager Fusion Middleware Control" in the *Oracle Fusion Middleware Administrator's Guide*.

6

Upgrading Your Oracle Virtual Directory Environment

This chapter describes how to upgrade your existing Oracle Virtual Directory 10*g* (10.1.4.3) to Oracle Virtual Directory 11*g*.

This chapter contains the following sections:

- Task 1: Decide Upon an Oracle Virtual Directory Topology
- Task 2: Install and Configure Oracle Fusion Middleware 11g
- Task 3: Use Upgrade Assistant to Upgrade Oracle Virtual Directory
- Task 4: Complete Any Required Oracle Virtual Directory Post-Upgrade Tasks
- Task 5: Verify the Oracle Virtual Directory Upgrade

6.1 Task 1: Decide Upon an Oracle Virtual Directory Topology

Before you install Oracle Virtual Directory 11*g*, consider the topology you currently have in Oracle Application Server 10*g* (10.1.4.3), as well as any requirements for your Oracle Fusion Middleware 11*g* environment.

Note that you can configure Oracle Virtual Directory with Oracle WebLogic Server domain or you can configure it without a domain.

For more information, refer to Chapter 4.3, "Oracle Virtual Directory Topologies".

6.2 Task 2: Install and Configure Oracle Fusion Middleware 11*g*

The following sections describes how to install and configure new Oracle Fusion Middleware 11*g* middle tier instances in preparation for an upgrade to Oracle Fusion Middleware 11*g*:

- Installing Oracle WebLogic Server Software and Creating the Middleware Home
- Installing Oracle Virtual Directory 11g Release 1 (11.1.1.6.0)

6.2.1 Installing Oracle WebLogic Server Software and Creating the Middleware Home

For information on installing the Oracle WebLogic Server, see "Preparing for Installation" and "Running the Installation Program in Graphical Mode" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

For more information about the Middleware home, see "Understanding Oracle Fusion Middleware Concepts" in the *Oracle Fusion Middleware Administrator's Guide*.

6.2.2 Installing Oracle Virtual Directory 11*g* Release 1 (11.1.1.6.0)

For complete instructions for installing the Oracle Virtual Directory 11*g*, including all the prerequisites and system requirements, refer to the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

6.3 Task 3: Use Upgrade Assistant to Upgrade Oracle Virtual Directory

The Oracle Fusion Middleware Upgrade Assistant automates the upgrade of many aspects of your Oracle Application Server 10*g* environment.

The Upgrade Assistant is installed into the `bin` directory of your Oracle Fusion Middleware Oracle home.

The following sections provide more information:

- Task 3a: Stop the Oracle Virtual Directory Instances
- Task 3b: Start the Upgrade Assistant for an Oracle Virtual Directory Upgrade
- Task 3c: Upgrade Oracle Virtual Directory

6.3.1 Task 3a: Stop the Oracle Virtual Directory Instances

Before you start the Upgrade Assistant, the Oracle Virtual Directory instance that you are about to upgrade must be stopped.

You must stop Oracle Virtual Directory manually for Linux and Windows, before you start the Upgrade Assistant.

For more information, refer to the section, "Starting & Stopping Oracle Virtual Directory" in the *Oracle Virtual Directory Installation Guide*, which is available in the Oracle Identity Management 10*g* (10.1.4.0.1) documentation library on the Oracle Technology Network (OTN):

http://download.oracle.com/docs/cd/B28196_01/index.htm

6.3.2 Task 3b: Start the Upgrade Assistant for an Oracle Virtual Directory Upgrade

To start the Upgrade Assistant using the graphical user interface:

> **Note:** You can also use the Upgrade Assistant command-line interface to upgrade your Oracle Application Server 10*g* Oracle homes. For more information, see "Using the Upgrade Assistant Command-Line Interface" in the *Oracle Fusion Middleware Upgrade Planning Guide*.

1. Change directory the *ORACLE_HOME*/bin directory of the Oracle Fusion Middleware installation.

2. Enter the following command to start the Upgrade Assistant.

   On UNIX system:

   ```
   ./ua
   ```

   On Windows systems:

   ```
   ua.bat
   ```

The Upgrade Assistant displays the Welcome screen as shown in Figure 6–1

Figure 6–1   Upgrade Assistant Welcome Screen
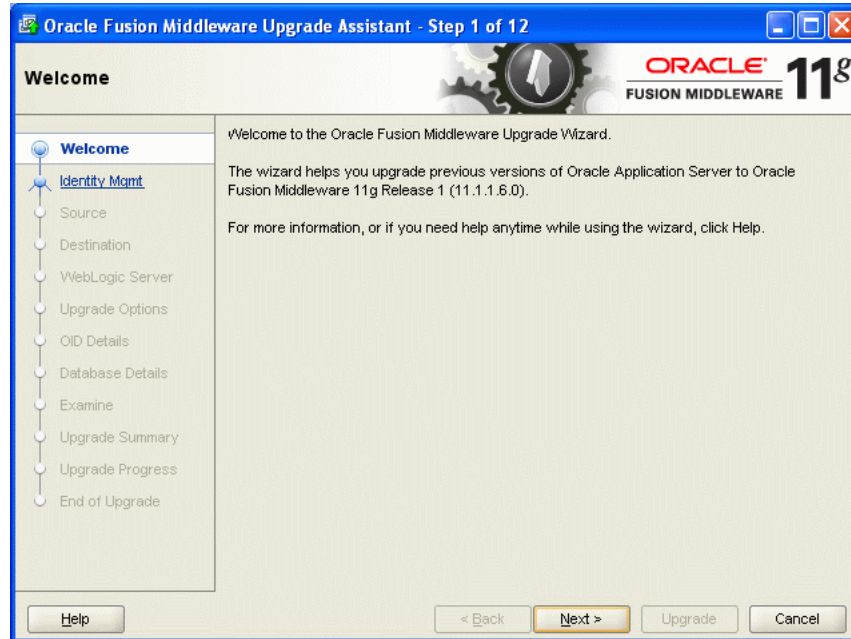
3. Click **Next** to display the Specify Operation screen (Figure 6–2).

   The options available in the Upgrade Assistant are specific to the Oracle home from which it started. When you start Upgrade Assistant from an Oracle Identity Management Oracle home, the options shown on the Specify Operation screen are the valid options for an Oracle Identity Management Oracle home.

Figure 6–2   Upgrade Assistant Specify Operation Screen for an Oracle Virtual Directory Upgrade
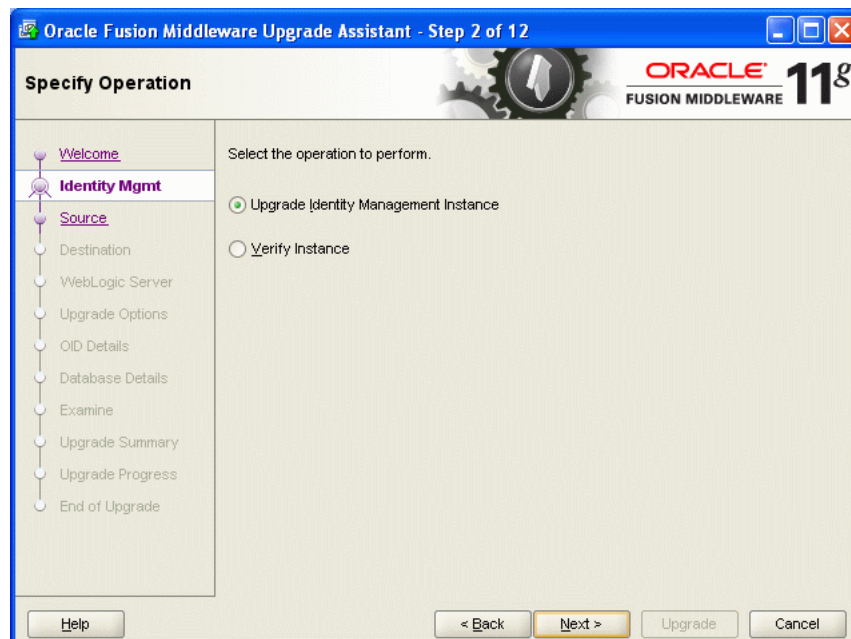
6.3.3 Task 3c: Upgrade Oracle Virtual Directory

To upgrade Oracle Virtual Directory:

1. Start the Upgrade Assistant as described in Task 3b: Start the Upgrade Assistant for an Oracle Virtual Directory Upgrade.

2. Select **Upgrade Identity Management Instance** on the Specify Operation screen (Figure 6–2).

3. Refer to Table 6–1 for a description of the Upgrade Assistant screens that require input from you during an Oracle Virtual Directory upgrade.

4. After you provide all required input, the Upgrade Assistant performs the following tasks:

   - Examines the components and schemas to be upgraded and verifies that they can be upgraded successfully.

   - Provides a summary of the components to be upgraded so you can verify that Upgrade Assistant is upgrading the components and schemas you expect.

   - Provides a progress screen so you can see the status of the upgrade as it proceeds.

   - Alerts you of any errors or problems that occur during the upgrade.

      See Also: "Troubleshooting Your Upgrade" in the *Oracle Fusion Middleware Upgrade Planning Guide* for specific instructions for troubleshooting problems that occur while running the Upgrade Assistant

   - Displays the End of Upgrade screen, which confirms that the upgrade was complete.

Table 6–1   Upgrade Assistant Screens That Require Input During an Oracle Virtual Directory Upgrade

Upgrade Assistant Screen	Description
Specify Source Home	Select the 10*g* (10.1.4.3) source Oracle home.
	If the Oracle home you want to upgrade does not appear in the drop-down lists, see "Source Oracle Home Not Listed by OracleAS Upgrade Assistant" in the *Oracle Fusion Middleware Upgrade Planning Guide*.
Specify Destination Instance	Enter the complete path to the destination 11*g* Oracle instance that you installed inside the middleware home. This is the Oracle instance that contains the Oracle Virtual Directory software.
	Alternatively, click **Browse** to select the Oracle instance.
Specify WebLogic Server	Enter the host, Administration Server port, and administration user credentials for the Oracle WebLogic Server domain you configured in Section 6.2.1, "Installing Oracle WebLogic Server Software and Creating the Middleware Home".
	This screen appears only if you chose to associate the Oracle Virtual Directory 11*g* instance with Oracle WebLogic Server during the Oracle Virtual Directory installation.
	It does not appear if you selected to install Oracle Virtual Directory without an Oracle WebLogic Server domain.

Table 6–1   (Cont.) Upgrade Assistant Screens That Require Input During an Oracle Virtual Directory Upgrade

Upgrade Assistant Screen	Description
Warning Dialog Box	The Upgrade Assistant displays this warning dialog box if the source Oracle home contains Oracle Application Server components that are not installed and configured in the destination Oracle instance.
	This warning appears, for example, if the source Oracle home contains an instance of Oracle HTTP Server, which is not available in the 11*g* Oracle home.
	If the information in the dialog box is accurate and you understand which components will be upgraded, click **Yes** to continue. Otherwise, click **No** and verify which components are installed and configured in each 11*g* Oracle instance.
Specify Upgrade Options	This screen offers these upgrade options:
	■ **Use source Oracle home ports in destination:** If you want to migrate the port assignments used by your Oracle Application Server 10g Oracle home to your new Oracle Fusion Middleware Oracle instance. Note if you select this option, you will not be able to run both the 10*g* and 11*g* middle tiers at the same time; otherwise, port conflicts will occur. If you do not select this option, then you will have to manually reconfigure the port number on every middle tier.
	■ **Start destination components after successful upgrade:** if you want the Upgrade Assistant to automatically start the components in the destination Oracle home after the upgrade is complete. If you do not select this option, then you will have to manually start the destination instance after the upgrade.
	Click **Help** to display more information about the upgrade options on this screen.

6.4 Task 4: Complete Any Required Oracle Virtual Directory Post-Upgrade Tasks

After you upgrade Oracle Virtual Directory by running the Upgrade Assistant, you must perform the following post-upgrade tasks:

■ Configuring Anonymous Ciphers for Oracle Virtual Directory SSL Listeners

■ Starting Oracle Virtual Directory After Upgrade When Using Privileged Ports

■ Upgrading Oracle Virtual Directory Logging Configuration Settings

6.4.1 Configuring Anonymous Ciphers for Oracle Virtual Directory SSL Listeners

Oracle Virtual Directory 10*g* (10.1.4.3) and later LDAP SSL listeners supports anonymous ciphers (in no-auth SSL mode) by default. The list of enabled cipher suites are set in Oracle Virtual Directory start-up scripts:

■ `vde_start.sh` on UNIX systems

■ `OViDServer.lax` on Windows systems

The list of ciphers can be modified by editing the `-D` Java system property `vde.ldap.ciphers` in these start-up scripts. This list is applicable across all LDAP SSL listeners. There was no option to enable different cipher suites for each LDAP listener.

In Oracle Virtual Directory 11*g*, the `vde.ldap.ciphers` Java system property is no longer supported. Instead, you can enable different cipher suites for each Oracle Virtual Directory listener when configuring SSL with Oracle Enterprise Manager Fusion Middleware Control or with the WLST command-line tool.

Anonymous cipher suites are disabled on Oracle Virtual Directory SSL listeners for security, by default. For information on enabling anonymous ciphers as part of configuring SSL security for your Oracle Virtual Directory environment, see "SSL Configuration in Oracle Fusion Middleware" in the *Oracle Fusion Middleware Administrator's Guide*.

6.4.2 Starting Oracle Virtual Directory After Upgrade When Using Privileged Ports

If you select the **Use source Oracle home ports in destination** option when upgrading an Oracle Virtual Directory 10*g* instance that is configured to listen on privileged ports, then the Upgrade Assistant cannot start Oracle Virtual Directory 11*g* after the upgrade.

Instead, the following error message appears in the Oracle Virtual Directory log file:

```
Cannot start Oracle Virtual Directory server: Permission denied.
```

To start an Oracle Virtual Directory 11*g* instance that is listening on privileged ports, perform the following steps:

1. Stop Oracle Process Manager and Notification Server (OPMN) and its managed processes, by using the following command in the Oracle instance directory where Oracle Virtual Directory 11*g* is configured:

   ORACLE_INSTANCE/bin/opmnctl stopall

2. Execute following commands as root:

   To start OPMN:

   ORACLE_INSTANCE/bin/opmnctl start

   Start Oracle Virtual Directory 11*g*:

   ORACLE_INSTANCE/bin/opmnctl startproc ias-component=*OVDCompName*

   In this example, replace *OVDCompName* with the name of the Oracle Virtual Directory instance.

For more information, see "Managing Oracle Virtual Directory Server Processes" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*.

6.4.3 Upgrading Oracle Virtual Directory Logging Configuration Settings

When you upgrade Oracle Virtual Directory, the logging settings you configured in Oracle Virtual Directory 10*g* are not upgraded.

Instead you will find that after upgrade:

- The log levels in the upgraded Oracle Virtual Directory 11*g* instance are set to "Notification", and the access log is enabled by default after upgrade, irrespective of its configuration in Oracle Virtual Directory 10*g*.

  To disable the access log, modify log level of logger name `com.octetstring.accesslog` to "ERROR:1".

For more information, see "Managing Oracle Virtual Directory Logging and Auditing" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*.

- If the Oracle Virtual Directory Dump Transactions plug-in is configured, then the log level for the plug-in must be changed to one of the following values: SEVERE, WARNING, INFO, FINE, FINER, or FINEST.

  For more information, see "Using the Dump Transactions Plug-In to Gather Information About Data Transformation Errors" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*.

6.5 Task 5: Verify the Oracle Virtual Directory Upgrade

To verify that your Oracle Virtual Directory upgrade was successful:

1. Run the Upgrade Assistant again and select **Verify Instance** on the Specify Operation page.

   Follow the instructions on the screen for information on how to verify that specific Oracle Fusion Middleware components are up and running.

2. Use the Fusion Middleware Control to verify that the Oracle Virtual Directory components are up and running.

   For more information, see "Getting Started Using Oracle Enterprise Manager Fusion Middleware Control" in the *Oracle Fusion Middleware Administrator's Guide*.

7

Upgrading Your Oracle Identity Federation Environment

This chapter describes how to upgrade your existing 10*g* (10.1.4.0.1) Oracle Identity Federation to Oracle Identity Federation 11*g*.

This chapter contains the following sections:

- Task 1: Decide Upon an Oracle Identity Federation Topology
- Task 2: Use the Repository Creation Utility to Install the Oracle Identity Federation Schema in the Database
- Task 3: Install and Configure Oracle Fusion Middleware 11g
- Task 4: Use the Upgrade Assistant to Upgrade Oracle Identity Federation
- Task 5: Complete Any Required Oracle Identity Federation Post-Upgrade Tasks
- Task 6: Verify the Oracle Identity Federation Upgrade

7.1 Task 1: Decide Upon an Oracle Identity Federation Topology

Before you install Oracle Identity Federation 11*g*, consider the topology you currently have in Oracle Application Server 10*g* (10.1.4.0.1), as well as any requirements for your Oracle Fusion Middleware 11*g* environment.

For more information, refer to Chapter 4.4, "Oracle Identity Federation Topologies".

7.2 Task 2: Use the Repository Creation Utility to Install the Oracle Identity Federation Schema in the Database

Before you can upgrade to Oracle Identity Federation 11*g*, you must first install the Oracle Identity Federation schema into a supported database.

For more information, see "Upgrading and Preparing Your Databases" in the *Oracle Fusion Middleware Upgrade Planning Guide*.

For more information about installing the Oracle Identity Federation schema, refer to the following sections:

- Verifying that the Database Meets the Minimum Requirements for the Oracle Identity Federation Schema
- Running the Repository Creation Utility in Preparation for Upgrading Oracle Identity Federation

7.2.1 Verifying that the Database Meets the Minimum Requirements for the Oracle Identity Federation Schema

Before performing any installation you should read the system requirements and certification documentation to ensure that your environment meets the minimum installation requirements for the products you are installing.

For more information, refer to "System Requirements and Specifications" in the *Oracle Fusion Middleware Installation Planning Guide*.

7.2.2 Running the Repository Creation Utility in Preparation for Upgrading Oracle Identity Federation

To run the Repository Creation Utility to install the Oracle Identity Federation schema in the database, refer to the following resources:

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

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

After you start the Repository Creation Utility, follow the instructions on the Repository Creation Utility screens to connect to the database and create the required schemas.

During the installation of the schema, note the following:

- On the Select Components screen, ensure that you select the **Oracle Identity Federation** schema.

- No other schemas are required unless you plan to use this database for installing other Oracle Fusion Middleware 11*g* components.

7.3 Task 3: Install and Configure Oracle Fusion Middleware 11*g*

The following sections describes how to install and configure new Oracle Fusion Middleware 11*g* middle tier instances in preparation for an upgrade to Oracle Fusion Middleware 11*g*:

- Task 3a: Install Oracle WebLogic Server Software and Create the Middleware Home

- Task 3b: Install Oracle Identity Federation 11g Release 1 (11.1.1.6.0)

- Task 3e: Create an Oracle HTTP Server Instance and Link It to Oracle Identity Federation 11g

7.3.1 Task 3a: Install Oracle WebLogic Server Software and Create the Middleware Home

For information on installing the Oracle WebLogic Server, see "Preparing for Installation" and "Running the Installation Program in Graphical Mode" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

7.3.2 Task 3b: Install Oracle Identity Federation 11*g* Release 1 (11.1.1.6.0)

For installing Oracle Identity Management, refer to the section "Installing and Configuring Oracle Identity Management (11.1.1.6.0)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

7.3.3 Task 3e: Create an Oracle HTTP Server Instance and Link It to Oracle Identity Federation 11*g*

For specific instructions, refer to "Create and Manage Oracle HTTP Server" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*.

7.4 Task 4: Use the Upgrade Assistant to Upgrade Oracle Identity Federation

The Oracle Fusion Middleware Upgrade Assistant automates the upgrade of many aspects of your Oracle Application Server 10*g* environment.

The Upgrade Assistant is installed automatically into the `bin` directory of your Oracle Fusion Middleware Oracle home.

You run the Upgrade Assistant once for each Oracle Application Server 10*g* Oracle home that you are upgrading. For example, if you are upgrading two different 10*g* Release 2 (10.1.2) Oracle homes that are a part of the same 10*g* Release 2 (10.1.2) farm, then you would run the Upgrade Assistant two times, once for each of the 10*g* Release 2 (10.1.2) Oracle homes.

Similarly, if you configure multiple Oracle instances in your new Oracle Fusion Middleware 11*g* environment, you must run the Upgrade Assistant once for each Oracle instance.

> **Note:** If you have configured more than one data store, Authentication Engine, or SP Engine in your Oracle Identity Federation environment, the Upgrade Assistant will upgrade only the enabled resources to 11*g*. Any additional data stores, authentication engines, or SP engines that are configured, but not enabled, will not be upgraded to the new Oracle Identity Federation 11*g* environment.
>
> After you upgrade, you can reconfigure the resources that were not upgraded. In addition, unlike Oracle Identity Federation 10g, you can enable more than one of these resources at a time in 11*g*.

The following sections provide more information:

- Task 4a: Start the Upgrade Assistant for an Oracle Identity Federation Upgrade
- Task 4b: Upgrade Oracle Identity Federation

7.4.1 Task 4a: Start the Upgrade Assistant for an Oracle Identity Federation Upgrade

To start the Upgrade Assistant using the graphical user interface:

> **Note:** You can also use the Upgrade Assistant command-line interface to upgrade your Oracle Application Server 10*g* Oracle homes. For more information, see "Using the Upgrade Assistant Command-Line Interface" in the *Oracle Fusion Middleware Upgrade Planning Guide*.

1. Change directory the *ORACLE_HOME*/bin directory of the Oracle Fusion Middleware installation.

2. Enter the following command to start the Upgrade Assistant.

On UNIX system:

`./ua`

On Windows systems:

`ua.bat`

The Upgrade Assistant displays the Welcome screen as shown in Figure 7–1

Figure 7–1   Upgrade Assistant Welcome Screen
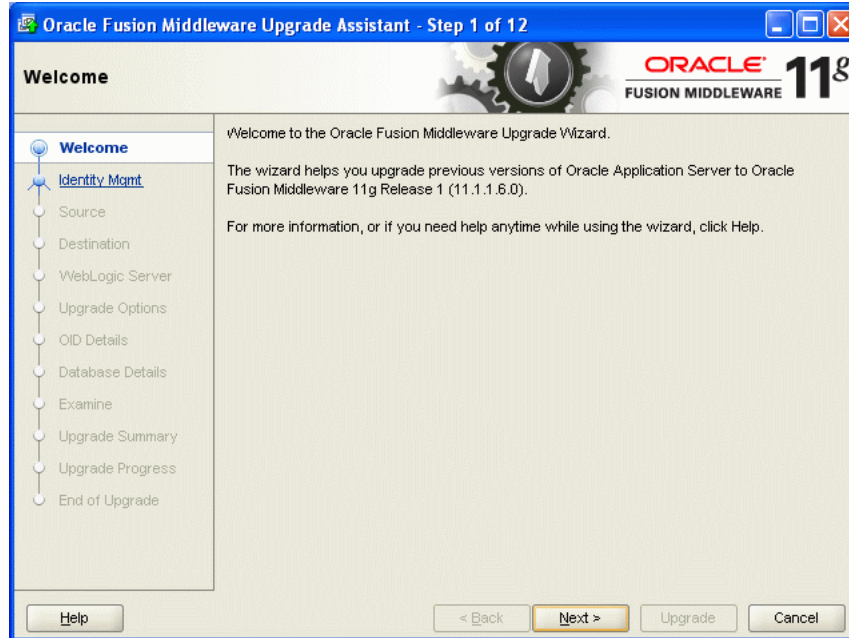
3. Click **Next** to display the Specify Operation screen (Figure 7–2).

   The options available in the Upgrade Assistant are specific to the Oracle home from which it started. When you start Upgrade Assistant from an Oracle Identity Management Oracle home, the options shown on the Specify Operation screen are the valid options for an Oracle Identity Management Oracle home.

Figure 7–2   Upgrade Assistant Specify Operation Screen for an Oracle Identity Federation Upgrade
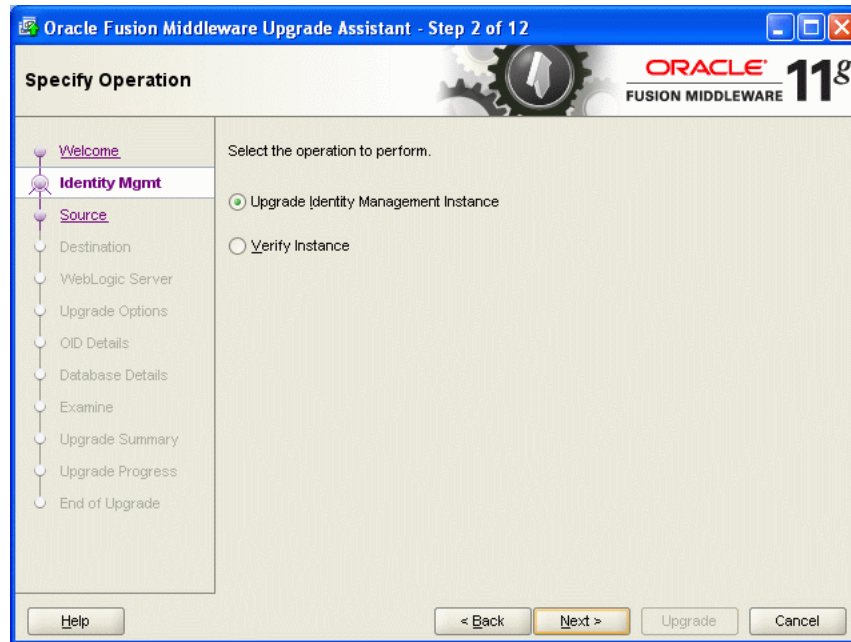
7.4.2 Task 4b: Upgrade Oracle Identity Federation

When you upgrade Oracle Identity Federation, the Upgrade Assistant upgrades the configuration files in the Oracle Identity Federation middle tier.

To upgrade Oracle Identity Federation when they reside in the same Oracle instance:

1. Start the Upgrade Assistant as described in Task 4a: Start the Upgrade Assistant for an Oracle Identity Federation Upgrade.

2. Select **Upgrade Identity Management Instance** on the Specify Operation screen (Figure 7–2).

3. Refer to Table 7–1 for a description of the Upgrade Assistant screens that require input from you during an Oracle Identity Federation upgrade.

4. After the Specify Upgrade Options screen, the Upgrade Assistant performs the following tasks and provides the progress on each task:

   - Examines the components and schemas to be upgraded and verifies that they can be upgraded successfully.

   - Provides a summary of the components to be upgraded so you can verify that Upgrade Assistant is upgrading the components and schemas you expect.

   - Provides a progress screen so you can see the status of the upgrade as it proceeds.

   - Alerts you of any errors or problems that occur during the upgrade.

     See Also: "Troubleshooting Your Upgrade" in the *Oracle Fusion Middleware Upgrade Planning Guide* for specific instructions for troubleshooting problems that occur while running the Upgrade Assistant

- Displays the End of Upgrade screen, which confirms that the upgrade was complete.

5. Exit the Upgrade Assistant.

Table 7–1 Upgrade Assistant Screens That Require Input During an Oracle Internet Directory and Oracle Directory Integration Platform Upgrade

Upgrade Assistant Screen	Description
Specify Source Home	Select the 10*g* (10.1.4.0.1) source Oracle home.
	If the Oracle home you want to upgrade does not appear in the drop-down lists, see "Source Oracle Home Not Listed by OracleAS Upgrade Assistant" in the *Oracle Fusion Middleware Upgrade Planning Guide.*
Specify Destination Instance	Enter the complete path to the destination 11*g* Oracle home that you installed inside the middleware home. This is the Oracle home that contains the Oracle Identity Federation software.
	Alternatively, click **Browse** to select the directory.
Specify WebLogic Server	Enter the host, Administration Server port, and administration user credentials for the Oracle WebLogic Server domain you configured in Section 7.3, "Task 3: Install and Configure Oracle Fusion Middleware 11g".
Warning Dialog Box	The Upgrade Assistant displays this warning dialog box if the source Oracle home contains Oracle Application Server components that are not installed and configured in the destination Oracle instance.
	This warning appears, for example, if the source Oracle home contains an instance of Oracle HTTP Server, which is not available in the 11*g* Oracle home.
	If the information in the dialog box is accurate and you understand which components will be upgraded, click **Yes** to continue. Otherwise, click **No** and verify which components are installed and configured in each 11*g* Oracle instance.
Specify Upgrade Options	This screen offers these upgrade options:
	- **Use source Oracle home ports in destination:** If you want to migrate the port assignments used by your Oracle Application Server 10g Oracle home to your new Oracle Fusion Middleware Oracle instance.
	Note that Oracle recommends that you always select this option when upgrading Oracle Identity Federation.
	- **Start destination components after successful upgrade:** if you want the Upgrade Assistant to automatically start the components in the destination Oracle home after the upgrade is complete. If you do not select this option, then you will have to manually start the destination instance after the upgrade.
	Click **Help** to display more information about the upgrade options on this screen.

7.5 Task 5: Complete Any Required Oracle Identity Federation Post-Upgrade Tasks

The following sections describe the manual upgrade steps required when you upgrading to Oracle Identity Federation 11*g*:

- Integrating Oracle Identity Federation 11g with Oracle Access Manager 10g

- Using a Custom Authentication Engine or Custom SP Engine with Oracle Identity Federation 11g

- Reconfiguring Oracle Single Sign-On Server After Upgrade to Work with Oracle Identity Federation 11g

- About Backwards Compatibility for ShareID Service URLs

- Upgrading Oracle Identity Federation SSL Configuration

- Setting Oracle Identity Federation System Properties After Upgrade

- Updating the Configuration File

- Additional Oracle Identity Federation Post-Upgrade Tasks

7.5.1 Integrating Oracle Identity Federation 11*g* with Oracle Access Manager 10*g*

If you were previously using Oracle Identity Federation 10*g* with Oracle Access Manager, you can use the following procedure to configure Oracle Identity Federation 11*g* so it can work successfully with your existing Oracle Access Manager 10*g* software.

Note that the steps described here are based on the instructions available in the section, "Deploying Oracle Identity Federation with Oracle Access Manager" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*.

To use Oracle Identity Federation 11*g* with Oracle Access Manager 10*g*:

1. Upgrade to Oracle Identity Federation 11*g* using the instructions in the previous sections of this chapter.

   Specifically, be sure you have installed and configured Oracle Identity Federation 11*g* and that you have used the Upgrade Assistant to upgrade the Oracle Identity Federation instance to 11*g*.

2. Optionally, use Oracle Access Manager 10*g* as the authentication engine for Oracle Identity Federation 11*g*.

   For specific instructions, refer to "Integrate Oracle Access Manager as an Authentication Engine" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*.

3. Optionally, integrate Oracle Access Manager 10*g* as an SP integration module.

   For specific instructions, refer to "Integrate Oracle Access Manager as an SP Integration Module" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*.

4. Optionally, configure Oracle Access Manager 10*g* so that protected resources are using the new Oracle Identity Federation 11*g* authentication schemes.

   To perform this task, use the instructions that help you verify the proper integration of Oracle Access Manager by allowing Oracle Identity Federation 11*g* to create policy objects and authentication schemes in Oracle Access Manager.

   These instructions are located in the section, "Integrate Oracle Identity Federation with Oracle Access Manager" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*.

5. When the integration with Oracle Access Manager is complete, delete any old access gates, authentication schemes, and policies for Oracle Identity Federation 10*g* from Oracle Access Manager 10*g*.

For more information, refer to the Oracle Access Manager documentation in the Oracle Identity Management 10*g* (10.1.4.0.1) documentation library, which is available on the Oracle Technology Network (OTN):

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

7.5.2 Using a Custom Authentication Engine or Custom SP Engine with Oracle Identity Federation 11*g*

If your Oracle Identity Federation 10*g* instance is integrated with a custom authentication engine, then use the information in the following sections to configure the custom authentication engine with Oracle Identity Federation 11*g*:

- Modifying the Authentication Engine Code
- Modifying the SP Engine Code
- Changes to the Logout Service for Authentication or SP Engines
- Deploying the Authentication or SP Engine
- Creating the Authentication Engine in Oracle Identity Federation 11g
- Creating the SP Engine in Oracle Identity Federation 11g

7.5.2.1 Modifying the Authentication Engine Code

The `HTTPServletRequestAttributes` available to the authentication engines Oracle Identity Federation 11*g* are different from those in 10*g*. As a result, you must modify the authentication engine code so it can read the attribute values from their new parameter names.

Refer to the following sections for more information:

- Changes to Parameters and Attributes Received by Oracle Identity Federation 11g
- New Incoming Attributes Supported by Oracle Identity Federation 11g
- Changes to Parameters and Attributes Sent to Oracle Identity Federation 11g
- Additional Attributes to Include in a Request to Oracle Identity Federation 11g

Changes to Parameters and Attributes Received by Oracle Identity Federation 11*g*

Table 7–2 shows the new and changed parameters used for authentication engines in Oracle Identity Federation 11*g*.

Table 7–2   Parameters and Attributes received from Oracle Identity Federation

Parameter or Attribute	Changes in Oracle Identity Federation 11*g*
`doneURL` `getUsrSess`	These query parameters are not available in 11*g*. In 11g, there is no need to consult these parameters to find where the user has to be forwarded after being identified by the authentication engine. In 11g, after successful authentication, the engine must forward the user to Oracle Identity Federation. To do this use the root context, `/fed`, and the relativePath, `/user/loginsso`.

Table 7–2   (Cont.) Parameters and Attributes received from Oracle Identity Federation

Parameter or Attribute	Changes in Oracle Identity Federation 11*g*
`authnMech`	This 10*g* query parameter has been changed to the following attribute in 11*g*: `oracle.security.fed.authn.authnmech` As a result, any occurrences of `request.getParameter("authnMech")` in the custom engine will have to be changed to the following: `request.getAttribute("oracle.security.fed.authn.authnmech")` In 10g, the value of the `authnMech` parameter was always as follows: `oracle:fed:authentication:password-protected` In 11g, the `oracle.security.fed.authn.authnmech` attribute can have other values. For more information, see "Configuring Authentication Mechanisms" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*.
`refID`	This 10*g* query parameter has been changed to the following attribute in 11*g*: `oracle.security.fed.authn.refid` As a result, any occurrences of `request.getParameter("refID")` in the custom engine will have to be changed to the following: `request.getAttribute("oracle.security.fed.authn.refid")`

New Incoming Attributes Supported by Oracle Identity Federation 11*g*

In addition to the changes described in Table 7–2, the following new incoming attributes are available in Oracle Identity Federation 11*g*; these attributes have no equivalents in Oracle Identity Federation 10*g*, but are available to the authentication engine in 11g:

■   oracle.security.fed.authn.providerid

■   oracle.security.fed.authn.providerdescription

■   oracle.security.fed.authn.engineid

■   oracle.security.fed.authn.userid

■   oracle.security.fed.authn.forceauthn

■   oracle.security.fed.authn.passive

■   oracle.security.fed.authn.attributes

■   oracle.security.fed.sessionid

For more information about these new attributes, see "Implementing the Service" the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*.

Changes to Parameters and Attributes Sent to Oracle Identity Federation 11*g*

The following attribute names must be changed after you upgrade to Oracle Identity Federation 11*g*:

■   Change `oracle.security.sso.sasso.uid` to `oracle.security.fed.authn.userid`

■   Change `oracle.security.sso.sasso.refID` to `oracle.security.fed.authn.refid`

■   Change `oracle.security.sso.sasso.authnMech` to `oracle.security.fed.authn.authnmech`

■   Change `oracle.security.sso.sasso.authnInst` to `oracle.security.fed.authn.authntime`

For example, suppose you have the following attribute in Oracle Identity Federation 11*g*:

```
request.setAttribute("oracle.security.sso.sasso.uid", userID)
```

For Oracle Identity Federation 11*g*, you must change this attribute as follows:

```
request.setAttribute("oracle.security.fed.authn.userid". userID);
```

For more information about the values that must be set by the authentication engine before doing an internal forward to Oracle Identity Federation 11*g*, see "Implementing the Service" the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*.

Additional Attributes to Include in a Request to Oracle Identity Federation 11*g*

In addition to the existing 10*g* attributes, Oracle Identity Federation 11*g* expects the additional attributes shown in Table 7–3 in each request.

Table 7–3   Additional Attributes to Include in a Request to Oracle Identity Federation 11g

Attribute	Description
oracle.security.fed.authn.expirationtime	Expiration time of the authenticated session as a Date Object
oracle.security.fed.authn.engineid	The identifier referencing the engine used to authenticate the user.
	The engine is created in the configuration of Oracle Identity Federation 11*g*. For more information, see Section 7.5.2.5, "Creating the Authentication Engine in Oracle Identity Federation 11g".
oracle.security.fed.authn.attributes	This optional map of attributes is stored in the user session. It will have String objects as the keys and Set of Objects as values.
oracle.security.fed.sessionid	This optional string contains the Oracle Identity Federation session identifier that Oracle Identity Federation will need to use to reference the user session.
	This allows the engine and the Oracle Identity Federation server to share the same identifier to reference the user session. Later, when the logout flow is being executed, Oracle Identity Federation will pass the `sessionID` that is being logged out to the engine, so that the engine can delete the data that was used for this user session.

7.5.2.2 Modifying the SP Engine Code

Similar to the its affect on authentication engines, the `HTTPServletRequestAttributes` available to the SP engines in Oracle Identity Federation 11*g* are different from those in 10*g*. As a result, you must modify the SP engine code so it can read the attribute values from their new parameter names.

Refer to the following sections for more information:

- Initiating a Federation SSO Operation
- Processing the Request from the Federation Server

Initiating a Federation SSO Operation

In Oracle Identity Federation 10*g*, if the Service Provider Engine did not find a valid user, then it initiated single sign-on by redirecting to the Oracle Identity Federation server function as the service provider. The URL it redirects to is as follows:

```
http://SP_HOST_NAME:SP_PORT/fed/sp/initiatesso
```

The following values are set to Oracle Identity Federation as query parameters:

- `providerid` – the provider ID of the IdP to use for single sign-on

- `returnurl` – the URL to which Oracle Identity Federation should send the user after single sign-on

In Oracle Identity Federation 11*g* these query parameters have changed:

- The `providerId` should now be specified as the `HTTPServletRequest` attribute `oracle.security.fed.sp.providerid`

- The `returnurl` query parameter no longer exists; instead, it can be specified in the `HTTPServelet` request attribute `oracle.security.fed.sp.relaystate`.

- There are additional attributes in Oracle Identity Federation 11*g* that can be passed to the Oracle Identity Federation servers when initiating single sign-on. These additional attributes are as follows:

  – oracle.security.fed.sp.authnmech

  – oracle.security.fed.sp.federationid

  – oracle.security.fed.sp.engineid

  – oracle.security.fed.sp.localauthn

  – oracle.security.fed.sp.usedefault

  – oracle.security.fed.sp.forceauthn

  – oracle.security.fed.sp.allowfedcreation

  – oracle.security.fed.sp.passive

  – oracle.security.fed.sp.requestbinding

  – oracle.security.fed.sp.responsebinding

  – oracle.security.fed.sp.authnmechcomparison

  – oracle.security.fed.sp.nameidformat

  For more information, see "Implementing the Service" the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*.

Processing the Request from the Federation Server

The following incoming parameter names for SP engines have changed in Oracle Identity Federation 11*g*:

- The `oracle.security.sso.sasso.uid` attribute has changed to `oracle.security.fed.sp.userid`

- `oracle.security.sso.sasso.authnInst` has changed to `oracle.security.fed.sp.authntime`

- `oracle.security.sso.sasso.expiryInst` has changed to `oracle.security.fed.sp.expirationtime`

- `oracle.security.sso.sasso.targetURL` is no longer available in Oracle Identity Federation 11*g*.

  The SP Engine can store the `targetURL` (to which the user will be forwarded) in `oracle.security.fed.sp.relaystate` before forwarding to Oracle Identity Federation to initiate an single sign-on operation. Oracle Identity Federation will pass this parameter back to the SP after doing an single sign-on.

The following additional, new parameters are available in Oracle Identity Federation 11*g* for the SP Engine to use. These new parameters include:

- oracle.security.fed.sp.authnresult
- oracle.security.fed.sp.authnmech
- oracle.security.fed.sp.attributes
- oracle.security.fed.sp.topstatus
- oracle.security.fed.sp.lowstatus
- oracle.security.fed.sp.statusmessage
- oracle.security.fed.sp.providerid
- oracle.security.fed.sp.engineid
- oracle.security.fed.sp.sessionid

For more information, see "Implementing the Service" the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*.

7.5.2.3 Changes to the Logout Service for Authentication or SP Engines

When using the logout service for an authentication or SP engine with Oracle Identity Federation 11*g*, consider the information in the following sections:

- Changes When the Engine Initiates a Logout
- Changes When Oracle Identity Federation Forwards to the Engine for Logout

Changes When the Engine Initiates a Logout

In Oracle Identity Federation 11*g*, an authentication or SP engine can initiate a logout operation. For more information, see "Logout" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*.

Changes When Oracle Identity Federation Forwards to the Engine for Logout

The following changes need to be made to the logout service of the authentication or SP engine if it is present:

- The `invokeOSFSLogout` parameter and the `doneUrl` parameters are no longer sent to the engine. In Oracle Identity Federation 11*g*, the engine should always perform an internal forward to the `/fed web context` and `/user/logoutretsso` relative path.

- The `engineId` of the invoked engine is available to the logout service through the http request attribute `oracle.security.fed.authn.engineid`

- The `oracle.security.fed.sessionid` HTTP request attribute can optionally contain the session identifier of the session being logged out.

- In Oracle Identity Federation 11*g*, the logout service should redirect the user to `/fed/user/logoutretsso` after logout rather than to the `/fed/user/logoutsso` URL.

- Specify the `engineId` in the attribute referenced by `oracle.security.fed.authn.engineid` (if the engine is an Authentication Engine) or `oracle.security.fed.sp.engineid` (if the engine is an SP Engine).

7.5.2.4 Deploying the Authentication or SP Engine

You deploy the authentication or SP engine just the same as you deploy any Java EE application. For more information, refer to "Deploying Applications" in the *Oracle Fusion Middleware Administrator's Guide*.

7.5.2.5 Creating the Authentication Engine in Oracle Identity Federation 11*g*

To create an authentication engine for Oracle Identity Federation 11*g*:

1. In Oracle Enterprise Manager Fusion Middleware Control, navigate to the Oracle Identity Federation home page.

   For more information, see "Getting Started Using Oracle Enterprise Manager Fusion Middleware Control" in the *Oracle Fusion Middleware Administrator's Guide*.

2. From the **Oracle Identity Federation** menu, select **Administration**, then **Authentication Engines**.

3. On the Custom Authentication Engines tab, click **Add** to create a new Authentication Engine, and then enter values for the following fields:

   - **Name** – a name for the engine

   - **Enabled** – selected

   - **Web Context** – the root context where the engine is deployed

   - **Authentication Relative Path** – the relative path to the engine

   - **Logout Enabled** – select this check box if the engine needs to perform logout when a logout operation is performed.

   - **Logout Relative Path** – the relative path of the engine logout service.

4. Click **Save**.

The Oracle Identity Federation server generates an Engine ID for the new engine. The Engine ID is the value of the `oracle.security.fed.authn.engineid` attribute that the custom engine needs to send to the Oracle Identity Federation server after authenticating the user.

7.5.2.6 Creating the SP Engine in Oracle Identity Federation 11*g*

To create an SP engine for Oracle Identity Federation 11*g*:

1. In Oracle Enterprise Manager Fusion Middleware Control, navigate to the Oracle Identity Federation home page.

   For more information, see "Getting Started Using Oracle Enterprise Manager Fusion Middleware Control" in the *Oracle Fusion Middleware Administrator's Guide*.

2. From the **Oracle Identity Federation** menu, select **Administration**, then **Service Provider Integration Modules**.

3. On the Custom SP Engines tab, click **Add** to create a new Authentication Engine, and then enter values for the following fields:

   - **Name** – a name for the engine

   - **Enabled** – selected

   - **Web Context** – the root context where the engine is deployed

   - **Authentication Relative Path** – the relative path to the engine

- **Logout Enabled** – select this check box if the engine needs to perform logout when a logout operation is performed.

- **Logout Relative Path** – the relative path of the engine logout service.

4. Click **Save**.

The Oracle Identity Federation server generates an Engine ID for the new engine. The Engine ID is the value of the `oracle.security.fed.sp.engineid` attribute that the custom engine needs to send to the Oracle Identity Federation server after authenticating the user.

7.5.3 Reconfiguring Oracle Single Sign-On Server After Upgrade to Work with Oracle Identity Federation 11*g*

If you are using Oracle Single Sign-On with Oracle Identity Federation 10*g*, then after you upgrade to Oracle Identity Federation 11*g*, you must reconfigure Oracle Single Sign-On.

This step is necessary because the values required for the `SASSOAuthnUrl` and `SASSOLogoutUrl` properties have changed for Oracle Identity Federation 11*g*.

For more information, see "Configuring Single Sign-On" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*.

7.5.4 About Backwards Compatibility for ShareID Service URLs

Oracle Identity Federation 10*g*, as well as SHAREid/COREid Federation 2.x, provided service URLs for its SAML 1.x and WS-Federation protocol support, which were different from the SAML 2.0 and Liberty 1.x service URLs.

These URLs have been modified in the 11g Oracle Identity Federation server for consistency with the SAML 2.0 and Liberty 1.x service URLs. This means that customers upgrading to Oracle Identity Federation 11*g*, who use SAML 1.x or WS-Federation, will need to inform their partner providers of the new single sign-on service URLs.

To ease that transition, Oracle Identity Federation 11*g* provides a separate module that allows backwards compatibility with the SHAREid service URLs. This module is an installable J2EE application that is deployed alongside Oracle Identity Federation, which will handle requests for the ShareID/Oracle Identity Federation 10*g* service URLs and redirect or forward them to the corresponding Oracle Identity Federation 11*g* service URLs.

For information on how to set up this application, see "Setting up Backwards Compatibility for Oracle Identity Federation 10g and ShareID service URLs" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*.

7.5.5 Upgrading Oracle Identity Federation SSL Configuration

If you are using a shareId keystore for SSL support in Oracle Virtual Directory 10*g*, then the Upgrade Assistant automatically imports the keystore into Oracle Identity Federation 10*g*.

If the SSL identity and trust keystores you use in Oracle Virtual Directory 10*g* are stored in the following location, then there are no additional tasks to perform:

`ORACLE_HOME/fed/shareid/oblix/config /keystore`

However, if the keystores are stored in any other location, then you must perform the following tasks:

1. Copy the identify and trust keystores to a subdirectory inside the following directory:

   WLS_HOME/user_projects/domains/*domain_name*/servers/*server_name*/stage/OIF

2. Configure Oracle WebLogic Server to point to the new keystore location, as follows:

   a. Log in to the Oracle WebLogic Server Administration Console and select **Environment**, then **Servers**.

   b. Select the server for which you want to set up SSL.

   c. In the Keystores section, select **Custom Identity and Custom Trust**.

   d. In the Identity section, fill in the properties as follows:

   Custom Identity Keystore: *location_of_keystore_containing_SSL_private key_ and_certificate*

   Custom Identity Keystore type: jks

   Custom Identity Keystore Passphrase: *storepassword*

   e. In the Trust section, fill in properties as follows:

   Custom Identity Keystore: *location_of_keystore_containing_the_trusted certificate_entries*

   Custom Identity Keystore type: jks

   Custom Identity Keystore Passphrase: *storepassword*

7.5.6 Setting Oracle Identity Federation System Properties After Upgrade

If you configured Oracle Identity Federation 10*g* by setting system properties, then you will have to manually configure those properties in the upgraded Oracle Identity Federation 11*g* instance. The Upgrade Assistant does not apply these settings to your 11*g* instance.

Table 7–4 lists the system properties that are not upgraded and explains how to set the equivalent properties in Oracle Identity Federation 11*g*. In many cases, the instructions refer to Oracle Enterprise Manager Fusion Middleware Control, the Oracle WebLogic Server Administration Console, or the WebLogic Scripting Tool (WLST), which are used to manage Oracle Fusion Middleware11*g* components.

For more information, see "Overview of Oracle Fusion Middleware Administration Tools" in the *Oracle Fusion Middleware Administrator's Guide*.

Note that these properties are documented in Section 9.3, "Managing Oracle Identity Federation Performance," in the *Oracle Identity Federation Administrator's Guide* for 10*g* (10.1.4.0.1). This document can be found in the Oracle Application Server 10*g* (10.1.4.0.1) documentation library on the Oracle Technology Network (OTN):

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

Table 7–4   Setting Oracle Identity Federation 10g System Properties in Oracle Identity Federation 11g

Oracle Identity Federation 10*g* System Property	How to Set the Property in Oracle Identity Federation 11*g*
-Dhttp.fed.host=*VALUE*	In Fusion Middleware Control, you can set this property as follows: 1. Navigate to the Oracle Identity Federation Home page. 2. From the **Oracle Identity Federation** menu, select **Administration**, then **Server Properties**. 3. Enter a value in the **Maximum SOAP Connection per Server** field.
-Dhttp.fed.max.conn=*VALUE*	In Fusion Middleware Control, you can set this property as follows: 1. Navigate to the Oracle Identity Federation Home page. 2. From the **Oracle Identity Federation** menu, select **Administration**, then **Server Properties**. 3. Enter a value in the **Maximum SOAP Connection** field.

-Dfed.ldap.ha=[true | false]	In Oracle Identity Federation 10*g*, you used this system property to set one flag for all datastores.
	In 11g you can set this flag seperately for the LDAP user datastore, LDAP federation datastore, and LDAP authentication engine.
	Enter the WLST script environment for the Oracle Identity Federation instance, and set the `ldaphaenabled`, `userldaphaenabled`, or `fedldaphaenabled` property to TRUE as follows:
	To enable this property for the LDAP authentication engine:
	`setConfigProperty('authnengines', 'ldaphaenabled',`
	`        'true', 'boolean')`
	To enable this for the LDAP user datastore:
	`setConfigProperty('datastore', 'userldaphaenabled',`
	`        'true', 'boolean')`
	For enabling this for LDAP federation datastore:
	`setConfigProperty('datastore', 'fedldaphaenabled',`
	`        'true', 'boolean')`

-Dfed.jdbc.min.conn=*VALUE* -Dfed.jdbc.max.conn=*VALUE* -Dfed.jdbc.max.usage=*VALUE*	Use the Oracle WebLogic Server Administration Console to set the appropriate values on the JDBC data source that you are using for your Oracle Identity Federation 11*g* datastores or authentication engines.

7.5.7 Updating the Configuration File

To update the configuration files, complete the following steps:

1. Set up the WLST Environment by executing the following commands:

   On UNIX:

   ```
   bash
   export $DOMAIN_HOME=PATH_TO_DOMAIN_HOME
   source $ORACLE_HOME/fed/scripts/setOIFEnv.sh
   ```

   Replace `ORACLE_HOME` with the correct path for your environment.

   On Windows:

   ```
   set DOMAIN_HOME=PATH_TO_DOMAIN_HOME
   ORACLE_HOME\fed\scripts\setOIFEnv.cmd
   ```

2. Run the following command:

```
java weblogic.WLST oif-upgrade-11.1.1.2.0-11.1.1.6.0.py
```

7.5.8 Additional Oracle Identity Federation Post-Upgrade Tasks

The following additional post-upgrade tasks should be performed after upgrading to Oracle Identity Federation 11*g*, in addition to those described in the *Oracle Fusion Middleware Upgrade Guide for Oracle Identity Management*:

- If you are have configured Oracle Identity Federation 10*g* to use the SAML 1.x/WS-FED protocol, then after you upgrade to Oracle Identity Federation 11*g*, you must set a default single sign-on identity provider.

  For more information, see "Configuring Service Providers" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*.

- Export the Identity Provider self-signed certificate to the service provider

  The procedure you use to perform this task varies, depending on whether your service provider is a 10*g* or 11*g* service provider:

  - If you are using a 10*g* service provider, then refer to "Exporting the IdP's self-signed certificate to the SP" in the *Oracle Identity Federation Administrator's Guide* in the Oracle Application Server 10*g* (10.1.4.0.1) documentation library on the Oracle Technology Network (OTN):

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

  - If you are using an 11*g* service provider, then refer to "Set Up Single Sign-On for SAML 1.x and WS-Federation" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*.

- If you are using an 11*g* Identity Provider and a 10*g* service provider, and you are using the SAML 1.x/WS-FED protocol, then you configure the 10g service provider.

  Specifically, for the 10*g* service provider, you must change the "Signing Certificate Subject DN" and "Signing Certificate Issuer DN" to 11g IdP format, which is of the form "CN=<host> Signing Certificate".

  For more information, see "Configure This Domain as a Source/Identity Provider" in the *Oracle Identity Federation Administrator's Guide* in the Oracle Application Server 10*g* (10.1.4.0.1) documentation library on the Oracle Technology Network (OTN).

- Enable "Send Signed Assertion" in Oracle Identity Federation 10*g*, or disable "Require Signed Assertions" in Oracle Identity Federation 11*g*.

  This task is necessary because in 10g, signed assertions are disabled by default, and in 11*g*, signed assertions are enabled by default.

  Depending whether you perform this task in 10*g* or 11*g*, refer to one the following:

  - "Configuring Service Providers" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*.

  - Section 6.5.5, "Add Assertion Profile" in the *Oracle Identity Federation Administrator's Guide* in the Oracle Application Server 10*g* (10.1.4.0.1) documentation library on the Oracle Technology Network (OTN).

7.6 Task 6: Verify the Oracle Identity Federation Upgrade

To verify that your Oracle Internet Directory and Oracle Directory Integration Platform upgrade was successful:

1. Run the Upgrade Assistant again and select **Verify Instance** on the Specify Operation page.

   Follow the instructions on the screen for information on how to verify that specific Oracle Fusion Middleware components are up and running.

2. Use the following URL to verify that Oracle Identity Federation 11*g* is up and running:

   ```
   http://<host>:<port>/fed/sp/metadata
   ```

   For example:

   ```
   http://host42.exmaple.com:7001/fed/sp/metadata
   ```

   Alternatively, you can use Fusion Middleware Control to verify that Oracle Identity Federation and any other Oracle Identity Management components are up and running in the Oracle Fusion Middleware environment.

   For more information, see "Getting Started Using Oracle Enterprise Manager Fusion Middleware Control" in the *Oracle Fusion Middleware Administrator's Guide*.

Part III

Upgrading Your Oracle Single Sign-On and Oracle Identity and Access Management Environments

Part III contains the following chapters:

8

Summary of Upgrade Process for Oracle Single Sign-On and Oracle Identity and Access Management

This chapter provides a high-level overview of the Oracle Single Sign-On and Oracle Identity and Access Management upgrade process. Refer to the following sections for more information:

- Flow Chart of the Oracle Single Sign-On and Oracle Identity and Access Management Upgrade Processes
- Table Describing the Steps in the Oracle Identity and Access Management Upgrade Process

8.1 Flow Chart of the Oracle Single Sign-On and Oracle Identity and Access Management Upgrade Processes

Figure 8–1 provides a flow chart of the Oracle Single Sign-On and Oracle Identity and Access Management upgrade process. Review this chart to get familiar with the steps you will be required to take, based on your existing version of Oracle Single Sign-On, Oracle Adaptive Access Manager, and Oracle Identity Manager.

Figure 8–1   Flow Chart of the Oracle Single Sign-On and Oracle Adaptive Access Manager Upgrade Processes
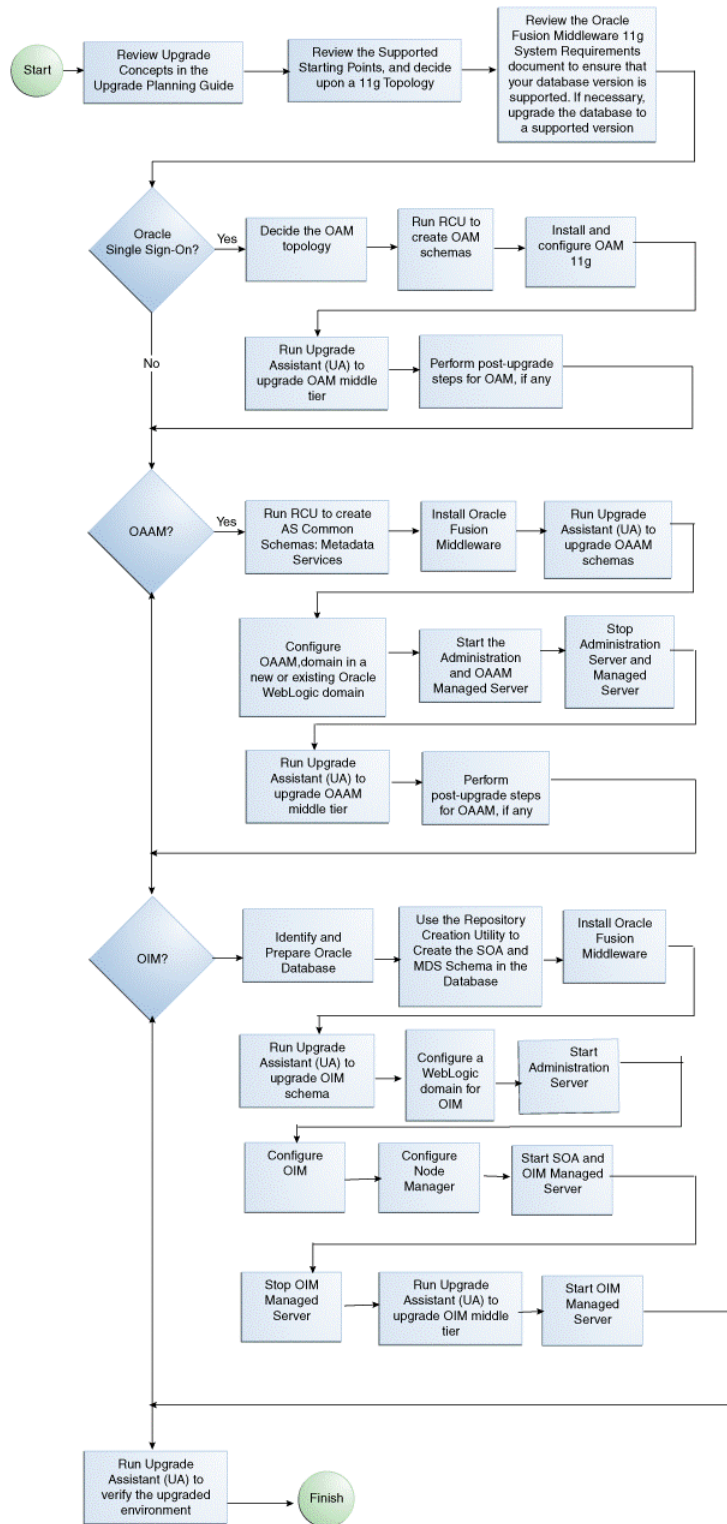
8.2 Table Describing the Steps in the Oracle Identity and Access Management Upgrade Process

Table 8–1 describes each of the steps in the upgrade process flow chart, which is shown in Figure 8–1. The table also provides information on where to get more information on each step in the process.

Table 8–1   Table Describing the Steps in the Oracle Identity Management *Upgrade Process*

Step	Description	More Information
Review Upgrade Concepts in the Upgrade Planning Guide	The *Oracle Fusion Middleware Upgrade Planning Guide* provides a high-level overview of how to upgrade your entire Oracle Application Server environment to Oracle Fusion Middleware. It includes compatibility information and instructions for upgrading any databases that support your middleware components.	*Oracle Fusion Middleware Upgrade Planning Guide*
Review the Supported Starting Points and 11*g* Topologies	Before starting your upgrade, you should be familiar with the new features, supported started points, and recommended topologies for Oracle Fusion Middleware 11*g*. Based this knowledge, you can then decide upon an 11*g* topology.	Chapter 9, "Supported Starting Points for Upgrading Oracle Single Sign-On and Oracle Identity and Access Management" Chapter 10, "Types of Environments for Oracle Single Sign-On and Oracle Identity and Access Management"
Decide Upon an 11*g* Identity Management Topology	Oracle Fusion Middleware 11*g* introduces a new architecture, based on Oracle WebLogic Server. As a result, you should review your current Oracle Application Server topology and decide upon an equivalent Oracle Fusion Middleware topology before you begin the upgrade process.	Chapter 10, "Types of Environments for Oracle Single Sign-On and Oracle Identity and Access Management"
If necessary, upgrade the Identity Management database to a supported database version	When you upgrade to Oracle Fusion Middleware 11*g*, the OracleAS Identity Management schemas are upgraded to 11*g*. As a result, before you upgrade, you must be sure the database that hosts the schemas is a supported version.	*Oracle Fusion Middleware Upgrade Planning Guide*
Oracle Single Sign-On?	You can only upgrade Oracle Single Sign-On to Oracle Access Manager, then be sure to follow the appropriate instructions in this guide.	Chapter 11, "Upgrading Oracle Single Sign-On Environment"
Install and Configure Oracle Access Manager 11*g*	Install and configure an instance of Oracle Access Manager 11*g* on the same host as the Oracle Application Server 10*g* installation or you can use a new host.	Section 11.6, "Task 4: Install and Configure the Oracle Access Manager Middle Tier"

Table 8–1   (Cont.) Table Describing the Steps in the Oracle Identity Management *Upgrade Process*

Step	Description	More Information
Use Upgrade Assistant to Upgrade Oracle Access Manager middle tier	Run the Upgrade Assistant from your new 11*g* Oracle home and upgrade the Oracle Single Sign-On 10*g*.	Section 11.7, "Task 5: Upgrade Oracle Access Manager Middle Tier Using Upgrade Assistant"
Perform any Post-Upgrade Oracle Access Manager Tasks	The Upgrade Assistant automates many of the upgrade procedures, but in some cases, there are additional, manual tasks that you might have to perform.	Section 11.8, "Task 6: Complete Any Required Oracle Access Manager Post-Upgrade Tasks"
Oracle Adaptive Access Manager?	If you are upgrading Oracle Adaptive Access Manager, then be sure to follow the appropriate instructions in this guide.	Chapter 12, "Upgrading Oracle Adaptive Access Manager Environment"
Install and Configure Oracle Adaptive Access Manager 11*g*	Install and configure an instance of Oracle Adaptive Access Manager 11*g* on the same host as the Oracle Application Server 10*g* installation.	Section 12.6, "Task 4: Install Oracle Fusion Middleware"
Use Upgrade Assistant to Upgrade Oracle Adaptive Access Manager schema and middle tier	Run the Upgrade Assistant from your new 11*g* Oracle home and upgrade the Oracle Adaptive Access Manager schemas and middle tiers.	Section 12.7, "Task 5: Use Upgrade Assistant to Upgrade the Oracle Adaptive Access Manager Schema" Section 12.11, "Task 9: Use Upgrade Assistant to Upgrade Oracle Adaptive Access Manager Middle Tier"
Perform any Post-Upgrade Oracle Adaptive Access Manager Tasks	The Upgrade Assistant automates many of the upgrade procedures, but in some cases, there are additional, manual tasks that you might have to perform.	Section 12.13, "Task 11: Complete Any Required Oracle Adaptive Access Manager Post-Upgrade Tasks"
Oracle Identity Manager?	If you are upgrading Oracle Identity Manager, then be sure to follow the appropriate instructions in this guide.	Chapter 13, "Upgrading Oracle Identity Manager Environment"
Install and Configure Oracle Identity Manager 11*g*	Install and configure an instance of Oracle Identity Manager 11*g*.	Section 13.5, "Task 3: Install Oracle Fusion Middleware" Section 13.7, "Task 5: Create a WebLogic Domain for Oracle Identity Manager" Section 13.9, "Task 7: Configure Oracle Identity Manager Server 11g"

Table 8–1 (Cont.) Table Describing the Steps in the Oracle Identity Management *Upgrade Process*

Step	Description	More Information
Use Upgrade Assistant to Upgrade Oracle Identity Manager schema and middle tier	Run the Upgrade Assistant from your new Oracle Identity and Access Management 11*g* Oracle home and upgrade the Oracle Identity Manager schemas and middle tiers.	Section 13.6, "Task 4: Use Upgrade Assistant to Upgrade the Oracle Identity Manager Schema" Section 13.14, "Task 12: Use Upgrade Assistant to Upgrade Oracle Identity Manager Middle Tier"
Perform any Post-Upgrade Oracle Identity Manager Tasks	The Upgrade Assistant automates many of the upgrade procedures, but in some cases, there are additional, manual tasks that you might have to perform.	Section 13.16, "Task 14: Complete Any Required Oracle Identity Manager Post-Upgrade Tasks"
Run Upgrade Assistant to verify the Upgraded Environment	You can use the Upgrade Assistant to validate the upgrade and verify that the upgraded environment is up and running successfully.	Section 11.9, "Task 7: Verify the Oracle Access Manager Upgrade" Section 12.14, "Task 12: Verify the Oracle Adaptive Access Manager Upgrade" Section 13.17, "Task 15: Verify the Oracle Identity Manager Upgrade"

9

Supported Starting Points for Upgrading Oracle Single Sign-On and Oracle Identity and Access Management

This chapter describes the supported starting points for Oracle Identity Management upgrade. This chapter contains the following sections:

- Supported Starting Points for Oracle Single Sign-On
- Supported Starting Points for Oracle Adaptive Access Manager
- Supported Starting Points for Oracle Identity Manager

> **Note:** The starting point patchsets listed in this chapter were the latest patchsets available at the time this guide was published.
>
> For a list of the latest patchsets available for your installation, refer to *My Oracle Support*.

9.1 Supported Starting Points for Oracle Single Sign-On

This guide provides instructions for upgrading from the Oracle Single Sign-On releases described in Table 9–1.

Table 9–1   Oracle Access Manager Releases Supported By This Guide

Release	Description or Notes
Oracle Single Sign-On 10*g* (10.1.2) and 10*g* (10.1.4)	This version of Oracle Single Sign-On was available as part of Oracle Application Server 10*g* Release 2 (10.1.2.3) and 10*g* (10.1.4).

9.2 Supported Starting Points for Oracle Adaptive Access Manager

This guide provides instructions for upgrading from the Oracle Adaptive Access Manager releases described in Table 9–2.

Table 9–2   Oracle Adaptive Access Manager Releases Supported By This Guide

Release	Description or Notes	Latest Patchset
10*g* (10.1.4.5)	This version of Oracle Adaptive Access Manager was available as a standalone product.	Bundle Patch 7 Oracle Adaptive Access Manager 10*g* (10.1.4.5.2) is the latest patchset release.

9.3 Supported Starting Points for Oracle Identity Manager

This guide provides instructions for upgrading from the Oracle Identity Manager releases described in Table 9–3.

Table 9–3   Oracle Identity Manager Releases Supported By This Guide

Release	Description or Notes	Latest Patchset
9.1.0.1 and 9.1.0.2	This version of Oracle Identity Manager was available as part of Oracle Application Server 10*g* Release 2 (10.1.2.3) and 10*g* (10.1.4).	Bundle Patch 11 Oracle Identity Manager 9.1.0.1 and Bundle Patch 14 Oracle Identity Manager 9.1.0.2 are the latest patchset releases.

10

Types of Environments for Oracle Single Sign-On and Oracle Identity and Access Management

This chapter describes the most common topologies for Oracle Identity Management 10*g* and how they compare with equivalent topologies in Oracle Fusion Middleware 11*g*.

This chapter contains the following sections:

- Oracle Single Sign-On Topologies
- Oracle Adaptive Access Manager Topologies
- Oracle Identity Manager Topologies

10.1 Oracle Single Sign-On Topologies

Figure 10–1 compares a typical Oracle Single Sign-On topology in Oracle Application Server 10*g* with a Oracle Access Manager topology in Oracle Fusion Middleware 11*g*.

Figure 10–1   Comparison of Typical Oracle Single Sign-On Topologies in Oracle Application Server 10g and Oracle Fusion Middleware 11g
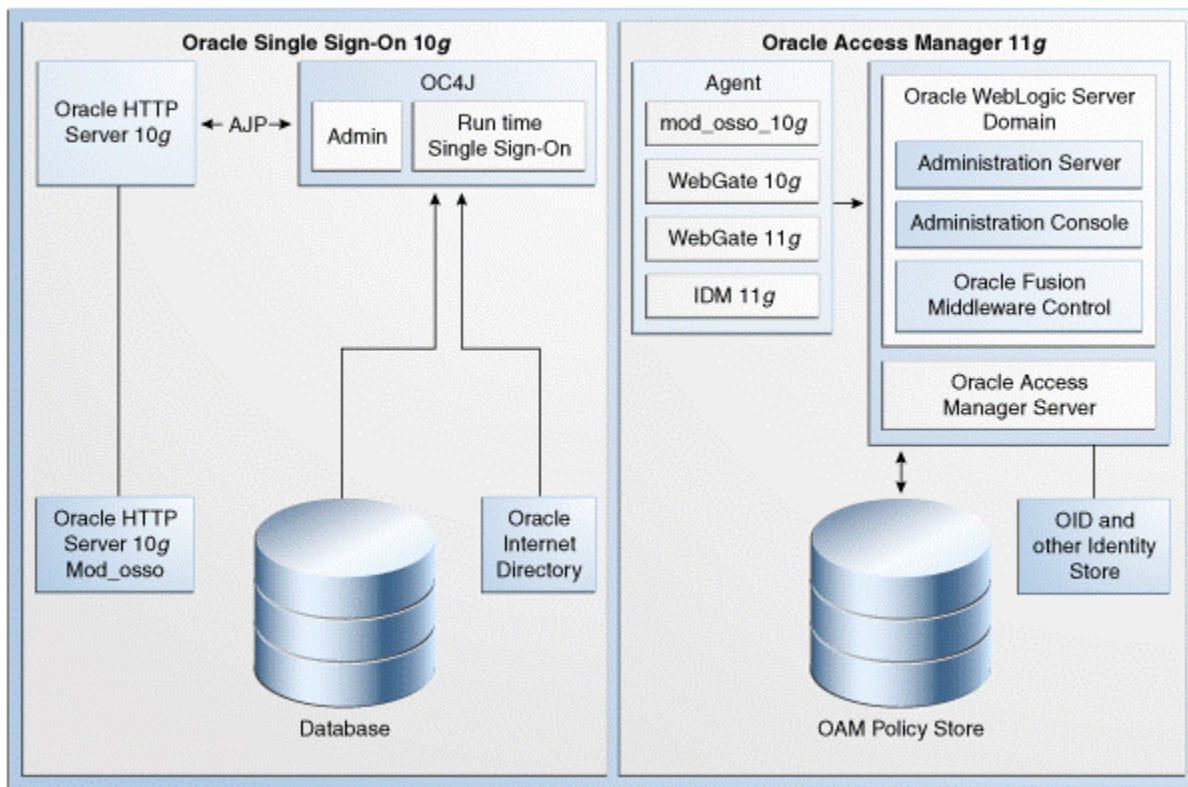
10.2 Oracle Adaptive Access Manager Topologies

Figure 10–2 compares a typical Oracle Adaptive Access Manager topology in Oracle Application Server 10g with a similar topology in Oracle Fusion Middleware 11g.

Figure 10–2   Comparison of Typical Oracle Adaptive Access Manager Topologies in Oracle Application Server 10g and Oracle Fusion Middleware 11g
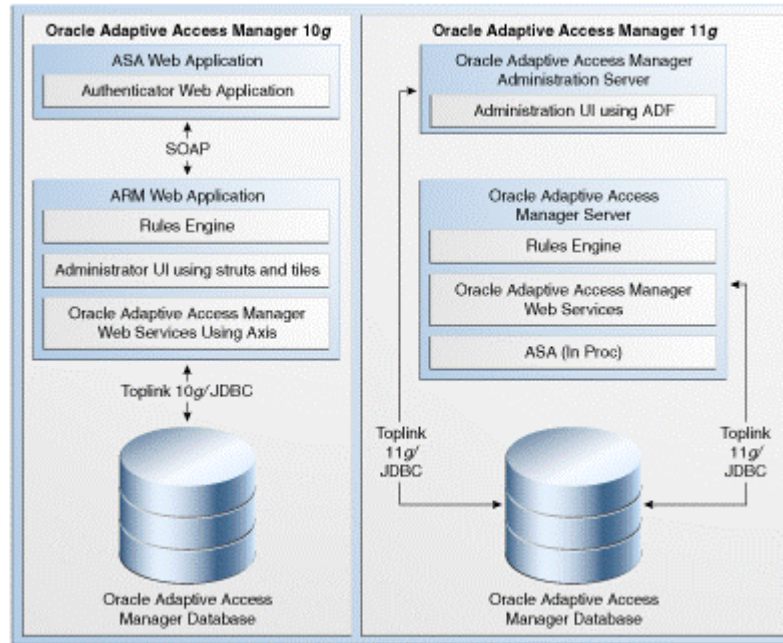
10.3 Oracle Identity Manager Topologies

Figure 10–3 and Figure 10–4 compares a typical Oracle Identity Manager topology in Oracle Application Server 10g with a similar topology in Oracle Fusion Middleware 11g.

Figure 10–3   Oracle Identity Manager 9.1
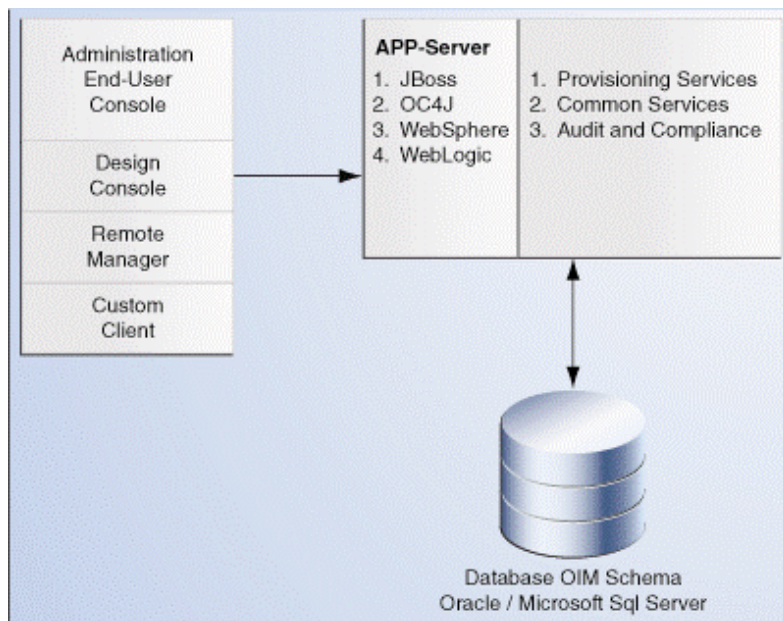
Figure 10–4   Oracle Identity Manager 11g

11
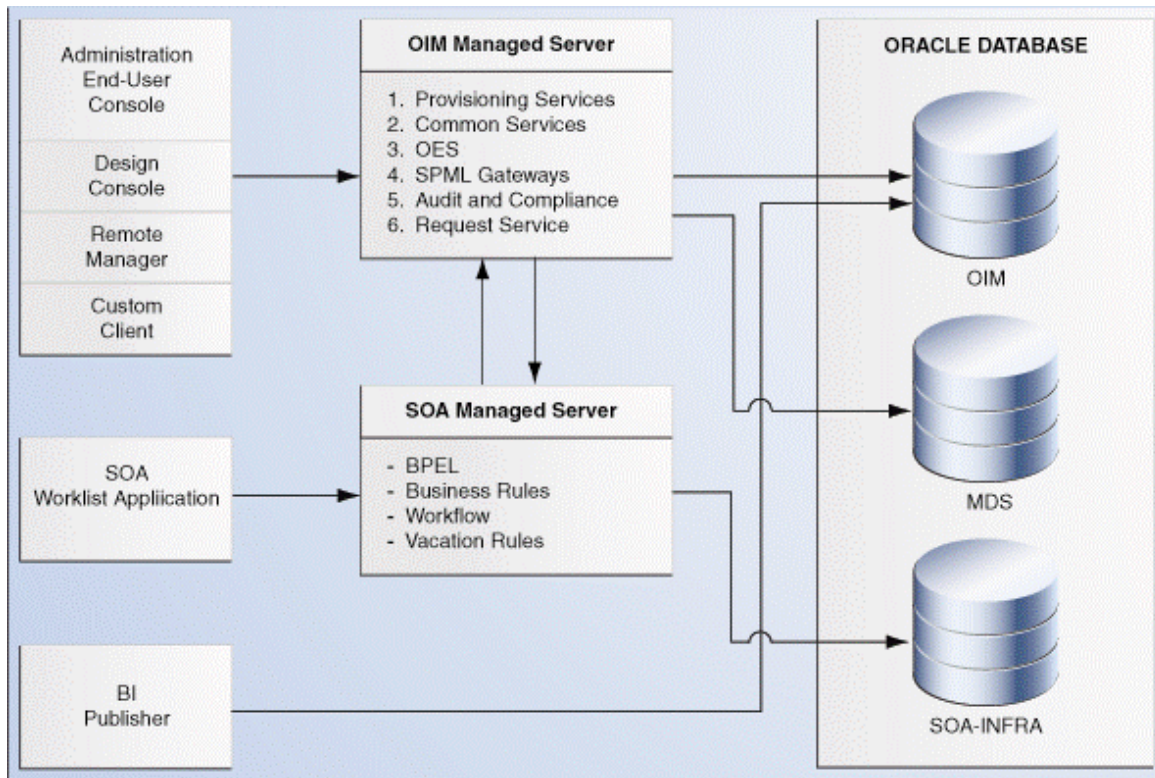
Upgrading Oracle Single Sign-On Environment

This chapter describes how to upgrade your existing Oracle Single Sign-On 10*g* Release 2 (10.1.2.3) or Oracle Single Sign-On 10g Release 2 (10.1.4.3) to Oracle Access Manager 11*g* Release 1 (11.1.1.5.0).

This chapter contains the following sections:

- Overview
- Upgrade Scenarios
- Task 1: Decide Upon an Oracle Access Manager Topology
- Task 2: If Necessary, Upgrade the Oracle Database
- Task 3: Use Repository Creation Utility to Create 11g Oracle Access Manager Schemas
- Task 4: Install and Configure the Oracle Access Manager Middle Tier
- Task 5: Upgrade Oracle Access Manager Middle Tier Using Upgrade Assistant
- Task 6: Complete Any Required Oracle Access Manager Post-Upgrade Tasks
- Task 7: Verify the Oracle Access Manager Upgrade

Before performing any installation or upgrade, you should read the system requirements and certification documentation to ensure that your environment meets the minimum installation requirements for the products you are installing.

For more information, refer to "System Requirements and Specifications" in the *Oracle Fusion Middleware Installation Planning Guide*.

> **Note:** On AIX platforms, ensure that you have patched your Oracle Internet Directory 10*g* (10.1.4.0.1) to Oracle Internet Directory 10.1.4.3.0 before upgrading to Oracle Access Manager 11*g*.

11.1 Overview

You can use Oracle Fusion Middleware Upgrade Assistant to upgrade the following:

- Oracle Single Sign-On 10*g* configurations and artifacts
- Partner metadata stored by Oracle Single Sign-On 10*g* Server
- Partners registered with Oracle Single Sign-On 10*g* Server

After you complete the upgrade, Oracle Internet Directory becomes the primary identity store for Oracle Access Manager 11*g*.

The following components are not upgraded to the Oracle Access Manager 11*g* environment when you run Upgrade Assistant to upgrade from Oracle Single Sign-On 10*g*:

- Oracle Single Sign-On 10*g* with Window Native Authentication integration. For more information, see "Configuring Oracle Access Manager to use Windows Native Authentication" in the *Oracle Fusion Middleware Integration Guide for Oracle Access Manager*.

- Logging configuration. For more information see "Logging Component Event Messages" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager*.

- Oracle Single Sign-On 10*g* with Oracle Identity Federation integration. For more information see "Integrating Oracle Identity Federation" in the *Oracle Fusion Middleware Integration Guide for Oracle Access Manager*.

- Custom authentication.

- X509 configurations. For more information see the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager*.

- External Application

- Pstore

- Multirealm Configuration

11.2 Upgrade Scenarios

Before you upgrade Oracle Single Sign-On 10*g* to Oracle Access Manager 11*g*, you must consider your Oracle Single Sign-On 10*g* infrastructure (Figure 11–1) and depending on the functionality you choose to retain, you must select one of the following scenarios:

- Oracle Delegated Administration Services Required After Upgrading from Oracle Single Sign-On to Oracle Access Manager

- Oracle Delegated Administration Services Required, but Oracle Single Sign-On Admin Not Required After Upgrading from Oracle Single Sign-On to Oracle Access Manager 11g

- Oracle Delegated Administration Services Not Required After Upgrading from Oracle Single Sign-On to Oracle Access Manager

Oracle Single Sign-On 10*g* Infrastructure Before Upgrade

Figure 11–1 illustrates the Oracle Single Sign-On 10*g* topology, which is the starting point for upgrading to Oracle Access Manager 11*g*.

Figure 11–1   Oracle Single Sign-On 10g Infrastructure
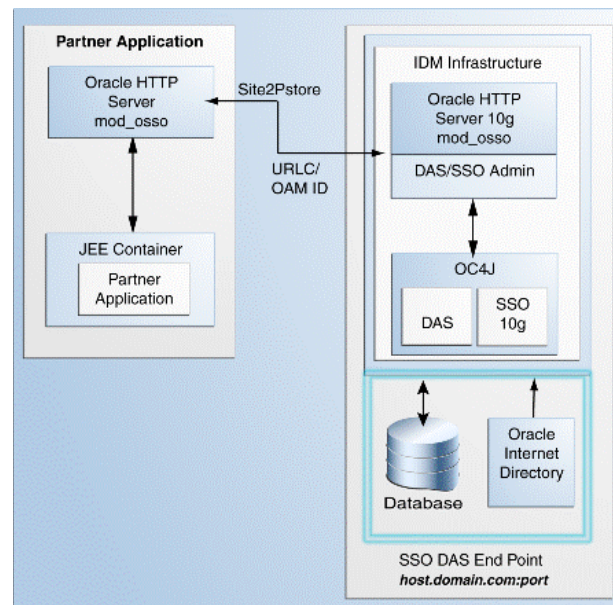
The topology comprises the following:

- Partner applications in a JEE container front-ended by Oracle HTTP Server to communicate with the Oracle Single Sign-On infrastructure

- Oracle Identity Management infrastructure that includes the Oracle HTTP Server 10*g* front-ending the Oracle Delegated Administration Services application and the Oracle Single Sign-On Server

The Oracle Single Sign-On endpoint, which consists of a host name and a port number, represents the URL that Oracle Single Sign-On users can use to access the Oracle Single Sign-On Server and the Oracle Delegated Administration Services application.

An example Oracle Single Sign-On endpoint is `host.domain.com:port`.

> **Note:**   This example is used in this section to illustrate different upgrade scenarios and their Oracle Single Sign-On endpoints.

Oracle Delegated Administration Services Required After Upgrading from Oracle Single Sign-On to Oracle Access Manager

Use this upgrade scenario if you want to continue to use the Oracle Delegated Administration Services application and the Oracle Single Sign-On Admin tool after upgrading from Oracle Single Sign-On 10*g* to Oracle Access Manager 11*g*. Figure 11–2 illustrates the scenario.

Note the following points when using this upgrade scenario:

- Use this scenario if you are using Oracle Portal, Oracle Forms, Oracle Reports, or Oracle Discoverer partner applications because you require Oracle Delegated Administration Services and Oracle Single Sign-On Admin. Upgrade all partner applications at once.

- The Oracle Delegated Administration Services application runs on a new port.

- Any Oracle Delegated Administration Services requests from partner applications, such as Oracle Portal, arrive at the Oracle HTTP Server 11*g* and redirected to Oracle HTTP Server 10*g*, which front-ends the Oracle Delegated Administration Services 10*g* application. The Oracle HTTP Server 11*g* front-ends Oracle Access Manager 11*g*. Such requests are redirected to Oracle HTTP Server 10*g* port, which front-ends the Oracle Delegated Administration Services 10*g* application.

  > **Note:** You must reregister Oracle Delegated Administration Services and Oracle Single Sign-On Admin with Oracle Access Manager 11*g* because their port is changed.

- You are using the same OHS 10*g* port that front-ended Oracle Single Sign-On 10*g* as the new port for Oracle Access Manager 11*g*. Therefore, the Oracle Single Sign-On 10*g* server goes down.

- The Oracle Single Sign-On-Oracle Delegated Administration Services endpoint (`same_host.domain.com:same_port`) remains the same for all the partner applications.

- After you perform the upgrade, Oracle Internet Directory is selected as the user identity store automatically.

Figure 11–2 Oracle Delegated Administration Services Required After Upgrading from Oracle Single Sign-On
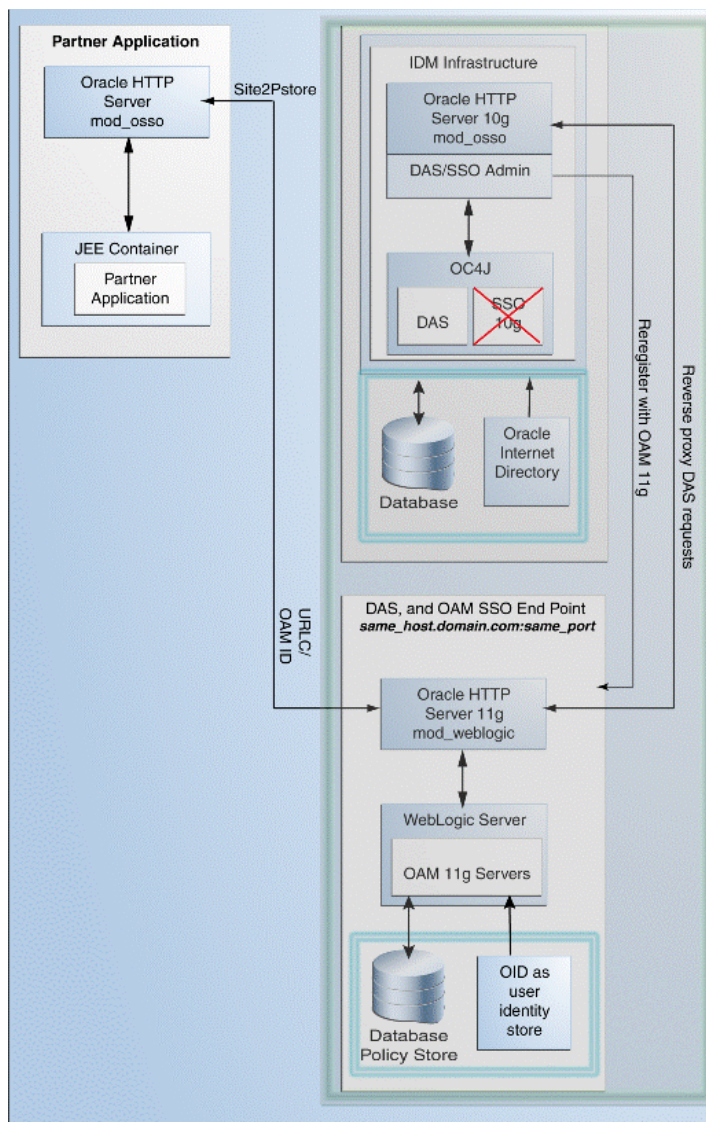
To use this upgrade scenario, follow the steps listed in Table 11–1.

Oracle Delegated Administration Services Required, but Oracle Single Sign-On Admin Not Required After Upgrading from Oracle Single Sign-On to Oracle Access Manager 11*g*

Use this upgrade scenario if you do not require the Oracle Single Sign-On Admin tool application, but you require the Oracle Delegated Administration Services application after upgrading from Oracle Single Sign-On 10*g* to Oracle Access Manager 11*g*. Figure 11–3 illustrates the scenario.

Note the following points when using this upgrade scenario:

- You are using the OHS 10*g* port for Oracle Delegated Administration Services. Therefore, you must install Oracle Access Manager 11*g* on a different machine.

- Upgrade your partner applications in a phased manner.

■ Oracle Single Sign-On will no longer work after the upgrade. However, Oracle Delegated Administration Services will continue to work.

■ You must copy the osso.conf files generated during the upgrade manually for each OHS/mod_osso fronting a set of partner applications. This step associates these applications with Oracle Access Manager as their new Oracle Single Sign-On provider. This step is also necessary for Oracle Delegated Administration Services.

■ The Oracle Delegated Administration Services endpoint (same_host.domain.com:same_port) remains the same for all the partner applications.

■ The Oracle Access Manager Oracle Single Sign-On endpoint is new, such as new_host.domain.com:new_port.

■ After you perform the upgrade, Oracle Internet Directory is selected as the user identity store automatically.

Figure 11–3   Oracle Single Sign-On Administration Server Not required
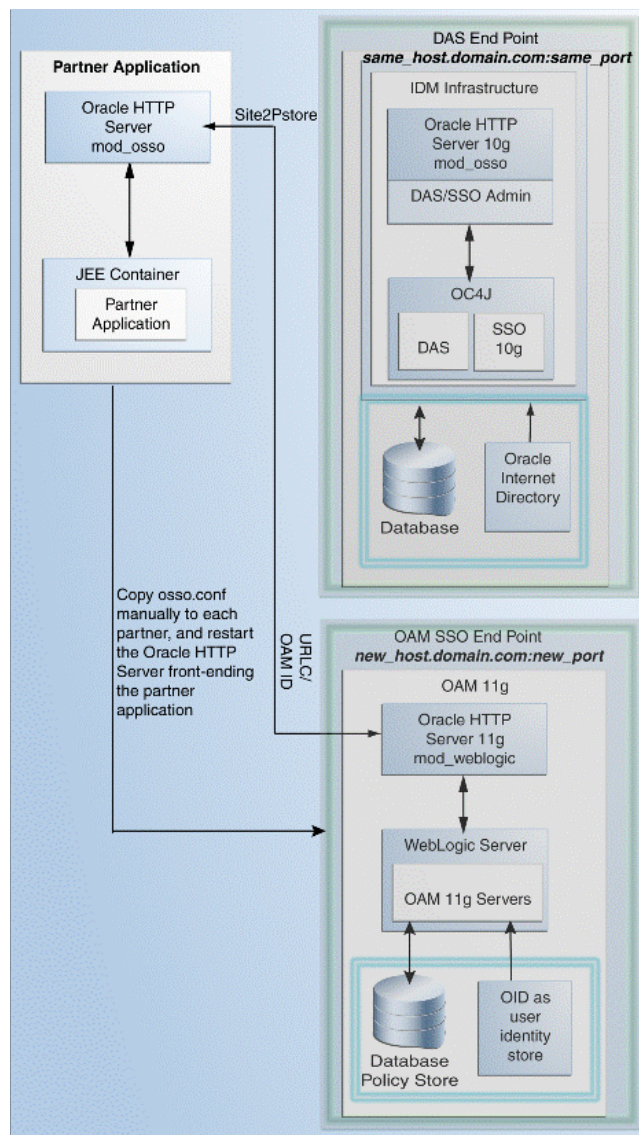
To use this upgrade scenario, follow the steps listed in Table 11–1.

Oracle Delegated Administration Services Not Required After Upgrading from Oracle Single Sign-On to Oracle Access Manager

Use this upgrade scenario if you do not require the Oracle Delegated Administration Services application or the Oracle Single Sign-On Admin tool. Figure 11–4 illustrates the scenario.

Note the following points when using this upgrade scenario:

- Oracle Single Sign-On and Oracle Delegated Administration Services will no longer work after the upgrade.

- Upgrade all partner applications at once.

- You are using the same OHS 10*g* port that front-ended Oracle Single Sign-On 10*g* as the new port for Oracle Access Manager 11*g*. Therefore, the Oracle Single Sign-On 10*g* server as well as the Oracle Delegated Administration Services application cannot be accessed.

- The Oracle Single Sign-On endpoint (`same_host.domain.com:same_port`) remains the same for all the partner applications.

- After you perform the upgrade, Oracle Internet Directory is selected as the user identity store automatically.

Figure 11–4   Oracle Delegated Administration Services Not Required
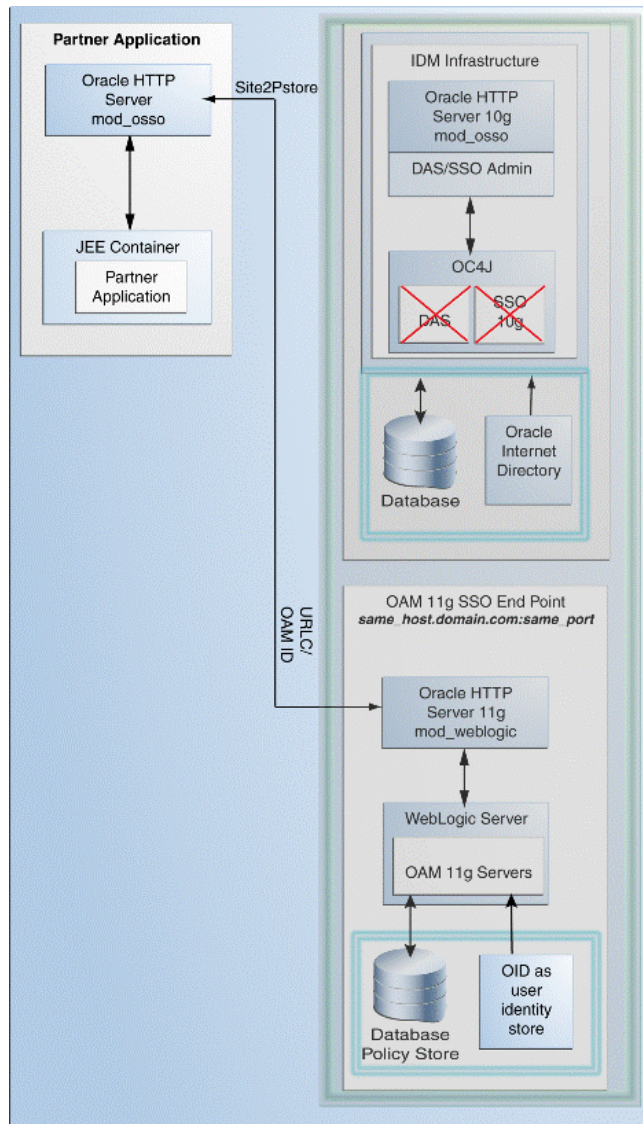
To use this upgrade scenario, follow the steps listed in Table 11–1.

Table 11–1 describes the Oracle Single Sign-On 10*g* upgrade scenarios.

Table 11–1   Upgrade Scenarios and Tasks

Scenario	Steps
Oracle Delegated Administration Services Required After Upgrading from Oracle Single Sign-On to Oracle Access Manager	Complete the following tasks: ■ Task 1: Decide Upon an Oracle Access Manager Topology ■ Task 2: If Necessary, Upgrade the Oracle Database ■ Task 3: Use Repository Creation Utility to Create 11g Oracle Access Manager Schemas ■ Task 4: Install Oracle Access Manager 11g Using Oracle Single Sign-On 10g Host Name and Port Number ■ Task 5: Upgrade Oracle Access Manager Middle Tier Using Upgrade Assistant ■ Task 6: Complete Any Required Oracle Access Manager Post-Upgrade Tasks ■ Task 7: Verify the Oracle Access Manager Upgrade
Oracle Delegated Administration Services Required, but Oracle Single Sign-On Admin Not Required After Upgrading from Oracle Single Sign-On to Oracle Access Manager 11g	Complete the following tasks: ■ Task 1: Decide Upon an Oracle Access Manager Topology ■ Task 2: If Necessary, Upgrade the Oracle Database ■ Task 3: Use Repository Creation Utility to Create 11g Oracle Access Manager Schemas ■ Task 4: Install Oracle Access Manager 11g Using New Host Name or New Port Number ■ Task 5: Upgrade Oracle Access Manager Middle Tier Using Upgrade Assistant ■ Task 6: Complete Any Required Oracle Access Manager Post-Upgrade Tasks ■ Task 7: Verify the Oracle Access Manager Upgrade
Oracle Delegated Administration Services Not Required After Upgrading from Oracle Single Sign-On to Oracle Access Manager	Complete the following tasks: ■ Task 1: Decide Upon an Oracle Access Manager Topology ■ Task 2: If Necessary, Upgrade the Oracle Database ■ Task 3: Use Repository Creation Utility to Create 11g Oracle Access Manager Schemas ■ Task 4: Install Oracle Access Manager 11g Using New Host Name or New Port Number ■ Task 5: Upgrade Oracle Access Manager Middle Tier Using Upgrade Assistant ■ Task 6: Complete Any Required Oracle Access Manager Post-Upgrade Tasks ■ Task 7: Verify the Oracle Access Manager Upgrade

11.3 Task 1: Decide Upon an Oracle Access Manager Topology

Before you begin the upgrade process, consider the topology you currently have in Oracle Single Sign-On 10*g* (10.1.2 and 10.1.4) as well as any requirements for your Oracle Fusion Middleware 11*g* environment.

For more information, refer to Chapter 10.1, "Oracle Single Sign-On Topologies".

11.4 Task 2: If Necessary, Upgrade the Oracle Database

When you are upgrading an Oracle Access Manager environment, you must ensure that the version of the database where you plan to install the Oracle Access Manager schemas is supported by Oracle Fusion Middleware 11g.

You can install a new database, or upgrade your existing database to a supported version.

For instructions on verifying that your database meets the requirements of Oracle Fusion Middleware 11*g*, see "Upgrading and Preparing Your Databases" in the *Oracle Fusion Middleware Upgrade Planning Guide*.

11.5 Task 3: Use Repository Creation Utility to Create 11*g* Oracle Access Manager Schemas

When you are upgrading to Oracle Access Manager, use the Repository Creation Utility to install the schemas in the database you identified and prepared in Task 2: If Necessary, Upgrade the Oracle Database.

For more information, refer to the following sections:

- Running Repository Creation Utility for Oracle Access Manager
- Selecting the Schemas Required for Oracle Access Manager Upgrade

11.5.1 Running Repository Creation Utility for Oracle Access Manager

To run the Repository Creation Utility to install the Oracle Access Manager schema in the database, refer to the following resources:

- *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*
- *Oracle Fusion Middleware Repository Creation Utility User's Guide*

After you start the Repository Creation Utility, follow the instructions on the Repository Creation Utility screens to connect to the database and create the required schemas.

11.5.2 Selecting the Schemas Required for Oracle Access Manager Upgrade

You use Repository Creation Utility to install the schemas required for all of the Oracle Fusion Middleware software components that require a schema. However, you do not need to install all the schemas unless you plan to install a complete Oracle Fusion Middleware environment and you plan to use the same database for all the Oracle Fusion Middleware component schemas.

For Oracle Access Manager upgrade, you must select the following schemas when you are prompted by the Repository Creation Utility:

- Expand **AS Common Schemas**, and select the **Metadata Services** schema in the category.

  This schema supports Oracle Fusion Middleware Metadata Services (MDS), which is required by the Oracle Access Manager component.

- Expand **Identity Management**, and select **Oracle Access Manager** schema.

11.6 Task 4: Install and Configure the Oracle Access Manager Middle Tier

Depending on the Upgrade Scenarios you choose, you must complete one of the following tasks:

- Install Oracle Access Manager 11g Using Oracle Single Sign-On 10g Host Name and Port Number

- Install Oracle Access Manager 11g Using New Host Name or New Port Number

> **Note:** If you are installing 32-bit Oracle Identity and Access Management on a 64-bit Operating System, then you must run the `setup.exe` file located at `Disk1\install\win32` for the Windows 32-bit file. Other setup files are located in similar locations under the `\install` directory depending on the platform.

11.6.1 Install Oracle Access Manager 11*g* Using Oracle Single Sign-On 10*g* Host Name and Port Number

Table 11–2 lists the steps to install and configure the Oracle Access Manager middle for using the Oracle Delegated Administration Services application and the Oracle Single Sign-On Admin tool after upgrading from Oracle Single Sign-On 10*g* to Oracle Access Manager 11*g*.

Table 11–2   Steps to Install and Configure the Oracle Access Manager Middle Tier

Step	Description	Section
1	Installing Oracle WebLogic Server and Creating the Oracle Middleware Home	See section "Installing Oracle WebLogic Server 10.3.4 and Creating the Oracle Middleware Home" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.
		For more information about the Middleware home, see "Understanding Oracle Fusion Middleware Concepts" in the *Oracle Fusion Middleware Administrator's Guide*.
2	Stopping and Configuring the Oracle HTTP Server 10g	See Reconfiguring Oracle HTTP Server 10g.
3	Installing Oracle HTTP Server 11*g*	Install Oracle HTTP Server 11*g* and specify the Oracle HTTP Server 10*g* port number. For more information, see *Oracle Fusion Middleware Installation Guide for Web Tier*.
4	Installing Oracle Access Manager	See "Installing OAM" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.
5	Configuring Oracle Access Manager	See "Configuring Oracle Access Manager (OAM)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.
6	Configuring Node Manager to Start Managed Servers	To configure Node Manager, refer to the section "Configuring Node Manager to Start Managed Servers" in the *Oracle Fusion Middleware Administrator's Guide*.
7	Starting the Oracle WebLogic Server domain	See section "Starting the Stack" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

Table 11–2   (Cont.) Steps to Install and Configure the Oracle Access Manager Middle

Step	Description	Section
8	Front-ending the Oracle Access Manager Managed Server with the Oracle HTTP Server 11g	See Front-Ending Oracle Access Manager Managed Server with Oracle HTTP Server 11g
9	Registering the Oracle HTTP Server 10g as a Partner Application	See Registering Your Applications as Partner Applications of Oracle Access Manager 11g.
10	Redirecting the OIDDAS Request to the Oracle HTTP Server 10g server	See Redirecting the Partner Application Request to Oracle HTTP Server 10g server.
11	Verifying the installation	See "Verifying the OAM Installation" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

Reconfiguring Oracle HTTP Server 10*g*

Perform the following steps:

1. Open the `httpd.conf` file (Located at `ORACLE_HOME\Apache\Apache\conf` in Windows or `ORACLE_HOME/Apache/Apache/conf` in UNIX) in a text editor and change the existing port number and provide a new port number.

2. Stop Oracle HTTP Server 10*g* by running the `opmnctl` command-line tool (Located at `ORACLE_HOME\opmn\bin`) as follows:

   ```
   opmnctl stopproc ias-component=<name_of_the_OHS_instance>
   ```

3. Restart Oracle HTTP Server 10*g* by running the following `opmnctl` command:

   ```
   OHS_INSTANCE_HOME/bin/opmnctl stopall
   OHS_INSTANCE_HOME/bin/opmnctl startall
   ```

Front-Ending Oracle Access Manager Managed Server with Oracle HTTP Server 11*g*

You must use `mod_wl_ohs` to front-end Oracle Access Manager Managed Server with Oracle HTTP Server 11*g*. To do so, complete the following steps:

1. Open the `mod_wl_ohs.conf` file (Located at `OHS_INSTANCE_ HOME\config\OHS\<ohs_instance_name>` on Windows) in a text editor and edit as follows:

   ```
   <IfModule weblogic_module>
               WebLogicHost <OAM Managed Server Host>
               WebLogicPort <OAM Managed Server Port>
               Debug ON
            WLLogFile /tmp/weblogic.log
         MatchExpression *.jsp
      </IfModule>
      <Location />
           SetHandler weblogic-handler
           PathTrim /
           ErrorPage  http://WEBLOGIC_HOST:WEBLOGIC_PORT/
      </Location>
   ```

2. Restart Oracle HTTP Server 11*g* by running the following `opmnctl` command from the 11*g* ORACLE_INSTANCE (Located at *ORACLE_INSTANCE*\bin directory on Windows or *ORACLE_INSTANCE*/bin directory on UNIX):

   ```
   opmnctl stopall
   opmnctl startall
   ```

3. Open the `oam-config.xml` file (Located at `MW_HOME\user_projects\domains\<domain_name>\config\fmwconfig` directory on Windows) in a text editor and edit `serverhost` and `serverport` entries as shown in the following example:

```
<Setting Name="OAMSERVER" Type="htf:map">
    <Setting Name="serverhost" Type="xsd:string"><OHS 11G HOST></Setting>
    <Setting Name="serverprotocol" Type="xsd:string">http</Setting>
    <Setting Name="serverport" Type="xsd:string"><OHS 11G PORT></Setting>
    <Setting Name="MaxRetryLimit" Type="xsd:integer">5</Setting>
</Setting>
```

4. Restart the Oracle Access Manager Administration Server and Managed server as follows:

   On Windows:

   ```
   MW_HOME\user_projects\domains\domain_name\startWebLogic.cmd
   MW_HOME\user_projects\domains\domain_name\bin\startManagedWebLogic.cmd oam_server1
   ```

   On UNIX:

   ```
   MW_HOME/user_projects/domains/domain_name/startWebLogic.sh
   MW_HOME/user_projects/domains/domain_name/bin/startManagedWebLogic.sh oam_server1
   ```

Registering Your Applications as Partner Applications of Oracle Access Manager 11*g*

You must register the Oracle Internet Directory and Oracle Delegated Administration Services deployed on Oracle HTTP Server 10*g* partners with Oracle Access Manager 11*g*. To do so, complete the following steps:

1. Log in to the Oracle Access Manager console.

2. Click the **System Configuration** tab.

3. In the **Welcome** page, select **Add OSSO Agents**.

4. In the **Create OSSO Agent** page, enter the following details:

   – **Agent Name**: The identifying name for the `mod_osso` Agent.

   – **Agent Base URL**: The required protocol, host, and port of the computer on which the Web server for the agent is installed. For example, `http://ohs_host:port:ohs_port`.

5. Click **Apply**.

   The agent is created and the `osso.conf` file is generated at `DOMAIN_HOME\output\AGENT_NAME` (Windows).

6. Copy the newly generated agent file to Oracle HTTP Server 10*g* at `OHS_CONF\osso`.

7. Restart Oracle HTTP Server 10*g* by running the following `opmnctl` command:

   ```
   OHS_INSTANCE_HOME/bin/opmnctl stopall
   OHS_INSTANCE_HOME/bin/opmnctl startall
   ```

Redirecting the Partner Application Request to Oracle HTTP Server 10*g* server

You must use `mod_proxy` to redirect the Oracle Internet Directory and Oracle Delegated Administration Services request to the Oracle HTTP Server 10*g*.

Open the Oracle HTTP Server 11*g* `httpd.conf` file in a text editor and add entries of OHS 10*g* host name and post name front-ending Oracle Internet Directory and Oracle Delegated Administration Services as shown in the following example:

```
ProxyPass         /oiddas http://pdcasqa14-3.us.abc.com:8888/oiddas
ProxyPassReverse  /oiddas http://pdcasqa14-3.us.abc.com:8888/oiddas
```

> **Note:** The above example is using the OHS 10*g* port number.

Restart Oracle HTTP Server 11*g* by running the following `opmnctl` command:

```
OHS_INSTANCE_HOME/bin/opmnctl stopall
OHS_INSTANCE_HOME/bin/opmnctl startall
```

If your Oracle HTTP Server 10*g* is SSL enabled, then you must complete the following:

1. Create a wallet for the proxy.

2. If the root certificate of Oracle HTTP Server 10*g* is not well-known then you must import it into the above created wallet as a trusted certificate.

3. Open the Oracle HTTP Server 11*g* `ssl.conf` file (located under `ORACLE_INSTANCE/config/OHS/{COMPONENT_NAME}/`) in a text editor and add the following line under `<VirtualHost *:PORTNUMBER><IfModule ossl_module>`:

   ```
   SSLProxyEngine On
   SSLProxyWallet <PATH of the wallet created above>
   ```

4. Restart Oracle HTTP Server 11*g* by running the following `opmnctl` command:

   ```
   OHS_INSTANCE_HOME/bin/opmnctl stopall
   OHS_INSTANCE_HOME/bin/opmnctl startall
   ```

11.6.2 Install Oracle Access Manager 11*g* Using New Host Name or New Port Number

Table 11–3 lists the steps you must perform when installing and configuring the Oracle Access Manager middle tier, using a new host name or port number for Oracle Access Manager.

Table 11–3   Steps to Install and Configure the Oracle Access Manager Middle Tier

Step	Description	For More Information
1	Installing Oracle WebLogic Server and Creating the Oracle Middleware Home	See section "Installing Oracle WebLogic Server 10.3.4 and Creating the Oracle Middleware Home" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.
		For more information about the Middleware home, see "Understanding Oracle Fusion Middleware Concepts" in the *Oracle Fusion Middleware Administrator's Guide*.
2	Installing Oracle Access Manager	See "Installing OAM" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

Table 11–3   (Cont.) Steps to Install and Configure the Oracle Access Manager Middle

Step	Description	For More Information
3	Configuring Oracle Access Manager	See "Configuring Oracle Access Manager (OAM)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.
4	Configuring Node Manager to Start Managed Servers	To configure Node Manager, refer to the section "Configuring Node Manager to Start Managed Servers" in the *Oracle Fusion Middleware Administrator's Guide*.
5	Starting the Oracle WebLogic Server domain	See section "Starting the Stack" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.
6	Verifying the installation	See "Verifying the OAM Installation" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

11.7 Task 5: Upgrade Oracle Access Manager Middle Tier Using Upgrade Assistant

When you install Oracle Access Manager 11*g*, Upgrade Assistant is installed automatically into the `bin` directory of your Oracle home.

You run Upgrade Assistant once for each Oracle home that you are upgrading. For example, if you are upgrading two different 10*g* Release 2 (10.1.2) Oracle homes that are part of the same 10*g* Release 2 (10.1.2) farm, then you must run Upgrade Assistant two times, once for each of the 10*g* Release 2 (10.1.2) Oracle homes.

> **Note:**   You can also use the Upgrade Assistant command-line interface to upgrade your Oracle Application Server 10*g* Oracle homes. For more information, see "Using the Upgrade Assistant Command-Line Interface" in the *Oracle Fusion Middleware Upgrade Planning Guide*.

To upgrade the middle tier, complete the following steps:

1. Enter the following command to launch Upgrade Assistant.

    On UNIX systems (Located at *MW_HOME*/Oracle_IDM_Home/bin):

    `./ua`

    On Windows systems (Located at *MW_HOME*\Oracle_IDM_Home\bin):

    `ua.bat`

    The Oracle Fusion Middleware Upgrade Assistant **Welcome** screen is displayed, as shown in Figure 11–5.

Figure 11–5   Upgrade Assistant Welcome Screen
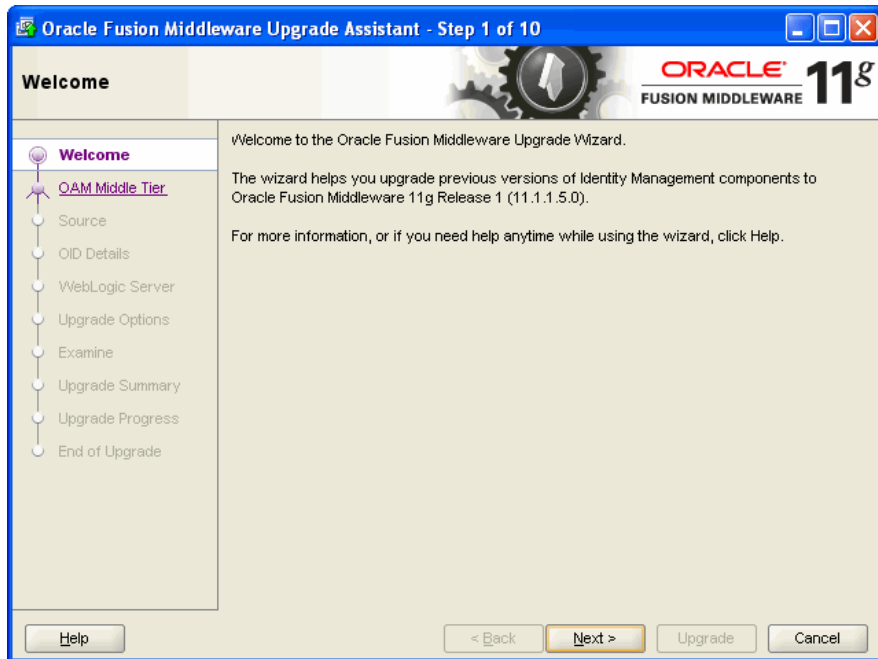
2. Click **Next**.

    The **Specify Operation** screen is displayed.

Figure 11–6   Specify Operation

This screen capture shows the Specify Operation screen of the Oracle Fusion Middleware Upgrade Assistant.

****

3. Select **Upgrade Oracle Access Manager Middle Tier**.

The options available in Upgrade Assistant are specific to the Oracle home from which it started. When you start Upgrade Assistant from an Oracle Application Server Identity Management Oracle home, the options shown on the Specify Operation screen are the valid options for an Oracle Application Server Identity Management Oracle home.

4. Click **Next**.

The **Specify Source Details** screen is displayed.

5. Enter the following information:

   ■ **Properties File**: Click **Browse** and specify the path of the Oracle Single Sign-On 10*g* `policy.properties` file.

   If your Oracle Access Manager 11*g* installation is on a separate host from the Oracle Single Sign-On 10*g* installation, then you must copy the 10*g* `policy.properties` file to a temporary directory on the Oracle Access Manager 11*g* host. Then specify the path of the `policy.properties` file located in your temporary folder.

   ■ **Database Host**: Enter the database host name that contains the Oracle Single Sign-On schema.

   ■ **Database Port**: Enter the database port number.

   ■ **Database Service**: Enter the database service name.

   ■ **SYS Password**: Enter the password for the SYS database account of the database that you selected from the Database drop-down menu. Upgrade Assistant requires these login credentials before it can upgrade the 10*g* components schemas.

   > **Note:** Ensure that you enter database details for the Oracle Single Sign-On 10*g* database configuration.

6. Click **Next**.

The **Specify OID Details** screen is displayed.

7. Enter the following information:

   ■ **OID Host**: Enter the host name of the Oracle Internet Directory 10*g* server.

   ■ **OID SSL Port**: Enter your Oracle Internet Directory 10*g* port number.

   ■ **OID Password**: Enter the password for the Oracle Internet Directory 10*g* administration account (`cn=orcladmin`).

8. Click **Next**.

The **Specify WebLogic Server** screen is displayed.

9. Enter the following information:

   ■ **Host**: Enter the host name of the Oracle WebLogic Server domain.

   ■ **Port**: Enter the listening port of the Administration Server. The default server port is `7001`.

   ■ **Username**: The user name that is used to log in to the Administration Server. This is the same user name you use to log in to the Administration Console for the domain.

- **Password**: The password for the administrator account that is used to log in to the Administration Server. This is the same password you use to log in to the Administration Console for the domain.

10. Click **Next**.

    The **Specify Upgrade Options** screen is displayed

11. Select **Start destination components after successful upgrade**, and click **Next**.

    > **Note:** If you are using external application, then select **Upgrade even with external applications**.

    The **Examining Components** screen is displayed.

12. Click **Next**.

    The **Upgrade Summary** screen is displayed.

13. Click **Upgrade**.

    The **Upgrade Progress** screen is displayed. This screen provides the following information:

    - The status of the upgrade

    - Any errors or problems that occur during the upgrade

      > **See Also:** "Troubleshooting Your Upgrade" in the *Oracle Fusion Middleware Upgrade Planning Guide* for specific instructions for troubleshooting problems that occur while running the Upgrade Assistant.

14. Click **Next**.

    The **Upgrade Complete** screen is displayed. This screen confirms that the upgrade was complete.

15. Click **Close**.

11.8 Task 6: Complete Any Required Oracle Access Manager Post-Upgrade Tasks

The following sections describe the manual steps that you must perform after upgrading to Oracle Access Manager 11*g*:

- Configuring Oracle Portal 10g with Oracle Access Manager Server If the Oracle HTTP Server Port Is Changed

- Configuring Oracle Access Manager Administration Console to Align the Roles

- Copying the osso.conf File

- Configuring Oracle Business Intelligence Discoverer 11g with Oracle Access Manager 11g

- Additional Oracle Access Manager Post-Upgrade Tasks

- Decommissioning Oracle Single Sign-On 10g

11.8.1 Configuring Oracle Portal 10*g* with Oracle Access Manager Server If the Oracle HTTP Server Port Is Changed

After upgrading the Oracle Portal's Oracle Single Sign-On server to the Oracle Access Manager server, you must update the Oracle Portal schema with information about the Oracle Access Manager server. To do so, you must update the `wwsec_enabler_config_info$` table as follows:

1. Connect to the database hosting the Oracle Portal schema, and log in with the Portal schema user name and password.

2. Run the following command to retrieve the Portal schema password.

   ```
   ldapsearch -v -D "cn=orcladmin" -w "orcladminpassword" -h OIDHost -p OIDPort -s
   sub -b "cn=IAS  Infrastructure Databases, cn=IAS, cn=Products,
   cn=OracleContext" "orclresourcename=PORTAL"  orclpasswordattribute
   ```

3. Run the `portal_post_upgrade.sql` script (located at `ORACLE_HOME\oam\server\upgrade\sql`).

4. When prompted, enter your Oracle Access Manager Managed Server Host name and Port number.

11.8.2 Configuring Oracle Access Manager Administration Console to Align the Roles

After upgrade, the Oracle Access Manager Administration Console uses the System Identity Store for run-time authentication and authorization. To align the existing roles, you can use the following WLST command:

1. Start the WebLogic Scripting Tool located at (*ORACLE_IDM*\common\bin):

   ```
   wlst.sh
   ```

2. In the WLST shell, enter the following command:

   ```
   editUserIdentityStore (
   name="UserIdentityStoreName",roleSecAdmin="SecurityAdminRoleName" )
   ```

   Example:

   ```
   ( name="MigratedUserIdentityStore",roleSecAdmin="Administrators" )
   ```

If you want to configure a group for Oracle Access Manager Administrator for the Oracle Access Manager Administration Console, complete the following steps:

1. Create a group for example Administrators in the Oracle Internet Directory.

2. Add the fully qualified `dn` for Oracle Access Manager Administrator privileges. For example, enter the following as the unique member of the group:

   ```
   cn=orcladmin,cn=users,dc=us,dc=abc,dc=com
   ```

3. Start the WebLogic Scripting Tool located at (*ORACLE_IDM*\common\bin):

   ```
   wlst.sh
   ```

4. In the WLST shell, enter the following command:

   ```
   editUserIdentityStore(name="MigratedUserIdentityStore",roleSecAdmin="SecurityAd
   minRoleName")
   ```

   Example:

   ```
   editUserIdentityStore(name="MigratedUserIdentityStore",roleSecAdmin="Administra
   ```

```
tors")
```

11.8.3 Copying the osso.conf File

If you have retained your existing Oracle Single Sign-On 10*g* host name and port number during the upgrade process, then the Oracle Upgrade Assistant will generate the `osso.conf` file for each partner application, in the *Oracle_Home*/upgrade/temp directory. You must copy this `osso.conf` file to the location of the partner application registered with Oracle Access Manager 11*g*.

You must identify the correct `osso.conf` file associated with the partner application.

Example:

```
F78CFE57-dadvmb0097.us.abc.com_22776_769_osso.conf
```

To identify the correct `osso.conf` file see the `oam-config.xml` file (Located at, `IDM_HOME/oam/server/config`). The `oam-config.xml` file provides the partner application details and the Oracle HTTP Server host address and port number.

11.8.4 Configuring Oracle Business Intelligence Discoverer 11*g* with Oracle Access Manager 11*g*

After upgrading the Oracle Business Intelligence Discoverer's Oracle Single Sign-On server to the Oracle Access Manager server, you must update the Oracle Business Intelligence Discoverer Single Sign-On configuration as follows:

1. Open the `mod_osso.conf` file (Located at, `ORACLE_INSTANCE/config/OHS/<COMPONENT_NAME>/moduleconf` in the Oracle Business Intelligence Discoverer instance) in a text editor.

2. Add the following line in the `<IfModule mod_osso.c>`:

    ```
    OssoHTTPOnly Off
    ```

3. Restart Oracle HTTP Server by running the following `opmnctl` command:

    ```
    OHS_INSTANCE_HOME/bin/opmnctl stopall
    OHS_INSTANCE_HOME/bin/opmnctl startall
    ```

11.8.5 Additional Oracle Access Manager Post-Upgrade Tasks

You must perform the following additional post-upgrade tasks after upgrading to Oracle Access Manager 11*g*:

- If the destination topology is front-ended by Oracle HTTP server 11g (installed through the 11*g* companion CD) on the same machine as the source, then you can run Upgrade Assistant from the Oracle HTTP server 11*g* installation directory to upgrade the Oracle HTTP server that front-ends Oracle Single Sign-On. In such cases, if you use the Upgrade Assistant retain port option, then no re-association of `mod_osso` partners with Oracle Access Manager is required.

- If you are using Oracle Portal 11*g* that you have upgraded from Oracle Portal 10*g*, then you must run the `portal_post_upgrade.sql` script (Located at `Oracle_IDM1/oam/server/upgrade/sql`) to update the Oracle Single Sign-On configuration and to use Oracle Access Manager 11*g* for Single Sign-On authentication.

- In all other cases, the post-upgrade step of re-associating `mod_osso` partners with the newly upgraded Oracle Access Manager 11*g* is required. The `mod_osso` configurations generated as part of the upgrade can be used for this purpose.

■ Before login to the Oracle Portal, you must restart Oracle Web Cache by running the following opmnctl command (Located at *ORACLE_INSTANCE*\bin directory on Windows or *ORACLE_INSTANCE*/bin directory on UNIX):

```
opmnctl stopall
opmnctl startall
```

11.8.6 Decommissioning Oracle Single Sign-On 10*g*

After upgrading to Oracle Access Manager 11*g*, if you are not using Oracle Single Sign-On 10*g* on Oracle Internet Directory 10*g* or Oracle Delegated Administration Services 10*g*, then you can deinstall Oracle Single Sign-On 10*g*. To do so, undeploy the Oracle Single Sign-On 10*g* server from the Oracle Identity Manager 10*g* Server (OC4J_SECURITY) by running the following command on the command line:

```
java -jar admin_client.jar <uri> <adminId> <adminPassword> -undeploy sso
```

11.9 Task 7: Verify the Oracle Access Manager Upgrade

After the upgrade is complete, the Oracle Access Manager will be in the co-exist mode, by default. To verify that your Oracle Access Manager upgrade was successful:

1. Run the Upgrade Assistant again, and select **Verify Instance** on the Specify Operation screen.

   Follow the instructions on the screen for information on how to verify that specific Oracle Fusion Middleware components are up and running.

2. Use the following URL to verify that Oracle Access Manager 11*g* Administration server is up and running:

   Oracle Access Manager Administration server

   ```
   http://server:port/oam_admin
   ```

3. To verify that Oracle Access Manager 11*g* Managed Server is up and running, do the following:

   a. Login to Oracle WebLogic Server Administration Console using the required Administrator credentials.

   b. Expand **Domain Structure** on the left pane, and select **Deployments**.

   c. Verify that your managed server is listed in the **Summary of Deployments** page.

Alternatively, you can check the upgrade log file for any error messages or use Fusion Middleware Control to verify that Oracle Access Manager and any other Oracle Identity Management components are up and running in the Oracle Fusion Middleware environment.

For more information, see "Getting Started Using Oracle Enterprise Manager Fusion Middleware Control" in the *Oracle Fusion Middleware Administrator's Guide*.

12

Upgrading Oracle Adaptive Access Manager Environment

This chapter describes how to upgrade your existing Oracle Adaptive Access Manager 10*g* (10.1.4.5) to Oracle Adaptive Access Manager 11*g* Release 1 (11.1.1.5.0).

This chapter contains the following sections:

- Overview
- Prerequisites
- Task 1: Decide Upon an Oracle Adaptive Access Manager Topology
- Task 2: If Necessary, Upgrade the Oracle Database That Contains Oracle Adaptive Access Manager Schemas
- Task 3: Run Repository Creation Utility to Create Schemas
- Task 4: Install Oracle Fusion Middleware
- Task 5: Use Upgrade Assistant to Upgrade the Oracle Adaptive Access Manager Schema
- Task 6: Configure Oracle Adaptive Access Manager in a New or Existing Oracle WebLogic Domain
- Task 7: Configure Node Manager to Start Managed Servers
- Task 8: Stop the Administration Server and Oracle Adaptive Access Manager Managed Servers
- Task 9: Use Upgrade Assistant to Upgrade Oracle Adaptive Access Manager Middle Tier
- Task 10: Start the Administration Server and Oracle Adaptive Access Manager Managed Servers
- Task 11: Complete Any Required Oracle Adaptive Access Manager Post-Upgrade Tasks
- Task 12: Verify the Oracle Adaptive Access Manager Upgrade

12.1 Overview

When you run Upgrade Assistant to upgrade from Oracle Adaptive Access Manager 10*g*, the Upgrade Assistant upgrades most of the Oracle Adaptive Access Manager 10*g* configuration to Oracle Adaptive Access Manager 11*g*. In some cases, you have to upgrade manually after you run the Upgrade Assistant.

When you run Upgrade Assistant to upgrade from Oracle Adaptive Access Manager 10*g*, the Upgrade Assistant upgrades the following:

- Symmetric keys (used for encryption and decryption) in the Adaptive Risk Manager Web Application (ARM) keystores, `system_config.keystore`, and `system_db.keystoreKeys` are migrated to the Credential Store Framework (CSF) with the same aliases under the credential map `oaam`.

- The following Oracle Adaptive Access Manager properties files of Authenticator Web Application (ASA):

  - `bharosauio.properties`

  - `bharosa_client.properties`

  - `bharosa_common.properties`

- The following Oracle Adaptive Access Manager properties files of Adaptive Risk Manager Web Application (ARM):

  - `bharosa_server.properties`

  - `bharosa_common.properties`

The following components are not upgraded to the Oracle Adaptive Access Manager 11*g* environment when you run Upgrade Assistant to upgrade from Oracle Adaptive Access Manager 10*g*:

- ARM WebApp User Roles and Users

- `Log4j` settings

- Client-side Web Service configuration/settings in the ASA Web Application

- Client-side SOAP keystore with SOAP user password

- Any customizations, such as the following:

  - Custom Web Content (JSPs, CSS, etc)

  - Custom images

  - Custom Dynamic actions

  - Custom Loaders

  - Custom property files

You must upgrade such configuration manually after running Upgrade Assistant. For more information, see Task 11: Complete Any Required Oracle Adaptive Access Manager Post-Upgrade Tasks, *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*, and *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager*.

12.2 Prerequisites

You must complete the following prerequisites for upgrading to the Oracle Adaptive Access Manager 11*g* environment:

- Ensure that you have applied the Bundle Patch 07 to the Oracle Adaptive Access Manager 10*g* (10.1.4.5) and to the Oracle Database.

- Ensure that your database meets the system requirements. For more information see "*Oracle Fusion Middleware Installation Guide for Oracle Identity Management*". If it does not meet the requirement, then you must upgrade the database software before upgrading to Oracle Adaptive Access Manager 11*g*.

- Make sure that the Oracle Adaptive Access Manager 10*g* web applications are in exploded format.

- Ensure that Oracle Adaptive Access Manager 10*g* `webapp` folders and files can be accessed by Upgrade Assistant.

12.3 Task 1: Decide Upon an Oracle Adaptive Access Manager Topology

Before you install Oracle Adaptive Access Manager 11*g*, consider the topology you currently have in Oracle Adaptive Access Manager 10*g* (10.1.4.5) with Bundle Patch 07, as well as any requirements for your Oracle Fusion Middleware 11*g* environment.

For more information, refer to Chapter 10.2, "Oracle Adaptive Access Manager Topologies".

12.4 Task 2: If Necessary, Upgrade the Oracle Database That Contains Oracle Adaptive Access Manager Schemas

If you are upgrading an Oracle Adaptive Access Manager environment, you must ensure that the version of the database where you plan to install the Oracle Adaptive Access Manager schemas is supported by Oracle Fusion Middleware 11*g*.

For instructions on verifying that your database meets the requirements of Oracle Fusion Middleware 11*g*, see "Upgrading and Preparing Your Databases" in the *Oracle Fusion Middleware Upgrade Planning Guide*.

12.5 Task 3: Run Repository Creation Utility to Create Schemas

Run the Repository Creation Utility to create the Oracle Meta Data Services (MDS) schema into a supported database and complete the following:

- Running Repository Creation Utility in Preparation for an Oracle Adaptive Access Manager Upgrade

- Selecting the Schemas Required for Oracle Adaptive Access Manager Upgrade

12.5.1 Running Repository Creation Utility in Preparation for an Oracle Adaptive Access Manager Upgrade

For information about running Repository Creation Utility to install the Oracle Adaptive Access Manager schema, refer to the following documents:

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

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

After you start the Repository Creation Utility, follow the instructions on the Repository Creation Utility screens to connect to the database and create the required schemas.

12.5.2 Selecting the Schemas Required for Oracle Adaptive Access Manager Upgrade

You can use Repository Creation Utility to install the schemas required for all of the Oracle Fusion Middleware software components that require a schema. However, there is no need to install all the schemas unless you plan to install a complete Oracle Fusion Middleware environment and you plan to use the same database for all the Oracle Fusion Middleware component schemas.

For Oracle Adaptive Access Manager upgrade, you must select the following schemas when prompted by the Repository Creation Utility:

■ Expand **AS Common Schemas**, and select **Metadata Services** and **Audit Services**.

This schema supports Oracle Fusion Middleware Metadata Services (MDS), which is required by the Oracle Adaptive Access Manager component.

Note: The MDS Schema can be installed in a database other than the one where the Oracle Adaptive Access Manager schema is installed. However, ensure that the Oracle Adaptive Access Manager Managed Server can access your MDS schema.

12.6 Task 4: Install Oracle Fusion Middleware

Before you upgrade to Oracle Fusion Middleware 11g, you must install and configure an Oracle Fusion Middleware environment that is similar to the topology you set up for Oracle Application Server 10*g*. To do so, complete the following steps:

1. Installing Oracle WebLogic Server and Creating a Middleware Home

2. Installing Oracle Adaptive Access Manager 11g Release 1 (11.1.1.5.0)

12.6.1 Installing Oracle WebLogic Server and Creating a Middleware Home

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

For more information, see "Install Oracle WebLogic Server" in *Oracle Fusion Middleware Installation Planning Guide*.

In addition, see *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server* for complete information about installing Oracle WebLogic Server.

12.6.2 Installing Oracle Adaptive Access Manager 11*g* Release 1 (11.1.1.5.0)

For information about installing Oracle Adaptive Access Manager 11*g* Release 1 (11.1.1.5.0), refer to "Installing OAAM" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

Note: Do not configure the Oracle Adaptive Access Manager domain during the installation process.

12.7 Task 5: Use Upgrade Assistant to Upgrade the Oracle Adaptive Access Manager Schema

To upgrade the Oracle Adaptive Access Manager schema using Upgrade Assistant, perform the following steps:

1. Enter the following command to start the Upgrade Assistant:

   On UNIX systems (Located at *MW_HOME*/Oracle_<IDM_Home>/bin):

   ```
   ./ua
   ```

   On Windows systems (Located at *MW_HOME*\Oracle_<IDM_Home>\bin):

ua.bat

The Oracle Fusion Middleware Upgrade Assistant **Welcome** screen is displayed, as shown in Figure 12–1.

Figure 12–1   Upgrade Assistant Welcome Screen
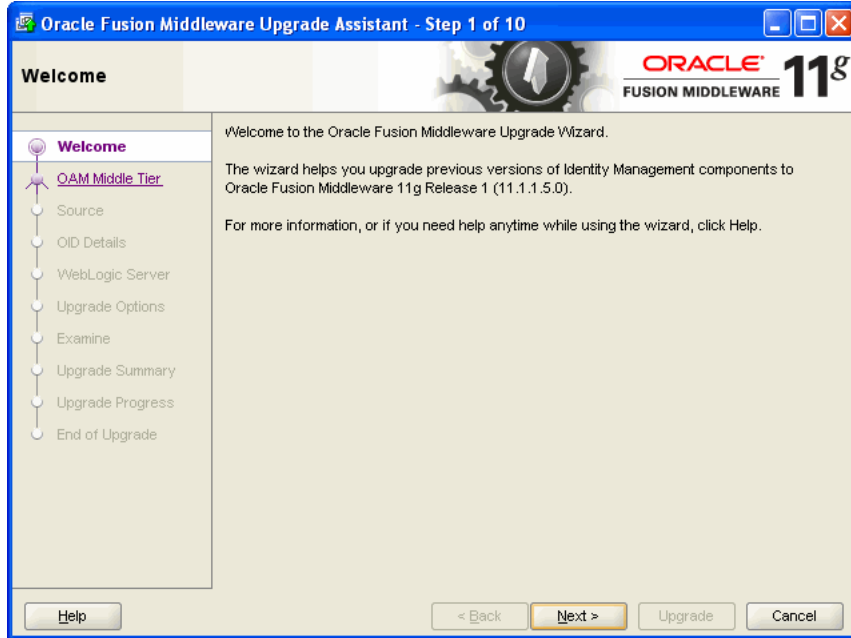
2.   Click **Next**.

The **Specify Operation** screen is displayed, as shown in Figure 12–2.

Figure 12–2   Upgrade Assistant Specify Operation Screen
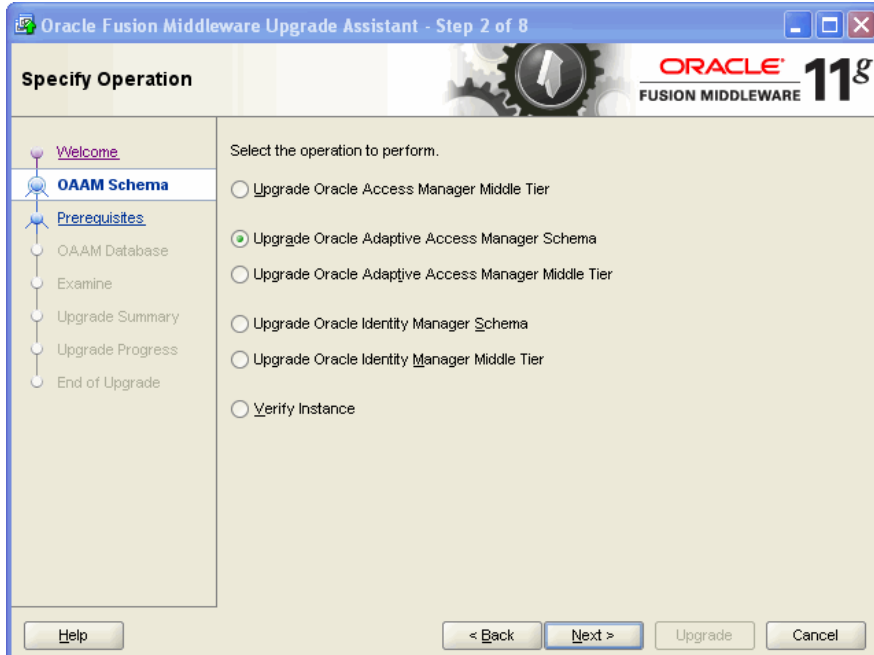
3. Select the **Upgrade Oracle Adaptive Access Manager Schema** option.

4. Click **Next**.

   The **Prerequisites** screen is displayed.

5. Select the **Database Schema backup completed** and **Database version is certified by Oracle for Fusion Middleware upgrade** options.

   Note:

   - Ensure that the database has been upgraded before checking the **Database Schema backup completed** option. For more information, see Task 2: If Necessary, Upgrade the Oracle Database That Contains Oracle Adaptive Access Manager Schemas.

   - For instructions on verifying that your database meets the requirements of Oracle Fusion Middleware 11*g*, see http://www.oracle.com/technology/software/products/ias/files/fusion_certification.html.
   ---

6. Click **Next**.

   The **Specify OAAM Source Database** screen is displayed.

7. Enter the following information:

   - **Database Type**: Select the database type from the drop-down list.

   - **Connect String**: Enter the connect string for the database.

     For example:

     ```
     host:port:sid
     ```

   - **OAAM Schema User**: Specify the Oracle Adaptive Access Manager 10*g* schema user name.

   - **DBA User**: Enter the user name for your database.

   - **DBA Password**: Enter the password for your database user.

8. Click **Next**.

   The **Examining Components** screen is displayed.

   Upgrade Assistant examines the components and checks that the source and target schemas contain the expected columns.

   Under the **Status** column, the word **succeeded** should appear. If instead, the word **failed** appears, inspect the log file for details.

   Note: If you want to view the log file for the current session, click on the link at the bottom of the screen to view the ua.log file.
   ---

9. Click **Next**.

   The **Upgrade Summary** screen is displayed.

10. Click **Upgrade**.

The **Upgrade Progress** screen is displayed. This screen provides the following information:

- Status of the upgrade

- Any errors or problems that occur during the upgrade

> **See Also:** "Troubleshooting Your Upgrade" in the *Oracle Fusion Middleware Upgrade Planning Guide* for specific instructions for troubleshooting problems that occur while running the Upgrade Assistant

11. Click **Next**.

The **Upgrade Complete** screen is displayed. This screen confirms that the upgrade was complete.

12. Click **Close**.

12.8 Task 6: Configure Oracle Adaptive Access Manager in a New or Existing Oracle WebLogic Domain

To configure Oracle Adaptive Access Manager in a new or existing Oracle WebLogic domain, refer to the "Configuring Oracle Adaptive Access Manager" section in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*. When you run the Oracle Fusion Middleware Configuration Wizard ensure that you configure the Managed Servers and assign them to machine.

> **Note:** Ensure that you specify the Oracle Adaptive Access Manager 10*g* database details in the screen where it prompts you to enter the Oracle Adaptive Access Manager 11*g* database details. You must enter the 10*g* credentials because there is no separate 11*g* database. It checks the database for a few system tables, which will not be present in Oracle Adaptive Access Manager 10*g* database. You can ignore these errors and complete the Oracle Adaptive Access Manager 11*g* installation.

12.9 Task 7: Configure Node Manager to Start Managed Servers

For information about configuring Node Manager, refer to the "Configuring Node Manager to Start Managed Servers" section in the *Oracle Fusion Middleware Administrator's Guide*.

12.10 Task 8: Stop the Administration Server and Oracle Adaptive Access Manager Managed Servers

If you have started the Oracle Adaptive Access Manager Administration Server and the Oracle Adaptive Access Manager Managed Servers, then you must stop the Oracle Adaptive Access Manager Administration Server and Managed Servers by running the following command on the command line:

Windows

```
stopManagedWebLogic.cmd oaam_admin_server1
stopManagedWebLogic.cmd oaam_server_server1
```

UNIX

```
stopManagedWebLogic.sh oaam_admin_server1
stopManagedWebLogic.sh oaam_server_server1
```

12.11 Task 9: Use Upgrade Assistant to Upgrade Oracle Adaptive Access Manager Middle Tier

To upgrade the Oracle Adaptive Access Manager middle tier:

> **Note:**   You can also use the Upgrade Assistant command-line interface to upgrade your Oracle Application Server 10*g* Oracle homes. For more information, see "Using the Upgrade Assistant Command-Line Interface" in the *Oracle Fusion Middleware Upgrade Planning Guide*.

1. If you have started the Oracle Adaptive Access Manager Managed Servers, then they will auto-generate symmetric keys required for encryption or decryption. You must delete keys before performing middle tier upgrade. To do so, complete the following steps:

    a. Log in to Oracle Enterprise Manager.

    b. Expand the WebLogic Domain on the left pane, and select the **OAAM** domain.

    The OAAM domain page is displayed.

    c. From the OAAM Domain, select **Security**, and then **Credentials**.

    The **Credentials** page is displayed.

    d. Expand **oaam** and delete the symmetric key related entries.

2. Run the following command to launch Upgrade Assistant:

    On UNIX systems (Located at *MW_HOME*/Oracle_<IDM_Home>/bin):

    ```
    ./ua
    ```

    On Windows systems (Located at *MW_HOME*\Oracle_<IDM_Home>\bin):

    ```
    ua.bat
    ```

    The Oracle Fusion Middleware Upgrade Assistant **Welcome** screen is displayed, as shown in Figure 12–3.

Figure 12–3   Upgrade Assistant Welcome Screen
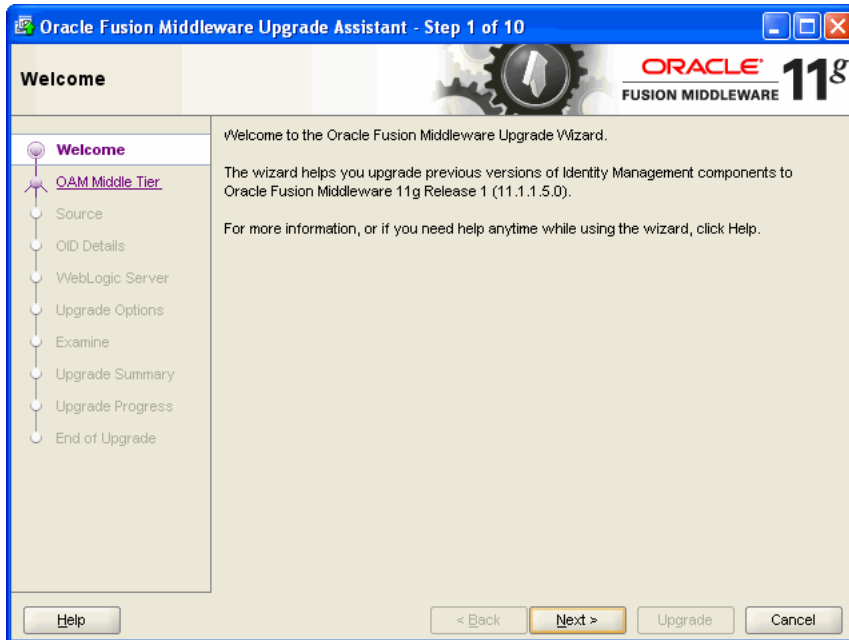
3. Click **Next**.

   The **Specify Operation** screen is displayed, as shown in Figure 12–4.

Figure 12–4   Upgrade Assistant Specify Operation Screen
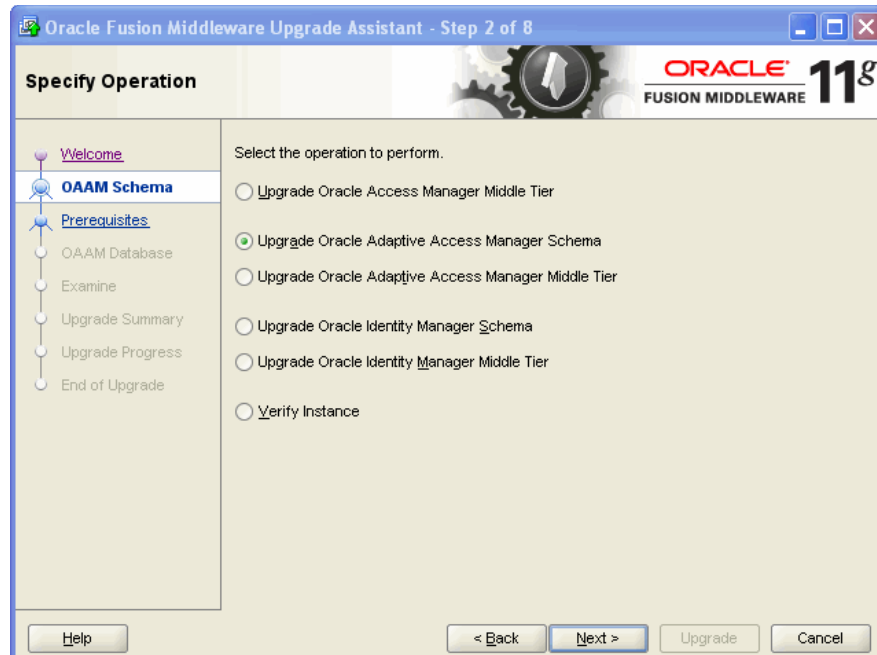
4. Select **Upgrade Oracle Adaptive Access Manager Middle Tier**.

   The options available in Upgrade Assistant are specific to the Oracle home from which it started. When you start Upgrade Assistant from an Oracle Application Server Identity Management Oracle home, the options shown on the Specify

Operation screen are the valid options for an Oracle Application Server Identity Management Oracle home.

5. Click **Next**.

   The **Specify Source Details** screen is displayed.

6. Enter the following information:

   - Click **Browse** and enter the directory location for Oracle Adaptive Access Manager Adaptive Strong Authenticator Web Application 10*g* (ASA) and Adaptive Risk Manager Web Application 10*g* (ARM) applications.

   - Database Type: Select the database type from the drop-down list.

   - Connect String: Enter the name of the server where your database is running. Use one of the following format for Oracle Database:

     `//host:port/service` or `host:port:sid`

   - Schema User Name: Enter the user name for the schema.

   - Schema Password: Enter the password for the schema.

7. Click **Next**.

   The **Specify WebLogic Server** screen is displayed.

8. Enter the following information about your Oracle WebLogic Server domain:

   - **Host**: The host name of the Oracle WebLogic Server domain.

   - **Port**: The listening port of the administration server. The default administration server port is `7001`.

   - **Username**: The user name that is used to log in to the administration server. This is the same username you use to log in to the Administration Console for the domain.

   - **Password**: The password for the administrator account that is used to log in to the administration server. This is the same password you use to log in to the Administration Console for the domain.

   - Click **Next**.

   The **Specify Upgrade Options** screen is displayed.

9. Select **Start destination components after successful upgrade**, and click **Next**.

   The **Examining Components** screen is displayed.

   Note: Ensure that Node Manager is running, before you select **Start destination components after successful upgrade**.

   ---

10. Click **Next**.

    The **Upgrade Summary** screen is displayed.

11. Click **Upgrade**.

    The **Upgrade Progress** screen is displayed. This screen provides the following information:

    - The status of the upgrade

    - Any errors or problems that occur during the upgrade

> **See Also:** "Troubleshooting Your Upgrade" in the *Oracle Fusion Middleware Upgrade Planning Guide* for specific instructions for troubleshooting problems that occur while running the Upgrade Assistant.

12. Click **Next**.

    The **Upgrade Complete** screen is displayed. This screen confirms that the upgrade was complete.

13. Click **Close**.

12.12 Task 10: Start the Administration Server and Oracle Adaptive Access Manager Managed Servers

You must start the Oracle Adaptive Access Manager Administration Server and the Oracle Adaptive Access Manager Managed Servers by running the following command on the command line:

Windows

```
startManagedWebLogic.cmd oaam_admin_server1
startManagedWebLogic.cmd oaam_server_server1
```

UNIX

```
startManagedWebLogic.sh oaam_admin_server1
startManagedWebLogic.sh oaam_server_server1
```

12.13 Task 11: Complete Any Required Oracle Adaptive Access Manager Post-Upgrade Tasks

You must perform the following additional post-upgrade tasks after upgrading your Oracle Adaptive Access Manager 10*g* environment to Oracle Adaptive Access Manager 11*g*:

- If you have any customizations in Oracle Adaptive Access Manager 10*g*, then you can migrate these customizations using the customizations or extensions shared library for Oracle Adaptive Access Manager. For more information, see the *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager*.

- You must manually configure the Java logging setting because `log4j` is not used in Oracle Adaptive Access Manager 11*g*.

- Configure application logging using Oracle Fusion Middleware Enterprise Manager or configure the logging properties file that is used by the servers.

- You must reconfigure users with relevant Oracle Adaptive Access Manager groups in Oracle Adaptive Access Manager domain by using the Oracle WebLogic Administration console. These users can then use the `oaam_admin` application. The User Group roles used in Oracle Adaptive Access Manager 10*g* use a different set of names in Oracle Adaptive Access Manager 11*g*. Table 12–1 lists the role mapping from 10*g* to 11*g*.

Table 12–1   User Group Mapping

Oracle Adaptive Access Manager 10.1.4.5 User Group	Oracle Adaptive Access Manager 11G User Group
CSRGroup	OAAMCSRGroup
CSRManagerGroup	OAAMCSRManagerGroup
CSRInvestigator	OAAMCSRInvestigatorGroup
Investigator	OAAMInvestigatorGroup
InvestigationManager	OAAMInvestigationManagerGroup
RuleAdministratorsGroup	OAAMRuleAdministratorGroup
EnvAdminGroup	OAAMEnvAdminGroup
AuditorsGroup	Not Available
SOAPServicesGroup	OAAMSOAPServicesGroup

- Basic required entities are shipped along with Oracle Adaptive Access Manager in the `Auth_EntityDefinition.zip` file, which is located in the *MW_HOME*/IDM_ ORACLE_HOME/oaam/init directory.You must import the basic entities into your system by completing the following steps:

  1. Log in to the Oracle Adaptive Access Manager Administration Console.

  2. Navigate to the Entities search page, by clicking **Entities** in the Navigation tree, or right-click **Entities** in the Navigation tree and select **Open** from the context menu that is displayed.

  3. In the Entities search page, click **Import**.

  4. In the Entities Import screen, click **Browse** and locate the `Auth_ EntityDefinition.zip` file.

  5. Click **OK**.

- You must back-up the symmetric keys used for encryption and decryption. You may need this keys, if you have to recreate the Oracle Adaptive Access Manager 11*g* domain. Steps to access these keys

  a. Log in to Oracle Enterprise Manager.

  b. Expand the WebLogic Domain on the left pane, and select **OAAM** domain.

     The OAAM domain page is displayed.

  c. From the OAAM Domain, select **Security**, and then **Credentials**.

     The **Credentials** page is displayed.

  d. Expand **oaam** and select the symmetric key related entries associated with the Type **Generic**.

  e. Click **Edit**.

  f. Go to the **Credentials** section then copy the symmetric key related entries and note the key name.

     Note: Repeat the above steps to back-up database and configuration keys.

12.14 Task 12: Verify the Oracle Adaptive Access Manager Upgrade

To verify that your Oracle Adaptive Access Manager upgrade was successful:

1. Run Upgrade Assistant again, and select **Verify Instance** on the Specify Operation page.

   Follow the instructions on the screen for information about how to verify that specific Oracle Fusion Middleware components are up and running.

2. Use the following URL to verify that Oracle Adaptive Access Manager 11*g* is up and running:

   Oracle Adaptive Access Manager Administration Server:

   ```
   http://hostname:oaam_admin_port/oaam_admin/ping
   ```

   Oracle Adaptive Access Manager Managed Server:

   ```
   http://hostname:oaam_server_port/oaam_server/ping
   ```

   Alternatively, you can check the upgrade log file for any error messages or use Fusion Middleware Control to verify that Oracle Adaptive Access Manager and any other Oracle Identity Management components are up and running in the Oracle Fusion Middleware environment.

   For more information, see "Getting Started Using Oracle Enterprise Manager Fusion Middleware Control" in the *Oracle Fusion Middleware Administrator's Guide*.

3. To verify that the Symmetric keys are created in CSF, perform the following:

   a. Log in to Oracle Enterprise Manager.

   b. Expand the WebLogic Domain on the left pane, and select **OAAM** domain.

      The OAAM domain page is displayed.

   c. From the OAAM Domain, select **Security**, and then **Credentials**.

      The **Credentials** page is displayed.

   d. Verify that **oaam** is listed in the **Credential Store Provider** table. Expand **oaam** and ensure that it includes the DESede_db_key_alias and DESede_config_key_alias entries.

4. Check the Oracle Adaptive Access Manager schema version, to ensure that the schema upgrade was successful.

5. Log in to the Oracle Adaptive Access Manager Administration Console as an existing user and ensure that you are able to access it.

6. To verify that you can search and view existing Sessions, perform the following:

   a. Log in to the Oracle Adaptive Access Manager Administration Console.

   b. In the Navigation tree, select **Sessions**. The Sessions search page is displayed.

   c. Search for the session by the details you are interested in.

   For more information, see the chapter "Using Session Details" in *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*.

13

Upgrading Oracle Identity Manager Environment

This chapter describes how to upgrade the existing 9.1 Oracle Identity Manager to Oracle Identity Manager 11*g*. For information on starting point for Oracle Identity Manager upgrade, see Section 9.3, "Supported Starting Points for Oracle Identity Manager".

This chapter contains the following sections:

Notes:

- You cannot upgrade Oracle Identity Manager 9.1 running on Microsoft SQL database to Oracle Identity Manager 11*g*.

- If you have an existing Oracle Identity and Access Management 11*g* Release 1 (11.1.1.3.0) installation then you can patch it to Oracle Identity and Access Management 11*g* Release 1 (11.1.1.5.0) as described in the chapter "Patching Oracle Identity and Access Management" in the *Oracle Fusion Middleware Patching Guide*.

- Upgrade Overview
- Prerequisites
- Task 1: Identify and Prepare Oracle Database for Oracle Identity Manager 11g (Optional)
- Task 2: Use the Repository Creation Utility to Create the Schema in the Database
- Task 3: Install Oracle Fusion Middleware
- Task 4: Use Upgrade Assistant to Upgrade the Oracle Identity Manager Schema
- Task 5: Create a WebLogic Domain for Oracle Identity Manager
- Task 6: Start the WebLogic Administration Server
- Task 7: Configure Oracle Identity Manager Server 11g
- Task 8: Configure Node Manager to Start Managed Servers
- Task 9: Start the SOA Managed Server
- Task 10: Start the Oracle Identity Manager Managed Server
- Task 11: Stop the Oracle Identity Manager Managed Server
- Task 12: Use Upgrade Assistant to Upgrade Oracle Identity Manager Middle Tier

- Task 13: Start the Oracle Identity Manager Managed Server

- Task 14: Complete Any Required Oracle Identity Manager Post-Upgrade Tasks

- Task 15: Verify the Oracle Identity Manager Upgrade

13.1 Upgrade Overview

When you run Upgrade Assistant to upgrade from Oracle Identity Manager 9.1 to Oracle Identity Manager 11*g*, the Upgrade Assistant upgrades most of the Oracle Identity Manager 9.1 configuration to Oracle Identity Manager 11*g*.

This section describes some of the key differences in Oracle Identity Manager 11*g* such as the following:

- Application Server and JVM Support

- Database Support

- Request Management

- Authorization

- Access Policy

- Approval Process

- Scheduled Tasks

- User Interfaces Customization

- Object Forms

- Prepopulate Adapters

- Task Assignment Adapters

- Event Handlers

- Signature-Based Login

- Application Programming Interface

- Task Assignments

- After You Upgrade

13.1.1 Application Server and JVM Support

Oracle Identity Manager 11*g* only supports Oracle WebLogic Server as the deployment platform. Other application Servers such as OC4J, IBM WebSphere, and JBoss are not supported. Table 13–1 gives a comparison between the Application Server and JVM combinations supported for Oracle Identity Manager 9.1 and Oracle Identity Manager 11*g*.

Table 13–1   Application Server and JDK Support for Oracle Identity Manager 11g

Oracle Identity Manager 9.1	Oracle Identity Manager 11*g*
Oracle WebLogic Server on Sun JDK, Oracle JRockit, or HP JDK.	Oracle WebLogic Server on Sun JDK or JRockit JDK.
JBoss Application Server on Sun JDK, Oracle JRockit, or HP JDK.	Oracle WebLogic Server on Sun JDK or JRockit JDK.
OC4J on Sun JDK, Oracle JRockit, or HP JDK.	Oracle WebLogic Server on Sun JDK or JRockit JDK.

Table 13–1   (Cont.) Application Server and JDK Support for Oracle Identity Manager 11g

Oracle Identity Manager 9.1	Oracle Identity Manager 11*g*
IBM WebSphere Application Server on IBM JDK	Oracle WebLogic Server on Sun JDK or JRockit JDK.

> **Note:**   When you are upgrading to Oracle Identity Manager 11*g* ensure that you use the same JDK provided that you used in Oracle Identity Manager 9.1.

13.1.2 Database Support

Oracle Identity Manager 9.1 supports Microsoft SQL Server and Oracle Database. In Oracle Identity Manager 11*g* only Oracle Database is supported.

13.1.3 Request Management

Oracle Identity Manager 11*g* supports:

- SOA Composite based approval processes
- New types of Requests like Create User and Assign Roles
- Enhanced Bulk Request
- Request Templates

> **Note:**   Oracle Identity Manager 11*g* does not support organization - based request - provisioning.

Many Oracle Identity Manager 9.1 request related customizations may no longer be necessary after upgrading to Oracle Identity Manager 11*g*, since they are available out-of-the box. For more information about request related features refer to the *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*.

13.1.4 Authorization

Application access controls to perform various operations are controlled by the authorization engine embedded in Oracle Identity Manager 11*g* with the help of authorization policies. The authorization policies determine at runtime whether a user is allowed to perform a particular action or not. You can define authorization policies that satisfy the authorization requirements within Oracle Identity Manager 11*g*.

In Oracle Identity Manager 9.1, each component defined and managed its own authorization policy user interface and backend implementation.

In Oracle Identity Manager 11*g*, authorization policy management is centralized as an administrative feature and enforced by an embedded version of Oracle Entitlements Server. These authorization policies secure access control to the Oracle Identity Manager 11*g* application, thereby defining "who can do what" inside the application.

In Oracle Identity Manager 9.1, all data related to Organization Administrator was stored in the AAD table in the Oracle Identity Manager schema. This information is primarily used to ascertain the user groups which are allowed to perform operations on the respective organizations and hence the users in that organization.

In Oracle Identity Manager 11*g*, during the upgrade process the contents of AAD table will be read and an Oracle Entitlements Server policy will be created for User Management feature.

In Oracle Identity Manager 9.1, all data related to Group Administrator was stored in GPP table in the Oracle Identity Manager schema. This information is primarily used to ascertain the user groups, which are allowed to perform operations on the other groups they manage.

In Oracle Identity Manager 11*g*, during the upgrade process the contents of GPP table will be read and an Oracle Entitlements Server policy will be created for User Management feature.

For more details about Oracle Entitlements Server, see http://www.oracle.com/technology/products/id_mgmt/oes/index.html.

13.1.5 Access Policy

Access policies are a list of roles to which you define roles for provisioning resources to users that are members of the roles to which the access policy is attached. Access policies are defined using the Create Access Policy and Manage Access Policies menu items in the Oracle Identity Manager 11*g* Administrative and User Console. For more information, see the *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*.

13.1.6 Approval Process

Table 13–2 shows how the approval process differ when you upgrade from Oracle Identity Manager 9.1 to Oracle Identity Manager 11*g*.

Table 13–2   Approval Process

Oracle Identity Manager 9.1	Oracle Identity Manager 11*g*
Approval Processes	SOA Composites
Process Determination Rules	Approval Policies

When you run Upgrade Assistant for upgrading the Oracle Identity Manager middle tier upgrade, a report is generated. This report lists the new approval policies and SOA composites that will be created during the upgrade. This report is located at IDM_HOME/upgrade/workflow/report.html.

After upgrading from Oracle Identity Manager 9.1 to Oracle Identity Manager 11*g*, note the following:

- Some of the approval processes may not be fully converted to SOA composites. These SOA composites must be manually modified.

- The generated SOA composites are not automatically deployed to the SOA Server. After you complete the upgrade process, you can deploy SOA composite to SOA server as described in "Deploying the SOA Composite" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

- For all the approval processes that are specific to a resource, the corresponding approval policies created as part of the upgrade will be at the operational level. For the approval processes associated with the resource "Request", the corresponding approval policies created will be at the request level. For more information about approval policy, refer to the *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*.

- Approval processes associated with organization provisioning are not upgraded as part of the middle tier upgrade. Request-based organization provisioning is not supported in Oracle Identity Manager 11*g*.

- Approval policies that are created during the upgrade will always be associated with DefaultOperationalApproval. Workflow upgrade report will specify this information.

- E-mail templates associated with approval processes will not be migrated to SOA composites.

> **Note:** Oracle recommends you to reuse similar SOA composites as approval processes for different resources.

For more information, see Task 14: Complete Any Required Oracle Identity Manager Post-Upgrade Tasks.

The Approval process is partially upgraded if:

- Event handlers or adapters are associated with System Validation and provide Information tasks.

- Task information is used in creating the task assignment rule.

- Process information is used in framing the task assignment rule with attributes, such as Process Name and Process Type.

- Task of the approval process is associated with the Task Assignment Adapter or Event Handler or Process Task Adapter.

13.1.7 Scheduled Tasks

After upgrade, all scheduled tasks are migrated automatically to the Oracle Identity Manager 11*g* Scheduled Tasks and Jobs. For more information, see "Managing Scheduled Tasks" in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager*.

The content of the Oracle Identity Manager 9.1 Job History will be obsolete after you upgrade to Oracle Identity Manager 11*g*.

13.1.8 User Interfaces Customization

In Oracle Identity Manager 9.1 you can customize the following components of your Oracle Identity Manager Administrative and User Console:

- General page layout

- Descriptive text, labels, and error messages

- Colors, fonts, and alignment

- Logos

- Self-registration, user initiated profile editing, and related approvals

- Field configuration on pages

- Menu selections that are available to users

Oracle Identity Manager 11*g* upgrade process does not retain the above customizations done in Oracle Identity Manager 9.1 environment. You must recreate user interface customizations after you upgrade to Oracle Identity Manager 11*g*. If the

user interface is an ADF-based page, then the user interface customization needs to done using ADF Faces technology. Transitional-UI-based pages can be customized using the same Oracle Identity Manager 9.1 Struts-based technology. For more information on user interface customizations, see "Customizing Oracle Identity Manager Interfaces"refer to the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

> **Notes:**
>
> - Visible menu items cannot be customized by changing menu permissions.
> - User Defined Fields request form are not upgraded to Oracle Identity Manager 11*g*.

13.1.9 Object Forms

As part of the upgrade process, all the object forms are converted to request datasets. The dataflow mappings are also migrated to request datasets. After upgrading to Oracle Identity Manager 11*g* you must reattach a prepopulate adapter to a form field. For more information, see Rewriting Prepopulate Adapters.

13.1.10 Prepopulate Adapters

Prepopulate adapters attached to Oracle Identity Manager 9.1 Object Forms should be converted or re-implemented as prepopulate plug-ins in Oracle Identity Manager 11*g*. For Process Forms, the prepopulate adapters work similarly to how Prepopulate adapters worked in Oracle Identity Manager 9.1. After upgrade you must complete the steps described in Rewriting Prepopulate Adapters.

13.1.11 Task Assignment Adapters

Task Assignment adapters associated with approval tasks are not upgraded. The task assignment logic of approval tasks that correspond to approval processes should be re-written as SOA composites. For more information, see Using Generated SOA Composite as Approval Process.

13.1.12 Event Handlers

In Oracle Identity Manager 9.1, event handlers provided the capability to add various customizations on a certain data object life cycle events like Insert, Update, or Delete using Data Object Manager in the Design Console.

In Oracle Identity Manager 11*g*, User Management, Role Management and Request have been redesigned to use the Orchestration Framework where you can define various event handlers for life cycle management events like Create, Update, or Delete. The orchestration framework also provides the capability for event handlers to be executed in either a synchronous or asynchronous fashion. Table 13–3 shows the mapping for Role entity. Similar mapping will also be applicable for User and Request entities.

Table 13–3　Event Handlers Mapping

Form Name	Handler	Stage	Action
User Group	Pre Insert	Pre Processing	CREATE
User Group	Post Insert	Post Processing	CREATE

Table 13–3   (Cont.) Event Handlers Mapping

Form Name	Handler	Stage	Action
User Group	Pre Update	Pre Processing	MODIFY
User Group	Post Update	Post Processing	MODIFY
User Group	Pre Delete	Pre Processing	DELETE
User Group	Post Delete	Post Processing	DELETE

13.1.13 Signature-Based Login

In Oracle Identity Manager 9.1, connecting remotely to Oracle Identity Manager and execute Oracle Identity Manager APIs was done by signature-based login. Oracle Identity Manager 11*g* supports signature-based login. However, Oracle recommends that you use the username-password approach for logging into Oracle Identity Manager. To do this in a secure manner, use the Credential Store Framework. For more information, see *Oracle Fusion Middleware Application Security Guide*.

13.1.14 Application Programming Interface

Oracle provides a network-aware, Java-based application programming interface (API) that exposes services available in Oracle Identity Manager. This API is based on Plain Old Java Objects (POJO) and handles the plumbing required to interact with Oracle Identity Manager. This API can be used for building clients for Oracle Identity Manager and for integrating third-party products with the Oracle Identity Manager platform.

In Oracle Identity Manager 11*g*, some of the legacy APIs have been rewritten to use the new architecture. The corresponding utility services or interface classes have been changed. Table 13–4 provides a high-level mapping between the legacy and new interfaces.

Table 13–4   API Mapping

Legacy Service	New Service
`Thor.API.Operations.tcUserOperationsIntf`	`oracle.iam.identity.usermgmt.api.UserManager`
`Thor.API.Operations.tcGroupOperationsIntf`	`oracle.iam.identity.rolemgmt.api.RoleManager`
`Thor.API.Operations.tcOrganizationOperationsIntf`	`oracle.iam.identity.orgmgmt.api.OrganizationManager`
`Thor.API.Operations.tcRequestOperationsIntf`	`oracle.iam.request.api.RequestService`
Thor.API.Operations.tcSchedulerOperationsIntf	`oracle.iam.scheduler.api.SchedulerService`
`Thor.API.Operations.tcEmailOperationsIntf`	`oracle.iam.notification.api.NotificationService`

> **Note:**   You must manually implement and compile the APIs after you upgrade to Oracle Identity Manager 11*g*. For more information, see "Using APIs" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

13.1.15 Task Assignments

In Oracle Identity Manager 11*g*, some of the task assignments have been rewritten to use new architecture. Table 13–5 provides a high-level mapping between the legacy and new assignment types.

After upgrading to Oracle Identity Manager 11*g*, you need to manually reimplement task assignment logic in SOA composite.

Table 13–5   Assignment Types

Assignment Types in Oracle Identity Manager 9.1	Assignment Types in Oracle Identity Manager 11*g*
Object Administrator User with Least Load	Object Administrator User with Least Load
Object Administrator	Object Administrator
Object Authorizer User with Highest Priority	This will be assigned to role Object Authorizer
Group User With Highest Priority	'This will assigned to role
Object Authorizer User with Least Load	Object Authorizer User with Least Load
Requestor's Manager	Requestor's Manager
Request Target Users Manager	Beneficiary Manager Approval
Group User with Least Load	Group User with Least Load
Group	This will be assigned to role

After upgrading to Oracle Identity Manager 11*g*:

- Process tasks assigned to Group User With Highest Priority will be modified and assigned to Group User With Least Load.

- Process tasks assigned to Object Authorizer User With Highest Priority will be modified and assigned to Object Authorizer User With Least Load.

13.1.16 After You Upgrade

After upgrading to Oracle Identity Manager 11*g*:

- Event handlers associated with User data object has been removed from Oracle Identity Manager 11*g*:

  - `tcUSRcheckACT`

  - `tcUSRTriggerUserProcesses`

  - `tcUSRCheckUsrOrgChange`

  - `tcUSRautoGroupMembership`

  - `tcUSRevaluatePolicies`

- The logged-in user can not create a user in other organizations but can see all the organizations.

- Users cannot modify manager or organization attributes that is created by other organization.

- All approval tasks for new requests will be assigned to System Administrator (`xelsysadm`).

- All credentials are moved to the CSF Store.

- Vacation rules for each Oracle Identity Manager 9.1 proxy user is automatically created.

- Custom jars (Located at `OIM_HOME/JavaTasks`, `OIM_HOME/ScheduleTask`, and OIM_HOME/ThirdParty) and custom resource bundles stored in the file system folder in Oracle Identity Manager 9.1 are move to Oracle Identity Manager 11*g* schema.

- The ALL USERS role cannot be assigned to the `XELSYSADM` user. Oracle recommends that you do not have resources or entitlements in target applications granted due to the ALL USERS role.

13.2 Prerequisites

You must complete the following prerequisites before upgrading to the Oracle Identity Manager 11*g* environment:

- Backing Up the Oracle Identity Manager 9.1 Database
- Running Pending Transaction Report Utility
- Running OSI Data Upgrade Utility
- Running Schedule Task to Process the Audit Messages
- Emptying JMS queues
- Circular Dependencies for Approval Workflow

13.2.1 Backing Up the Oracle Identity Manager 9.1 Database

Ensure that you back up your existing Oracle Identity Manager database. For more information see:

- *Oracle9i Backup and Recovery Documentation Online Roadmap*
- *Oracle Database Backup and Recovery Basics 10g Release 2 (10.2)*
- *Oracle Database Backup and Recovery Reference 11g Release 1 (11.1)*

13.2.2 Running Pending Transaction Report Utility

You must run the pending transaction report utility to analyze your Oracle Identity Manager 9.1 before you start the upgrade process. You must download the pending transaction report utility as described in the note 1316738.1 note at `https://support.oracle.com` and complete the following steps:

1. Set the environment variables as shown in Table 13–6:

Table 13–6   Environment Variables

Environment Variable	Values
MW_HOME	Specify the path of the Oracle Identity Manager's Middleware home. The following example shows the full path: `/oracle/Middleware`
WL_HOME	Specify the path of the Oracle WebLogic Server home. The following example shows the full path: `oracle/Middleware/wlserver_10.3`

Table 13–6 (Cont.) Environment Variables

Environment Variable	Values
JAVA_HOME	Specify the path of the Java home. The following example shows the full path:
	MW_HOME/jdk160_24/
XEL_HOME	Specify the path of the Oracle Identity Manager 9.1 server home. The following example shows the full path:
	/installServer/Xellerate

2. Run generatePendingTransactionReport.bat (Located at MW_HOME\Oracle_IDM1\server\bin) for Windows or generatePendingTransactionReport.sh (Located at MW_HOME/Oracle_IDM1/server/bin) for UNIX and provide the following details:

   - jdbc url [hostname:portname:sid]

   - Oracle Identity Manager schema username

   - Oracle Identity Manager schema password

   - Directory where you save the reports.

The pending transaction report utility generates a report which includes the following details:

- Pending Recon: This includes all events that are deferred to a later date.

- Pending Request: This includes all requests (including self registration) pending approval.

- JMS Queues: This includes all messages, which are in unprocessed state. A JMS message is submitted in case of off-line provisioning. So this report will provide details of the entire pending provisioning task including task, which are initiated in offline mode.

The following are the pending transactions which can exist in your environment:

- All pending recon events generated in OIM 9.1 must be processed. Failed events will not be upgraded, if left unaddressed.

- All pending approval tasks generated in Oracle Identity Manager 9.1 must be processed. Pending approval tasks will not be upgraded, if left unaddressed. Ensure that these reach a final state before the Upgrade.

- Scheduled task execution history in Oracle Identity Manager 9.1 will not be upgraded. Ensure that you finish all pending scheduled tasks and there is no scheduled task running during the upgrade period.

- Any asynchronous audit processing must be processed in Oracle Identity Manager 9.1 before upgrading to Oracle Identity Manager 11*g*.

- All JMS queues should be empty. JMS messages in regular or error queues will not be migrated in Oracle Identity Manager 11*g*. Wait for all JMS messages to be consumed, take proper manual actions for JMS error messages and clean all JMS tables before upgrading to Oracle Identity Manager 11*g*. For more information, see Emptying JMS queues.

13.2.3 Running OSI Data Upgrade Utility

You must run the OSI Data Upgrade utility for Oracle Identity Manager 9.1 before you start the upgrade process. To do so, refer to the note 1303215.1 at https://support.oracle.com.

> **Notes:**
>
> - Ensure that you back up your existing Oracle Identity Manager database as described in Section 13.2.1, "Backing Up the Oracle Identity Manager 9.1 Database".
>
> - OSI Data Upgrade utility is available with the Oracle Identity Manager 9.1.0.2 Bundle Patch 15.

13.2.4 Running Schedule Task to Process the Audit Messages

Oracle recommends you to run the `Issue Audit Messages Task` schedule task to process pending audit messages for Oracle Identity Manager 9.1.

13.2.5 Emptying JMS queues

You must empty the JMS queues to ensure that the JMS messages are processed before you start the upgrade. To do so, complete the following:

1. Disable access by end-users, SPML, or API clients to Oracle Identity Manager. The steps to do this will depend on your existing environment. For example, you can modify the firewall configuration to deny end-users access to Oracle Identity Manager or if you have fronted the Oracle Identity Manager application server with a Oracle HTTP server then you can shutdown the Oracle HTTP server but ensure that the application server is up and running. Any SPML or API clients (For example, Active Directory Password Synch or any custom clients) can be shutdown.

2. Disable all scheduled tasks using the Design Console. For more information, see *Oracle Identity Manager Design Console Guide*.

3. Monitor the JMS queues and allow Oracle Identity Management to run for some time, until all JMS queues except error queues (e.g. xlErrorQueue), are empty.

4. Stop the Oracle Identity Manager 9.1. Depending on the application server you use, see the Oracle Identity Management Release 9.1.0.1 documentation library for more information.

   > **See:** For more information, see the Oracle Identity Management Release 9.1.0.1 documentation library at: http://download.oracle.com/docs/cd/E14049_01/index.htm

13.2.6 Circular Dependencies for Approval Workflow

Oracle Identity Manager 11*g* does not support circular dependencies for approval workflow where a approval task you create for example task1 response to another approval task for example task2, and task2 response is set to task1. Before you start the upgrade process, you must remove task2 from the response generated tasks in task1 using the Design Console. For more information, see *Oracle Identity Manager Design Console Guide*.

13.3 Task 1: Identify and Prepare Oracle Database for Oracle Identity Manager 11*g* (Optional)

This is an optional step, for an out-of-place upgrade using a new database instance and schema. Before upgrading to Oracle Identity Manager 11*g*, you must decide on one of the following option for the Oracle database:

- Importing the Existing Oracle Identity Manager 9.1 Database
- Installing a New Oracle Database

The database must also be compatible with Oracle Fusion Middleware 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/technetwork/middleware/ias/downloads/fusion-requirements-1
00147.html

13.3.1 Importing the Existing Oracle Identity Manager 9.1 Database

You can import the Oracle Identity Manager 9.1 Database to Oracle Identity Manager 11*g* database. To do so, complete the following steps:

1. Set the environment variables, by running the following commands on the command line:

    ```
    export ORACLE_HOME= <Installlation directory of oracle Database, for example:
    /app/product/11.1.0/db_1
    export ORACLE_SID=orcl
    export PATH=$PATH:app/product/11.1.0/db_1/bin
    ```

2. Create the user, by running `prepare_xl_db.sh` command (Located at: `OIM9101/installServer/Xellerate/db/oracle` in UNIX) or `prepare_xl_db.bat` command (Located at: `OIM9101\installServer\Xellerate\db\oracle` in Windows) on the command line and enter the required information as shown in the following example:

    ```
    ## Enter the ORACLE HOME directory or Press [Enter] to
       accept the default Oracle/product/11.1.0/db_1 as ORACLE_HOME.

    ## Current database <ORACLE_SID> is orcl
       Do you want to continue with this database [y,Y,n,N] ?

    y

    ## Enter the Oracle Identity Manager user name

    oim1

    ## Enter the password for Oracle Identity Manager (oimn1) user

    ## Enter the tablespace to hold the Oracle Identity Manager user data

    oimn1

    ## Enter the directory to store the datafile for the Oracle Identity Manager
    tablespace

    /Oracle
    ```

```
## Enter the name of the datafile without the extension .dbf
   (For e.g. xeltspace_01)

oim1

## Enter the Temporary tablespace for Oracle Identity Manager User

temp

Validating the given inputs...
Validating the given inputs is done.

Preparing the database for Oracle Identity Manager. Please wait...

Database preparation is successful. Please check the log
file prepare_xell_db.lst for more info.
```

3. Export Oracle Identity Manager 9.1 database, as shown in the following example:

```
expdp system/welcome@psr  DIRECTORY=DATA_PUMP_DIR SCHEMAS=Name_OIM  DUMPFILE=
expmOIMa%U.dmp,expmOIMb%U.dmp,expmOIMc%U.dmp,expmOIMd%U.dmp PARALLEL=4
LOGFILE=exp_ilt_oim_OIM_05jan.log   content=ALL JOB_NAME=exp_05jan
```

4. Import Oracle Identity Manager 9.1 database, as shown in the following example:

> **Note:** Ensure that you set NLS_LANG to match the database charset
> before importing. If you do not set the NLS_LANG correctly, you will
> get the following warnings:
>
> - EXP-00091: Exporting questionable statistics
> - non-English characters in your data may become corrupted

```
impdp system/welcome@psr  DIRECTORY=DATA_PUMP_DIR SCHEMAS=Name_OIM  DUMPFILE=
expmOIMa%U.dmp,expmOIMb%U.dmp,expmOIMc%U.dmp,expmOIMd%U.dmp PARALLEL=4
LOGFILE=imp_ilt_oim_OIM_05jan.log   content=ALL JOB_NAME=imp_05jan
```

13.3.2 Installing a New Oracle Database

If you do not have an Oracle Database installed, then you can install an Oracle
Database before you can install Oracle Identity Manager 11*g*. The database must be up
and running to install the Oracle Identity Manager 11*g*. The database does not have to
be on the same system where you are installing the Oracle Identity Manager 11*g*.

> **Note:** Ensure that the following database parameters are set:
>
> - `'aq_tm_processes' >= 1`
> - `'db_cache_size' >= '150994944'`
> - `'java_pool_size'>= '125829120'`
> - `'shared_pool_size' >= '183500800'`
>
> If you are installing a new database, be sure to configure your database to use AL32UTF8 character set encoding. If your database does not use the AL32UTF8 character set, you will see the following warning when running RCU: "The database you are connecting is with non-AL32UTF8 character set. Oracle strongly recommends using AL32UTF8 as the database character set." You can ignore this warning and continue using RCU. You need AL32UTF8 for globalization support in Oracle Identity Manager.

The following database versions are supported:

- 10.2.0.4
- 11.1.0.7
- 11.2

> **Note:** For the latest information about supported databases, visit the following Web site:
>
> http://www.oracle.com/technetwork/middleware/ias/downloads/fusion
> -certification-100350.html

Table 13–7 lists the databases requirements for RCU at the time of publication:

Table 13–7 RCU Database Requirements

Category	Minimum or Accepted Value
Version	Oracle Database 10.2.0.4, 11.1.0.7, or 11.2 (11.1.0.7 or later for non-XE database). **Note**: When installing the database, you must choose the AL32UTF8 character set.
Shared Pool Size	147456 KB
SGA Maximum Size	147456 KB
Block Size	8 KB
Processes	500

> **Note:** After installing the Oracle 11*g* database, you must complete the following steps:
>
> 1. Log in to the database as the `sys` (default) user.
> 2. Run the following commands:
>
>    ```
>    alter system set session_cached_cursors=100
>    scope=spfile;
>    ```
>
>    ```
>    alter system set processes=500 scope=spfile;
>    ```
>
> 3. Bounce the database and continue with the installation of Oracle Fusion Middleware Repository Creation Utility (RCU) and loading of schemas.

13.4 Task 2: Use the Repository Creation Utility to Create the Schema in the Database

Before you can upgrade to Oracle Identity Manager 11*g*, you must first create the Oracle Meta Data Services (MDS) schema and SOA schema into a supported database.

For more information, see "Upgrading and Preparing Your Databases" in the *Oracle Fusion Middleware Upgrade Planning Guide*.

For more information about installing the Oracle Meta Data Services (MDS) schema and SOA schema, refer to the following sections:

- Verifying that the Database Meets the Minimum Requirements for the Oracle Identity Manager Schema
- Running the Repository Creation Utility in Preparation for Upgrading Oracle Identity Manager

13.4.1 Verifying that the Database Meets the Minimum Requirements for the Oracle Identity Manager Schema

Before performing any installation you should read the system requirements and certification documentation to ensure that your environment meets the minimum installation requirements for the products you are installing.

For more information, refer to "System Requirements and Prerequisites" in the *Oracle Fusion Middleware Installation Planning Guide*.

13.4.2 Running the Repository Creation Utility in Preparation for Upgrading Oracle Identity Manager

To run the Repository Creation Utility to install the Oracle Identity Manager schema in the database, refer to the following resources:

- Creating Database Schema Using the Oracle Fusion Middleware Repository Creation Utility (RCU) in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*
- *Oracle Fusion Middleware Repository Creation Utility User's Guide*.

After you start the Repository Creation Utility, follow the instructions on the Repository Creation Utility screens to connect to the database and create the required schemas.

During the installation of the schema, on the **Select Components** screen, expand **Oracle AS Repository Components**, and select the following:

- Select **Metadata Services** under **AS Common Schemas**.

- Select **SOA Infrastructure** and **User Messaging Service** under **SOA and BPM Infrastructure**.

13.5 Task 3: Install Oracle Fusion Middleware

The following sections describes how to install Oracle Fusion Middleware 11*g* middle tier instances in preparation for an upgrade to Oracle Fusion Middleware 11*g*:

- Task 3a: Installing Oracle WebLogic Server and Creating the Middleware Home

- Task 3b: Installing Oracle Identity Manager 11g Release 1 (11.1.1.5.0)

- Task 3c: Installing Oracle SOA 11g Release 1 (11.1.1.5.0) Suite

13.5.1 Task 3a: Installing Oracle WebLogic Server and Creating the Middleware Home

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

For more information, see "Install Oracle WebLogic Server" in *Oracle Fusion Middleware Installation Planning Guide*.

In addition, see *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server* for complete information about installing Oracle WebLogic Server.

13.5.2 Task 3b: Installing Oracle Identity Manager 11*g* Release 1 (11.1.1.5.0)

You must install Oracle Identity Manager in the new middleware home you created in Task 3a: Installing Oracle WebLogic Server and Creating the Middleware Home. For installing Oracle Identity Management, refer to the section "Installing Oracle Identity and Access Management (11.1.1.5.0)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

> **Note:** Do not configure the Oracle Identity Manager domain during the installation process.

13.5.3 Task 3c: Installing Oracle SOA 11*g* Release 1 (11.1.1.5.0) Suite

You must install Oracle SOA Suite in the new middleware home you created in Task 3a: Installing Oracle WebLogic Server and Creating the Middleware Home.To install Oracle SOA Suite, refer to the "Installing Oracle SOA Suite" chapter in the *Oracle Fusion Middleware Installation Guide for Oracle SOA Suite*.

> **Note:** Ensure that you install a dedicated Oracle SOA Suite for Oracle Identity Manager.

13.6 Task 4: Use Upgrade Assistant to Upgrade the Oracle Identity Manager Schema

To upgrade the Oracle Identity Manager schema using Upgrade Assistant, perform the following steps:

1. Enter the following command to launch Upgrade Assistant.

On UNIX systems (Located at *MW_HOME*/Oracle_IDM1/bin):

```
./ua
```

On Windows systems (Located at *MW_HOME*\Oracle_IDM1\bin):

```
ua.bat
```

The Oracle Fusion Middleware Upgrade Assistant **Welcome** screen is displayed, as shown in Figure 13–1.

Figure 13–1   Upgrade Assistant Welcome Screen
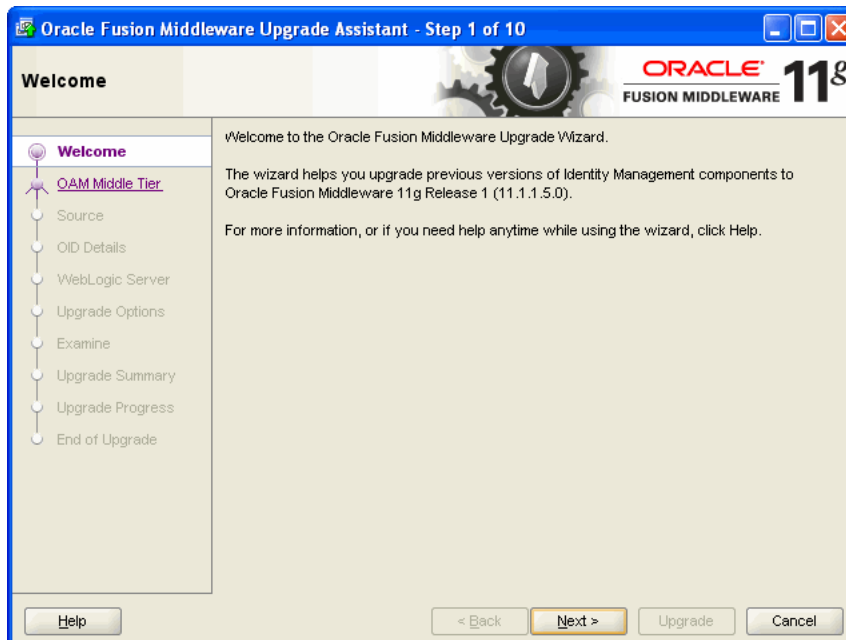
2. Click **Next**.

    The **Specify Operation** screen is displayed.

3. Select the **Upgrade Oracle Identity Manager Schema**.

4. Click **Next**.

    The **Prerequisite** screen is displayed.

5. Check the **Database Schema backup completed**, **Database version is certified by Oracle for Fusion Middleware upgrade**, and **OSI Data Upgrade Performed** check boxes.

    Database schema backup completed - Oracle recommends that you backup your Oracle Identity Manager repositories on the database before upgrading. The Upgrade Assistant does not verify that the repositories have been backed up, so this option serves as a reminder.

    Database version is certified by Oracle for Fusion Middleware upgrade - The Upgrade Assistant requires that the Oracle Data Integrator repositories reside on a supported database.

    A list of supported databases can also be found on the Oracle Technology Network (OTN) at

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

OSI Data Upgrade Performed - Ensure that you complete the required steps described in Running OSI Data Upgrade Utility.

6. Click **Next**.

   The **Specify OIM Database** screen is displayed.

7. Enter the following information:

   - Host: Enter the name of the server where your database is running.

   - Port: Enter the port number for your database. The default port number for Oracle databases is 1521.

   - Service Name: Specify the service name for the database. Typically, the service name is the same as the global database name.

   - OIM Schema: Specify the Oracle Identity Manager schema name.

   - SYS Password: Enter the password for your SYS user.

8. Click **Next**.

   The **Examining Components** screen is displayed.

9. Click **Next**.

   The **Upgrade Summary** screen is displayed.

10. Click **Upgrade**.

    The **Upgrade Progress** screen is displayed. This screen provides the following information:

    - The status of the upgrade

    - Any errors or problems that occur during the upgrade

      See Also: "Troubleshooting Your Upgrade" in the *Oracle Fusion Middleware Upgrade Planning Guide* for specific instructions for troubleshooting problems that occur while running the Upgrade Assistant

11. Click **Next**.

    The **Upgrade Complete** screen is displayed. This screen confirms that the upgrade was complete.

12. Click **Close**.

13.7 Task 5: Create a WebLogic Domain for Oracle Identity Manager

To create a WebLogic Domain for Oracle Identity Manager, refer to the section "OIM Without LDAP Sync in a New Domain" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

> **Notes:**
>
> - Ensure that the Oracle WebLogic Domain for Oracle Identity Manager includes Oracle SOA 11*g*. Oracle Identity Manager uses process workflows and approvals provided by Oracle SOA 11*g*. When the domain is configured the Administration Server and Managed Servers for Oracle Identity Manager and Oracle SOA 11*g* are created.
>
> - Ensure that you use the schemas created in Task 2: Use the Repository Creation Utility to Create the Schema in the Database.

13.8 Task 6: Start the WebLogic Administration Server

You can start the Oracle WebLogic Server Administration Server by using the following command on the command line:

> **Note:** If you want to automatically generate a `boot.properties` file, ensure that the `security` folder is created at `MW_HOME/user_projects/domains/domain_name/servers/AdminServer`. If this folder does not exist then you must create the folder.

UNIX

```
MW_HOME/user_projects/domains/domain_name/bin/startWebLogic.sh
        -Dweblogic.management.username=weblogic
        -Dweblogic.management.password=password
        -Dweblogic.system.StoreBootIdentity=true
```

Windows

```
MW_HOME\user_projects\domains\domain_name\bin\startWebLogic
        -Dweblogic.management.username=weblogic
        -Dweblogic.management.password=password
        -Dweblogic.system.StoreBootIdentity=true
```

13.9 Task 7: Configure Oracle Identity Manager Server 11*g*

To install Oracle Identity Manager, refer to the chapter "Configuring Oracle Identity Manager Server" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

> **Notes:**
>
> - When configuring Oracle Identity Manager Server, ensure that you do not select the Enable LDAP Sync option on the BI Publisher screen in the Oracle Identity Manager Configuration Wizard. LDAP Sync is not supported when you upgrade from Oracle Identity Management 9.1 to Oracle Identity Management 11*g*.
>
> - If you are importing the Oracle Identity Management 9.1 database, then ensure that you copy the `.xldatabasekey` database keystore (Located in `OIM9101\xellerate\config` directory) to the `config/fmwconfig` location under the Oracle WebLogic Domain you have created.

13.10 Task 8: Configure Node Manager to Start Managed Servers

For information about configuring Node Manager, refer to the "Configuring Node Manager to Start Managed Servers" section in the *Oracle Fusion Middleware Administrator's Guide*.

> **Note:** Ensure that you enter the value `true` for `StartScriptEnabled` parameter in the `nodemanager.properties` file.

13.11 Task 9: Start the SOA Managed Server

You can start the SOA Managed Server by using the following command on the command line:

UNIX

```
MW_HOME/user_projects/domains/domain_name/bin/startManagedWebLogic.sh
        managed_server_name admin_url
```

Windows

```
MW_HOME\user_projects\domains\domain_name\bin\startManagedWebLogic.cmd
        managed_server_name admin_url
```

When prompted, enter your user name and password.

13.12 Task 10: Start the Oracle Identity Manager Managed Server

You must start the Oracle Identity Manager Managed Server to populate the MDS by using the following command on the command line:

UNIX

```
MW_HOME/user_projects/domains/domain_name/bin/startManagedWebLogic.sh
        managed_server_name admin_url
```

Windows

```
MW_HOME\user_projects\domains\domain_name\bin\startManagedWebLogic.cmd
        managed_server_name admin_url
```

For `managed_server_name admin_url`, specify your Oracle Identity Manager Managed Server name and URL. When prompted, enter your user name and password.

> **Note:** The following error message is displayed:
>
> ```
> Password for .xldatabasekey is not seeded in CSF.
> .
> oracle.iam.platform.utils.OIMAppInitializationException:
> OIM application intialization failed because of the following
> reasons:
> Password for .xldatabasekey is not seeded in CSF.
>
>         at
> oracle.iam.platform.utils.OIMAppInitializationListener.preStart(OIM
> AppInitializationListener.java:145)
>         at
> weblogic.application.internal.flow.BaseLifecycleFlow$PreStartAction
> .run(BaseLifecycleFlow.java:282)
>         at
> weblogic.security.acl.internal.AuthenticatedSubject.doAs(Authentica
> tedSubject.java:321)
>         at
> weblogic.security.service.SecurityManager.runAs(SecurityManager.jav
> a:120)
>         at
> weblogic.application.internal.flow.BaseLifecycleFlow$LifecycleListe
> nerAction.invoke(BaseLifecycleFlow.java:199)
>         Truncated. see log file for complete stacktrace
> Caused By: oracle.iam.platform.utils.OIMAppInitializationException:
> OIM application intialization failed because of the following
> reasons:
> Password for .xldatabasekey is not seeded in CSF.
>
>         at
> oracle.iam.platform.utils.OIMAppInitializationListener.preStart(OIM
> AppInitializationListener.java:145)
>         at
> weblogic.application.internal.flow.BaseLifecycleFlow$PreStartAction
> .run(BaseLifecycleFlow.java:282)
>         at
> weblogic.security.acl.internal.AuthenticatedSubject.doAs(Authentica
> tedSubject.java:321)
>         at
> weblogic.security.service.SecurityManager.runAs(SecurityManager.jav
> a:120)
>         at
> weblogic.application.internal.flow.BaseLifecycleFlow$LifecycleListe
> nerAction.invoke(BaseLifecycleFlow.java:199)
>         Truncated. see log file for complete stacktrace
> >
> ```
>
> You can ignore the above error message.

13.13 Task 11: Stop the Oracle Identity Manager Managed Server

You can stop the Oracle Identity Manager Managed Server by using the following command on the command line:

UNIX

```
MW_HOME/user_projects/domains/domain_name/bin/stopManagedWebLogic.sh
        managed_server_name admin_url
```

Windows

```
MW_HOME\user_projects\domains\domain_name\bin\stopManagedWebLogic.cmd
        managed_server_name admin_url
```

When prompted, enter your user name and password.

> **Note:** If you get any error message, you can ignore it.

13.14 Task 12: Use Upgrade Assistant to Upgrade Oracle Identity Manager Middle Tier

To upgrade the Oracle Identity Manager middle tier, complete the following steps:

> **Notes:**
>
> - Ensure that your Administration Server and the SOA Managed Server are up and running.
>
> - You can also use the Upgrade Assistant command-line interface to upgrade your Oracle Identity Manager 9.1 Oracle homes. For more information, see "Using the Upgrade Assistant Command-Line Interface" in the *Oracle Fusion Middleware Upgrade Planning Guide*.

1. Enter the following command to launch Upgrade Assistant.

   On UNIX systems (Located at *MW_HOME*/Oracle_IDM1/bin):

   ```
   ./ua
   ```

   On Windows systems (Located at *MW_HOME*\Oracle_IDM1\bin):

   ```
   ua.bat
   ```

   The Oracle Fusion Middleware Upgrade Assistant **Welcome** screen is displayed, as shown in Figure 13–2.

Figure 13–2   Upgrade Assistant Welcome Screen
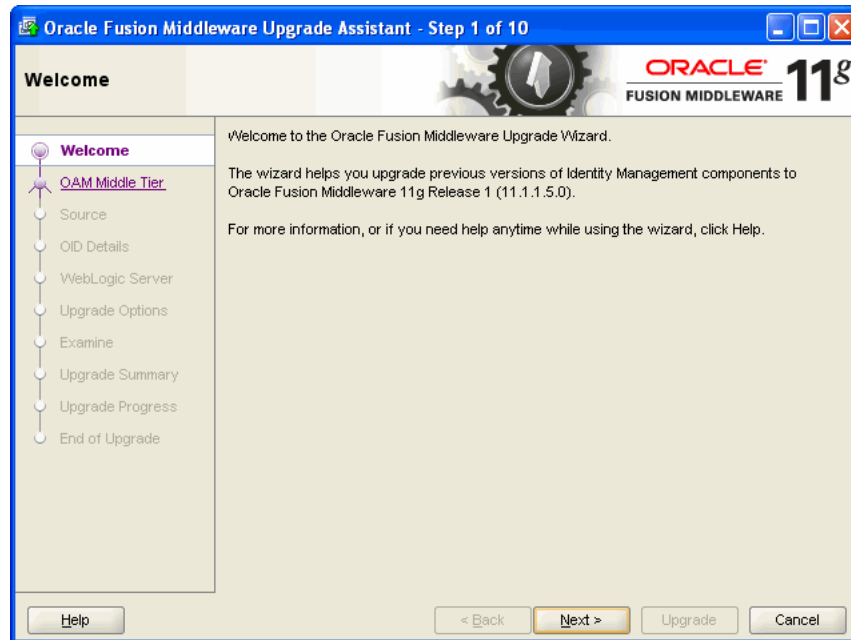
2. Click **Next**.

    The **Specify Operation** screen is displayed.

3. Select **Upgrade Oracle Identity Manager Middle Tier**.

4. Click **Next**.

    The **Specify Source Directory** screen is displayed.

5. Click **Browse** and enter the directory location of your Oracle Identity Manager 9.1 installation.

6. Click **Next**.

    The **Specify OIM Database** screen is displayed.

7. Enter the following information:

    ■   **Host**: Enter the name of the host computer where the database resides.

    ■   **Port**: Enter the listening port of the database; for example, 1521.

    ■   **Service Name**: Enter the service name of the database. Note that the service name typically consists of the system identifier (SID) and the network domain address of the database.

    ■   **OIM Schema**: Enter the name of the Oracle Identity Manager 9.1 schema that resides in the database.

    ■   **SYS Password**: Enter the password for the SYS database account of the database that hosts the Oracle Identity Manager 9.1 schema. The Upgrade Assistant needs these login credentials to connect to the database and read the contents of the Oracle Identity Manager schema.

8. Click **Next**.

    The **Specify MDS Database** screen is displayed.

9. Enter the following information:

- **Host**: Enter the name of the host computer where the database resides.

- **Port**: Enter the listening port of the database; for example, `1521`.

- **Service Name**: Enter the service name of the database. Note that the service name typically consists of the system identifier (SID) and the network domain address of the database.

- **SYS Password**: Enter the password of the database SYS user. The Upgrade Assistant needs these login credentials to connect to the database and read the contents of the MDS schema.

10. Click **Next**.

    The **Specify MDS Schema** screen is displayed.

11. Complete the following:

    - Select the MDS schemas from the drop-down menu.

    - Enter the password for the schema in the **Password** field. This password is required so that the Upgrade Assistant can upgrade and modify the schema. This is the Oracle MDS schema password that you set in the Repository Creation Utility (RCU) when you installed the schema in the database.

12. Click **Next**.

    The **Specify WebLogic Server** screen is displayed.

13. Enter the following information:

    - **Host**: The host where the Oracle WebLogic Server domain resides.

      Ensure to include the full host name; for example:

      `IDMHost1.example.com`

    - **Port**: The listening port of the administration server. Typically, the administration server listens on port `7001`.

    - **Username**: The user name that is used to log in to the administration server. This is the same username you use to log in to the Administration Console for the domain.

    - **Password**: The password for the administrator account that is used to log in to the administration server. This is the same password you use to log in to the Administration Console for the domain.

14. Click **Next**.

    The **Specify SOA Server** screen is displayed.

15. Enter the following information:

    - **Host**: The host where the SOA Managed Server resides.

    - **Port**: The listening port of the SOA Managed Server.

    - **Username**: The user name that is used to log in to the SOA Managed Server. This is the same username you use to log in to the Administration Console for the domain.

    - **Password**: The password for the administrator account that is used to log in to the SOA Managed Server. This is the same password you use to log in to the Administration Console for the domain.

16. Click **Next**.

The **Specify Upgrade Options** screen is displayed.

17. Select **Start destination components after successful upgrade** and click **Next**.

> **Note:** Select this option, if you want the Upgrade Assistant to automatically start the components in the destination Oracle home after a successful upgrade is complete. If you do not select this option, then you will have to manually start the destination instance after the upgrade. Note that this option works only if the upgrade is successful.

The **Examining Components** screen is displayed.

18. Click **Next**.

The **Upgrade Summary** screen is displayed.

19. Click **Upgrade**.

The **Upgrade Progress** screen is displayed. This screen provides the following information:

- The status of upgrade

- Any errors or problems that occur during the upgrade

  > **See Also:** "Troubleshooting Your Upgrade" in the *Oracle Fusion Middleware Upgrade Planning Guide* for specific instructions for troubleshooting problems that occur while running the Upgrade Assistant

20. Click **Next**.

The **Upgrade Complete** screen is displayed. This screen confirms that the upgrade was complete.

21. Click **Close**.

The Post upgrade summary report is generated (Located at `IDM_HOMe\upgrade\temp\oimUpgradeReportDi\index.html`). This report gives detail on the feature name, its upgrade status and feature related report.

13.15 Task 13: Start the Oracle Identity Manager Managed Server

You can start the Oracle Identity Manager Managed Server by using by using the following command in the command line:

UNIX

```
MW_HOME/user_projects/domains/domain_name/bin/startManagedWebLogic.sh
        managed_server_name admin_url
```

Windows

```
MW_HOME\user_projects\domains\domain_name\bin\startManagedWebLogic.cmd
        managed_server_name admin_url
```

When prompted, enter your user name and password.

13.16 Task 14: Complete Any Required Oracle Identity Manager Post-Upgrade Tasks

The following sections describe the manual steps that you must perform after upgrading to Oracle Identity Manager 11*g*:

- Customizing Oracle Identity Manager User Interfaces
- Recompiling Adapters
- Rewriting Prepopulate Adapters
- Disabling User Login
- Upgrading Oracle Identity Management Reports
- Using Generated SOA Composite as Approval Process
- Defining Connectors
- Configuring Auto-Approval for Self-Registration
- Generating an Audit Snapshot
- Upgrading User Defined Fields
- Enabling Audit
- Importing and Exporting Data Using the Deployment Manager

13.16.1 Customizing Oracle Identity Manager User Interfaces

If you used any user interfaces in Oracle Identity Manager 9.1 then after the upgrade you can customize the user interfaces for Oracle Identity Manager 11*g* as described in "Customizing Oracle Identity Manager Interfaces" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

13.16.2 Recompiling Adapters

After you upgrade to Oracle Identity Management 11*g*, you must recompile the adapters as described in "Compiling Adapters" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*. Some of your adapters may fail to compile. You must identify and recompile the adapters as described in the note 1311574.1 note at `https://support.oracle.com`.

13.16.3 Rewriting Prepopulate Adapters

After you upgrade to Oracle Identity Management 11*g*, you must rewrite the prepopulate adapter as described in "Prepopulation of an Attribute Value During Request Creation" in the Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager.

13.16.4 Disabling User Login

In Oracle Identity Manager 11*g* the User login field is not mandatory. You must disable the user login mandatory option by completing the following steps:

1. Export the `user.xml` file (Located at `/file/User.xml` in the MDS) as described in "Using the Export Utility" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

2. Open the `user.xml` file in text editor and set the `User Login` attribute to `false`, as shown in following example:

```
<attribute name="User Login">
 <required>false</required>
```

3. Import the `user.xml` file as described in "Using the Import Utility" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

13.16.5 Upgrading Oracle Identity Management Reports

If you have a configured Oracle Identity Management Reports in Oracle Identity Manager 9.1 then you must upgrade the reports as described in "Upgrading to 11*g* Release 1 (11.1.1)" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

> **Note:** BI Publisher cannot be accessed through the Oracle Identity Manager Administrative and User Console. You must open BI Publisher explicitly to access the Oracle Identity Manager 11*g* reports.

13.16.6 Using Generated SOA Composite as Approval Process

If you use a generated SOA composite as approval process then you must complete the following steps:

> **Notes:**
>
> - `report.html` (Located at, `MW_HOME/Oracle_IDM1/upgrade/workflow`) lists out the list of approval processes that are successfully upgraded as SOA Composites and the list of approval processes that are partially upgraded as SOA Composites. The partially upgrade SOA composites need to be manually updated as per the corresponding Oracle Identity Manager 9.1 Approval process using the Cause and Action information provided in the report.
>
> - SOA composites generated as part of the middle tier upgrade is located at, `IDM_HOME/upgrade/workflow/BPELComposites`.

1. Configure the SOA Composite as described in "Configuring the SOA Composite By Using JDeveloper" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*. After you configure the SOA Composite you need to recreate the task assignment and implement it in the corresponding SOA Composite. For more information, see "*Oracle Fusion Middleware Developer's Guide for Oracle SOA Suite*"

2. Deploy SOA composite to SOA server as described in "Deploying the SOA Composite" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

3. Register the SOA composite with Oracle Identity Manager 11*g* before it can be used as an approval process as described in "Registering a SOA Composite with Oracle Identity Manager" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

4. Specify SOA composite as approval process in the corresponding Approval Policy(ies) as described in "Understanding Approval Process Development in

Oracle SOA Suite" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

> **Note:** For the e-mail notifications in Oracle Identity Manager 9.1 approval process, you need to configure it to the corresponding generated SOA Composite and use the Oracle SOA server to send e-mail notifications. For configuring Oracle SOA server to send e-mail notifications, see "Configuring Oracle User Messaging Service" in the Oracle Fusion Middleware Administrator's Guide for Oracle SOA Suite and Oracle Business Process Management Suite.

13.16.7 Defining Connectors

After upgrading to Oracle Identity Manager, you must define the connectors as described in "Defining Connectors" in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager*.

13.16.8 Configuring Auto-Approval for Self-Registration

After upgrading from Oracle Identity Manager 9.1 the auto approval feature is disabled for Oracle Identity Manager 11*g*. You must configure auto-approval for self-registration as described in "Configuring Auto-Approval for Self-Registration" in the *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*.

13.16.9 Generating an Audit Snapshot

You must generate an audit snapshot of the audit tables as described in "Generating an Audit Snapshot" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

13.16.10 Upgrading User Defined Fields

If your Oracle Identity Manager 9.1 organization data model contain User Defined Fields (UDFs) then you must complete the following steps:

1. Start the Design Console.

2. In the Design Console Explorer, expand **Administration** and then select User Defined Field Definition.

3. Open Organizations form and click **Save**.

   This will update the MDS definitions for the organization UDFs, which will then be visible in the OIM 11g Administrator UI.

13.16.11 Enabling Audit

The audit features will not be enabled after upgrade if it was not there in Oracle Identity Manager 9.1. You can enable audit as described in "Modifying System Properties" in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager*.

13.16.12 Importing and Exporting Data Using the Deployment Manager

If you have any issue with importing and exporting data Using the Deployment Manager then see "Troubleshooting Deployment Manager" in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager*.

13.17 Task 15: Verify the Oracle Identity Manager Upgrade

To verify your Oracle Identity Manager upgrade, perform the following steps:

1. Run Upgrade Assistant, and select **Verify Instance** on the Specify Operation page.

   Follow the instructions on the screen for information on how to verify that specific Oracle Fusion Middleware components are up and running.

2. Run `sqlplus` and connect to your database and then run the following query, to ensure that the schema upgrade was successful:

   ```
   select feature_id,feature_upgrade_state,is_feature_upgraded from upgrade_
   feature_state;
   ```

3. Use the following URL in a web browser to verify that Oracle Identity Manager 11*g* is up and running:

   ```
   http://oim.example.com:14000/oim
   ```

   Alternatively, you can use Fusion Middleware Control to verify that Oracle Identity Manager and any other Oracle Identity Management components are up and running in the Oracle Fusion Middleware environment.

   For more information, see "Getting Started Using Oracle Enterprise Manager Fusion Middleware Control" in the *Oracle Fusion Middleware Administrator's Guide*.

4. Install the Diagnostic Dashboard and run the following tests:

   - Oracle Database Connectivity Check
   - Account Lock Status
   - Data Encryption Key Verification
   - Scheduler Service Status
   - JMS Messaging Verification
   - SOA-Oracle Identity Manager Configuration Check
   - SPML Web Service
   - Test OWSM setup
   - Test SPML to Oracle Identity Manager request invocation
   - SPML attributes to Oracle Identity Manager attributes
   - Username Test

   For more information, see "Working with the Diagnostic Dashboard" in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager*.

Part IV

Upgrading Oracle Identity Management High Availability Environments

Part IV contains the following chapters:

14

Upgrading Oracle Internet Directory High Availability Environments

This chapter describe how to upgrade Oracle Internet Directory high availability environments that were supported in Oracle Application Server 10*g* Release 2 (10.1.2) and 10*g* (10.1.4).

This chapter contains the following sections:

- Summary of Oracle Internet Directory High Availability Upgrade Starting Points
- Before You Begin Upgrading Your Oracle Identity Management High Availability Environment
- Upgrading Oracle Internet Directory and Oracle Directory Integration Platform in a High Availability Environment
- Upgrading Oracle Internet Directory and Oracle Directory Integration Platform in a Colocated High Availability Environment
- Upgrading Oracle Internet Directory Only

14.1 Summary of Oracle Internet Directory High Availability Upgrade Starting Points

The following high availability topologies are supported for upgrade from Oracle Identity Management 10*g* Release 2 (10.1.2) and 10*g* (10.1.4):

- High Availability Topologies Based on a Distributed Identity Management Environment
- High Availability Topologies Based on a Colocated Identity Management Environment
- High Availability Environments Based on Standalone Oracle Internet Directory Instances

14.1.1 High Availability Topologies Based on a Distributed Identity Management Environment

This type of topology is based on the Oracle Internet Directory and Oracle Directory Integration Platform components when they are installed on a separate host from Oracle Single Sign-On and Oracle Delegated Administration Services.

This was the recommended topology for high availability environments in Oracle Application Server 10*g*. It is sometimes referred to as a distributed Oracle Identity Management environment or a non-colocated Identity Management environment.

Refer to Section 4.2.2, "Upgrading a Non-Colocated Identity Management Environment" for a description the single-node variant of a non-colocated Identify Management high availability environment.

14.1.2 High Availability Topologies Based on a Colocated Identity Management Environment

This type of topology is based on the Oracle Internet Directory and Oracle Directory Integration Platform components when they are installed and configured in the same Oracle home as Oracle Single Sign-On and Oracle Delegated Administration Services.

This type of environment is referred to as a colocated Identity Management environment. For more information, refer to Section 4.2.1, "Upgrading a Colocated Identity Management Environment" for a description of a single-node variant of a colocated Identity Management high availability environment.

Because Oracle Single Sign-On and Oracle Delegated Administration Services are not available in Oracle Fusion Middleware 11*g*, the upgrade of this topology requires some additional steps.

14.1.3 High Availability Environments Based on Standalone Oracle Internet Directory Instances

This type of topology is based on Oracle Internet Directory when it is upgraded without an associated Oracle Directory Integration Platform instance.

This Oracle Internet Directory topology can be upgraded and associated with a local Oracle WebLogic Server domain, an existing remote domain, or with no Oracle WebLogic Server domain.

For more information, see Section 5.3.2.1, "When is Oracle WebLogic Server Required?".

14.2 Before You Begin Upgrading Your Oracle Identity Management High Availability Environment

Before you begin using the procedures in this chapter, note the following:

- Conventions Used in This Chapter
- Prerequisites for Oracle Identity Management High Availability Upgrade
- Supported High Availability Environments for Upgrade
- Reducing Downtime During Upgrade With Directory Replication

14.2.1 Conventions Used in This Chapter

The procedures in this chapter typically involve two host computers. For the purposes of the examples in this chapter, the two hosts are referred to as IDMHOST1 and IDMHOST2.

Some of the examples in this chapter provide the commands required to perform particular tasks on a UNIX system. The commands for Windows are similar, but you would replace the environment variables with the Windows equivalent (for example, `%ORACLE_HOME%`).

14.2.2 Prerequisites for Oracle Identity Management High Availability Upgrade

Before you begin the upgrade procedures in this chapter, be sure the following prerequisites have been met.

Oracle Identity Management 10*g* Components Are Installed and Running on IDMHOST1

It is assumed that the Oracle Identity Management 10*g* components you are about to upgrade are installed and running on IDMHOST1. This is important because the Oracle Identity Management 11*g* components that you are upgrading must be installed on the same host as the Oracle Identity Management 10*g* components.

All Other Oracle Application Server 10*g* Instances That Use the Same Metadata Repository Are Stopped

Before you begin the upgrade, stop all the Oracle Internet Directory and Oracle Directory Integration Platform 10*g* instances, except the instances that you are about to upgrade.

In addition, stop all the Oracle Application Server 10*g* instances that share the same OracleAS Metadata Repository as the Oracle Internet Directory instance you are about to upgrade. For example, if you have any Oracle Portal 10*g* or other Oracle Identity Management 10*g* instances running, be sure to stop those instances as well. This will ensure that no other Oracle Application Server components are accessing the repository during the upgrade.

All Instances of Oracle Enterprise Manager Are Stopped

Before you begin any of the high availability procedures documented in this chapter, be sure to stop all instances of Oracle Enterprise Manager that are managing the Oracle Internet Directory instances you are about to upgrade.

This step is important because Oracle Enterprise Manager Application Server Control sometimes accesses the Oracle Internet Directory schema (the ODS schema) when it monitors and configures the Oracle Internet Directory target. To avoid any possibility of conflict when you are upgrading the Oracle Internet Directory middle tier and schema, it is important to stop all instances of Oracle Enterprise Manager during the upgrade process.

For information on stopping and starting Application Server Control, refer to the *Oracle Application Server Administrator's Guide* in the Oracle Application Server 10*g* documentation library.

Load Balancer Is Configured to Route Only to Primary Instance

Before you begin the upgrade, make sure the load balancer virtual servers are routing requests only to the primary instance of the OracleAS Cluster (Identity Management) node.

The primary instance of the OracleAS Cluster is the first node where you installed Oracle Internet Directory.

Any Modifications to ias.properties Have Been Removed

If you have modified the `ias.properties` file in the Oracle Identity Management Oracle home to redefine port values, then you must update the ias.properties file with the actual, physical port values for each OID instance before upgrade.

Some organizations modify the `ias.properties` file, for example, to reference specific load balancer ports. If you performed such a customization, be sure to restore

the `ias.properties` to its original state so it references the actual ports of the Oracle Internet Directory instances in your environment.

The Current Version of the Database is Supported by Oracle Fusion Middleware 11*g*

The procedures in this chapter assume you are storing the Oracle Internet Directory schema (the ODS schema) in a Real Application Clusters (RAC) database that has been upgraded to a database version supported by Oracle Fusion Middleware 11*g*.

For more information database requirements for upgrade, as well as additional upgrade information for Oracle Fusion Middleware 11*g*, see the *Oracle Fusion Middleware Upgrade Planning Guide*.

14.2.3 Supported High Availability Environments for Upgrade

This chapter describes how to upgrade Oracle Internet Directory high availability environments that were supported in Oracle Application Server 10*g* Release 2 (10.1.2) and 10*g* (10.1.4).

High Availability Configurations for Administration Tools

This chapter does not provide information on configuring the administration tools (such as Oracle WebLogic Server Administration Console, Oracle Enterprise Manager Fusion Middleware Control, or Oracle Directory Services Manager) for high availability.

Additional Resources

For information about the supported high availability topologies in Oracle Fusion Middleware 11*g*, see the *Oracle Fusion Middleware High Availability Guide*.

Before you begin these procedures, review the procedures and prerequisites available in Chapter 5, "Upgrading Your Oracle Internet Directory Environment".

14.2.4 Reducing Downtime During Upgrade With Directory Replication

The procedures in this chapter assume your organization can support a limited amount of Identity Management downtime.

If your organization has no tolerance for Identity Management downtime, consider the following approach to the upgrade process:

1. Configure your existing Oracle Identity Management 10*g* environment using Oracle Internet Directory Advanced Replication.

2. Use the upgrade procedures in Section 16.3.2, "Upgrading One Replica at a Time".

When you implement Oracle Internet Directory Advanced Replication, you can route client traffic to one replica while upgrading the other replica. The result is an upgrade procedure that requires little or no downtime while each replica is upgraded.

For more information about using Oracle Internet Directory replication, refer to the following sections in the Oracle Internet Directory Administrator's Guide in the 10*g* (10.1.4) documentation library on the Oracle Technology Network (OTN):

■ "Oracle Internet Directory Replication Concepts"

■ "Oracle Internet Directory Replication Installation and Configuration"

The Oracle Identity Management 10*g* (10.1.4) documentation library is available on OTN at the following URL:

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

14.3 Upgrading Oracle Internet Directory and Oracle Directory Integration Platform in a High Availability Environment

Perform the following tasks to upgrade an Oracle Internet Directory and Oracle Directory Integration Platform high availability environment when both components are installed on a separate host from Oracle Single Sign-On and Oracle Delegated Administration Services:

- Task 1: On IDMHOST1, Install Oracle WebLogic Server and Create the Middleware Home

- Task 2: On IDMHOST1, Install and Configuring Oracle Internet Directory and Oracle Directory Integration Platform 11g Release 1 (11.1.1.6.0)

- Task 3: On IDMHOST1, Upgrade Oracle Internet Directory and Oracle Directory Integration Platform to 11g

- Task 4: On IDMHOST1, Configure Oracle Directory Integration Platform to Use the Oracle Internet Directory Virtual Host

- Task 5: On IDMHOST1, Verify the Oracle Internet Directory and Oracle Directory Integration Platform Upgrade

- Task 6: On IDMHOST2, Install Oracle WebLogic Server and Create the Middleware Home

- Task 7: On IDMHOST2, Install and Configure the Oracle Internet Directory and Oracle Directory Integration Platform 11g Release 1 (11.1.1.6.0)

- Task 8: Copy the Oracle Directory Integration Platform Directory from IDMHOST1 to IDMHOST2

- Task 9: On IDMHOST2, Set the Anonymous Bind Property to Allow

- Task 10: Start the Managed Server on IDMHOST2

- Task 11: Verify That the Components Are Up and Running on IDMHOST2

14.3.1 Task 1: On IDMHOST1, Install Oracle WebLogic Server and Create the Middleware Home

For information on installing the Oracle WebLogic Server, see "Preparing for Installation" and "Running the Installation Program in Graphical Mode" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

When you install Oracle WebLogic Server, make a note of the complete path to the Middleware home. You will need this information later in the upgrade procedure.

14.3.2 Task 2: On IDMHOST1, Install and Configuring Oracle Internet Directory and Oracle Directory Integration Platform 11*g* Release 1 (11.1.1.6.0)

To install and configure Oracle Internet Directory 11*g* on IDMHOST1, refer to the chapter "Installing and Configuring Oracle Identity Management (11.1.1.6.0)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

For complete instructions on configuring Oracle Internet Directory and Oracle Directory Integration Platform, see the "Configuring Oracle Internet Directory (OID)" and "Configuring Oracle Directory Integration Platform (ODIP)" chapters in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*. For more

information, see the "Creating a WebLogic Domain in Graphical Mode" topic in the *Oracle Fusion Middleware Creating Domains Using the Configuration Wizard* guide.

14.3.3 Task 3: On IDMHOST1, Upgrade Oracle Internet Directory and Oracle Directory Integration Platform to 11*g*

Use the Oracle Fusion Middleware Upgrade Assistant to upgrade the Oracle Internet Directory and Oracle Directory Integration Platform 10*g* instances on IDMHOST1 to 11*g*:

1. Change directory the `ORACLE_HOME`/bin directory of the Oracle Fusion Middleware installation.

2. Enter the following command to start the Upgrade Assistant.

   On UNIX system:

   ```
   ./ua
   ```

   On Windows systems:

   ```
   ua.bat
   ```

   The Upgrade Assistant displays the Welcome screen.

3. Click **Next** to display the Specify Operation screen.

4. Select **Upgrade Identity Management Instance** on the Specify Operation screen.

5. Refer to Table 14–1 for a description of the Upgrade Assistant screens that require input from you during an Oracle Internet Directory and Oracle Directory Integration Platform upgrade.

6. After the Target Database Details screen, the Upgrade Assistant performs the following tasks and provides the progress on each task:

   - Examines the components and schemas to be upgraded and verifies that they can be upgraded successfully.

   - Provides a summary of the components to be upgraded so you can verify that Upgrade Assistant is upgrading the components and schemas you expect.

   - Provides a progress screen so you can see the status of the upgrade as it proceeds.

   - Alerts you of any errors or problems that occur during the upgrade.

     See Also: "Troubleshooting Your Upgrade" in the *Oracle Fusion Middleware Upgrade Planning Guide* for specific instructions for troubleshooting problems that occur while running the Upgrade Assistant

   - Displays the End of Upgrade screen, which confirms that the upgrade was complete.

7. Exit the Upgrade Assistant.

Table 14–1   Upgrade Assistant Screens That Require Input During an Oracle Internet Directory and Oracle Directory Integration Platform Upgrade

Upgrade Assistant Screen	Description
Specify Source Home	Select the 10*g* Release 2 (10.1.2) or 10*g* (10.1.4) source Oracle home.
	If the Oracle home you want to upgrade does not appear in the drop-down lists, see "Source Oracle Home Not Listed by OracleAS Upgrade Assistant" in the *Oracle Fusion Middleware Upgrade Planning Guide*.
Specify Destination Instance	Enter the complete path to the 11*g* Oracle instance, or click **Browse** to locate the instance directory.
Specify WebLogic Server	Enter the host and Administration Server port for the Oracle WebLogic Server you configured in "Task 1: On IDMHOST1, Install Oracle WebLogic Server and Create the Middleware Home".
	Note this information is required if you are upgrading Oracle Directory Integration Platform. It is also required if you associated your Oracle Internet Directory 11*g* installation with Oracle WebLogic Server.
Warning Dialog Box	The Upgrade Assistant displays this warning dialog box if the source Oracle home contains Oracle Application Server components that are not installed and configured in the destination Oracle instance.
	This warning appears, for example, if the source Oracle home contains an instance of Oracle HTTP Server, which is not available in the 11*g* Oracle home.
	If the information in the dialog box is accurate and you understand which components will be upgraded, click **Yes** to continue. Otherwise, click **No** and verify which components are installed and configured in each 11*g* Oracle instance.
Specify Upgrade Options	Select the upgrade options you want to apply to the Oracle Identity Management upgrade:
	■ **Use source Oracle home ports in destination:** If you want to migrate the port assignments used by your Oracle Application Server 10g Oracle home to your new Oracle Fusion Middleware Oracle instance. Note if you select this option, you will not be able to run both the 10*g* and 11*g* middle tiers at the same time; otherwise, port conflicts will occur. If you do not select this option, then you will have to manually configure your Oracle Internet Directory port number.
	■ **Start destination components after successful upgrade:** if you want the Upgrade Assistant to automatically start the components in the destination Oracle home after the upgrade is complete. If you do not select this option, then you will have to manually start the destination instance after the upgrade.
	Click **Help** to display more information about the upgrade options on this screen.
Specify OID Details	Use this screen to enter the details required to connect to the Oracle Internet Directory 10*g* instance, including the physical host and the password to the Oracle Internet Directory super user account (`cn=orcladmin`).
	For more information, click **Help**.

Table 14–1 (Cont.) Upgrade Assistant Screens That Require Input During an Oracle Internet Directory and Oracle Directory Integration Platform Upgrade

Upgrade Assistant Screen	Description
Specify Database Details	Use this screen to enter the details required to connect to the database where the Oracle Identity Management schemas reside, including the host, service name, port, and SYS password for the database.
	Note the following important information about this screen:
	■ You must enter the password for the ODS schema password. The default ODS password is the same as the Oracle Application Server administrator password, but this password can be changed after installation, using the OID Database Password Utility.
	■ The instructions for identifying a Real Application Clusters (RAC) database are different, depending upon whether you are identifying the RAC database that contains the Oracle Internet Directory (ODS) schema or a RAC database that is being used for Oracle Directory Integration Platform.
	For more information, see Section 5.4.3.2, "About Specifying Real Application Clusters (RAC) Database Details on the Specify Database Details Screen".
Root action required screen	This is only if you are using privileged port on a UNIX system.
	A configuration script needs to be run as root before upgrade can proceed.
	Leaving this window open, open another window, and run the upgroot.sh file as root:
	When the script has completed, return to the Upgrade Assistant and click **OK**.

14.3.4 Task 4: On IDMHOST1, Configure Oracle Directory Integration Platform to Use the Oracle Internet Directory Virtual Host

After you upgrade the Oracle Internet Directory and Oracle Directory Integration Platform instances to 11*g*, update the dip-config.xml file so it references the Oracle Internet Directory Virtual Host Name (for example, oid.mycompany.com), which is associated with the load balancer that is directing traffic to your Oracle Internet Directory instances.

If the load balancer/virtual host has a different port value than the Oracle Internet Directory physical port value, then you must also change the port.

This task is accomplished using the manageDIPServerConfig command, as described in the following procedure.

Use the following procedure perform this step on IDMHOST1:

1. Make a backup of the dip-config.xml file, which is located under the following directory:

```
MW_HOME/user_projects/domains/IDMDomain/config/fmwconfig/servers
        /wls_ods1/applications/DIP_11.1.1.2.0/configuration/
```

2. Set the ORACLE_HOME environment variable to the directory where you installed the Identity Management binaries.

    For example:

```
export ORACLE_HOME=/u01/app/oracle/product/11g/mw_home/idm
```

3. Set the WLS_HOME environment variable to the directory where you installed the WebLogic Server. For example:

```
export WLS_HOME=/u01/app/oracle/product/11g/fmw_home/wlserver_10.3
```

4. Run the following command to update the value of the Oracle Internet Directory host and port:

```
ORACLE_HOME/bin/manageDIPServerConfig set
     -h hostName
     -p port -D wlsuser
     -attr oidhostport
     -val OIDVIRTUALHOSTNAME:PORT
```

For example, on IDMHOST1, the command and output are shown below:

```
ORACLE_HOME/bin/manageDIPServerConfig set
     -h idmhost1.mycompany.com
     -p 7005
     -D weblogic
     -attr oidhostport
     val oid.mycompany.com:636

     [Weblogic user password]
     Connection parameters initialized.
     Connecting at idmhost1.mycompany.com:7005, with userid "weblogic"..
     Connected successfully

     The attribute oidhostport is successfully changed to value
     oid.mycompany.com:636
```

5. Using the WebLogic Server Administration Console, stop and start the wls_ods1 managed server.

14.3.5 Task 5: On IDMHOST1, Verify the Oracle Internet Directory and Oracle Directory Integration Platform Upgrade

Step 1 Verify the Oracle Internet Directory is up and running

Use the following OPMN command to verify that Oracle Internet Directory is up and running:

```
ORACLE_INSTANCE/opmnctl status
```

The output of the command should be similar to the following example:

```
Processes in Instance: oid_instance1
---------------------------------+--------------------+---------+---------
ias-component                    | process-type       |     pid | status
---------------------------------+--------------------+---------+---------
oid1                             | oidldapd           |   31394 | Alive
oid1                             | oidldapd           |   31392 | Alive
oid1                             | oidmon             |   31384 | Alive
```

Use the ldapbind command-line tool to ensure that you can connect to each Oracle Internet Directory instance and the LDAP Virtual Server. The ldapbind tool enables you to determine whether you can authenticate a client to a server.

For non-SSL:

```
ldapbind -h idmhost1.mycompany.com -p 389 -D "cn=orcladmin" -q
```

```
ldapbind -h idmhost2.mycompany.com -p 389 -D "cn=orcladmin" -q
ldapbind -h oid.mycompany.com -p 389 -D "cn=orcladmin" -q
```

For SSL:

```
ldapbind -h idmhost1.mycompany.com -p 636 -D "cn=orcladmin" -q -U 1
ldapbind -h idmhost2.mycompany.com -p 636 -D "cn=orcladmin" -q -U 1
ldapbind -h oid.mycompany.com -p 636 -D "cn=orcladmin" -q -U 1
```

where:

- U = SSL authentication mode

- 1 = No authentication required

- 2 = One way authentication required. With this option, you must also supply a wallet location (-W "file:/home/my_dir/my_wallet") and wallet password (-P wallet_password).

- 3 = Two way authentication required. With this option, you must also supply a wallet location (-W "file:/home/my_dir/my_wallet") and wallet password (-P wallet_password).

Step 2 Verify the Oracle Directory Integration Platform is up and running

Validate the Oracle Directory Integration Platform installation by using the WLST dipStatus command. To run this command, follow these steps:

1. Set the ORACLE_HOME environment variable to the directory where you installed the Identity Management binaries. For example:

   ```
   export ORACLE_HOME=/u01/app/oracle/product/11g/fmw_home/ods
   ```

2. Set the WLS_HOME environment variable to the directory where you installed the WebLogic Server.

   For example:

   ```
   export WLS_HOME=/u01/app/oracle/product/11g/fmw_home/wlserver_10.3
   ```

3. Run the following command:

   ```
   $ORACLE_HOME/bin/dipStatus -h <hostName> -p <port> -D <wlsuser>
   ```

   For example, on IDMHOST1, the command and successful output are shown below:

   ```
   $ORACLE_HOME/bin/dipStatus
       -h idmhost1.mycompany.com
       -p 7005
       -D weblogic
       [Weblogic user password]
        Connection parameters initialized.
        Connecting at idmhost1.mycompany.com:7005, with userid "weblogic"..
        Connected successfully.
        ODIP Application is active at this host and port.
   ```

Step 3 Verify Oracle Directory Services Manager (ODSM)

Verify the Oracle Directory Services Manager installation by bringing up the ODSM Administration Console in a web browser.

The URL to access the ODSM Administration Console is:

```
http://hostname.mycompany.com:<port>/odsm/faces/odsm.jspx
```

For example, on IDMHOST1, enter this URL:

```
http://idmhost1.us.oracle.com:7005/odsm/faces/odsm.jspx
```

14.3.6 Task 6: On IDMHOST2, Install Oracle WebLogic Server and Create the Middleware Home

For information on installing the Oracle WebLogic Server, see "Preparing for Installation" and "Running the Installation Program in Graphical Mode" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

When you install Oracle WebLogic Server, make a note of the complete path to the Middleware home. You will need this information later in the upgrade procedure.

14.3.7 Task 7: On IDMHOST2, Install and Configure the Oracle Internet Directory and Oracle Directory Integration Platform 11*g* Release 1 (11.1.1.6.0)

To install and configure Oracle Internet Directory 11*g* on IDMHOST2, refer to the chapter "Installing and Configuring Oracle Identity Management (11.1.1.6.0)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

For complete instructions on configuring Oracle Internet Directory and Oracle Directory Integration Platform, see the "Configuring Oracle Internet Directory (OID)" and "Configuring Oracle Directory Integration Platform (ODIP)" chapters in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*. For more information, see the "Creating a WebLogic Domain in Graphical Mode" topic in the *Oracle Fusion Middleware Creating Domains Using the Configuration Wizard* guide.

14.3.8 Task 8: Copy the Oracle Directory Integration Platform Directory from IDMHOST1 to IDMHOST2

The Oracle Directory Integration Platform application is deployed on IDMHOST1 as an externally staged application. The application must be copied from IDMHOST1 to IDMHOST2; otherwise, the managed server on IDMHOST2 is listed in the Oracle WebLogic Server administration console as being in an "unknown" state:

1. Locate the `applications` directory in the Oracle WebLogic Server domain directory on IDMHOST1:

```
MW_HOME/user_projects/domains/IDMDomain/config/fmwconfig/servers
       /wls_ods1/applications
```

2. Copy the `applications` directory on and its contents on IDMHOST1 to the same location in the domain directory on IDMHOST2.

   For example:

```
scp -rp MW_HOME/user_projects/domains/IDMDomain/config/fmwconfig/servers
               /wls_ods1/applications
     user@IDMHOST2:MW_HOME/user_projects/domains/IDMDomain/config/fmwconfig
               /servers/wls_ods2/applications
```

14.3.9 Task 9: On IDMHOST2, Set the Anonymous Bind Property to Allow

After you install and configure the second Oracle Internet Directory instance on IDMHOST2, you must set the "Anonymous Bind" server property to "allow," so it matches the first, upgraded Oracle Internet Directoryinstance on IDMHOST1.

This property allows the Oracle Single Sign-On 10*g* and Oracle Delegated Administration Services 10*g* (specifically, OC4J_Security) to correctly use the second Oracle Internet Directory instance on IDMHOST2. Without this alteration to the second Oracle Internet Directory, the OC4J_Security instance on IDMHOST2 will not start.

To modify the anonymous bind property with Oracle Enterprise Manager Fusion Middleware Control:

1. Log in to Fusion Middleware Control.

2. Navigate to the home page of the Oracle Internet Directory instance on IDMHOST2.

3. From the **Oracle Internet Directory** menu, select **Administration**, and then **Server Properties**.

4. Select **Allows** from the **Anonymous Bind** drop-down menu.

5. Click Apply

6. Start Oracle Single Sign-On as you normally would.

14.3.10 Task 10: Start the Managed Server on IDMHOST2

Follow these steps to start the wls_ods2 managed server in a cluster:

1. Open a browser and navigate to the WebLogic Administration Console at:

   ```
   http://idmhost1.mycompany.com:port/console
   ```

2. Login to the WebLogic Administration Console using the administrator credentials.

3. In the left pane of the WebLogic Administration Console, expand Environment and select Clusters.

4. Select the cluster (`cluster_ods`) containing the managed server (wls_ods2) you want to start.

5. Select **Control**.

6. Under Managed Server Instances in this Cluster, select the check box next to the managed server (`wls_ods2`) you want to start and click **Start**.

7. On the Server Life Cycle Assistant page, click **Yes** to confirm.

> **Note:** Node Manager starts the server on the target machine. When the Node Manager finishes its start sequence, the server's state is indicated in the **State** column in the Server Status table.

14.3.11 Task 11: Verify That the Components Are Up and Running on IDMHOST2

Use the procedure documented in "Task 5: On IDMHOST1, Verify the Oracle Internet Directory and Oracle Directory Integration Platform Upgrade" to verify the Oracle Internet Directory, Oracle Directory Integration Platform, and Oracle Directory Services Manager components on IDMHOST2.

14.4 Upgrading Oracle Internet Directory and Oracle Directory Integration Platform in a Colocated High Availability Environment

The procedure for upgrading an Oracle Internet Directory high availability environment based on colocated Oracle Identity Management components is similar to the procedure described in Section 14.3, "Upgrading Oracle Internet Directory and Oracle Directory Integration Platform in a High Availability Environment".

However, there are additional steps required when upgrading this specific topology. Specifically, after you upgrade Oracle Internet Directory and Oracle Directory Integration Platform to 11*g*, you must then disable Oracle Internet Directory and Oracle Directory Integration Platform in the Oracle Application Server 10*g* Oracle home.

Perform the following tasks to upgrade an Oracle Internet Directory and Oracle Directory Integration Platform high availability environment when both components are installed on a separate host from Oracle Single Sign-On and Oracle Delegated Administration Services:

- Task 1: On IDMHOST1, Install Oracle WebLogic Server and Create the Middleware Home

- Task 2: On IDMHOST1, Install and Configure the Oracle Internet Directory and Oracle Directory Integration Platform 11g Release 1 (11.1.1.6.0)

- Task 3: On IDMHOST1, Upgrade Oracle Internet Directory and Oracle Directory Integration Platform to 11g

- Task 4: On IDMHOST1, Configure Oracle Directory Integration Platform to Use the Oracle Internet Directory Virtual Host

- Task 5: On IDMHOST1, Disable Oracle Internet Directory and Oracle Directory Integration Platform in the 10g Oracle Home

- Task 6: On IDMHOST1, Verify the Oracle Internet Directory and Oracle Directory Integration Platform Upgrade

- Task 7: On IDMHOST2, Install Oracle WebLogic Server and Create the Middleware Home

- Task 9: On IDMHOST2, Install and Configure Oracle Internet Directory and Oracle Directory Integration Platform 11g Release 1 (11.1.1.6.0)

- Task 10: Copy the Oracle Directory Integration Platform Directory from IDMHOST1 to IDMHOST2

- Task 11: On IDMHOST2, Set the Anonymous Bind Property to Allow

- Task 12: On IDMHOST2, Disable Oracle Internet Directory and Oracle Directory Integration Platform in the 10g Oracle Home

- Task 13: Start the Managed Server on IDMHOST2

- Task 14: Verify That the Components Are Up and Running on IDMHOST2

14.4.1 Task 1: On IDMHOST1, Install Oracle WebLogic Server and Create the Middleware Home

For information on installing the Oracle WebLogic Server, see "Preparing for Installation" and "Running the Installation Program in Graphical Mode" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

When you install Oracle WebLogic Server, make a note of the complete path to the Middleware home. You will need this information later in the upgrade procedure.

14.4.2 Task 2: On IDMHOST1, Install and Configure the Oracle Internet Directory and Oracle Directory Integration Platform 11*g* Release 1 (11.1.1.6.0)

To install and configure Oracle Internet Directory 11*g* on IDMHOST1, refer to the chapter "Installing and Configuring Oracle Identity Management (11.1.1.6.0)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

For complete instructions on configuring Oracle Internet Directory and Oracle Directory Integration Platform, see the "Configuring Oracle Internet Directory (OID)" and "Configuring Oracle Directory Integration Platform (ODIP)" chapters in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*. For more information, see the "Creating a WebLogic Domain in Graphical Mode" topic in the *Oracle Fusion Middleware Creating Domains Using the Configuration Wizard* guide.

14.4.3 Task 3: On IDMHOST1, Upgrade Oracle Internet Directory and Oracle Directory Integration Platform to 11*g*

Use the Oracle Fusion Middleware Upgrade Assistant to upgrade the Oracle Internet Directory and Oracle Directory Integration Platform 10*g* instances on IDMHOST1 to 11*g*:

1. Change directory the `ORACLE_HOME`/bin directory of the Oracle Fusion Middleware installation.

2. Enter the following command to start the Upgrade Assistant.

   On UNIX system:

   ```
   ./ua
   ```

   On Windows systems:

   ```
   ua.bat
   ```

   The Upgrade Assistant displays the Welcome screen.

3. Click **Next** to display the Specify Operation screen.

4. Select **Upgrade Identity Management Instance** on the Specify Operation screen.

5. Refer to Table 14–1 for a description of the Upgrade Assistant screens that require input from you during an Oracle Internet Directory and Oracle Directory Integration Platform upgrade.

6. After the Target Database Details screen, the Upgrade Assistant performs the following tasks and provides the progress on each task:

   - Examines the components and schemas to be upgraded and verifies that they can be upgraded successfully.

   - Provides a summary of the components to be upgraded so you can verify that Upgrade Assistant is upgrading the components and schemas you expect.

   - Provides a progress screen so you can see the status of the upgrade as it proceeds.

   - Alerts you of any errors or problems that occur during the upgrade.

> **See Also:** "Troubleshooting Your Upgrade" in the *Oracle Fusion Middleware Upgrade Planning Guide* for specific instructions for troubleshooting problems that occur while running the Upgrade Assistant

- Displays the End of Upgrade screen, which confirms that the upgrade was complete.

7. Exit the Upgrade Assistant.

14.4.4 Task 4: On IDMHOST1, Configure Oracle Directory Integration Platform to Use the Oracle Internet Directory Virtual Host

After you upgrade the Oracle Internet Directory and Oracle Directory Integration Platform instances to 11*g*, update the `dip-config.xml` file so it references the Oracle Internet Directory Virtual Host Name (for example, `oid.mycompany.com`). This can be done using the `manageDIPServerConfig` command.

Refer to Section 14.3.4, "Task 4: On IDMHOST1, Configure Oracle Directory Integration Platform to Use the Oracle Internet Directory Virtual Host" for specific instructions for this task.

14.4.5 Task 5: On IDMHOST1, Disable Oracle Internet Directory and Oracle Directory Integration Platform in the 10*g* Oracle Home

After you upgrade the Oracle Internet Directory and Oracle Directory Integration Platform components on IDMHOST1, you cannot start Oracle Internet Directory or use the Oracle Single Sign-On 10*g* component until you disassociate Oracle Internet Directory from the Oracle Single Sign-On and Oracle Delegated Administration Services components in the 10*g* Oracle home.

For specific instructions for performing this task, see the following:

- Section 5.5.2, "Disabling the Oracle Internet Directory and Oracle Directory Integration Platform 10g Components"
- Section 5.5.6, "Removing Oracle Internet Directory and Oracle Directory Integration Platform 10g from Application Server Control"

14.4.6 Task 6: On IDMHOST1, Verify the Oracle Internet Directory and Oracle Directory Integration Platform Upgrade

Use the procedure documented in "Task 5: On IDMHOST1, Verify the Oracle Internet Directory and Oracle Directory Integration Platform Upgrade" to verify the Oracle Internet Directory, Oracle Directory Integration Platform, and Oracle Directory Services Manager components on IDMHOST2.

14.4.7 Task 7: On IDMHOST2, Install Oracle WebLogic Server and Create the Middleware Home

Before you can expand the Oracle WebLogic Server cluster you created on IDMHOST1 to include IDMHOST2, you must install the Oracle WebLogic Server binary files on IDMHOST2 and create Middleware home on IDMHOST2.

> **Note:** When installing the Middleware home for the second (and any subsequent) Oracle Internet Directory installations, you must specify a path for the Middleware home that is identical to the first Oracle Internet Directory.
>
> For example, suppose you are using the Linux operating system and you installed the first Oracle Internet Directory in a Middleware home in the following directory on IDMHOST1:
>
> ```
> /dua1/Oracle/Middleware/
> ```
>
> When you are prompted for the Middleware home on IDMHOST2, you must enter the identical path specification.

For information on installing the Oracle WebLogic Server, see "Preparing for Installation" and "Running the Installation Program in Graphical Mode" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

14.4.8 Task 9: On IDMHOST2, Install and Configure Oracle Internet Directory and Oracle Directory Integration Platform 11*g* Release 1 (11.1.1.6.0)

To install and configure Oracle Internet Directory 11*g* on IDMHOST2, refer to the chapter "Installing and Configuring Oracle Identity Management (11.1.1.6.0)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

For complete instructions on configuring Oracle Internet Directory and Oracle Directory Integration Platform, see the "Configuring Oracle Internet Directory (OID)" and "Configuring Oracle Directory Integration Platform (ODIP)" chapters in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*. For more information, see the "Creating a WebLogic Domain in Graphical Mode" topic in the *Oracle Fusion Middleware Creating Domains Using the Configuration Wizard* guide.

14.4.9 Task 10: Copy the Oracle Directory Integration Platform Directory from IDMHOST1 to IDMHOST2

The Oracle Directory Integration Platform application is deployed on IDMHOST1 as an externally staged application. The application must be copied from IDMHOST1 to IDMHOST2; otherwise, the managed server on IDMHOST2 is listed in the Oracle WebLogic Server administration console as being in an "unknown" state:

1. Locate the `applications` directory in the Oracle WebLogic Server domain directory on IDMHOST1:

   ```
   MW_HOME/user_projects/domains/IDMDomain/config/fmwconfig/servers
         /wls_ods1/applications
   ```

2. Copy the `applications` directory on and its contents on IDMHOST1 to the same location in the domain directory on IDMHOST2.

   For example:

   ```
   scp -rp MW_HOME/user_projects/domains/IDMDomain/config/fmwconfig/servers
             /wls_ods1/applications
       user@IDMHOST2:MW_HOME/user_projects/domains/IDMDomain/config/fmwconfig
             /servers/wls_ods2/applications
   ```

14.4.10 Task 11: On IDMHOST2, Set the Anonymous Bind Property to Allow

After you install and configure the second Oracle Internet Directory instance on IDMHOST2, you must set the "Anonymous Bind" server property to "allow," so it matches the first, upgraded Oracle Internet Directoryinstance on IDMHOST1.

This property allows the Oracle Single Sign-On 10*g* and Oracle Delegated Administration Services 10*g* (specifically, `OC4J_Security`) to correctly use the second Oracle Internet Directory instance on IDMHOST2. Without this alteration to the second Oracle Internet Directory, the OC4J_Security instance on IDMHOST2 will not start.

To modify the anonymous bind property with Oracle Enterprise Manager Fusion Middleware Control:

1. Log in to Fusion Middleware Control.

2. Navigate to the home page of the Oracle Internet Directory instance on IDMHOST2.

3. From the **Oracle Internet Directory** menu, select **Administration**, and then **Server Properties**.

4. Select **Allows** from the **Anonymous Bind** drop-down menu.

5. Click Apply

6. Start Oracle Single Sign-On as you normally would.

14.4.11 Task 12: On IDMHOST2, Disable Oracle Internet Directory and Oracle Directory Integration Platform in the 10*g* Oracle Home

After you upgrade the Oracle Internet Directory and Oracle Directory Integration Platform components on IDMHOST1, you cannot start Oracle Internet Directory or use the Oracle Single Sign-On 10*g* component until you disassociate Oracle Internet Directory from the Oracle Single Sign-On and Oracle Delegated Administration Services components in the 10*g* Oracle home.

For specific instructions for performing this task, see the following:

- Section 5.5.2, "Disabling the Oracle Internet Directory and Oracle Directory Integration Platform 10g Components"

- Section 5.5.6, "Removing Oracle Internet Directory and Oracle Directory Integration Platform 10g from Application Server Control"

14.4.12 Task 13: Start the Managed Server on IDMHOST2

Follow these steps to start the wls_ods2 managed server in a cluster:

1. Open a browser and navigate to the WebLogic Administration Console at:

   ```
   http://idmhost1.mycompany.com:port/console
   ```

2. Login to the WebLogic Administration Console using the administrator credentials.

3. In the left pane of the WebLogic Administration Console, expand Environment and select Clusters.

4. Select the cluster (`cluster_ods`) containing the managed server (wls_ods2) you want to start.

5. Select **Control**.

6. Under Managed Server Instances in this Cluster, select the check box next to the managed server (`wls_ods2`) you want to start and click **Start**.

7. On the Server Life Cycle Assistant page, click **Yes** to confirm.

Note: Node Manager starts the server on the target machine. When the Node Manager finishes its start sequence, the server's state is indicated in the **State** column in the Server Status table.

14.4.13 Task 14: Verify That the Components Are Up and Running on IDMHOST2

Use the procedure documented in "Task 5: On IDMHOST1, Verify the Oracle Internet Directory and Oracle Directory Integration Platform Upgrade" to verify the Oracle Internet Directory, Oracle Directory Integration Platform, and Oracle Directory Services Manager components on IDMHOST2.

14.5 Upgrading Oracle Internet Directory Only

If you are using Oracle Internet Directory in a high availability environment without Oracle Directory Integration Platform or the other Oracle Identity Management 10*g* components, then the following procedure applies.

When you upgrade such an environment to Oracle Fusion Middleware 11*g*, note that you can choose to install Oracle Internet Directory in one of the following topologies:

- Upgrading Oracle Internet Directory With a Local Oracle WebLogic Server Domain

- Upgrading Oracle Internet Directory With a Remote Domain or No Domain

14.5.1 Upgrading Oracle Internet Directory With a Local Oracle WebLogic Server Domain

Perform the following tasks to upgrade an Oracle Internet Directory-only high availability environment to 11*g*:

- Task 1: On IDMHOST1, Install Oracle WebLogic Server and Create the Middleware Home

- Task 2: On IDMHOST1, Install and Configure Oracle Internet Directory 11g Release 1 (11.1.1.6.0)

- Task 3: On IDMHOST1, Upgrade Oracle Internet Directory to 11g

- Task 4: On IDMHOST1, Verify the Upgraded Oracle Internet Directory Instance

- Task 5: On IDMHOST2, Install Oracle Internet Directory 11g Release 1 (11.1.1.6.0)

- Task 6: On IDMHOST2, Register the Oracle Internet Directory Instance with the Domain on IDMHOST1

- Task 7: On IDMHOST2, Verify the Oracle Internet Directory Instance

14.5.1.1 Task 1: On IDMHOST1, Install Oracle WebLogic Server and Create the Middleware Home

For information on installing the Oracle WebLogic Server, see "Preparing for Installation" and "Running the Installation Program in Graphical Mode" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

When you install Oracle WebLogic Server, make a note of the complete path to the Middleware home. You will need this information later in the upgrade procedure.

14.5.1.2 Task 2: On IDMHOST1, Install and Configure Oracle Internet Directory 11*g* Release 1 (11.1.1.6.0)

To install and configure Oracle Internet Directory 11*g* on IDMHOST1, refer to the chapter "Installing and Configuring Oracle Identity Management (11.1.1.6.0)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

For complete instructions on configuring Oracle Internet Directory and Oracle Directory Integration Platform, see the "Configuring Oracle Internet Directory (OID)" and "Configuring Oracle Directory Integration Platform (ODIP)" chapters in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*. For more information, see the "Creating a WebLogic Domain in Graphical Mode" topic in the *Oracle Fusion Middleware Creating Domains Using the Configuration Wizard* guide.

14.5.1.3 Task 3: On IDMHOST1, Upgrade Oracle Internet Directory to 11*g*

Use the Oracle Fusion Middleware Upgrade Assistant to upgrade the Oracle Internet Directory 10*g* instance on IDMHOST1 to Oracle Internet Directory 11*g*.

Use the instructions in Section 14.3.3, "Task 3: On IDMHOST1, Upgrade Oracle Internet Directory and Oracle Directory Integration Platform to 11g" to upgrade the Oracle Internet Directory instance.

14.5.1.4 Task 4: On IDMHOST1, Verify the Upgraded Oracle Internet Directory Instance

Use the following OPMN command to verify that Oracle Internet Directory is up and running:

```
ORACLE_INSTANCE/opmnctl status
```

The output of the command should be similar to the following example:

```
Processes in Instance: oid_instance1
---------------------------------+--------------------+---------+---------
ias-component                    | process-type       |     pid | status
---------------------------------+--------------------+---------+---------
oid1                             | oidldapd           |   31394 | Alive
oid1                             | oidldapd           |   31392 | Alive
oid1                             | oidmon             |   31384 | Alive
```

Use the `ldapbind` command-line tool to ensure that you can connect to each Oracle Internet Directory instance and the LDAP Virtual Server. The `ldapbind` tool enables you to determine whether you can authenticate a client to a server.

For non-SSL:

```
ldapbind -h idmhost1.mycompany.com -p 389 -D "cn=orcladmin" -q
ldapbind -h idmhost2.mycompany.com -p 389 -D "cn=orcladmin" -q
ldapbind -h oid.mycompany.com -p 389 -D "cn=orcladmin" -q
```

For SSL:

```
ldapbind -h idmhost1.mycompany.com -p 636 -D "cn=orcladmin" -q -U 1
ldapbind -h idmhost2.mycompany.com -p 636 -D "cn=orcladmin" -q -U 1
ldapbind -h oid.mycompany.com -p 636 -D "cn=orcladmin" -q -U 1
```

where:

- U = SSL authentication mode

- 1 = No authentication required

- 2 = One way authentication required. With this option, you must also supply a wallet location (-W "file:/home/my_dir/my_wallet") and wallet password (-P wallet_password).

- 3 = Two way authentication required. With this option, you must also supply a wallet location (-W "file:/home/my_dir/my_wallet") and wallet password (-P wallet_password).

14.5.1.5 Task 5: On IDMHOST2, Install Oracle Internet Directory 11*g* Release 1 (11.1.1.6.0)

To install and configure Oracle Internet Directory 11*g* on IDMHOST2, refer to the chapter "Installing and Configuring Oracle Identity Management (11.1.1.6.0)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

For complete instructions on configuring Oracle Internet Directory and Oracle Directory Integration Platform, see the "Configuring Oracle Internet Directory (OID)" and "Configuring Oracle Directory Integration Platform (ODIP)" chapters in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*. For more information, see the "Creating a WebLogic Domain in Graphical Mode" topic in the *Oracle Fusion Middleware Creating Domains Using the Configuration Wizard* guide.

14.5.1.6 Task 6: On IDMHOST2, Register the Oracle Internet Directory Instance with the Domain on IDMHOST1

Register the Oracle Internet Directory instance on IDMHOST2 with the Oracle WebLogic Server domain on IDMHOST1, using the following OPMN command.

```
ORACLE_INSTANCE/opmnctl registerinstance
    -adminHost adminHostName
    -adminPort adminServerPort
    -adminUsername DOMAIN_ADMINISTRATOR_USERNAME
    -oracleInstance ORACLE_INSTANCE_HOME
```

For example:

```
ORACLE_INSTANCE/opmnctl registerinstance
    -adminHost IDMHOST1 MYCOMPANY.COM
    -adminPort 7001
    -adminUsername weblogic
    -oracleInstance /u01/app/oracle/product/11g/instances/oid_inst2
```

14.5.1.7 Task 7: On IDMHOST2, Verify the Oracle Internet Directory Instance

Use the procedure in Section 14.5.1.4, "Task 4: On IDMHOST1, Verify the Upgraded Oracle Internet Directory Instance" to verify the Oracle Internet Directory instance on IDMHOST2.

14.5.2 Upgrading Oracle Internet Directory With a Remote Domain or No Domain

This section provides the upgrade procedure when you want to use a remote Oracle WebLogic Server domain to register the upgraded Oracle Internet Directory 11*g* instances.

These steps are also applicable if you do not plan to register the Oracle Internet Directory instances with an Oracle WebLogic Server domain:

- Task 1: On IDMHOST1, Install and Configure Oracle Internet Directory 11g Release 1 (11.1.1.6.0)

- Task 2: On IDMHOST1, Upgrade Oracle Internet Directory to 11g

- Task 3: On IDMHOST1, Verify the Oracle Internet Directory Instance

- Task 4: On IDMHOST2, Install and Configure Oracle Internet Directory 11g Release 1 (11.1.1.6.0)

- Task 5: Verify the Oracle Internet Directory Instances on IDMHOST1 and IDMHOST2

- Task 6: Optionally, Register the Oracle Internet Directory Instances on IDMHOST1 and OIDHOST2 with an Existing Remote Domain

14.5.2.1 Task 1: On IDMHOST1, Install and Configure Oracle Internet Directory 11*g* Release 1 (11.1.1.6.0)

To install and configure Oracle Internet Directory 11*g* on IDMHOST1, refer to the chapter "Installing and Configuring Oracle Identity Management (11.1.1.6.0)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

For complete instructions on configuring Oracle Internet Directory and Oracle Directory Integration Platform, see the "Configuring Oracle Internet Directory (OID)" and "Configuring Oracle Directory Integration Platform (ODIP)" chapters in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*. For more information, see the "Creating a WebLogic Domain in Graphical Mode" topic in the *Oracle Fusion Middleware Creating Domains Using the Configuration Wizard* guide.

14.5.2.2 Task 2: On IDMHOST1, Upgrade Oracle Internet Directory to 11*g*

Use the Oracle Fusion Middleware Upgrade Assistant to upgrade the Oracle Internet Directory 10*g* instance on IDMHOST1 to Oracle Internet Directory 11*g*.

Use the instructions in Section 14.3.3, "Task 3: On IDMHOST1, Upgrade Oracle Internet Directory and Oracle Directory Integration Platform to 11g" to upgrade the Oracle Internet Directory instance.

14.5.2.3 Task 3: On IDMHOST1, Verify the Oracle Internet Directory Instance

Use the procedure in Section 14.5.1.4, "Task 4: On IDMHOST1, Verify the Upgraded Oracle Internet Directory Instance" to verify the Oracle Internet Directory instance on IDMHOST1.

14.5.2.4 Task 4: On IDMHOST2, Install and Configure Oracle Internet Directory 11*g* Release 1 (11.1.1.6.0)

To install and configure Oracle Internet Directory 11*g* on IDMHOST2, refer to the chapter "Installing and Configuring Oracle Identity Management (11.1.1.6.0)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

For complete instructions on configuring Oracle Internet Directory and Oracle Directory Integration Platform, see the "Configuring Oracle Internet Directory (OID)" and "Configuring Oracle Directory Integration Platform (ODIP)" chapters in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*. For more information, see the "Creating a WebLogic Domain in Graphical Mode" topic in the *Oracle Fusion Middleware Creating Domains Using the Configuration Wizard* guide.

14.5.2.5 Task 5: Verify the Oracle Internet Directory Instances on IDMHOST1 and IDMHOST2

Use the procedure in Section 14.5.1.4, "Task 4: On IDMHOST1, Verify the Upgraded Oracle Internet Directory Instance" to verify the Oracle Internet Directory instance on IDMHOST1.

14.5.2.6 Task 6: Optionally, Register the Oracle Internet Directory Instances on IDMHOST1 and OIDHOST2 with an Existing Remote Domain

Register both Oracle Internet Directory instances on IDMHOST1 and IDMHOST2 with the existing, remote Oracle WebLogic Server domain, using the following OPMN command.

```
ORACLE_INSTANCE/opmnctl registerinstance
    -adminHost adminHostName
    -adminPort adminServerPort
    -adminUsername DOMAIN_ADMINISTRATOR_USERNAME
    -oracleInstance ORACLE_INSTANCE_HOME
```

For example:

```
ORACLE_INSTANCE/opmnctl registerinstance
    -adminHost IDMHOST1 MYCOMPANY.COM
    -adminPort 7001
    -adminUsername weblogic
    -oracleInstance /u01/app/oracle/product/11g/instances/oid_inst2
```

15

Upgrading an Oracle Identity Management Cold Failover Cluster Environment

This chapter describes how to upgrade an Oracle Identity Management Cold Failover Cluster environment to Oracle Fusion Middleware 11*g*.

This upgrade procedure involves the following tasks:

- Task 1: Preparing for Upgrading Your Oracle Fusion Middleware Cold Failover Cluster Environment

- Task 2: Install Oracle WebLogic Server and Create the Middleware Home

- Task 3: Install and Configure the Oracle Internet Directory and Oracle Directory Integration Platform 11g Release 1 (11.1.1.6.0)

- Task 4: Verify the Oracle Internet Directory and Oracle Directory Integration Platform Installation

- Task 5: Upgrade Oracle Internet Directory and Oracle Directory Integration Platform

- Task 6: Verify the Upgrade of Oracle Internet Directory and Oracle Directory Integration Platform

- Task 7: Configuring the Upgraded Components for Active-Passive Deployments

- Task 8: Configure Fusion Middleware Control to Monitor the Upgraded Components

- Task 9: Verify the Upgraded High Availability Environment

15.1 Task 1: Preparing for Upgrading Your Oracle Fusion Middleware Cold Failover Cluster Environment

The procedures in this chapter provide instructions for upgrading high availability environments supported in Oracle Application Server 10*g* Release 2 (10.1.2) and 10*g* (10.1.4.0.1).

Before you begin, review the following sections for important prerequisite for the upgrade process.

Oracle Identity Management 10*g* Components Must Be Installed and Running on IDMHOST1

It is assumed that your Oracle Identity Management 10*g* components are installed and running on IDMHOST1. This is important because the Oracle Identity Management

11*g* components that you are upgrading must be installed on the same host as the Oracle Identity Management 10*g* components.

Only Oracle Internet Directory and Oracle Directory Integration Platform Components are Upgraded to 11*g*

As part of this procedure, only Oracle Internet Directory and Oracle Directory Integration Platform are upgraded to Oracle Fusion Middleware 11*g*. For more information about the differences between the components available in Oracle Application Server 10*g* and Oracle Fusion Middleware 11*g*, see Section 4.1, "Summary of the Oracle Identity Management 10g and 11g Components".

Understanding Oracle Fusion Middleware Cold Failover Cluster for 11*g*

Oracle Fusion Middleware provides an active-passive model for all its components using Oracle FMW Cold Failover Clusters. In an Oracle FMW Cold Failover Cluster configuration, two or more application server instances are configured to serve the same application workload but only one is active at any particular time.

For more information, see "Oracle Fusion Middleware Cold Failover Cluster Topology Concepts" in the *Oracle Fusion Middleware High Availability Guide*.

Database High Availability and Version Requirements

For information database requirements for upgrade, as well as additional upgrade information for Oracle Fusion Middleware 11*g*, see the *Oracle Fusion Middleware Upgrade Planning Guide*.

Additional Resources

For information about the supported high availability topologies in Oracle Fusion Middleware 11*g*, see the *Oracle Fusion Middleware High Availability Guide*.

Before you begin these procedures, review the procedures and prerequisites available in Chapter 5, "Upgrading Your Oracle Internet Directory Environment".

15.2 Task 2: Install Oracle WebLogic Server and Create the Middleware Home

For information on installing the Oracle WebLogic Server, see "Preparing for Installation" and "Running the Installation Program in Graphical Mode" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

When you install Oracle WebLogic Server, make a note of the complete path to the Middleware home. You will need this information later in the upgrade procedure.

15.3 Task 3: Install and Configure the Oracle Internet Directory and Oracle Directory Integration Platform 11*g* Release 1 (11.1.1.6.0)

To install and configure Oracle Internet Directory and Oracle Directory Integration Platform 11*g*, refer to the chapter "Installing and Configuring Oracle Identity Management (11.1.1.6.0)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

For complete instructions on configuring Oracle Internet Directory and Oracle Directory Integration Platform, see the "Configuring Oracle Internet Directory (OID)" and "Configuring Oracle Directory Integration Platform (ODIP)" chapters in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*. For more

information, see the "Creating a WebLogic Domain in Graphical Mode" topic in the *Oracle Fusion Middleware Creating Domains Using the Configuration Wizard* guide.

15.4 Task 4: Verify the Oracle Internet Directory and Oracle Directory Integration Platform Installation

Before you upgrade run the Upgrade Assistant, use the following procedure to ensure that Oracle Internet Directory and Oracle Directory Integration Platform 10*g* and 11*g* are up and running on the host.

Step 1 Verify the status of Oracle Internet Directory 10g instance

For example, you can use the `opmnctl` command:

```
ORACLE_HOME/opmm/bin/opmnctl status
Processes in Instance: cfc.mycompany.com
------------------+-------------------+---------+---------
ias-component     | process-type      |     pid | status
------------------+-------------------+---------+---------
DSA               | DSA               |     N/A | Down
LogLoader         | logloaderd        |     N/A | Down
dcm-daemon        | dcm-daemon        |     N/A | Down
HTTP_Server       | HTTP_Server       |   26117 | Alive
OID               | OID               |   26121 | Alive
```

Step 2 Verify the status of the Oracle Directory Integration Platform 10*g* instance

For example, on a UNIX system, you can use the `ps` command and the `grep` command to search for the `odisrv` process in the resulting output:

```
$ ps -ef | grep odisrv
oracle    15711 15552  0 21:17 pts/0    00:00:00 grep odisrv
oracle    21597     1  0 Feb18 ?        00:00:00 /bin/sh
/u01/app/oracle/product/10g/idm/odisrv instance=1 configset=0 port=636 sslauth=1
host=idmhost1.mycompany.com
```

Step 3 Verify the status of the Oracle Internet Directory 11*g* instance

Use the following OPMN command to verify that Oracle Internet Directory is up and running:

```
ORACLE_INSTANCE/opmnctl status
```

The output of the command should be similar to the following example:

```
Processes in Instance: oid_instance1
-------------------------------+-------------------+---------+---------
ias-component                  | process-type      |     pid | status
-------------------------------+-------------------+---------+---------
ohs1                           | OHS               |    2492 | Alive
ovd1                           | OVD               |    2536 | Alive
oid1                           | oidldapd          |    8152 | Alive
oid1                           | oidldapd          |    7988 | Alive
oid1                           | oidmon            |    7964 | Alive
EMAGENT                        | EMAGENT           |    2484 | Alive
```

Use the `ldapbind` command-line tool to ensure that you can connect to each Oracle Internet Directory instance and the LDAP Virtual Server. The `ldapbind` tool enables you to determine whether you can authenticate a client to a server.

For non-SSL:

```
ldapbind -h idmhost1.mycompany.com -p 389 -D "cn=orcladmin" -q
```

For SSL:

```
ldapbind -h idmhost1.mycompany.com -p 636 -D "cn=orcladmin" -q -U 1
```

where:

- U = SSL authentication mode

- 1 = No authentication required

- 2 = One way authentication required. With this option, you must also supply a
  wallet location (`-W "file:/home/my_dir/my_wallet"`) and wallet password
  (`-P wallet_password`).

- 3 = Two way authentication required. With this option, you must also supply a
  wallet location (`-W "file:/home/my_dir/my_wallet"`) and wallet password
  (`-P wallet_password`).

Step 4 Verify the status of the Oracle Directory Integration Platform 11*g* instance

Validate the Oracle Directory Integration Platform installation by using the WLST
dipStatus command. To run this command, follow these steps:

1. Set the ORACLE_HOME environment variable to the directory where you
    installed the Identity Management binaries. For example:

    ```
    export ORACLE_HOME=/u01/app/oracle/product/11g/fmw_home/ods
    ```

2. Set the WLS_HOME environment variable to the directory where you installed the
    WebLogic Server.

    For example:

    ```
    export WLS_HOME=/u01/app/oracle/product/11g/fmw_home/wlserver_10.3
    ```

3. Run the following command:

    ```
    $ORACLE_HOME/bin/dipStatus -h <hostName> -p <port> -D <wlsuser>
    ```

    For example, on IDMHOST1, the command and successful output are shown
    below:

    ```
    $ORACLE_HOME/bin/dipStatus
        -h idmhost1.mycompany.com
        -p 7005
        -D weblogic
        [Weblogic user password]
         Connection parameters initialized.
         Connecting at idmhost1.mycompany.com:7005, with userid "weblogic"..
         Connected successfully.
         ODIP Application is active at this host and port.
    ```

Step 5 Verify Oracle Directory Services Manager (ODSM)

Verify the Oracle Directory Services Manager installation by bringing up the ODSM
Administration Console in a web browser.

The URL to access the ODSM Administration Console is:

```
http://hostname.mycompany.com:<port>/odsm/faces/odsm.jspx
```

For example, on IDMHOST1, enter this URL:

```
http://idmhost1.us.oracle.com:7005/odsm/faces/odsm.jspx
```

15.5 Task 5: Upgrade Oracle Internet Directory and Oracle Directory Integration Platform

Use the Oracle Fusion Middleware Upgrade Assistant to upgrade the Oracle Internet Directory and Oracle Directory Integration Platform 10*g* instances on IDMHOST1 to 11*g*:

1. Change directory the *ORACLE_HOME*/bin directory of the Oracle Fusion Middleware installation.

2. Enter the following command to start the Upgrade Assistant.

   On UNIX system:

   ```
   ./ua
   ```

   On Windows systems:

   ```
   ua.bat
   ```

   The Upgrade Assistant displays the Welcome screen.

3. Click **Next** to display the Specify Operation screen.

4. Select **Upgrade Identity Management Instance** on the Specify Operation screen.

5. Refer to Table 15–1 for a description of the Upgrade Assistant screens that require input from you during an Oracle Internet Directory and Oracle Directory Integration Platform upgrade.

6. After the Target Database Details screen, the Upgrade Assistant performs the following tasks and provides the progress on each task:

   - Examines the components and schemas to be upgraded and verifies that they can be upgraded successfully.

   - Provides a summary of the components to be upgraded so you can verify that Upgrade Assistant is upgrading the components and schemas you expect.

   - Provides a progress screen so you can see the status of the upgrade as it proceeds.

   - Alerts you of any errors or problems that occur during the upgrade.

     See Also: "Troubleshooting Your Upgrade" in the *Oracle Fusion Middleware Upgrade Planning Guide* for specific instructions for troubleshooting problems that occur while running the Upgrade Assistant

   - Displays the End of Upgrade screen, which confirms that the upgrade was complete.

7. Exit the Upgrade Assistant.

Table 15–1   Upgrade Assistant Screens That Require Input During an Oracle Internet Directory and Oracle Directory Integration Platform Upgrade

Upgrade Assistant Screen	Description
Specify Source Home	Select the 10*g* Release 2 (10.1.2) or 10*g* (10.1.4) source Oracle home.
	If the Oracle home you want to upgrade does not appear in the drop-down lists, see "Source Oracle Home Not Listed by OracleAS Upgrade Assistant" in the *Oracle Fusion Middleware Upgrade Planning Guide*.
Specify Destination Instance	Enter the complete path to the 11*g* Oracle instance, or click **Browse** to locate the instance directory.
Specify WebLogic Server	Enter the host and Administration Server port for the Oracle WebLogic Server you configured in "Task 2: Install Oracle WebLogic Server and Create the Middleware Home".
	Note this information is required if you are upgrading Oracle Directory Integration Platform. It is also required if you associated your Oracle Internet Directory 11*g* installation with Oracle WebLogic Server.
Warning Dialog Box	The Upgrade Assistant displays this warning dialog box if the source Oracle home contains Oracle Application Server components that are not installed and configured in the destination Oracle instance.
	This warning appears, for example, if the source Oracle home contains an instance of Oracle HTTP Server, which is not available in the 11*g* Oracle home.
	If the information in the dialog box is accurate and you understand which components will be upgraded, click **Yes** to continue. Otherwise, click **No** and verify which components are installed and configured in each 11*g* Oracle instance.
Specify Upgrade Options	Select the upgrade options you want to apply to the Oracle Identity Management upgrade:
	■ **Use source Oracle home ports in destination:** If you want to migrate the port assignments used by your Oracle Application Server 10g Oracle home to your new Oracle Fusion Middleware Oracle instance. Note if you select this option, you will not be able to run both the 10*g* and 11*g* middle tiers at the same time; otherwise, port conflicts will occur.
	■ **Start destination components after successful upgrade:** if you want the Upgrade Assistant to automatically start the components in the destination Oracle home after the upgrade is complete. If you do not select this option, then you will have to manually start the destination instance after the upgrade.
	Click **Help** to display more information about the upgrade options on this screen.
Specify OID Details	Use this screen to enter the details required to connect to the Oracle Internet Directory 10*g* instance, including the password to the Oracle Internet Directory super user account (`cn=orcladmin`).
	For more information, click **Help**.

Table 15–1   (Cont.) Upgrade Assistant Screens That Require Input During an Oracle Internet Directory and Oracle Directory Integration Platform Upgrade

Upgrade Assistant Screen	Description
Specify Database Details	Use this screen to enter the details required to connect to the database where the Oracle Identity Management schemas reside, including the host, service name, port, and SYS password for the database.
	Note the following important information about this screen:
	■ You must enter the password for the ODS schema password. The default ODS password is the same as the Oracle Application Server administrator password, but this password can be changed after installation, using the OID Database Password Utility.
	■ The instructions for identifying a Real Application Clusters (RAC) database are different, depending upon whether you are identifying the RAC database that contains the Oracle Internet Directory (ODS) schema or a RAC database that is being used for Oracle Directory Integration Platform.
	For more information, see Section 5.4.3.2, "About Specifying Real Application Clusters (RAC) Database Details on the Specify Database Details Screen".
Root action required screen	This is only if you are using privileged port on a UNIX system.
	A configuration script needs to be run as root before upgrade can proceed.
	Leaving this window open, open another window, and run the upgroot.sh file as root:
	When the script has completed, return to the Upgrade Assistant and click **OK**.

15.6 Task 6: Verify the Upgrade of Oracle Internet Directory and Oracle Directory Integration Platform

Use Steps 3 through 5 of Section 15.4, "Task 4: Verify the Oracle Internet Directory and Oracle Directory Integration Platform Installation" to verify that the upgraded Oracle Identity Management components are up and running.

15.7 Task 7: Configuring the Upgraded Components for Active-Passive Deployments

Use the following steps to configure the upgraded components in an active-passive high availability environment.

Note that these steps reference specific sections in the *Oracle Fusion Middleware High Availability Guide*, which provides comprehensive instructions for configuring high availability in Oracle Fusion Middleware 11*g*:

■ Task 7a: Transform the Infrastructure Components for Cold Failover Clusters

■ Task 7b: Transforming Oracle Internet Directory and Its Clients for Cold Failover Clusters

15.7.1 Task 7a: Transform the Infrastructure Components for Cold Failover Clusters

Transform the infrastructure components that support the Oracle Internet Directory environment. For each step in this process, refer to the corresponding procedure in the *Oracle Fusion Middleware High Availability Guide*:

Table 15–2   Steps to Transform the Infrastructure Components for Cold Failover Cluster

Step #	Description	Section in Oracle Fusion Middleware High Availability Guide
1	Transform the Oracle WebLogic Server administration server	"Transforming the Administration Server for Cold Failover Clusters"
2	Transform the wls_ods managed server	"Transforming Oracle WebLogic Managed Servers"
3	Transform the Oracle WebLogic Server node manager	"Transforming Node Manager"
4	Transform the Fusion Middleware Control	"Transforming Oracle Enterprise Manager"
5	Transform the Oracle Process Manager and Notification Server (OPMN)	"Transforming Oracle Process Management and Notification Server"
6	Transform the Oracle HTTP Server	"Transforming Oracle HTTP Server"

15.7.2 Task 7b: Transforming Oracle Internet Directory and Its Clients for Cold Failover Clusters

After you have transformed the infrastructure components for Cold Failover Cluster, you can do the same for the upgraded Oracle Internet Directory 11*g* instance.

Refer to "Transforming Oracle Internet Directory and Its Clients" in the *Oracle Fusion Middleware High Availability Guide*.

15.8 Task 8: Configure Fusion Middleware Control to Monitor the Upgraded Components

After the Cold Failover Cluster transformation, the Oracle Enterprise Manager Fusion Middleware Control cannot display the correct status for some of the upgraded components.

To fix this problem, you must modify specific Fusion Middleware Control configuration files so they reference to the virtual host name used for the Cold Failover transformation instead of the physical host name.

Follow the steps below to update the Fusion Middleware Control configuration files:

1. Stop the Oracle Enterprise Manager Fusion Middleware Control agent:

    ```
    ORACLE_HOME/bin/emctl stop agent
    ```

2. Modify the emd.properties file in the Oracle instance directory:

    a. Change directory to the following directory in the Oracle instance:

    ```
    ORACLE_INSTANCE/emagent/em_agent_name/sysman/config
    ```

    b. Make a backup copy of the emd.properties file:

    For example, on UNIX systems:

    ```
    cp emd.properties emd.properties.bak
    ```

c. Edit the `emd.properties` file so it references the virtual host name, rather than the physical host name.

For example, if the physical host name is `host1.mycompany.com` and the virtual host name is `cfcvip.mycompany.com`, then you must change the reference accordingly in the following attributes in the `emd.properties` file:

`REPOSITORY_URL`

`EmdWalletSrcUrl`

`emd_url`

3. Modify the `targets.xml` file in the Oracle instance:

a. Change directory to the `emd` directory of the Oracle instance:

INSTANCE_HOME/emagent/*em_agent_name*/sysman/emd

b. Make a backup copy of the `targets.xml` file:

For example, on UNIX systems:

`cp targets.xml targets.xml.bak`

c. Modify `targets.xml`, as follows:

Modify the entries related to `host` and `oracle_emd` so they reference the virtual host name (for example, `cfcvip.mycompany.com`):

For example:

```
<Targets AGENT_TOKEN="ad4e5899e7341bfe8c36ac4459a4d569ddbf03bc">
    <Target TYPE="oracle_emd" NAME=cfcvip.mycompany.com:5157"/>
    <Target TYPE="host" NAME=cfcvip.mycompany.com
                    DISPLAY_NAME=cfcvip.mycompany.com/>
</Targets>
```

Remove all other `<Target>` entries in the file.

4. Modify the `targets.xml` file in the domain directory:

a. Change directory to the following directory in the Oracle WebLogic Server domain directory inside the Middleware home:

`MW_HOME/user_projects/domains/domain_name/sysman/state`

b. Make a backup copy of the `targets.xml` file:

For example, on UNIX systems:

`cp targets.xml targets.xml.bak`

c. Edit the `targets.xml` file and change all occurrences of the physical host name to the virtual host name.

For example, change all occurrences of `host1.mycompany.com` to `cfcvip.mycompany.com`.

5. Modify the `topology.xml` file in the domain directory:

a. Change directory to the following location in the domain directory inside the Middleware home:

MW_HOME/user_projects/domains/*domainName*/opmn

b. Make a backup copy of the `topology.xml` file:

For example, on UNIX systems:

```
cp topology.xml topology.xml.bak
```

    c. Edit the `topology.xml` file and change all occurrences of the physical host name to the virtual host name.

    For example, change all occurrences of `host1.mycompany.com` to `cfcvip.mycompany.com`.

6. Restart the administration server for the Oracle WebLogic Server domain.

7. Restart the Oracle Enterprise Manager Fusion Middleware Control agent:

```
INSTANCE_HOME/emagent/em_agent_name/emctl start agent
INSTANCE_HOME/emagent/em_agent_name/emctl status agent
```

15.9 Task 9: Verify the Upgraded High Availability Environment

This section provides the steps to verify the transformation of the infrastructure and Oracle Identity Management components to Cold Failover Cluster:

1. Use the Virtual Hostname instead of the physical hostname to display the Fusion Middleware Control and the Oracle WebLogic Server Administration Console in your Web browser. The URLs are listed below:

- Fusion Middleware Control: `http://VirtualHostname:port/em`

- Oracle WebLogic Server Console: `http://VirtualHostname:port/console`

For example use a web browser and access the following consoles:

- Fusion Middleware Control: `http://idmhost-vip.mycompany.com/em`

- Oracle WebLogic Server Console: `http://idmhost-vip.mycompany.com`

2. Verify that the Oracle Identity Management 11*g* components are up and running. Use steps 3 through 5 in Section 15.4, "Task 4: Verify the Oracle Internet Directory and Oracle Directory Integration Platform Installation".

16

Performing an Oracle Identity Management Multimaster and Fan-Out Replication Upgrade

This appendix describes how to upgrade to Oracle Identity Management 11*g* Release 1 (11.1.1) in an Oracle Internet Directory replicated environment.

Refer to the following sections for more information:

- Task 1: Review the Terminology, Prerequisites, and Key Concepts For Upgrading a Replication Environment

- Task 2: Prepare for the Oracle Identity Management Multimaster or Fan-Out Replication Upgrade

- Task 3: Perform the Oracle Internet Directory Replica Upgrade

- Task 4: Completing the Upgrade of Each Replica

16.1 Task 1: Review the Terminology, Prerequisites, and Key Concepts For Upgrading a Replication Environment

Review the following prerequisites and requirements before proceeding with the upgrade procedures in this chapter:

- Terminology Conventions for This Chapter

- Valid Starting Points When Upgrading a Replication Environment

- Oracle Recommendations When Upgrading a Replication Environment

16.1.1 Terminology Conventions for This Chapter

In this chapter, the **destination replica** is the newly installed and upgraded 11*g* Release 1 (11.1.1) replica; the **source replica** is the 10*g* Release 2 (10.1.2) or 10*g* (10.1.4.0.1) replica you are upgrading.

16.1.2 Valid Starting Points When Upgrading a Replication Environment

The upgrade procedures in this chapter are designed for administrators who have installed and configured an Oracle Internet Directory 10*g* Release 2 (10.1.2) or 10*g* (10.1.4.0.1) multimaster or fan-out replication environment.

This chapter assumes that the Oracle Identity Management components in the replication environment are distributed. In other words, you have installed the Oracle Internet Directory (and optionally Oracle Directory Integration Platform) components

in one or more Oracle homes, and you installed the Oracle Single Sign-On and Oracle Delegated Administration Services components in one or more additional Oracle homes.

Figure 16–1 shows a typical Oracle Identity Management 10g Release 2 (10.1.2) multimaster replication environment, which is described in detail in "Deploying Identity Management with Multimaster Replication," in the 10g Release 2 (10.1.2) *Oracle Fusion Middleware High Availability Guide*.

Figure 16–1   A Typical Oracle Identity Management 10g Release 2 (10.1.2) Multimaster Replication Environment
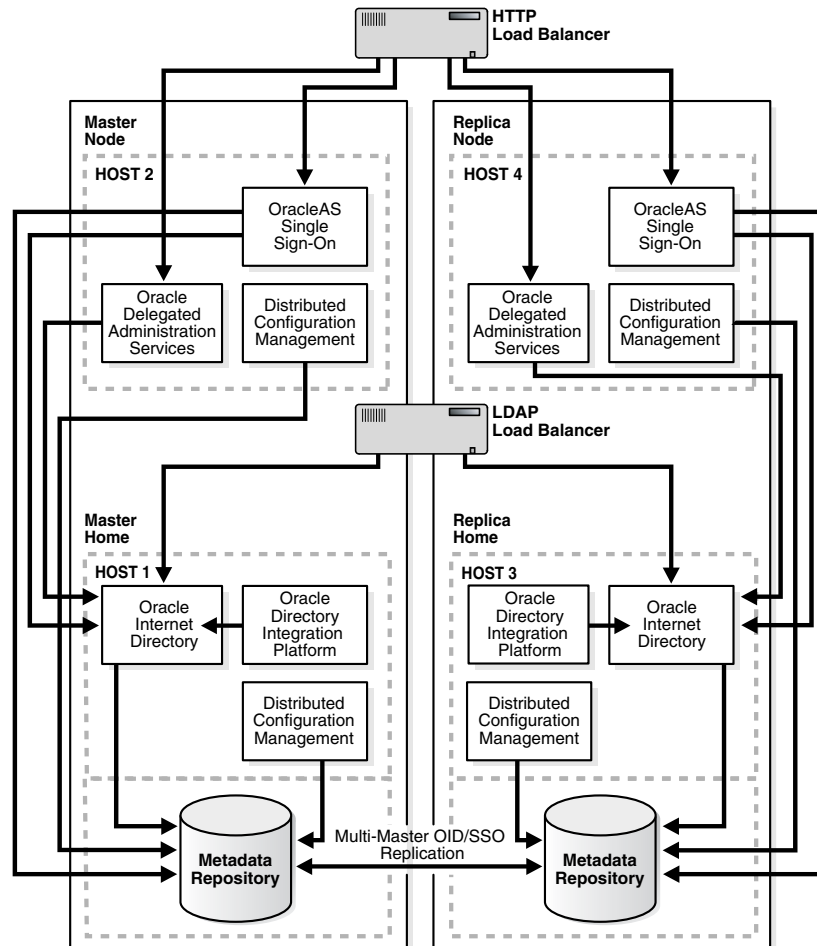
Information about deploying Oracle Identity Management with fan-out replication can be found in the Oracle Application Server 10*g* (10.1.4.0.1) *Oracle Identity Management Concepts and Deployment Planning Guide*, which is available in the Oracle Application Server 10g Release 2 (10.1.2) documentation library.

16.1.3 Oracle Recommendations When Upgrading a Replication Environment

Oracle Corporation recommends the following during the upgrade procedure:

- After you upgrade the destination replica, disable replication between the destination replica and the source replica. The destination replica can receive and process changes from source replica, but the source replica cannot process changes originated and received from destination replica.

■ The replication environment can be a Single Master (that is, only one replica is set to read and write, and all others are set to read only).

16.2 Task 2: Prepare for the Oracle Identity Management Multimaster or Fan-Out Replication Upgrade

Before you begin upgrading Oracle Internet Directory in a replicated environment, you must perform the following steps for all replicas other than Master Definition Site (MDS) Replica or Primary supplier replica:

1. Locate the database registration entry of the database of replica to be upgraded.

   On Window systems:

   ```
   SOURCE_ORACLE_HOME\bin\ldapsearch
        -h hostname_of_replica_being_upgraded
        -p port
        -D cn=orcladmin
        -w superuser_password
        -b "cn=oraclecontext"
        -s one "(objectclass=orcldbserver)" dn
   ```

   On UNIX systems:

   ```
   SOURCE_ORACLE_HOME/bin/ldapsearch
        -h hostname_of_replica_being_upgraded
        -p port
        -D cn=orcladmin
        -w superuser_password
        -b "cn=oraclecontext"
        -s one "(objectclass=orcldbserver)" dn
   ```

   This will return a list of Distinguished Names (DNs) corresponding to all the Databases registered in Oracle Internet Directory in the following form:

   ```
   cn=database_name,cn=oraclecontext
   ```

   From the returned list of entries, locate and make a note of the DN of the following entry, which corresponds to the replica upgraded:

   ```
   cn=dbname_of_replica_to_be_upgraded,cn=oraclecontext
   ```

2. Identify the replica ID of the replica to be upgraded by issuing following command:

   On Windows systems:

   ```
   SOURCE_ORACLE_HOME\bin\ldapsearch
        -h hostname_of_replica_being_upgraded
        -p port
        -D cn=orcladmin
        -w superuser_password
        -b "" -s base "(objectclass=*)" orclreplicaid
   ```

   On UNIX systems:

   ```
   SOURCE_ORACLE_HOME/bin/ldapsearch
        -h hostname_of_replica_being_upgraded
        -p port
        -D cn=orcladmin
        -w superuser_password
        -b ""
   ```

```
-s base "(objectclass=*)" orclreplicaid
```

3. Modify the `seeAlso` attribute of the replica subentry so that it points to the database you are about to upgrade.

   The `seeAlso` attribute is a standard Oracle Internet Directory attribute. For more information, refer to "seeAlso" in the *Oracle Fusion Middleware User Reference for Oracle Identity Management*.

   To modify the `seeAlso` attribute:

   a. Create a file, for example `mod.ldif`, with following contents:

   ```
   #File Name : mod.ldif
   dn: orclreplicaid=replicaid_from_step_2,cn=replication configuration
   changetype: modify
   replace: seeAlso
   #The DN used in seealso attribute is obtained in Step #1.
   seeAlso: cn=dbname_of_replica_being_upgraded,cn=oraclecontext
   ```

   b. Modify the replica subentry using ldapmodify command.

   On Windows systems:

   ```
   SOURCE_ORACLE_HOME\bin\ldapmodify
       -h hostname_of_replica_being_upgraded
       -p port
       -D superuser_DN
       -w superuser_password
       -v
       -f mod.ldif
   ```

   On UNIX systems:

   ```
   SOURCE_ORACLE_HOME/bin/ldapmodify
       -h hostname_of_replica_being_upgraded
       -p port
       -D superuser_DN
       -w superuser_password
       -v
       -f mod.ldif
   ```

4. Navigate to the following directory and locate `ias.properties` file:

   On Windows systems:

   ```
   SOURCE_ORACLE_HOME\config
   ```

   On UNIX systems:

   ```
   SOURCE_ORACLE_HOME/config
   ```

5. Open the `ias.properties` file and verify that the properties shown in Table 16–1 are correct and valid.

6. Make sure the Oracle Internet Directory server is up and running.

   To verify that Oracle Internet Directory is running, enter one of the following commands.

> **Note:** You may have to temporarily set the ORACLE_HOME environment variable to the Oracle Internet Directory Oracle home before running the `ldapbind` command.
>
> After you verify that the Oracle Internet Directory is running, you must then make sure the ORACLE_HOME environment variable is not defined before you start the 11*g* Release 1 (11.1.1) installer to begin the upgrade procedure.

If you are running Oracle Internet Directory on a non-secure port:

SOURCE_ORACLE_HOME/bin/ldapbind -p *Non-SSL_port*

If you are running Oracle Internet Directory on a secure port:

SOURCE_ORACLE_HOME/bin/ldapbind -p *SSL_port* -U 1

These commands should return a "bind successful" message.

7. Stop the second LDAP server as shown below.

This example assumes that the instance number used for the second instance was 2.

SOURCE_ORACLE_HOME/bin/oidctl connect=*connect_string_of_db* server=oidldapd
instance=2 stop

Table 16–1   Properties to Verify in ias.properties Before Replication Upgrade

Property Name	Correct Value Before Replication Upgrade
OID.LaunchSuccess	True
OIDhost	*host name of replica*
OIDport	*port of replica*
OIDsslport	*SSL port for replica*

16.3 Task 3: Perform the Oracle Internet Directory Replica Upgrade

You can upgrade one replica at a time, or all of the replicas simultaneously. Refer to the following sections for more information:

- Selecting a Replica Upgrade Method
- Upgrading One Replica at a Time
- Upgrading Oracle Internet Directory on Multiple Replicas Simultaneously

16.3.1 Selecting a Replica Upgrade Method

Upgrading one computer at a time in a replicated environment ensures that Oracle Internet Directory is available during the upgrade for additions, modifications, and searching. When you use this method, only the replica you are upgrading is down. The other replicas continue to run and are available to your users.

Upgrading multiple replicas simultaneously ensures that the entire network is upgraded without a transient stage. The procedure is simpler than upgrading one replica at a time, but involves directory service downtime.

16.3.2 Upgrading One Replica at a Time

Follow these steps to upgrade one replica at a time:

1. Make sure you have completed the procedure in Section 16.2, "Task 2: Prepare for the Oracle Identity Management Multimaster or Fan-Out Replication Upgrade".

2. Identify the replication server on the replica to be upgraded.

   The replica can be an LDAP-based partial or fan-out replica, or it can be an Oracle Advanced Replication (ASR) based multimaster replica.

   > **See Also:** "Directory Replication Concepts" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

3. Modify your load balancer to route traffic away from the replica you are about to upgrade; instead route all client traffic to the other replicas.

4. Make sure the replica is up-to-date with changes from the other replica.

   This check is required to make sure that all the changes from the first replica are captured in the second replica before we turn off replication.

5. Stop the replication server on the replica to be upgraded.

   On UNIX systems:

   ```
   SOURCE_ORACLE_HOME/oidctl
       connect=db_connect_string
       server=OIDREPLD
       instance=1
       flags="-p port_at_which_ldap_server_is_listening"
       stop
   ```

   On Windows systems:

   ```
   SOURCE_ORACLE_HOME\oidctl
       connect=db_connect_string
       server=OIDREPLD
       instance=1
       flags="-p port_at_which_ldap_server_is_listening"
       stop
   ```

   > **See Also:** "Oracle Identity Management Server Administration Tools" in the *Oracle Fusion Middleware User Reference for Oracle Identity Management* for more information about the `oidctl` administration tool

6. Make sure that the Oracle Internet Directory server, the Oracle Internet Directory database, and the database listener are up and running.

7. If you are upgrading an ASR-based replica, then delete all ASR jobs on other replicas by issuing the oidrdjob.sql script.

   For example:

   ```
   export TWO_TASK=db_name_of_replica_being_upgraded
   ORACLE_HOME/bin/sqlplus repadmin/password@connect_string_of_db
           @ORACLE_HOME/ldap/admin/oidrdjob.sql
   ```

   All ASR jobs on other master sites that transfer changes to this replica are deleted. This has the effect of taking the replica currently being upgraded out of the

replication environment, so that no changes come to it, while other replicas continue to operate and replicate changes.

8. Depending on the configuration of the replica, refer to the following documentation resources to perform the upgrade of the replica:

   ■ If the replica you are upgrading is configured for Oracle Identity Management high availability, then use the instructions in Section 14.3, "Upgrading Oracle Internet Directory and Oracle Directory Integration Platform in a High Availability Environment".

   ■ If the replica you are upgrading is not configured for high availability, then use the instructions in Chapter 5, "Upgrading Your Oracle Internet Directory Environment" to upgrade the replica to Oracle Internet Directory 11*g*.

   Note that upgrading the replica involves the following steps:

   ■ Installing Oracle WebLogic Server and creating the Middleware home

   ■ Installing and configuring Oracle Internet Directory.

   ■ Running the Upgrade Assistant to upgrade the configuration from the Oracle Internet Directory 10*g* instance to 11*g*

   ■ Performing any post-upgrade tasks for your environment.

9. After you upgrade the replica, verify that the database in the upgraded replica Oracle home is up and running.

10. Test the connectivity to the other replicas.

    The Net Services Upgrade assistant might have modified `listener.ora` and `tnsnames.ora,` breaking connectivity. If connectivity is broken, identify the entries that were modified in the files, and restore the entries from the corresponding files in the source Oracle home.

    For example, copy the original entries from the following files in the source Oracle home to the corresponding files in the destination Oracle home:

    ```
    SOURCE_ORACLE_HOME/network/admin/listener.ora
    SOURCE_ORACLE_HOME/network/admin/sqlnet.ora
    SOURCE_ORACLE_HOME/network/admin/tnsnames.ora
    ```

11. If you are upgrading an Oracle Advanced Replication (ASR) based Replica, recreate the jobs on each replica, after it is upgraded, by issuing the following command:

    ```
    export LD_LIBRARY_PATH=DESTINATION_ORACLE_HOME/lib
    DESTINATION_ORACLE_HOME/ldap/bin/remtool -asrrectify
    ```

    The jobs that were deleted in previously are re-created. They will begin transferring the existing changes and new changes from other replicas to the upgraded replicas.

12. Perform the procedures described in Section 16.4, "Task 4: Completing the Upgrade of Each Replica" for the newly upgraded replica.

13. Stop the 10*g* replication servers.

    This is to avoid replicating the upgraded replica with those that have not been upgraded yet.

    Run the following command:

    ```
    export TWO_TASK=db_name_of_second_replica
    ```

```
sqlplus repadmin/welcome1@db_connect_string
        @$ORACLE_HOME/ldap/admin/oidrdjob.sql
```

14. Redefine the following environment variables:

For example:

```
export INSTANCE_NAME=asinst_1
export COMPONENT_NAME=oid1
export ORACLE_HOME=11g_ORACLE_HOME_PATH
export ORACLE_INSTANCE=11g_ORACLE_INSTANCE_PATH
```

15. Start the replication server on the newly upgrade replica, if it is not already running:

```
DESTINATION_ORACLE_HOME/oidctl
    connect=db_connect_string
    server=OIDREPLD
    instance=1
    flags="-p port_at_which_ldap_server_is_listening"
    start
```

> **See Also:** "Oracle Identity Management Server Administration Tools" in the *Oracle Fusion Middleware User Reference for Oracle Identity Management* for more information about the `oidctl` administration tool

16. Modify the load balancer to route client traffic back to the newly upgraded replica.

17. Upgrade the remaining replicas using the same procedures you used to upgrade the first replica.

16.3.3 Upgrading Oracle Internet Directory on Multiple Replicas Simultaneously

Use the following procedure to upgrade all the replicas simultaneously:

1. In all replicas other than MDS replica or primary supplier replica, make sure you have completed the pre-upgrade steps provided in Section 16.2, "Task 2: Prepare for the Oracle Identity Management Multimaster or Fan-Out Replication Upgrade".

2. Stop the replication server on all replicas in the Directory Replication Group (DRG):

```
SOURCE_ORACLE_HOME/oidctl
    connect=db_connect_string
    server=OIDREPLD
    instance=1
    flags="-p port_at_which_ldap_server_is_listening"
    stop
```

> **See Also:** "Oracle Identity Management Server Administration Tools" in the *Oracle Fusion Middleware User Reference for Oracle Identity Management* for more information about the `oidctl` administration tool

3. Use the instructions in Chapter 5, "Upgrading Your Oracle Internet Directory Environment" to upgrade the replica to Oracle Internet Directory 11*g*.

Note that upgrading the replica involves the following steps, which are documented in Chapter 5:

- Installing Oracle WebLogic Server and creating the Middleware home

- Installing and configuring Oracle Internet Directory.

- Running the Upgrade Assistant to upgrade the configuration from the Oracle Internet Directory 10*g* instance to 11*g*

- Performing any post-upgrade tasks for your environment.

4. After you upgrade the replica, verify that the database on each upgraded replica is up and running.

5. Test the connectivity to the other replicas.

   The Net Services Upgrade assistant might have modified `listener.ora` and `tnsnames.ora,` breaking connectivity. If connectivity is broken, identify the entries that were modified in the files, and restore the entries from the corresponding files in the source Oracle home.

   For example, copy the original entries from the following files in the source Oracle home to the corresponding files in the destination Oracle home:

   ```
   SOURCE_ORACLE_HOME/network/admin/listener.ora
   SOURCE_ORACLE_HOME/network/admin/sqlnet.ora
   SOURCE_ORACLE_HOME/network/admin/tnsnames.ora
   ```

6. For each upgraded replica, perform the steps in Section 16.4, "Task 4: Completing the Upgrade of Each Replica".

7. Start the replication server on each of the upgraded replicas:

   ```
   DESTINATION_ORACLE_HOME/oidctl
      connect=db_connect_string
      server=OIDREPLD
      instance=1
      flags="-p port_at_which_ldap_server_is_listening"
      start
   ```

   > **See Also:**   "Oracle Identity Management Server Administration Tools" in the *Oracle Fusion Middleware User Reference for Oracle Identity Management* for more information about the `oidctl` administration tool

16.4 Task 4: Completing the Upgrade of Each Replica

The following sections describe tasks you must perform after you have completed the upgrade of a replica:

- Changing the Replication DN Password in the Oracle Internet Directory Wallet for Each Replica

- Setting the orclreplicationid Attribute in the Upgraded 11g Directory

16.4.1 Changing the Replication DN Password in the Oracle Internet Directory Wallet for Each Replica

After you upgrade a replica, change the password for the replication distinguished name (DN). After you change or reset the password, you can then start `oidmon`, LDAP server, and replication server.

Refer to the following sections for more information:

- Changing the Replication DN Password

■ Resetting the Replication DN Password

16.4.1.1 Changing the Replication DN Password

After you upgrade each replica, you must change the replication distinguished name (DN) password, using the Replication Environment Management Tool (`remtool`), as follows:

```
DESTINATION_ORACLE_HOME/ldap/bin/remtool
    -pchgwalpwd -v -bind host:port/repl_dn_pwd
```

Note that you must provide the existing password on the `remtool` command line. If you do not know the replication DN password, see Section 16.4.1.2, "Resetting the Replication DN Password".

> **See Also:** "remtool" in the *Oracle Fusion Middleware User Reference for Oracle Identity Management* for details about the arguments you can use with the `remtool` command, including the `-pchgwalpwd` and `-presetpwd` arguments

16.4.1.2 Resetting the Replication DN Password

If you do not know replication DN password, reset the replication DN password using the following command:

```
DESTINATION_ORACLE_HOME/ldap/bin/remtool -presetpwd -v -bind host:port
```

If you are upgrading a fan-out replica, you must also reset the password of the replication DN at its supplier. To reset the password of replication DN at its supplier:

1. Create an LDIF file (for example, `modpwd.ldif`), with following information:

   ```
   dn: cn=replication dn,orclreplicad=consumer_replicaid,cn=replication
   configuration
         changetype: modify
         replace: userpassword
         userpassword: new_password
   ```

2. Identify the replica ID of the replica to be upgraded by issuing following command:

   > **Note:** Before running the command, ensure that you set the `ORACLE_INSTANCE` environment variable.

   On Windows systems:

   ```
   SOURCE_ORACLE_HOME\bin\ldapsearch
       -h hostname_of_replica_being_upgraded
       -p port
       -D cn=orcladmin
       -w superuser_password
       -b "" -s base "(objectclass=*)" orclreplicaid
   ```

   On UNIX systems:

   ```
   SOURCE_ORACLE_HOME/bin/ldapsearch
       -h hostname_of_replica_being_upgraded
       -p port
       -D cn=orcladmin
       -w superuser_password
   ```

```
-b ""
-s base "(objectclass=*)" orclreplicaid
```

3. Create an LDIF file (for example, `modpwd.ldif`), with following contents:

```
dn: cn=replication dn,orclreplicad=consumer_replicaid,cn=replication
configuration
changetype: modify
replace: userpassword
userpassword: new_password
```

4. Apply the change at supplier using ldapmodify tool as shown below:

```
ldapmodify  -h supplier_hostname
            -p supplier_port_number>
            -D cn=orcladmin
            -w super_user_password_of_supplier
            -f modpwd.ldif
```

16.4.2 Setting the orclreplicationid Attribute in the Upgraded 11*g* Directory

If you are upgrading a 10*g* Release 2 (10.1.2) replica in an environment with fan-out replication, you must set the `orclreplicationid` in the Oracle Internet Directory attribute to a valid value.

This procedure is not necessary if you are upgrading from 10*g* (10.1.4.0.1), because this is a new attribute that was introduced in Oracle Identity Management 10*g* (10.1.4.0.1).

Oracle recommends that you set the value of this attribute so it matches the value of the existing `orclagreementID` attribute. To perform this task:

1. Identify the replica ID of the replica to be upgraded by issuing following command:

On Windows systems:

```
SOURCE_ORACLE_HOME\bin\ldapsearch
    -h hostname_of_replica_being_upgraded
    -p port
    -D cn=orcladmin
    -w superuser_password
    -b "" -s base "(objectclass=*)" orclreplicaid
```

On UNIX systems:

```
SOURCE_ORACLE_HOME/bin/ldapsearch
    -h hostname_of_replica_being_upgraded
    -p port
    -D cn=orcladmin
    -w superuser_password
    -b ""
    -s base "(objectclass=*)" orclreplicaid
```

2. Create an LDIF file called `id.ldif` with the following content:

```
dn: orclagreementid=000002,orclreplicaid=replicaid,cn=replication configuration
changetype: modify
replace: orclreplicationid
orclreplicationid: 2
```

Note that in the above example, the first two lines should appear all in one line in the LDIF file.

3. Apply the LDIF file by using the following `ldapmodify` command:

```
ldapmodify -p port
           -h host
           -D DN
           -w password
           -f id.ldif
```

In this example, replace *port*, *host*, *DN*, and *password* with the appropriate values for your environment.

> **See Also:**   "The Replication Agreement Entry" in the chapter, "Oracle Internet Directory Replication Concepts" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory* for information about the `orclreplicationid` attribute
>
> "Oracle Internet Directory Data Management Tools" in the *Oracle Fusion Middleware User Reference for Oracle Identity Management* for more information about using the `ldapmodify` command

17

Upgrading an Oracle Virtual Directory High Availability Environment

This chapter describes how to upgrade Oracle Virtual Directory in a high availability environment.

The upgrade steps vary slightly depending on whether you are registering with a domain and the location of the domain. Refer to the following for more information:

- Upgrading Oracle Virtual Directory When Using a Local Oracle WebLogic Server Domain
- Upgrading Oracle Virtual Directory When Using a Remote Oracle WebLogic Server Domain or No Domain

17.1 Understanding the Oracle Virtual Directory High Availability Upgrade

Before you begin using the procedures in this chapter, note the following.

Assumptions About the Active-Active Oracle Virtual Directory Upgrade

This chapter describes how to upgrade Oracle Virtual Directory in an active-active high-availability environment.

In this type of high availability environment, you upgrade Oracle Virtual Directory on two independent hosts. In this example, the two hosts are identified as IDMHOST1 and IDMHOST2.

The procedures included here assume that Oracle Virtual Directory is the only component being upgraded in the Oracle Application Server 10*g* topology and that the Oracle Virtual Directory 10*g* instance and the Oracle Virtual Directory 11*g* instance are on the same host.

Upgrading Oracle Virtual Directory With and Without an Oracle WebLogic Server Domain

In Oracle Fusion Middleware 11*g*, you can optionally register Oracle Virtual Directory with an Oracle WebLogic Server domain. However, if you want to manage Oracle Virtual Directory with Oracle Enterprise Manager Fusion Middleware Control, then you must register the Oracle Virtual Directory instance with a domain.

Further, you can register Oracle Virtual Directory with a local or remote Oracle WebLogic Server domain. The registration can be completed during the upgrade or as a post-upgrade step.

17.2 Upgrading Oracle Virtual Directory When Using a Local Oracle WebLogic Server Domain

The following procedure describes how to upgrade Oracle Virtual Directory in a high availability environment when you are planning to create a new, local Oracle WebLogic Server domain as part of the Oracle Virtual Directory installation and upgrade process.

In this scenario, you create an Oracle WebLogic Server domain on IDMHOST1 along with the first Oracle Virtual Directory instance. Then, you install and configure the second Oracle Virtual Directory instance on IDMHOST2 and register the second Oracle Virtual Directory instance with the domain on IDMHOST1.

To upgrade Oracle Virtual Directory in this scenarios, refer to the following tasks:

- Task 1: On IDMHOST1, Optionally Install Oracle WebLogic Server and Create the Middleware Home

- Task 2: On IDMHOST1, Install and Configure the Oracle Virtual Directory 11g Release 1 (11.1.1.6.0)

- Task 3: On IDMHOST1, Upgrade the Oracle Virtual Directory Instance to 11g

- Task 4: On IDMHOST2, Install and Configure the Oracle Virtual Directory 11g Release 1 (11.1.1.6.0)

- Task 5: On IDMHOST2, Upgrade the Second Oracle Virtual Directory Instance

- Task 6: On IDMHOST2, Register the Second Oracle Virtual Directory Instance with the Domain on IDMHOST1

- Task 7: On IDMHOST1 and IDMHOST2, Import the Oracle Virtual Directory Listener keystore Certificates

17.2.1 Task 1: On IDMHOST1, Optionally Install Oracle WebLogic Server and Create the Middleware Home

If you want to associate the upgraded Oracle Virtual Directory instances with Oracle WebLogic Server, you must first install Oracle WebLogic Server and create the Middleware home.

For information on installing the Oracle WebLogic Server, see "Preparing for Installation" and "Running the Installation Program in Graphical Mode" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

When you install Oracle WebLogic Server, make a note of the complete path to the Middleware home. You will need this information later in the upgrade procedure.

17.2.2 Task 2: On IDMHOST1, Install and Configure the Oracle Virtual Directory 11*g* Release 1 (11.1.1.6.0)

To install and configure Oracle Virtual Directory 11*g* on IDMHOST1, refer to the chapter "Installing and Configuring Oracle Identity Management (11.1.1.6.0)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

For complete instructions on configuring Oracle Virtual Directory, see the "Configuring Oracle Virtual Directory (OVD)" chapter in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*. For more information, see the "Creating a WebLogic Domain in Graphical Mode" topic in the *Oracle Fusion Middleware Creating Domains Using the Configuration Wizard* guide.

17.2.3 Task 3: On IDMHOST1, Upgrade the Oracle Virtual Directory Instance to 11*g*

Use the following procedure to upgrade the Oracle Virtual Directory instance to 11*g*:

1. Change directory the *ORACLE_HOME*/bin directory of the Oracle Fusion Middleware installation.

2. Enter the following command to start the Upgrade Assistant.

    On UNIX system:

    `./ua`

    On Windows systems:

    `ua.bat`

    The Upgrade Assistant displays the Welcome screen.

3. Refer to Table 17–1 for instructions on how to respond to each Upgrade Assistant screen.

Table 17–1   Summary of Upgrade Screens When Upgrading Oracle Virtual Directory for High Availability

Screen	Instructions
Welcome	Click **Next**.
Specify Operation	Select Upgrade Identity Management Instance. Click **Next**.
Specify Source Home	Select the 10*g* Release 2 (10.1.2) or 10*g* (10.1.4) source Oracle home. If the Oracle home you want to upgrade does not appear in the drop-down lists, see "Source Oracle Home Not Listed by OracleAS Upgrade Assistant" in the *Oracle Fusion Middleware Upgrade Planning Guide*.
Specify Destination Instance	Enter the complete path to the 11*g* Oracle instance, or click **Browse** to locate the instance directory.
Specify WebLogic Server	This screen appears only if you chose to associate the Oracle Virtual Directory 11*g* instance with Oracle WebLogic Server during the Oracle Virtual Directory installation. If you selected to install Oracle Virtual Directory without an Oracle WebLogic Server domain, then this screen does not appear. Enter the host and Administration Server port for the Oracle WebLogic Server you configured in Section 17.2.1, "Task 1: On IDMHOST1, Optionally Install Oracle WebLogic Server and Create the Middleware Home".
Specify Upgrade Options	Select **Use source Oracle Home ports in destination**. Select **Start destination components after upgrade**. Click **Next**.
Examining Components	Click **Next**.
Summary	Click **Upgrade** to proceed with the upgrade process.
Upgrade Progress	Monitor the upgrade progress until the Upgrade Complete screen appears.
Upgrade Complete	Click **Close**.

4. Verify the upgraded Oracle Virtual Directory instance using the following OPMN command:

    ORACLE_INSTANCE/bin/opmnctl status

    You should see output similar to the following:

```
Processes in Instance: asinst_1
-------------------------+-------------------+---------+---------
ias-component            | process-type      |     pid | status
-------------------------+-------------------+---------+---------
ovd1                     | OVD               |   22091 | Alive
EMAGENT                  | EMAGENT           |       0 | NONE
```

5. Update the NonJ2EEManagement application installed on the WebLogic Server:

   UNIX:

   ```
   INSTANCE_HOME/bin/opmnctl redeploy
   ```

   Windows:

   ```
   INSTANCE_HOME\bin\opmnctl redeploy
   ```

6. Re-register the instance so that component property information (such as component version) are updated:

   UNIX:

   ```
   INSTANCE_HOME/bin/opmnctl unregisterinstance
   INSTANCE_HOME/bin/opmnctl registerinstance
   ```

   Windows:

   ```
   INSTANCE_HOME\bin\opmnctl unregisterinstance
   INSTANCE_HOME\bin\opmnctl registerinstance
   ```

17.2.4 Task 4: On IDMHOST2, Install and Configure the Oracle Virtual Directory 11*g* Release 1 (11.1.1.6.0)

To install and configure Oracle Virtual Directory 11*g* on IDMHOST2, refer to the chapter "Installing and Configuring Oracle Identity Management (11.1.1.6.0)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

Use the Oracle Fusion Middleware Configuration Wizard to configure Oracle Virtual Directory. For more information, see the "Creating a WebLogic Domain in Graphical Mode" topic in the *Oracle Fusion Middleware Creating Domains Using the Configuration Wizard* guide. For more information, see the "Creating a WebLogic Domain in Graphical Mode" topic in the *Oracle Fusion Middleware Creating Domains Using the Configuration Wizard* guide.

17.2.5 Task 5: On IDMHOST2, Upgrade the Second Oracle Virtual Directory Instance

Use the following procedure to upgrade the Oracle Virtual Directory instance to 11*g*:

1. Change directory the *ORACLE_HOME*/bin directory of the Oracle Fusion Middleware installation.

2. Enter the following command to start the Upgrade Assistant.

   On UNIX system:

   ```
   ./ua
   ```

   On Windows systems:

   ```
   ua.bat
   ```

   The Upgrade Assistant displays the Welcome screen.

3. Refer to Table 17–1 for instructions on how to respond to each Upgrade Assistant screen.

4. Verify the upgraded Oracle Virtual Directory instance using the following OPMN command:

```
ORACLE_INSTANCE/bin/opmnctl status
```

You should see output similar to the following:

```
Processes in Instance: asinst_1
------------------------+-------------------+---------+---------
ias-component           | process-type      |     pid | status
------------------------+-------------------+---------+---------
ovd1                    | OVD               |   22091 | Alive
EMAGENT                 | EMAGENT           |       0 | NONE
```

17.2.6 Task 6: On IDMHOST2, Register the Second Oracle Virtual Directory Instance with the Domain on IDMHOST1

Register the upgraded Oracle Virtual Directory instance with the Oracle WebLogic Server domain you created and configured on IDMHOST1:

Use the following OPMN command:

```
ORACLE_INSTANCE/opmnctl registerinstance
        -adminHost adminHostName
        -adminPort adminServerPort
        -adminUsername DOMAIN_ADMINISTRATOR_USERNAME
        -oracleInstance ORACLE_INSTANCE
```

17.2.7 Task 7: On IDMHOST1 and IDMHOST2, Import the Oracle Virtual Directory Listener keystore Certificates

Run the following commands On IDMHOST1 and IDMHOST2 to import the Oracle Virtual Directory listener keystore certificates into the Fusion Middleware Control agent wallet:

1. Export Oracle Virtual Directory server certificate:

```
keytool -exportcert
        -keystore OVD_KEYSTORE_FILE
        -storepass passwd
        -alias OVD_SERVER_CERT_ALIAS
        -rfc
        -file OVD_SERVER_CERT_FILE
```

2. Add the Oracle Virtual Directory server certificate to Oracle Management Agent wallet:

```
ORACLE_HOME/bin/orapki wallet add
          -wallet ORACLE_INSTANCE/EMAGENT/EMAGENT/sysman/config/monwallet
          -trusted_cert
          -cert OVD_SERVER_CERT_FILE
          -pwd WALLET_PASSWD
```

For example, if you're using default values configured at installation time, you would use the following values for the variables in the above example:

Replace *OVD_KEY_STORE_FILE* with *ORACLE_ INSTANCE*/config/OVD/ovd1/keystores/keys.jks.

Replace *OVD_SERVER_CERT_ALIAS* with serverselfsigned.

Replace *passwd* with the password for the Oracle Virtual Directory administrator account.

17.3 Upgrading Oracle Virtual Directory When Using a Remote Oracle WebLogic Server Domain or No Domain

The following procedure describes how to upgrade Oracle Virtual Directory in a high availability environment in either of the following scenarios:

- When you are planning to register the Oracle Virtual Directory environment with an existing remote Oracle WebLogic Server domain (on the host other than the hosts where Oracle Virtual Directory is installed).

- When you are planning to install and configure the Oracle Virtual Directory environment in standalone mode (with no Oracle WebLogic Server domain).

This procedure assumes you either have a remote Oracle WebLogic Server domain already installed and configured on a remote host, or you have no plans to register Oracle Virtual Directory with Oracle WebLogic Server.

To upgrade Oracle Virtual Directory in these scenarios, refer to the following tasks:

- Task 1: On IDMHOST1, Install and Configure the Oracle Virtual Directory 11g Release 1 (11.1.1.6.0)

- Task 2: On IDMHOST1, Upgrade the Oracle Virtual Directory Instance to 11g

- Task 3: On IDMHOST2, Install and Configure the Oracle Virtual Directory 11g Release 1 (11.1.1.6.0)

- Task 4: On IDMHOST2, Upgrade the Second Oracle Virtual Directory Instance

- Task 5: On IDMHOST2, Optionally Register the Second Oracle Virtual Directory Instance with the Domain on WLSHOST1

- Task 6: On IDMHOST1 and IDMHOST2, Import the Oracle Virtual Directory Listener keystore Certificates

17.3.1 Task 1: On IDMHOST1, Install and Configure the Oracle Virtual Directory 11*g* Release 1 (11.1.1.6.0)

To install and configure Oracle Virtual Directory 11*g* on IDMHOST1, refer to the chapter "Installing and Configuring Oracle Identity Management (11.1.1.6.0)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

Use the Oracle Fusion Middleware Configuration Wizard to configure Oracle Virtual Directory. For more information, see the "Creating a WebLogic Domain in Graphical Mode" topic in the *Oracle Fusion Middleware Creating Domains Using the Configuration Wizard* guide. For more information, see the "Creating a WebLogic Domain in Graphical Mode" topic in the *Oracle Fusion Middleware Creating Domains Using the Configuration Wizard* guide.

17.3.2 Task 2: On IDMHOST1, Upgrade the Oracle Virtual Directory Instance to 11*g*

Use the following procedure to upgrade the Oracle Virtual Directory instance to 11*g*:

1. Change directory the *ORACLE_HOME*/bin directory of the Oracle Fusion Middleware installation.

2. Enter the following command to start the Upgrade Assistant.

   On UNIX system:

   ```
   ./ua
   ```

   On Windows systems:

   ```
   ua.bat
   ```

   The Upgrade Assistant displays the Welcome screen.

3. Refer to Table 17–1 for instructions on how to respond to each Upgrade Assistant screen.

4. Verify the upgraded Oracle Virtual Directory instance using the following OPMN command:

   ```
   ORACLE_INSTANCE/bin/opmnctl status
   ```

   You should see output similar to the following:

   ```
   Processes in Instance: asinst_1
   -------------------------+--------------------+---------+---------
   ias-component            | process-type       |     pid | status
   -------------------------+--------------------+---------+---------
   ovd1                     | OVD                |   22091 | Alive
   EMAGENT                  | EMAGENT            |       0 | NONE
   ```

17.3.3 Task 3: On IDMHOST2, Install and Configure the Oracle Virtual Directory 11*g* Release 1 (11.1.1.6.0)

To install and configure Oracle Virtual Directory 11*g* on IDMHOST2, refer to the chapter "Installing and Configuring Oracle Identity Management (11.1.1.6.0)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

Use the Oracle Fusion Middleware Configuration Wizard to configure Oracle Virtual Directory. For more information, see the "Creating a WebLogic Domain in Graphical Mode" topic in the *Oracle Fusion Middleware Creating Domains Using the Configuration Wizard* guide. For more information, see the "Creating a WebLogic Domain in Graphical Mode" topic in the *Oracle Fusion Middleware Creating Domains Using the Configuration Wizard* guide.

17.3.4 Task 4: On IDMHOST2, Upgrade the Second Oracle Virtual Directory Instance

Use the following procedure to upgrade the Oracle Virtual Directory instance to 11*g*:

1. Change directory the *ORACLE_HOME*/bin directory of the Oracle Fusion Middleware installation.

2. Enter the following command to start the Upgrade Assistant.

   On UNIX system:

   ```
   ./ua
   ```

   On Windows systems:

   ```
   ua.bat
   ```

The Upgrade Assistant displays the Welcome screen.

3. Refer to Table 17–1 for instructions on how to respond to each Upgrade Assistant screen.

4. Verify the upgraded Oracle Virtual Directory instance using the following OPMN command:

```
ORACLE_INSTANCE/bin/opmnctl status
```

You should see output similar to the following:

```
Processes in Instance: asinst_1
------------------------+-------------------+---------+---------
ias-component           | process-type      |     pid | status
------------------------+-------------------+---------+---------
ovd1                    | OVD               |   22091 | Alive
EMAGENT                 | EMAGENT           |       0 | NONE
```

17.3.5 Task 5: On IDMHOST2, Optionally Register the Second Oracle Virtual Directory Instance with the Domain on WLSHOST1

Register the upgraded Oracle Virtual Directory instance with an existing Oracle WebLogic Server domain you created and configured on WLSHOST1:

Use the following OPMN command:

```
ORACLE_INSTANCE/opmnctl registerinstance
        -adminHost adminHostName
        -adminPort adminServerPort
        -adminUsername DOMAIN_ADMINISTRATOR_USERNAME
        -oracleInstance ORACLE_INSTANCE
```

17.3.6 Task 6: On IDMHOST1 and IDMHOST2, Import the Oracle Virtual Directory Listener keystore Certificates

Run the following commands On IDMHOST1 and IDMHOST2 to import the Oracle Virtual Directory listener keystore certificates into the Fusion Middleware Control agent wallet:

1. Export Oracle Virtual Directory server certificate:

```
keytool -exportcert
        -keystore OVD_KEYSTORE_FILE
        -storepass passwd
        -alias OVD_SERVER_CERT_ALIAS
        -rfc
        -file OVD_SERVER_CERT_FILE
```

2. Add the Oracle Virtual Directory server certificate to Oracle Management Agent wallet:

```
ORACLE_HOME/bin/orapki wallet add
        -wallet ORACLE_INSTANCE/EMAGENT/EMAGENT/sysman/config/monwallet
        -trusted_cert
        -cert OVD_SERVER_CERT_FILE
        -pwd WALLET_PASSWD
```

For example, if you're using default values configured at installation time, you would use the following values for the variables in the above example:

Replace *OVD_KEY_STORE_FILE* with *ORACLE_INSTANCE*`/config/OVD/ovd1/keystores/keys.jks`.

Replace *OVD_SERVER_CERT_ALIAS* with `serverselfsigned`.

Replace *passwd* with the password for the Oracle Virtual Directory administrator account.

18

Upgrading an Oracle Identity Federation High Availability Environment

This chapter describes how to upgrade Oracle Identity Federation in a high availability environment.

This chapter contains the following sections:

- Task 1: Understand the Oracle Identity Federation High Availability Upgrade
- Task 2: Install the Oracle Identity Federation Schema in the Database
- Task 3: Install Oracle WebLogic Server and Create the Middleware Home
- Task 4: Install Oracle Identity Federation 11gRelease 1 (11.1.1.6.0)
- Task 5: Configure the Oracle WebLogic Server Domain with Only Oracle Enterprise Manager Fusion Middleware Control
- Task 6: Extend the Domain and Create the First Oracle Identity Federation 11g Oracle Instance
- Task 7: Use the Upgrade Assistant to Upgrade the First Oracle Identity Federation Oracle Instance
- Task 8: Install Oracle WebLogic Server and Create the Middleware Home on IDMHOST2
- Task 9: Deinstall the Oracle Identity Federation 10g Instance on IDMHOST2
- Task 10: Install Oracle Identity Federation 11g Release 1 (11.1.1.6.0) on the Second Instance IDMHOST2
- Task 11: Configure the Oracle WebLogic Server Domain on IDMHOST2
- Task 12: Copy the Oracle Identity Federation Application from IDMHOST1 to IDMHOST2
- Task 13: Start the Managed Server on IDMHOST2
- Task 14: Complete Post-Upgrade Procedures
- Task 15: Verify the Oracle Identity Federation High Availability Upgrade

18.1 Task 1: Understand the Oracle Identity Federation High Availability Upgrade

Refer to the following sections to prepare for the Oracle Identity Federation high availability upgrade:

- Prerequisites for Oracle Identity Federation High Availability Upgrade

-

18.1.1 Prerequisites for Oracle Identity Federation High Availability Upgrade

Before you begin this upgrade procedure, it is assumed that:

- The 10g source topology is equivalent to the 11g destination topology.

  In other words, the Oracle Identity Federation topology that you are planning to install should be similar in its design to the 10*g* environment. For example, it is assumed that you will be running the same number hosts and the same number Oracle Identity Federation instances in the 11*g* environment.

- For each Oracle Identity Federation instance you are upgrading, the target Oracle Identity Federation 11*g* Oracle Home must be on the same host as the source Oracle Identity Federation 10*g* Oracle home.

- The database that will be used to host the Oracle Identity Federation schema has been upgraded to a version supported by Oracle Fusion Middleware 11*g*.

  For more information, see "Upgrading and Preparing Your Databases" in the *Oracle Fusion Middleware Upgrade Planning Guide*.

- If you are also upgrading the associated Oracle HTTP Server, stop all processes for any additional Oracle Identity Federation 10*g* installations on other hosts, prior to beginning the upgrade process.

  For more information about upgrading the Oracle HTTP Server associated with your Oracle Identity Federation 10*g* installations, see Section 18.6.2, "About Selecting and Configuring Oracle HTTP Server with Oracle Identity Federation".

18.1.2 Conventions Used in This Chapter

The examples in this chapter assume you are upgrading two Oracle Identity Federation instances running on two separate host computers. These are referred to as IDMHOST1 and IDMHOST2.

In addition, the examples assume you have two database servers, also running two separate hosts, DBHOST1 and DBHOST2.

18.2 Task 2: Install the Oracle Identity Federation Schema in the Database

Before you can install Oracle Identity Federation 11*g* in preparation for upgrade, you must install the Oracle Identity Federation 11*g* schema in a supported database.

You use the Repository Creation Utility to create the schema and select the Oracle Identity Federation component on the Select Components screen of the Repository Creation Utility.

For more information, refer to Section 7.2, "Task 2: Use the Repository Creation Utility to Install the Oracle Identity Federation Schema in the Database".

18.3 Task 3: Install Oracle WebLogic Server and Create the Middleware Home

For information on installing the Oracle WebLogic Server, see "Preparing for Installation" and "Running the Installation Program in Graphical Mode" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

18.4 Task 4: Install Oracle Identity Federation 11*g*Release 1 (11.1.1.6.0)

To install and configure Oracle Identity Federation 11*g*, refer to the chapter "Installing and Configuring Oracle Identity Management (11.1.1.6.0)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

18.5 Task 5: Configure the Oracle WebLogic Server Domain with Only Oracle Enterprise Manager Fusion Middleware Control

Use the Oracle Fusion Middleware Configuration Wizard to configure Oracle Virtual Directory. For more information, see the "Creating a WebLogic Domain in Graphical Mode" topic in the *Oracle Fusion Middleware Creating Domains Using the Configuration Wizard* guide.

> **Note:** Make sure that the port numbers 7001 and 5556 are not in use by any service on the computer.
>
> For example, on UNIX systems, enter the following commands. If a port is not in use, no output is returned from the command:
>
> ```
> netstat -an | grep "7001"
> netstat -an | grep "5556"
> ```
>
> On the Windows operating system:
>
> ```
> netstat -an | findstr "LISTEN" | findstr "7001"
> netstat -an | findstr "LISTEN" | findstr "5556"
> ```
>
> If the ports are in use (if the command returns output identifying the port), you must free them.
>
> For example, on UNIX systems, if the port is in use by one or more services, remove the entries for ports 7001 and 5556 in the /etc/services file and restart the services, or restart the computer.

18.6 Task 6: Extend the Domain and Create the First Oracle Identity Federation 11*g* Oracle Instance

Now that you have configured an Oracle WebLogic Server domain, you can extend the domain and create the first Oracle Identity Federation component Oracle instance. Refer to the following sections for more information:

- Extending the Domain and Configuring Oracle Identity Federation
- About Selecting and Configuring Oracle HTTP Server with Oracle Identity Federation

18.6.1 Extending the Domain and Configuring Oracle Identity Federation

To extend the domain and configure Oracle Identity Federation:

1. Review the first four chapters of the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

   These chapters include important pre-installation information, such as system requirements and prerequisite tasks.

2. Make sure that the port number `7499` is not in use by any service on the computer.

On the UNIX operating system:

```
netstat -an | grep "7499"
```

On the Windows operating system:

```
netstat -an | findstr "LISTEN" | findstr "7499"
```

If the ports are in use (if the command returns output identifying the port), you must free them.

For example, on UNIX systems, if the port is in use by a service, remove the entry for port `7499` in the `/etc/services` file and restart the service, or restart the computer.

3. Locate the Oracle Identity Management CD–ROM.

Alternatively, you can download and unpack the installation kit from the Oracle Technology Network:

http://www.oracle.com/technology

4. Copy the `staticports.ini` file from the following directory on the CD–ROM, or from the directory where you downloaded and unpacked the software download, to a temporary directory:

```
Disk1/stage/Response
```

5. Edit the `staticports.ini` file that you copied to the temporary directory and assign the following custom ports:

```
[OIF]
# The OIF Server Port
OIF Server Port = 7499
```

You will need to reference the location of this file later in the installation procedure of the first Oracle Identity Federation instance.

6. Start Oracle Identity Management configuration tool by running the following command:

```
OIF_ORACLE_HOME/bin/config.sh
```

For example:

```
/u01/app/oracle/product/fmw/idm/bin/config.sh
```

7. Follow the instructions in the configuration wizard to extend the existing domain.

Refer to the following resources during the installation and configuration:

- Table 18–1, which provides information on specific instructions required when installing and configuring the software for an Oracle Identity Federation high availability upgrade.

- *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* or click **Help** for general information about the prerequisites and other prompts required during an Oracle Identity Federation installation.

8. When the installation and configuration is complete, exit from the configuration tool.

Table 18–1 Summary of the Configuration Screens When Configuring the First Oracle Identity Federation Oracle Instance

Screen	Description and Actions to Take
Welcome	Click **Next** to start configuring the Oracle Identity Federation
Select Domain	■ Select **Extend Existing Domain**. ■ Enter the host, port, and administration credentials for the domain you created in "Task 5: Configure the Oracle WebLogic Server Domain with Only Oracle Enterprise Manager Fusion Middleware Control".
Specify Installation Locations	■ The first two fields on this page are read-only. ■ In the **WebLogic Server Directory** field, enter the name and path of the `wlserver_10.3` directory inside the existing Middleware home. ■ In the **Oracle Instance Location** field, Enter the path to the location where you want to create the Oracle Instance directory. 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. ■ In the **Instance Name** field, enter `oif_inst1` to identify this as the first Oracle Identity Federation instance in the high availability topology. For more information, click **Help** or refer to the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*. For more information about the Middleware home, see "Understanding Oracle Fusion Middleware Concepts" in the *Oracle Fusion Middleware Administrator's Guide*.
Specify Email for Security Updates	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.
Configure Components	This screen identifies the components to configure during this installation and configuration session. For the purposes of this procedure: ■ Select only **Oracle Identity Federation**. Do not select any other components on this screen. Oracle Identity Federation can be configured with Oracle HTTP Server. For more information, see Section 18.6.2, "About Selecting and Configuring Oracle HTTP Server with Oracle Identity Federation" ■ Select the **Clustered** check box.
Configure Ports	Select **Specify Ports using Configuration file** and enter the full path to `staticports.ini` file that you edited and saved in the temporary directory.
Specify OIF Details	For this example, enter the following in the fields on this screen: ■ **PKCS12 Password:** Enter a security password. ■ **Confirm Password:** Enter the password again to confirm you typed it correctly. ■ **Server Id:** For this example, enter `oif_OIFDomain`.

Table 18–1 (Cont.) Summary of the Configuration Screens When Configuring the First Oracle Identity Federation Oracle Instance

Screen	Description and Actions to Take
OIF Advanced Flow Attributes	Enter the following for each field on this screen: **Authentication Type:** JAAS **User Store:** NONE **Federation Store:** NONE **User Session Store:** RDBMS (default selection, which cannot be changed for a cluster) **Message Store:** RDBMS (default selection, which cannot be changed for a cluster. **Configuration Store:** RDBMS (default selection, which cannot be changed for a cluster.

Transient Store Database Details	Enter the following information on this screen:
	■ **Connect String:** Provide the connect string to your database. If it is a RAC database, then enter each node, separated with the carot character (^). For example:
	`oifdbhost1-vip.mycompany.com:1521:oifdb1^`
	`oifdbhost2-vip.mycompany.com:1521:oifdb2@ oifdb.mycompany.com`
	■ **User Name:** Enter the name (including the prefix) for the Oracle Identity Federation schema that you created in Section 18.2, "Task 2: Install the Oracle Identity Federation Schema in the Database"
	■ **Password:** The password you entered when you created the Oracle Identity Federation schema.

Installation Summary	Review the review the choices you made. If you need to make any changes click **Back**. If you made the correct selections, click **Install**.
Installation Progress	Monitor the progress of the installation of the files onto disk.
oracleRoot.sh script dialog box	During installation on UNIX platforms, this dialog box 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.
Configuration progress	Monitor the progress of the software configuration.
Installation Complete	Click **Finish** to finish the installation and quit the installer.

18.6.2 About Selecting and Configuring Oracle HTTP Server with Oracle Identity Federation

Oracle Identity Federation requires an Oracle HTTP Server instance. However, you can choose to install and configure the Oracle HTTP Server instance on the same host as Oracle Identity Federation, or you can install it on a separate host as part of a Web tier installation.

Note the following when deciding whether or not to install Oracle HTTP Server on the same host or not:

■ If you install Oracle HTTP Server on the same host as Oracle Identity Federation, you can use the Oracle Fusion Middleware Upgrade Assistant to upgrade the Oracle HTTP Server instance at the same time you are upgrading Oracle Identity Federation.

This means that the Upgrade Assistant can then migrate all your SSL certificates, OSSO integration configuration from the source Oracle Identity Federation 10*g* source topology to the Oracle Identity Federation 11*g* destination topology.

- If you install Oracle HTTP Server on a separate host, the Upgrade Assistant will not migrate the SSL certificates and OSSO integration configuration. These artifacts will have to be migrated manually post upgrade.

18.7 Task 7: Use the Upgrade Assistant to Upgrade the First Oracle Identity Federation Oracle Instance

The Oracle Fusion Middleware Upgrade Assistant automates the upgrade of many aspects of your Oracle Application Server 10*g* environment.

The Upgrade Assistant is installed automatically into the `bin` directory of your Oracle Fusion Middleware Oracle home.

The following sections provide more information:

- Task 7a: Start the Upgrade Assistant for an Oracle Identity Federation Upgrade
- Task 7b: Upgrade Oracle Identity Federation

18.7.1 Task 7a: Start the Upgrade Assistant for an Oracle Identity Federation Upgrade

To start the Upgrade Assistant using the graphical user interface:

> **Note:** You can also use the Upgrade Assistant command-line interface to upgrade your Oracle Application Server 10*g* Oracle homes. For more information, see "Using the Upgrade Assistant Command-Line Interface" in the *Oracle Fusion Middleware Upgrade Planning Guide*.

1. Change directory the *ORACLE_HOME*/bin directory of the Oracle Fusion Middleware installation.

2. Enter the following command to start the Upgrade Assistant.

   On UNIX system:

   ```
   ./ua
   ```

   On Windows systems:

   ```
   ua.bat
   ```

   The Upgrade Assistant displays the Welcome screen as shown in Figure 18–1

Figure 18–1   Upgrade Assistant Welcome Screen

3. Click **Next** to display the Specify Operation screen (Figure 18–2).

    The options available in the Upgrade Assistant are specific to the Oracle home from which it started. When you start Upgrade Assistant from an Oracle Identity Management Oracle home, the options shown on the Specify Operation screen are the valid options for an Oracle Identity Management Oracle home.

Figure 18–2   Upgrade Assistant Specify Operation Screen for an Oracle Identity Federation Upgrade
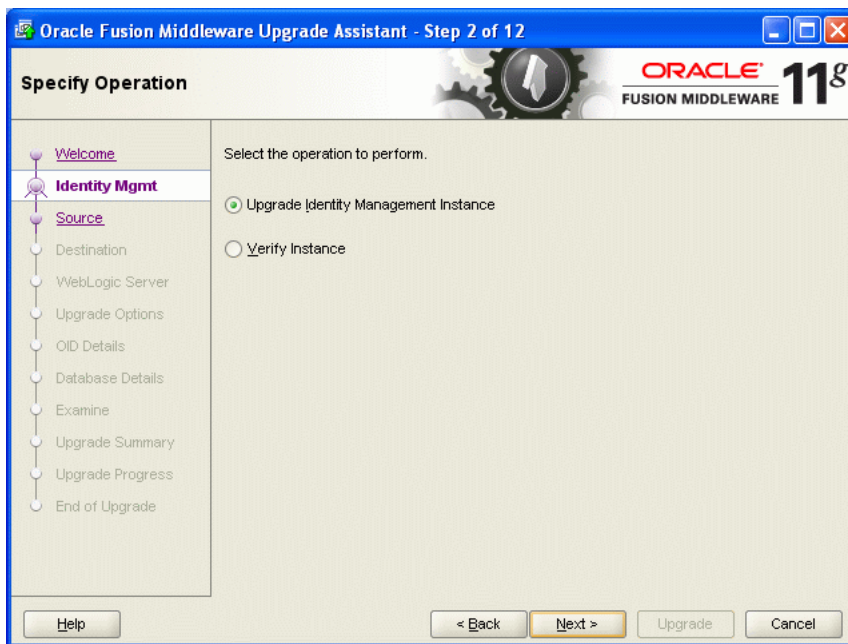
18.7.2 Task 7b: Upgrade Oracle Identity Federation

When you upgrade Oracle Identity Federation, the Upgrade Assistant upgrades the configuration files in the Oracle Identity Federation middle tier.

To upgrade Oracle Identity Federation when they reside in the same Oracle instance:

1. Start the Upgrade Assistant as described in Task 7a: Start the Upgrade Assistant for an Oracle Identity Federation Upgrade.

2. Select **Upgrade Identity Management Instance** on the Specify Operation screen (Figure 18–2).

3. Refer to Table 18–2 for a description of the Upgrade Assistant screens that require input from you during an Oracle Identity Federation upgrade.

4. After the Specify Upgrade Options screen, the Upgrade Assistant performs the following tasks and provides the progress on each task:

   - Examines the components and schemas to be upgraded and verifies that they can be upgraded successfully.

   - Provides a summary of the components to be upgraded so you can verify that Upgrade Assistant is upgrading the components and schemas you expect.

   - Provides a progress screen so you can see the status of the upgrade as it proceeds.

   - Alerts you of any errors or problems that occur during the upgrade.

     See Also: "Troubleshooting Your Upgrade" in the *Oracle Fusion Middleware Upgrade Planning Guide* for specific instructions for troubleshooting problems that occur while running the Upgrade Assistant

   - Displays the End of Upgrade screen, which confirms that the upgrade was complete.

5. Exit the Upgrade Assistant.

Table 18–2 Upgrade Assistant Screens That Require Input During an Oracle Internet Directory and Oracle Directory Integration Platform Upgrade

Upgrade Assistant Screen	Description
Specify Source Home	Select the 10*g* (10.1.4.0.1) source Oracle home.
	If the Oracle home you want to upgrade does not appear in the drop-down lists, see "Source Oracle Home Not Listed by OracleAS Upgrade Assistant" in the *Oracle Fusion Middleware Upgrade Planning Guide*.
Specify Destination Instance	Enter the complete path to the destination 11*g* Oracle home that you installed inside the middleware home. This is the Oracle home that contains the Oracle Identity Federation software.
	Alternatively, click **Browse** to select the directory.
Specify WebLogic Server	Enter the host, Administration Server port, and administration user credentials for the Oracle WebLogic Server domain you configured in Section 18.5, "Task 5: Configure the Oracle WebLogic Server Domain with Only Oracle Enterprise Manager Fusion Middleware Control".

Table 18–2   (Cont.) Upgrade Assistant Screens That Require Input During an Oracle Internet Directory and Oracle Directory Integration Platform Upgrade

Upgrade Assistant Screen	Description
Warning Dialog Box	The Upgrade Assistant displays this warning dialog box if the source Oracle home contains Oracle Application Server components that are not installed and configured in the destination Oracle instance.
	This warning appears, for example, if the source Oracle home contains an instance of Oracle HTTP Server, which is not available in the 11*g* Oracle home.
	If the information in the dialog box is accurate and you understand which components will be upgraded, click **Yes** to continue. Otherwise, click **No** and verify which components are installed and configured in each 11*g* Oracle instance.
Specify Upgrade Options	This screen offers these upgrade options:
	■ **Use source Oracle home ports in destination:** If you want to migrate the port assignments used by your Oracle Application Server 10g Oracle home to your new Oracle Fusion Middleware Oracle instance.
	Note that Oracle recommends that you always select this option when upgrading Oracle Identity Federation.
	■ **Start destination components after successful upgrade:** if you want the Upgrade Assistant to automatically start the components in the destination Oracle home after the upgrade is complete. If you do not select this option, then you will have to manually start the destination instance after the upgrade.
	For the purposes of this example, select both of these upgrade options.

18.8 Task 8: Install Oracle WebLogic Server and Create the Middleware Home on IDMHOST2

Before you can expand the Oracle WebLogic Server cluster you created on IDMHOST1 to include IDMHOST2, you must install the Oracle WebLogic Server binary files on IDMHOST2 and create Middleware home on IDMHOST2.

For information on installing the Oracle WebLogic Server, see "Preparing for Installation" and "Running the Installation Program in Graphical Mode" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

When you install Oracle WebLogic Server, make a note of the complete path to the Middleware home. You will need this information later in the upgrade procedure.

18.9 Task 9: Deinstall the Oracle Identity Federation 10*g* Instance on IDMHOST2

Before you install Oracle Identity Federation 11*g* on the second host in your Oracle Identity Federation high availability environment, Oracle recommends that you remove (deinstall) the Oracle Identity Federation 10*g* instance that is currently running on the second host.

This step is necessary to avoid port conflicts between the existing Oracle Identity Federation 10*g* instance and the new Oracle Identity Federation 11*g* instance.

For more information, see the following topics:

- Procedure for Deinstalling the Oracle Identity Federation 10g Instance
- Alternative Procedure to Avoid Port Conflicts

18.9.1 Procedure for Deinstalling the Oracle Identity Federation 10*g* Instance

For instructions on deinstalling Oracle Identity Federation 10*g*, refer to Section 5.4, "Un-installing Oracle Identity Federation" in the *Oracle Identity Federation Administrator's Guide*, which is available in the Oracle Application Server 10*g* (10.1.4.0.1) documentation library on the Oracle Technology Network (OTN):

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

18.9.2 Alternative Procedure to Avoid Port Conflicts

If deinstalling Oracle Identity Federation 10*g* is not an option for your organization, you can consider the following alternative solution, which involves modifying Oracle HTTP Server 10*g* configuration files.

To modify the Oracle HTTP Server 10*g* instance to avoid port conflicts during the Oracle Identity Federation 11*g* installation:

1. Change directory to the Oracle HTTP Server configuration directory:

   10g_ORACLE_HOME\Apache\Apache\conf\

2. Create a backup copy of the files following files in this directory:

   ```
   httpd.conf
   ssl.conf
   ```

3. Edit the file `httpd.conf`, and search for any occurrence of the HTTP Non-SSL Port that you need to reuse during the Oracle Identity Federation 11*g* installation.

4. For each occurrence, edit or remove the value from the `httpd.conf` file.

   For example, if the HTTP Non-SSL port is `7786`, remove the value, or change the value from `7786` to `77861`.

5. In a similar manner, edit the file `ssl.conf` file and search for any occurrence of the HTTP SSL Port that you need to reuse.

6. For each occurrence, edit or remove the value from the `ssl.conf` file.

18.10 Task 10: Install Oracle Identity Federation 11*g* Release 1 (11.1.1.6.0) on the Second Instance IDMHOST2

To install and configure Oracle Identity Federation 11*g* on IDMHOST2, refer to the chapter "Installing and Configuring Oracle Identity Management (11.1.1.6.0)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

18.11 Task 11: Configure the Oracle WebLogic Server Domain on IDMHOST2

Use the Oracle Fusion Middleware Configuration Wizard to configure Oracle Virtual Directory. For more information, see the "Creating a WebLogic Domain in Graphical Mode" topic in the *Oracle Fusion Middleware Creating Domains Using the Configuration Wizard* guide.

> **Note:** Make sure that the port numbers 7499 is not in use by any service on the computer.
>
> For example, on UNIX systems, enter the following commands. If a port is not in use, no output is returned from the command:
>
> ```
> netstat -an | grep "7499"
> ```
>
> On the Windows operating system:
>
> ```
> netstat -an | findstr "LISTEN" | findstr "7499"
> ```
>
> If the port is in use (if the command returns output identifying the port), you must free them.
>
> For example, on UNIX systems, if the port is in use by one or more services, remove the entries for port 7499 in the /etc/services file and restart the services, or restart the computer.

18.12 Task 12: Copy the Oracle Identity Federation Application from IDMHOST1 to IDMHOST2

The Oracle Directory Integration Platform application is deployed on IDMHOST1 as an externally staged application. The application must be copied from IDMHOST1 to OIFHOST2; otherwise the managed server on IDMHOST2 is listed in the Oracle WebLogic Server administration console as being in an "unknown" state:

1. Locate the `applications` directory in the Oracle WebLogic Server domain directory on IDMHOST1:

   ```
   MW_HOME/user_projects/domains/OIFDomain/config/fmwconfig/servers
           /wls_oif1/applications
   ```

2. Copy the `applications` directory on and its contents on IDMHOST1 to the same location in the domain directory on IDMHOST2.

   For example:

   ```
   scp -rp MW_HOME/user_projects/domains/OIFDomain/config/fmwconfig/servers
                 /wls_oif1/applications
        user@IDMHOST2:MW_HOME/user_projects/domains/OIFDomain/config/fmwconfig
                 /servers/wls_oif2/applications
   ```

18.13 Task 13: Start the Managed Server on IDMHOST2

Follow these steps to start the wls_ods2 managed server in a cluster:

1. Open a browser and navigate to the WebLogic Administration Console at:

   ```
   http://idmhost1.mycompany.com:port/console
   ```

2. Log in to the WebLogic Administration Console using the administrator credentials.

3. In the left pane of the WebLogic Administration Console, expand **Environment** and select **Clusters**.

4. Select the cluster (`cluster_oif`) containing the managed server (`wls_oif2`) you want to start.

5. Select **Control**.

6. Under Managed Server Instances in this Cluster, select the check box next to the managed server (`wls_ods2`) you want to start and click **Start**.

7. On the Server Life Cycle Assistant page, click **Yes** to confirm.

> **Note:** Node Manager starts the server on the target machine. When the Node Manager finishes its start sequence, the server's state is indicated in the **State** column in the Server Status table.

18.14 Task 14: Complete Post-Upgrade Procedures

Refer to the following sections for information about important post-upgrade Oracle Identity Federation high availability procedures:

- Configuring Routing Between Oracle Identity Federation and Oracle HTTP Server
- Configuring the Load Balancer
- Set Oracle Identity Federation Configuration Properties

18.14.1 Configuring Routing Between Oracle Identity Federation and Oracle HTTP Server

Follow the steps shown below to create a new Oracle HTTP Server instance and to enable communication between the Oracle HTTP Server instance and the Oracle Identity Federation server instance on IDMHOST1 and IDMHOST2.

When you install and configure Oracle Identity Federation, the Oracle HTTP Server software is installed in the Oracle home, but an Oracle HTTP Server instance is not configured by default:

1. Create an Oracle HTTP Server instance to configure with Oracle Identity Federation:

```
INSTANCE_HOME/bin/opmnctl createcomponent
          -componentType OHS
          -componentName ohs1
```

2. On IDMHOST2, edit the following configuration file:

```
INSTANCE_HOME/config/OHS/ohs_name/moduleconf/oif.conf
```

In this example, *ohs_name* is the name of the Oracle HTTP Server component; for example: `ohs1`

3. Uncomment and set the `WebLogicCluster` variable to reference the managed servers running the Oracle Identity Federation Server instances.

For example, if the host and port of each managed server is as follows:

```
idmhost1.mycompany.com:7499
idmhost2.mycompany.com:7499
```

Then update the file to contain the following entry:

```
<Location /fed>
    WebLogicCluster idmhost1.mycompany.com:7499,idmhost2.mycompany.com:7499
    SetHandler weblogic-handler
</Location>
```

4. Save the `oif.conf` file.

5. Start the Oracle HTTP Server as shown below:

   ```
   INSTANCE_HOME /bin/opmnctl startproc process-type=OHS
   ```

18.14.2 Configuring the Load Balancer

Oracle Identity Federation topologies deployed in high availability configurations are front-ended by an external load balancer, which provides load balancing of the HTTP requests between the various OIF instances.

After upgrading the Oracle Identity Federation high availability environment, configure your load balancer to listen to the Oracle HTTP Server instances on IDMHOST1 and IDMHOST2.

Refer to the documentation provided by the load balancer vendor to accomplish this task.

18.14.3 Set Oracle Identity Federation Configuration Properties

Follow the steps below to enable the Oracle Identity Federation instances on IDMHOST1 and IDMHOST2 to recognize the Load Balancer Virtual Hostname.

Use Oracle Enterprise Manager Fusion Middleware Control to complete this task.

1. Log in to Fusion Middleware Control and locate the Oracle Identity Federation instance home page.

2. Modify the server properties as follows:

   a. From the **Oracle Identity Federation** menu, select **Administration**, and then **Server Properties**.

   b. Change the **Host** field to reflect the virtual host name of the load balancer.

   c. Change the **Port** and **SSL Enabled**, as well as the **SOAP Port** and **SSL Enabled** options to reflect the ports used by the load balancer.

   d. Save the changes.

3. Modify the Identity Provider properties as follows:

   a. From the **Administration** menu, select **Identity Provider**.

   b. In the Provider ID field, enter the URL for the load balancer virtual host name and port.

      For example:

      ```
      http://load_balancer_host:port
      ```

4. Modify the Service Provider properties as follows:

   a. From the **Administration** menu, select **Service Provider**.

   b. In the **Provider ID** field, enter the URL for the load balancer virtual host name and port.

      For example:

      ```
      http://load_balancer_host:port
      ```

5. Repeat Steps 2 through 4 for the subsequent Oracle Identity Federation instances in the high availability environment.

6. Because the Oracle Identity Federation metadata will have changed, redistribute the metadata to any remote partners to notify them of the configuration changes you just made.

18.14.4 Additional High Availability Tasks Associated

In addition to this tasks listed in this section, be sure to review any additional tasks required to configure the Oracle Identity Federation 11*g* high availability environment.

In particular, refer to these sections of the *Oracle Fusion Middleware High Availability Guide*:

- "Configuring Oracle HTTP Server for Oracle Directory Services Manager High Availability"
- "Configure Oracle HTTP Server"
- "Oracle Identity Federation Configuration"

18.15 Task 15: Verify the Oracle Identity Federation High Availability Upgrade

Follow the steps below to validate the upgraded Oracle Identity Federation high availability upgrade:

1. Use a web browser to access the URL's shown below:

   ```
   http://<LoadBalancerHost>:<LoadBalancerPort>/fed/sp/metadata
   http://<LoadBalancerHost>:<LoadBalancerPort>/fed/idp/metadata
   ```

2. Follow the instructions in the following sections of the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation* to import metadata from the SP into the IdP and the IDP metadata into the SP:

   - "Obtain Server Metadata"
   - "Add Trusted Providers"

3. Go to the following URL and do a Single Sign-On operation:

   ```
   http://Loadbalancer_SP_Host:Loadbalancer SP_port/fed/user/testspsso
   ```

4. During the upgrade, the single sign-on configurations from your 10*g* environment should have been migrated to the upgraded instances. As a result, you should be able to access those URLs, if the upgrade process completed successfully.

Index