Oracle® Fusion Middleware

Identity Management Provisioning Guide (Oracle Fusion Applications Edition)

11*g* Release 7 (11.1.7)

E41444-02

September 2013

Documentation for system administrators that describes how to use the Identity Management Provisioning Wizard and related tools to provision Identity Management for Oracle Fusion Applications.

ORACLE

Oracle Fusion Middleware Identity Management Provisioning Guide (Oracle Fusion Applications Edition), 11*g* Release 7 (11.1.7)

E41444-02

Primary Author: Ellen Desmond (Writer)

Contributors: Kopal Sinha, Jatan Rajvanshi, Anupama Pundpal, Michael Rhys

Contents

5 Performing Oracle Identity Management Provisioning

6 Post Provisioning Tasks

7 Troubleshooting Identity Management Provisioning

Preface

This guide describes how to use the new Identity Management Provisioning Wizard and related tools.

Audience

This document is intended for administrators who must configure Oracle Identity Management for Oracle Fusion Applications. For more details about who should use this guide, see Section 1.2, "Who Should Use this Guide."

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/pls/topic/lookup?ctx=acc&id=info or visit
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documents

For more information, see the following documents in the Oracle Fusion Applications Release 11.1.7 documentation set or in the Oracle Fusion Middleware Release 11.1.1.7 documentation set:

- *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management (Oracle Fusion Applications Edition)*
- *Oracle Fusion Applications Installation Guide*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*
- *Oracle Fusion Middleware Administrator's Guide for Oracle SOA Suite and Oracle Business Process Management Suite*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*

- *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager with Oracle Security Token Service*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*
- *Oracle Fusion Middleware Administrator's Guide for Oracle HTTP Server*
- *Oracle Fusion Middleware Installing WebGates for Oracle Access Manager*

Conventions

The following text conventions are used in this document:

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

1

Introduction to Identity Management Provisioning

This chapter provides an introduction to Identity Management Provisioning.

This chapter contains the following sections:

1.1 Introduction to Administration for Identity Management Provisioning

The Identity Management Provisioning Wizard and related tools were developed to automate Identity Management Provisioning and reduce the time required to configure Identity Management for Oracle Fusion Applications.

1.2 Who Should Use this Guide

You should use this guide if you are configuring a simple, single host Oracle Identity Management topology. This Identity Management configuration is a prerequisite for installing Oracle Fusion Applications, as described in the *Oracle Fusion Applications Installation Guide*.

If you are configuring a multiple host topology, such as those described in "Introduction to the Enterprise Deployment Reference Topologies" in *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management (Oracle Fusion Applications Edition)*, and your hosts are running Linux, you should use the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management (Oracle Fusion Applications Edition)* instead of the current guide and *Oracle Fusion Applications Installation Guide*.

If you are configuring a multiple host topology, but you are using a platform other than Linux, you should use *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management (Oracle Fusion Applications Edition)*, but you should refer to the current guide for non-Linux platform-specific information.

Also see the *Technical Release Notes* for Oracle Fusion Applications 11g Release 7 (11.1.7) for more information.

1.3 Understanding Identity Management Provisioning Concepts

Oracle Identity Management consists of a number of products, which can be used either individually or collectively. The section "Oracle Identity Management" in *Oracle Fusion Applications Installation Guide* lists the Identity Management products used with Oracle Fusion Applications. The section "Installing Oracle Identity Management Components" in *Oracle Fusion Applications Installation Guide* describes how to install them.

In previous releases, configuring the individual Identity Management products and integrating them to create an Identity Management environment required you to perform several steps, using several consoles and commands. In the current release, these steps are automated.

1.4 Basic Tasks for Identity Management Provisioning

Before you attempt to perform Identity Management Provisioning, there are a number of preliminary tasks you must perform. These are described in Chapter 2, "Installing the Software" and Chapter 3, "Preparing for Identity Management Provisioning."

The Identity Management Provisioning process itself consists of two tasks:

1. Running the Identity Management Provisioning Wizard, a graphical user interface that uses an interview process to gather information about the environment and store it in a Provisioning Response file. This task is described in Chapter 4, "Creating a Provisioning Profile."
2. Executing command-line tools to set up the environment on the selected host machines. In many cases, you can monitor the progress of the command-line tools by using the wizard. This task is described in Chapter 5, "Performing Oracle Identity Management Provisioning."

After provisioning, perform the tasks in Chapter 6, "Post Provisioning Tasks."

2

Installing the Software

This chapter describes how to install the software required for Identity Management Provisioning.

This chapter contains the following topics:

2.1 Installing the Identity Management Provisioning Tools

The Identity Management Provisioning tools share a repository with the Oracle Fusion Applications Provisioning tools.

The software required by Oracle Identity Management is located in the Oracle Fusion Applications repository. If you have not already done so then you need to create an Oracle Fusion Applications provisioning repository as described in "Creating the Provisioning Repository" in *Oracle Fusion Applications Installation Guide*.

2.2 Verifying Java and Ant

Make sure that your Provisioning Repository contains Java and Ant. Java should reside in a directory called `jdk6`. Ant should reside in a directory called `ant`. The paths should be:

On UNIX

repository_location`/jdk6`
repository_location`/provisioning/ant`

On Windows

repository_location`\jdk6`
repository_location`\provisioning\ant`

2.3 Installing the Database

Install and configure the Oracle Database, as described in "RCU System and Database Requirements" in *Oracle Fusion Middleware Repository Creation Utility User's Guide*. Use Oracle Database 11.2.0.3.0 or newer.

2.4 Preparing the Database for Repository Creation Utility (RCU)

To prepare the Oracle Database, follow the instructions in the section "RCU Requirements for Oracle Databases" in the *Oracle Fusion Middleware System Requirements and Specifications*.

On UNIX, execute the following commands to create XATRANS Views:

```
cd $ORACLE_HOME/rdbms/admin
sqlplus / as sysdba
@xaview.sql
```

On Windows, the commands are:

```
cd %ORACLE_HOME%\rdbms\admin
sqlplus / as sysdba
@xaview.sql
```

2.5 Running Oracle Identity Management Repository Creation Utility (Oracle Identity Management RCU)

Unzip the RCU zip file *repository_location*`/installers/fmw_rcu/linux/rcuHome.zip` (on Linux) or *repository_location*`/installers/fmw_rcu/windows/rcuHome.zip` (on Windows) to:

repository_location`/installers/rcu`

where *repository_location* is the Oracle Fusion Applications provisioning repository, as described in "Creating the Provisioning Repository" in *Oracle Fusion Applications Installation Guide*.

Use the Identity Management version of RCU, which now exists in that directory.

The Identity Management RCU needs to be set up for the following components: ODS, OIF, OIM, OAM. You must use FA as the prefix for the schema names.

Optionally, you can use two database instances for Identity Management. If you do this, install ODS in one database instance and other components in the second database instance

You must select a single password for all the schema while running the RCU.

> **Note:** The Oracle Identity Management RCU is available only on Windows and Linux platforms. For other platforms, such as Solaris and AIX, you must install and run the Oracle Identity Management RCU from a Windows or Linux machine.

For more information about RCU, see *Oracle Fusion Middleware Repository Creation Utility User's Guide*.

2.6 Installing the Identity Management Lifecycle Tools

The Identity Management Provisioning Wizard is a component of the Identity Management Lifecycle Tools, which also includes the Identity Management Patching Framework. You must install the tools by running an installer, which is located in the provisioning repository. In a multi-host environment, the Identity Management Provisioning Wizard must be visible to each host in the topology. The wizard is only required during the provisioning process, and can be removed after provisioning.

The installation script for the Identity Management Lifecycle Tools resides in the directory:

repository_location/installers/idmlcm/idmlcm/Disk1

where *repository_location* is the Oracle Fusion Applications provisioning repository, as described in "Creating the Provisioning Repository" in *Oracle Fusion Applications Installation Guide*

To begin installing the tools, change to that directory and start the script.

On UNIX:

```
cd repository_location/installers/idmlcm/idmlcm/Disk1
./runInstaller -jreLoc repository_location/jdk6
```

On Windows:

```
cd repository_location\installers\idmlcm\idmlcm\Disk1
setup.exe -jreLoc repository_location\jdk6
```

Then proceed as follows:

1. On the Welcome page, click **Next**.
2. If you are running on a UNIX platform, and you have not previously installed an Oracle product on this host, you might be presented with the Specify Inventory Directory page, which prompts you for the location of the **Inventory Directory**. This directory is used to keep track of all Oracle products installed on this host. If you see this page, proceed as follows:

   In the **Operating System Group ID** field, select the group whose members you want to grant access to the inventory directory. All members of this group can install products on this host. Click **OK** to continue.

   The **Inventory Location Confirmation** dialog prompts you to run the *inventory_directory*/createCentralInventory.sh script as root to create the /etc/oraInst.loc file. This file is a pointer to the central inventory and must be present for silent installations. It contains two lines:

   ```
   inventory_loc=path_to_central_inventory
   ```

   ```
   inst_group=install_group
   ```

   The standard location for this file is /etc/oraInst.loc, but it can be created anywhere. If you create it in a directory other than /etc, you must include the -invPtrLoc argument and enter the location of the inventory when you run the Identity ManagementProvisioningWizard or the runIdentity ManagementProvisioning script.

   If you do not have root access on this host but want to continue with the provisioning, select **Continue installation with local inventory**.

   Click **OK** to continue.

3. On the Prerequisite Checks page, verify that checks complete successfully, then click **Next**.
4. On the Specify Install Location page, enter the following information:
   a. **Oracle Middleware Home** - This is the parent directory of the directory where the Identity Management Provisioning Wizard will be installed. In a multi-host Identity Management environment, this must be on shared storage. for example:

      ```
      /u01/tools
      ```

   b. **Oracle Home Directory** - This is a subdirectory of the Oracle Middleware Home directory where the wizard will be installed. For example:

      ```
      idmlcm
      ```

      In the current guide, this subdirectory is referred to as *IDMLCM_HOME*.

   Click **Next**.
5. On the Installation Summary page, click **Install**.
6. On the Installation Progress page, click **Next**.
7. On the Installation Complete page, click **Finish**.

3

Preparing for Identity Management Provisioning

This chapter describes tasks you must perform before running the Identity Management Provisioning Wizard. Many of these tasks are platform-specific.

This chapter contains the following sections:

3.1 Ensuring Software Install Location is 45 Characters or Fewer

When planning the Identity Management deployment, ensure that the **Software Installation Location** directory path is 45 characters or fewer in length. You specify this directory on the Installation and Configuration page when you create the provisioning profile. A longer pathname can cause errors during Identity Management provisioning. See Section 7.2.2, "Null Error Occurs When WebLogic Patches Are Applied."

3.2 Configuring Kernel Parameters (UNIX)

The kernel parameter and shell limit values shown below are recommended values only. For production database systems, Oracle recommends that you tune these values to optimize the performance of the system. See your operating system documentation for more information about tuning kernel parameters.

Kernel parameters must be set to a minimum of those below on all nodes in the cluster.

The values in the following table are the current Linux recommendations. For more information, refer to *Oracle Fusion Middleware System Requirements and Specifications*.

If you are deploying a database onto the host, you might need to modify additional kernel parameters. Refer to the 11*g* Release 2 *Oracle Grid Infrastructure Installation Guide* for your platform.

Table 3–1 UNIX Kernel Parameters

Parameter	Value
kernel.sem	256 32000 100 142
kernel.shmmax	4294967295

To set these parameters:

1. Log in as `root` and add or amend the entries in the file `/etc/sysctl.conf`.
2. Save the file.
3. Activate the changes by issuing the command:

```
/sbin/sysctl -p
```

3.3 Configuring Kernel Parameters (AIX Only)

You must set the following AIX Kernel parameters before starting Identity Management Provisioning:

```
no -o tcp_recvspace=262144
no -o tcp_sendspace=262144
no -o udp_recvspace=262144
no -o udp_sendspace=262144
no -o rfc1323=1
no -o sb_max=4194304
/usr/sbin/no -o tcp_timewait=1
```

3.4 Setting the Open File Limit (UNIX)

On all UNIX operating systems, the minimum Open File Limit should be 150000.

> **Note:** The following examples are for Linux operating systems. Consult your operating system documentation to determine the commands to be used on your system.

You can see how many files are open with the following command:

```
/usr/sbin/lsof | wc -l
```

To check your open file limits, use the commands below.

C shell:

```
limit descriptors
```

Bash:

```
ulimit -n
```

3.5 Setting Shell Limits (UNIX)

To change the shell limits, login as `root` and edit the `/etc/security/limits.conf` file.

Add the following lines:

```
* soft  nofile  150000
* hard  nofile  150000
* soft  nproc   16384
* hard  nproc   16384
```

If you are installing on Oracle Linux Server Release 6, also edit the /etc/security/limits.d/90-nproc.conf file, and ensure it has the following line:

```
* soft nproc 16384
```

After editing the files, reboot the machine.

See the *Oracle Fusion Middleware System Requirements and Specifications* for the latest suggested value.

3.6 Setting Up Required User (Windows)

Proceed as follows:

1. Create a `domain\user` that is part of the Administrators group.
2. Log in as the user that you created.
3. Run `secpol.msc` (security policy). To do this, click **Start > Run**, type `secpol.msc`, and press Enter. Add the `domain\user` that you created to **Log on as service** under the Local Policies, User Rights Assignment option.
4. Reboot the machine.

3.7 Enabling IPV4 and Disabling IPV6 (Windows)

Ensure that IPV4 is enabled and IPV6 is disabled, as follows:

To enable the IPV4 address, execute the command:

```
netsh interface ipv4 install
```

To disable the IPV6 address, execute the command:

```
netsh interface ipv6 uninstall
```

A method for completely disabling IPV6 on a Windows host is documented at:

http://support.microsoft.com/kb/929852

To list all the IP addresses for verification, execute the command:

```
netsh interface ipv4 show ipaddresses
netsh interface ipv6 show ipaddresses
```

3.8 Installing OpenSSL (Windows)

The `openssl` command is not available by default on Microsoft Windows.

You must install OpenSSL on the Windows machine. See:
http://www.openssl.org

The directory containing the binary `openssl` must be in the `PATH` environment variable.

3.9 Enabling Unicode Support

Your operating system configuration can influence the behavior of characters supported by Oracle Fusion Middleware products.

On UNIX operating systems, Oracle highly recommends that you enable Unicode support by setting the `LANG` and `LC_ALL` environment variables to a locale with the UTF-8 character set. This enables the operating system to process any character in Unicode. Oracle SOA Suite technologies, for example, are based on Unicode.

If the operating system is configured to use a non-UTF-8 encoding, Oracle SOA Suite components may function in an unexpected way. For example, a non-ASCII file name might make the file inaccessible and cause an error. Oracle does not support problems caused by operating system constraints.

4 Creating a Provisioning Profile

This chapter describes how to create a provisioning profile using the Identity Management Provisioning Wizard.

This chapter contains the following sections:

- Section 4.1, "Introduction to Creating a Provisioning Profile"
- Section 4.2, "Creating a Provisioning Profile"

4.1 Introduction to Creating a Provisioning Profile

Before you can perform provisioning, you must provide information about your topology to the Identity Management Provisioning Wizard. Once you have provided all the necessary input, the wizard will create a provisioning file called `provisioning.rsp` that you use to perform the provisioning operation.

> **Note:** Even if you select a single node install, the screens in the Identity Management Provisioning Wizard show multinode items such as Virtual Host Configuration and Load Balancer Configuration. Ignore the unused fields and click **Next**.

4.2 Creating a Provisioning Profile

Before running the provisioning tool, set the following environment variables:

- Set `ANT_HOME` to: *`repository_location`*`/provisioning/ant`
- Set `JAVA_HOME` to: *`repository_location`*`/jdk6`

To start the Identity Management Provisioning Wizard, execute the following commands from: *`IDMLCM_HOME`*`/provisioning/bin`, where *`IDMLCM_HOME`* is the place where you installed the Oracle Home Directory for Identity Management, using the installation script for the Identity Management Provisioning Wizard and Identity Management Patching Tools, as described in Section 2.6, "Installing the Identity Management Lifecycle Tools."

On Linux or UNIX, issue the command:

```
./idmProvisioningWizard.sh
```

On Windows, issue the command

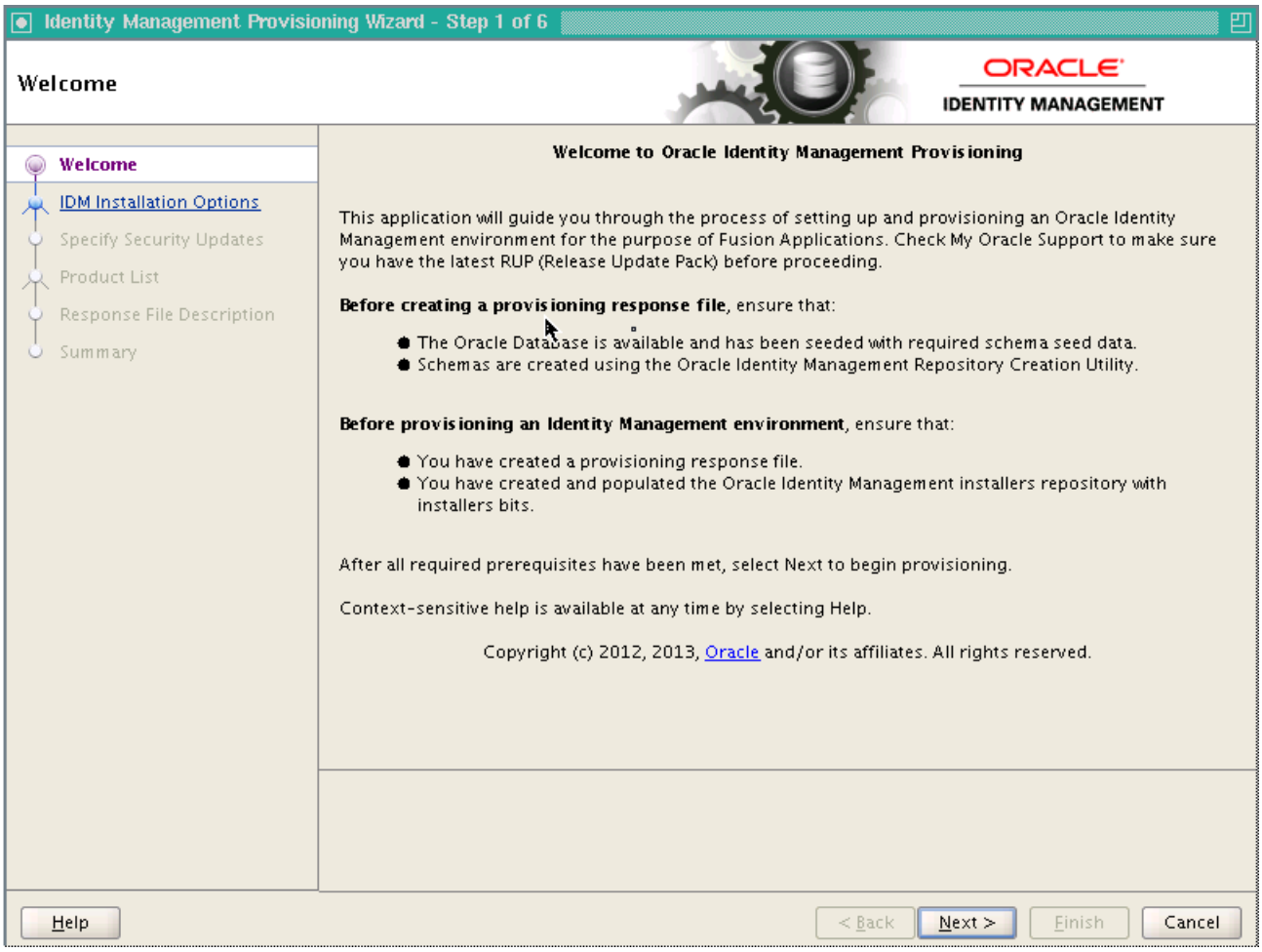
```
idmProvisioningWizard.bat
```

When the wizard starts, proceed as described in the following sections:

4.2.1 Welcome Page

Use the Welcome Page to learn more about the wizard, including some prerequisites for using it.

The Welcome Page provides a brief overview of the wizard and lists some requirements that must be met.



Click **Next** to continue.

4.2.2 Specify Inventory Directory

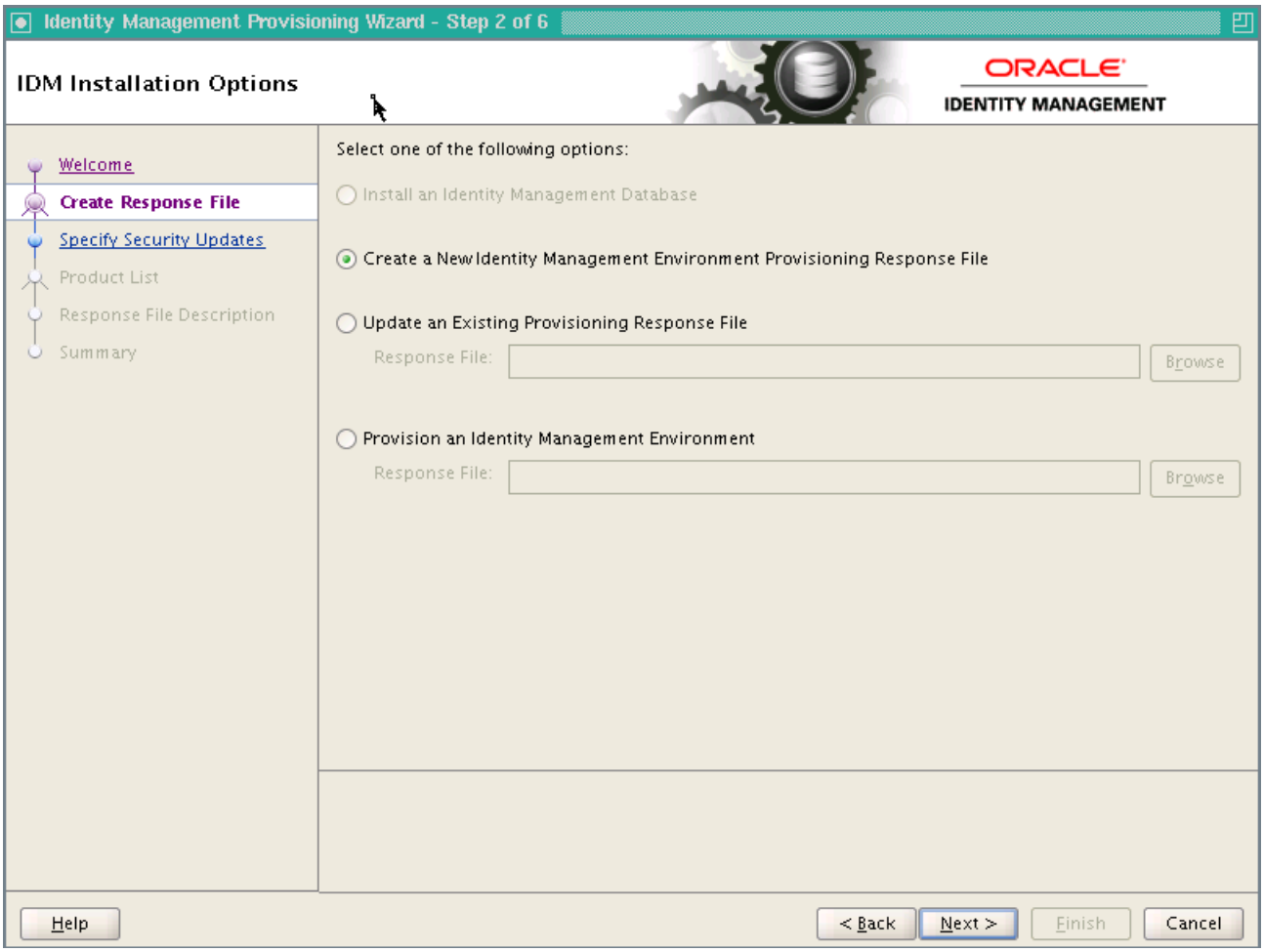
If you are presented with the Specify Inventory Directory page, proceed as described in Step 2 in Section 2.6, "Installing the Identity Management Lifecycle Tools."

Click **OK** to continue.

4.2.3 Identity Management Installation Options Page

Select **Create a New Identity Management Environment Provisioning Response File** if you are creating a response file for the first time.

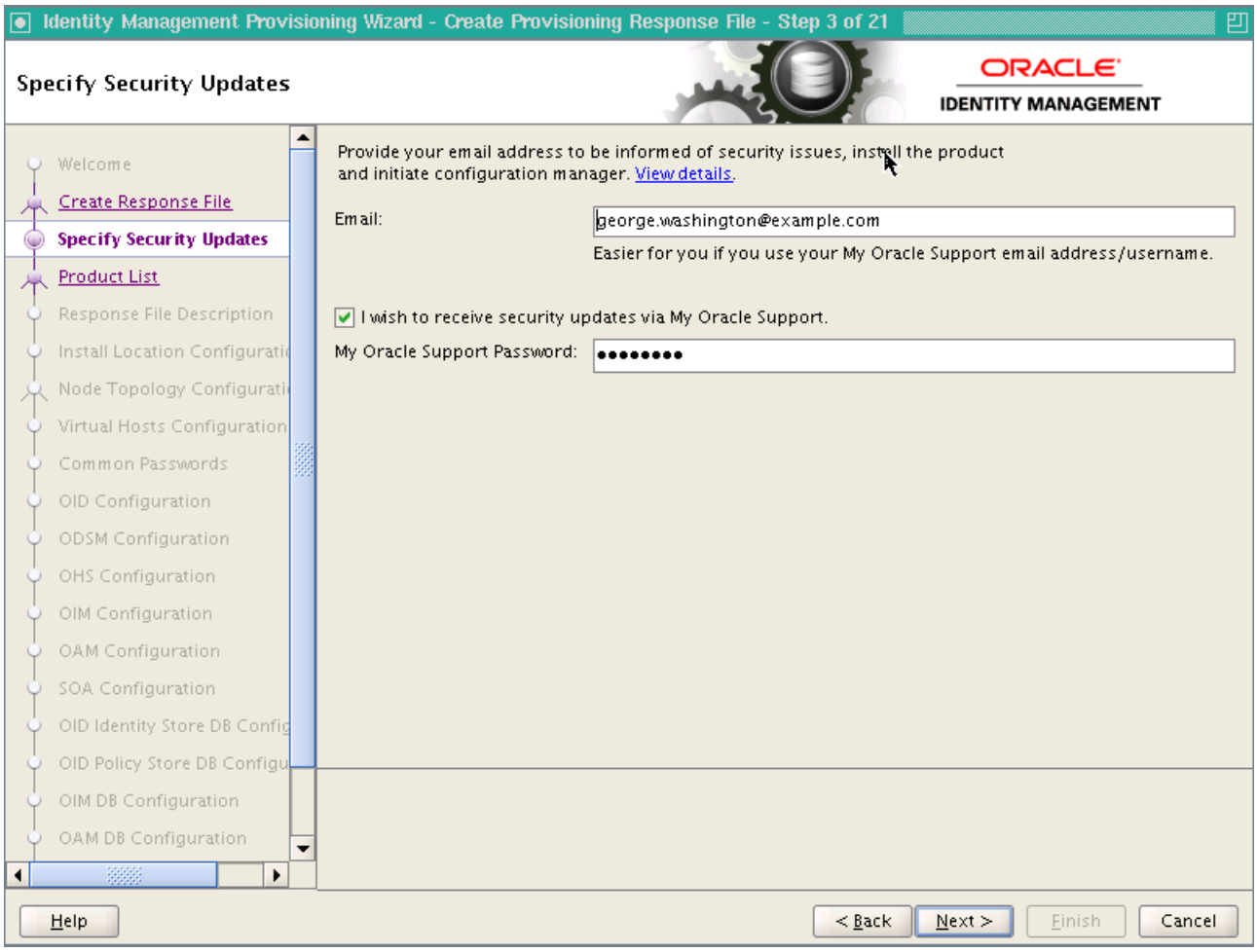
Update an Existing Identity Management Environment Provisioning Response File is not supported.



Click **Next** to continue.

4.2.4 Specify Security Updates Page

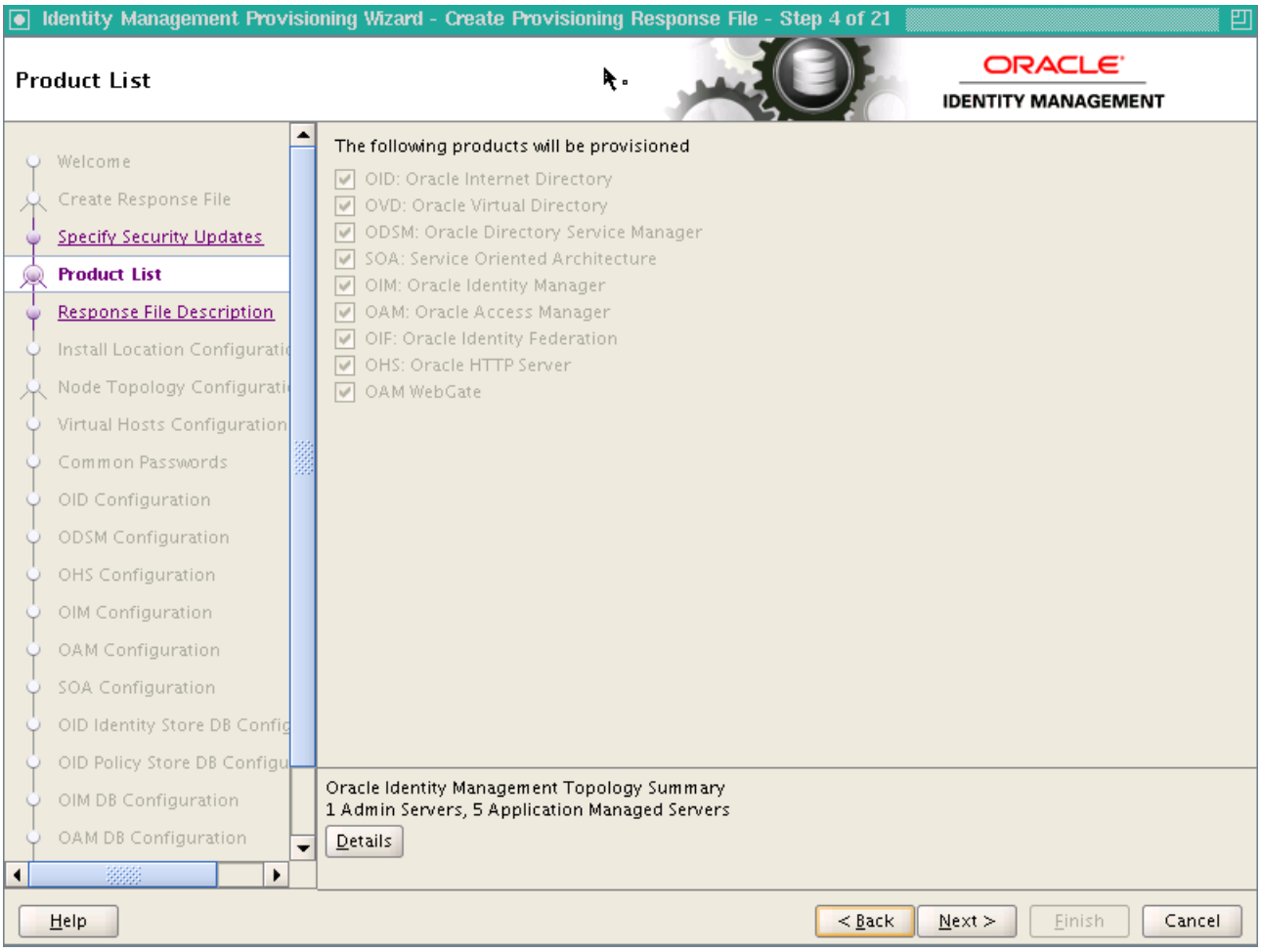
The check box should be unchecked, as this feature is not supported.



Click **Next** to continue.

4.2.5 Product List Page

The Product List Page is purely informational. It displays the list of products that are installed and configured by the Identity Management Provisioning Wizard.

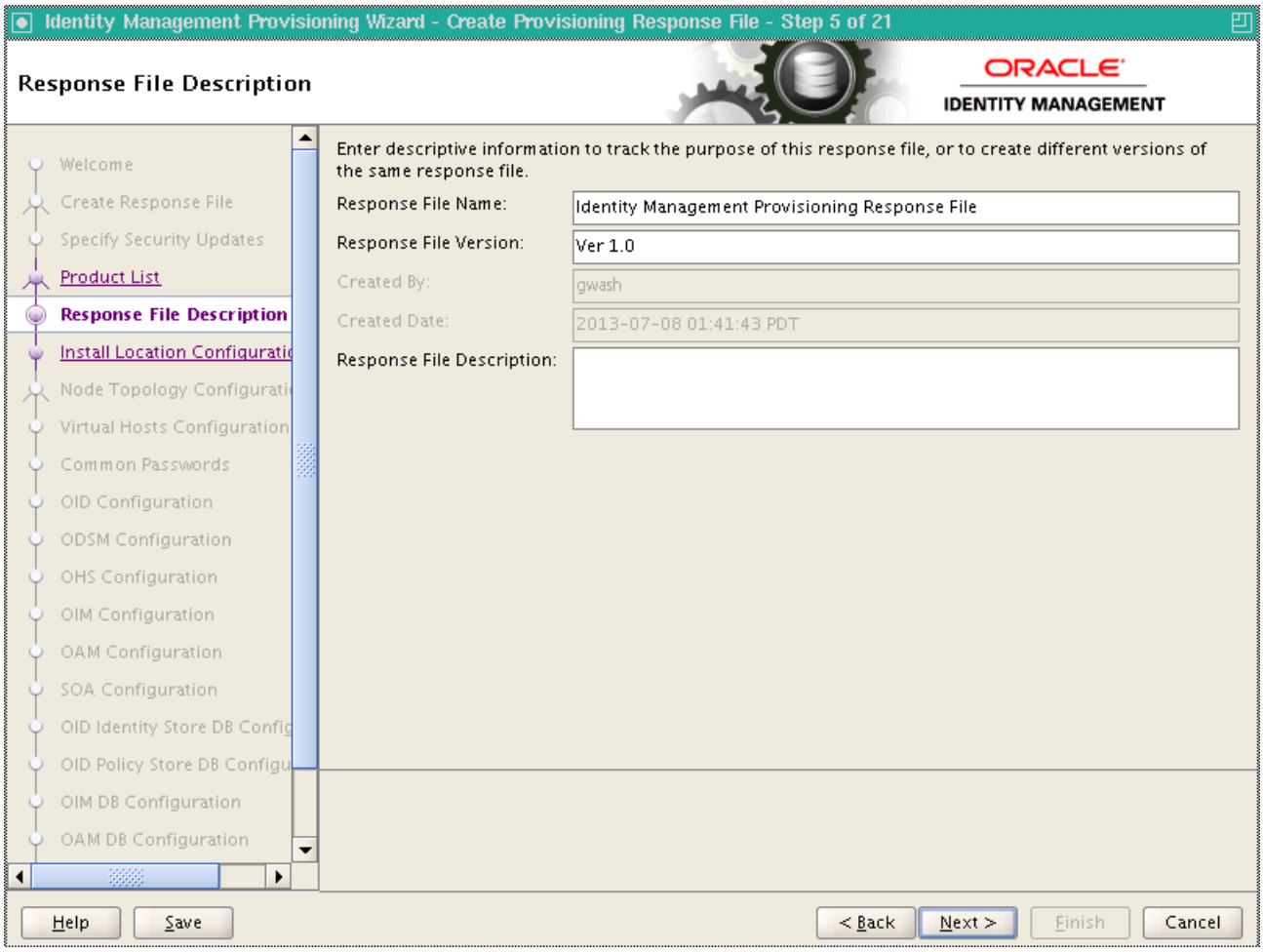


Click **Next** to continue.

4.2.6 Response File Description Page

Specify descriptive information to identify this response file. This description is not associated in any way with the executable plan file, or the summary file, that you save at the end of the response file creation process.

- **Response File Name**: The Identity Management Provisioning Wizard provides the default title Identity Management Provisioning Response File. You can change this.
- **Response File Version**: The Identity Management Provisioning Wizard provides a default value, which you can change. You can use this to keep track of different file versions.
- **Created By**: Defaults to the operating system user who invoked the Provisioning Wizard. Set when the response file is initially created and cannot be modified for the current response file.
- **Created Date**: Defaults to the date that the response file was initially created. Set when the response file was initially created and cannot be modified for the current response file.
- **Response File Description**: Provide a description of this response file. This is an optional field.



Click **Next** to continue.

4.2.7 Install Location Configuration Page

Use the Install Location Configuration Page to supply the location of the various directories required for installation and configuration actions.

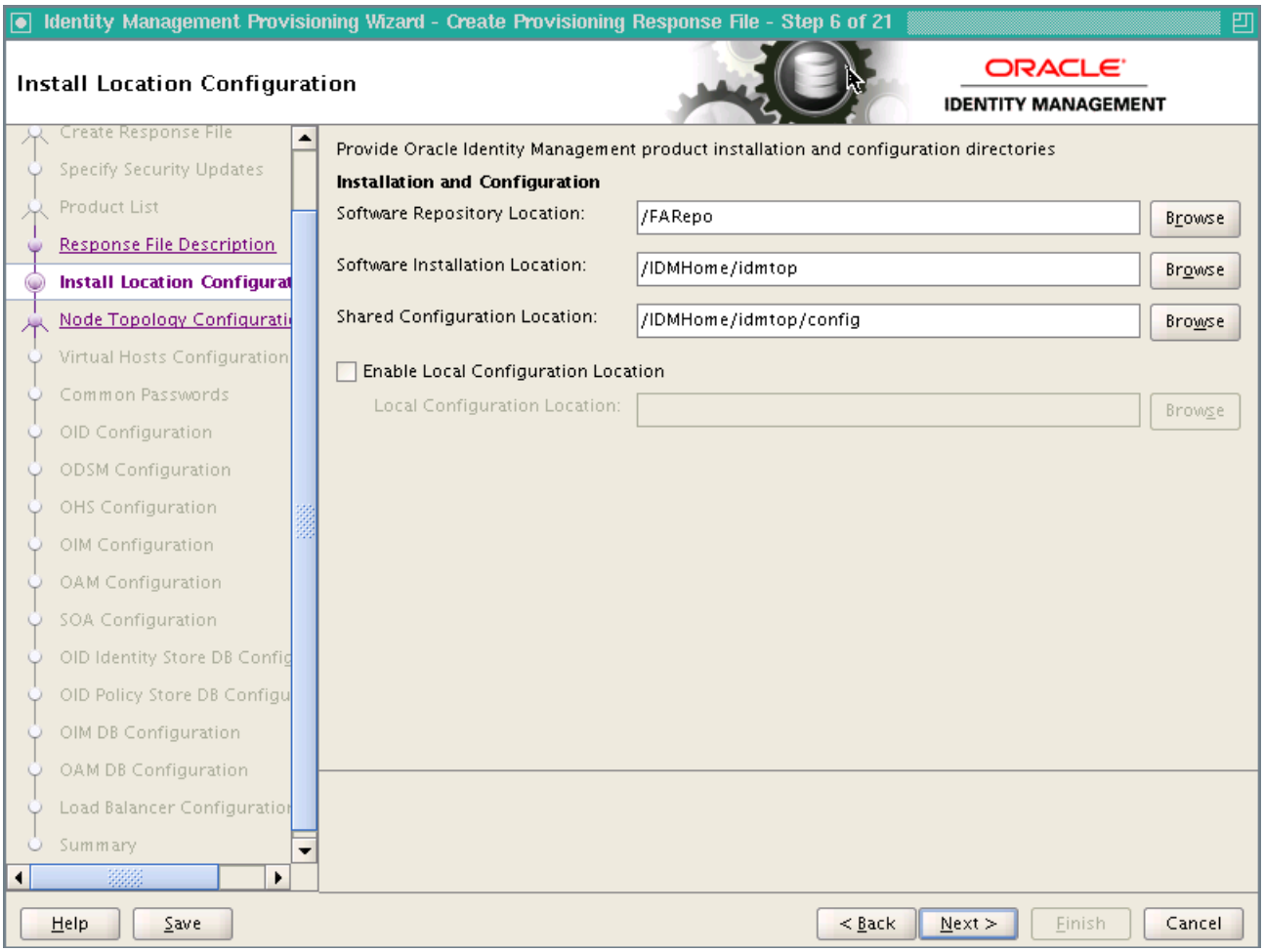
Installation and Configuration

- **Software Repository Location**: Specify the location of the software repository, either by typing it in the field or by clicking the **Browse** button, navigating to the desired location, and selecting it. This location must contain a folder named `installers`, which contains the software to install.
- **Software Installation Location**: Specify the location on shared storage where you want the Middleware Homes to be placed, either by typing it in the field or by clicking the **Browse** button, navigating to the desired location, and selecting it. In a multinode scenario, this folder must be shared across all machines.

  Ensure that this directory path is 45 characters or fewer in length. A longer pathname can cause errors during Identity Management provisioning. See Section 7.2.2, "Null Error Occurs When WebLogic Patches Are Applied."
- **Shared Configuration Location**: Specify the shared configuration location, either by typing it in the field or by clicking the **Browse** button, navigating to the desired

location, and selecting it. (In a single host environment, the shared configuration location is not actually shared.)

- **Enable Local Configuration Location**: Do not select this option, as it is not relevant when provisioning a single host environment.

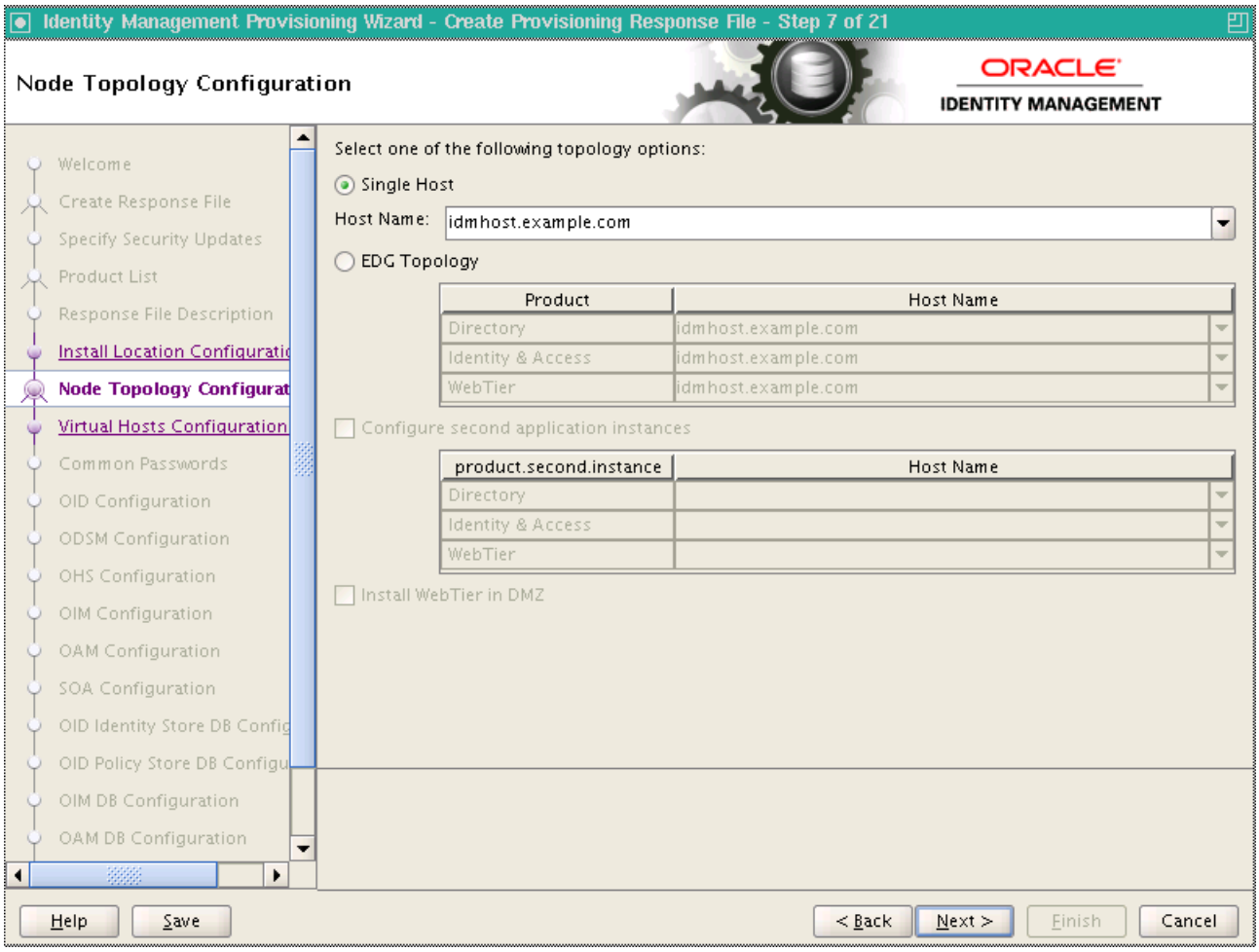


Click **Next** to continue.

4.2.8 Node Topology Configuration Page

Use the Node Topology Configuration Page to select configuration options and provide information about hosts and products.

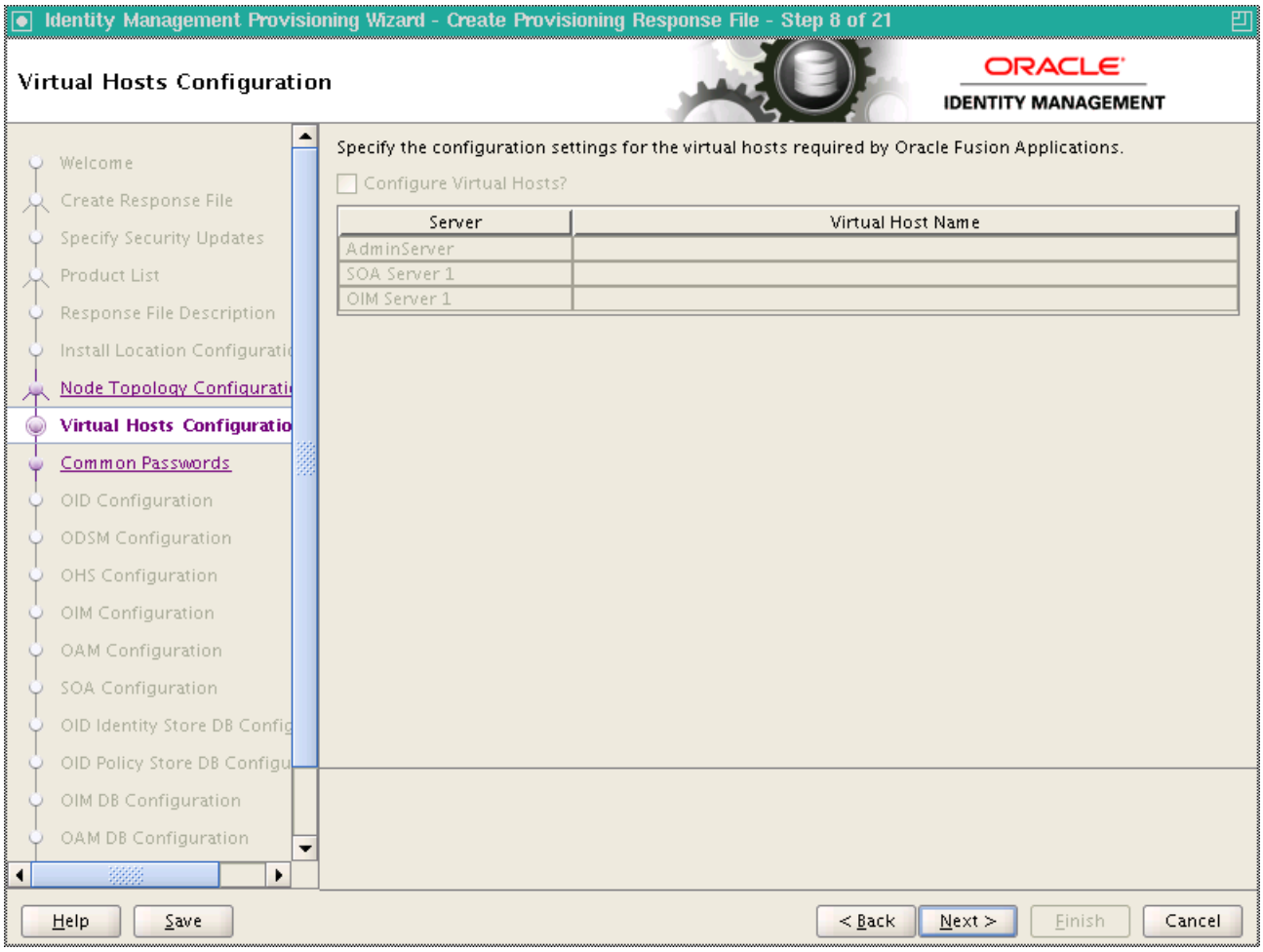
- **Single Host**: Select to provision a simple, single host topology.
  - **Host Name**: Specify the host where you want to provision Identity Management, as a fully-qualified host name.
- **EDG Topology**: Do not select this topology. If you want to provision a multiple host topology, you should be using *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management (Oracle Fusion Applications Edition)*, not the current guide.
- **Install WebTier in DMZ**: Do not select this option, as it is not relevant when provisioning a single-host environment.



Click **Next** to continue.

4.2.9 Virtual Hosts Configuration Page

Use the Virtual Hosts Configuration Page to select virtual host configuration options. If you selected **Single Host**, the Virtual Hosts Configuration Page is not editable.

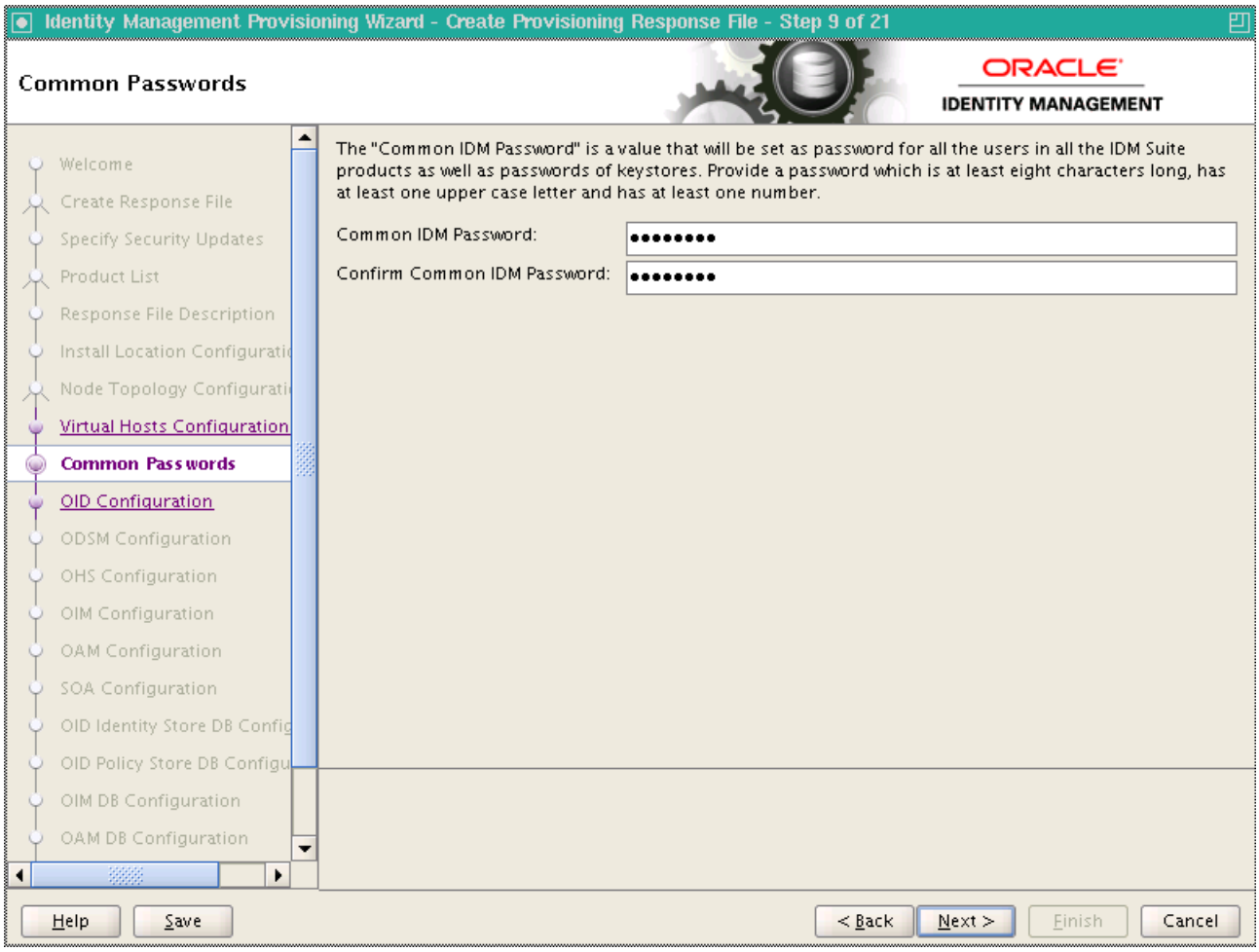


Click **Next** to continue.

4.2.10 Common Passwords Page

Use the Common Passwords Page to select a common password.

- **Common Identity Management Password**: Specify a password to be used for all administrative users in the Identity Management Suite and for keystores. The password must be at least eight characters long and must contain at least one uppercase letter and at least one number.
- **Confirm Common Identity Management Password**: Reenter the password.



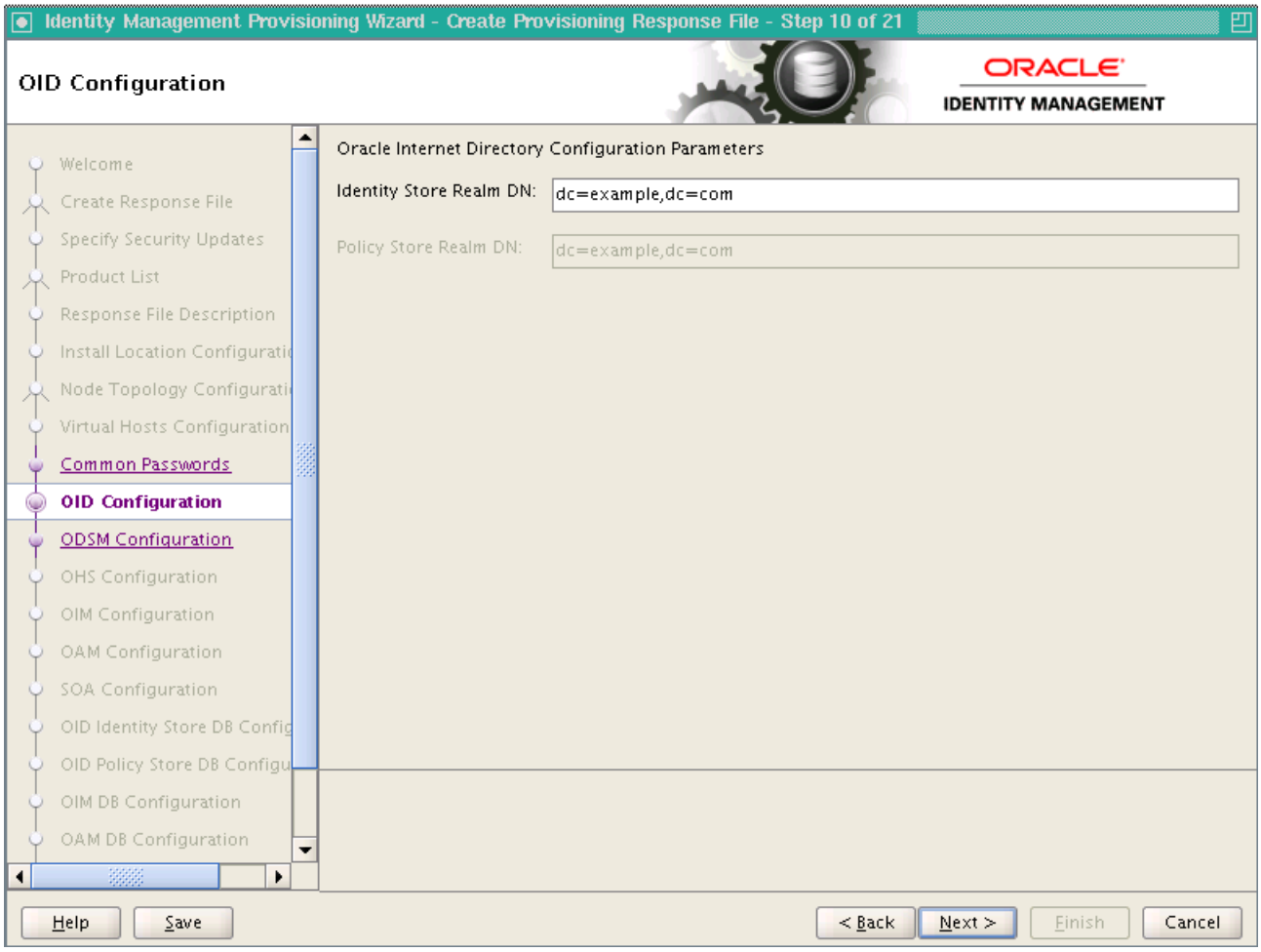
Click **Next** to continue.

4.2.11 OID Configuration Page

Use the OID Configuration Page to select configuration options for Oracle Internet Directory.

Oracle Internet Directory Configuration Parameters

- **Identity Store Realm DN**: Specify the Distinguished Name of the Oracle Internet Directory realm, for example: `dc=mycompany,dc=com`
- **Policy Store Realm DN**: This field cannot be edited. The Policy Store and Identity Store will always be the same.

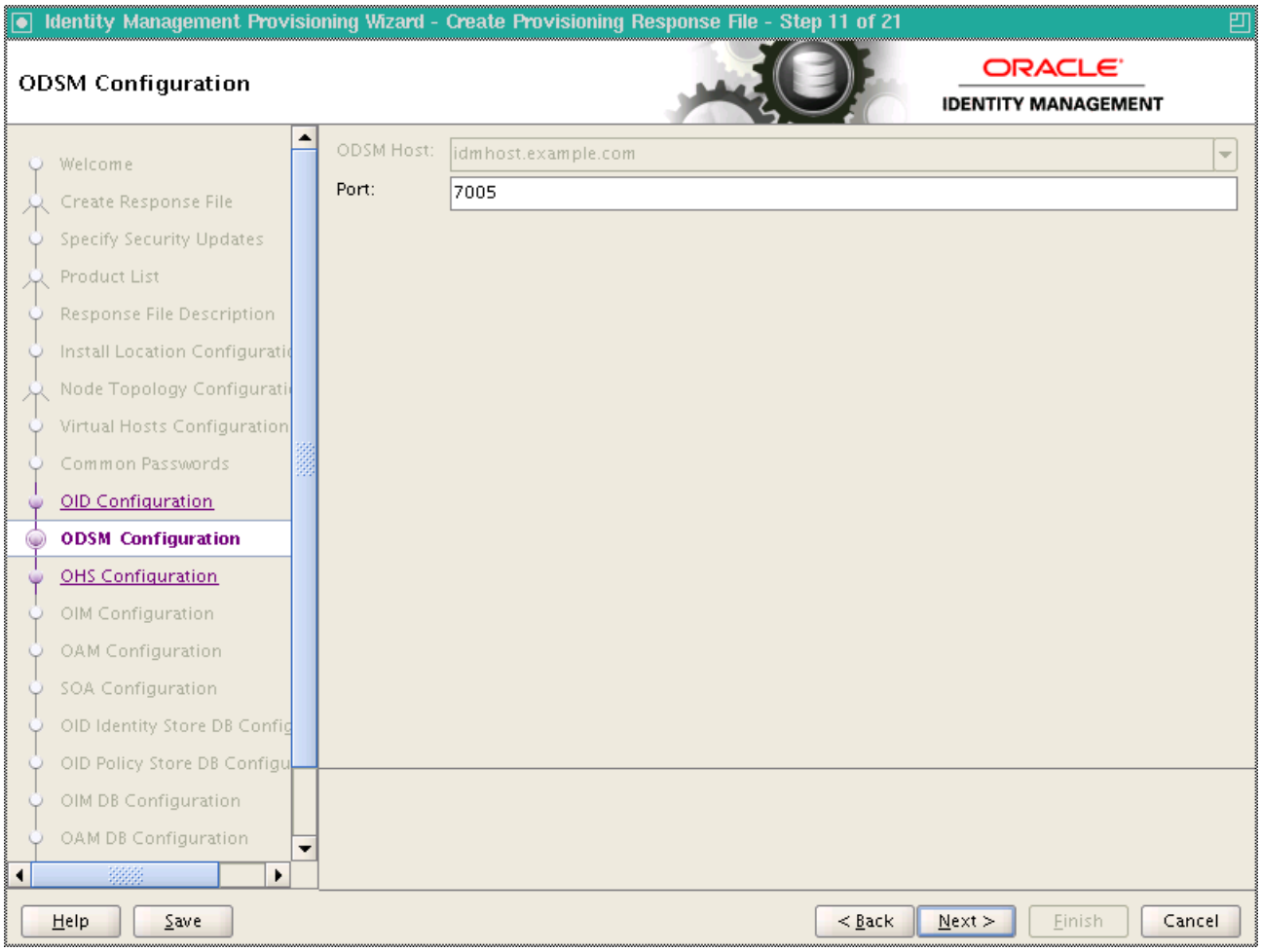


Click **Next** to continue.

4.2.12 ODSM Configuration Page

Use the ODSM Configuration Page to select configuration options for Oracle Directory Services Manager (ODSM). Information about the second host will appear on the page only if Configure Second Instances Topology was selected in the Node Topology Configuration Page.

- **ODSM Host**: This field is purely informational. The value is determined by the host entered in the Node Topology Configuration Page.
- **Port**: Specify the port to be used by the first ODSM instance.
- **Second ODSM Host**: This field is purely informational. The value is determined by the host entered in the Node Topology Configuration Page.
- **Second ODSM Port**: Specify the port to be used by the second ODSM instance.



Click **Next** to continue.

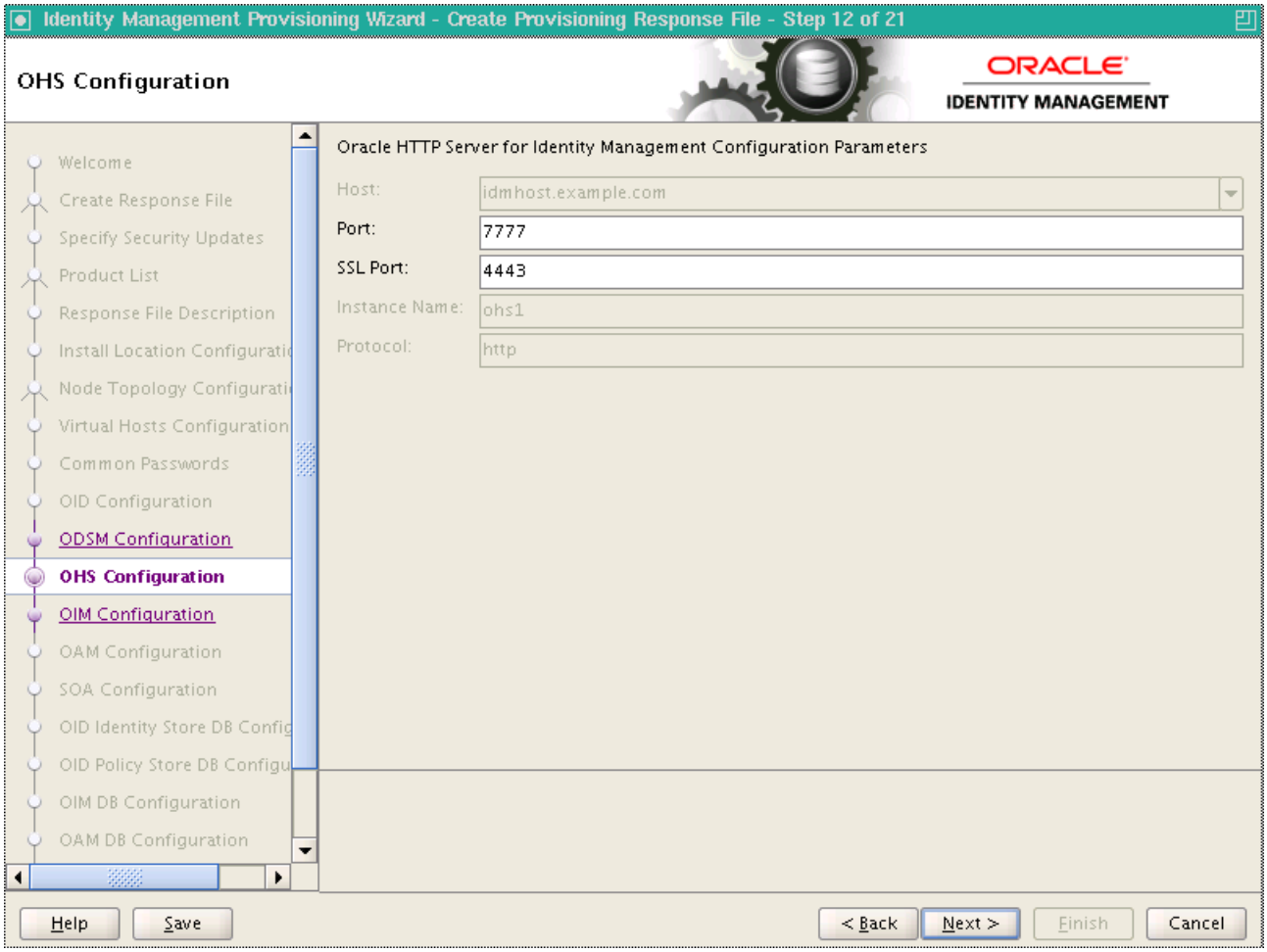
4.2.13 OHS Configuration Page

Use the OHS Configuration Page to change the installation ports used for Oracle HTTP Server (OHS). Information about the second host will appear on the page only if Configure Second Instances Topology was selected in the Node Topology Configuration Page.

Oracle HTTP Server for Identity Management Configuration Parameters

- **Host**: This field is purely informational. The value is determined by the host entered in the Node Topology Configuration Page.
- **Port**: Specify the non-SSL port number to be used for the first instance of the Oracle HTTP Server.
- **SSL Port**: Specify the SSL port number to be used for the first instance of the Oracle HTTP Server.
- **Instance Name**: This field is purely informational. It displays the instance name of the first Oracle HTTP Server.
- **Second OHS Host**: This field is purely informational. The value is determined by the host entered in the Node Topology Configuration Page.

- **Second OHS Port**: Specify the non-SSL port number to be used for the second instance of the Oracle HTTP Server.
- **Second OHS SSL Port**: Specify the SSL port number to be used for the second instance of the Oracle HTTP Server.
- **Second Instance Name**: This field is purely informational. It displays the instance name of the second Oracle HTTP Server.
- **Protocol**: This field is purely informational.



Click **Next** to continue.

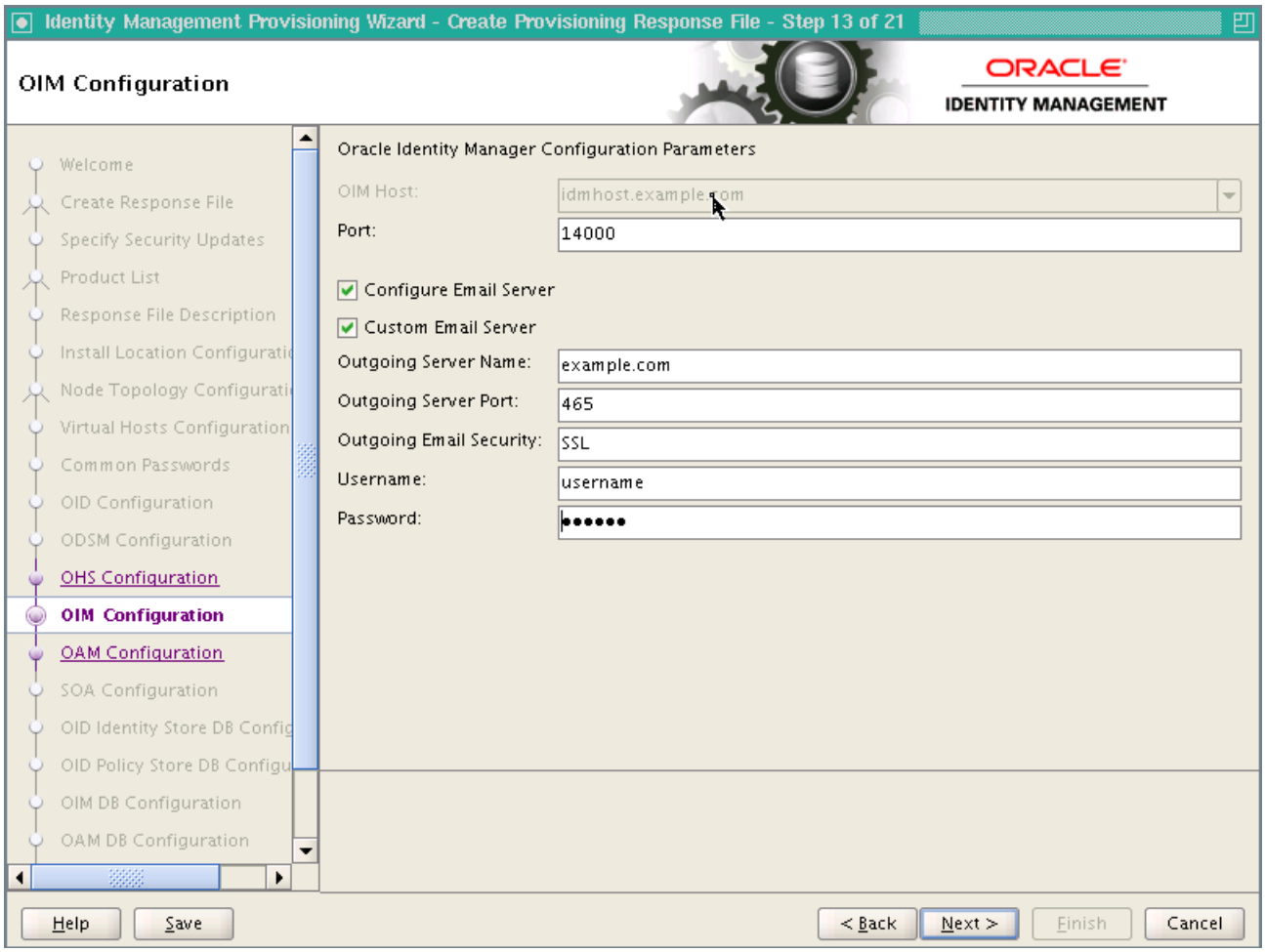
4.2.14 OIM Configuration Page

Use the OIM Configuration Page to modify the ports used by Oracle Identity Manager and, optionally, to configure an email server. Information about the second host will appear on the page only if Configure Second Instances Topology was selected in the Node Topology Configuration Page.

Oracle Identity Manager Configuration Parameters

- **OIM Host**: This field is purely informational. The value is determined by the host entered in the Node Topology Configuration Page.
- **OIM Port**: Specify the port to be used by the Oracle Identity Manager managed servers.

- **Second OIM Host**: This field is purely informational. The value is determined by the host entered in the Node Topology Configuration Page.
- **Second OIM Port**: Specify the port to be used by the Oracle Identity Manager managed servers.
- **Configure Email Server**: Select to configure the default email server on Linux. If you select this option on Windows, you must also select **Custom Email Server**.
- **Custom Email Server**: Select to configure a custom email server. On Windows, you must select this option if you selected **Configure Email Server**.
- **Outgoing Server Name**: Specify the name of your outgoing email server, for example: mail.mycompany.com
- **Outgoing Server Port**: Specify the port that your outgoing email server uses. This is typically 465.
- **Outgoing Email Security**: The security used by SMTP server. Possible values are `None`, `TLS` and `SSL`.
- **Username**: If you require a username to authenticate with the email server, enter that username.
- **Password**: Enter the password for the username.



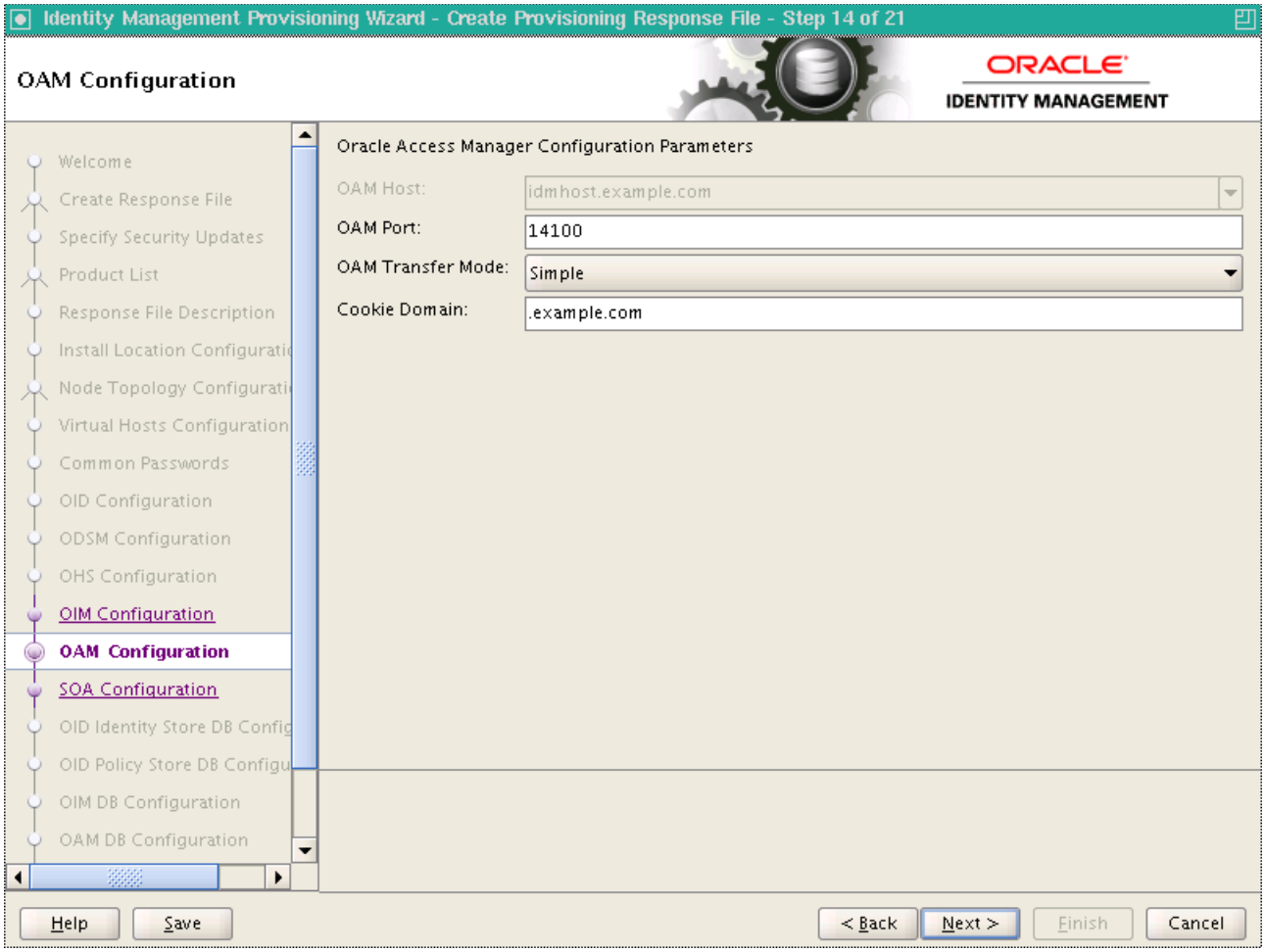
Click **Next** to continue.

4.2.15 OAM Configuration Page

Use the OAM Configuration Page to select installation options for Oracle Access Manager. Information about the second host will appear on the page only if Configure Second Instances Topology was selected in the Node Topology Configuration Page.

Oracle Access Manager Configuration Parameters

- **OAM Host**: This field is purely informational. The value is determined by the host entered in the Node Topology Configuration Page.
- **OAM Port**: Specify the port number of the first instance.
- **Second OAM Host**: This field is purely informational. The value is determined by the host entered in the Node Topology Configuration Page.
- **Second OAM Port**: Specify the port number of the second instance.
- **OAM Transfer Mode**: Specify the transfer mode to be used by Oracle Access manager. This must be `Open` on AIX and `Simple` on other platforms.
- **Cookie Domain**: Specify the cookie domain. For example: `.mycompany.com`



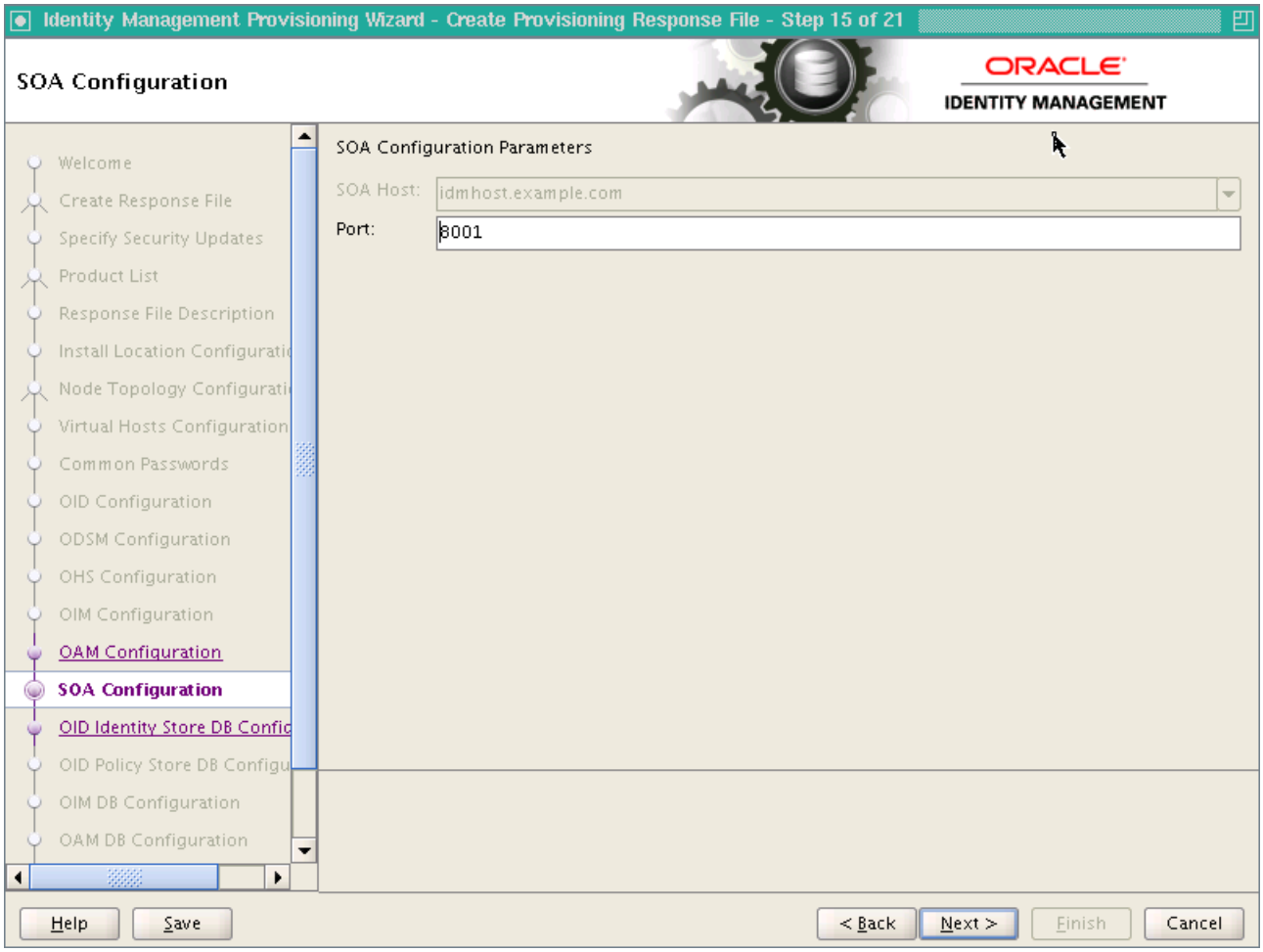
Click **Next** to continue.

4.2.16 SOA Configuration Page

Use the SOA Configuration Page to enter the ports to be used by the SOA Managed servers. Information about the second host will appear on the page only if Configure Second Instances Topology was selected in the Node Topology Configuration Page.

SOA Configuration Parameters

- **SOA Host**: This field is purely informational
- **Port**: This field specifies the port for the first SOA instance. You can change this.
- **Second SOA Host**: This field is purely informational
- **Second SOA Port**: This field specifies the port for the second SOA instance. You can change this



Click **Next** to continue.

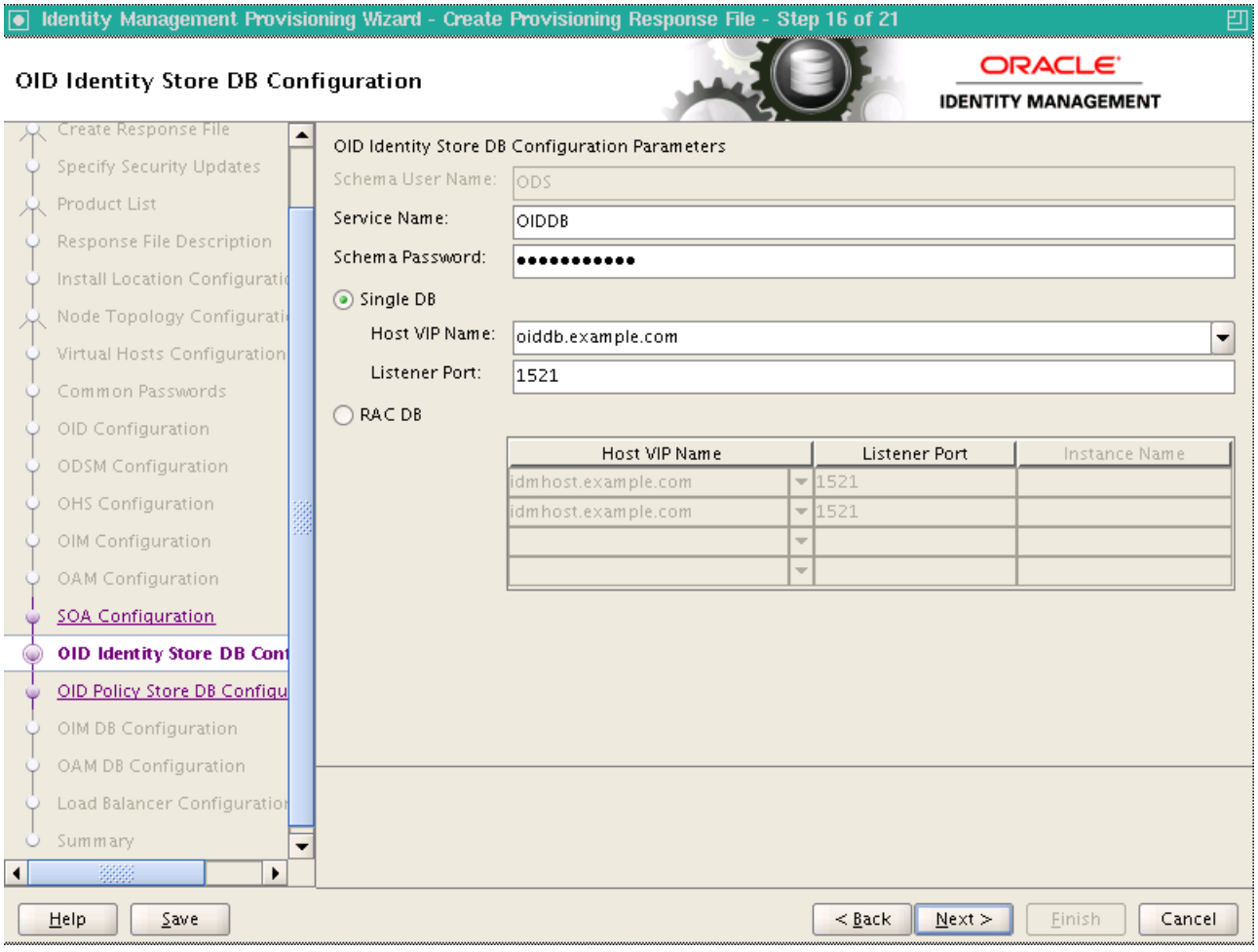
4.2.17 OID Identity Store DB Configuration Page

Use the OID Identity Store DB Configuration Page to enter the database connection details for your Oracle Internet Directory Database.

OID Identity Store DB Configuration Parameters

- **Schema User Name**: This field specifies the name of the Oracle Internet Directory schema user, ODS. You cannot change this name.

- **Service Name**: Specify the service name of the database service, for example: oiddb.mycompany.com
- **Schema Password**: Specify the password you used when creating the Oracle Internet Directory schema using the Identity Management RCU.
- **Single DB**: Select if you are using a single Oracle Database.
  - **Host VIP Name**: Specify the host name of the Oracle Database.
  - **Listener Port**: Specify the database listener port.
- **RAC DB**: Select if you are using an Oracle RAC Database. Up to four RAC instances are supported.
  - **Host VIP Name**: Specify the host name of the Oracle RAC Database instance. If you are using Oracle Database 11.2, this must be the SCAN address.
  - **Listener Port**: Specify the database listener port
  - **Instance Name**: Specify the database instance name, for example, oiddb1.

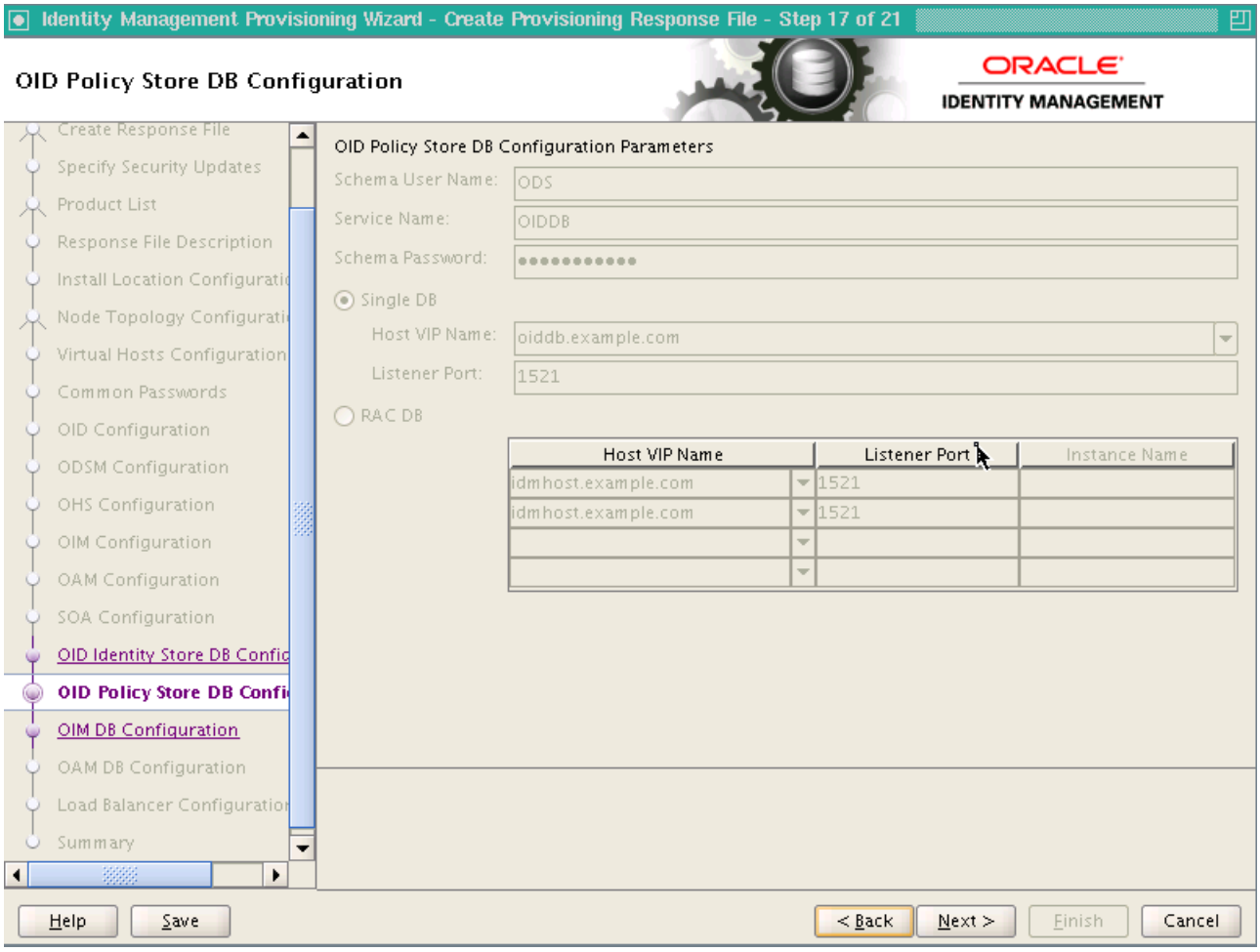


Click **Next** to continue.

4.2.18 OID Policy Store DB Configuration Page

The OID Policy Store DB Configuration page cannot be edited. The values are purely informational and are the same as those entered on the OID Identity Store DB Configuration Page.

- **Schema User Name**: The name of the Oracle Internet Directory schema user, ODS.
- **Service Name**: The service name of the database service, for example: oiddb.mycompany.com
- **Schema Password**: The password you used when creating the Oracle Internet Directory schema using the Identity Management RCU.
- **Single DB**: Selected if you are using a single Oracle Database.
  - **Host VIP Name**: The host name of the Oracle Database.
  - **Listener Port**: The database listener port.
- **RAC DB**: Selected if you are using an Oracle RAC Database. Up to four RAC instances are supported.
  - **Host VIP Name**: The host name of the RAC database instance. If you are using Oracle Database 11.2, this must be the SCAN address.
  - **Listener Port**: The database listener port.
  - **Instance Name**: The database instance name, for example, oiddb1.



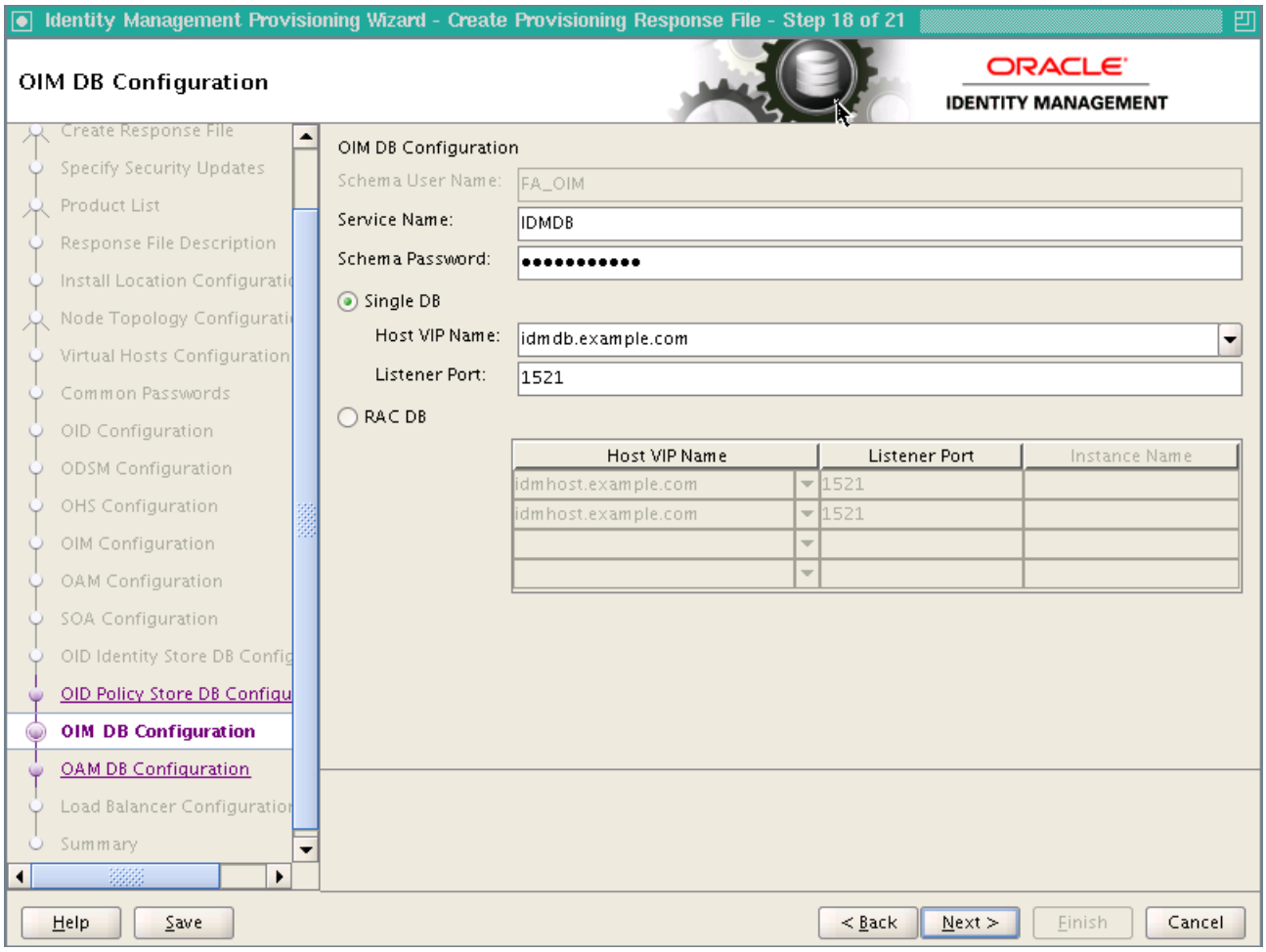
Click **Next** to continue.

4.2.19 OIM DB Configuration Page

Use the OIM DB Configuration Page to enter information about the Database that contains the schemas for Oracle Identity Manager, SOA, Oracle Access Manager, and Oracle Identity Federation.

OIM DB Configuration Page

- **Schema User Name**: This field specifies the name of the schema user, `FA_OIM`. You cannot change this name.
- **Service Name**: Specify the service name of the database service, for example: oiddb.mycompany.com
- **Schema Password**: Specify the password you used when creating the Oracle Internet Directory schema using the Identity Management RCU.
- **Single DB**: Select if you are using a single Oracle Database.
  - **Host VIP Name**: Specify the host name of the Oracle Database.
  - **Listener Port**: Specify the database listener port.
- **RAC DB**: Select if you are using an Oracle RAC Database.
  - **Host VIP Name**: Specify the host name of the RAC database instance. If you are using Oracle Database 11.2, this must be the SCAN address.
  - **Listener Port**: Specify the database listener port.
  - **Instance Name**: Specify the database instance name, for example, oiddb1.



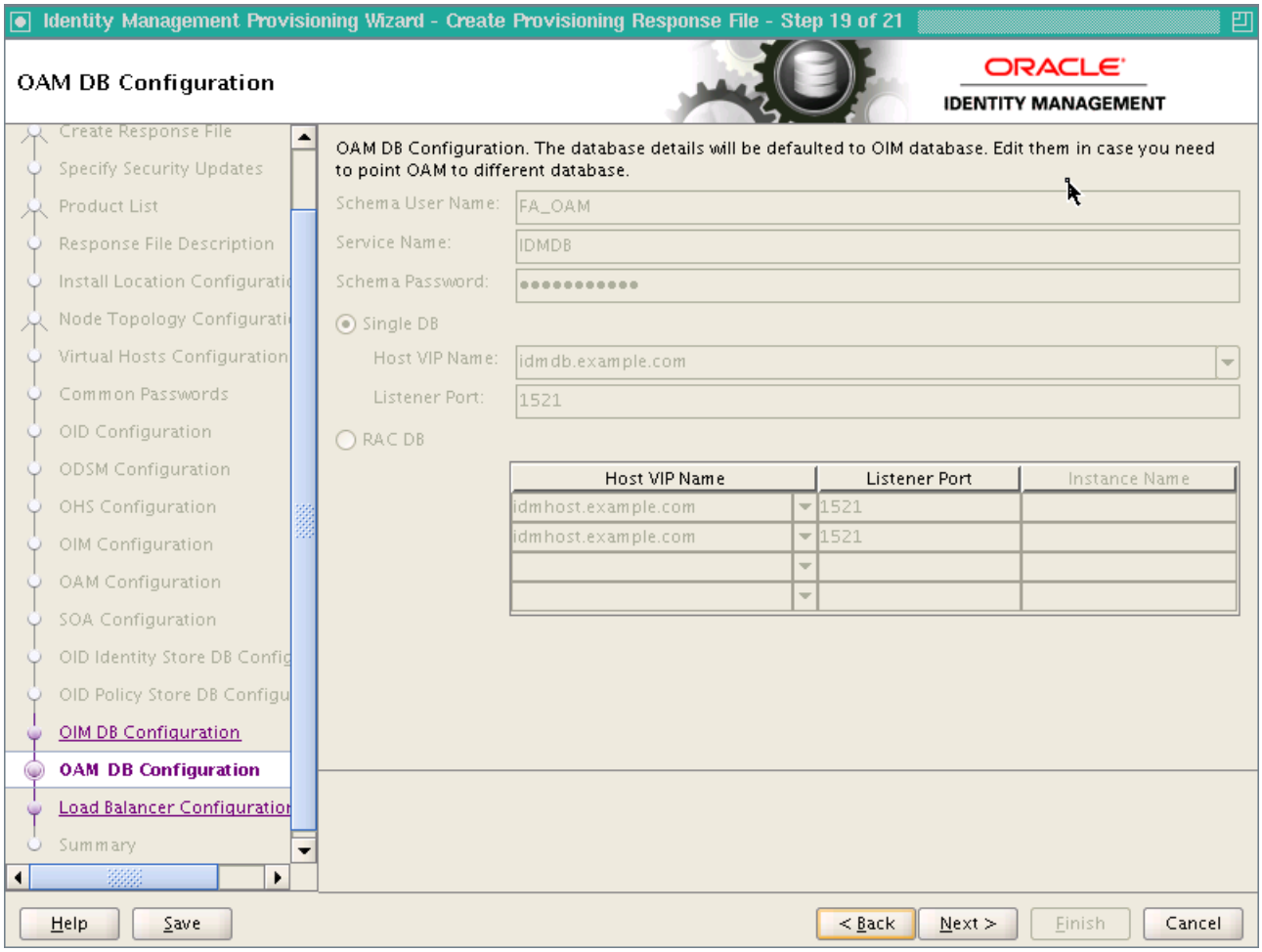
Click **Next** to continue.

4.2.20 OAM DB Configuration Page

The OAM DB Configuration Page cannot be edited. The values are purely informational and are the same as those entered on the OIM DB Configuration Page, except for the **Schema User Name**.

- **Schema User Name**: The name of the schema user, `FA_OAM`.
- **Service Name**: The service name of the database service, for example: oiddb.mycompany.com
- **Schema Password**: The password you used when creating the Oracle Internet Directory schema using the Identity Management RCU.
- **Single DB**: Selected if you are using a single Oracle Database.
  - **Host VIP Name**: The host name of the Oracle Database.
  - **Listener Port**: Specify the database listener port.
- **RAC DB**: Selected if you are using an Oracle RAC Database. Up to four instances are supported.
  - **Host VIP Name**: The host name of the RAC database instance. If you are using Oracle Database 11.2, this must be the SCAN address.

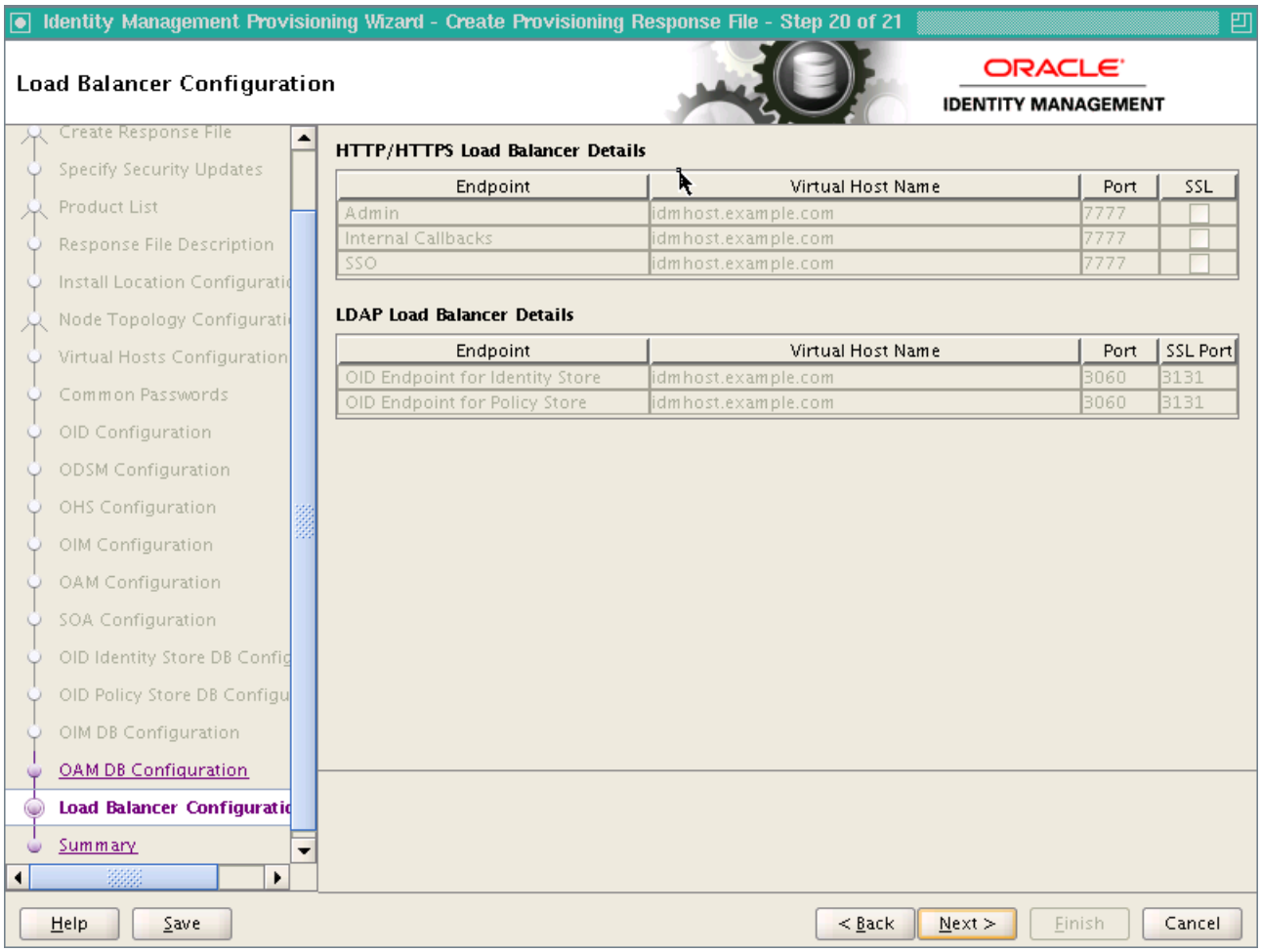
- **Listener Port**: The database listener port.
- **Instance Name**: The database instance name, for example, oiddb1.



Click **Next** to continue.

4.2.21 Load Balancer Page

In a single-host environment, the Load Balancer Page is not editable.

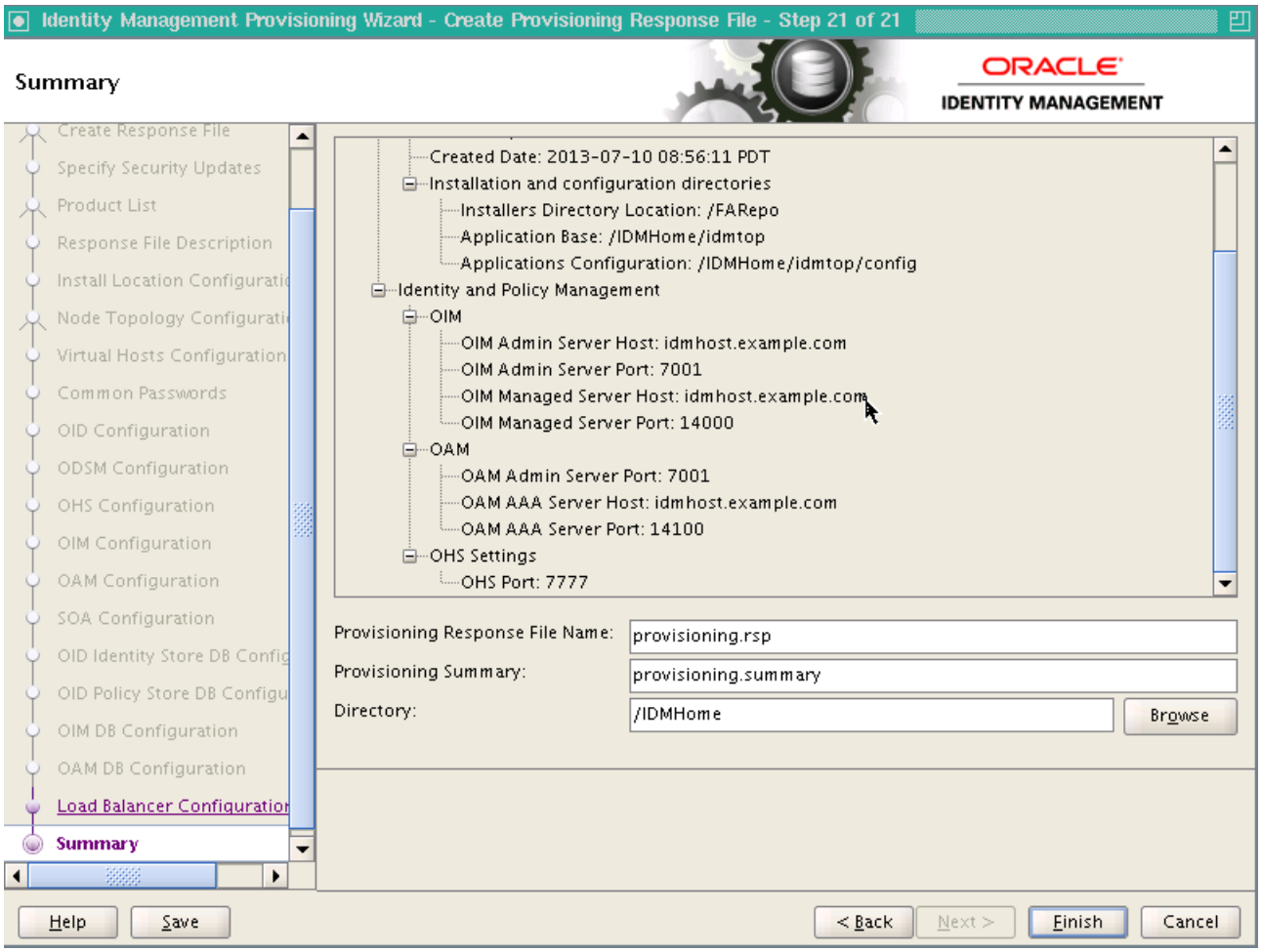


Click **Next** to continue.

4.2.22 Summary Page

Use the Summary Page to view a summary of your selections and enter additional information.

- **Response File Name**: Provide the name of the response file to be created.
- **Provisioning Summary**: Provide the name of the provisioning summary file to be created.
- **Directory**: Specify the directory where you want this Provisioning Response File to be saved.


Identity Management Provisioning Wizard - Create Provisioning Response File - Step 21 of 21
Summary
ORACLE
IDENTITY MANAGEMENT
Create Response File
Specify Security Updates
Product List
Response File Description
Install Location Configurati
Node Topology Configurati
Virtual Hosts Configuration
Common Passwords
OID Configuration
ODSM Configuration
OHS Configuration
OIM Configuration
OAM Configuration
SOA Configuration
OID Identity Store DB Config
OID Policy Store DB Configu
OIM DB Configuration
OAM DB Configuration
Load Balancer Configuratio
Summary
Created Date: 2013-07-10 08:56:11 PDT
Installation and configuration directories
Installers Directory Location: /FARepo
Application Base: /IDMHome/idmtop
Applications Configuration: /IDMHome/idmtop/config
Identity and Policy Management
OIM
OIM Admin Server Host: idmhost.example.com
OIM Admin Server Port: 7001
OIM Managed Server Host: idmhost.example.com
OIM Managed Server Port: 14000
OAM
OAM Admin Server Port: 7001
OAM AAA Server Host: idmhost.example.com
OAM AAA Server Port: 14100
OHS Settings
OHS Port: 7777
Provisioning Response File Name:
provisioning.rsp
Provisioning Summary:
provisioning.summary
Directory:
/IDMHome
Browse
Help
Save
< Back
Next >
Finish
Cancel

5

Performing Oracle Identity Management Provisioning

This chapter describes how to perform provisioning.

This chapter contains the following sections:

5.1 Introduction to Performing Oracle Identity Management Provisioning

After you create the provisioning response file, you use it to provision the Identity Management Environment.

There are eight stages to provisioning. These stages must be run in the following order:

1. preverify - This checks that each of the servers being used in the topology satisfies the minimum requirements of the software being installed and configured.
2. install - This installs all of the software and related patches present in Provisioning Repository.
3. preconfigure - This does the following:
   - Creates OID and seeds it with Users/Groups.
   - Creates OVD
   - Configures ODSM
   - Creates the WebLogic Domain
   - Creates OHS instance
4. configure - This does the following:
   - Associates the Policy Store to OID
   - Starts managed servers as necessary
   - Associates OAM with OID
   - Configure OIM
5. configure-secondary - This does the following:
   - Integrates Weblogic Domain with Webtier

- Register webtier with domain
- Integrate OAM and OIM

6. postconfigure - This does the following:
   - Register OID with Weblogic Domain
   - SSL Enable OID and OVD
   - Tune OID
   - Run OIM Reconciliation
   - Configure UMS Mail Server
   - Generate OAM Keystore
   - Configure OIF
   - Configure Webgates
7. startup - This starts up all components in the topology
8. validate - This performs a number of checks on the built topology to ensure that everything is working as it should be.

You specify the stage using the `-target` option to the `runIDMProvisioning.sh` or `runIDMProvisioning.bat` command. Each stage must be completed before the next stage can begin. Failure of a stage will necessitate a cleanup and restart.

5.2 Performing Provisioning

Provisioning is accomplished by using either the command line or the Oracle Identity Management Provisioning Wizard.

This section contains the following topics:

- Section 5.2.1, "Performing Provisioning by Running the Provisioning Commands"
- Section 5.2.2, "Monitoring Provisioning Using the Identity Management Provisioning Wizard"

5.2.1 Performing Provisioning by Running the Provisioning Commands

To use the command line, you must run the command `runIDMProvisioning.sh` or `runIDMProvisioning.bat` a number of times, specifying the provisioning stage with the `-target` option. You MUST complete each command, in order, before running the next command.

Before running the provisioning tool, set the following environment variables:

- Set `ANT_HOME` to: *`repository_location`*`/provisioning/ant`
- Set `JAVA_HOME` to: *`repository_location`*`/jdk6`

The command syntax for the provisioning tool on UNIX is:

```
runIDMProvisioning.sh -responseFile RESPONSE_FILE -target STAGE
```

The command syntax on Windows is:

```
runIDMProvisioning.bat -responseFile RESPONSE_FILE -target STAGE
```

Where:

RESPONSE_FILE is the provisioning response file. You specified the file name and directory on the Summary Page when you ran the wizard to create the file. See Section 4.2.22, "Summary Page." The default value is *IDMLCM_HOME*/provisioning/bin/provisioning.rsp on UNIX and *IDMLCM_HOME*\provisioning\bin\provisioning.rsp on Windows.

STAGE is one of the stages listed in Section 5.1, "Introduction to Performing Oracle Identity Management Provisioning."

5.2.2 Monitoring Provisioning Using the Identity Management Provisioning Wizard

If you want to use the Identity Management Provisioning Wizard to monitor the progress of provisioning, follow these steps:

1. Set ANT_HOME to: *repository_location*/provisioning/ant
2. Set JAVA_HOME to: *repository_location*/jdk6
3. Invoke idmProvisioningWizard.sh (on Linux or UNIX) or idmProvisioningWizard.bat (on Windows).
4. When you get to the Identity Management Installation Options Page, select **Provision an Identity Management Environment** and specify the provisioning.rsp file you created in Chapter 4, "Creating a Provisioning Profile."

Then proceed as described in the following sections.

Note: In the Prerequisite Checks, Installation, Preconfigure, Configure, Configure Secondary, Postconfigure, and Startup pages, the Status of each build is indicated by one of these icons:

- **Block**: Processing has not yet started for the named phase.
- **Clock**: Performing the build for a phase.
- **Check mark**: The build was completed successfully.
- **x** mark: The build has failed for this phase. You must correct the errors before you can continue.

Click an **x** to display information about failures. Click the host-level **Log** file for details about this phase. Click a build **Log** file to see details specific to that build.

In case of errors, you must manually clean up everything. Kill all running processes, delete the directories, rerun RCU, and start over from the beginning.

- Section 5.2.2.1, "Identity Management Installation Options Page"
- Section 5.2.2.2, "Install Location Configuration Page"
- Section 5.2.2.3, "Review Provisioning Configuration Page"
- Section 5.2.2.4, "Summary Page"
- Section 5.2.2.5, "Prerequisite Checks Page"
- Section 5.2.2.6, "Installation Page"
- Section 5.2.2.7, "Preconfigure Page"
- Section 5.2.2.8, "Configure Page"

5.2.2.1 Identity Management Installation Options Page

Select **Provision an Identity Management Environment** to use an existing provisioning response file to provision the environment.

In the **Response File** field, specify the path name of the file you want to use, either by typing it in the field or by clicking the **Browse** button, navigating to the desired file, and selecting it.

Click **Next** to continue.

5.2.2.2 Install Location Configuration Page

Use the Install Location Configuration Page to specify Oracle Identity Management installation and configuration directories.

Installation and Configuration.

- **Software Repository Location**: Specify the location of the software repository, either by typing it in the field or by clicking the **Browse** button, navigating to the desired location, and selecting it.
- **Software Installation Location**: Specify the location on shared storage where you want the Middleware Home to be placed, either by typing it in the field or by clicking the **Browse** button, navigating to the desired location, and selecting it.
- **Shared Configuration Location**: Specify the shared configuration location, either by typing it in the field or by clicking the **Browse** button, navigating to the desired location, and selecting it.
- **Enable Local Configuration Location**: Do not select this check box if you are provisioning a single host environment.

5.2.2.3 Review Provisioning Configuration Page

The Review Provisioning Configuration Page enables you to select configurations you want to review. Select a configuration and click **Next** to view the corresponding configuration page.

- **Node Topology Configuration**
- **Virtual Hosts Configuration**
- **Common Passwords**
- **OID: Oracle Internet Directory Configuration**
- **ODSM: Oracle Directory Services Manager Configuration**
- **OHS: Oracle HTTP Server Configuration**
- **OAM: Oracle Access Manager Configuration**
- **OIM: Oracle Identity Manager Configuration**
- **Load Balancer Configuration**

Click **Next** to continue.

5.2.2.4 Summary Page

Use the Summary Page to view a summary of your selections and enter additional information.

Review the information displayed to ensure that the installation details are what you intend. To make changes, click **Back** to return to previous screens in the interview.

Click **Next** to continue.

5.2.2.5 Prerequisite Checks Page

Use the Prerequisite Checks Page to observe the progress of the preverification steps. During this stage, the Identity Management Provisioning Wizard checks for the basic prerequisites, such as free disk space, port availability, and Database connections.

See the note at the beginning of Section 5.2.2 for information about viewing build status on this page.

Click **Next** to continue.

5.2.2.6 Installation Page

Use the Installation Page to install the Oracle Fusion Middleware products. The host is marked with a Home symbol in the Host column. The Domains column lists the domains deployed in the new environment.

During this stage, the Identity Management Provisioning Wizard installs the software bits and applies the patches present in the repository.

See the note at the beginning of Section 5.2.2 for information about viewing build status on this page.

Click **Next** to proceed.

5.2.2.7 Preconfigure Page

During this stage, the Identity Management Provisioning Wizard configures Oracle Internet Directory, Oracle Virtual Directory, and Oracle Directory Services Manager. It also creates the domain and extends it for all the necessary components.

Note: Each new phase must run sequentially; that is, you cannot start a new phase until the previous phase has been completed successfully.

See the note at the beginning of Section 5.2.2 for information about viewing build status on this page.

Click **Next**. The Identity Management Provisioning Wizard starts the configure phase and displays the Configure screen.

5.2.2.8 Configure Page

During this stage, the Identity Management Provisioning Wizard performs OIM configuration.

See the note at the beginning of Section 5.2.2 for information about viewing build status on this page.

Click **Next**. The Identity Management Provisioning Wizard starts the Configure-secondary phase and displays the Configure Secondary screen.

5.2.2.9 Configure Secondary Page

During this stage, the Identity Management Provisioning Wizard performs Oracle Identity Manager-Oracle Access Manager integration.

See the note at the beginning of Section 5.2.2 for information about viewing build status on this page.

Click **Next**. The Identity Management Provisioning Wizard starts the Postconfigure phase and displays the Postconfigure screen.

5.2.2.10 Postconfigure Page

During this stage, the Identity Management Provisioning Wizard performs tuning and enables the environment for SSL communication. Oracle Identity Federation is configured in this stage.

See the note at the beginning of Section 5.2.2 for information about viewing build status on this page.

Click **Next**. The Identity Management Provisioning Wizard starts the Startup phase and displays the Startup screen.

5.2.2.11 Startup Page

During this stage, the Identity Management Provisioning Wizard starts or restarts all the services except for Oracle Identity Federation. You must start Oracle Identity Federation after provisioning is complete, as described in Section 6.8.1, "Start OIF Managed Server."

The Domains column lists the domains deployed in the new environment.

See the note at the beginning of Section 5.2.2 for information about viewing build status on this page.

Click **Next**. The Identity Management Provisioning Wizard starts the Validate phase and displays the Validation screen.

5.2.2.12 Validation Page

During this stage, the Identity Management Provisioning Wizard performs the basic validations, such as server status and Oracle Internet Directory connectivity.

The host is marked with a Home symbol in the Host column. The Domains column lists the domains deployed in the new environment.

See the note at the beginning of Section 5.2.2 for information about viewing build status on this page.

Click **Next**. The Identity Management Provisioning Wizard starts the Validate phase on the host and displays the Validation screen.

5.2.2.13 Install Complete

This page appears after provisioning has completed successfully. It shows a summary of the products that have been installed.

Click **Finish** to save the summary and exit the Identity Management Provisioning Wizard.

6

Post Provisioning Tasks

This chapter describes tasks you must perform after you have completed Identity Management Provisioning.

This chapter contains the following sections:

6.1 Correcting Datasource Configuration

Due to Bugs 17075699 and 17076033 in Identity Management Provisioning, you must make changes to the following datasources:

- **EDNLocalTxDataSource-rc*n***
- **mds-oim-rc*n***
- **mds-owsm-rc*n***
- **mds-soa-rc*n***
- **oamDS-rc*n***
- **oimJMSStoreDS-rc*n***
- **OraSDPMDataSource-rc*n***
- **SOALocalTxDataSource-rac*n***

To make the changes, proceed as follows:

1. Log in to the WebLogic Administration Console.
2. Click **Lock & Edit**.
3. Navigate to **Services -> Data Sources**.
4. Click on the data source to be updated, for example, **mds-soa-rc0**
5. Click the **Transaction** tab.

6. Deselect **Supports Global Transactions**.
7. Click **Save**.
8. Repeat Steps 4 through 7 for all the listed datasources.
9. Click **Activate Changes**.
10. Restart all servers.

6.2 Increasing Server Heap Size

Increase the maximum heap size for servers as follows:

1. Edit the file: *DOMAIN_HOME*/bin/setDomainEnv.sh
2. Locate the last occurrence of the line:

```
JAVA_PROPERTIES="${JAVA_PROPERTIES} ${EXTRA_JAVA_PROPERTIES}"
```

3. Replace that line with the following lines:

```
if [ "${SERVER_NAME}" = "wls_oim1" -o "${SERVER_NAME}" = "wls_oim2" ]
then
  EXTRA_JAVA_PROPERTIES="${EXTRA_JAVA_PROPERTIES} -Xmx2048m"
  export EXTRA_JAVA_PROPERTIES
else
  EXTRA_JAVA_PROPERTIES="${EXTRA_JAVA_PROPERTIES} -Xmx1536m"
  export EXTRA_JAVA_PROPERTIES
fi
JAVA_PROPERTIES="${JAVA_PROPERTIES} ${EXTRA_JAVA_PROPERTIES}"
```

6.3 Configuring SSL and Generating a Certificate (Windows)

On Windows, some Identity Management Provisioning Wizard procedures are not automated because they require a UNIX shell. You must install a UNIX emulation package such as Cygwin (see http://www.cygwin.com) and then perform these four manual procedures:

- Section 6.3.1, "Generating a Certificate to be Used by the Identity Management Domain"
- Section 6.3.2, "Configuring Oracle Virtual Directory to Accept Server Authentication Only Mode SSL Connections"
- Section 6.3.3, "Configuring Oracle Internet Directory to Accept Server Authentication Mode SSL Connections"
- Section 6.3.4, "Creating a Client Keystore"

6.3.1 Generating a Certificate to be Used by the Identity Management Domain

External domains communicate with the Identity Management domain using SSL Server Authentication Only Mode. To enable the Identity Management domain to support this SSL mode, you must generate a certificate and store it in the Policy Store. This adds an extra layer of security, ensuring that only those domains with access to the security certificate can communicate with the domain. The domain level certificate is generated once per domain.

To generate a certificate for the IDMDomain execute the following commands on the host.

1. Set ORACLE_HOME to the *ORACLE_HOME*.

   Set JAVA_HOME to *JAVA_HOME*.

2. Generate the certificate using the SSLGenCA command which is located in *ORACLE_COMMON_HOME*/bin

   For example:

   ```
   cd ORACLE_COMMON_HOME/bin
   ./SSLGenCA.sh
   ```

3. When the command executes supply the following information:

   - LDAP host Name: The host where the policy store is located.

     Note: It is recommended that you use the Policy Store directory, not the Identity Store.

   - LDAP Port: 389
   - Admin User: cn=orcladmin
   - Password: *admin_password*
   - LDAP sslDomain where your CA will be stored: for example, IDMDomain
   - Password to protect your CA wallet: *wallet_password*
   - Confirmed password for your CA wallet: *wallet_password*

This script performs the following tasks:

- Creates a Demo Signing CA wallet for use in the domain.
- Extracts the public Demo CA Certificate from the CA wallet.
- Uploads the wallet and the certificate to LDAP and stores them in the entry: cn=demoCA,Deployment_SSL_Domain
- Creates an access group in LDAP: cn=SSLDomains,cn=IDMDomain,cn=demoCA and grants that group administrative privileges to the parent container. All other entities are denied access. Add users to the group to give access. The Demo CA Certificate is now available for download by an anonymous or authenticated user.
- The Demo CA Wallet password is stored locally in an obfuscated wallet for future use. Its path is: *ORACLE_HOME*/credCA/castore

  As administrator, you must secure this wallet so that only SSL administrators can read it.

  The best place to locate the Certificate is in the Policy Store.

6.3.2 Configuring Oracle Virtual Directory to Accept Server Authentication Only Mode SSL Connections

Before configuring Oracle Virtual Directory for SSL, set the *ORACLE_HOME*, *ORACLE_INSTANCE* and *JAVA_HOME* variables. For example, you might set *ORACLE_HOME* to IDM_ORACLE_HOME, and set *ORACLE_INSTANCE* to OVD_ORACLE_INSTANCE.

Set JAVA_HOME to *JAVA_HOME*, and add *JAVA_HOME* to your *PATH* variable.

Start the SSL Configuration tool by issuing the command SSLServerConfig command which is located in the directory *ORACLE_COMMON_HOME*/bin directory.

For example:

```
ORACLE_COMMON_HOME/bin/SSLServerConfig.sh -component ovd
```

When prompted, enter the following information:

- LDAP Hostname: Central LDAP host, for example: `POLICYSTORE.mycompany.com`

  Note: It is recommended that you use the Policy Store directory, not the Identity Store.

- LDAP port: LDAP port, for example: `389`
- Admin user DN: `cn=orcladmin`
- Password: *`administrator_password`*
- sslDomain for the CA: for example, `IDMDomain`
- Password to protect your SSL wallet/keystore: *`password_for_local_keystore`*
- Enter confirmed password for your SSL wallet/keystore: *`password_for_local_keystore`*
- Password for the CA wallet: *`certificate_password`*. This is the one created in the previous procedure, "Generating a Certificate to be Used by the Identity Management Domain."
- Country Name 2 letter code: Two letter country code, such as `US`
- State or Province Name: State or province, for example: `California`
- Locality Name: Enter the name of your city, for example: `RedwoodCity`
- Organization Name: Company name, for example: `mycompany`
- Organizational Unit Name: Leave at the default
- Common Name: Name of this host, for example: `HOST1.mycompany.com`
- OVD Instance Name: for example, `ovd1`. If you need to determine what your OVD component name is, execute the command:

  ```
  ORACLE_INSTANCE/bin/opmnctl status
  ```

- Oracle instance name: Name of your Oracle instance, for example: `ovd1`
- WebLogic admin host: Host running the WebLogic Administration Server, for example:. `ADMINVHN.mycompany.com`
- WebLogic admin port: WebLogic Administration Server port, for example: `7001`
- WebLogic admin user: Name of your WebLogic administration user, for example: `weblogic`
- WebLogic password: *`password`*.
- SSL wallet name for OVD component [ovdks1.jks]: Accept the default

When asked if you want to restart your Oracle Virtual Directory component, enter `Yes`.

When asked if you would like to test your OVD SSL connection, enter `Yes`. Ensure that the test is a success.

Repeat for each Oracle Virtual Directory instance in the configuration.

6.3.3 Configuring Oracle Internet Directory to Accept Server Authentication Mode SSL Connections

If you plan to enable SSL Server Authentication Only Mode for your domain and have created a domain level SSL certificate as described in Section 6.3.1, "Generating a Certificate to be Used by the Identity Management Domain," you must perform the following to ensure that your Oracle Internet Directory instances are capable of accepting requests using this mode. You must configure each Oracle Internet Directory instance independently.

6.3.3.1 Prerequisites

Prior to running this command ensure that:

- Oracle Internet Directory is installed.
- Oracle Identity Management is installed on the host.
- Site certificate has been generated as described in Section 6.3.1, "Generating a Certificate to be Used by the Identity Management Domain."
- If you are using Windows, you have installed a UNIX emulation package such as Cygwin in order to run the scripts contained in this section. See `http://www.cygwin.com`.

6.3.3.2 Configuring Oracle Internet Directory for SSL

To enable Oracle Internet Directory to communicate using SSL Server Authentication Mode, perform the following steps on LDAPHOST1 and LDAPHOST2:

> **Note:** When you perform this operation, only the Oracle Internet Directory instance you are working on should be running.

1. Set the *ORACLE_HOME*, *ORACLE_INSTANCE* and *JAVA_HOME* variables. For example, on LDAPHOST1:
   - Set `ORACLE_HOME`.
   - Set `ORACLE_INSTANCE` to the Oracle instance directory.
   - Set `JAVA_HOME` to the Java home.
   - Set the `PATH` variable to include *JAVA_HOME*.
2. To enable SSL Server Authentication use the tool SSLServerConfig which is located in:

   ORACLE_COMMON_HOME`/bin`

   For example

   ```
   $ORACLE_COMMON_HOME/bin/SSLServerConfig.sh -component oid
   ```

3. When prompted, enter the following information:
   - LDAP Hostname: Central LDAP host, for example: `POLICYSTORE.mycompany.com`
   - LDAP port: For example: `389`
   - Admin user DN: `cn=orcladmin`
   - Password: *administrator_password*

- sslDomain for the CA: `IDMDomain` Oracle recommends that the SSLDomain name be the same as the Weblogic domain name to make reference easier.
- Password to protect your SSL wallet/keystore: *`password_for_local_keystore`*
- Enter confirmed password for your SSL wallet/keystore: *`password_for_local_keystore`*
- Password for the CA wallet: *`certificate_password`*. This is the one created in Section 6.3.1, "Generating a Certificate to be Used by the Identity Management Domain."
- Country Name 2 letter code: Two letter country code, such as `US`
- State or Province Name: State or province, for example: `California`
- Locality Name: Enter the name of your city, for example: `RedwoodCity`
- Organization Name: Company name, for example: `mycompany`
- Organizational Unit Name: Leave at the default
- Common Name: Name of this host, for example: `LDAPHOST1.mycompany.com`
- OID component name: Name of your Oracle Instance, for example: `oid1`. If you need to determine what your OID component name is, execute the command:

  `OID_ORACLE_INSTANCE``/bin/opmnctl status`

- WebLogic admin host: Host running the WebLogic Administration Server.
- WebLogic admin port: For example: `7001`
- WebLogic admin user: Name of your WebLogic administration user, for example: `weblogic`
- WebLogic password: *`password`*.
- AS instance name: Name of the Oracle instance, for example: `oid1`.
- SSL wallet name for OID component [oid_wallet1]: Accept the default
- Do you want to restart your OID component: `Yes`
- Do you want to test your SSL setup? `Yes`
- SSL Port of your OID Server: `3131`

Sample output:

```
Server SSL Automation Script: Release 11.1.1.4.0 - Production
Copyright (c) 2010 Oracle. All rights reserved.

Downloading the CA wallet from the central LDAP location...
>>>Enter the LDAP Hostname [SLC00DRA.mycompany.com]: POLICYSTORE.mycompany.com
>>>Enter the LDAP port [3060]: 3060
>>>Enter an admin user DN [cn=orcladmin]
>>>Enter password for cn=orcladmin:
>>>Enter the sslDomain for the CA [idm]: IDMDomain
>>>Enter a password to protect your SSL wallet/keystore:
>>>Enter confirmed password for your SSL wallet/keystore:
>>>Enter password for the CA wallet:
>>>Searching the LDAP for the CA usercertificate ...
Importing the CA certifcate into trust stores...
>>>Searching the LDAP for the CA userpkcs12 ...
```

```
Invoking OID SSL Server Configuration Script...
Enter attribute values for your certificate DN
>>>Country Name 2 letter code [US]:
>>>State or Province Name [California]:
>>>Locality Name(eg, city) []:Redwood
>>>Organization Name (eg, company) [mycompany]:
>>>Organizational Unit Name (eg, section) [oid-20110524015634]:
>>>Common Name (eg, hostName.domainName.com) [SLC00XXX.mycompany.com]:
The subject DN is
cn=SLC00DRA.mycompany.com,ou=oid-20110524015634,l=Redwood,st=California,c=US

Creating an Oracle SSL Wallet for oid instance...
/u01/oracle/products/access/idm/../oracle_common/bin
>>>Enter your OID component name: [oid1]
>>>Enter the weblogic admin server host [SLC00XXX.mycompany.com] ADMINVHN
>>>Enter the weblogic admin port: [7001]
>>>Enter the weblogic admin user: [weblogic]
>>>Enter weblogic password:
>>>Enter your AS instance name:[asinst_1] oid1
>>>Enter an SSL wallet name for OID component [oid_wallet1]
Checking the existence of oid_wallet1 in the OID server...
Configuring the newly generated Oracle Wallet with your OID component...
Do you want to restart your OID component?[y/n]y

Do you want to test your SSL set up?[y/n]y
>>>Please enter your OID ssl port:[3131] 3131
Please enter the OID hostname:[SLC00DRA.mycompany.com] LDAPHOST1.mycompany.com
>>>Invoking IDM_ORACLE_HOM/bin/ldapbind -h LDAPHOST1.mycompany.com -p 3131-U 2 -D
cn=orcladmin ...
Bind successful

Your oid1 SSL server has been set up successfully
```

Confirm that the script has been successful.

Repeat all the steps in this section for each Oracle Internet Directory instance.

6.3.4 Creating a Client Keystore

To enable Fusion Applications to communicate with the Identity Management domain using SSL Server Authentication Mode, you must generate a client certificate and provide it to the Fusion Applications Provisioning process. You must provide a keystore containing the Trust point used by the Identity Management domain to the Fusion Applications.

To generate a keystore containing a client certificate, perform the following steps on LDAPHOST1:

1. Set the `ORACLE_HOME` to the Oracle home directory.

   Set `JAVA_HOME` to *`JAVA_HOME`*.

   Ensure that *`JAVA_HOME`* is in your *`PATH`* variable.

2. To generate the certificate, use the tool `./SSLClientConfig.sh`, which is located in: *`ORACLE_COMMON_HOME`*`/bin`

   For example

   ```
   ./SSLClientConfig.sh -component cacert
   ```

As the command runs, enter the following values when prompted:

- LDAP Host Name: Name of the host where the policy store is located.
- LDAP Port: `389`
- LDAP User: `cn=orcladmin`
- Password: *`Password_for_cn=orcladmin`*
- SSL Domain: Domain name.
- Keystore Password: Enter a password to protect the keystore
- Confirm Password: Reenter the password.

This creates a file called `trust.jks` which must be provided to the Fusion Applications Provisioning process. After creating this certificate, you must delete the private key within this key. Use the following command:

```
keytool -delete -keystore trust.jks -alias testkey -storepass store_password
```

Oracle Fusion Applications provisioning uses this file to validate that the Identity Management installation is set up appropriately before provisioning takes place. In addition to this certificate, the keystore must also contain the certificate used by the load balancer for `SSO.mycompany.com`.

Before you start this procedure, obtain a copy of the certificate by using your browser. First access `https://SSO.mycompany.com:4443`, then follow the instructions to download the certificate to a file. (Each browser does this differently.)

After you have obtained the certificate, load it into the keystore using the following command:

```
keytool -import -v -noprompt -trustcacerts -alias "OIM" -file loadbalancer.cer
-keystore ORACLE_HOME/rootCA/keystores/common/trust.jks
```

where *`ORACLE_HOME`* is the Oracle home directory and `loadbalancer.cer` is the name of the file where the load balancers SSL certificate is stored. Once created, the keystore should be moved to the domain keystore location for consistency.

6.4 Using Oracle Virtual Directory as an Identity Store

Identity Management Provisioning installs a single node environment with Oracle Internet Directory as the Identity Store in Oracle Access Manager. If you want to use Oracle Virtual Directory as the Identity Store instead of Oracle Internet Directory, proceed as follows:

1. Log in to the OAM Console, `http://`*`host`*`:`*`port`*`/oamconsole`, as the OAM administrator.
2. Click on the **System Configuration** tab at the top.
3. Navigate to **Data Sources -> User Identity Stores -> OIMIDStore**.
4. In the **Store Type** dropdown menu, select **OVD: Oracle Virtual Directory**
5. In the **Location** field, provide the correct port number for OVD. Usually it is `6501`. Leave the **Host** field unchanged
6. Click **Test Connection** at the top right corner to validate the change.
7. If you get the **Connection to the User Identity Store successful!** message, click **Apply** to commit the change.

8. Restart the WebLogic Administration Server and the OAM Managed Server or use the `stopall` and `startall` scripts to restart the environment.

6.5 Passing Configuration Properties File to Oracle Fusion Applications

Oracle Fusion Applications requires a property file which details the IDM deployment. After provisioning, this file can be found at the following location:

SHARED_CONFIG_DIR`/fa/idmsetup.properties`
where *SHARED_CONFIG_DIR* is the **Shared Configuration Location** you specified on the Install Location Configuration Page.

6.6 Post-Provisioning Steps for Oracle Identity Manager

Perform the following task to ensure that Oracle Identity Manager works correctly after provisioning.

- Section 6.6.1, "Add an Oracle Identity Manager Property"

6.6.1 Add an Oracle Identity Manager Property

As a workaround for a bug in the Identity Management Provisioning tools, you must add an Oracle Identity Manager property. Perform the following steps:

1. Log in to the WebLogic Console.
2. Navigate to **Environment -> Servers**.
3. Click **Lock and Edit**.
4. Click on the server **WLS_OIM1**.

   Click on the managed WebLogic server.
5. Click on the **Server Start** subtab
6. Add the following to the **Arguments** field:

   ```
   -Djava.net.preferIPv4Stack=true
   ```
7. Click **Save**.
8. Repeat Steps 4-7 for the managed server **WLS_OIM2**.
9. Click **Activate Changes**.
10. Restart the managed servers WLS_OIM1 and WLS_OIM2, as described in Section 16.1, "Starting and Stopping Components."

    Restart the managed WebLogic server.

6.7 Post-Provisioning Steps for Oracle Access Manager

Perform the tasks in the following sections:

6.7.1 Updating Existing WebGate Agents

Update the OAM Security Model of all WebGate profiles, with the exception of Webgate_IDM and Webgate_IDM_11g, which should already be set

To do this, perform the following steps:

1. Log in to the Oracle Access Manager Console as the administration user.

2. Click the **System Configuration** tab.
3. Expand **Access Manager Settings - SSO Agents**.
4. Click **OAM Agents** and select **Open** from the **Actions** menu.
5. In the Search window, click **Search**.
6. Click an Agent, for example: **IAMSuiteAgent**.
7. Set the Security value to the security model in the **OAM Configuration** screen of the Identity Management Provisioning Wizard. Select **Simple** for the security model, except on AIX, where only **Open** mode is supported.

   Click **Apply**.
8. Restart the managed WebLogic server.

6.7.2 Creating Oracle Access Manager Policies for WebGate 11*g*

In order to allow WebGate 11*g* to display the credential collector, you must add `/oam` to the list of public policies.

Proceed as follows:

1. Log in to the OAM console.
2. Select the **Policy Configuration** tab.
3. Expand **Application Domains - IAM Suite**
4. Click **Resources**.
5. Click **Open**.
6. Click **New resource**.
7. Provide the following values:
   - **Type**: `HTTP`
   - **Description**: `OAM Credential Collector`
   - **Host Identifier**: `IAMSuiteAgent`
   - **Resource URL**: `/oam`
   - **Protection Level**: `Unprotected`
   - **Authentication Policy**: `Public Policy`
8. Leave all other fields at their default values.
9. Click Apply.

6.8 Post -Provisioning Steps for Oracle Identity Federation

Perform the tasks in the following sections:

6.8.1 Start OIF Managed Server

Start the managed WebLogic server, as follows:

1. Stop all the components.

2. Update the Oracle Identity Federation Property File `oif_startup.conf` to automatically start Oracle Identity Federation. To do this, edit the file `oif_startup.conf`.

   Edit the file so that it looks like this:

```
#
# OIF is enabled OOTB for Shared IDM
#
# OIF_ENABLED indicates whether or not OIF should be started/stopped
# as part of the startoif.sh/stopoif.sh scripts. Valid values are true or false
# If false, the OIF will not be started or stopped
OIF_ENABLED=true
# OPMN_EMAGENT_MANAGED_BY_OIF_SCRIPT indicates whether or not OPMN and
# the EMAgent components for the OIM domain should be started, when OIF is
enabled.
# Valid values are true or false. If false, OPMN and the EMAgent components
will not
# be started or stopped when OIF is enabled.
# If OIF is disabled, OPMN and the EMAgent components will not be started or
stopped
OPMN_EMAGENT_MANAGED_BY_OIF_SCRIPT=true
```

   Save the file.

3. Start all the components.

6.8.2 Integrating Oracle Identity Federation with Oracle Access Manager 11*g*

In Service Provider (SP) mode, Oracle Access Manager delegates user authentication to Oracle Identity Federation, which uses the Federation Oracle Single Sign-On protocol with a remote Identity Provider. Once the Federation Oracle Single Sign-On flow is performed, Oracle Identity Federation will create a local session and then propagates the authentication state to Oracle Access Manager, which maintains the session information.

This section provides the steps to integrate OIF with OAM11g in authentication mode and SP mode.

This section contains the following topics:

- Section 6.8.2.1, "Updating the Oracle Identity Federation Authentication Scheme in Oracle Access Manager."

6.8.2.1 Updating the Oracle Identity Federation Authentication Scheme in Oracle Access Manager

Oracle Access Manager ships with an Oracle Identity Federation Authentication Scheme. This scheme needs to be updated before it can be used. To update the scheme, log in to the OAM console as the OAM administration user.

Then perform the following steps:

1. Click the **Policy Configuration** tab.
2. Expand **Authentication Schemes** under the Shared Components tree.
3. Select **OIFScheme** from under the Authentication Schemes and then select **Open** from the menu.
4. On the Authentication Schemes page, provide the following information
   - **Challenge URL**: `https://SSO.mycompany.com:443/fed/user/spoam11g`

- **Context Type**: Select **external** from the list.

Accept the defaults for all other values

5. Click **Apply** to update the `OIFScheme`.

7

Troubleshooting Identity Management Provisioning

This chapter describes common problems that you might encounter when using Identity Management Provisioning and explains how to solve them.

In addition to this chapter, review the *Oracle Fusion Middleware Error Messages Reference* for information about the error messages you may encounter.

This chapter contains the following sections:

7.1 Getting Started with Troubleshooting

This section describes how to use the log files and how to recover from provisioning failures. It contains the following topics:

7.1.1 Using the Log Files

If you are monitoring provisioning using the wizard, from any phase screen, click on the icon under the **Log** field to see the logs for the current phase. A new window opens showing the logs. The logs are searchable using the search box at the top of this new window. The log window does not refresh on its own, so click on the refresh button besides the search box at the top of this window to refresh the logs.

To check why a phase failed when the wizard is not running, check the corresponding logs files present under the logs directory. On Linux, this is `IDMTOP/config/provisioning/logs/hostname`. On Windows, this is `IDMTOP\config\provisioning\logs\hostname`.

`IDMTOP` is the **Software Installation Location** directory you specified on the Installation and Configuration page when you created the provisioning profile. See Section 4.2.7, "Install Location Configuration Page."

7.1.2 Recovering From Identity Management Provisioning Failure

Identity Management Provisioning does not have any backup or recovery mechanism, so you must to start from the beginning if case of a failure.

If you perform a workaround that requires you to rerun Identity Management Provisioning, you must clean up the environment before rerunning it. Proceed as follows:

1. Stop all running services and servers using *idmtop*`\config\scripts\stopall.bat` on Windows or *idmtop*`/config/scripts/stopall.sh` on UNIX. Then remove the *idmtop* folder. If you used a Shared Configuration Location, as described in Section 4.2.7, "Install Location Configuration Page," delete that directory.
2. Remove previously created Identity Management directories from the `PATH` environment variable, including `DIR`, `APP`, and the OHS Oracle home.
3. Run RCU to drop all schema before the next attempt.

   Note: While dropping schema using RCU, ensure that you explicitly select the ODS schema so that it also gets dropped. It is NOT selected by default, unlike other schema.

4. Reboot the machine to ensure that all server instances are stopped.

7.2 Resolving Common Problems

This section describes common problems and solutions. It contains the following topics:

- Section 7.2.1, "Missing ODSM Instance Directory on Second Node"
- Section 7.2.2, "Null Error Occurs When WebLogic Patches Are Applied"
- Section 7.2.3, "Identity Management Patch Manager progress Command Shows Active Session After Provisioning"
- Section 7.2.4, "Spurious OPatch Error Messages Printed to Log During Install Phase"
- Section 7.2.5, "Identity Management Provisioning Wizard Hangs (Linux and UNIX)"
- Section 7.2.6, "Provisioning Fails During Install Phase (Linux)"
- Section 7.2.7, "Identity Management Provisioning Wizard install Fails Due to Oracle Internet Directory Configuration Failure (Windows)"
- Section 7.2.8, "Provisioning Fails if Installer Repository Location Is a UNC Path (Windows)"
- Section 7.2.9, "Identity Management Provisioning Fails During Preconfigure Phase (Windows)"
- Section 7.2.10, "Cannot Log In to the Oracle Identity Federation Server (Windows)"
- Section 7.2.11, "Error When Starting Oracle Access Manager Managed Servers (Windows)"

7.2.1 Missing ODSM Instance Directory on Second Node

Problem

After you run the Identity Management Provisioning Wizard, only one instance directory for Oracle Directory Services Manager is installed.

Solution

The absence of the ODSM instance directory on the second node does not result in any loss of function.

7.2.2 Null Error Occurs When WebLogic Patches Are Applied

Problem

During IDM provisioning, patches are applied to all products provisioned, including WebLogic. This entails running the Smart Update `bsu` command. This command may fail without producing a detailed error message.

Cause

In this case, the failure is likely caused by directory paths that are longer than what the `bsu` command supports. You can verify this by running the `bsu` command manually, passing it the `-log` option, and looking for a stack trace containing a message such as the following:

```
java.lang.IllegalArgumentException:
Node name
?a?very?long?path?which?may?cause?problems?leading?to?an?IDMTOP?products?dir?utils
?bsu?cache_dir too long
```

For more information, see the chapter "Using the Command Line Interface" in *Oracle Smart Update Applying Patches to OracleWebLogic Server*.

Solution

When planning the IDM deployment, ensure that the `IDM_TOP` path is 45 characters or fewer in length.

7.2.3 Identity Management Patch Manager progress Command Shows Active Session After Provisioning

Problem

If you run the Identity Management Patch Manager `progress` command after Identity Management Provisioning completes, the output shows an active session specific to Identity Management Provisioning, which is listed as ACTIVE, and contains a set of PLANNED steps.

Solution

You can safely ignore this output. The provisioning-driven patch session is complete, and all steps which needed to run have run. Creating a new patch session will silently replace this special session without error.

7.2.4 Spurious OPatch Error Messages Printed to Log During Install Phase

Problem

During the install phase of provisioning, you may see a message `Starting binary patching for all-binary-patch components ...`, followed by a series of OPatch failure messages prefaced with the string `prepatch` within the provisioning log. These errors contain the string `Failed to load the patch object`.

Solution

These messages are harmless and can be safely ignored.

7.2.5 Identity Management Provisioning Wizard Hangs (Linux and UNIX)

Problem

The IdentityManagement Deployment Wizard hangs. Neither the **Next** nor the **Back** button is active.

Cause

This problem is due to stale NFS file handles.

Solution

On Linux or UNIX, issue the following command:

```
df -k
```

Record the output of the df command, even if it is successful, in case further analysis is necessary. For example, take a screenshot.

If the `df` command hangs or is unsuccessful, work with your system administrator fix the NFS problem.

After the NFS problem has been resolved and the `df` command finishes successfully, run provisioning again.

7.2.6 Provisioning Fails During Install Phase (Linux)

Problem

Provisioning fails during the Install phase.

Cause

Some 32-bit libraries such as `crt1.o` are missing.

Solution

There are two ways to fix this. Do one of the following:

- Copy the 32 -bit libraries `gcrt1.o`, `crtn.o`, `crti.o`, `crt1.o`, `Scrt1.o`, and `Mcrt1.o` from `/usr/lib/` on another machine running the same version.
- Install the missing package `glibc-devel.i686`

7.2.7 Identity Management Provisioning Wizard install Fails Due to Oracle Internet Directory Configuration Failure (Windows)

Problem

The Oracle Internet Directory configuration fails on the Windows 2008 Server R2 +SP1, causing the IdentityManagement Provisioning Wizard to fail.

Solution

After the installation of the Identity Management Provisioning Wizard has finished:

1. Edit the `sqlnet.ora` file in the Oracle Internet Directory environment folder

`%ORACLE_HOME%\network\admin`

Set the `ADR_BASE` parameter to a folder other than the Oracle home, for example,

`C:\temp.`

2. If it does not exist already, add an `sqlnet.ora` file to that folder and ensure that it contains the `ADR_BASE` parameter, set to the same value as in Step 1.

7.2.8 Provisioning Fails if Installer Repository Location Is a UNC Path (Windows)

Problem

Provisioning fails at install time on Microsoft Windows with an error message similar to this:

```
[logStatus] STATE=BUILD_STARTED!TIMESTAMP=2013-03-26 04:56:28
MDT!TARGET=installwls!
CATEGORY=Weblogic!DOMAIN=NONE!HOSTNAME=slc02jqf!PRODUCT
FAMILY=orchestration!PRODUCT=orchestration!TASK=install!TASKID=orchestration.orche
stration.NONE.installwls.
NONE!MESSAGE=Starting install for weblogic for
C:\idmtop/products/dir!DETAIL=!BUILDFILE=c:\idminstaller\Oracle_
IDMLCM1\provisioning\idm-provisioning-build\idm-commonbuild.
xml!LINENUMBER=33!
[2013-03-26T04:56:30.693-06:00] [runIDMProvisioning-install]
[NOTIFICATION]
[] [runIDMProvisioningt-install] [tid: 12] [ecid:
0000JqaLtN_B1FH5Ivt1if1HKNuO000003,0] [exec]
java.lang.ClassNotFoundException:
com.bea.cie.gpr.internal.model.DelegateHomeListHelper
```

Cause

This error occurs because you are accessing the Software Repository using a UNC path. That is, you are using a path of the form \\server\share.

Solution

To resolve this issue, map the share to a local disk and then specify the repository location using the local disk path.

7.2.9 Identity Management Provisioning Fails During Preconfigure Phase (Windows)

Problem

When you attempt to perform provisioning, using the provisioning response file, it fails during the Preconfigure phase, with an error similar to this:

```
TASKID=orchestration.orchestration.BUILD_ERROR.NONE.installNodeManager!MESSAGE
=Error exit code 1069 from C:\Windows\system32\sc.exe!DETAIL=Error exit code
1069 from C:\Windows\system32\sc.exe!
```

Cause

Node Manager fails to start due to a password error.

Solution

Perform the steps described in Section 3.6, "Setting Up Required User (Windows)."

7.2.10 Cannot Log In to the Oracle Identity Federation Server (Windows)

Problem

On a Windows system, after performing Identity Management Provisioning, you cannot log in to the Oracle Identity Federation server even though it is running.

Solution

Make sure that the Oracle Identity Federation server is using IPv4.

To verify this, look in the file *setDomainEnv.cmd*,

Locate the line `EXTRA_JAVA_PROPERTIES` and add the following to the entry if it is not already present:

```
-Djava.net.preferIPv6Addresses -DuseIPv6Address=false
-Djava.net.preferIPv6Addresses=false
```

Save the file and restart the Oracle Identity Federation servers.

7.2.11 Error When Starting Oracle Access Manager Managed Servers (Windows)

Problem

On Windows, after performing Identity Management Provisioning, when you start the OAM managed servers, you see an error similar to this:

```
Caused by: java.net.SocketException: Address family not supported by protocol
family: bind
```

Solution

Edit `setDomainEnv.cmd` and add the following parameters to the environment variable `EXTRA_JAVA_PROPERTIES`:

```
-DuseIPv6Address=false -Djava.net.preferIPv6Addresses=false
```

Restart the Administration Server and all Managed Servers that are running.

7.3 Using My Oracle Support for Additional Troubleshooting Information

You can use My Oracle Support (formerly MetaLink) to help resolve Oracle Fusion Middleware problems. My Oracle Support contains several useful troubleshooting resources, such as:

- Knowledge base articles
- Community forums and discussions
- Patches and upgrades
- Certification information

Note: You can also use My Oracle Support to log a service request.

You can access My Oracle Support at https://support.oracle.com.