Oracle® Identity Manager

Tools Reference

Release 9.1.0.2

E14763-02

June 2009

ORACLE®

Oracle Identity Manager Tools Reference, Release 9.1.0.2

E14763-02

Primary Author: Debapriya Datta

Contributing Author: Lyju Vadassery

Contents

Preface ix

Audience ix
Documentation Accessibility ix
Related Documents x
Documentation Updates x
Conventions x
Online Help x

1 Introduction to the Integration

1.1 The Integration Problem 1-1
1.2 The Oracle Identity Manager Solution 1-1
1.3 About Adapters 1-2
1.4 Tabs of the Adapter Factory Form 1-3
1.4.1 Adapter Tasks 1-3
1.4.2 Execution Schedule 1-3
1.4.3 Resources 1-4
1.4.4 Variable List 1-4
1.4.5 Usage Lookup 1-4
1.4.6 Responses 1-4

2 Getting Started

2.1 Overview of Oracle Identity Manager Configuration 2-1
2.2 Configuring Oracle Identity Manager to Reference JAR and Class Files 2-2
2.3 Installing the Remote Manager 2-2
2.4 Adding the Trust Relation 2-2

3 Creating Adapters

3.1 Overview of Adapter Creation 3-1
3.2 Defining Adapters 3-1
3.3 Disabling and Re-enabling Adapters 3-2
3.4 About Adapter Variables 3-3
3.4.1 Creating an Adapter Variable 3-3
3.4.2 Modifying an Adapter Variable 3-4
3.4.3 Deleting an Adapter Variable 3-5
3.5 Creating Adapter Tasks 3-5

3.5.1 Creating a Java Task ... 3-7
3.5.2 To Create a Remote Task ... 3-10
3.5.3 To Create a Stored Procedure Task ... 3-12
3.5.4 To Create a Utility Task ... 3-14
3.5.5 To Create an Oracle Identity Manager API Task ... 3-16
3.5.6 Reassigning the Value of an Adapter Variable ... 3-17
3.5.7 Adding an Error Handler Task ... 3-19
3.5.8 Creating a Logic Task ... 3-20
3.6 Modifying Adapter Tasks ... 3-22
3.7 Changing the Order and Nesting of Tasks ... 3-23
3.8 Deleting Adapter Tasks ... 3-24
3.9 Working with Responses ... 3-24
3.9.1 To Create a Response ... 3-25
3.9.2 To Modify a Response ... 3-25
3.9.3 To Delete a Response ... 3-26
3.10 Scheduling Rule Generators and Entity Adapters ... 3-26
3.10.1 Scheduling Rule Generators and Entity Adapters ... 3-27

4 About Process Task Adapters

4.1 Introduction to Processes and Process Tasks ... 4-1
4.2 How a Process Task Adapter Works ... 4-2
4.3 Attaching Process Task Adapters to Process Tasks ... 4-3
4.4 Removing Process Task Adapters from Process Tasks ... 4-6
4.4.1 To Remove a Process Task Adapter from a Process Task ... 4-6

5 Applying Task Assignment Adapters

5.1 Overview ... 5-1
5.2 Attaching Task Assignment Adapters to Process Tasks ... 5-2
5.2.1 To Attach a Task Assignment Adapter to a Process Task ... 5-2
5.3 Removing Task Assignment Adapters from Process Tasks ... 5-5
5.3.1 To Remove a Task Assignment Adapter from a Process Task ... 5-5

6 Understanding Rule Generators

6.1 Overview ... 6-1
6.2 Mapping Rule Generator Adapter Variables ... 6-2
6.3 Associating Rule Generators with Processes ... 6-5
6.4 Removing Rule Generators from Form Fields ... 6-5

7 Using Prepopulate Adapters

7.1 Overview ... 7-1
7.2 Attaching Prepopulate Adapters to Form Fields ... 7-2
7.3 Removing Prepopulate Adapters from Form Fields ... 7-5

8 Managing Entities

9 Compiling Adapters

9.1 Automatic Compilation of Adapters 9-1
9.2 Compiling Adapters Manually 9-1

10 Exporting and Importing Adapters

11 Creating and Testing a Remote Manager IT Resource

11.1 Postinstallation Configuration 11-1
11.2 To Create and Test a Remote Manager IT Resource 11-3

12 SPML Web Service

12.1 Introduction to the SPML Web Service 12-1
12.1.1 Functional Architecture of the SPML Web Service 12-2
12.2 Provisioning Operations Supported by the SPML Web Service 12-3
12.3 Deploying the SPML Web Service 12-6
12.3.1 Deploying the SPML Web Service on Oracle WebLogic Server 12-7
12.3.2 Deploying the SPML Web Service on IBM WebSphere Application Server 12-8
12.3.3 Deploying the SPML Web Service on JBoss Application Server 12-8
12.3.4 Deploying the SPML Web Service on Oracle Application Server 12-8
12.4 Enabling Security by Using Oracle Web Services Manager and Then Deploying the SPML Web Service 12-10
12.4.1 Configuring the Oracle WSM Server Agent 12-11
12.4.1.1 Adding a Server Agent 12-11
12.4.1.2 Defining a Policy for the Server Agent 12-11
12.4.1.3 Injecting the Server Agent 12-12
12.4.1.4 Deploying the SPML Web Service 12-14
12.4.2 Configuring the Oracle WSM Gateway 12-14
12.4.2.1 Registering the Oracle WSM Gateway 12-14
12.4.2.2 Registering the SPML Web Service with the Gateway 12-14
12.4.2.3 Adding a Custom Policy to the Gateway 12-15
12.4.2.4 Deploying the SPML Web Service 12-16
12.4.2.5 Viewing the WSDL File 12-16
12.5 Postdeployment Tasks 12-16
12.6 Enabling SSL Communication 12-16
12.6.1 JBoss Application Server 12-17
12.6.1.1 Prerequisites 12-17
12.6.1.2 SSL Certificate Setup 12-17
12.6.2 Oracle WebLogic Server 12-18
12.6.2.1 Prerequisites 12-18
12.6.2.2 SSL Certificate Setup 12-19
12.6.3 IBM WebSphere Application Server 12-21
12.6.3.1 Prerequisites 12-21
12.6.3.2 SSL Certificate Setup 12-21
12.6.4 Oracle Application Server 12-22

12.6.4.1 Prerequisites 12-22
12.6.4.2 SSL Certificate Setup 12-22
12.6.5 Enabling SSL for HTTP Communication to Oracle HTTP Server 12-24
12.6.5.1 Exporting Certificate 12-24
12.7 Developing the Client for the SPML Web Service 12-24
12.7.1 Supported SPML Operations 12-25
12.7.2 Authentication 12-26
12.7.3 Fields Included in SPML Requests 12-26
12.7.4 Structure of the SOAP Header 12-29
12.7.5 Sample SOAP SPML Message 12-31

13 Segregation of Duties (SoD) in Oracle Identity Manager

13.1 SoD Implementation in Oracle Identity Manager 13-1
13.2 SoD Validation Process in Oracle Identity Manager 13-3
13.3 Implementing and Enabling SoD 13-3
13.3.1 Creating the SIL Database Schema 13-4
13.3.2 Installing and Configuring the Oracle Identity Manager Connector 13-4
13.3.3 Copying Files Required by the SIL Providers 13-4
13.3.3.1 Copying Files Required by the OAACG SIL Provider 13-5
13.3.3.2 Copying Files Required by the SAP GRC SIL Provider 13-5
13.3.4 Configuring the SoD Engine 13-6
13.3.4.1 Configuring Oracle Application Access Controls Governor 13-6
13.3.4.2 Configuring SAP GRC 13-6
13.3.5 Deploying the SIL and SIL Providers 13-9
13.3.5.1 Creating an IT Resource to Hold Information about the SoD Engine 13-9
13.3.5.2 Running the Registration Script and Providing Registration Information 13-10
13.3.5.3 Recording the Names of the System Types 13-16
13.3.5.4 Deploying the SIL_HOME Directory in a Clustered Environment 13-17
13.3.6 Enabling SSL Communication Between the SoD engine and Oracle Identity Manager ... 13-17
13.3.6.1 Enabling SSL Communication Between Oracle Application Access Controls Governor and Oracle Identity Manager 13-18
13.3.6.2 Enabling SSL Communication Between SAP GRC and Oracle Identity Manager 13-19
13.3.7 Enabling SoD 13-19
13.3.8 Enabling Logging for SoD-Related Events 13-20
13.4 Configuring Connectors for SoD 13-21
13.4.1 Addressing Prerequisites 13-21
13.4.2 Creating the Transformation Layer 13-22
13.4.3 Modifying the Registration XML File 13-22
13.4.4 Configuring the Provisioning and Approval Workflows for SoD 13-23
13.4.4.1 Modifying the Approval Workflow for SoD 13-24
13.4.4.2 Modifying the Provisioning Workflow for SoD 13-31
13.4.5 Marking Child Process Form Tables That Hold Entitlement Data 13-34
13.4.6 Registering the New Target System 13-34
13.5 Creating SIL Providers 13-35
13.5.1 Addressing Prerequisites 13-35

13.5.2 Implementing the Interfaces for the Provider 13-35
13.5.3 Modifying the Registration XML File for the New SoD Engine 13-35
13.5.4 Registering the New SIL Provider 13-36

14 Using Entitlement Data

14.1 Available Entitlements and Assigned Entitlements 14-2
14.2 Entitlement Data Capture Process 14-2
14.2.1 Capture of Data About Available Entitlements 14-2
14.2.2 Capture of Data About Assigned Entitlements 14-2
14.3 Configuring the Oracle Application Server Installation to Use This Feature 14-4
14.4 Marking Entitlement Attributes on Child Process Forms 14-4
14.5 Configuring Scheduled Tasks for Working with Entitlement Data 14-7
14.5.1 Entitlement List 14-7
14.5.2 Entitlement Assignments 14-8
14.5.3 Entitlement Updations 14-8
14.6 Disabling the Capture of Modifications to Assigned Entitlements 14-8
14.7 Entitlement-Related Reports 14-8
14.7.1 Entitlement Access List 14-9
14.7.2 Entitlement Access List History 14-9
14.7.3 User Resource Entitlement 14-9
14.7.4 User Resource Entitlement History 14-9
14.8 Archiving Data Stored in the ENT_ASSIGN_HIST Table 14-9
14.8.1 Creating a Tablespace to Store Archived Entitlement Data 14-10
14.8.2 Running the Entitlement Archival Utility 14-10

15 Bulk Load Utility

15.1 Features of the Bulk Load Utility 15-1
15.2 Installing the Bulk Load Utility 15-2
15.2.1 Scripts That Constitute the Utility 15-3
15.2.2 Options Offered by the Utility 15-3
15.3 Temporary Tables Used During a Bulk Load Operation 15-3
15.4 Loading OIM User Data 15-4
15.4.1 Creating a Tablespace for Temporary Tables 15-5
15.4.2 Creating a Datafile in the Oracle Identity Manager Tablespace 15-5
15.4.3 Setting a Default Password for OIM Users Added by the Utility 15-6
15.4.4 Creating the Input Source for the Bulk Load Operation 15-6
15.4.4.1 Using CSV Files As the Input Source 15-7
15.4.4.2 Creating Database Tables As the Input Source 15-8
15.4.5 Determining Values for the Input Parameters of the Utility 15-9
15.4.6 Running the Utility 15-10
15.4.7 Monitoring the Progress of the Operation 15-11
15.4.7.1 Data Recorded During the Operation 15-11
15.4.7.2 Querying the OIM_BLKLD_LOG Table for Progress and Error Messages 15-12
15.4.8 Handling Exceptions Recorded During the Operation 15-12
15.4.9 Fixing Exceptions and Reloading Data Records 15-13
15.4.10 Verifying the Outcome of the Bulk Load Operation 15-14

15.4.11 Gathering Performance Data from the Bulk Load Operation 15-14
15.4.12 Cleaning Up After a Bulk Load Operation 15-15
15.4.13 Generating an Audit Snapshot 15-15
15.5 Loading Account Data 15-16
15.5.1 Creating a Tablespace for Temporary Tables 15-17
15.5.2 Creating a Datafile in the Oracle Identity Manager Tablespace 15-17
15.5.3 Creating the Input Source for the Bulk Load Operation 15-17
15.5.3.1 Using CSV Files As the Input Source 15-18
15.5.3.2 Creating Database Tables As the Input Source 15-18
15.5.4 Determining Values for the Input Parameters of the Utility 15-19
15.5.5 Running the Utility 15-21
15.5.6 Monitoring the Progress of the Operation 15-21
15.5.6.1 Data Recorded During the Operation 15-21
15.5.6.2 Querying the OIM_BLKLD_LOG Table for Progress and Error Messages 15-22
15.5.7 Handling Exceptions Recorded During the Operation 15-23
15.5.8 Fixing Exceptions and Reloading Data Records 15-23
15.5.9 Verifying the Outcome of the Bulk Load Operation 15-24
15.5.10 Gathering Performance Data from the Bulk Load Operation 15-24
15.5.11 Cleaning Up After a Bulk Load Operation 15-25
15.5.12 Generating an Audit Snapshot 15-25

A Reference for Design Console Users

B Sample SPML Messages

Index

Preface

This guide provides information that can be applied when creating adapters, assigning and removing process tasks, and compiling, importing, and exporting adapters.

Audience

This guide is intended for users of the Oracle Identity Manager Design Console. The information in this guide can be used by developers, who are responsible for creating adapters, and by Oracle Identity Manager administrators, who attach these adapters to process tasks, forms that are predefined in Oracle Identity Manager, and user-created forms.

Documentation Accessibility

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

Deaf/Hard of Hearing Access to Oracle Support Services

To reach Oracle Support Services, use a telecommunications relay service (TRS) to call Oracle Support at 1.800.223.1711. An Oracle Support Services engineer will handle technical issues and provide customer support according to the Oracle service request process. Information about TRS is available at

http://www.fcc.gov/cgb/consumerfacts/trs.html, and a list of phone numbers is available at http://www.fcc.gov/cgb/dro/trsphonebk.html.

Related Documents

For more information, see the other documents in the Oracle Identity Manager documentation set for this release.

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager documentation set, visit Oracle Technology Network at

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

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), and names of files, directories, attributes, and parameters.

Online Help

Oracle Identity Manager comes equipped with a suite of online Help systems, designed to assist you with locating relevant information when you need it. The various books within the Help system library are available using the Help menu (located in the main screen). To open a particular book, select it from the Help menu.

In addition, Oracle Identity Manager provides content-sensitive Help for a number of forms. The contents of the content-sensitive Help topic reflect the form that is active within the Oracle Identity Manager main screen. To launch a context-sensitive Help topic for a particular form, ensure that it is active. Then, press F1.

Note: In addition to context-sensitive Help, the Oracle Identity Manager online Help system can also be invoked by pressing the F1 key.

1 Introduction to the Integration

This chapter describes the challenges of integrating access rights management applications with other software solutions, and the solution that Oracle Identity Manager offers. It discusses the following topics:

- The Integration Problem
- The Oracle Identity Manager Solution
- About Adapters
- Tabs of the Adapter Factory Form

1.1 The Integration Problem

An access rights management application cannot be successful today unless it can be integrated with other software solutions. Not only are there many resources, but also there is no single integration standard for connecting to these resources.

One way to tackle this challenge is by using the common functionality that is supported by all the integrations. To do this, you need developers who can write this code. In addition, every time an existing software resource is modified, or a new one is added, you must write more code.

1.2 The Oracle Identity Manager Solution

The Adapter Factory is a code-generation tool provided by Oracle Identity Manager. It helps you create Java classes, known as adapters.

An adapter provides the following benefits:

- It extends the internal logic and functionality of Oracle Identity Manager.
- It interfaces with any software resource, by connecting to that resource by using the API of the resource.
- It enables the integration between Oracle Identity Manager and an external system.
- It can be generated without manually writing code.
- It is lightweight and specific to your needs.
- It can be maintained easily because all of the definitions for the adapter are stored in a repository. This repository can be edited through a GUI.
- One Oracle Identity Manager user can retain the domain knowledge about the integration, while another user can maintain the adapter.

- It can be modified and upgraded efficiently.

1.3 About Adapters

As stated earlier, an adapter is a Java class created by an Oracle Identity Manager user through the Adapter Factory. In addition, it is an aggregation of atomic function calls in a logical flow. These atomic steps are known as adapter tasks.

> **Note:** Oracle Identity Manager can connect to external systems such as databases and directory servers by using Java APIs for JDBC and LDAP. In addition, for all other APIs, such as C, C++, VB, and COM/DCOM, you can create a Java wrapper so that Oracle Identity Manager can communicate with the API directly.

There are five types of adapters:

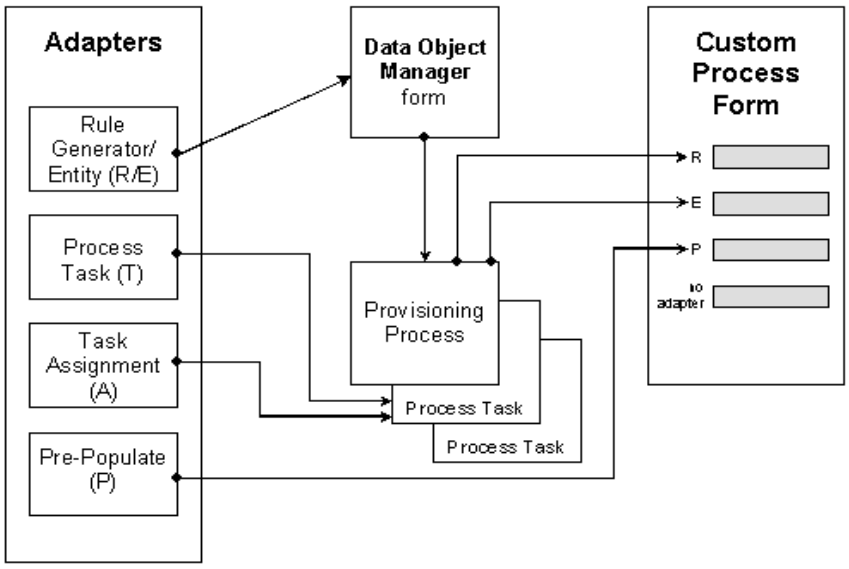
- A process task adapter, which allows Oracle Identity Manager to automate the completion of a process task.
- A task assignment adapter, which enables Oracle Identity Manager to automate the assignment of a process task to a user or group.
- A rule generator, which incorporates business rules to the fields of either an Oracle Identity Manager form or a user-defined form (created by using the Form Designer form), so these fields can be populated automatically and saved to the Oracle Identity Manager database.

> **Note:** For more information about the Form Designer form, refer to *Oracle Identity Manager Design Console Guide*

- A pre-populate adapter, which is a specific type of rule generator adapter that can be attached to a user-created form field. The data generated by this type of adapter can appear either automatically or manually. In addition, it uses criteria that enable Oracle Identity Manager to determine which pre-populate adapter will be applied to the designated form field. It then populates the designated form field without saving this information to the Oracle Identity Manager database.
- An entity adapter, which is attached to an Oracle Identity Manager or user-created form field. Oracle Identity Manager triggers an entity adapter on preinsert, preupdate, predelete, postinsert, postupdate, or postdelete. Once this occurs, the field to which the adapter is attached is populated automatically and saved to the Oracle Identity Manager database.

Figure 1–1 illustrates the functionality of five different types of adapters.

Figure 1–1 Adapter Functionality



These five types of adapters will be explained in greater detail in the chapters that follow.

1.4 Tabs of the Adapter Factory Form

The Adapter Factory form in the Design Console contains the following tabs:

- Adapter Tasks
- Execution Schedule
- Resources
- Variable List
- Usage Lookup
- Responses

Each of these tabs is explained in greater detail in the following sections.

1.4.1 Adapter Tasks

In the Adapter Tasks tab, you can create and manage the atomic function calls of an adapter. These function calls are known as adapter tasks.

1.4.2 Execution Schedule

The Execution Schedule tab lets you specify when you want Oracle Identity Manager to trigger a rule generator or an entity adapter. You can schedule Oracle Identity Manager to run a rule generator (Adapter Type *R*) on preinsert and/or preupdate. You can also configure Oracle Identity Manager to execute an entity adapter (Adapter Type *E*) on preinsert, preupdate, predelete, postinsert, postupdate, or postdelete.

Caution: **Process task adapters and task assignment adapters, which are attached to process tasks, are triggered once the process task's status becomes *Pending*. Therefore, you do not specify when Oracle Identity Manager will trigger these types of adapters, Oracle Identity Manager disables the Execution Schedule tab for them.**

Also, because Oracle Identity Manager always triggers pre-populate adapters on preinsert, Oracle Identity Manager disables the check boxes of this tab for pre-populate adapters.

1.4.3 Resources

From the Resources tab, you can:

- Click the Java APIs subtab to see the Java APIs that are being used by the adapter.
- Click the Other subtab to document a non-Java API file to the adapter, if necessary.

1.4.4 Variable List

From the Variable List tab, you can:

- Create, modify, and delete adapter variables.
- Set the data type and provide a description for each variable.
- Map an adapter variable to a literal or an adapter reference. You can also postpone the mapping until it is attached to a process task or a form field.

You also can resolve the value of the adapter variable at run time, when it is attached to a process task and the process task is run. As a result, process-specific data is available to map to this variable.

1.4.5 Usage Lookup

For a process task or task assignment adapter, the Usage Lookup tab displays the process task to which the adapter is attached, as well as the process of which this process task is a member.

For a rule generator or entity adapter, this tab shows the Oracle Identity Manager form and associated data object to which the adapter is attached. In addition, it displays the execution schedule of the adapter, along with a sequence number that represents the order in which Oracle Identity Manager will trigger the adapter.

For a pre-populate adapter, this tab displays the user-defined form and form field to which the adapter is attached. Also, it shows the pre-populate rule that is associated with the adapter.

Note: For more information about the different types of adapters, refer to the Chapter 3, "Creating Adapters" on page 3-1.

1.4.6 Responses

The Responses tab is used for defining meaningful responses to the process task. These responses depend on the execution result of the adapter. The various error messages returned by the external system can then be mapped to these responses in a way that they make sense in the context of the process task. On attaching the adapter to a process task, the status bucket, which consists of Pending, Completed, and Rejected, of

the process task (and subsequently the Object status) can be set, based on the adapter response code.

Tip: Oracle Identity Manager enables the Responses tab only for process task adapters. If an adapter is a task assignment, rule generator, pre-populate, or entity adapter, then Oracle Identity Manager disables this tab.

2

Getting Started

This chapter describes the configuration of Oracle Identity Manager and installation of the Remote Manager. It contains the following topics:

- Overview of Oracle Identity Manager Configuration
- Configuring Oracle Identity Manager to Reference JAR and Class Files
- Installing the Remote Manager
- Adding the Trust Relation

2.1 Overview of Oracle Identity Manager Configuration

To construct adapter tasks, ensure that Oracle Identity Manager has access to the target API JAR files and third-party applications to which you want to connect.

When your adapter uses Java tasks, you must configure Oracle Identity Manager to find the appropriate Java APIs. To do this, you must place the .jar files that contain these APIs into the JavaTasks subdirectory of the *OIM_HOME*`/xellerate` folder path, such as `C:\oracle\Xellerate\JavaTasks`. Then, you can access the Java classes associated with these Java APIs and use them in the Java task you are creating.

Sometimes, instead of directly communicating with the third-party system, Oracle Identity Manager must use an Oracle Identity Manager component that acts like a proxy. This component is known as Remote Manager.

The Remote Manager is used for:

- Invoking nonremotable APIs through Oracle Identity Manager
- Invoking APIs that do not support Secure Sockets Layer (SSL) over secure connections

The procedures in the following sections show you how to:

- Configure Oracle Identity Manager to reference JAR and class files for Java tasks.
- Configure the Remote Manager.

See Also:

"Creating a Java Task" on page 3-7 for more information about Java tasks

Oracle Identity Manager Administrative and User Console Guide to learn more about the Remote Manager

2.2 Configuring Oracle Identity Manager to Reference JAR and Class Files

To configure Oracle Identity Manager to reference JAR and class files:

1. Open the JavaTasks subdirectory, which can be found within the *OIM_HOME*/xellerate folder path. For example, C:\oracle\Xellerate\JavaTasks.
2. Place the JAR file or files into this subdirectory. You can then use these files to create Java tasks within an adapter without restarting the server.

2.3 Installing the Remote Manager

To configure the Remote Manager, follow the instructions described in Oracle Identity Manager installation guide for the application server that you use.

2.4 Adding the Trust Relation

To import a trusted certificate, at the command prompt, navigate to the following location:

JAVA_HOME\jre\lib\security

Enter the command:

```
JAVA_HOME/jre/bin/keytool -import -file
XLREMOTE_HOME\xlremote\config\xlserver.cert -keystore cacerts -trustcacerts -
alias rmtrust1 -storepass changeit

Owner: CN=Customer, OU=Customer, O=Customer, L=City, ST=NY, C=US
Issuer: CN=Customer, OU=Customer, O=Customer, L=City, ST=NY, C=US
Serial number: 41dee35a
Valid from: Fri Jan 07 11:30:34 PST 2005 until: Mon Jan 05 11:30:34 PST 2015
Certificate fingerprints:
         MD5:  B0:F2:33:C8:69:E4:25:A3:CB:59:E8:51:27:EE:5C:52
         SHA1: 3D:6A:6D:14:33:B5:5C:19:85:CC:EE:77:7F:7F:22:1D:56:48:47:4D
Trust this certificate? [no]:  yes
```

The certificate is added to the keystore.

3

Creating Adapters

This chapter describes how to create and define adapters. It contains the following topics:

- Overview of Adapter Creation
- Defining Adapters
- Disabling and Re-enabling Adapters
- About Adapter Variables
- Creating Adapter Tasks
- Modifying Adapter Tasks
- Changing the Order and Nesting of Tasks
- Deleting Adapter Tasks
- Working with Responses
- Scheduling Rule Generators and Entity Adapters

3.1 Overview of Adapter Creation

Now that you have set up Oracle Identity Manager, you are ready to create the five types of Oracle Identity Manager adapters. These are:

- Process task adapters
- Task assignment adapters
- Rule generators
- Pre-populate adapters
- Entity adapters

> **See Also:** "About Adapters" on page 1-2 for a detailed description of these adapters

3.2 Defining Adapters

To define an adapter:

1. Log in to Oracle Identity Manager.
2. Open the Adapter Factory form. This form is in the Development Tools folder in the Design Console.

3. In the Adapter Name field, enter the name of the adapter, for example, `Create Solaris User`.

   Note: Although the adapter name can contain special characters, Oracle recommends that you do not use them because there might be run-time errors.

4. Double-click the Adapter Type lookup field.

   The Lookup window is displayed, displaying the five types of Oracle Identity Manager adapters. These are:

   - Process Task
   - Rule Generator
   - Pre-populate Rule Generator
   - Entity
   - Task Assignment

5. To enable the adapter to automate a process task, select **Process Task (T)**.

   To incorporate business rules into an Oracle Identity Manager or user-defined form field, select **Rule Generator (R)**. For example, for the User ID field of a form, you can configure Oracle Identity Manager to concatenate the initial letter of the user's first name with the user's last name.

   You can attach a type of rule generator adapter to a user-created form field, so that it can:

   - Display the data, which is generated by the adapter, automatically or manually.
   - Use criteria that enable Oracle Identity Manager to determine which adapter is applied to the designated form field.

   To attach the adapter to an Oracle Identity Manager or user-defined form field, and have Oracle Identity Manager trigger the adapter on preinsert, preupdate, predelete, postinsert, postupdate, or postdelete, select **Entity (E)**.

   To allow the adapter to automate the allocation of a process task to a user or group, select **Task Assignment (A)**.

6. Select the type of adapter you want, for example, Process Task (T). Then, click **OK**.

   See Also: *Oracle Identity Manager Administrative and User Console Guide* for more information about the Form Designer form

7. In the Description field, type a description for the adapter, for example, `This adapter is used to create a new user for the Solaris environment`.

8. From the toolbar, click **Save**.

   The adapter is now stored in the Oracle Identity Manager database.

3.3 Disabling and Re-enabling Adapters

To disable an adapter so that it cannot be used with a process task or form field, select the **Disable Adapter** option, and then save the adapter.

To re-enable it, clear the **Disable Adapter** option, and save the adapter.

3.4 About Adapter Variables

For a newly-created adapter to work, you can map data to the parameters of the adapter tasks. For this reason, you create placeholders, also known as adapter variables, to map the data at run time.

Note: An adapter variable can be reused for all adapter tasks.

Once an adapter variable is not needed for the adapter to run, you can remove it from the adapter. After you have deleted the adapter variable, ensure to recompile the adapter.

3.4.1 Creating an Adapter Variable

To create an adapter variable:

1. Select the adapter to which you wish to add an adapter variable, for example, the `Create Solaris User` adapter.
2. Select the Variable List tab.
3. Click **Add**.

   The Add a Variable window is displayed.
4. When you do not want Oracle Identity Manager to be able to change the adapter variable value after it is activated, select **Final**.
5. In the Variable Name field, enter the name of the adapter variable, for example, `SolarisUserID`.

   Caution: The adapter variable name cannot contain spaces.
6. From the Type menu, select the classification type of the adapter variable, such as String. The available items are:
   - Object
   - IT Resource
   - String
   - Boolean
   - Character
   - Byte
   - Date
   - Integer
   - Float
   - Long
   - Short
   - Double

7. Within the Description text area, you can enter explanatory information about the adapter variable.
8. From the Map To menu, you can map your adapter variable to one of the items listed in Table 3–1.

Table 3–1 Items on the Map To Menu

Name	Description
Literal	This adapter variable is mapped to a constant (or literal).
Resolve at Run time	This adapter variable's mapping occurs later, at run time. Selecting this option increases the reusability of the adapter.
Adapter References	This adapter variable gives access to an Oracle Identity Manager database reference or an Oracle Identity Manager data object reference.
System Date	When this adapter variable is triggered by Oracle Identity Manager, it is mapped to the current date and time of the Server. **Note**: This option appears only when you select the Date type.

Note: When you select the object type, a Qualifier menu is displayed within the Add a Variable window. From this menu, you can select either of the following:

- Database Reference. If you select this item, then the adapter variable is mapped to the reference of the database that the Oracle Identity Manager is currently running against.
- Data Object Reference. If you select this item, then the adapter variable is mapped to an Oracle Identity Manager data object.

Note: If you select the IT Resource type, then a Resource Type menu is displayed within the Add a Variable window. From this menu, you can select one of the IT resource types that have been created by using the IT Resource Type Definition form. By doing so, you can map the adapter variable to a parameter of this IT resource type.

9. On the toolbar in the Add a Variable window, click **Save**. The information for your adapter variable is stored in the Oracle Identity Manager database.

   Close the Add a Variable window to activate the main screen. The name, classification type, mapping selection, and description of the adapter variable you created appear in the child table of the Variable List tab.

This adapter variable now belongs to the adapter in the Adapter Factory form. It is saved to the Oracle Identity Manager database, and the adapter variable is ready to use.

3.4.2 Modifying an Adapter Variable

To modify an adapter variable:

1. Select the adapter that contains the adapter variable you want to edit, for example, the `Create Solaris User` adapter.

2. Click the Variable List tab and double-click the row header of the adapter variable you want to modify. The Edit a Variable window is displayed, showing information about the adapter variable.
3. Make the necessary edits, for example, changing the adapter variable's data type from String to Character.
4. On the Edit a Variable toolbar, click **Save**. The modified information about the adapter variable is stored in the Oracle Identity Manager database.
5. Close the Edit a Variable window to activate the main screen. The adapter variable you modified appears within the child table of the Adapter Factory form.

Note: Ensure that you check your data mappings and recompile the adapter, especially if you change the adapter variable's data type.

3.4.3 Deleting an Adapter Variable

When an adapter variable is no longer necessary for the adapter to run, you can remove it from the adapter. To do this:

1. Select the adapter that contains an adapter variable you want to remove, for example, the `Create Solaris User` adapter.
2. Select the Variable List tab.
3. From the list of this tab, select the adapter variable you want to delete.
4. Click **Delete**.
5. Recompile the adapter after deleting any variable.

The adapter variable disappears from the child table. The adapter variable has been deleted.

3.5 Creating Adapter Tasks

After you construct the adapter and create its variables, you can create the atomic function calls of an adapter. These function calls are known as adapter tasks.

Oracle Identity Manager allows you to create the following adapter tasks:

- A Java task, which allows an adapter to communicate with an external source by invoking Java API.
- A remote task, which enables an adapter to call a method on an API. This API resides on a computer that is external to Oracle Identity Manager.

  This type of task is used mostly with integrations of third-party APIs that are not network-enabled. A remote manager executes the remote API method, which is located on a remote computer. In addition, if the third-party API does not use Secure Sockets Layer (SSL), then you can use the remote manager to invoke third-party APIs over SSL-protected communication. Remote tasks can also be used with integrations of third-party APIs, which are network-enabled, but are not located on the Oracle Identity Manager server for scalability purposes. The remote API method is still executed by a remote manager. However, because the third-party API is network-enabled, the remote manager does not have to reside on the target system.
- A stored procedure task, which allows Oracle Identity Manager to map to and execute SQL programs located within a particular database schema. These

programs are known as stored procedures. They contain information, such as SQL statements, which are pre-compiled for greater efficiency.

By incorporating a stored procedure task into an adapter, and attaching this adapter to a process task, Oracle Identity Manager can incorporate stored procedures on any Oracle Database or Microsoft SQL Server database that is accessible on its network. This includes retrieving primitive values from stored procedures.

- A utility task, which enables you to populate an adapter with methods and APIs that come packaged with Oracle Identity Manager. In addition, this type of task provides you with access to the Java Standard Library APIs.
- An Oracle Identity Manager API task, which enables access to Oracle Identity Manager published APIs from adapter tasks. This allows for enhanced portability of adapter code.
- A set variable task, which allows you to set a variable within an adapter.
- An error handler task, which lets you display any errors associated with an adapter that occur at run time. In addition, you can see the reasons for the errors, along with possible solutions.
- A logic task, which lets you build a conditional statement within an adapter.

You can create the following types of logic tasks:

- FOR loops
- WHILE loops
- IF statements
- ELSE statements
- ELSE IF statements
- BREAK statements
- RETURN statements
- CONTINUE statements
- SET VARIABLE statements
- Handle Error statements

See Also: "Creating a Logic Task" on page 3-20 for more information about the types of logic tasks you can build

For classification purposes, Oracle Identity Manager represents each type of adapter task by an icon. The icon, which precedes the task name, is a visual indicator of the type of task it is. For example, "J" represents a Java task, and "LT" represents a logic task.

To see a list of these icons, select the Adapter Tasks tab, and click **Legend**. The Legend window appears, displaying the following list of icons:

- Functional Task
  - Java
  - Remote
  - Stored Procedure
- Utility Task

  - Utility
  - Oracle Identity Manager API
- Logical Task

3.5.1 Creating a Java Task

Oracle Identity Manager can handshake with an external source through a Java API. To make this happen, you must add a task to an adapter, which, when triggered by Oracle Identity Manager, initiates communications with the external source. This type of task is called a Java task.

To create a Java task:

1. Select the adapter to which you want to add a Java task, for example, the Update Solaris Password adapter.
2. Select the Adapter Tasks tab.
3. Click **Add**.

   After the Adapter Task Selection window is displayed, select the **Functional Task** option.
4. From the display area to the right of this option, select the Java item, and click **Continue**.

   The Object Instance Selection window is displayed.

   Table 3–2 explains the options in the Object Instance Selection window.

Table 3–2 Options in the Object Instance Selection Window

Option	Description
New Object Instance	When you click this option, you are creating a new Java object instance.
Persistent Instance	You can call the method on a persistent object by clicking this option, clicking the adjacent combo box, and selecting an object instance from the drop-down menu.
Task Return Value Instance	You can call this method on an object returned by an adapter task defined earlier by clicking this option, clicking the combo box, and selecting an adapter task from the drop down list.

Note: When the Persistent Instance option is grayed out, you have not defined any persistent objects for your adapter. Similarly, if the Task Return Value Instance option is grayed out, none of the tasks have Java Object return values associated with them.

5. Click an option—for example, New Object Instance—and click **Continue**. The Add an Adapter Factory Task window is displayed.

   Table 3–3 lists and describes the various regions of the Add an Adapter Factory Task window:

Table 3–3 Regions of the Add an Adapter Factory Task Window

Name	Description
Task Name	This field displays the name of the Java task.

Table 3–3 (Cont.) Regions of the Add an Adapter Factory Task Window

Name	Description
Persistent Instance	If this Java object is to be used again, the check box is selected, and the name of the task instance is entered in the adjacent field.
API Source	This combo box contains a list of all JAR and class files to which you have access.
Application API	This combo box contains a list of all class files to which you have access, and which belong to the JAR file that has been selected from the API Source list.
Constructors	This text area displays all the constructors, which are available for the Java object.
Methods	This text area shows a list of all the methods, which are available for the Java object.
Application Method Parameters	This area contains the parameters of the selected constructor and method. These parameters are mapped to the adapter variables and Oracle Identity Manager components.

6. In the Task Name field, enter the name of the task you are creating, for example, `Update Password`.
7. (Optional.) To make your Java object reusable, select **Persistent Instance**, then type the name of the instance of this task in the text field located to the right of the check box.

Caution: Ensure that name of the instance contains no spaces.

Note: To reference a session with the target resource multiple times during the life of the adapter, and not just once, select **Persistent Instance**.

Tip: By setting the Java object to be persistent, the next time you create a Java object, it appears in the Persistent Instance list of the Object Instance Selection window. In addition, you do not have to map the constructor to all adapter tasks of the same Java object.

8. Select the API Source. The JAR files appear, which Oracle Identity Manager references from the JavaTasks subdirectory of the *`OIM_HOME`*`/xellerate` folder path—for example, `C:\oracle\Xellerate\JavaTasks`.

See Also: "Configuring Oracle Identity Manager to Reference JAR and Class Files" on page 2-2 for instructions on how to enable Oracle Identity Manager to use third-party JAR files with a Java task

9. Select the Application API. The class files, which belong to the JAR file you selected in the API Source, appear.
10. From the Constructors area, select the method to be used to initialize the Java class you selected.
11. From the Methods area, select the method that will be used with your Java task.
12. From the toolbar, click **Save**.

The information pertaining to the Java task is stored in the Oracle Identity Manager database. You can now access the parameters of your Java task's constructors and methods. These parameters appear in the Application Method Parameters region of the Add an Adapter Factory Task window.

13. To display the Java class constructors and methods for which you must set mappings, click the plus icons displayed to the left of the Constructor and Method icons.
14. Select the parameter of the constructor or method for which you must set a mapping.
15. In the Description text area, you can enter a description for this mapping.
16. Click the Map to combo box, and select an item that you can map to the parameter of the constructor or method, for example, Adapter Variables.
17. Set the appropriate mappings.

    See Also: The "Adapter Mapping Information" section on *Oracle Identity Manager Reference* for more information about which mappings to set

18. Click **Set**.

    The parameter of the selected constructor or method now appears in blue. This signifies that it has been mapped.

    Tip: To remove a parameter mapping, right-click the appropriate parameter, and select Un-Map Parameter from the popup menu that appears.

19. Repeat steps 15 through 18 for all parameters of the constructors and methods that appear in the Application Method Parameters region.
20. On the Add an Adapter Factory Task window toolbar, click **Save**. The information pertaining to the Java task is stored in the Oracle Identity Manager database.
21. On the toolbar, click **Close**. The Add an Adapter Factory Task window disappears, and the main screen is active once again. The Java task that you created—for example, Update Password—appears within the Adapter Factory form.
22. (Optional.) To create additional Java tasks for the adapter, repeat steps 3-21.

    Tip: You can create different types of adapter tasks, and add them to the adapter.

    If the adapter is logically complete, and all variables on the adapter tasks are mapped, you can compile it to use with a process task or form field.

23. To compile the adapter, click **Build**.

    The text in the Compile Status field changes from Recompile to OK. This indicates that Oracle Identity Manager compiled the adapter and found no errors. You can now attach the adapter to a process task or form field.

24. (Optional.) To see the code that Oracle Identity Manager generates, from the toolbar, click **Notes**.

    The Notes window is displayed, containing the code that Oracle Identity Manager generated.

Note: If, after clicking Build, CODE GEN ERROR appears in the Compile Status field, it means that Oracle Identity Manager encountered one of two types of errors while validating and compiling the adapter:

- Validation Error

  While Oracle Identity Manager is checking the adapter to verify that it is valid, an error is found. This error can result from a parameter of an adapter task not being mapped, a parameter being mapped improperly, or an adapter task being placed out of order.

  Because Oracle Identity Manager generates code for an adapter only after it is validated, if Oracle Identity Manager encounters a validation error, it does not create any code.

- Java Compilation Error

  Oracle Identity Manager has verified that the adapter is valid. However, while Oracle Identity Manager is compiling the adapter, an error is found. This error can result from assigning an incorrect data type to an adapter task parameter.

  Because Oracle Identity Manager has validated the adapter, it generates code. However, Oracle Identity Manager stops building code at the point of the compilation where it encounters the error.

Tip: Once you create a Java task, and add it to an adapter, you can see the following information by accessing the Resources tab of the Adapter Factory form:

- The JAR and class files used to create the Java task.
- The name, which represents the directory path that contains these JAR and class files.

3.5.2 To Create a Remote Task

A remote task enables an adapter to invoke an API method by using the Remote Manager. This API resides on a computer that is external to Oracle Identity Manager. This section explains how to create a remote task.

Note: Before creating a remote task, ensure that you define an adapter variable with a classification type of IT Resource, as well as select one of the IT resources that have been created by using the IT Resource Type Definition form.

1. Select the adapter to which you wish to add a remote task.
2. Click the Adapter Tasks tab.
3. Click **Add**.

   The Adapter Task Selection window is displayed.
4. Select the Functional Task option.
5. From the display area to the right of the button, select the Remote item to create a remote task. Then, click **Continue**.

   The Object Instance Selection window is displayed.

Note: To learn more about the choices of this window, refer to "Creating a Java Task" on page 3-7.

6. Click **Continue**.

   The Add an Adapter Factory Task window is displayed.

7. In the Task Name field, enter the name of the remote task you are creating.

8. (Optional.) If you want your remote task to be reusable, select the **Persistent Instance** option. Then, type the name of the instance of this task in the text field, located to the right of the check box.

   Caution: Ensure that the name of the instance contains no spaces.

   See Also:

   "Creating a Java Task" on page 3-7 for more information about the regions of the Add an Adapter Factory Task window

   "Configuring Oracle Identity Manager to Reference JAR and Class Files" on page 2-2 for information about how to enable Oracle Identity Manager to use third-party JAR files with a Java task

9. From the Add an Adapter Factory Task window, select a JAR file, class file, constructor, and method. Then, set the mappings for the parameters of the constructor and method.

   Note: One of the input parameters will have a classification type of IT Resource. You must associate this parameter with an adapter variable of type IT Resource.

   See Also: The "Adapter Mapping Information" section in *Oracle Identity Manager Reference* for more information about which mappings to select

10. From the Add an Adapter Factory Task window toolbar, click **Save**.

    The information pertaining to the remote task is stored in the Oracle Identity Manager database.

11. From this window toolbar, click **Close**.

    The Add an Adapter Factory Task window disappears, and the main screen is active once again. The remote task that you created appears within the Adapter Factory form.

12. (Optional.) To create additional remote tasks for the adapter, repeat Steps 3 through 11.

    You are now ready to compile the adapter, so it can be used with a process task or form field.

13. To compile the adapter, click **Build**.

    The text in the Compile Status field changes from Recompile to OK. This indicates that Oracle Identity Manager compiled the adapter and did not find any errors.

You can now attach the adapter to a process task or form field, so Oracle Identity Manager can communicate with the external API.

3.5.3 To Create a Stored Procedure Task

Through Oracle Identity Manager, you can map to and execute SQL programs that are located within a particular database schema. These SQL programs are known as stored procedures. Stored procedures contain information, such as SQL statements, which are precompiled for greater efficiency.

For this to occur, you must add a stored procedure task to an adapter. When triggered by Oracle Identity Manager, this task incorporates stored procedures on any Oracle Database or Microsoft SQL Server database that is accessible on its network. This includes retrieving primitive values from stored procedures.

To create a stored procedure task:

Note: The parameter values and server type for the database schema are set within the IT Resources form.

The server type of the schema must be set to Database. Otherwise, Oracle Identity Manager cannot reference the database schema during the creation of a stored procedure task, the execution of a stored procedure task, or both.

In addition, Oracle Identity Manager uses values, which are represented by parameters—for example, Database Name or *URL*—to connect to the schema. As a result, the stored procedures contained within the schema, can be executed.

---

1. For Oracle Identity Manager Installations that use Oracle Database, copy the ojdbc14.jar file from the *OIM_HOME*/xellerate/ext/ directory to the *OIM_DC_HOME*/xlclient/ext directory.

   For Oracle Identity Manager Installations that use Microsoft SQL Server, you must obtain the following files from Microsoft and copy them to the *OIM_DC_HOME*/xlclient/ext directory:

   - msbase.jar
   - mssqlserver.jar
   - msutil.jar

2. Select the adapter to which you wish to add a stored procedure task, for example, the Update User ID adapter.
3. Click the Adapter Tasks tab.
4. Click **Add**.

   The Adapter Task Selection window is displayed.

5. Select the **Functional Task** option.
6. From the display area to the right of the option, select **Stored Procedure**, and click **Continue**. The Add an Adapter Factory Task window is displayed.

   The following table lists and describes the regions of the Add an Adapter Factory Task window.

Table 3–4 Regions of the Add an Adapter Factory Task Window

Name	Description
Task Name	Displays the name of the stored procedure task.
Description	Displays explanatory information about the stored procedure task.
Database	Lists the databases defined in the IT Resources form. Important: Only those IT resources with a server type of Database appear in the Database list.
Schema	Lists the schemas, which are associated with the database that appears in the Database list.
Procedure	Lists the stored procedures, which reside within the database schema that is displayed in the Schema list.

Connection Status	Displays the status of the connection between Oracle Identity Manager and the database that contains the target stored procedure.
	When Oracle Identity Manager can connect to the database, Connection Established is displayed in the Connection Status region.
	Note: If Oracle Identity Manager cannot connect, Connection Failed appears in the display area. In addition, the **Notes** button of the Add an Adapter Factory Task window is enabled. Clicking this button shows you why a connection could not be established, for example:
	`Exception Type:`
	`java.lang.ClassNotFoundExceptionMessage:`
	`java.lang.ClassNotFoundException:`
	`oracle.jdbc.driver.OracleDriver`
	In this example, Oracle Identity Manager could not connect to the designated database because it could not find a particular Java class.

Parameters	Contains parameters that can be mapped to the stored procedure. These parameters appear after you select a database, schema, and stored procedure and save this information to the Oracle Identity Manager database.

7. In the Task Name field, enter the name of the stored procedure task you are creating (for example, Update ID).
8. In the Description text area, you can enter a description for this stored procedure task.
9. Click the Database list. The databases, which are defined in the IT Resources form, appear.

Note: If Oracle Identity Manager cannot connect to the database you selected, *Connection Failed* appears in the display area. In addition, the **Notes** button of the Add an Adapter Factory Task window is enabled. Clicking this button shows you why a connection could not be established.

Tip: Schemas and stored procedures appear only after you select a database to which Oracle Identity Manager can connect. Based on this selection, related schemas and stored procedures appear in the corresponding combo boxes.

See Also: *Oracle Identity Manager Administrative and User Console Guide* for more information about using the IT Resources form to define the settings for databases that contain stored procedures

10. Click the **Schema list**. The schemas appear, which are associated with the database you selected.
11. Click the **Procedure list**. The stored procedures, which reside within the database schema that you selected from the Schema combo box, appear.
12. From the Add an Adapter Factory Task window's toolbar, click **Save**. The information pertaining to the stored procedure task is saved into the Oracle Identity Manager database.

    You can now set the mappings for the parameter(s) of the stored procedure. These parameters appear in the Parameters region of the Add an Adapter Factory Task window.

    Note: Oracle Identity Manager automatically maps the database and schema of the selected stored procedure. However, Oracle Identity Manager enables you to override these mappings.

    See Also: The "Adapter Mapping Information" section in *Oracle Identity Manager Reference* for more information about which mappings to select

13. From the Add an Adapter Factory Task window's toolbar, click **Save**. The mappings that you have set for the parameter(s) of the stored procedure task are stored in the Oracle Identity Manager database.
14. From this window's toolbar, click **Close**.

    The Add an Adapter Factory Task window disappears, and the main screen is active once again. The stored procedure task you created (for example, Update ID) appears within the Adapter Factory form.
15. (Optional.) Repeat steps 3 through 13 to create additional stored procedure tasks for the adapter.
16. To compile the adapter, click **Build**.

    The text in the Compile Status field changes from Recompile to OK. This indicates that Oracle Identity Manager compiled the adapter and did not find any errors. You can now attach the adapter to a process task or form field, so Oracle Identity Manager can map to and execute the stored procedure you selected.

3.5.4 To Create a Utility Task

The Adapter Factory is shipped with a library of utility classes and methods, which increase the efficiency of developing adapters.

These utility classes and methods are contained within the **xlUtils.jar**, **xlIntegration.jar**, and **rt.jar** files. A Java task you create by using a class or method from one of these JAR files is called a **utility task**.

> **See Also:** *Java API Documentation* for more information about the class files that contains the *xlUtils.jar*, *xlAPI.jar*, *xlIntegration.jar*, and `rt.jar` files.

1. Select the adapter to which you wish to add a utility task, for example, the Update Solaris User Group adapter.
2. Click the Adapter Tasks tab.
3. Click **Add**.

   The Adapter Task Selection window is displayed.
4. Select the **Utility Task** option.
5. From the display area to the right of the option, select **Utility**, and click **Continue**. The Object Instance Selection window is displayed.

   > **See Also:** "Creating a Java Task" on page 3-7 to learn more about the choices of this window
6. Click **Continue**. The Add an Adapter Factory Task window is displayed
7. In the **Task Name** field, enter the name of the utility task you are creating, for example, Update User Group.
8. (Optional.) If you want your utility task to be reusable, select **Persistent Instance**, then type the name of the instance of this task in the text field to the right of the check box.

   Caution: Ensure that name of the instance does not contain any spaces.

   See Also:

   "Creating a Java Task" on page 3-7 for more information about the regions of the Add an Adapter Factory Task window

   "Configuring Oracle Identity Manager to Reference JAR and Class Files" on page 2-2
9. Click the Application API list. The class files appear, which belong to the `xlUtils.jar`, `xlIntegration.jar`, and `rt.jar` files.

   Note: The xlUtils.jar, xlIntegration.jar, and rt.jar files contain all of the class files that you can use for a utility task. Therefore, you do not have to access the API Source list.

   ---
10. From the Add an Adapter Factory Task window, select a constructor and method. Then, set the mappings for the parameters of the constructor and method.

> **See Also:** The "Adapter Mapping Information" section in *Oracle Identity Manager Reference* for more information about which mappings to select

11. From the Add an Adapter Factory Task window's toolbar, click **Save**. The information pertaining to the utility task is stored in the Oracle Identity Manager database.
12. From this window's toolbar, click **Close**.

    The Add an Adapter Factory Task window disappears, and the main screen is active once again. The utility task that you created (for example, Update User Group) appears within the Adapter Factory form.
13. (Optional.) Repeat steps 3 through 12 to create additional utility tasks for the adapter.

    You are now ready to compile the adapter, so it can be used with a process task or form field.
14. To compile the adapter, click **Build**.

    The text in the Compile Status field changes from Recompile to OK. This indicates that Oracle Identity Manager compiled the adapter and did not find any errors. You can now attach the adapter to a process task or form field.

3.5.5 To Create an Oracle Identity Manager API Task

For greater portability of the adapter code, an Oracle Identity Manager API task enables Adapter tasks to call APIs published by Oracle Identity Manager. This is better than accessing Oracle Identity Manager data directly through hardcoded SQL statements.

The Adapter Factory is shipped with a library of utility classes and methods, which increase the efficiency of developing adapters that contain Oracle Identity Manager API tasks. These utility classes and methods are contained within the xlAPI.jar file.

> **See Also:** Java API Documentation for more information about the class files that contain the `xlUtils.jar`, `xlAPI.jar`, `xlIntegration.jar`, and `rt.jar` files

To create this type of adapter task:

1. Select the adapter to which you wish to add an Oracle Identity Manager API task, for example, the Get User's Password adapter.
2. Click the Adapter Tasks tab.
3. Click **Add**.

   The Adapter Task Selection window is displayed.
4. Select the **Utility Task** option.
5. From the display area to the right of the option, select Xellerate API, and click **Continue**. The Object Instance Selection window is displayed.

   > **See Also:** "Creating a Java Task" on page 3-7 to learn more about this window
6. Click **Continue**. The Add an Adapter Factory Task window is displayed.

7. In the Task Name field, enter the name of the Oracle Identity Manager API task you are creating, for example, Retrieve Password).
8. (Optional.) If you want your Oracle Identity Manager API task to be reusable, select Persistent Instance. Then, type the name of the instance of this task in the text field to the right of the check box.

   Tip: Ensure that name of the instance contains no spaces.

   See Also:

   "Creating a Java Task" on page 3-7 for more information about the regions of the Add an Adapter Factory Task window

   "Configuring Oracle Identity Manager to Reference JAR and Class Files" on page 2-2 to learn how to enable Oracle Identity Manager to use third-party JAR files with a Java task

9. Click the Application API list. The class files appear, which belong to the `xlAPI.jar` file.

   Note: `The xlAPI.jar` file contains all of the class files that you can use for an Oracle Identity Manager API task. Therefore, you do not have to access the API Source list.

10. From the Add an Adapter Factory Task window, select a class file, constructor, and method. Then, set the mappings for the parameters of the constructor and method.

    See Also: The "Adapter Mapping Information" section in *Oracle Identity Manager Reference* for more information about which mappings to select

11. From the Add an Adapter Factory Task window's toolbar, click **Save**. The information pertaining to the Oracle Identity Manager API task is stored in the Oracle Identity Manager database.
12. Close the Add an Adapter Factory window to activate the main screen. The Oracle Identity Manager API task that you created—for example, *Retrieve Password*—appears within the Adapter Factory form.
13. (Optional.) To create additional Oracle Identity Manager API tasks for the adapter, repeat steps 3 through 12.

    You are now ready to compile the adapter, so it can be used with a process task or form field.
14. To compile the adapter, click **Build**.

    The text in the **Compile Status** field changes from Recompile to OK. This indicates that Oracle Identity Manager compiled the adapter and did not find any errors. You can now attach the adapter to a process task or form field, so Oracle Identity Manager can communicate with a third-party application.

3.5.6 Reassigning the Value of an Adapter Variable

Sometimes, for an adapter to accomplish its required objective, you must reassign the value of one adapter variable to another adapter variable, a different type of adapter

task, or a constant (or literal). The task that enables you to reallocate an adapter variable value is known as a set variable task.

> **See Also:** "About Adapter Variables" on page 3-3

For example, you can create a set variable task to set the adapter variable return value to equal the output of an adapter task (UserName) if the User ID length is fewer than 11 characters.

To create a set variable task:

1. Select the adapter to which you wish to add a set variable task (for example, the Check the Solaris User ID adapter).
2. Click the Adapter Tasks tab.
3. Click **Add**. The Adapter Task Selection window is displayed.
4. Select the Logic Task option.
5. From the display area, select SET VARIABLE, and click **Continue**. The Add Set Variable Task Parameters window is displayed.
6. From the Variable Name list, select the adapter variable that has a value you want to reassign—for example, Adapter return value.
7. From the Operand Type list, select the type of operand that will provide the value for the variable.

   > **Tip:** You can reassign an adapter variable's value to another adapter variable, a different type of adapter task, or a literal.

   Use Table 3–5 to understand the various types of operands.

Table 3–5 Types of Operands

Operand Name	Description
Variable	If you select this operand type, then adapter variables appear in the Operand Qualifier list. From this list, select the specific adapter variable that will provide the reassigned value. **Note**: The only adapter variables that will appear in the Operand Qualifier combo box will be those variables that have the same data type as the adapter variable that is displayed within the Variable Name combo box.
Adapter Task	By selecting this operand type, adapter tasks are displayed in the Operand Qualifier combo box. From this combo box, select the particular adapter task that will provide the reallocated value. **Note**: The only adapter tasks that will appear in the Operand Qualifier combo box will be those tasks that have the same data type as the adapter variable that is displayed within the Variable Name combo box.
Literal	When you select this operand type, types of literals appear in the Operand Qualifier combo box. From this combo box, select the type of literal that will provide the reallocated value. Then, type the specific literal into the field that appears underneath the combo box.

The following task sets the adapter variable's return value to be equal to the UserName adapter variable.

1. On the toolbar in the Add Set Variable Task Parameters window, click **Save**. The set variable task you created is stored in the Oracle Identity Manager database.
2. On the Add Set Variable Task Parameters window toolbar, click **Close**. The Add Set Variable Task Parameters window disappears, and the main screen is active once again. The set variable task that you created, for example, `Set Adapter return value = UserName`, appears in the Adapter Factory form.
3. (Optional.) Repeat Steps 3-9 to create additional set variable tasks for the adapter.

   You are now ready to compile the adapter, so it can be used with a process task or form field.
4. To compile the adapter, click **Build**. The text in the Compile Status field changes from Recompile to OK. Oracle Identity Manager compiled the adapter and found no errors. You can attach the adapter to a process task or form field.

3.5.7 Adding an Error Handler Task

To add an error handler task:

1. An adapter task can return errors. When this occurs, the process task or form field to which the adapter is attached gets rejected.

   You can attach your own customizable error messages, which will be displayed to the user. These messages are known as error handler tasks.

   For example, you can attach an error handler task to an adapter that will display an error message when the length of a User ID is greater than 10 characters.
2. Select the adapter to which you wish to add an error handler task (for example, the *Check the Solaris User ID* adapter).
3. Click the Adapter Tasks tab.
4. Click **Add**.

   The Adapter Task Selection window is displayed.
5. Select the **Logic Task** option.
6. From the display area, select Handle Error, and click **Continue**. The Add an Adapter Factory Task window is displayed.
7. Double-click this window's lookup field. The Lookup window is displayed, displaying the error handler tasks you can add to the adapter.

   Note: The only error handler tasks that appear in this Lookup window are the ones that begin with ADAPTER—such as ADAPTER.USERIDLENERR).

   If you do not see the error handler task that you want to incorporate into the adapter, you can create one by accessing the Error Message Definition form. Refer to *Oracle Identity Manager Design Console Guide* for information about the Error Message Definition form.
8. Select the error handler task you want, for example, ADAPTER.USERIDLENERR.
9. Click **OK**. The Lookup window disappears, and the Add an Adapter Factory Task window is active. In addition, the error handler task you selected appears in the field of this window.

10. From the Add an Adapter Factory Task window toolbar, click **Save**. The error handler task you incorporated into the adapter is stored in the Oracle Identity Manager database.
11. From this window's toolbar, click **Close**.

    The Add an Adapter Factory Task window disappears, and the main screen is active once again. The error handler task you added, for example, `Handle Error.ADAPTER.USERIDLENERR`, appears within the child table of the Adapter Factory form.
12. (Optional.) Repeat Steps 3-10 to create additional error handler tasks for the adapter.

    If the adapter is logically complete and all variables on the adapter tasks are mapped, you can compile it to use with a process task or form field.
13. To compile the adapter, click **Build**.

    The text in the Compile Status field changes from *Recompile* to *OK*. This indicates that Oracle Identity Manager compiled the adapter and did not find any errors. You can now attach the adapter to a process task or form field.

See Also:

- *Oracle Identity Manager Design Console Guide* for information about creating error messages by using the Error Message Definition form
- *Oracle Identity Manager Globalization Guide* for information about localizing user-defined data by using custom resource bundles

3.5.8 Creating a Logic Task

While defining the adapter, you can add conditional statements to the adapter to control its logic flow. These conditional statements are known as logic tasks. For example, you can create a logic task that will trigger an action if the length of a User ID is greater than 10 characters.

To create a logic task:

1. Select the adapter to which you wish to add a logic task (for example, the Check the Solaris User ID adapter).
2. Click the Adapter Tasks tab.
3. Click **Add**. The Adapter Task Selection window is displayed.
4. Select the **Logic Task** option.
5. From the display area, select the type of logic task you want to create. Then, click **Continue**.

Note: If you select a conditional expression, and click **Continue**, one of the following actions occurs:

Oracle Identity Manager adds the conditional statement to the adapter directly; or

A secondary window is displayed, containing fields about the conditional expression that you can configure.

To see what happens when you select a particular conditional statement, refer to Table 3–6.

Table 3–6 Actions Resulting from Particular Conditional Statements

Conditional Statement	Statement Is Added to the Adapter Directly	Secondary Window Appears
FOR		X
WHILE		X
IF		X
ELSE	X	
ELSE IF		X
BREAK	X	
RETURN	X	
CONTINUE	X	

Table 3–7 explains the various regions of the Add Adapter Factory Logic Task Parameters window:

Table 3–7 Regions of the Add Adapter Factory Logic Task Window

Name	Description
Operand Type	These combo boxes contain types of operands, such as adapter tasks and adapter variables.
Comparator Combo Box	From this combo box, you can set the relationship between two operands (for example, <, =, >).
Operand Qualifier	These combo boxes contain the qualifiers for the operands.
Literal Text Box	When you select the Literal operand type, enter the specific literal into this field.

Note: By selecting the FOR conditional statement, an Add Adapter Factory Logic Task Parameters window is displayed. However, it contains different text and combo boxes.

For the FOR conditional expression, use Table 3–8 to understand the various regions of this Add Adapter Factory Logic Task Parameters window.

Table 3–8 Add Adapter Factory Logic Task Parameters for FOR Conditional Statement

Name	Description
Operand Type	These combo boxes contain types of operands, such as adapter tasks and adapter variables.
Comparator Combo Box	From this combo box, you can set the relationship between two operands (for example, <, =, >).
Operand Qualifier	These combo boxes contain the qualifiers for the operands.
Increment Combo Box	Within this area, you can set whether the initial value will increase or decrease, and by how much.

Note: If you select the ELSE, BREAK, RETURN, or CONTINUE conditional expressions, proceed to Step 8.

6. Set the parameters for your conditional expression.

   This logic task will check to see if the length of the User ID is greater than 10 characters.

7. From the Add Adapter Factory Logic Task Parameters window toolbar, click **Save**.

   The logic task you created is stored in the Oracle Identity Manager database.

8. From this window toolbar, click **Close**. The Add Adapter Factory Logic Task Parameters window disappears, and the main screen is active once again. The logic task that you created—for example, If (Check ID Length > 10)—appears within the Adapter Factory form.

9. (Optional.) Repeat Steps 3-8 to create additional logic tasks for the adapter.

   Caution: All adapter tasks that can be executed for a condition of a logic task should be nested properly under that logic task.

   See Also: "Changing the Order and Nesting of Tasks" on page 3-23 for more information about nesting tasks

   You are now ready to compile the adapter, so it can be used with a process task or form field.

10. To compile the adapter, click **Build**.

    The text in the Compile Status field changes from *Recompile* to *OK*. This indicates that Oracle Identity Manager compiled the adapter and did not find any errors. You can now attach the adapter to a process task or form field.

3.6 Modifying Adapter Tasks

The following procedure will show you how to edit an adapter task, in case you must make changes to it. To modify an adapter task

1. Select the adapter that contains the adapter task you wish to edit (for example, the *Update Solaris User Group* adapter).
2. Click the **Adapter Tasks** tab.
3. Double-click the adapter task that you want to modify.

   The Edit Adapter Factory Task Parameters window is displayed, displaying information that relates to the adapter task you selected. Within this window, make the necessary modifications.

4. On the Edit Adapter Factory Task Parameters window toolbar, click **Save**.

   The information you modified is stored in the Oracle Identity Manager database.

5. On the toolbar, click **Close**.

   The Edit Adapter Factory Task Parameters window disappears. The main screen is active again. The modified task appears within the child table of the **Adapter**

Factory form. You must re-compile the adapter, so it can be used with a process task or form field.

6. To recompile the adapter, click **Build**.

   The text in the **Compile Status** field changes from *Recompile* to *OK*. This indicates that Oracle Identity Manager compiled the adapter and did not find any errors. You can now attach the adapter to a process task or form field.

   Caution: You cannot modify the API call inside a Java, Xellerate API, or Utility task. The adapter task has to be deleted and re-created.

   In addition, if *CODE GEN ERROR* appears in the Compile Status field, Oracle Identity Manager encountered errors while compiling the adapter. Rectify the errors, if necessary re-do the adapter task modifications, and compile the adapter again.

3.7 Changing the Order and Nesting of Tasks

If you add multiple tasks to an adapter, you can either change the order in which the tasks are executed, or place one task inside of another task for the adapter to work.

The following procedure will show you how to change the order and nesting of tasks.

Caution: You should not change the order and nesting of adapter tasks unless you understand the mapping dependencies of the adapter tasks.

To change the order and nesting of tasks:

1. Select the adapter that contains tasks of which you want to change the order and/or nest (for example, the *Check the Solaris User ID* adapter).
2. Click the **Adapter Tasks** tab.

   The tasks appear, which belong to the current adapter.

   In this example, the following changes must occur:

   - The error handler task must be nested inside of the *IF (Check ID Length > 10)* logic task.
   - The set variable task has to be nested inside of the **ELSE** logic task.
   - The **IF** logic task precedes the **ELSE** logic task.

   Therefore, you must first reorganize the logic tasks. Then, you must nest the error handler task and set variable task inside of the **IF** and **ELSE** logic tasks, respectively. To reorganize tasks:

3. Select the task that must run before another task, and click the **Up** arrow button. The selected task will switch places with the task that precedes it.

   or

   Select the task that must be executed after another task, and click the **Down** arrow button. The highlighted task is displayed below the task that previously followed it.

   To nest tasks/remove task nestings:

4. Select the task that must be placed inside of another task, and click the **Right** arrow button. The selected task will be nested inside of the task that appears above it.

   or

   Select the task that no longer be nested inside of another task, and click the **Left** arrow button. The highlighted task will not be nested inside of the task that is displayed above it.

5. On the toolbar, click **Save**.

   The order and nesting of the adapter's tasks is stored in the Oracle Identity Manager database. If the adapter is logically complete and all variables on the adapter tasks are mapped, you can compile it to use with a process task or form field.

6. To compile the adapter, click **Build**.

   The text in the Compile Status field changes from *Recompile* to *OK*. This indicates that Oracle Identity Manager compiled the adapter and did not find any errors. You can now attach the adapter to a process task or form field.

Caution: If you see *CODE GEN ERROR* in the Compile Status field, Oracle Identity Manager found errors while compiling the adapter. Rectify the errors, if necessary re-do the adapter task modifications, and compile the adapter again.

3.8 Deleting Adapter Tasks

When an adapter task is no longer necessary for the adapter to run, you must remove it from the adapter. To delete an adapter task:

1. Select the adapter that contains the task you wish to remove (for example, the *Update Solaris User Group* adapter).
2. Click the **Adapter Tasks** tab.
3. Select the task that you want to remove (for example, the *CONTINUE* logic task).
4. Click **Delete**.

   The selected task is deleted and disappears from the child table.

5. On the toolbar, click **Save**.
6. Recompile the adapter.

Caution: While deleting adapter tasks, ensure that the logic of the adapter is consistent and maintained.

3.9 Working with Responses

Adapters can have different outcomes, called **responses**. Based on these responses, adapters can trigger other process tasks.

For example, if the adapter returns a *True* response, the process task's status can be set automatically to *Completed*. However, if the adapter returns a *False* response, the process task's status can be set automatically to *Rejected*, and another process task can be triggered.

These responses can be added, modified, or removed on the Responses tab of the Adapter Factory form.

The following procedures will show you how to create, modify, and delete responses.

Note: Responses are used only with process task adapters, because these adapters are attached to process tasks. Rule generators, pre-populate adapters, and entity adapters are not connected to processes. In addition, task assignment adapters are not associated with responses. Therefore, if the active adapter is a task assignment adapter, rule generator, pre-populate adapter, or entity adapter, Oracle Identity Manager disables the Responses tab.

3.9.1 To Create a Response

1. Select the adapter to which you want to add responses (for example, the *Create Solaris User* adapter).
2. Click the **Responses** tab.
3. Click **Add**.

   An empty row is inserted into the **Responses** tab.
4. Click the field that appears within the **Code Name** column.
5. Enter a code, which represents a response type that can be generated (for example, *True*).
6. Click the field that appears within the **Description** column.
7. Enter a description for this response (for example, *The user was created successfully*.).
8. Double-click the field that appears within the **Status** column.

   The Lookup popup window is displayed, containing the different status levels that you can associate with the response.

   Note: For more information about Oracle Identity Manager's status levels, refer to Chapter 4, "About Process Task Adapters" on page 4-1.
9. Click the desired status level (for example, *Completed (C)*). Then, click **OK**.

   The Lookup window disappears, and the **Responses** tab is active once again.
10. Create another response, by clicking the **Add** button, and entering *False* and *The user was not created successfully.* into the Code Name and Description fields, respectively. Then, access the Lookup window, and assign the *Rejected (R)* status level to this response.
11. On the toolbar, click **Save**.

    The responses that you created for this adapter have been stored in the Oracle Identity Manager database. After you attach this adapter to a process task, these responses will appear in the Responses tab of the Editing Task window of the Process Definition form.

3.9.2 To Modify a Response

The following procedure demonstrates how to edit a response.

1. Select the adapter that contains the response you want to edit (for example, the *Create Solaris User* adapter).
2. Click the **Responses** tab.
3. Double-click the field of the response, which contains information that you want to modify.
   a. If the field is a text field, Oracle Identity Manager enables it. You can now edit the contents within this field.
   b. When the field is a lookup field, the Lookup popup window is displayed, containing the different status levels that you can associate with the response. Click the desired **status level**, then click **OK**.

   For example, double-click the **Status** column of the *False* response, select the *Suspended (S)* status level, and click **OK**.
4. On the toolbar, click **Save**.

   The information that you modified for the response is stored in the Oracle Identity Manager database.

3.9.3 To Delete a Response

When a response is no longer necessary, you can delete it from the adapter.

1. Select the adapter, which contains a response that you want to remove.
2. Click the **Responses** tab.
3. Select the response that you want to delete.
4. Click **Delete**.

The response disappears. This indicates that Oracle Identity Manager has deleted the response.

3.10 Scheduling Rule Generators and Entity Adapters

Oracle Identity Manager triggers a process task adapter or a task assignment adapter automatically if it is attached to a process task, and the process task's status is *Pending*. In addition, Oracle Identity Manager always triggers pre-populate adapters on pre-insert. Therefore, you do not schedule when process task adapters, task assignment adapters, or pre-populate adapters will be executed.

On the other hand, a rule generator and an entity adapter are attached to a form field. The only way that Oracle Identity Manager will be able to execute the rule generator or entity adapter is for you to specify when it will be triggered. You do this through the Execution Schedule tab.

> **Note:** If an entity adapter is attached to a process form or an object form for validation of field values, then these adapters will trigger if we edit data in these forms after completing direct or request provisioning.

Using this tab, you can determine that Oracle Identity Manager will trigger the rule generator or entity adapter on preinsert or preupdate. In addition, you can also schedule an entity adapter to be executed on predelete, postinsert, postupdate, and postdelete.

This procedure demonstrates how to configure Oracle Identity Manager to trigger a rule generator or entity adapter.

3.10.1 Scheduling Rule Generators and Entity Adapters

To schedule rule generator and entity adapters:

1. Select the rule generator or entity adapter that you want Oracle Identity Manager to trigger (for example, *Solaris User ID Generator*).

   Note: When you work with process task adapters or pre-populate adapters, you do not use the Execution Schedule tab. As a result, this tab, as well as its contents, are grayed out.

2. Click the **Execution Schedule** tab.

   The contents of the Execution Schedule tab appear.

   The following table will help you understand the various check boxes of the **Execution Schedule** tab:

Name	Description
Pre-Insert	By clicking this check box, Oracle Identity Manager can trigger the rule generator or entity adapter before the record is inserted into the database.
Pre-Update	When you click this check box, Oracle Identity Manager can trigger the rule generator or entity adapter before the record is updated in the database.
Pre-Delete	By clicking this check box, Oracle Identity Manager can trigger the entity adapter before the record is deleted from the database.
Post-Insert	When you click this check box, Oracle Identity Manager can trigger the entity adapter after the record is inserted into the database.
Post-Update	By clicking this check box, Oracle Identity Manager can trigger the entity adapter after the record is updated in the database.
Post-Delete	When you click this check box, Oracle Identity Manager can trigger the entity adapter after the record is deleted from the database.

   Note: By clicking the check boxes of the Execution Schedule tab, you are defining the times when Oracle Identity Manager *can* trigger the rule generator or entity adapter. The Data Object Manager form allows you to specify when Oracle Identity Manager *will* trigger the rule generator or entity adapter.

   For more information about the Data Object Manager form, refer to "Mapping Rule Generator Adapter Variables" on page 6-2.

3. Enable the desired check boxes. Then, from the toolbar, click **Save**.

   The criteria you set for Oracle Identity Manager to execute the rule generator or entity adapter is stored in the Oracle Identity Manager database.

4

About Process Task Adapters

This chapter describes the process task adapters. It contains the following topics:

- Introduction to Processes and Process Tasks
- How a Process Task Adapter Works
- Attaching Process Task Adapters to Process Tasks
- Removing Process Task Adapters from Process Tasks

4.1 Introduction to Processes and Process Tasks

A process task adapter is Java code created through the adapter factory. It enables the Oracle Identity Manager to automatically execute process tasks in provisioning processes.

Each process and process task has a status, which indicates the stage of its completion. The statuses for a process or process task are listed in the following table in the order of importance.

> **Note:** The UT, UCR, and XLR statuses are not mentioned in the following table. Do not use these status values because they have been deprecated and will be removed in a future release of Oracle Identity Manager.

Task Status	Description
C	Completed: This process/process task has been completed successfully.
MC	Manually Completed: This process task has been completed successfully by an Oracle Identity Manager user (that is, manually).
P	Pending: This process/process task is in the process of being completed. All preceding tasks and processes, respectively, have been completed.
PX	Pending Cancellation: This process task will be canceled, but this task has to be completed first before it can be canceled.
R	Rejected: This process/process task has not been completed successfully or has not been approved. The status of rejected process tasks can only be changed to *Canceled* or *Unsuccessfully Completed*.

Task Status	Description
S	Suspended: This process/process task has been put on hold temporarily.
UC	Unsuccessfully Completed: This process task has been set to *Completed*. However, it had been rejected before.
W	Waiting: This process/process task cannot be completed until all preceding process tasks or processes are completed.
X	This process/process task has been stopped. Its status cannot change anymore

The status level of a process represents the most important status level of its process tasks, which must be completed for the process to be completed. Suppose a process has three process tasks, each process task has a different status level (*Completed*, *Waiting*, and *Rejected*), and all three process tasks must be completed for the process to be completed. Because the highest task status level is *Rejected*, the status level of the process is also *Rejected*.

A process task can be managed in one of the following ways:

- It can be handled manually by using the Object Process Console tab of the Organizations or Users forms, or the Oracle Identity Manager Web Application.
- An Oracle Identity Manager process can be configured so that one (or more) of its tasks is triggered automatically once it achieves a status of *Pending*.

The Java code that enables Oracle Identity Manager to automatically execute a process task is referred to as a process task adapter. The Oracle Identity Manager tool that allows developers to create and manage process task adapters is known as the Adapter Factory.

Note: For more information about handling process tasks manually, refer to the *Oracle Identity Manager Administrative and User Console Guide*.

4.2 How a Process Task Adapter Works

After you create a process task adapter, you attach it to the appropriate process task by using the Integration tab of the Process Definition form. From this tab, you can also map any variables of the adapter to their proper locations, which were designated as either *Resolve at Run time* or as an adapter return variable.

For example, the adapter named *adpSOLARISPASSWORDUPDATED* is connected to the *Password Updated* task of the *Solaris* process.

After you attach an adapter to a process task, for the adapter to be functional, it might need data from fields of other forms. For this example, the *adpSOLARISPASSWORDUPDATED* adapter cannot work unless it obtains the following information:

- The user's Oracle Identity Manager ID and password.
- The user's Solaris ID and password.
- The IP address where Solaris is located.

Therefore, it must get this information from the *UserID*, *Passwd*, *SolarisUserID*, *SolarisUserPasswd*, and *ServerAddress adapter* variables respectively. These five variables

are created by using the Adapter Factory form. The "Y" that precedes each adapter variable signifies that it has been mapped correctly.

The form that enables you to create process-specific fields, which will be used by a process to obtain the information it needs, is called the Form Designer. When you create these fields, Oracle Identity Manager stores them into a table. Then, by associating this table with a process (through the Table Name lookup field of the Process Definition form), the adapter, which you attach to a task of this process, will use the table to retrieve the appropriate data.

If you want to modify this table, you can do so through the Form Designer form.

The *UD_SOLARIS* table contains two fields: *UD_SOLARIS_USERID* and *UD_SOLARIS_PASSWD*. By accessing this record of the Form Designer form, you can edit the fields of the table.

Note: For more information about using the Form Designer form to create and modify process-specific fields, refer to the *Oracle Identity Manager Administrative and User Console Guide*.

Once you attach the process task adapter to a dependent process task, and the status of this process task is *Pending* (the status of the previous process task is *Completed*), Oracle Identity Manager will trigger the adapter automatically. When the process task is an independent task, Oracle Identity Manager will execute the adapter as soon as the process is requested.

The result of the adapter being executed represents the state of the process task. When the adapter is finished successfully, the process task to which this adapter is attached will have a status of *Completed*.

On the other hand, if the adapter cannot perform its designated function, the process task to which this adapter is attached will have a status of *Rejected*. By discovering the cause of the error, you can modify the process task and/or adapter so it can run successfully.

Note: To determine why a process task might have failed:

Find the process task. When the process task has not yet been provisioned to the target user or organization, it is located in the To Do List or Pending Approvals. To find the task:

1. Log in as the user.
2. Select the To Do List link or the Pending Approvals links in the left side of the window.

4.3 Attaching Process Task Adapters to Process Tasks

In the previous chapter, you learned how to create a process task adapter. You must attach it to a process task to execute that process task automatically.

To connect an adapter to a process task, access the Integration tab (from the Process Definition form). From this tab, you can also map any adapter variables to their proper locations.

The following procedure shows you how to attach a process task adapter to a process task:

1. Open the Process Definition form, which is located in the Process Management folder.

   In the Oracle Identity Manager Workspace, the Process Definition form appears.

2. Select the process, which contains a task to which you want to attach an adapter. The selected process, along with its tasks, appears in the Process Definition form. For this example, the Solaris process has been selected.

3. Double-click the row header of the task to which you want to attach an adapter. The Editing Task window appears, containing information about the task (for example, the *Password Updated* process task).

4. Click the **Integration** tab.

5. Click **Add**.

   The Handler Selection window appears.

6. To access Oracle Identity Manager adapters, click the **Adapter** option.

   The adapters appear, which you can attach to the process task.

7. From this region, select the adapter that you want to attach to the process task, for example, the adp*SOLARISPASSWORDUPDATED* adapter.

   Tip: For classification purposes, the first three letters of each adapter's name are adp. For classification purposes, the first three letters of each adapter's name are *adp*.

8. From the Handler Selection window's toolbar, click **Save**.

   A dialog box appears, stating that the adapter was successfully added to the process task.

9. Click **OK**.

   The dialog box disappears, and the **Integration** tab is now active. This tab now displays the following:

   - The name of the adapter that is attached to the process task;
   - The status of the adapter; and
   - The names, descriptions, and mapping statuses of the adapter's variables.

   Note: An adapter can have one of three mapping statuses:

   Ready. This adapter has been successfully compiled, and all of its variables have been mapped correctly.

   Mapping Incomplete. This adapter has been successfully compiled, but at least one of its variables have not been mapped correctly.

   Adapter Unavailable. After this adapter had been compiled successfully, it was modified, and recompiled.

   Note: If an adapter does not have any mappable variables, the Adapter Variables region is empty. In addition, the Status field will display either *Ready* or *Adapter Unavailable*, depending on whether the adapter has to be recompiled.

Note: A mappable adapter variable either has been designated as *Resolve at Run time* or it is an adapter return variable.

Note: Once you attach the adapter to the process task, any responses that you defined for the adapter appear in the Responses tab of the Editing Task window.

10. Set the mappings for each variable that appears in the Adapter Variables region of the Integration tab. To do so, double-click the row header of the variable you want to map (for example, *SolarisUserID*).

The Data Mapping for Variable window is displayed.

The following table describes the fields of the Data Mapping for Variable window:

Field Name	Description
Variable Name	This field displays the name of the adapter variable for which you are setting a mapping (for example, *SolarisUserID*).
Data Type	This field shows the data type of the adapter variable (for example, *String* is the data type for the *SolarisUserID* variable).
Map To	This field contains the types of mappings that you can set for the adapter variable (for example, *IT Resources*).When you map the adapter variable to a location or a contact, Oracle Identity Manager enables the adjacent combo box. From this combo box, select the specific type of location or contact to which you are mapping the adapter variable. In addition, if you map the adapter variable to a custom process form, and this form contains child table(s), Oracle Identity Manager enables the adjacent combo box. From this combo box, select the child table to which you are mapping the adapter variable. If you are not mapping the adapter variable to a location, contact, or child table of a custom process form, this combo box is grayed out.
Qualifier	This field contains the qualifiers for the mapping you selected in the **Map to** combo box (for example, *IT Asset*).
IT Asset Type	This field enables you to select a specific IT Resource (for example, *Solaris*) when you map an adapter variable to an IT Resource, and this variable's data type is *String*. If you are not mapping the adapter variable to an IT Resource, or the variable's data type is not *String*, this field does not appear.
IT Asset Property	This field enables you to select a specific field that will receive the results of the mapping (for example, *User Name*), when you map an adapter variable to an IT Resource, and this variable's data type is *String*. If you are not mapping the adapter variable to an IT Resource, or the variable's data type is not String, this field does not appear. **Important**: The **IT Asset Type** and **IT Asset Property** fields are included within this window for backward compatibility. The preferred way is to create an adapter variable with a data type of *IT Resource,* in which case these fields will not appear.
Literal Value	When you map the adapter variable to a literal, use this field to specify the specific literal value. If you are not mapping the adapter variable to a literal, this field does not appear.

Field Name	Description
Old Value	By selecting this check box, you map the adapter variable to the value that was originally in the selected Qualifier field before modification. Process task adapters associated with process tasks are conditionally triggered when some field on the process form gets changed. If you click the Old Value option, and the process task is marked Conditional, then the value that is passed to the adapter is the previous value of the field, before it got modified. This is useful in cases of fields that accept passwords. For example, if you want to disallow setting the password to the same value, you can use the old value for comparison. If you are not mapping the adapter variable to a field that belongs to a child table of a custom process form, this check box is grayed out.

11. Complete the Map To, Qualifier, IT Asset Type, IT Asset Property, Literal Value, and Old Value fields.

    Note: For more information about which mappings to select, refer to the "Adapter Variable Mapping" section in *Oracle Identity Manager Reference*

12. On the toolbar, click **Save**. Then, click **Close**.

    The Data Mapping for Variable window disappears. The **Integration** tab is active again.

13. On the Editing Task window toolbar, click **Save**.

    The contents in the **Status** field change from *Mapping Incomplete* to *Ready*. In addition, the mapping statuses for the adapter's variables change from *No (N)* to *Yes (Y)*.

14. On the toolbar, click **Close**.

    The Editing Task window disappears, and the main screen is active once again. The adapter you added to the *Password Updated* task (*adpSOLARISPASSWORDUPDATED*) appears in the **Process Definition** form.

    This signifies that the *adpSOLARISPASSWORDUPDATED* process task adapter was attached to the *Password Updated* process task.

    Tip: Once you attach a process task adapter to a process task, a quick way to see the process and task to which it is connected is by accessing the Usage Lookup tab of the Adapter Factory form.

4.4 Removing Process Task Adapters from Process Tasks

If a process task adapter is no longer necessary for Oracle Identity Manager to complete the process task automatically, or when you wish to attach a different adapter to a process task, you must first remove the adapter that is attached to the process task.

This procedure will show you how to remove a process task adapter from a process task.

4.4.1 To Remove a Process Task Adapter from a Process Task

1. Open the Process Definition form.

In the Design Console workspace, the **Process Definition** form appears.

2. Select the process, which contains a task from which you want to remove an adapter (for example, the *Solaris* process).

   The selected process, along with its tasks, appears in the **Process Definition** form.

3. Double-click the row header of the process task from which you want to remove the adapter (for example, the *Password Updated* task).

   The Editing Task window appears, containing information about the process task. Click the Integration tab.

4. Click the **Integration** tab.

   The Integration tab displays information about the adapter that is attached to the process task.

5. Click **Remove**.

   A dialog box appears, asking if you want to remove the adapter from the process task.

6. Click **OK**.

   A dialog box appears, signifying that the adapter has been removed from the process task.

7. Click **OK**.

   The contents of the adapter no longer appear in the Integration tab.

8. On the toolbar, click **Close**.

   The Editing Task window disappears, and the main screen is active once again. The adapter that was once linked to the *Password Updated* task *(adpSOLARISPASSWORDUPDATED)* no longer appears in the child table of the **Process Definition** form.

   This signifies that you have removed the adapter from the process task.

5

Applying Task Assignment Adapters

This chapter describes the process of applying task assignment adapters. It contains the following topics:

- "Overview" on page 5-1
- "Attaching Task Assignment Adapters to Process Tasks" on page 5-2
- "Removing Task Assignment Adapters from Process Tasks" on page 5-5

5.1 Overview

For a process task that must be completed manually, you can configure Oracle Identity Manager to automate the assignment of the task to either a specific user or to a user who belongs to a particular user group.

The Java code that enables Oracle Identity Manager to assign a process task to a user or group automatically is known as a task assignment adapter.

For efficiency purposes, a task assignment adapter can be used repeatedly for different process tasks. In addition, multiple task assignment adapters can be designated to be associated with a particular task. Therefore, Oracle Identity Manager selects the task assignment adapter for the process task. This occurs through task assignment rules.

Task assignment rules are criteria. These standards enable Oracle Identity Manager to select the task assignment adapter that is to be used to allocate the process task to the target user or group.

> **Note:** In other words, the task assignment rule allows Oracle Identity Manager to decide whether to assign a process task to a user or group. The task assignment adapter enables Oracle Identity Manager to determine which user or group will be the recipient of the process task.

Each task assignment adapter has a task assignment rule associated with it. In addition, every rule has a priority number, which indicates the order in which Oracle Identity Manager will trigger it.

For this example, Oracle Identity Manager will trigger the Associate Adapter with User rule first (because it has the highest priority). If the condition of this rule is TRUE, then it is successful. As a result, Oracle Identity Manager will associate the related task assignment adapter (the Assign Task to User adapter) with the Get Solaris UUID process task.

On the other hand, when the condition of a rule is FALSE, then the rule has failed. Oracle Identity Manager will then trigger the rule with the next highest priority. If this rule is successful, then Oracle Identity Manager will assign the designated adapter to the target process task.

So, in this example, if the Associate Adapter with User rule fails, then Oracle Identity Manager will trigger the Associate Adapter with Group rule. If this rule is successful, then Oracle Identity Manager will attach the related task assignment adapter (the Assign Task to Group adapter) to the Get Solaris UUID process task.

After assigning a rule to a task assignment adapter, if this type of adapter contains adapter variables, then you must map these variables to their proper locations. Otherwise, the adapter will not be functional.

Finally, when a task assignment adapter either becomes invalid, or is no longer necessary for Oracle Identity Manager to allocate the process task to a user or group, you must remove the adapter from the task.

The following sections demonstrate how to attach a task assignment adapter to a process task, and remove a task assignment adapter from a process task.

5.2 Attaching Task Assignment Adapters to Process Tasks

In the Chapter 3, "Creating Adapters", you learned how to create a task assignment adapter. You must attach it to a process task so that Oracle Identity Manager can automate the assignment of the task to a user or group.

To connect a task assignment adapter to a process task, access the Assignment tab (from the Process Definition form). From this tab, you can also map any adapter variables to their proper locations.

This procedure will show you how to attach a task assignment adapter to a process task.

5.2.1 To Attach a Task Assignment Adapter to a Process Task

1. Open the Process Definition form, which is located in the Process Management folder.

   Within the Oracle Identity Manager workspace, the Process Definition form appears.

2. Select the process, which contains a task to which you want to attach an adapter.

   The selected process, along with its tasks, appears in the Process Definition form.

3. Double-click the row header of the task to which you want to attach a task assignment adapter.

   The Editing Task window appears, containing information about the task (for example, the Get Solaris UUID process task).

4. Click the **Assignment** tab. The Assignment dialog box is displayed.

5. From this tab, click **Add**.

   A blank row appears within the Assignment tab.

   The following table lists the relevant fields of the Assignment tab:

Field Name	Description
Priority	From this field, set the priority number for the associated task assignment rule.
Rule	From this lookup field, select the rule that will determine if the associated adapter will be used to automate the assignment of the process task to a user or group.
Target Type	From this lookup field, specify whether the task is to be assigned to an Oracle Identity Manager user or group.
Adapter	From this lookup field, select the adapter that is to be associated with the designated task assignment rule.
Adapter Status	This field displays the mapping status of the adapter's variables. To learn more about the various mapping statuses for an adapter, refer to the "Attaching Process Task Adapters to Process Tasks" on page 4-3.

6. Double-click the **Priority** field. From this field, set the priority number for the associated task assignment rule.
7. Double-click the **Rule** lookup field. From the Lookup dialog box that is displayed, select the rule that will determine if the associated adapter will be used to automate the assignment of the process task to a user or group.
8. Double-click the **Target Type** lookup field. From the Lookup dialog box that is displayed, specify whether the task is to be assigned to an Oracle Identity Manager user or group.
9. Double-click the **Adapter** lookup field. From the Lookup dialog box that is displayed, specify the task assignment adapter that is to be associated with the rule you selected in Step 7 of this procedure.
10. On the toolbar that is displayed within the Assignment tab, click **Save**.

    The mapping status of the task assignment adapter variables is displayed within the Adapter Status field. Use the following table to decide which action to perform, based on the adapter's mapping status.

Mapping Status	Action
Ready	The adapter does not have any variables that can be mapped. In other words, none of the adapter variables are return variables or have been designated as Resolve at Run time. So, proceed to Step 14 of this procedure.
Mapping Incomplete	At least one of the adapter's variable must be mapped. So, proceed to Step 11 of this procedure.
Adapter Unavailable	After the adapter had been compiled successfully, it was modified. As a result, you must recompile the adapter.

Note: To learn more about the various mapping statuses for an adapter, refer to the "Attaching Process Task Adapters to Process Tasks" on page 5-2.

11. Click **Map**.

    The Adapter Variables window appears. It displays the following information:

- The name of the task assignment adapter that is attached to the process task;
- The status of the adapter; and
- The mapping statuses, names, and descriptions of the adapter's variables.

12. Set the mappings for each variable that appears in the **Adapter Variables** region of this window. To do so, double-click the row header of the variable you want to map (for example, UUID).

The Edit Data Mapping for Variable dialog box is displayed.

The following table lists the fields of the Edit Data Mapping for Variable dialog box is displayed:

Field Name	Description
Variable Name	This field displays the name of the adapter variable for which you are setting a mapping (for example, UUID).
Data Type	This field shows the data type of the adapter variable (for example, *String* is the data type for the UUID variable).
Map To	This field contains the types of mappings that you can set for the adapter variable (for example, IT Resources). When you map the adapter variable to a location or a contact, Oracle Identity Manager enables the adjacent combo box. From this combo box, select the specific type of location or contact to which you are mapping the adapter variable. In addition, if you map the adapter variable to a custom process form, and this form contains child table(s), then Oracle Identity Manager enables the adjacent combo box. From this combo box, select the child table to which you are mapping the adapter variable. If you are not mapping the adapter variable to a location, contact, or child table of a custom process form, this combo box is grayed out.
Qualifier	This field contains the qualifiers for the mapping you selected in the Map To combo box (for example, IT Asset).
IT Asset Type	This field enables you to select a specific IT Resource (for example, *Solaris*) when you map an adapter variable to an IT Resource, and this variable's data type is String. If you are not mapping the adapter variable to an IT Resource, or the variable's data type is not String, this field does not appear.
IT Asset Property	This field enables you to select a specific field that will receive the results of the mapping (for example, Unique ID), when you map an adapter variable to an IT Resource, and this variable's data type is *String*. If you are not mapping the adapter variable to an IT Resource, or if the variable's data type is not String, then this field does not appear. I**mportant**: The IT Asset Type and IT Asset Property fields are included within this window for backward compatibility. The preferred way is to create an adapter variable with a data type of IT Resource, in which case these fields will not appear.
Literal Value	When you map the adapter variable to a literal, use this field to specify the specific literal value. If you are not mapping the adapter variable to a literal, then this field does not appear.

Field Name	Description
Old Value	By selecting this check box, you map the adapter variable to the value that was originally in the selected Qualifier field before modification. Process task adapters associated with process tasks are conditionally triggered when some field on the process form is changed. If you click the Old Value option, and the process task is marked Conditional, then the value that is passed to the adapter is the previous value of the field. This is useful in cases of fields that accept passwords. For example, if you want to disallow setting the password to the same value, you can use the old value for comparison. If you are not mapping the adapter variable to a field that belongs to a child table of a custom process form, this check box is grayed out.

13. Complete the Map To, Qualifier, IT Asset Type, IT Asset Property, Literal Value, and Old Value fields.

    Note: For more information about which mappings to select, refer to the "Adapter Mapping Information" section in *Oracle Identity Manager Reference*.

14. On the toolbar, click **Save**. Then, click **Close**.

    The Edit Data Mapping for Variable window disappears. The Adapter Variables dialog box is active again.

    The contents in the Status field change from Mapping Incomplete to Ready. In addition, the mapping statuses for the adapter's variables change from No (N) to Yes (Y).

15. Click **Save**. Then, click **Close**.

    The Adapter Variable dialog box disappears, and the Assignment tab is active once again.

    The adapter that you assigned to the process task (for example, *Assign Solaris Task*) now has a status of Ready.

16. From the toolbar that appears within the Assignment tab, click **Save** and **Close**

    The Assignment tab disappears, and the main screen is active once again. This signifies that the task assignment adapter is attached to the process task.

    Note: Once you attach a task assignment adapter to a process task, a quick way to see the process and the task to which it is connected is by accessing the Usage Lookup tab of the Adapter Factory form.

5.3 Removing Task Assignment Adapters from Process Tasks

When a task assignment adapter either becomes invalid, or is no longer necessary for Oracle Identity Manager to allocate the process task to a user or group, you must remove the adapter from the task.

5.3.1 To Remove a Task Assignment Adapter from a Process Task

To detach a task assignment adapter from a process task, perform the following tasks:

1. Open the Process Definition form.

   The Process Definition form appears in the Design Console workspace.

2. Select the process, which contains a task from which you want to remove an adapter (for example, the Solaris 8 process).

   The selected process, along with its tasks, appears in the Process Definition form.

3. Double-click the row header of the process task from which you want to remove the adapter (for example, the Get Solaris UUID task).

   The Editing Task dialog box is displayed, containing information about the process task.

4. Click the **Assignment** tab.

   The Assignment tab appears, displaying information about the adapter that is attached to the process task.

5. Highlight the row, containing the adapter that you want to remove from the process task.

6. Click **Delete**. The adapter no longer appears within the Assignment tab.

7. Click **Save**. Then, click **Close**.

   The Assignment tab disappears, and the Main Screen is active once again. This signifies that the task assignment adapter is removed from the process task.

6

Understanding Rule Generators

This chapter describes the rule generators. It contains the following topics:

- "Overview" on page 6-1
- "Mapping Rule Generator Adapter Variables" on page 6-2
- "Associating Rule Generators with Processes" on page 6-5
- "Removing Rule Generators from Form Fields" on page 6-5

6.1 Overview

To perform field validations and enter default values into forms, which either come packaged with Oracle Identity Manager or are created by Oracle Identity Manager users, certain business rules must be applied. For example, for the Users form, you might want Oracle Identity Manager to generate the User ID automatically by concatenating the user's first name and last name.

To do this, you must create a specific type of adapter, which is designed to modify the field value in a form. You can do this by using the Adapter Factory form. Then, when you attach this adapter to the form, Oracle Identity Manager will automatically update the field value for all records of that form, and save this information to the Oracle Identity Manager database.

This type of adapter, which can generate, modify, or verify the value of a form field automatically, is called a rule generator. Oracle Identity Manager triggers a rule generator on preinsert and preupdate.

If you create a rule generator and it contains adapter variables, then you must map these adapter variables to their proper locations. Otherwise, the adapter will not be functional.

Also, you can attach this adapter to a provisioning process for the adapter to work. Then, once the process is provisioned to a target user or organization, Oracle Identity Manager will trigger the associated rule generator.

On occasion, a rule generator, which has been assigned to a provisioning process, might no longer be needed for the process to be completed. If this happens, then you can remove the rule generator from the provisioning process. Similarly, after you attach one rule generator to a form field, you can connect a different rule generator to that form field. When this occurs, you must first remove the rule generator that is currently attached to the form field.

The following sections will show you how to:

- Map the adapter variables of a rule generator.

- Associate rule generators with provisioning processes.
- Remove a rule generator from a form field.

6.2 Mapping Rule Generator Adapter Variables

In the Chapter 3, "Creating Adapters", you learned how to create a rule generator. Now, you must map the adapter variables of the rule generator to their proper locations. This will ensure that the adapter will work.

To map these adapter variables, access the Data Object Manager form from the Development Tools/Business Rule Definition folder of the Design Console.

To map the adapter variables of a rule generator to their proper locations:

1. Open the Data Object Manager form. In the Design Console workshops, the Data Object Manager form is displayed.

   The following table lists and describes the various regions of the Data Object Manager form:

Name	Description
Form Description Field	From this lookup field, select the form that contains the field to which you are attaching the rule generator.
Data Object Field	This field displays the name of the data object, which is represented by the selected form.
Attach Handlers Tab	This tab displays: ■ The rule generators that are attached to the selected form. ■ The execution schedule of the rule generators associated with this form. ■ The order in which Oracle Identity Manager will run the rule generators. ■ Insert, update, and delete permissions for user groups.
Map Adapters Tab	This tab displays: ■ The names of the rule generators that are associated with the form; ■ The status of these adapters. ■ The names, descriptions, and mapping statuses of the rule generators' adapter variables. **Note**: The Map Adapters tab is grayed out until an adapter is assigned to the current data object. For more information about assigning an adapter to a data object, refer to *Oracle Identity Manager Administrative and User Console Guide*.

2. Double-click the **Form Description** field. A Lookup dialog box appears with the forms to which you can attach rule generators.
3. Select the form you want (for example, *Solaris*). Then, click **OK**.
4. On the toolbar, click **Save**.

   The selected form, the form's data object, and the rule generator adapters associated with the form appear. In addition, Oracle Identity Manager enables the Map Adapters tab.

For this example, the Solaris form has been selected. Its data object appears, along with the four rule generator adapters associated with it (adpCONVERTTOLOWERCASE, adpSOLARISHMDSTRINGGEN, adpSETSOLARISASSET, and adpSETPASSWORDFROMMAIN). Oracle Identity Manager will trigger these four rule generators on preinsert.

Based on the sequence numbers of these adapters, Oracle Identity Manager will trigger the adpCONVERTTOLOWERCASE adapter first, followed by the adpSOLARISHMDSTRINGGEN, adpSETSOLARISASSET, and adpSETPASSWORDFROMMAIN adapters respectively.

Tip: To change the sequence of triggering a rule generator:

1. Click **Assign**. The Event Handlers dialog box is displayed.
2. Select the rule generator from.
3. Click the up arrow and down arrow buttons to modify the order of the rule generator.

For these rule generators to work properly, you must map the adapter variables to their proper locations.

5. Click the **Map Adapters** tab.
6. From the Name combo box, select the rule generator, which has adapter variables that can be mapped (for example, the adpCONVERTTOLOWERCASE rule generator).

   The Map Adapters tab now displays the following:

   - The name of the rule generator that is to be attached to the form.
   - The status of the rule generator.
   - The names, descriptions, and mapping statuses of the rule generator's adapter variables.

   Note: To learn more about the various mapping statuses for an adapter, refer to the "Attaching Process Task Adapters to Process Tasks" on page 4-3.

7. Set the mappings for each variable that appears in the Adapter Variables region of the Map Adapters tab. To do so, double-click the row header of the variable you want to map (for example, *Data*). The Data Mapping for Variable dialog box is displayed.

   The following table describes the various fields of the Data Mapping for Variable dialog box:

Field Name	Description
Variable Name	This field displays the name of the adapter variable for which you are setting a mapping (for example, Data).
Data Type	This field shows the data type of the adapter variable (for example, String is the data type for the Data adapter variable).

Field Name	Description
Map To	This field contains the source and target locations of the mappings you can set for the adapter variable (for example, User Definition). When you map the adapter variable to a location or a contact, Oracle Identity Manager enables the adjacent combo box. From this combo box, select the specific type of location or contact to which you are mapping the adapter variable. If you are not mapping the adapter variable to a location or contact, this combo box is grayed out.
Qualifier	This field contains the qualifiers for the mapping you selected in the Map To combo box (for example, User Login).
IT Asset Type	This field enables you to select a specific IT Resource (for example, *Solaris*) when you map an adapter variable to an IT Resource, and this variable's data type is String. If you are not mapping the adapter variable to an IT Resource, or the variable's data type is not String, this field does not appear.
IT Asset Property	This field enables you to select a specific field that will receive the results of the mapping (for example, *User Name*), when you map an adapter variable to an IT Resource, and this variable's data type is String. If you are not mapping the adapter variable to an IT Resource, or the variable's data type is not *String*, this field does not appear. **Important**: The IT Asset Type and IT Asset Property fields are included within this window for backward compatibility. The preferred way is to create an adapter variable with a data type of IT Resource, in which case these fields will not appear.
Literal Value	When you map the adapter variable to a literal, type the name of the specific literal in this field (for example, IBM). If you are not mapping the adapter variable to a literal, this field does not appear.

Complete the Map To, Qualifier, IT Asset Type, IT Asset Property, and Literal Value fields.

Note: For more information about which mappings to select, refer to the "Adapter Mapping Information" section in *Oracle Identity Manager Reference*.

8. Click **Save**. Then, click **Close**

   The Data Mapping for Variable window disappears. The Map Adapters tab is active again.

9. On the main screen toolbar, click **Save**.

Repeat Steps 7 and 8 for all adapter variables that can be mapped.

The contents in the Status field change from Mapping Incomplete to Ready. In addition, the mapping statuses for the adapter variables change from *No (N)* to *Yes (Y)*.

This signifies that all the adapter variables for the rule generator adapter have been mapped correctly. You are now ready to attach this rule generator to a provisioning

process, so it can be triggered after the process is provisioned to a target user or organization.

Tip: When you map all the adapter variables for a rule generator that is associated with a form, a quick way to see the form to which it is attached as well as the execution schedule of the rule generator, is by accessing the Usage Lookup tab of the Adapter Factory form.

After the rule generator is assigned to a process, and the process is provisioned, the rule generator will be executed by Oracle Identity Manager.

6.3 Associating Rule Generators with Processes

After you map the adapter variables of a rule generator to their proper locations, you must attach it to a provisioning process. Then, once the process is provisioned to a target user or organization, Oracle Identity Manager will trigger the associated rule generator.

Similarly, when a rule generator, which has been assigned to a provisioning process, is no longer needed for the process to be completed, you must remove the rule generator from the provisioning process.

To assign a rule generator to a provisioning process or remove a rule generator from a provisioning process, access the Event Handlers/Adapters tab in the Process Definition form. This form can be found in the Process Management folder.

6.4 Removing Rule Generators from Form Fields

Sometimes, after you attach a rule generator to a form field, you can connect a different rule generator to that form field. When this occurs, you must first remove the rule generator that is currently attached to the form field.

Caution: If you remove a rule generator from a form and if the class name of the form's data object matches the table name of a provisioning process, then you will not be able to assign the rule generator to that provisioning process.

For example, suppose the adpCONVERTTOLOWERCASE rule generator is removed from the Solaris form. If the class name of the form's associated data object is UD_SOLARIS, then the rule generator cannot be assigned to any provisioning process with a table name of UD_SOLARIS.

To remove a rule generator from a form field, perform the following steps:

1. Open the Data Object Manager form.
2. Select the form that contains a rule generator you want to remove.
3. The selected form, along with its rule generators, appear in the Data Object Manager form.
4. Click the rule generator that you want to remove from the form field.
5. Click **Delete**.

The selected rule generator no longer appears in the Data Object Manager form. This indicates that you have removed the rule generator from the form field.

Caution: **If you attempt to remove a rule generator from a form field, and if an error box appears, then the adapter has already been associated with a provisioning process. First, detach the rule generator from the process. Then, you can remove it from the form field.**

7

Using Prepopulate Adapters

This chapter describes the prepopulate adapters. It contains the following topics:

- "Overview" on page 7-1
- "Attaching Prepopulate Adapters to Form Fields" on page 7-2
- "Removing Prepopulate Adapters from Form Fields" on page 7-5

7.1 Overview

Sometimes, a user-created form contains fields that can be populated by Oracle Identity Manager and fields into which an Oracle Identity Manager user must enter data. When the information that the user types into a field is contingent upon the data that appears in a system-generated field, Oracle Identity Manager must first populate this field. When the form is displayed, an Oracle Identity Manager user can view the system-generated data, and as a result, enter information into the appropriate fields.

For this to happen, you must create a specific type of rule generator. Then, by attaching it to the field that is designated to be system-generated, Oracle Identity Manager will automatically populate this field with the appropriate information, without saving this information to the Oracle Identity Manager database.

This type of rule generator is known as a prepopulate adapter. The data, which is generated by a prepopulate adapter can appear automatically or manually entering it. Oracle Identity Manager displays this information automatically when the Auto-prepopulate check box is selected for a provisioning process. When this check box is cleared, an Oracle Identity Manager user must manually generate the displaying of the data that is generated by the prepopulate adapter. To do this, click the prepopulate button on the form section of the Direct Provisioning wizard in the Web client, while provisioning the form to a user.

You can repeatedly use a prepopulate adapter for different form fields. In addition, you can designate multiple prepopulate adapters to be associated with a particular field. As a result, Oracle Identity Manager must know which prepopulate adapter it must select for the form field. This occurs by using the prepopulate rules.

prepopulate rules are criteria. These rules enable Oracle Identity Manager to select one prepopulate adapter, which is associated with a form field, when this prepopulate adapter is assigned to the field.

Each prepopulate adapter has a prepopulate rule associated with it. In addition, every rule has a priority number, which indicates the order in which Oracle Identity Manager will trigger it.

For this example, Oracle Identity Manager will trigger the Rule for Uppercase User ID rule first because it has the highest priority. If the condition of this rule is TRUE, then it

is successful. As a result, Oracle Identity Manager will attach the related prepopulate adapter (the Display Uppercase Letters for User ID adapter) to the User ID field.

On the other hand, when the condition of a rule is FALSE, then the rule has failed. Oracle Identity Manager will then trigger the rule with the next highest priority. If this rule is successful, then Oracle Identity Manager will attach the associated adapter to the designated field.

So, in this example, if the Rule for Uppercase User ID rule fails, Oracle Identity Manager will trigger the Rule for Lowercase User ID rule. If this rule is successful, Oracle Identity Manager will attach the related prepopulate adapter (the Display Lowercase Letters for User ID adapter) to the User ID field.

After assigning a rule to a prepopulate adapter, if this type of adapter contains adapter variables, then you must map these adapter variables to their proper locations. Otherwise, the adapter will not be functional.

Finally, when a prepopulate adapter, which has been associated with a field, is no longer valid, you must remove the adapter from the field.

7.2 Attaching Prepopulate Adapters to Form Fields

To attach a prepopulate adapter to a form field, perform the following steps:

1. Select the field to which a prepopulate adapter will be attached.
2. Select the rule that will determine if the adapter will be used to populate the designated field with information.
3. Select the adapter that will be associated with the designated field.
4. Set the priority number of the selected rule.
5. Map the adapter variables of the prepopulate adapter to their proper locations.

   Note: To attach a prepopulate adapter to a form field, you must ensure the following:

   - The form is not in an active state. Otherwise, create a new form version.
   - After attaching the adapter, you must activate the form to be able to use it.

6. Open the Form Designer form.
7. Query for the form to which you want to attach a prepopulate adapter (for example, Solaris).
8. Click the **prepopulate** tab.

   The prepopulate adapters, which have already been attached to the form you queried, appear within this tab.

   Note: If no adapters have been attached to a form field, then the prepopulate tab will be empty.

9. Click **Add**.

   The prepopulate Adapters dialog box is displayed.

The following table lists and describes the fields of the Prepopulate Adapters dialog box:

Name	Description
Field Name	This combo box contains a list of all of the form fields to which a prepopulate adapter can be attached.
Rule	From this lookup field, select the rule that will determine if the associated adapter will be used to populate the designated form field with information.
Adapter	From this lookup field, select the adapter that will be associated with the designated field.
Order	From this field, set the priority number of the selected rule.
Adapter Status	This field displays the mapping status of the adapter variables. To learn more about the various mapping statuses for an adapter, refer to the "Attaching Process Task Adapters to Process Tasks" on page 4-3.
Adapter Variables	This area displays the following: ■ Mapped: The mapping statuses of the adapter's variables. "Y" indicates that an adapter variable has been mapped properly; "N" indicates that this variable has not been mapped correctly. ■ Name: The names of the adapter variables. ■ Mapped to: The form fields to which the variables are mapped If an adapter variable is not yet mapped, then the corresponding cell in this column will be empty.

10. From the **Field Name** combo box, select the form field, such as User ID, to which the prepopulate adapter will be attached.
11. Double-click the **Rule** lookup field. From the Lookup dialog box that is displayed, select the rule that will determine if the associated adapter will be used to populate the designated form field with information (for example, Rule for Lowercase User ID).
12. Double-click the **Adapter** lookup field. From the Lookup dialog box that is displayed, choose the adapter that will be associated with the field you selected in Step 10, for example, Display Lowercase Letters for User ID.
13. In the **Order** field, enter the priority number of the rule you selected in Step 11, for example, 2.
14. On the prepopulate Adapters window toolbar, click **Save**.
15. Mapping Incomplete appears within the Adapter Status field. This signifies that the adapter you selected contains variables that have not been mapped correctly. These variables can be mapped to their proper locations. Otherwise, the adapter will not work.
16. Set the mappings for each variable that appears in the Adapter Variables region of the prepopulate Adapters window. To do so, double-click the row header of the variable you want to map, for example, UserID.

    The Map Adapter Variables window is displayed.

    The following table describes the fields of the Map Adapter Variables window:

Field Name	Description
Variable Name	This field displays the name of the adapter variable for which you are setting a mapping (for example, UserID).
Data Type	This field shows the data type of the adapter variable (for example, *String* is the data type for the UserID adapter variable).
Map To	This field contains the types of mappings that you can set for the adapter variable (for example, Process Data). When you map the adapter variable to a location or a contact, Oracle Identity Manager enables the adjacent combo box. From this combo box, select the specific type of location or contact to which you are mapping the adapter variable. If you are not mapping the adapter variable to a location or contact, this combo box is grayed out.
Qualifier	This field contains the qualifiers for the mapping you selected in the **Map to** combo box (for example, User ID).
IT Asset Type	This field enables you to select a specific IT Resource (for example, Solaris) when you map an adapter variable to an IT Resource, and this variable's data type is String. If you are not mapping the adapter variable to an IT Resource, or the variable's data type is not String, this field does not appear.
IT Asset Property	This field enables you to select a specific field that will receive the results of the mapping (for example, *User Name*), when you map an adapter variable to an IT Resource, and this variable's data type is String. If you are not mapping the adapter variable to an IT Resource, or the variable's data type is not String, then this field does not appear. **Important**: The IT Asset Type and IT Asset Property fields are included within this window for backward compatibility. The preferred way is to create an adapter variable with a data type of IT Resource, in which case these fields will not appear.
Literal Value	When you map the adapter variable to a literal, use this field to specify the specific literal value. If you are not mapping the adapter variable to a literal, this field does not appear.

17. Complete the Map To, Qualifier, IT Asset Type, IT Asset Property, and Literal Value fields.

    Note: For more information about which mappings to select, refer to the "Adapter Mapping Information" section in *Oracle Identity Manager Reference*.

18. On the Map Adapter Variable window toolbar, click **Save**. Then, click **Close**.

    The Map Adapter Variables window disappears. The prepopulate Adapters window is active again.

    The text in the Adapter Status field changes from Mapping Incomplete to Ready. In addition, the mapping statuses for the adapter's variables change from No (N) to Yes (Y).

19. On the prepopulate Adapters window toolbar, click **Close**.

The prepopulate Adapters window disappears, and the Form Designer form is active again. The prepopulate adapter, which you attached to the User ID form field (Display Lowercase Letters for User ID), appears in the prepopulate tab of the Results of 1Q Sales 2003 form.

After a process, which references this form, is provisioned to a target user or organization, the form will appear. Oracle Identity Manager will then check to see if the prepopulate rule, which has the highest priority, is valid. If so, then Oracle Identity Manager will assign the associated prepopulate adapter to the designated field (User ID), and execute it. At this point, one of the following actions occur:

- If the Auto-prepopulate check box is selected for the provisioning process, Oracle Identity Manager will display the data that is generated by the prepopulate adapter automatically.
- If the Auto-prepopulate check box is cleared, an Oracle Identity Manager user must manually trigger the displaying of the data that is generated by the prepopulate adapter. To do this, the administrator must click the prepopulate button on the form section of the direct provisioning wizard in the Web client, while provisioning the form to a user.

Tip: Once you allocate a prepopulate adapter to a form field, and assign a prepopulate rule to the adapter, a quick way to see the association among the adapter, the form field, and the rule is by accessing the Usage Lookup tab of the Adapter Factory form.

7.3 Removing Prepopulate Adapters from Form Fields

If a prepopulate adapter, which has been associated with a form field, is no longer valid, then you must remove the adapter from the field.

Note: Before removing the prepopulate adapter from a form field, you must create a new version of the form.

To remove a prepopulate adapter from a form field:

1. Select the prepopulate adapter that you want to remove.
2. Click **Delete**. The prepopulate adapter is removed from the form field. It cannot be triggered when the form is launched.
3. After removing the adapter, you must activate the form.

8

Managing Entities

Similar to rule generator adapters, entity adapters are also responsible for generating, modifying, or verifying the value of a form field automatically, and saving this information to the Oracle Identity Manager database. However, the differences between rule generators and entity adapters are as follows:

- **Execution schedule**. Entity adapters can be triggered by Oracle Identity Manager on preinsert, preupdate, predelete, postinsert, postupdate, and postdelete. A rule generator adapter can be executed only on preinsert and preupdate.
- **Manual field value modification**. The adapter populates the form field to which an entity adapter is attached. An Oracle Identity Manager user should not edit this value because the entity adapter will overwrite this modification. As a result, the modification will not be saved to the database.

  Similarly, the adapter also populates the form field to which a rule generator adapter is attached. However, an Oracle Identity Manager user can edit this value because this modification will take precedence over the value that the rule generator adapter generates. Because of this, the modification will be saved to the database.
- **Background color of form field**. If a rule generator is attached to a form field, then the field will appear in a particular background color such as pink. This is a visual indicator that the field has a rule generator attached to it. On the other hand, when an entity adapter is attached to a form field, the field will not have a distinct background color.

Note: For more information about mapping the variables of an entity adapters with Oracle Identity Manager forms and/or provisioning processes, refer to the procedures in the Chapter 6, "Understanding Rule Generators" on page 6-1.

9

Compiling Adapters

When you are creating multiple adapters and compiling them, you can do so in one of two ways. First, you can access each adapter, and compile it individually. However, this method consumes a lot of time and effort.

A more efficient approach is to either select the adapters that you want to compile, and compile them in one shot, or, when necessary, to compile all adapters that exist in the Oracle Identity Manager database, by clicking a button.

9.1 Automatic Compilation of Adapters

From release 9.1.0 onward, adapters are compiled automatically when you import connector files by using the Deployment Manager. The compiled adapter classfiles are stored in the Oracle Identity Manager database, as opposed to the filesystem, from where they are loaded at run time. The following two APIs have been added to compile adapters programmatically:

- `public void compileAdapter (String adapterName)`: This API compiles a single adapter and stores the compiled classfile in the database. It takes the name of the adapter as a parameter. If the adapter is not found or if there are any errors, then the API throws an appropriate exception.
- `public void compileAll`: This API compiles all adapters in a system. If it encounters any errors during compilation, then it throws an exception of the type `tcBulkException`. This exception comprises all the individual errors that the API encounters during compilation.

However, you can modify the adapters manually if you make changes.

Note: You must set the path of the JDK directory in the `XL.CompilerPath` system property. If this is not done, then an error is encountered during the adapter compilation stage of the process performed when you import an XML file by using the Deployment Manager.

Refer to the "The System Configuration Form" section in *Oracle Identity Manager Design Console Guide* for information about setting values of system properties.

9.2 Compiling Adapters Manually

The Adapter Manager form is located in the Development Tools folder. It is used to compile multiple adapters simultaneously.

To manually compile multiple adapters, perform the following steps:

1. Open the Adapter Manager form.
2. To compile every adapter that resides within the Oracle Identity Manager database, select the **Compile All** option.

   To compile multiple adapters, select the adapters you want to compile. Then, select the **Compile Selected** option.

   To compile all adapters that do not have an OK status, select the **Compile Previously Failed** option.
3. Click the **Start** button.

   Oracle Identity Manager will compile the adapters that match the criteria you specified in Step 2.

   Tip: Oracle Identity Manager lets you look at the record of any adapter that appears within the Adapter Manager form. By doing so, you can see detailed information about the adapter.

   To view an adapter's record, select the desired adapter. Then, either double-click its row header, or right-click the adapter, and select the Launch Adapter command from the menu that appears.

10

Exporting and Importing Adapters

This chapter describes the exporting and importing adapters.

Sometimes, when you create an adapter for one database, you might want to use it with another database. One approach is to manually reconstruct the adapter for that database. However, besides this method being unproductive in terms of time, money, and resources, the developer might inadvertently introduce an error while re-creating the adapter. As a result, after the process with which this adapter is associated is provisioned to the target user or organization, the adapter will not be able to perform its designated function, and Oracle Identity Manager will not be able to provision the corresponding resource to that user or organization.

An alternate method, which is more efficient, and eliminates the chance for error, is to:

1. Create a bug-free adapter and apply it properly within one database. The Deployment Manager, internally, builds a `*.xml` file, which contains this adapter and all of its internal variable mappings.

   The Deployment Manager also exports this file into a designated location.

2. Retrieve the file from the location, and import it into the target database.

You can use Deployment Manager to transfer adapters from one database to another. Refer to the *Oracle Identity Manager Administrative and User Console Guide* for instructions about how to use Deployment Manager.

Note: Any adapter that you import into a target database must be recompiled within that database. Also, you should copy the third-party JAR files, after migrating the adapter. Otherwise, the adapter will not work.

11

Creating and Testing a Remote Manager IT Resource

This chapter describes the tasks for creating and testing a Remote Manager IT Resource. It contains the following topics:

- Postinstallation Configuration
- To Create and Test a Remote Manager IT Resource

Remote Manager is an Oracle Identity Manager component that acts like a proxy in directly communicating with a third-party system. The Remote Manager is used to invoke nonremotable APIs through Oracle Identity Manager and APIs that do not support Secure Sockets Layer (SSL) over secure connections.

After installing the Remote Manager and establishing the trust relation between the Oracle Identity Manager Server and the Remote Manager (trusting the certificate), you can create an IT Resource for the Remote Manager and then test it.

11.1 Postinstallation Configuration

After installing the Remote Manager, you can ensure that the certificate is trusted between the application server and the Remote Manager. To do so, first open the Remote Manager form in the Administration folder of the Design Console. The Remote Manager form shows all Remote Managers that are connected but not necessarily "trusted".

Perform the following steps to ensure that the trust relation between the application server and the Remote Manager is established through the certificate. In this procedure, the JBoss Application Server is used as an example. The keytool utility is used to import/export the certificates.

1. Using a command prompt, open the directory path and use the keytool utility to list the certificate fingerprints:

   XLREMOTE_HOME\xlremote

2. Enter the command:

   JAVA_HOME\jre\bin\keytool -list -keystore config\.xlkeystore

3. Enter the default password for xellerate keystore: `xellerate`

   ```
   Your keystore contains 1 entry

          xell, Jan 7, 2005, keyEntry,

          Certificate fingerprint (MD5):
   ```

B0:F2:33:C8:69:E4:25:A3:CB:59:E8:51:27:EE:5C:52

The certificate fingerprint is marked in bold. Compare this to the list of certificates in the keystore.

4. Open the Java SDK folder used for the application server. Again, enter the path and use the keytool to list the certificates in the keystore:

   JAVA_HOME\jre\lib\security\cacerts

5. Enter the following command to see the list of trusted certificates:

   JAVA_HOME\bin\keytool -keystore cacerts -storepass changeit -storetype jks -provider *provider_name*

   The output showing the keystore entries are as follows:

```
Your keystore contains 25 entries
equifaxsecureebusinessca1, Jul 23, 2003, trustedCertEntry,
Certificate fingerprint (MD5): 64:9C:EF:2E:44:FC:C6:8F:52:07:D0:51:73:8F:CB:3D
verisignclass4ca, Jun 29, 1998, trustedCertEntry,
Certificate fingerprint (MD5): 1B:D1:AD:17:8B:7F:22:13:24:F5:26:E2:5D:4E:B9:10
entrustglobalclientca, Jan 9, 2003, trustedCertEntry,
Certificate fingerprint (MD5): 9A:77:19:18:ED:96:CF:DF:1B:B7:0E:F5:8D:B9:88:2E
gtecybertrustglobalca, May 10, 2002, trustedCertEntry,
Certificate fingerprint (MD5): CA:3D:D3:68:F1:03:5C:D0:32:FA:B8:2B:59:E8:5A:DB
entrustgsslca, Jan 9, 2003, trustedCertEntry,
Certificate fingerprint (MD5): 9D:66:6A:CC:FF:D5:F5:43:B4:BF:8C:16:D1:2B:A8:99
verisignclass1ca, Jun 29, 1998, trustedCertEntry,
Certificate fingerprint (MD5): 51:86:E8:1F:BC:B1:C3:71:B5:18:10:DB:5F:DC:F6:20
thawtepersonalbasicca, Feb 12, 1999, trustedCertEntry,
Certificate fingerprint (MD5): E6:0B:D2:C9:CA:2D:88:DB:1A:71:0E:4B:78:EB:02:41
entrustsslca, Jan 9, 2003, trustedCertEntry,
Certificate fingerprint (MD5): DF:F2:80:73:CC:F1:E6:61:73:FC:F5:42:E9:C5:7C:EE
thawtepersonalfreemailca, Feb 12, 1999, trustedCertEntry,
Certificate fingerprint (MD5): 1E:74:C3:86:3C:0C:35:C5:3E:C2:7F:EF:3C:AA:3C:D9
verisignclass3ca, Oct 24, 2003, trustedCertEntry,
Certificate fingerprint (MD5): 10:FC:63:5D:F6:26:3E:0D:F3:25:BE:5F:79:CD:67:67
gtecybertrustca, May 10, 2002, trustedCertEntry,
Certificate fingerprint (MD5): C4:D7:F0:B2:A3:C5:7D:61:67:F0:04:CD:43:D3:BA:58
thawteserverca, Feb 12, 1999, trustedCertEntry,
Certificate fingerprint (MD5): C5:70:C4:A2:ED:53:78:0C:C8:10:53:81:64:CB:D0:1D
equifaxsecureca, Jul 23, 2003, trustedCertEntry,
Certificate fingerprint (MD5): 67:CB:9D:C0:13:24:8A:82:9B:B2:17:1E:D1:1B:EC:D4
thawtepersonalpremiumca, Feb 12, 1999, trustedCertEntry,
Certificate fingerprint (MD5): 3A:B2:DE:22:9A:20:93:49:F9:ED:C8:D2:8A:E7:68:0D
thawtepremiumserverca, Feb 12, 1999, trustedCertEntry,
Certificate fingerprint (MD5): 06:9F:69:79:16:66:90:02:1B:8C:8C:A2:C3:07:6F:3A
entrust2048ca, Jan 9, 2003, trustedCertEntry,
Certificate fingerprint (MD5): BA:21:EA:20:D6:DD:DB:8F:C1:57:8B:40:AD:A1:FC:FC
verisignserverca, Jun 29, 1998, trustedCertEntry,
Certificate fingerprint (MD5): 74:7B:82:03:43:F0:00:9E:6B:B3:EC:47:BF:85:A5:93
entrustclientca, Jan 9, 2003, trustedCertEntry,
Certificate fingerprint (MD5): 0C:41:2F:13:5B:A0:54:F5:96:66:2D:7E:CD:0E:03:F4
baltimorecybertrustca, May 10, 2002, trustedCertEntry,
Certificate fingerprint (MD5): AC:B6:94:A5:9C:17:E0:D7:91:52:9B:B1:97:06:A6:E4
geotrustglobalca, Jul 23, 2003, trustedCertEntry,
Certificate fingerprint (MD5): F7:75:AB:29:FB:51:4E:B7:77:5E:FF:05:3C:99:8E:F5
gtecybertrust5ca, May 10, 2002, trustedCertEntry,
Certificate fingerprint (MD5): 7D:6C:86:E4:FC:4D:D1:0B:00:BA:22:BB:4E:7C:6A:8E
equifaxsecureglobalebusinessca1, Jul 23, 2003, trustedCertEntry,
Certificate fingerprint (MD5): 8F:5D:77:06:27:C4:98:3C:5B:93:78:E7:D7:7D:9B:CC
baltimorecodesigningca, May 10, 2002, trustedCertEntry,
```

```
Certificate fingerprint (MD5): 90:F5:28:49:56:D1:5D:2C:B0:53:D4:4B:EF:6F:90:22
equifaxsecureebusinessca2, Jul 23, 2003, trustedCertEntry,
Certificate fingerprint (MD5): AA:BF:BF:64:97:DA:98:1D:6F:C6:08:3A:95:70:33:CA
verisignclass2ca, Oct 24, 2003, trustedCertEntry,
Certificate fingerprint (MD5): B3:9C:25:B1:C3:2E:32:53:80:15:30:9D:4D:02:77:3E
```

For clarity, the certificate fingerprints are highlighted in bold. The certificate fingerprint that is required is Certificate fingerprint (MD5.

`B0:F2:33:C8:69:E4:25:A3:CB:59:E8:51:27:EE:5C:52)` is not in the trusted certificates. Therefore, you can import the certificate.

6. Perform the procedure described in the "Trusting the Remote Manager Certificate" section in the installation guide for the application server that you use.

11.2 To Create and Test a Remote Manager IT Resource

To create and test a Remote Manager IT resource, perform the following steps:

Note: If you want to test the Remote Manager IT Resource over a non-SSL connection, then set the `<RMIOverSSL>` property in the following file to `false`:

OIM_HOME\xellerate\config\xlconfig.xml

---

1. In the Design Console, open the Resource Object form.
2. Create a resource object. In this example, the following parameters are set:
   - The name is `MyObj`
   - The option, `Order for User` is enabled
   - The Type is `Application`
   - The following check boxes are available:
     - Allowed Multiple
     - Auto Save
     - Self Request Allowed
     - Allow All
     - Auto Launch
3. Create an IT resource type for the resource object. Open the IT Resource Type Definition form. In this example, the following parameters are set:
   - Server Type: `MyObjServer`.

   Note: While defining the IT Resource Type parameter in the Design Console, you can specify which fields will be encrypted.

   ---

4. Create an IT resource for the Remote Manager. In this example, the following parameters are set:
   - The name of the IT Resource is `remote`.
   - The name of the Type is `Remote Manager`.

Ensure that the IT resource has the proper URL and service name, and that the Remote Manager is installed at the location indicated by the URL.

Note: Check to see if the name itself is not present in the URL. For example, the Remote Manager is composed of the service name and URL, as follows:

service name: RManager url: rmi://w2kevandanwkstn:12346

---

5. Create an instance of the `MyObjServer` IT Resource Type created previously. Open the IT Resource Information Form. In the Remote Manager field, ensure that the Remote Manager created in Step 4 (`remote`) is selected.
6. After saving the information in the IT Resources Information form, you can provide any additional details required for that IT resource. In this example, the user name and password are entered.
7. Create a JAR file for the following code:

```
package testme;
import java.io.PrintStream;
public class test
{
    public test ()
    {
    }
    public static int addme(int i, int j)
    {
     /*6*/System.out.println(i + "+" + j + "=" + (i + j));
     /*7*/return i + j;
     }
     public static void main(String args[])
     {
      /*  11*/addme(5, 10);
     }
}
```

   This code will be run on the Remote Manager.

8. Copy the JAR file into the *`xlremote_home`*`/JavaTasks` and *`OIM_HOME`*`/xellerate/JavaTasks` directories.
9. Create an adapter that will be run in the Remote Manager. Open the Adapter Factory form. In this example, the following parameters are set:
   - The Adapter Name is `remotetest`.
   - The Adapter Type is `Process Task`.

     For this example, you can create three variables for this adapter (based on example code in the .jar file). Click **Add.** The Java code takes two integers as arguments and the IT resource as the third variable.
10. In the first variable, the following parameters are set:
    - The Variable name is `var1`.
    - The Variable type is `Integer`.
    - The Map To option is set to Resolve at Run time.

11. Create the second variable in the same way you did the first. The following parameters are set:
    - The Variable name is `var2`.
    - The Variable type is `Integer`.
    - The Map To option is set to Resolve at Run time.
12. Create the third variable for IT Resource. The parameters are set as follows:
    - The Variable name is `ITRes`.
    - The Variable type is `ITResource`.
    - The Map To option is set to Resolve at Run time.
    - The Resource Type is `MyObjServer`.

    Note: The Resource Type field must be the same "ITResource Type" created in Step 5 and not Remote Manager.

13. Add a New Remote Java Task. In the Adapter Factory Form, click **Add**. Ensure that the Functional Task option is active. Select the **Remote** option. Click **Continue**.
14. The Object Instance Selection dialog box is displayed. Create a new Object Instance. Ensure that the New Object Instance option is active. Click **Continue**.
15. The Remote window is displayed. In this example, the following parameters are set:
    - The Task Name is `remote`.
    - The API Source references the .jar file in the JavaTask folder.
    - The Application API is `Testme.test`.
    - The Constructor is set to `0 public testme.test ()`.
    - The Method is set to `testme.test.addme (int, int)`.

      After clicking **Save**, the IT Resource is automatically added as an argument. The Application Method Parameters are ready for mapping.
16. Begin mapping the parameters by highlighting the first item in the Parameter Data Mapping list. This output parameter is an integer. The following mapping is set:
    - Map To: `Adapter Variables`
    - Name: `Return variable`
17. Click **Set**.
18. Highlight the second parameter to map. This input parameter is an integer. The following mapping is set:
    - Map: `Adapter Variables`
    - Name: `var1`
19. Click **Set**.
20. Select the third parameter to map. This input parameter is an integer. The following mapping is set:
    - Map To: `Adapter Variables`

- Name: `var2`

21. Click **Set**.
22. Select the final parameter to map. Map this ITResource to the variable passed as input to the adapter. The following mapping is set:
    - Map To: `Adapter Variables`
    - Name: `ITRes`
23. Click **Set**.
24. Click **Set**. Then click **Save**. The Adapter Factory form is displayed.
25. Compile the adapter by clicking **Build**.

To invoke the adapter, you can create a provisioning process that calls this adapter as one task. To do this:

1. Open the Process Definition Form. In this example, the following parameters are set:
    - The Name field is `MyObjProv`
    - The Type field is `Provisioning`
    - The Object name is `MyObj`

      The following check boxes are available:
      - Default Process
      - Auto Pre-populate
      - Auto Save Form
2. Click the **Save** icon. The provisioning tasks automatically appear in the Tasks tab.
3. Click **Add** to create a new task. In this example, the parameters are set:
    - The Task Name field is `Call Remote Adapter`.
    - The Task Description field explains the task's function.
4. Click the **Save** icon. Then click the **Integration** tab. Next, click **Add** to add an adapter to this task. The Handler Type window is displayed.
5. Enable the **Adapter** option and select the adapter to be executed.
6. Click the **Save** icon. In the Integration tab, the adapter name appears in the Name field. The Status field shows that the Mapping is incomplete. The Adapter Variables pane shows the variables are not mapped.
7. Select the first variable, Adapter return value, then click **Map**. The Edit Data Mapping for Variable window is displayed. The parameters are set to:
    - Data Type: `Object`
    - Map To: `Response Code`
8. Select the second variable, `var1` then click **Map**. The **Edit Data Mapping for Variable** window appears. The parameters are set to:
    - Data Type: `Integer`
    - Map To: `Literal`
    - Qualifier: `Integer`
    - Literal Value: `10`

9. Select the third variable, var2, then click **Map**. The Edit Data Mapping for Variable window is displayed. The parameters are set to:
   - Data Type: `set to Integer`
   - Map To: `Literal`
   - Qualifier: `Integer`
   - Literal Value: `20`
10. Select the fourth variable, ITRes, and then click **Map**. The Edit Data Mapping for Variable window is displayed. The parameters are set to:
   - Data Type: `IT Resource (MyObjServer)`
   - Map To: `IT Resource`
   - Qualifier: `MyObjServerInstance`
11. Click the **Responses** tab of the Editing Task window. Click **Add** to add the possible responses from the adapter. In this example, the only possible response is 30. Set Description to Completed and Status to C.
12. Click the **Task to Object Status Mapping** tab. In the Completed category, set **Object Status** to Provisioned.
13. At this point, you are ready to directly provision a user with the newly created resource to test the execution of the remote task. However, you must first ensure that the Remote Manager is running. Open the Remote Manager Form and verify that the service is available.
14. Start the Oracle Identity Manager Administrative and User Console and login as Administrator. Navigate to **Users, Manage** and select a user to provision this resource *(MyObj)*. The User Detail page appears with the selected user. In the View Additional Details About This User pull-down option, select **Resource Profile**.
15. The User Detail, Resource Profile page is displayed. Click **Provision New Resource** and select the newly created resource (*MyObj*).
16. The Provision Resource to User wizard is displayed. Click **Continue** to complete the provisioning process.
17. Continue with the provisioning process until you come to the **Resource Successfully Provisioned** page is displayed.
18. Check the Remote Manager log file to see if the code is executed. The Remote Manager log file is located in the *`OIM_HOME`*`/xlremote/log` directory. The last line in the log should be similar to the following:

    ```
    DONE5+10=15
    ```

    The preceding line shows that the two input integers are added to equal 15. This indicates that the code executed correctly and that the resource object was provisioned.

12

SPML Web Service

This chapter discusses the SPML Web Service interface of Oracle Identity Manager.

The following sections of this chapter provide basic information about the SPML Web Service:

- Introduction to the SPML Web Service
- Provisioning Operations Supported by the SPML Web Service

To deploy the SPML Web Service, you can follow the approach described in *one* of the following sections:

- Deploying the SPML Web Service
- Enabling Security by Using Oracle Web Services Manager and Then Deploying the SPML Web Service

The following sections describe procedures to be performed after you deploy the SPML Web Service:

- Postdeployment Tasks
- Enabling SSL Communication

The following section provides an overview of the procedure to develop a client for the SPML Web Service:

- Developing the Client for the SPML Web Service

12.1 Introduction to the SPML Web Service

Organizations can have multiple provisioning systems that exchange information about the modification of user records. In addition, there can be applications that interact with multiple provisioning systems. Connectors can enable the interaction between two provisioning systems or between an application and a provisioning system so that each application synchronizes with the other. However, configuring a custom connector for each combination of these systems leads to a lot of overhead.

The solution to this problem is the application of one common language or protocol that all these systems understand. The answer is SPML.

The SPML Web Service provides a layer over Oracle Identity Manager to interpret SPML requests and convert them to Oracle Identity Manager calls.

> **See Also:** Refer to the following Web page for information about the SPML v2.0 specification:
>
> `http://www.oasis-open.org/specs/index.php#spmlv2.0`

The SPML Web Service supports only inbound provisioning requests. It does not support any type of reconciliation because it does not generate reconciliation events. For example, if you request a resource to be provisioned to an OIM User in which data must be populated in the resource's process form and child table, the request will not be supported. This is because the SPML Web Service is not aware of any information associated with a resource object.

Note: Outbound provisioning requests can be sent by using a generic technology connector containing the SPML Provisioning Format Provider. Refer to *Oracle Identity Manager Administrative and User Console Guide* for information about generic technology connectors.

12.1.1 Functional Architecture of the SPML Web Service

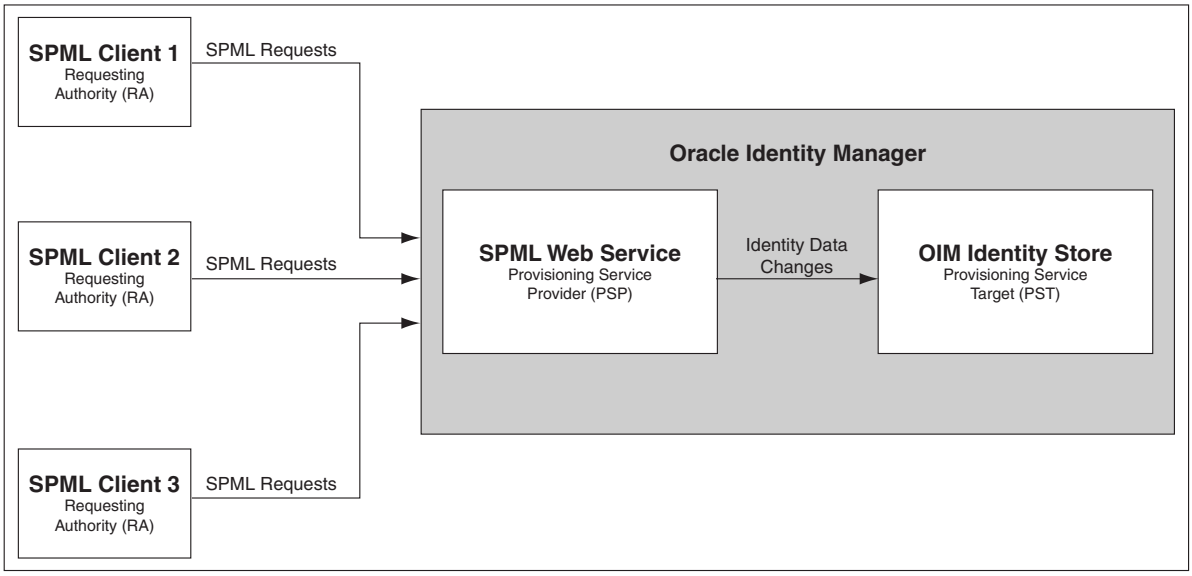
The SPML Web Service sends and receives SPML requests in the form of SOAP messages. The SPML model consists of the following entities that participate in an end-to-end provisioning scenario.

- Requesting Authority (RA): An RA or requestor is the component that issues well-formed SPML requests to a provisioning service provider.
- Provisioning Service Provider (PSP): A PSP or provider is the component that listens for, processes, and returns the results for well-formed SPML requests from a known requestor.
- Provisioning Service Target (PST): A PST or target represents a destination or an endpoint that a provider makes available for provisioning actions.

The implementation of the SPML protocol allows for the reliable exchange of provisioning requests and a model on which you can build a more complex application-level provisioning functionality. SPML is the language of exchanging the management requests used by provisioning systems to manage and control an identity.

Figure 12–1 illustrates the functional architecture of the SPML Web Service.

Figure 12–1 SPML Architecture



The provisioning application can play the role of both an RA and a PSP. Consider the following scenarios:

Provisioning Application as PSP

In this scenario, a client application sends an SPML request to the provisioning application. The provisioning application carried out the request and returns an SPML response to the client application. The request-response exchange is either synchronous or asynchronous. This is typically described as the "inbound" scenario. In Oracle Identity Manager, this is implemented through the SPML Web Service.

Provisioning Application as RA

In this scenario, the provisioning application plays the role of the SPML client and sends an SPML request to a PST, which carries the request and returns an SPML response. The request-response exchange is synchronous or asynchronous. This is typically described as the "outbound" scenario. In Oracle Identity Manager, this is implemented through the generic technology connector containing the SPML Format Provisioning Provider.

Provisioning Application as RA and PSP

Note: This feature is not supported in Oracle Identity Manager release 9.1.0.

In this scenario, a client application sends an SPML request to the provisioning application that cannot itself fulfill the request. Here, the provisioning application forwards the request to the provisioning target that fulfills the request and returns an SPML response. The provisioning application then returns an SPML response to the client application. The request-request-response-response exchange is synchronous or asynchronous.

12.2 Provisioning Operations Supported by the SPML Web Service

The SPML Web Service supports capabilities that meet the minimum conformance criteria described in the SPML v2.0 specification. This section discusses the various operations supported by the SPML Web Service.

Note: The SPML Web Service supports requests in UTF-8 encoding only.

You can use the psoID to uniquely identify an entity (User/Group/Organization) in a provisioning target. In Oracle Identity Manager, to specify an entity, the combination of an objectclass and an entity key is required. An entity key is the database key returned when you create an entity in Oracle Identity Manager. The psoID in Oracle Identity Manager is in the following format:

`objectclass:`*`entitykey`*

For example, objectclass can be Users and entity key can be 3. In this case, the psoID you specify is `Users:3`.

The SPML Web Service supports the following provisioning operations or requests:

- **Add Operations**

The Add Request operation creates an entry for the requested target type in Oracle Identity Manager. The supported target types are User, Group, and Organization. This operation checks if an entry exists and reports errors, if any. This operation can also include capability data for the User and Group target types when it associates a user or group with one or more groups by using the `memberOf` relationship. This function also supports the `administrator` reference capability, which you can use to assign one or more groups as the administrator of a new group.

> **See Also:** The "Add Request" section on page B-1 for a sample Add request

- **Modify Operations**

  The Modify Request operation updates the specified target entry for the requested target type in Oracle Identity Manager. The supported target types are User, Group, and Organization. This operation checks if an entry exists and reports errors, if any. If the entry exists, then the target is updated with the given data. This operation can also modify capability data. For the User target type, the supported reference capability is `memberOf`. This operation can also be used to update the references of the user. The user can be added to or removed from a group.

  Similarly, for the Group target type, the supported reference capabilities are `memberOf` and `administrator`. Modify requests can be used to create, replace, or delete these references.

  > **See Also:** The "Modify Request" section on page B-4 for a sample Modify request

- **Delete Operations**

  The Delete Request operation deletes the specified target entry from Oracle Identity Manager. The supported target types are User, Group, and Organization. This operation checks if an entry exists and reports errors, if any. If the entry exists, it is deleted. The recursive delete option is not supported.

- **Add, Replace, or Delete References**

  References are entities that can be referred to by other entities. For example, user John Doe is a member of a group. Now, you want to remove John Doe from that group and make him a member of another group. You can specify the details of the user in the new group through a reference, and the user becomes the member of the new group.

  The following references are supported by SPML:

  – Add/Replace/Delete Group membership references for users

  – Add/Replace/Delete Group membership references for groups

  – Add/Replace/Delete Group administrator references for groups

- **Lookup Operations**

  The Lookup Request operation looks up the specified target entry in Oracle Identity Manager. The supported target types are User, Group, and Organization. This operation checks if the entry exists, and it returns the lookup data or reports back errors. The user can be looked up in Oracle Identity Manager based on the user ID. The lookup operation also returns any *capability-specific* data that is

associated with the object if you specify everything as the value of `returnData` type.

- **Search Operations**

  The Search Request operation searches for the specified target entry in Oracle Identity Manager. The supported target types are User, Group, and Organization. This operation checks if the entry exists and returns the search response based on whether or not the entry is available.

  Search requests do not support query scope. Even if there is a query scope, it is ignored. The search query is formed by applying the AND operator to the search criteria specified in the request. Different search criteria can be specified in an SPML search request by using the Directory Services Markup Language (DSML) filter. The only operation supported in the DSML filter is `equalityMatch`.

  The `includeDataForCapability` element is not supported. If you specify everything as the value of `returnData`, then the search operation returns all the associated references. The search operation requires object class information based on which it can query the User, Group, and Organization containers. Therefore, it expects an object class as one of the query elements in the search query.

  For example, if you want to perform a search on the Users object class, then this information must be embedded in the request. This is described in the following code sample:

```
<searchRequest
returnData="identifier"xmlns="urn:oasis:names:tc:SPML:2:0:search"
xmlns:dsml="urn:oasis:names:tc:DSML:2:0:core">
 <query scope="pso">
  <basePsoID ID=""/><and>
  <dsml:filter><dsml:equalityMatch name="Users.LastName">
  <dsml:values>Doe
  </dsml:values>
  </dsml:equalityMatch>
  </dsml:filter>
  <dsml:filter><dsml:equalityMatch name="Users.XellerateType">
  <dsml:values>End-User
  </dsml:values>
  </dsml:equalityMatch>
  </dsml:filter>
  <dsml:filter>
  <dsml:equalityMatch name="ObjectClass"><dsml:values>Users
  </dsml:values>
  </dsml:equalityMatch>
  </dsml:filter>
  </and>
  </query>
 </searchRequest>
```

The `basePsoID` in which the search is performed must be `Organization` or an empty string. (The `basepsoID` is either the same as the psoID format `Organization:key` or it can be an empty string.)

For example: `<basePsoID ID="Organization:7"/>`, `<basePsoID ID=""/>`

- **Password Operations**

  There are two `passwordRequest` operations, `setPasswordRequest` and `resetPasswordRequest`. The former enables a user to change the password while the latter generates a new, randomly generated password for the user, based on the password policy defined for that user in Oracle Identity Manager. The

supported target type is User. By default, `resetPasswordRequest` sets the password to `default`.

- **Suspend, Resume, or Active User Operations**

  The `suspend` capability specified in the SPML v2.0 specification has three operations:

  - `suspend`: Disables the state of an active user in Oracle Identity Manager.
  - `resume`: Enables the state of a disabled user in Oracle Identity Manager.
  - `active`: Returns the state of a user (that is, specifies whether or not a user is in the `active` state).

- **ListTargets Operations**

  - The `listTargets` operation can be used to determine the targets that are available for provisioning. This operation can also be used to determine the attributes that are supported by the provisioning system for each supported target type. This operation returns the schema information of all three supported target types: User, Group, and Organization.

The SPML Web Service does *not* support the following operations:

- Search (iterate/closelterator/hasReference)
- Update (updates/iterate/closelterator)
- Asynchronous request (status/cancel)
- Batch processing
- Bulk update (bulkModify/bulkDelete)
- Password expiry or validation

Note: If you want to include the date attribute in a provisioning request, then you must use the following format:

```
yyyy-MM-dd hh:mm:ss.fffffffff
```

No other date format is supported. Refer to the "Add Request With Date Format" section on page B-8 for a sample Add request with the date attribute assigned.

12.3 Deploying the SPML Web Service

Note: If you are using SPML Web service along with Oracle Identity Manager, then you must redeploy the SPML Web service whenever you upgrade Oracle Identity Manager.

If you have customized the EAR file, then you must redo those changes in the EAR file and then redeploy it.

The SPML Web Service is packaged in a deployable Enterprise Archive (EAR) file named `OIMSpmlWS.ear`. This file is generated when you install Oracle Identity Manager. This file is stored at the following location:

OIM_HOME/SPMLWS

There is a separate EAR file for each application server, and each file is stored in its respective application server folder in the `SPMLWS` directory. This EAR file is generated when you install Oracle Identity Manager.

> **Note:** Oracle Identity Manager and the SPML Web Service must be deployed on the same application server. This is known as **collocated deployment**. In a clustered environment, ensure that the SPML Web Service is installed on each node on which Oracle Identity Manager is installed.

Use the following batch file to run the scripts that deploy the SPML Web Service on the application server on which Oracle Identity Manager is running:

OIM_HOME/xellerate/setup/spml_*AppServerName*

To run this batch file, perform the steps that correspond to your operating environment:

> **Note:** The following log file is created when you run the batch file:
>
> *OIM_HOME*/xellerate/logs/spml-*AppServerName*.log

- Deploying the SPML Web Service on Oracle WebLogic Server
- Deploying the SPML Web Service on IBM WebSphere Application Server
- Deploying the SPML Web Service on JBoss Application Server
- Deploying the SPML Web Service on Oracle Application Server

12.3.1 Deploying the SPML Web Service on Oracle WebLogic Server

On a nonclustered Oracle WebLogic Server installation:

Enter the following command:

For UNIX:

OIM_HOME/setup/spml_*weblogic*.sh *appserver_admin_password oim_db_user_password*

For Microsoft Windows:

OIM_HOME\setup\spml_*weblogic*.cmd *appserver_admin_password oim_db_user_password*

On a clustered Oracle WebLogic Server installation:

1. Enter the following command on the administrator node:

   For UNIX:

   OIM_HOME/xellerate/setup/spml_*weblogic*.sh *appserver_admin_password oim_db_user_password*

   For Microsoft Windows:

   OIM_HOME\xellerate\setup\spml_*weblogic*.cmd *appserver_admin_password oim_db_user_password*

2. Perform the procedure described in the "Configuring the Apache Proxy Plug-in" appendix of *Oracle Identity Manager Installation and Configuration Guide for Oracle WebLogic Server*.

12.3.2 Deploying the SPML Web Service on IBM WebSphere Application Server

On a nonclustered IBM WebSphere Application Server installation:

Enter the following command:

For UNIX:

```
OIM_HOME/setup/spml_websphere.sh appserver_admin_password oim_db_user_password
```

For Microsoft Windows:

```
OIM_HOME\setup\spml_websphere.cmd appserver_admin_password oim_db_user_password
```

On a clustered IBM WebSphere Application Server installation:

1. Enter the following command on the administrator node:

   For UNIX:

   ```
   OIM_HOME/xellerate/setup/spml_websphere.sh appserver_admin_password
   oim_db_user_password
   ```

   For Microsoft Windows:

   ```
   OIM_HOME\xellerate\setup\spml_websphere.cmd appserver_admin_password
   oim_db_user_password
   ```

2. Regenerate the `plugin-cfg.xml` file by performing the procedure described in the "Configuring the IIS Plug-in" section of *Oracle Identity Manager Installation and Configuration Guide for IBM WebSphere Application Server*.

12.3.3 Deploying the SPML Web Service on JBoss Application Server

Note: Deployment of the SPML Web Service in clustered JBoss Application Server environments is not supported.

On a nonclustered JBoss Application Server installation:

Enter the following command:

For UNIX:

```
OIM_HOME/xellerate/setup/spml_jboss.sh oim_db_user_password
```

For Microsoft Windows:

```
OIM_HOME\xellerate\setup\spml_jboss.cmd oim_db_user_password
```

12.3.4 Deploying the SPML Web Service on Oracle Application Server

On a nonclustered Oracle Application Server installation:

1. Enter the following command:

   For UNIX:

OIM_HOME/setup/spml_*oc4j*.sh *appserver_admin_password oim_db_user_password*

For Microsoft Windows:

OIM_HOME\setup\spml_*oc4j*.cmd *appserver_admin_password oim_db_user_password*

2. Enter the following command script:

   For UNIX:

   OIM_HOME\xellerate\setup\spml_oc4j.sh *appserver_admin_password oim_db_user_password*

   For Microsoft Windows:

   OIM_HOME\xellerate\setup\spml_oc4j.cmd *appserver_admin_password oim_db_user_password*

3. Open the following file in a text editor:

   OC4J_HOME/j2ee/*OC4J_instance*/config/application.xml

4. In the `<imported-shared-libraries>` section of the `application.xml` file, change `<import-shared-library name="apache.commons.logging"/>` to `<remove-inherited name="apache.commons.logging"/>`.

   In other words, the `<imported-shared-libraries>` section must appear as follows

```
<imported-shared-libraries>
  <import-shared-library name="adf.oracle.domain"/>
  <import-shared-library name="oracle.ifs.client"/>
  <remove-inherited name="apache.commons.logging"/>
</imported-shared-libraries>
```

On a clustered Oracle Application Server installation:

Perform the following steps on each node of the cluster:

1. Enter the following command script:

   For UNIX:

   OIM_HOME\xellerate\setup\spml_oc4j.sh *appserver_admin_password oim_db_user_password*

   For Microsoft Windows:

   OIM_HOME\xellerate\setup\spml_oc4j.cmd *appserver_admin_password oim_db_user_password*

2. Open the following file in a text editor:

   OC4J_HOME/j2ee/*OC4J_instance*/config/application.xml

3. In the `<imported-shared-libraries>` section of the `application.xml` file, change `<import-shared-library name="apache.commons.logging"/>` to `<remove-inherited name="apache.commons.logging"/>`.

   In other words, the `<imported-shared-libraries>` section must appear as follows

```
<imported-shared-libraries>
  <import-shared-library name="adf.oracle.domain"/>
  <import-shared-library name="oracle.ifs.client"/>
```

```
    <remove-inherited name="apache.commons.logging"/>
</imported-shared-libraries>
```

12.4 Enabling Security by Using Oracle Web Services Manager and Then Deploying the SPML Web Service

Note: Perform the procedure described in this section only if you want to secure the SPML Web Service by using Oracle Web Services Manager.

Oracle Web Services Manager (WSM) provides features that ease the installation, configuration, and management of Web services across a wide range of deployment environments.

See Also: *Oracle Web Services Manager Administrator's Guide* for detailed information about Oracle WSM

You use Oracle WSM to secure the SPML Web Service. When a request is sent to the SPML Web Service in a SOAP message, it is intercepted by Oracle WSM. The SOAP message contains the Web Services Security (wsse) tag in the SOAP header. This `wsse:security` tag contains the user credentials that must be authenticated. For securing the SPML Web Service, you can use either the Oracle WSM Server Agent or the Oracle WSM Gateway.

See Also:

- *Oracle Web Services Manager Installation Guide* for detailed information about installing Oracle WSM

- *Oracle Web Services Manager Deployment Guide* for detailed information about the Oracle WSM Server Agent and the Oracle WSM Gateway

The Oracle WSM Server Agent or the Oracle WSM Gateway strips off the `wsse:security` tag from the SOAP message before forwarding the request to the SPML Web Service. You must configure the Oracle WSM Server Agent or the Oracle WSM Gateway to use a custom policy step, which extracts the user credentials from the `wsse:security` tag and inserts them into a custom header tag of the SOAP header from where the SPML Web Service extracts the credentials.

The following sections describe the configuration steps that you must perform to secure the SPML Web Service by using the Oracle WSM Server Agent or the Oracle WSM Gateway.

- Configuring the Oracle WSM Server Agent
- Configuring the Oracle WSM Gateway

Note: The Oracle WSM Server Agent supports IBM WebSphere Application Server and Oracle Application Server. You can use the Oracle WSM Gateway for all the application servers.

12.4.1 Configuring the Oracle WSM Server Agent

The following steps are required to configure the Oracle WSM Server Agent for securing the SPML Web Service:

> **Note:** You configure the Oracle WSM Server Agent before deploying the SPML Web Service.

1. Adding a Server Agent
2. Defining a Policy for the Server Agent
3. Injecting the Server Agent
4. Deploying the SPML Web Service

12.4.1.1 Adding a Server Agent

To add a Server Agent:

> **See Also:** Chapter 6, "Installing Oracle WSM Agents" in *Oracle Web Services Manager Deployment Guide* for detailed information about adding a server agent

1. Use the Web Services Manager Control (for example, http://localhost:8888/ccore) to create a server agent , and select the following values from the list:
   - Component type: **Server Agent**
   - Container type: Select **OC4J** for Oracle Application Server. Select **OTHER** for IBM WebSphere Application Server.
2. Select **Register**. This generates a server agent component with a component ID.

12.4.1.2 Defining a Policy for the Server Agent

Use the Web Services Manager Control to define the policy that you want to associate with the server agent. The default implementation of the policy is provided at the following location:

OIM_HOME/SPMLWS/OWSMPolicy

> **See Also:** Chapter 5, "Oracle Web Services Manager Policy Management," in the *Oracle Web Services Manager Administrator's Guide* for detailed information about defining a policy for a server agent

You must associate a URL pattern with the policy. To do so, select **Policy Management**, **Manage Policies**, and then **Policies**. Then click the **Edit Mapping** button and enter the following as the URL pattern to associate with the policy:

```
/spmlws/HttpSoap11
```

To configure a custom policy, you must include the class file `com.oracle.xl.spmlws.ws.security.owsm.CustomPolicyStep` in *OIM_HOME*/SPMLWS/OWSMPolicy into the following file:

ORACLE_HOME/owsm/lib/extlib/coresvagent.jar

After creating the server agent component, you must add your custom step to that component. You can do this by clicking the **Steps** link for your registered component. Then, select the `CustomPolicyStep.xml` file from its location and click **Upload**. This XML file is located at *OIM_HOME*`/SPMLWS/OWSMPolicy/com/oracle/xl/spmlws/ws/security/owsm`.

At this stage, your custom policy step name is added to the list of available policies.

> **Note:** If you create a custom policy, then its class file must be included in the `coresvagent.jar` file that resides in the Web services EAR file.

12.4.1.3 Injecting the Server Agent

Injecting the server agent requires you to perform the following steps:

For Oracle Application Server

To inject the server agent:

1. Modify the attributes in the `ORACLE_HOME/owsm/bin/agent.properties` file with the following values:
   - agent.componentType: ServerAgent
   - agent.containerType: OC4J
   - agent.containerVersion: It must be "10.1.3" for Oracle Application Server.
   - agent.component.id: Enter the component ID that is generated when the agent is created and registered by using Web Services Manager Control.
2. Edit the following properties in the `agent.properties` file:
   - `webservice.application.input` - Enter the full path and name of the EAR file.
   - `webservice.application.webapp.name` - Uncomment and enter the WAR file name, `spmlws.war`.

     > **Note:** the WAR file is bundled in the `OIMSpmlWS.ear` file.

   - `webservice.application.contexturi` - Enter the context root, `/spmlws`.
3. Run the `wsmadmin installAgent` command.

For IBM WebSphere Application Server

To inject the server agent:

1. Because the Server Agent for SOA 10.1.3.1 release is supported only for Oracle Application Server, for WebSphere, you must first download the required ZIP file from the following location on Oracle Technology Network:

   For UNIX:

   `http://download.oracle.com/otn/linux/ias/101310/soa_linux_x86_ws_agent101310.zip`

For Microsoft Windows:

`http://download.oracle.com/otn/nt/ias/101310/soa_windows_x86_ws_agent101310.zip`

2. Extract the contents of the ZIP file to any location (for example `/owsm`).

   Tip: The Readme_Agentinstall.pdf file in the extracted ZIP file for more information about injecting the server agent

3. Browse to the `bin` directory, open the `agent.properties` file, and set the following properties in the file:
   - agent.componentType: serveragent
   - agent.containerType: For example, AXIS, WEBLOGIC, WEBSPHERE, TIBCO-BW, or OC4J
   - agent.containerVersion: The version of WebSphere on which you are deploying the SPML Web Service.
   - oc4j.home:`/owsm/oc4j` (assuming that `/owsm` is where you extracted the ZIP file)
   - oc4j.j2ee.home:`/owsm/oc4j/j2ee/home` (here `/owsm` is where you extracted the ZIP file)
   - webservice.application.input: Web application input file name with path location, that is, WAR or EAR file location. For example, `/owsm/wars/HelloWorldImpl.war`
   - webservice.application.webapp.name: not applicable if it is a WAR file
   - webservice.application.contexturi: not applicable if it is a WAR file
   - agent.component.id: Enter the component ID that is generated when the agent is created and registered by using Oracle Web Services Manager Control.
   - agent.policymanagerURL (for example, *`http://hostname:8888/policymanager`*. Provide a system name instead of localhost)
4. Open the `bin/coresv.properties` file and set the following properties:
   - coresv.home=`/owsm` (assuming `/owsm` is where you extracted the ZIP file)
   - ant.home: set home directory of the ANT installation
   - java.home: set home directory of the Java installation
   - lib.dir:`/owsm/lib` (assuming `/owsm` is where you extracted the ZIP file)
   - oc4j.j2ee.home:`/owsm/oc4j/j2ee/home` (optional if the properties are present)
   - external.oc4j.home:`/owsm/oc4j` (optional if the properties are present)
5. For configuring a custom policy, you must include the class file `com.oracle.xl.spmlws.ws.security.owsm.CustomPolicyStep` in *`OIM_HOME`*`/SPMLWS/OWSMPolicy` into the following file:

   `/owsm/lib/extlib/coresvagent.jar`

   (assuming `/owsm` is where you extracted the ZIP file)

6. In a command window, navigate to the `bin` directory. Run the `injectAgent` command. This command injects all the JAR files into the specified WAR or EAR file. (Before running this, set the path to the `ant bin` directory.)

12.4.1.4 Deploying the SPML Web Service

After you have installed the client agent, deploy the SPML Web Service. For information about how to deploy the SPML Web Service, refer to the "Deploying the SPML Web Service" section on page 12-6.

12.4.2 Configuring the Oracle WSM Gateway

The following steps are required to deploy the Oracle WSM Gateway for securing the SPML Web Service:

> **See Also:** *Oracle Web Services Manager Quick Start Guide* for detailed information about specific configurations of Oracle WSM

1. Registering the Oracle WSM Gateway
2. Registering the SPML Web Service with the Gateway
3. Adding a Custom Policy to the Gateway
4. Deploying the SPML Web Service
5. Viewing the WSDL File

12.4.2.1 Registering the Oracle WSM Gateway

To register the Gateway:

1. Click **Add New Component** in the Oracle Web Services Manager Control.
2. On the Add New Component page, enter the following values:
   - Component Name: for example, MyGateway
   - Component Type: Gateway (default value)
   - Container Type: Oracle Web Services Manager (default value)
   - Component URL: Enter the following: `http://fully_qualified_host_name:http_port/gateway` where fully_qualified_host_name is the URL for Oracle WSM, and http_port is the port on which Oracle WSM is hosted
   - Component Groups: accept the default values for the component groups
3. Click **Register**.
4. Click **OK**.

12.4.2.2 Registering the SPML Web Service with the Gateway

To register the SPML Web Service with the Gateway:

1. From the navigation pane of Oracle Web Services Manager Control, click **Policy Management**.
2. Click **Register Services**.
3. Click the **Services** link.

4. Click **Add New Service**. The Add New Service page is displayed. On this page, enter the following service details:
   - Service Name: SPMLService
   - Service Version: 1.0
   - Service Description: Processes SPML Requests
   - WSDL URL: The WSDL location, for example:

     `http://host:port/spmlws/.../HttpSoap11?wsdl`

5. Click **Next**. The Configure Messenger Step for New Service page is displayed. On this page, verify that the URL matches the URL you provided on the previous page. Click **Finish** to accept the default values for the remaining fields.
6. Click **Commit Policy**.

12.4.2.3 Adding a Custom Policy to the Gateway

Use the Oracle Web Services Manager Control to configure a policy that you want to associate with the Gateway. The default implementation of the policy is at the following location:

OIM_HOME/SPMLWS/OWSMPolicy

> **See Also:** Chapter 5, "Oracle Web Services Manager Policy Management," in *Oracle Web Services Manager Administrator's Guide* for more information about defining a policy for a Gateway

The policy extracts user credentials from the WSSE security tags and adds them to the SOAP header in the following custom tag.

```
<wsa1:OIMUser soap:mustUnderstand="0"
xmlns:wsa1="http://xmlns.oracle.com/OIM/provisioning">
<wsa1:OIMUserId
xlmns:wsa1="http://xmlns.oracle.com/OIM/provisioning">user1</wsa1:OIMUserId>
<wsa1:OIMUserPassword
xlmns:wsa1="http://xmlns.oracle.com/OIM/provisioning">password1</wsa1:OIMUserPassw
ord>
</wsa1:OIMUser>
```

The SPML Web Service interprets and processes this tag.

For configuring a custom policy, you must include the `com.oracle.xl.spmlws.ws.security.owsm.CustomPolicyStep` in *OIM_HOME*/SPMLWS/OWSMPolicy class file into the following file:

ORACLE_HOME/owsm/lib/coresv-4.0.jar

You must include the custom policy step file because the `coresv-4.0.jar` file contains all the policy-specific class files. Then, restart Oracle Application Server.

After you register the Gateway, you must add a custom step. To add a custom step:

1. Upload the `CustomPolicy.xml` file for the custom policy on the Add Step page. This XML file is located at the following path:

   OIM_HOME/SPMLWS/OWSMPolicy/com/oracle/xl/spmlws/ws/security/owsm

2. To open the Add Step page in the Oracle Web Services Manager Control, expand **Policy Management**, click **Manage Policies**, **Steps**, and then **Add Step**. Select the

`CustomPolicy.xml` file from its location and then click **Upload**. The name of the custom policy step is added to the list of available policies.

3. To add the custom policy to the pipeline in the Request block, browse to the Policy page. To open the Policy page, expand **Policy Management**, click **Manage Policies**, **Policies**, and finally click **Policy**.

   The Request block will enforce this configured custom policy for any valid incoming request sent to the SPML Web Service.

12.4.2.4 Deploying the SPML Web Service

After you have installed the client agent, deploy the SPML Web Service. For information about how to deploy the SPML Web Service, refer to the "Deploying the SPML Web Service" section on page 12-6.

12.4.2.5 Viewing the WSDL File

To view the Web Service Description Language (WSDL) file for the Web Service:

1. From the navigation pane of Web Services Manager Control, click **Policy Management**.
2. Click **Register Services**.
3. To access the Gateway (MyGateway), click **Services**.
4. From the list of services, click **Edit** for the required service.
5. In the Edit Service page, copy the URL displayed in the Service WSDL URL field.

You use this URL in the SPML client to access the SPML Web Service.

12.5 Postdeployment Tasks

If you are using JBoss Application Server, Oracle WebLogic Server, or IBM WebSphere Application Server, then there are no postdeployment steps to perform.

If you are using IBM WebSphere Application Server 6.1, extract the `xlDataObjectBeans.jar` file, and copy it into the `WEB-INF/lib` directory of the SPML Web Service WAR file. You must restart WebSphere after you copy this file.

> **See Also:** "Extracting xlDataObjectBeans.jar" in *Oracle Identity Manager Installation and Configuration Guide for IBM WebSphere Application Server*

12.6 Enabling SSL Communication

This section provides information about enabling Secure Sockets Layer (SSL) communication for the SPML Web Service. It is strongly recommended that you perform the instructions given in this section.

Note: Oracle recommends that you refer to application server-specific SSL configuration documentation for details. This section provides the minimum information required to enable SSL communication for the different application servers on which the SPML Web Service is supported.

Although this section provides information for specific releases of the application servers, if you are using a different release, then some steps of the procedure can vary.

12.6.1 JBoss Application Server

The following sections provide information required to enable SSL communication for the SPML Web Service installed on JBoss Application Server 4.2.3 GA.

12.6.1.1 Prerequisites

The following are the prerequisites for enabling SSL communication:

- JBoss Application Server is installed and Oracle Identity Manager and the SPML Web Service are deployed on it.
- The JBoss Application Server home directory is E:\jboss-4.2.3.GA.
- The identity store is `jbossserver.jks` and the password is `welcome`.
- Certificate request is made for localhost.
- The self-sign certificate is named `jbossserver.cert`.
- The private key alias is `serverjboss` and the password is `welcome`.

12.6.1.2 SSL Certificate Setup

This section discusses the following procedures for setting up SSL:

Tip: For enhanced protection, Oracle recommends that you create new certificates (either self-signed or CA certificates) and create a separate keystore and truststore for the client and the server with different passwords. Refer to the SSL configuration documentation of the application server for detail.

1. Generating Keys
2. Signing the Certificates
3. Exporting the Certificate
4. Configuring the server.xml File

Generating Keys

Generate keys by using the `keytool` command. The following keytool command generates an identity keystore `jbossserver.jks`:

```
keytool -genkey -alias serverjboss -keyalg RSA -keysize 1024 -dname
"CN=localhost,OU=Identity,O=Oracle,C=US" -keypass welcome -keystore
E:\jboss-4.2.3.GA\server\jbossserver.jks -storepass welcome -storetype jks
```

Signing the Certificates

Use the following `keytool` command to sign the certificates that were created:

```
keytool -selfcert -alias serverjboss -sigalg MD5withRSA -validity 2000 -keypass
welcome -keystore  E:\jboss-4.2.3.GA\server\jbossserver.jks -storepass welcome
```

Exporting the Certificate

Use the following `keytool` command to export the certificate from the identity keystore to a file (for example, `jbossserver.cert`):

```
keytool -export -alias serverjboss -file E:\jboss-4.2.3.GA\server\jbossserver.cert
-keypass welcome -keystore E:\jboss-4.2.3.GA\server\jbossserver.jks -storepass
welcome -storetype jks -provider sun.security.provider.Sun
```

Configuring the server.xml File

Make the following entry in the `server.xml` file:

```
<Connector port="8443" address="${jboss.bind.address}"
           maxThreads="100" strategy="ms" maxHttpHeaderSize="8192"
           emptySessionPath="true"
           scheme="https" secure="true" clientAuth="false"
              sslProtocol="TLS"
           keystoreFile="E:\jboss-4.2.3.GA\server\jbossserver.jks"
           keystorePass="welcome"
           truststoreFile="E:\jboss-4.2.3.GA\server\jbossserver.jks"
           truststorePass="welcome"/>
```

After you have performed the preceding steps, restart the server for the changes to take effect.

Note: You can use the certificate exported in the "Exporting the Certificate" step to import into the client-side truststore for SSL communication.

12.6.2 Oracle WebLogic Server

The following sections provide information required to enable SSL communication for the SPML Web Service installed on Oracle WebLogic Server.

12.6.2.1 Prerequisites

The following are the prerequisites for enabling SSL communication:

- Oracle WebLogic Server is installed.
- The WebLogic Domain directory is `C:\bea\user_projects\domains\oim`.
- The Oracle WebLogic Server home (*WL_HOME*) directory is `C:\bea\wlserver_10.3`.
- The identity store is `support.jks` and the password is `support`.
- The certificate request is made for xellerate.oracle.com host and for Oracle Identity Management Group.
- The self-sign certificate is named `supportcert.pem`.
- The private key alias is `support`, and the password is `weblogic`.

- The `setEnv.cmd` or `setEnv.sh` script is run to set up PATH, CLASSPATH, and other variables.

12.6.2.2 SSL Certificate Setup

This section discusses the following procedures for setting up SSL:

> **Tip:** For enhanced protection, Oracle recommends that you create new certificates (either self-signed or CA certificates) and create a separate keystore and truststore for the client and the server with different passwords. Refer to the SSL configuration documentation of the application server for detail.

1. Generating Keys
2. Signing the Certificates
3. Exporting the Certificate
4. Configuring the Oracle WebLogic Server

Generating Keys

Generate private/public certificate pairs by using the keytool command provided. The following command creates an identity keystore (`support.jks`). Change the parameter values passed to the keytool command according to your requirements. Ensure that there is no line break in the keytool argument.

```
keytool -genkey
        -alias support
        -keyalg RSA
        -keysize 1024
        -dname "CN=xellerate.oracle.com, OU=Identity, O=Oracle Corporation,
L=RedwoodShores, S=California, C=US"
        -keypass weblogic
        -keystore C:\bea\user_projects\domains\oim\support.jks
        -storepass support
```

> **Note:** Use the same host name that you would use in the `xlconfig.xml` file. For example, if you use `https://xellerate.oracle.com:7002` and `t3s://xellerate.oracle.com:7002` in the `xlconfig.xml` file, then the value of CN in the keytool command must be `xellerate.oracle.com`. Oracle recommends that you generate an SSL certificate by using the domain name (for example, `xellerate.oracle.com`) instead of the IP address.

Signing the Certificates

Use the following command to sign the certificates that you created.

```
keytool -selfcert -alias support
        -sigalg MD5withRSA
        -validity 2000
        -keypass weblogic
        -keystore C:\bea\user_projects\domains\oim\support.jks
        -storepass support
```

Note: Oracle recommends that you use trusted certificate authorities, for example, VeriSign or Thawte, for signing the certificates.

Exporting the Certificate

Use the following command to export the certificate from the identity keystore to a file, for example, `supportcert.pem`:

```
keytool -export -alias support
        -file C:\bea\user_projects\domains\oim\supportcert.pem
        -keypass weblogic
        -keystore C:\bea\user_projects\domains\oim\support.jks
        -storepass support
```

Configuring the Oracle WebLogic Server

To configure the Oracle WebLogic Server:

1. In the WebLogic Server Administration Console, click **Environment**, **Servers**, ***Server_Name***, **Configuration**, and then **General**.
2. Click **Lock & Edit**.
3. Select **SSL listen port enabled**. The default port is 7002.
4. Click the **Keystores** tab
5. From the **Keystore** list, select **Custom Identity and Java Standard Trust**.
6. In the **Custom Identity Keystore** field, specify `C:\bea\user_projects\domains\oim\support.jks` as the custom identity keystore file name.
7. Specify **JKS** as the custom identity keystore type.
8. Enter the password in the **Custom Identity Keystore Passphrase** and **Confirm Custom Identity Keystore Passphrase** fields.
9. Click **Save**.
10. Click the **SSL** tab.
11. Enter `support` as the private key alias.
12. Enter the password (for example, support) in the **Private Key Passphrase** and **Confirm Private Key Passphrase** fields.
13. Click **Save**.
14. Click **Activate changes**.
15. Restart the server for the changes to take effect.

Note: You can import the certificate exported in the "Exporting Certificate" step into the client-side truststore for SSL communication.

Import the certificate into the SPML client truststore by using the following keytool command:

```
keytool -import -alias serverwl -trustcacerts -file
D:\bea\user_projects\domains\ mydomain\wlservercert.pem -keystore
<client-trust store> -storepass <client-trust-store password>
```

12.6.3 IBM WebSphere Application Server

The following sections provide information required to enable SSL communication for the SPML Web Service installed on IBM WebSphere Application Server.

12.6.3.1 Prerequisites

The following are the prerequisites for enabling SSL communication:

- IBM WebSphere Application Server is installed and Oracle Identity Manager and the SPML Web Service are deployed on it.
- After configuring IBM WebSphere Application Server and deploying the SPML Web Service with Oracle Identity Manager, you can access the application by using SSL and non-SSL ports.
- To access the application securely by using SSL, you use port number 9443 or WC_defaulthost_secure. Consider the following example:

  ```
  https://localhost:9443/spmlws/HttpSoap11
  ```

- The default identity store is `key.p12`, and the password is `WebAS`.
- The default truststore is `trust.p12`, and the password is `WebAS`.

> **Note:** For SSL communication, export the default certificate from `key.p12`.

12.6.3.2 SSL Certificate Setup

The steps in this section enable you to do the following:

- Exporting Certificate to a File
- Importing the Certificate File

Exporting Certificate to a File

IBM WebSphere Application Server uses the IBM WebSphere default keystore (`key.p12`) and its default certificate. You must export this default certificate to a file. You can use the following keytool command to achieve this:

```
IBM_JDK_HOME/jre/bin/keytool -export -alias default -file <Exported Certificate
file> -keypass WebAS -keystore  FULL_PATH_OF_IBM_WEBSPHERE "key.p12" -storepass
WebAS -storetype pkcs12 -provider com.ibm.crypto.provider.IBMJCE
```

In the preceding command, replace the following to point to the appropriate location:

- The full path of IBM WebSphere Application Server `key.p12`, which is the default IBM keystore
- *IBM_JDK_HOME* to the IBM WebSphere Application Server Java folder
- Location for the exported certificate

Importing the Certificate File

Use the following keytool command to import the certificate file to the SPML Web Service client truststore:

```
keytool -import -alias serverws -trustcacerts -file <Exported Certificate file>
-keystore E:\SPMLTest\mykeystore -storepass mypass  -storetype jks
```

Tip: For enhanced protection, Oracle recommends that you create new certificates (either self-signed or CA certificates) and create a separate keystore and truststore for the client and the server with different passwords. Refer to the SSL configuration documentation of the application server for detail.

12.6.4 Oracle Application Server

The following sections provide information required to enable SSL communication for the SPML Web Service installed on Oracle Application Server.

12.6.4.1 Prerequisites

The following are the prerequisites for enabling SSL communication:

- Oracle Application Server is installed and Oracle Identity Manager and the SPML Web Service are deployed on it.
- Oracle Application Server 10.1.3 installation directory is `E:\product\10.1.3.1\OracleAS_1`.
- The identity store is `oc4jserver.jks`, and the password is `welcome`.
- Certificate request is made for localhost.
- The self-sign certificate is named `oc4jserver.cert`.
- The private key alias is `serveroc4j`, and the password is `welcome`.

12.6.4.2 SSL Certificate Setup

The steps in this section enable you to do the following:

Tip: For enhanced protection, Oracle recommends that you create new certificates (either self-signed or CA certificates) and create a separate keystore and truststore for the client and the server with different passwords. Refer to the SSL configuration documentation of the application server for details.

1. Generating Keys
2. Signing the Certificates
3. Exporting the Certificate
4. Configuring Oracle Application Server

Generating Keys

Generate keys by using the keytool command provided. The following keytool command creates an identity keystore `oc4jserver.jks`:

```
keytool -genkey -alias serveroc4j -keyalg RSA -keysize 1024 -dname
"CN=localhost,OU=Identity,O=Oracle,C=US" -keypass welcome -keystore
E:\product\10.1.3.1\OracleAS_1\oc4jserver.jks -storepass welcome -storetype jks
```

Signing the Certificates

Use the following keytool command to sign the certificates you created:

```
keytool -selfcert -alias serveroc4j -sigalg MD5withRSA -validity 2000 -keypass
welcome -keystore  E:\product\10.1.3.1\OracleAS_1\oc4jserver.jks -storepass
welcome
```

Exporting the Certificate

Use the following keytool command to export the certificate from the identity keystore to a file:

```
keytool -export -alias serveroc4j -file
E:\product\10.1.3.1\OracleAS_1\oc4jserver.cert -keypass welcome -keystore
E:\product\10.1.3.1\OracleAS_1\oc4jserver.jks -storepass welcome -storetype jks
-provider sun.security.provider.Sun
```

Configuring Oracle Application Server

To configure Oracle Application Server:

1. Make a copy of the `E:\product\10.1.3.1\OracleAS_1\j2ee\home\config\default-web-site.xml` file at the same location and rename the copy to `secure-web-site.xml`.
2. In the `secure-web-site.xml` file, modify the following:
   - port attribute=`4443`
   - secure=`true`
   - protocol=`https`

   For example:

   ```
   web-site xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:noNamespaceSchemaLocation="http://xmlns.oracle.com/oracleas/schema/web-site
   -10_0.xsd"  port="4443"  secure="true" protocol ="https" display-name="OC4J 10g
   (10.1.3) Default Web Site" schema-major-version="10" schema-minor-version="0">
   ```

3. In the same file, under the `web-site` node, add a new element `ssl-config` to point to the keystore as shown in the following example:

   ```
   <ssl-config keystore="E:/product/10.1.3.1/OracleAS_1/oc4jserver.jks"
   keystore-password="welcome" />
   ```

4. In the `E:\product\10.1.3.1\OracleAS_1\j2ee\home\config\server.xml` file, add the following entry:

   ```
   <web-site path="./secure-web-site.xml"/>
   ```

5. In the `E:\product\10.1.3.1\OracleAS_1\opmn\conf\opmn.xml` file, add the following:

   ```
   <port id="secure-web-site" range="4443" protocol="https"> under <ias-component
   id="default_group">
   ```

6. In the `opmn.xml` file, add the following in the `<data id="java-options" value="-Xrs" under <ias-component id="default_group">` tag:

   ```
   -Djavax.net.ssl.trustStore=E:\product\10.1.3.1\OracleAS_1\oc4jserver.jks
   -Djavax.net.ssl.trustStorePassword=welcome
   -Djavax.net.ssl.keyStore=E:\product\10.1.3.1\OracleAS_1\oc4jserver.jks
   -Djavax.net.ssl.keyStorePassword=welcome"
   ```

7. Restart the server for the changes to take effect.

12.6.5 Enabling SSL for HTTP Communication to Oracle HTTP Server

The following sections provide information about enabling SSL for HTTP communication to Oracle HTTP Server.

By default, the Oracle HTTP Server is configured with SSL and the SSL certificate store, which is located at *ORACLE_HOME*/Apache/Apache/conf/ssl.wlt/default/. The `listen` parameter in the *ORACLE_HOME*/Apache/Apache/conf/ssl.conf file points to the SSL port being used by the Oracle HTTP Server.

You do not make any configuration change to use the default certificate store that comes along with the installation.

> **Tip:** For enhanced protection, Oracle recommends that you create new certificates (either self-signed or CA certificates) and create a separate keystore and truststore for the client and the server with different passwords. Refer to the SSL configuration documentation of the application server for detail.

12.6.5.1 Exporting Certificate

You must export the certificate from the default Oracle wallet *ORACLE_HOME*/Apache/Apache/conf/ssl.wlt/default/ewallet.p12. This certificate is used for the Design Console to trust Oracle Application Server. To export the certificate:

1. Open the *ORACLE_HOME*/Apache/Apache/conf/ssl.wlt/default/ewallet.p12 file by using the Oracle Wallet Manager Console. To do so, click **Open Wallet** and browse to the location of the wallet.
2. When prompted, enter the store password as **welcome**.
3. Right click `Certificate (Ready)`, and click **Export User Certificate**.
4. Save the file as `server.cert`.

> **See Also:** The "Secure Sockets Layer" section in *Oracle Application Server Administrator's Guide* for more information about Oracle Wallet Manager

12.7 Developing the Client for the SPML Web Service

This section provides information and guidelines that you can apply while creating a client for the SPML Web Service.

> **Note:** In this chapter, the client for the SPML Web Service is referred to as the SPML client.

To develop an SPML client, you must refer to the WSDL file for each application server for which you develop the client. The WSDL files for each application server are in the *OIM_HOME*/SPMLWS/SampleHttpClient/wsdl directory.

The code files for a sample SPML client are available at the following location:

OIM_HOME/SPMLWS/SampleHttpClient

To keep sample code easy to understand, this SPML client uses an HTTP connection to the SPML Web Service instead of an HTTP/S connection.

This sample SPML client refers to XML files containing the SOAP requests and performs an HTTP post to the SPML Web Service.

A set of sample SOAP requests is shipped along with this release of Oracle Identity Manager. The following is the format of the path at which you can access the files for these sample SOAP requests:

`SampleHttpClient/sampleRequests/`*`Application Server`*

The `sampleRequests` directory contains separate SOAP requests for each of the supported application servers.

> **Note:** As mentioned earlier, the SPML Web Service supports requests in `UTF-8` encoding only. Therefore, Oracle recommends that you pass SPML requests over HTTP by specifying the charset as `UTF-8` in the content-type header in any client implementation. Refer to the implementation of the sendSOAPRequest function in the sample client provided in the *`OIM_HOME`*`/SPMLWS/SampleSPMLClient/src/testspml/HttpConnect.java` file. In addition, you must serialize the data into a `byte[]` before sending the request. The `main` function in the `SendSPMLRequest.java` file can copy files directly into a `byte[]` and then send it over the HTTP connection.

The following sections provide information that you can apply while developing the SPML client:

- Supported SPML Operations
- Authentication
- Fields Included in SPML Requests
- Structure of the SOAP Header
- Sample SOAP SPML Message

12.7.1 Supported SPML Operations

As mentioned earlier, the SPML Web Service supports the following operations:

- Add operations
- Modify operations

  You must ensure that the psoID is included in the SPML request for the modify operations.
- Delete operations

  You must ensure that the psoID is included in the SPML request for the delete operations.
- Add, Replace, or Delete references
- Lookup operations
- Search operations
- Password operations

You must ensure that the psoID is included in the SPML request for the password operations.

- Suspend, Resume, or Active User operations

  The suspend capability includes the `suspendRequest`, `resumeRequest`, and the `activeUser` operations. You must ensure to include psoID in the SPML request for the `resumeRequest` and the `activeUser` operations.

- ListTargets operations

Note: For more information about psoID, refer to the "Provisioning Operations Supported by the SPML Web Service" section on page 12-3.

12.7.2 Authentication

The SPML client must be authenticated for each SPML request sent. This is to ensure that unauthorized users are not allowed to use the SPML Web Service.

The SPML client can be authenticated in the following way. The SPML client sends the user credentials to the Web Service in the SOAP header. This can be done in the following ways:

- The credentials are provided as header information in a custom tag.
- Oracle WSM is configured to secure the SPML Web Service. In this case, the credentials are sent in standard WSSE tags. A default policy implementation processes these credentials. The default policy file, which is packaged along with the product, is located at the following path:

  OIM_HOME/SPMLWS/OWSMPolicy

Note: For details about configuring Oracle WSM with the SPML Web Service, refer to the "Enabling Security by Using Oracle Web Services Manager and Then Deploying the SPML Web Service" section on page 12-10.

12.7.3 Fields Included in SPML Requests

Table 12–1 lists the mandatory and nonmandatory fields that can be included in SPML requests.

Note: In the following table, certain rows list psoID in the Mandatory Fields column. These requests do not require any Oracle Identity Manager attributes.

Table 12–1 Mandatory and Nonmandatory Fields Included in SPML Requests

SPML Request	Mandatory Fields	Nonmandatory Fields
addRequest for User	Users.User ID Users.First Name Users.Last Name Organizations.Organization Name Users.Xellerate Type Users.Role Users.Password	The rest of the OIM User fields pertaining to the creation of users are nonmandatory.
addRequest for Group	Groups.Group Name	The rest of the OIM User fields pertaining to the creation of groups are nonmandatory.
addRequest for Organization	Organizations.Organization Name	Organizations.Type Organizations.Parent Name
deleteRequest for User	psoID ID="Users:7"	
deleteRequest for Group	psoID ID="Groups:7"	
deleteRequest for Organization	psoID ID="Organizations:9"	
modifyRequest for User	psoID ID="Users:5" One or more modification elements, each corresponding to an attribute to be modified	
modifyRequest for Group	psoID ID="Groups:5" One or more modification elements, each corresponding to an attribute to be modified	
modifyRequest for Organization	psoID ID="Organizations:3" One or more modification elements, each corresponding to an attribute to be modified	
lookupRequest for User	psoID ID="Users:7"	
lookupRequest for Group	psoID ID="Groups:7"	
lookupRequest for Organization	psoID ID="Organizations:9"	
suspendRequest for User	psoID ID="Users:7"	
resumeRequest for User	psoID ID="Users:7"	
activeRequest for User	psoID ID="Users:7"	
setPasswordRequest for User	psoID ID="Users:7"	
resetPasswordRequest for User	psoID ID="Users:7"	

Table 12–1 (Cont.) Mandatory and Nonmandatory Fields Included in SPML Requests

SPML Request	Mandatory Fields	Nonmandatory Fields
searchRequest for User	The `basePsoID` in which the search is performed must be `Organization` or an empty string. For example: `<basePsoID ID="Organization:7"/>, <basePsoID ID=""/>` A set of `dsml:filter` conditions specifying equality matches for the attributes based on which the search has to be performed. **Note**: The objectclass information is sent as a part of one of the filters to specify to the SPML Web Service the container on which the search must be performed. For example: `<dsml:filter><dsml:equalityMatch name="Object Class"><dsml:values>Users</dsml:values></dsml:equalityMatch></dsml:filter>`	

Table 12–1 (Cont.) Mandatory and Nonmandatory Fields Included in SPML Requests

SPML Request	Mandatory Fields	Nonmandatory Fields
searchRequest for Group	The `basePsoID` in which the search is performed must be an empty string. A set of `dsml:filter` conditions specifying equality matches for the attributes based on which the search has to be performed. **Note**: The objectclass information is sent as a part of one of the filters to specify to the SPML Web Service the container on which the search must be performed. For example: `<dsml:filter><dsml:equalityMatch name="Object Class"><dsml:values>Groups</dsml:values></dsml:equalityMatch></dsml:filter>`	
searchRequest for Organization	The `basePsoID` in which the search is performed must be `Organization` or an empty string. A set of `dsml:filter` conditions specifying equality matches for the attributes based on which the search has to be performed. **Note**: The objectclass information is sent as a part of one of the filters to specify to the SPML Web Service the container on which the search must be performed. For example: `<dsml:filter><dsml:equalityMatch name="Object Class"><dsml:values>Organizations</dsml:values></dsml:equalityMatch></dsml:filter>`	
listTargetRequest	None	

12.7.4 Structure of the SOAP Header

The SPML Web Service requires Oracle Identity Manager credentials, which must be provided in the SOAP header depending on whether Oracle WSM is used for securing SPML. This information is explained in the following sections.

Using Custom Security Tags

The custom security tags (`wsa1:OIMUser`) can be used in a SOAP header to embed Oracle Identity Manager credentials when the SOAP request is sent directly to the SPML Web Service. The SPML Web Service interprets these tags, and server-side handlers extract the credential information, as illustrated in the following sample SOAP header:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<soapenv:Header>
<wsa1:OIMUser soapenv:actor="http://schemas.xmlsoap.org/soap/actor/next"
```

```
soapenv:mustUnderstand="0" xmlns:wsa1="http://xmlns.oracle.com/OIM/provisioning">
<wsa1:OIMUserPassword>password1</wsa1:OIMUserPassword>
<wsa1:OIMUserId>user1</wsa1:OIMUserId>
</wsa1:OIMUser>
</soapenv:Header>
……..</soapenv:Envelope>
```

Using WSSE Security Tags

If the Oracle WSM Gateway or Agent is used for securing the SPML Web Service, then the SPML SOAP message is intercepted by that Gateway or Agent. In this case, Oracle Identity Manager credentials are provided in standard wsse security tags, as illustrated in the following sample:

```
soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<soapenv:Header>
  <wsse:Security
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-sec
ext-1.0.xsd">
  <wsse:UsernameToken>
  <wsse:Username>user1</wsse:Username>
<wsse:Password
Type="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profi
le-1.0#PasswordText">password1</wsse:Password>
  </wsse:UsernameToken>
 </wsse:Security>
</soapenv:Header>
……..</soapenv:Envelope>
```

wsa1:lang tag

In addition to Oracle Identity Manager credential information, the SPML client can also send locale information to the SPML Web Service in the SOAP header by using the `wsa1:lang` tag. These tags are then processed by the SPML Web Service. If Oracle Web Services Manager is configured, then the SPML Web Service ignores this tag. In this situation, the header information is as follows:

For custom tags:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<soapenv:Header>
<wsa1:OIMUser soapenv:actor="http://schemas.xmlsoap.org/soap/actor/next"
soapenv:mustUnderstand="0" xmlns:wsa1="http://xmlns.oracle.com/OIM/provisioning">
<wsa1:OIMUserPassword>password1</wsa1:OIMUserPassword>
<wsa1:OIMUserId>user1</wsa1:OIMUserId>
</wsa1:OIMUser>
<wsa1:lang soapenv:actor="http://schemas.xmlsoap.org/soap/actor/next"
soapenv:mustUnderstand="0" xmlns:wsa1="http://xmlns.oracle.com/OIM/provisioning">
<wsa1:language>en</wsa1:language>
<wsa1:sublanguage>US</wsa1:sublanguage>
</wsa1:lang>
</soapenv:Header>
……..</soapenv:Envelope>
```

For WSSE tags:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<soapenv:Header>
<wsse:Security
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-sec
ext-1.0.xsd">
<wsse:UsernameToken>
<wsse:Username>user1</wsse:Username>
<wsse:Password
Type="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profi
le-1.0#PasswordText">password1</wsse:Password>
</wsse:UsernameToken>
</wsse:Security>
<wsa1:lang soapenv:actor="http://schemas.xmlsoap.org/soap/actor/next"
soapenv:mustUnderstand="0" xmlns:wsa1="http://xmlns.oracle.com/OIM/provisioning">
<wsa1:language>en</wsa1:language>
<wsa1:sublanguage>US</wsa1:sublanguage>
</wsa1:lang>

</soapenv:Header>
.....</soapenv:Envelope>
```

12.7.5 Sample SOAP SPML Message

The following sample SOAP SPML message is an Add Request operation for the SPML Web Service on Oracle Application Server:

With custom security tags:

```
<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
<soap:Header>
<wsa1:OIMUser soap:mustUnderstand="0"
xmlns:wsa1="http://xmlns.oracle.com/OIM/provisioning">
<wsa1:OIMUserId
xmlns:wsa1="http://xmlns.oracle.com/OIM/provisioning">user1</wsa1:OIMUserId>
<wsa1:OIMUserPassword
xmlns:wsa1="http://xmlns.oracle.com/OIM/provisioning">password1</wsa1:OIMUserPassw
ord>
</wsa1:OIMUser>
</soap:Header>
<soap:Body>
<SPMLv2Document xmlns="http://xmlns.oracle.com/OIM/provisioning">
<addRequest returnData="everything" xmlns="urn:oasis:names:tc:SPML:2:0"
xmlns:dsml="urn:oasis:names:tc:DSML:2:0:core">
<data>
  <dsml:attr name="objectclass">
    <dsml:value>Users</dsml:value>
  </dsml:attr>
  <dsml:attr name="Users.User ID">
    <dsml:value>John Doe</dsml:value>
  </dsml:attr>
  <dsml:attr name="Users.First Name">
    <dsml:value>John</dsml:value>
  </dsml:attr>
  <dsml:attr name="Users.Last Name">
    <dsml:value>Doe</dsml:value>
  </dsml:attr>
```

```
  <dsml:attr name="Organizations.Organization Name">
    <dsml:value>Xellerate Users</dsml:value>
  </dsml:attr>
  <dsml:attr name="Users.Xellerate Type">
    <dsml:value>End-User</dsml:value>
  </dsml:attr>
  <dsml:attr name="Users.Role">
    <dsml:value>Full-Time</dsml:value>
  </dsml:attr>
  <dsml:attr name="Users.Password">
    <dsml:value>welcome</dsml:value>
  </dsml:attr>
</data>
</addRequest>
</SPMLv2Document>
</soap:Body>
</soap:Envelope>
```

With WSSE security tags:

```
<?xml version="1.0" encoding="utf-8"?>
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<soapenv:Header>
<wsse:Security
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-sec
ext-1.0.xsd">
<wsse:UsernameToken>
<wsse:Username>user1</wsse:Username>
<wsse:Password
Type="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profi
le-1.0#PasswordText">password1</wsse:Password>
</wsse:UsernameToken>
</wsse:Security>
</soapenv:Header>
<soapenv:Body>
<SPMLv2Document xmlns="http://xmlns.oracle.com/OIM/provisioning">
<addRequest returnData="everything" xmlns="urn:oasis:names:tc:SPML:2:0"
xmlns:dsml="urn:oasis:names:tc:DSML:2:0:core">
<data>
  <dsml:attr name="objectclass">
    <dsml:value>Users</dsml:value>
  </dsml:attr>
  <dsml:attr name="Users.User ID">
    <dsml:value>John Doe</dsml:value>
  </dsml:attr>
  <dsml:attr name="Users.First Name">
    <dsml:value>John</dsml:value>
  </dsml:attr>
  <dsml:attr name="Users.Last Name">
    <dsml:value>Doe</dsml:value>
  </dsml:attr>
  <dsml:attr name="Organizations.Organization Name">
    <dsml:value>Xellerate Users</dsml:value>
  </dsml:attr>
  <dsml:attr name="Users.Xellerate Type">
    <dsml:value>End-User</dsml:value>
  </dsml:attr>
  <dsml:attr name="Users.Role">
```

```
    <dsml:value>Full-Time</dsml:value>
  </dsml:attr>
  <dsml:attr name="Users.Password">
    <dsml:value>welcome</dsml:value>
  </dsml:attr>
</data>
</addRequest>
</SPMLv2Document>
</soapenv:Body>
</soapenv:Envelope>
```

13

Segregation of Duties (SoD) in Oracle Identity Manager

The concept of Segregation of Duties (SoD) is aimed at applying checks and balances on business processes. Each stage of a business process may require the involvement of more than one individual. An organization can convert this possibility into a requirement for all IT-enabled business processes by implementing SoD as part of its user provisioning solution. The overall benefit of SoD is the mitigation of risk arising from intentional or accidental misuse of an organization's resources.

In the Oracle Identity Manager implementation of SoD, IT privilege (entitlement) requests submitted by a user are checked and approved by an SoD engine and other users. Multiple levels of system and human checks can be introduced to ensure that even changes to the original request are vetted before the request is cleared. This preventive simulation approach helps identify and correct potentially conflicting assignment of entitlements to a user, before the requested entitlements are granted to the user.

This chapter describes how SoD is used to process entitlement requests generated in Oracle Identity Manager and the procedures that you can follow to implement SoD.

This chapter is divided into the following sections:

- Section 13.1, "SoD Implementation in Oracle Identity Manager" provides information about the implementation of SoD in Oracle Identity Manager.
- Section 13.2, "SoD Validation Process in Oracle Identity Manager" describes how the SoD validation process works in Oracle Identity Manager.
- Section 13.3, "Implementing and Enabling SoD" describes the procedures involved in implementing and enabling SoD in Oracle Identity Manager.
- Section 13.4, "Configuring Connectors for SoD" describes procedures that you must perform if you want to use a target system other than Oracle e-Business Suite, SAP CUA, and SAP R/3.
- Section 13.5, "Creating SIL Providers" describes procedures that you must perform if you want to use an SoD engine other than SAP GRC and Oracle Application Access Controls Governor.

13.1 SoD Implementation in Oracle Identity Manager

The SoD Invocation Library (SIL) forms the basis of the SoD implementation in Oracle Identity Manager. The SIL is a collection of Java-based adapters that enable integration with predefined Oracle Identity Manager connectors. The connectors, in turn, link

Oracle Identity Manager with the target systems. The following Oracle Identity Manager connectors are preconfigured for SoD validation:

- Oracle e-Business User Management release 9.1.0 and later
- SAP CUA release 9.1.0 and later
- SAP User Management release 9.1.0 and later

The SIL also acts as the base for specialized adapters that integrate the SIL with SoD engines. These adapters are called SIL providers. A SIL provider acts as the interface between the SIL and a specific SoD engine. There are predefined SIL providers for the following SoD engines:

- SIL Provider for SAP GRC

  This provider is also known as the SAP GRC SIL Provider.. The certified versions of SAP GRC are versions 5.2 SP4 or later and 5.3 SP5 or later

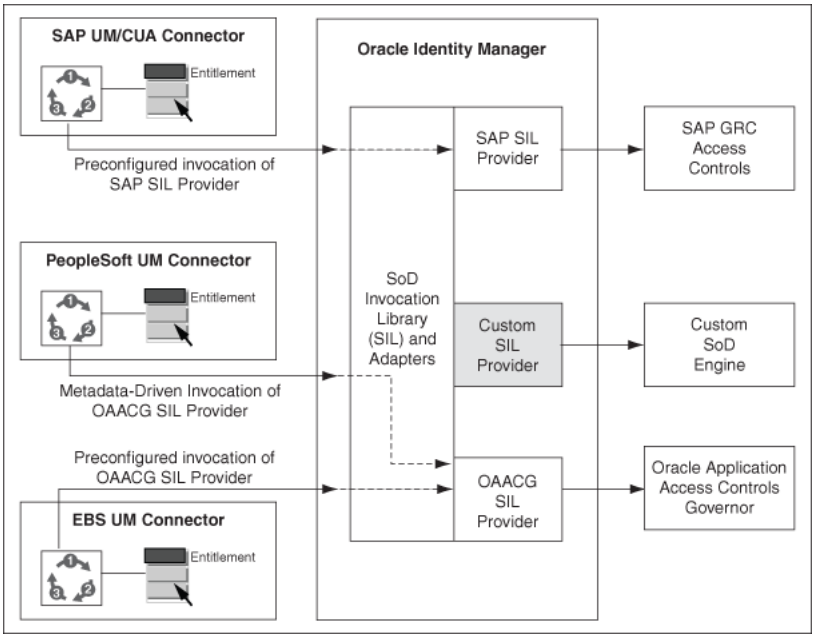
- SIL Provider for Oracle Application Access Controls Governor release 8.2.1 or later

  This provider is also known as the OAACG SIL Provider.

> **Note:** Contact Oracle Support for information about the latest patch set for Oracle Application Access Controls Governor. You must install the latest patch set before you start implementing and using SoD in Oracle Identity Manager.

Figure 13–1 shows the architecture of SoD implementation in Oracle Identity Manager.

Figure 13–1 Architecture of SoD Implementation in Oracle Identity Manager



If required, you can configure any Oracle Identity Manager connector with either the SAP GRC SIL Provider or OAACG SIL Provider. For example, you can use the PeopleSoft User Management connector and the OAACG SIL Provider to automate SoD validation of requests for entitlements on PeopleSoft Enterprise Applications.

You can also create and use a SIL provider for a custom SoD engine, along with either one of the preconfigured Oracle Identity Manager connectors or an Oracle Identity Manager connector that you configure for SoD validation.

13.2 SoD Validation Process in Oracle Identity Manager

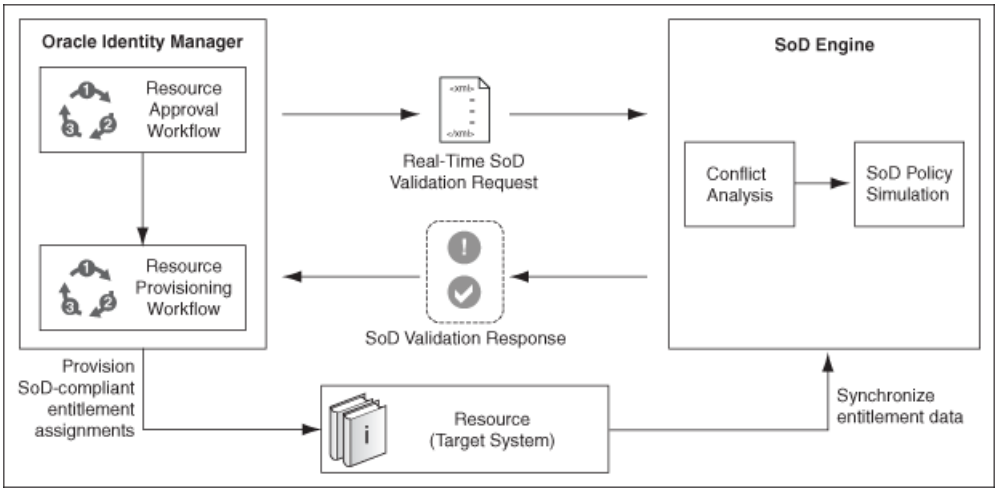
Oracle Identity Manager is a user provisioning solution. Entitlement requests can be managed on Oracle Identity Manager.

The SoD validation process in Oracle Identity Manager begins when a user creates a request for an entitlement on a particular target system. The resource approval workflow of Oracle Identity Manager can be configured to validate this request in real time with an SoD engine. The SoD engine uses predefined rules to check if the entitlement assignment would lead to SoD violations. The outcome of this check is then sent back to Oracle Identity Manager. If the request fails SoD validation, then the approval workflow can be configured to take remediation steps. If the request passes SoD validation and if the approver approves the request, then the resource provisioning workflow is initiated. This resource provisioning workflow can also be configured to perform the SoD validation again. This is to ensure SoD compliance of the entitlement assignment immediately before the entitlement assignment is provisioned to the target system. You can also configure the SoD validation check in the resource provisioning workflow to be bypassed if this validation has been passed in the resource approval workflow.

Oracle Identity Manager is integrated with both the SoD engine and the target system. In addition, the target system and SoD engine are integrated to enable the synchronization of entitlement data from the target system to the SoD engine.

Figure 13–2 shows the flow of data during the SoD validation process.

Figure 13–2 SoD Validation Process in Oracle Identity Manager



13.3 Implementing and Enabling SoD

The following is a summary of the steps involved in implementing and enabling SoD in Oracle Identity Manager:

1. The SoD process involves the use of dedicated database tables. These tables are automatically created when you install the database schema for Oracle Identity Manager release 9.1.0.2. If you decide not to use the Oracle Identity Manager

database schema, then perform the procedure described in Section 13.3.1, "Creating the SIL Database Schema" to create a schema for the SIL.

2. Install and configure the Oracle Identity Manager connector for the target system that you want to use for SoD validation.

   See Section 13.3.2, "Installing and Configuring the Oracle Identity Manager Connector" for instructions.

3. Download external files required by the SIL providers. See Section 13.3.3, "Copying Files Required by the SIL Providers" for instructions.
4. Import entitlement data from the target system into the SoD engine. See Section 13.3.4, "Configuring the SoD Engine" for instructions.
5. Perform the procedure described in Section 13.3.5, "Deploying the SIL and SIL Providers" to deploy and configure the SIL and SIL providers.
6. See Section 13.3.7, "Enabling SoD" for instructions on enabling SoD validation of entitlement requests.
7. See Section 13.3.8, "Enabling Logging for SoD-Related Events" for instructions on enabling logging for SoD-related events.

13.3.1 Creating the SIL Database Schema

Note: Perform the procedure described in this section only if you do not want to use the Oracle Identity Manager database schema for the SIL database tables.

The SIL database tables are created in the Oracle Identity Manager database schema when you perform the procedure to upgrade to Oracle Identity Manager release 9.1.0.2.

If you want to use a different schema for the SIL database tables, then:

To create the SIL database tables, run the SoDInvocationDBScript.sql script provided in one of the following directories:

For Microsoft SQL Server:

SIL_HOME/database/script/mssql

For Oracle Database:

SIL_HOME/database/script/oracle

13.3.2 Installing and Configuring the Oracle Identity Manager Connector

Install and configure the Oracle Identity Manager connector for the target system that you want use for SoD validation.

To access the complete Oracle Identity Manager connector documentation set, visit Oracle Technology Network at

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

13.3.3 Copying Files Required by the SIL Providers

Depending on the SIL provider that you plan to use, see the instructions in one of the following sections:

- Section 13.3.3.1, "Copying Files Required by the OAACG SIL Provider"
- Section 13.3.3.2, "Copying Files Required by the SAP GRC SIL Provider"

13.3.3.1 Copying Files Required by the OAACG SIL Provider

To copy the external files required by the OAACG SIL Provider:

1. Download the abdera.0.3.0-incubating.jdk142.zip file from the Apache Abdera Web site at

   `http://abdera.apache.org/`

2. Extract the contents of this ZIP file into a temporary directory.
3. From the extracted contents, copy the following jars to the *OIM_HOME*/ext directory.

   abdera.parser.0.3.0-incubating.retro.jar

   abdera.core.0.3.0-incubating.retro.jar

4. From the lib directory in the extracted contents, copy the following jars to the *OIM_HOME*/ext directory.

   abdera-i18n-0.3.0-incubating.retro.jar

   commons-codec-1.3.jar

   log4j-1.2.14.jar

   axiom-api-1.2.5.jar

   commons-logging-1.0.4.jar

   retroweaver-rt-2.0.jar

   axiom-impl-1.2.5.jar

   jaxen-1.1.1.jar

   stax-api-1.0.1.jar

5. Download a JAR file implementation of STAX (stax-1.2.0.jar) from the following Web page:

   `http://dist.codehaus.org/stax/jars`

6. Copy this JAR file into the *OIM_HOME*/ext directory.

13.3.3.2 Copying Files Required by the SAP GRC SIL Provider

To copy the external files required by the SAP GRC SIL Provider:

1. Search for and download the axis-bin-1_4.zip file from the following Web site:

   `http://www.apache.org`

2. Extract the contents of the axis2-1.4-bin.zip file to a temporary directory.
3. From the *TEMPORARY_DIRECTORY*/axis-1_4/lib directory, copy the following files into the *OIM_HOME*/xellerate/ext directory:
   - wsdl4j-1.5.1.jar
   - axis.jar
   - jaxrpc.jar
   - saaj.jar

- commons-discovery-0.2.jar
- commons-logging-1.0.4.jar

13.3.4 Configuring the SoD Engine

You must import entitlement data from the target system to the SoD engine. If required, you must also configure SoD validation rules on the SoD engine.

The following sections provide these instructions for the preconfigured SoD engines:

- Configuring Oracle Application Access Controls Governor
- Configuring SAP GRC

13.3.4.1 Configuring Oracle Application Access Controls Governor

Configuring Oracle Application Access Controls Governor involves the following procedures:

- Creating an Oracle Application Access Controls Governor Account for SoD Operations
- Synchronizing Role and Responsibility Data from Oracle e-Business Suite to Oracle Application Access Controls Governor
- Defining Access Policies in Oracle Application Access Controls Governor

Creating an Oracle Application Access Controls Governor Account for SoD Operations

Create an account of the Basic type for SoD validation operations. While performing the procedure described in Section 13.3.5.1, "Creating an IT Resource to Hold Information about the SoD Engine", you provide the user name and password of this account.

See Oracle Application Access Controls Governor documentation for information about creating the account.

Synchronizing Role and Responsibility Data from Oracle e-Business Suite to Oracle Application Access Controls Governor

You must import (synchronize) role and responsibility data from Oracle e-Business Suite into Oracle Application Access Controls Governor. After first-time synchronization, you must schedule periodic synchronization of data.

See Oracle Application Access Controls Governor documentation for more information.

Defining Access Policies in Oracle Application Access Controls Governor

After you import role and responsibility data, set up access policies in Oracle Application Access Controls Governor. These access policies are based on various combinations of roles and responsibilities.

See Oracle Application Access Controls Governor documentation for more information.

13.3.4.2 Configuring SAP GRC

SAP GRC uses user, role, and profile data from SAP R/3 to validate requests for accounts, roles, and responsibilities. Configuring SAP GRC involves the following procedures:

- Creating an SAP GRC Account for SoD Operations
- Generating the Keystore
- Configuring the Risk Terminator
- Synchronizing User, Role, and Profile Data from SAP ERP to SAP GRC
- Defining Risk Policies in SAP GRC
- Configuring the Oracle Identity Manager Application Server for SAP GRC

Creating an SAP GRC Account for SoD Operations

You must create an SAP GRC account for SoD operations. During SoD operations, this account is used to call the SAP GRC Web service.

When you create this user account, you must assign it to the following groups:

- Everyone
- Authenticated Users

You must not assign any roles to this account.

Generating the Keystore

To generate the keystore:

1. In a Web browser, open the Web Services Navigator page of SAP GRC Access Control. The URL is similar to the following:

   `https://`*`SAP_GRC_HOST`*`:`*`PORT_NUMBER`*`/VirsaCCRiskAnalysisService/Config1?wsdl`

2. Export the certificate.
3. Copy the certificate into the bin directory inside the JDK installation directory of SAP GRC.
4. Run the following command to create the keystore from the certificate file that you download:

   ```
   keytool -import -v -trustcacerts -alias sapgrc -file CERTIFICATE_FILENAME
   -keystore sgil.keystore -keypass changeit -storepass changeit
   ```

   Note: In this sample command, the keystore file name is sgil.keystore.

5. When prompted for the keystore password, specify `changeit`. This is the default keystore password.
6. When prompted to specify whether you want to trust the certificate, enter `yes`.
7. The sgil.keystore file is created in the bin directory. Copy the file to the *OIM_HOME*\config directory.

Configuring the Risk Terminator

The Risk Terminator is a feature of GRC Access Control. It is the main component of the SoD validation functionality of SAP GRC. Whenever a role is created in the profile generator or assigned to a user, the Risk Terminator verifies if this role creation or assignment would result in an SoD violation.

See the Risk Terminator Configuration document for detailed information.

Synchronizing User, Role, and Profile Data from SAP ERP to SAP GRC

User, role, and profile data must be imported (synchronized) from SAP ERP into SAP GRC. After first-time synchronization, you must schedule periodic synchronization of data.

Defining Risk Policies in SAP GRC

After you import role and responsibility data, use the Risk Analysis and Remediation feature of SAP GRC to define risk policies of type Segregation of Duty.

See SAP GRC documentation for more information.

Configuring the Oracle Identity Manager Application Server for SAP GRC

If Oracle Identity Manager is running on Oracle Application Server, then:

1. Extract the contents of the *OAS_HOME*/j2ee/home/oc4j.jar file into a temporary directory.
2. In a text editor, open the boot.xml file. This is one of the files in the oc4j.jar file.
3. Add the following lines under the <system-class-loader> element in the boot.xml file:

   ```
   <code-source path="OIM_HOME/xellerate/ext/wsdl4j-.5.1.jar"/>
   <code-source path="OIM_HOME/xellerate/ext/log4j-1.2.8.jar"/>
   <code-source path="OIM_HOME/xellerate/ext/saaj.jar"/>
   <code-source path="OIM_HOME/xellerate/ext/axis.jar"/>
   <code-source path="OIM_HOME/xellerate/ext/commons-discovery-0.2.jar"/>
   <code-source path="OIM_HOME/xellerate/ext/commons-logging-1.0.4.jar"/>
   <code-source path="OIM_HOME/xellerate/ext/jaxrpc.jar"/>
   ```

   Here, replace *OIM_HOME* with the full path of the *OIM_HOME* directory. For example, if *OIM_HOME* directory is c:/programfiles/oim, then the line of code must be:

   <code-source path="c:/programfiles/oim/xellerate/ext/wsdl4j-.5.1.jar"/>
4. Re-create the oc4j.jar file and copy it into the *OAS_HOME*/j2ee/home directory.

If Oracle Identity Manager is running on Oracle WebLogic Application Server, then:

1. Open the *OIM_HOME*/config/log.properties file in a text editor.
2. In this file, add the following line:

   ```
   log4j.logger.org.apache.axis.ConfigurationException = INFO
   ```
3. Save and close the file.
4. Open the *OIM_HOME*/bin/xlStartServer.bat file in a text editor.
5. Search for the Domain Location entry in this file. The following is a sample entry in the file:

   ```
   pushd "D:\bea\user_projects\domains\oim9102\bin"
   xlStartWLS.cmd
   popd
   ```

   Here `D:\bea\user_projects\domains\oim9102` is the Domain Location entry in the file.
6. Copy the commons-logging-1.0.4.jar file into the lib directory that is inside the Domain Location directory.

13.3.5 Deploying the SIL and SIL Providers

When you register the SIL, you provide details of the Oracle Identity Manager installation, SoD engine, and target system that you want to use. During a single registration session, you can register multiple Oracle Identity Manager installations, SoD engines, and target systems. Each combination of Oracle Identity Manager installation, SoD engine, and target system is assigned a unique ID during the registration process.

The registration script (registration.sh and registration.bat) drives the registration process. When you run this script, it prompts you for the required information. The initial set of prompts displayed by the script are read from the registration.xml file. The registration script is in the *SIL_HOME*/scripts directory. The registration.xml file is in the *SIL_HOME*/registrationXML directory.

Deploying the SIL and SIL providers involves the following procedures:

- Section 13.3.5.1, "Creating an IT Resource to Hold Information about the SoD Engine"
- Section 13.3.5.2, "Running the Registration Script and Providing Registration Information"
- Section 13.3.5.3, "Recording the Names of the System Types"
- Section 13.3.5.4, "Deploying the SIL_HOME Directory in a Clustered Environment"

13.3.5.1 Creating an IT Resource to Hold Information about the SoD Engine

As mentioned earlier, the registration.xml file provides the initial set of prompts that are displayed by the registration script. In this XML file, the SystemType element is used to display prompts that ask for information about the SoD engine.

You must create an IT resource to hold information about the SoD engine.

See *Oracle Identity Manager Design Console Guide* for detailed information about creating an IT resource type (if it does not already exist) and IT resource. You can specify any name for the IT resource type and IT resource. The following table specifies the names of the parameters that the IT resource must contain:

Parameter	Description	Sample Value
Source Datastore Name	Enter the name of the source data store (the target system) that you defined in the SoD engine. You specify a source data store name while performing the procedure described in the "Configuring Oracle Application Access Controls Governor" section.	`EBS STMD122`
dbuser	Enter the user name of the schema owner on the database used by the SoD engine. This account is used to access the Application Access Controls Governor database during SoD operations. **Note:** This parameter is specific to Oracle Application Access Controls Governor.	`databaseusr1`
dbpassword	Enter the password of the schema owner on the database used by the SoD engine. **Note:** This parameter is specific to Oracle Application Access Controls Governor.	`Cryp100ne`

Parameter	Description	Sample Value
jdbcURL	Enter the JDBC URL for connecting to the database used by the SoD engine. **Note:** This parameter is specific to Oracle Application Access Controls Governor.	`jdbc:oracle:thin:@10.123.123.123`
password	Enter the password of the account created on the SoD engine for API calls.	`K1rb1r0s`
port	Enter the number of the port at which the SoD engine is listening.	`8090`
server	Enter the IP address of the host computer on which the SoD engine is running.	`10.231.231.231`
sslEnable	Enter `true` if the SoD engine accepts only HTTPS communication requests. Otherwise, enter `false`.	`false`
username	Enter the user name of an account created on the SoD engine. This account is used to call the SoD engine APIs that are used during SoD validation.	`jdoe`

Note: If you want to use multiple SoD engines, then create multiple IT resources with the same IT resource type.

13.3.5.2 Running the Registration Script and Providing Registration Information

Note: You can run the registration script multiple times, at any time during the lifecycle of the Oracle Identity Manager installation. For example, you might want to register a new SoD engine. When you run the script, use the prompts to guide you to the section (set of prompts) in which you want provide input. You can skip the remaining sections.

See Example 13–1 for a sample run of the registration script. In that example, it is assumed that an IT resource has been created to provide information about the SoD engine.

To run the script and provide registration information for the Oracle Identity Manager installation, SoD engine, and target system:

1. Ensure that the appropriate Oracle Database or Microsoft SQL Server database drivers are available in the *OIM_HOME*/xellerate/ext directory.
2. Open the *SIL_HOME*/SILConfig.xml file in a text editor and provide values for the following elements:
   - **SecurityImpl**

     Enter one of the following class names as the value of this element:

     – Enter `oracle.iam.grc.sod.infrastructure.impl.OIM91CryptoOperations` if you want to use the security implementation (model) predefined in Oracle Identity Manager.

     – Enter `oracle.iam.grc.sod.infrastructure.impl.SILCryptoOperati`

`ons` if you want to use the security implementation (model) predefined in the SIL.

- **DirectDB:** Set values for the following elements:

Note: If the SIL is using the Oracle Identity Manager database schema, then the connection information must be the same as the information given in the xlconfig.xml file.

Provide the database connection parameters as follows:

a. Open the *SIL_HOME*/SILConfig.xml file in a text editor.

Note: Whenever you make changes in the SILConfig.xml file, you must restart Oracle Identity Manager for the changes to take effect. If you are going to perform the remaining procedures described in this chapter, then you need not restart Oracle Identity Manager at this point. You will be instructed to restart Oracle Identity Manager later.

---

b. In the SILConfig.xml file, search for the following lines:

```
<!-- SIL DB Parameters for jdbc connectivity -->
    <directDB>
        <driver>@jdbcDriver</driver>
        <url>@jdbcUrl</url>
        <username>@dbUserName</username>
        <password encrypted="false">@dbPassword</password>
    </directDB>
```

c. In these lines, replace the following with values from the database that you are using:

@jdbcDriver

Replace this string with the JDBC driver for the database that you want to use:

Sample driver for Microsoft SQL Server:

```
com.microsoft.sqlserver.jdbc.SQLServerDriver
```

Sample driver for Oracle Database:

```
oracle.jdbc.driver.OracleDriver
```

@jdbcUrl

Replace this string with the JDBC URL for the database that you want to use.

Sample URL for Microsoft SQL Server:

```
jdbc:sqlserver://HOST_NAME/IP_ADDRESS:DATABASE_PORT;DatabaseName=DATABASE_NAME
```

Sample URL for Oracle Database:

```
jdbc:oracle:thin:@HOST_NAME/IP_ADDRESS:DATABASE_PORT:SID
```

@dbUserName

Replace this string with the user name of the database account that you want to use for SoD operations.

@dbPassword

Replace this string with the password in plain text of the database account that you want to use for SoD operations.

Note: The password is converted to encrypted format at the end of the registration process.

---

d. Save and close the SILConfig.xml file.

- **DOMBuilderFactoryImpl**

  The value of the DOMBuilderFactoryImpl element depends on the JRE that you are using:

  – If you are using the Sun JRE or Oracle JRockit JRE, then uncomment the DOMBuilderFactoryImpl element containing the following value:

  ```
  com.sun.org.apache.xerces.internal.jaxp.DocumentBuilderFactoryImpl
  ```

  – If you are using the IBM JRE, then uncomment the DOMBuilderFactoryImpl element containing the following value:

  ```
  org.apache.xerces.jaxp.DocumentBuilderFactoryImpl
  ```

3. Save and close the SILConfig.xml file.
4. Open one of the following script files in a text editor:

   For Microsoft Windows: *SIL_HOME*/scripts/registration.bat

   For UNIX: *SIL_HOME*/scripts/registration.sh
5. In the script file, search for `OIM_HOME`.
6. Specify the full path of the Oracle Identity Manager installation directory as the value of the OIM_HOME variable in the file. For example:

   ```
   OIM_HOME = /Installations/OIM9102/server/xellerate
   ```
7. Save and close the file.
8. In a command window, switch to the *SIL_HOME*/scripts directory and run the registration script.

   Note: From this point onward, an explanation of each prompt displayed by the script is followed by the actual message of the prompt. The actual message is shown in monospace font in this document.

   ---
9. Select the security model that you want to use. You are prompted with the following message:

   ```
   Which Security Model you want to use? (1 or 2)
   1) Idm System
   2) SoD Invocation Library
   ```
10. Your response can be one of the following:

- Enter `1` if you want to use the security model offered by Oracle Identity Manager. When you enter 1, the full path of the *OIM_HOME* directory that you entered in the registration script is displayed:

  For example:

  ```
  /Installations/OIM9102/server/xellerate
  ```

- Enter `2` to select the SIL security model. You are prompted to specify whether or not you want to generate a keystore:

  ```
  Generate new Keystore?(y/n)
  ```

  – Enter `y`, because you are registering SIL for the first time. You are prompted to set a password for the keystore.

  ```
  Generating Keystore
  Password for DB Access:
  ```

  Note: You can ignore the warning messages that are displayed at this point.

  – Provide a password to generate the keystore. An encrypted password is generated by using the password provided. You must copy this encrypted password into the *SIL_HOME*/SILConfig.xml file.

  The following lines show a sample encrypted password value:

  ```
  Encrypted value of password: cuMcTHK60ZMa+HnX2FK9vw==
  Keystore Generated, Copy Encrypted Password in SIL_Config."
  ```

  The following is the block of code in the SILConfig.xml file where you must copy the encrypted password:

  Note: The placeholder that you must replace with the encrypted password is highlighted in bold.

```
<Security>
  <!-- Symmetric Encryption Provider implementation java class.
  A sample value is
"oracle.iam.grc.sod.encryption.DefaultDBEncryptionImpl"-->
       <!--<SymmetricProvider>@providerClass</SymmetricProvider>-->

<SymmetricProvider>oracle.iam.grc.sod.encryption.DefaultDBEncryptionImp
l</SymmetricProvider>
      <XLSymmetricProvider>
    <KeyStore>
        <!-- Location of the generated keystore, used during database
level encryption.
        The value of the directory location including the filename of
the keystore should
        be relative to SIL home directory. A sample value is
"security/.silkeystore"-->
        <!--<Location>@keystoreLocation</Location>-->
        <Location>security/.silkeystore</Location>
        <!-- Keystore password. It should be first encrypted using
"Encryptpassword.bat"
```

```
        and the encrypted value should be defined below.
         A sample value is "RN2+ji9vQ1OX6l/BQ6hPUA=="-->
        <Password encrypted="true">@keystorePassword</Password>
        <!-- Keystore Type. A sample value is "JCEKS"-->
        <!--<Type>@keystoreType</Type>-->
        <Type>JCEKS</Type>
        <!-- Keystore provider. A sample value is
"com.sun.crypto.provider.SunJCE"-->
        <!--<Provider>@providerClass</Provider>-->
        <Provider>com.sun.crypto.provider.SunJCE</Provider>
    </KeyStore>
    <Keys>
        <DBSecretKey>
      <!-- Alias for the symmetric key. Should be same the value
      of parameter "alias" in "SetDBKey.bat". A sample value is
"sil"-->
      <!--<Alias>@alias</Alias>-->
      <Alias>sil</Alias>
      <!-- Key password. It should be first encrypted using
"Encryptpassword.bat"
      and the encrypted value should be defined below.
       A sample value is "RN2+ji9vQ1OX6l/BQ6hPUA=="-->
      <Password encrypted="true">@keyPassword</Password>
   <!-- Block Mode for the symmetric key. A sample value is "CBC"-->
      <!--<BlockMode>@keyBlockMode</BlockMode>-->
      <BlockMode>CBC</BlockMode>
        </DBSecretKey>
    </Keys>
      </XLSymmetricProvider>
    </Security>
```

11. You are prompted to specify whether or not you want to proceed with registration:

    ```
    Do you want to proceed with registration? (y/n)
    ```

12. Enter `y` to proceed with the registration. You are prompted to specify whether or not you want to register an Oracle Identity Manager installation:

    ```
    Register System Instance for type OIM?(y/n)
    ```

13. Enter `y`.

14. You are prompted to enter an instance name for the Oracle Identity Manager installation:

    ```
    Provide instance name
    ```

15. Enter a name for the Oracle Identity Manager installation. For example:

    ```
    oim0
    ```

> **Note:** From this point onward, the flow is specific to the registration of an Oracle e-Business Suite and Oracle Application Access Controls Governor installation. The flow is almost the same for the SAP CUA or SAP R/3 and SAP GRC installation.

16. You are prompted to specify whether or not you want to register an Oracle e-Business Suite installation:

```
Register System Instance for type EBS? (y/n)
```

17. Enter `y` if you want to use an Oracle e-Business Suite installation as the target system. Otherwise, enter `n`.
18. If you enter `y`, then you are prompted to enter an instance name for the Oracle e-Business Suite installation:

    ```
    Provide instance name
    ```

    Enter a name for the Oracle e-Business Suite installation. For example:

    ```
    ebs2
    ```

19. You are prompted to specify whether or not you want to register an Oracle Application Access Controls Governor installation:

    ```
    Register System Instance for type OAACG? (y/n)
    ```

20. If you enter `y`, then you are prompted to enter an instance name for the Oracle Application Access Controls Governor installation:

    ```
    Provide instance name
    ```

    Enter a name for the Oracle Application Access Controls Governor installation. For example:

    ```
    oaacg01
    ```

21. You are prompted to enter the name of the IT resource that you have created:

    ```
    OIM ITResource Instance Name:
    ```

    Enter the name of the IT resource that you created: `OAACG ITR2`
22. If there are no more SoD components (system instances) to register, then enter `n` in response to the remaining prompts.

Example 13–1 shows the output of a sample run of the registration script. Here, it is assumed that an IT resource has been created to provide information about the SoD engine.

Example 13–1 Sample Run of the Registration Script

```
Which Security Model you want to use?(1 or 2)
1) IdM System
2) SoD Invocation Library
1
OIM_HOME provided by you via Registration.bat is: C:\OIM_installations\wls_ibm_2
\installation\xellerate
Do you want to proceed with registration? (y/n)
y
log4j:WARN No appenders could be found for logger (XELLERATE.JAVACLIENT).
log4j:WARN Please initialize the log4j system properly.
Register System Instance for type OIM ?(y/n)
y
Provide instance name
oim1
Register System Instance for type EBS ?(y/n)
y
Provide instance name
ebs1
Register System Instance for type OAACG ?(y/n)
```

```
y
Provide instance name
oaacg1
OIM ITResource Instance Name:
OAACG ITR2
Register System Instance for type SAP ?(y/n)
n
Register System Instance for type GRC ?(y/n)
n
```

13.3.5.3 Recording the Names of the System Types

At the end of the registration process, the names of the system types are set in the Oracle Identity Manager database. You can retrieve these names from the database by using the registration script. After you retrieve these names, you must enter them in the SILConfig.xml file.

To retrieve and record the names of the service components:

1. In a command window, switch to the following directory:

   SIL_HOME/script

2. Run one the following commands:

   For Microsoft Windows:

   ```
   registration.bat printRegistrationIDs
   ```

   For UNIX:

   ```
   registration.sh printRegistrationIDs
   ```

   The following is sample output of this command:

   ```
   ----------------------------------------------
   System Type     Instance Name  Registration ID
   ----------------------------------------------
   OIM                oim                     1
   EBS                Ebs                     2
   OAACG              oaacg                   3
   ```

3. Copy these instance names for your reference.

4. Open the *SIL_HOME*/SILConfig.xml file in a text editor and provide values for the Topologies element:

   The following block of XML shows the Topologies element and its child elements:

   Note: If you have multiple target system and SoD engine combinations, then you can add multiple Topology elements inside the Topologies element.

```
<Topologies>
  <Topology>
   <name>@topologyName</name>
   <IdmId>@Idm RegistrationId</IdmId>
   <SodId>@Sod RegistrationId</SodId>
   <SDSId>@Sds RegistrationId</SDSId>
  </Topology>
</Topologies>
```

Enter values for the following child elements of the Topologies element:

– `@topologyName`: Enter a name for the topology.

> **Note:** Later in this procedure, you set the value of the TopologyName IT resource parameter to the name that you specify for the Topology element.

– `@Idm RegistrationId`: Enter the registration ID of the Oracle Identity Manager installation.

– `@Sod RegistrationId`: Enter the registration ID of the SoD engine.

– `@Sds RegistrationId`: Enter the registration ID of the target system.

5. Set the value of the DataAccessImpl element in the SILConfig.xml file as follows

   a. Comment the following line:

   ```
   <DataAccessImpl>oracle.iam.grc.sod.infrastructure.impl.DBOperationsTest</DataAccessImpl>
   ```

   b. Uncomment the following line:

   ```
   <DataAccessImpl>oracle.iam.grc.sod.infrastructure.impl.OIM91DBOperations</DataAccessImpl>
   ```

6. Save and close the SILConfig.xml file.

13.3.5.4 Deploying the SIL_HOME Directory in a Clustered Environment

In a clustered environment, copy the *SIL_HOME* directory to each node of the cluster. In addition, ensure that the structure of this directory is the same across all nodes of the cluster.

> **Note:** Whenever you make changes in the SILConfig.xml file, you must restart Oracle Identity Manager for the changes to take effect. If you are going to perform the remaining procedures described in this chapter, then you need not restart Oracle Identity Manager at this point. You will be instructed to restart Oracle Identity Manager later.

13.3.6 Enabling SSL Communication Between the SoD engine and Oracle Identity Manager

> **Note:** This section describes an optional procedure. Perform this procedure only if you want to enable SSL communication between the SoD engine and Oracle Identity Manager.

Perform one of the following procedures:

- Section 13.3.6.1, "Enabling SSL Communication Between Oracle Application Access Controls Governor and Oracle Identity Manager"
- Section 13.3.6.2, "Enabling SSL Communication Between SAP GRC and Oracle Identity Manager"

13.3.6.1 Enabling SSL Communication Between Oracle Application Access Controls Governor and Oracle Identity Manager

To enable SSL communication between Oracle Application Access Controls Governor and Oracle Identity Manager:

Note: It is assumed that you have set sslEnable to `true` during the registration process.

---

1. Export the certificate on the Oracle Application Access Controls Governor host computer as follows:

   Note: In Step 1, *JAVA_HOME* refers to the directory on the Oracle Application Access Controls Governor host computer.

   ---

   a. Run the following commands from the *JAVA_HOME*/bin directory:

   ```
   keytool -genkey -alias tomcat -keyalg RSA -keystore
   JAVA_HOME/lib/security/.keystore
   keytool -certreq -alias tomcat -file JAVA_HOME/lib/security/xell.cvs
   -keystore JAVA_HOME/lib/security/.keystore
   keytool -export -alias tomcat -file JAVA_HOME/lib/security/server.cert
   -keystore JAVA_HOME/lib/security/.keystore
   ```

   After you run these commands, the server certificate (server.cert) is created in the *JAVA_HOME*/lib/security directory.

   b. In the *TOMCAT_HOME*/conf/server.xml file, enter the details of the keystore as attributes of the Connector element. See the following example:

   ```
   <Connector port="8443" maxHttpHeaderSize="8192"
   maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
   enableLookups="false" disableUploadTimeout="true"
   acceptCount="100" scheme="https" secure="true"
   clientAuth="false" sslProtocol="TLS"
   keystoreFile="JAVA_HOME/lib/security/.keystore">
   ```

   c. Restart Oracle Application Access Controls Governor.

2. Import the certificate on the Oracle Identity Manager host computer as follows:

   Note: In Step 2, *JAVA_HOME* refers to the directory on the Oracle Identity Manager host computer.

   ---

   a. Copy the server certificate created on the Oracle Application Access Controls Governor host computer to the *JAVA_HOME*/lib/security directory of the Oracle Identity Manager host computer.

   b. Run the following command from the *JAVA_HOME*/bin directory:

   ```
   keytool -import -alias oaacg_trusted_cert  -file
   JAVA_HOME/lib/security/server.cert -trustcacerts -keystore
   JAVA_HOME/lib/security/cacerts -storepass changeit
   ```

13.3.6.2 Enabling SSL Communication Between SAP GRC and Oracle Identity Manager

To enable SSL communication between SAP GRC and Oracle Identity Manager export the certificate on the SAP GRC host computer as follows:

> **Note:** In this section, *JAVA_HOME* refers to the directory on the Oracle Identity Manager host computer that is used to run the application server.

1. In a Web browser, open the Web Services Navigator page of SAP GRC Access Control. The URL is similar to the following:

   ```
   https://mysapserver01:50001/VirsaCCRiskAnalysisService/Config1?wsdl
   ```

2. The next step depends on the browser that you are using:
   - On Microsoft Internet Explorer: In the Security Alert dialog box, click **View Certificate**. On the Details tab of the dialog box, use the **Copy to file** button to export the certificate.
   - On Mozilla Firefox: Export the certificate as a `.pem` file. To be able to perform this step, you might need to download and install the Certificate Viewer enhancement from the Mozilla Web site.
3. Copy the certificate into the *JAVA_HOME*/lib/security directory used by the application server hosting Oracle Indentity Manager.
4. In a terminal window, change to the *JAVA_HOME*/bin directory.
5. Run the following command to import the GRC certificate to cacerts:

   ```
   keytool -import -alias sapgrc_trusted_cert -file JAVA_HOME/lib/security/
   CERTIFICATE_FILENAME -trustcacerts -keystore JAVA_HOME/lib/security/cacerts
   -storepass changeit
   ```

   In this command:
   - *CERTIFICATE_FILENAME* is the name of certificate that has been exported from the SAP GRC host computer
   - The `-storepass changeit` clause specifies the password for the cacerts keystore.
6. When prompted to specify whether or not you want to trust the certificate, enter `yes`.

   The "Certificate was added to keystore" message is displayed.

13.3.7 Enabling SoD

To enable the SoD feature:

1. Set the XL.SoDCheckRequired system property to `true`.
2. Set the XL.SIL.Home.Dir system property to the full path and name of the *SIL_HOME* directory.
3. If you are using SAP GRC as the SoD engine, then perform the following step:

   SAP GRC might take a long time to return the results of a request validation operation. If required, you can schedule the submission of requests for SoD

validation at a specified time instead of waiting for SAP GRC to process the SoD validation request right away. In other words, you can change the synchronous SoD validation process on SAP GRC to an asynchronous process. To do this:

See Also: *Oracle Identity Manager Design Console Guide* for detailed information about these steps

a. Set the XL.SoD.Offlined.Sync system property to `true`.

b. Configure the following scheduled tasks to run:

   – **Resubmit Uninitiated Provisioning SOD Checks**

     During direct provisioning, if the SoD validation process remains in the SODCheckNotInitinitated state or SODCheckCompletedWithError state, then you can run the Resubmit Uninitiated Provisioning SOD Checks scheduled task to initiate the SoD validation process. When you run the scheduled task, the status of the process task is changed from SODCheckNotInitinitated or SODCheckCompletedWithError to SODCheckPending. Tasks in the SODCheckPending state are completed in the next run of the Get SOD Check Results Provisioning scheduled task.

   – **Resubmit Uninitiated Approval SOD Checks**

     During request-based provisioning, if the SoD validation process remains in the SODCheckNotInitinitated state or SODCheckCompletedWithError state, then you can run the Resubmit Uninitiated Approval SOD Checks scheduled task to initiate the SoD validation process. When you run the scheduled task, the status of the process task is changed from SODCheckNotInitinitated or SODCheckCompletedWithError to SODCheckPending. Tasks in the SODCheckPending state will be completed in the next run of the Get SOD Check Results Provisioning scheduled task.

Note: If you set the XL.SoD.Offlined.Sync system property to `false`, then these scheduled tasks are automatically disabled.

Alternatively, you can manually run these scheduled tasks after you submit entitlement request data through direct or request-based provisioning.

4. Set the TopologyName parameter in the IT resource of the connector to the topology name specified during SIL registration.

Disabling SoD

At any time after you enable SoD, you can disable it by performing the following procedure:

1. Set the XL.SoDCheckRequired system property to `false`.
2. Disable the Holder andSODChecker process tasks.

   See the connector guide for detailed information about disabling these process tasks.

13.3.8 Enabling Logging for SoD-Related Events

If you want to enable logging for all SoD-related events

1. Open the *OIM_HOME*/xellerate/config/log.properties file in a text editor.

2. Add the following line to the log.properties file:

   ```
   log4j.logger.XELLERATE.SOD=DEBUG
   ```

3. Enable the JAVACLIENT logger as follows:

   a. Search for the following line in the log.properties file:

      ```
      #log4j.logger.XELLERATE.JAVACLIENT=DEBUG
      ```

   b. Uncomment the line by removing the number sign (#) at the start of the line as shown here:

      ```
      log4j.logger.XELLERATE.JAVACLIENT=DEBUG
      ```

13.4 Configuring Connectors for SoD

Note:

Perform the procedure described in this section only if you want to use a target system other than Oracle e-Business Suite, SAP CUA, and SAP R3. You must also perform the procedures given in Section 13.5, "Creating SIL Providers" if you are using an SoD engine other than Oracle Application Access Controls Governor and SAP GRC.

You can perform this procedure either before or at any time after first-time implementation of SoD in Oracle Identity Manager.

The following is a summary of the procedure to configure the SIL for a new target system:

1. Follow instructions given in the Section 13.4.1, "Addressing Prerequisites" section.
2. Create Java class implementations of the IdMvsSoDDataTransformationOper interface for the connector. See Section 13.4.2, "Creating the Transformation Layer" for instructions.
3. Add entries in the registration XML file for the new target system. See Section 13.4.3, "Modifying the Registration XML File" for instructions.
4. Perform the procedure described in Section 13.4.4, "Configuring the Provisioning and Approval Workflows for SoD".
5. Mark child process forms that hold entitlement data. See Section 13.4.5, "Marking Child Process Form Tables That Hold Entitlement Data" for instructions.
6. Register the new target system. See Section 13.4.6, "Registering the New Target System" for instructions.

13.4.1 Addressing Prerequisites

Ensure that the following prerequisites are addressed:

1. Load entitlement data from the target system to the SoD engine.

   If you are using Oracle Application Access Controls Governor, then create policy definitions by using the data loaded from the target system.

   If you are using SAP GRC, then create risk definitions by using the data loaded from the target system.

For details, see vendor documentation for the SoD engine.

2. Deploy the Oracle Identity Manager connector for the target system. See the connector documentation for more information.

13.4.2 Creating the Transformation Layer

The transformation layer is used to transform target system attribute values into values that can be used by the SoD engine.

You must create the transformation layer as an implementation of the IdMvsSoDDataTransformationOper interface.

> **See Also:** The Javadocs shipped with this release of Oracle Identity Manager

If you are using Oracle Application Access Controls Governor, then create an implementation of the transformInput method in the implementation class of the IdMvsSoDDataTransformationOper interface.

If you are using an SoD engine other than Oracle Application Access Controls Governor, then create implementations of the transformInput and transformSoDAnalysisInput methods in the implementation class of the IdMvsSoDDataTransformationOper interface.

13.4.3 Modifying the Registration XML File

Enter the details of the transformation layer in the registration.xml file as follows:

1. Open the registration.xml file in a text editor. This file is in the *SIL_HOME*/registrationXML directory.
2. Add the SystemType and ServiceComponent elements as shown in this block of XML lines:

> **Note:** Values that you must set are highlighted in bold. Guidelines and sample values are given after this block of XML.

```
        <SystemType name="SYSTEM_TYPE_NAME" type="Sod Source
DataStore"></SystemType>

        <ServiceComponent type="IdMvsSoDDataTransformationOper"
name="NAME_FOR_IMPLEMENTATION"
                <Impl-Class>NAME_OF_IPMLEMENTATION_CLASS</Impl-Class>
                <IdMSystemType>OIM</IdMSystemType>
                <SoDEngineType>SoD_ENGINE</SoDEngineType>
                <srcSystemType>SYSTEM_TYPE_NAME</srcSystemType>

              <DataTransformation>
                    <AttrSoD type="user"
name="NAME_OF_ATTRIBUTE_ON_TARGET_SYSTEM"
sourceIdMAttrName="NAME_OF_ATTRIBUTE_ON_SOD_ENGINE" isSourceKey="true"/>
                    <AttrSoD type="user" name="firstname"
sourceIdMAttrName="firstname" isSourceKey="false"/>
                    <AttrSoD type="user" name="lastname"
sourceIdMAttrName="lastname" isSourceKey="false"/>
                    <AttrSoD type="duty" dutyType="ENTITLEMENT_TYPE"
name="accessorigid"  sourceIdMAttrName="ENTITLEMENT_NAME" isSourceKey="true"/>
```

```
        </DataTransformation>

        <DataTransformation>
         . . .
        </DataTransformation>

        <DataTransformation>
         . . .
        </DataTransformation>
    </ServiceComponent>
```

Apply the following guidelines while adding the SystemType and ServiceComponent elements in the registration.xml file

- Replace the placeholders with the following values:
  - SYSTEM_TYPE_NAME: Specify a name for the system type.
  - NAME_FOR_IMPLEMENTATION: Specify a name for the service component. For example: `DBToOAACG`
  - NAME_OF_IPMLEMENTATION_CLASS: Specify the name that you have set for the class that you create by performing the procedure described in Section 13.4.2, "Creating the Transformation Layer". For example: `oracle.iam.grc.sod.scomp.impl.oaacg.transformation.IdMvsSoDDataTransformationOperDBvsOAACG`
  - SoD_ENGINE: Enter `OAACG` if you are using Oracle Application Access Controls Governor as the SoD engine. Enter `GRC` if you are using SAP GRC as the SoD engine. If you are using a custom SIL provider, then enter the name that you set for that SoD engine.

    See Also: Section 13.5, "Creating SIL Providers"

  - SYSTEM_TYPE_NAME: Specify the system type name that you entered earlier.
  - NAME_OF_ATTRIBUTE_ON_TARGET_SYSTEM: Specify the name of the attribute on the target system.
  - NAME_OF_ATTRIBUTE_ON_SOD_ENGINE: Specify the name of the corresponding attribute on the SoD engine.
  - ENTITLEMENT_TYPE: Enter the type of entitlement. For example: `ROLE`
  - ENTITLEMENT_NAME: Enter the name of one instance of the entitlement. For example: `Resource Manager`
- Add one DataTransformation element for each attribute mapping that you want to create.

3. Save and close the registration.xml file.

13.4.4 Configuring the Provisioning and Approval Workflows for SoD

Note: Perform the procedure described in this section only if you are not using one of the preconfigured SoD-compatible connectors (Oracle e-Business User Management, SAP User Management, and SAP CUA).

This section discusses the following procedures:

- Section 13.4.4.1, "Modifying the Approval Workflow for SoD"
- Section 13.4.4.2, "Modifying the Provisioning Workflow for SoD"

13.4.4.1 Modifying the Approval Workflow for SoD

To modify the approval workflow for SoD validation:

> **See Also:** *Oracle Identity Manager Design Console Guide* for detailed information about this procedure

1. If parent and child object forms are not already available in the predefined connector for the target system, then you must create these object forms.

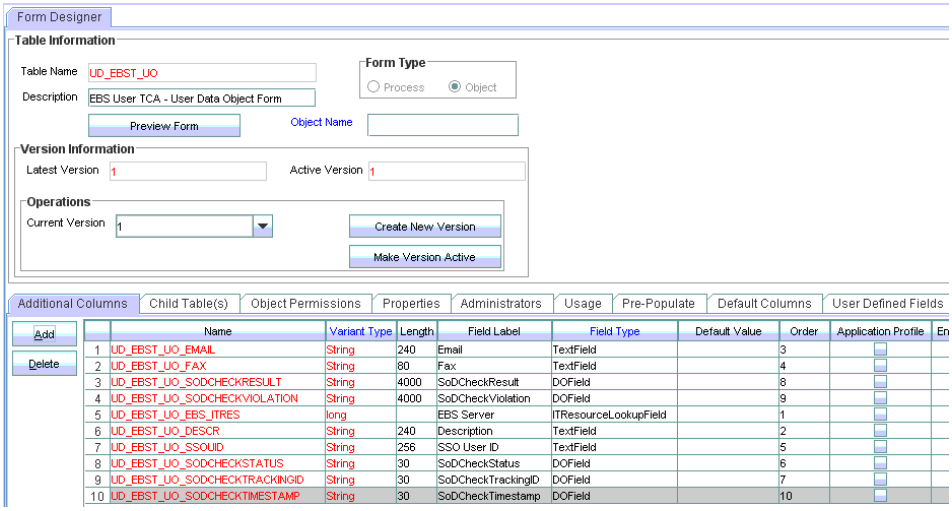
   > **Note:** The parent object form must contain a field of type ITResourceLookup that will point to the target system installation. The child forms must contain the entitlements.

2. Add the following text (string data type) fields on the parent object form:

   > **Note:** These fields must be made read-only fields. Only the SoD validation process adapter and scheduled task can modify them. During the SoD validation process, these fields hold the SoD validation process status and results returned by the SoD engine.

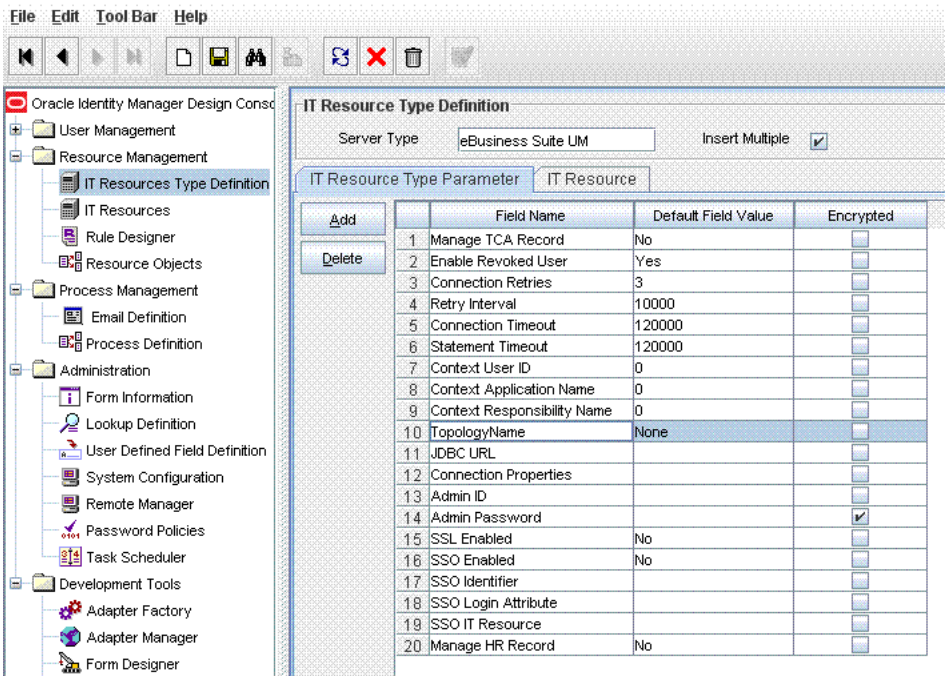
   - `SoDCheckStatus`: Valid values of this field are `SoDCheckNotInitiated`, `SoDCheckResultPending`, and `SoDCheckCompleted`. Set `SoDCheckNotInitiated` as the default value of this field.
   - `SoDCheckTrackingID`: The SoD framework library returns a string value for this when an SoD validation process is initiated. The value can be used later for polling SoD validation process results.
   - `SoDCheckResult`: The valid values of this field are `Passed` and `Failed`.
   - `SoDCheckTimestamp`: This field displays the date and time at which the SoD validation process results were generated.
   - `SoDCheckViolation`: This field displays policies in the SoD engine that are violated by the request and the corresponding entitlements. Set the length of this field to 4000 characters.

   The following screenshot shows an example of a parent object form:



3. In the IT resource of the connector, create the TopologyName parameter if it does not already exist.

The following screenshot shows a sample IT resource in which this parameter has been added:

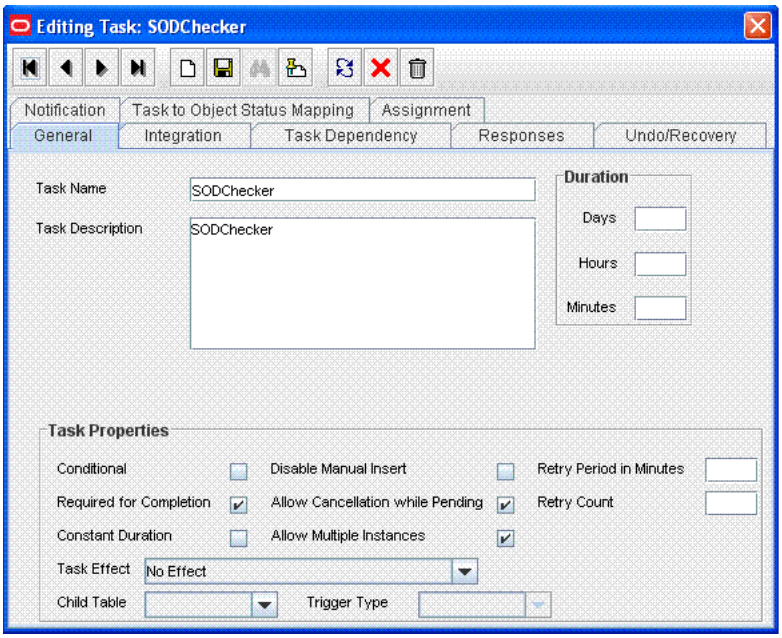


4. Modify the existing approval workflow or define an approval workflow.

Add the following process tasks to the approval workflow:

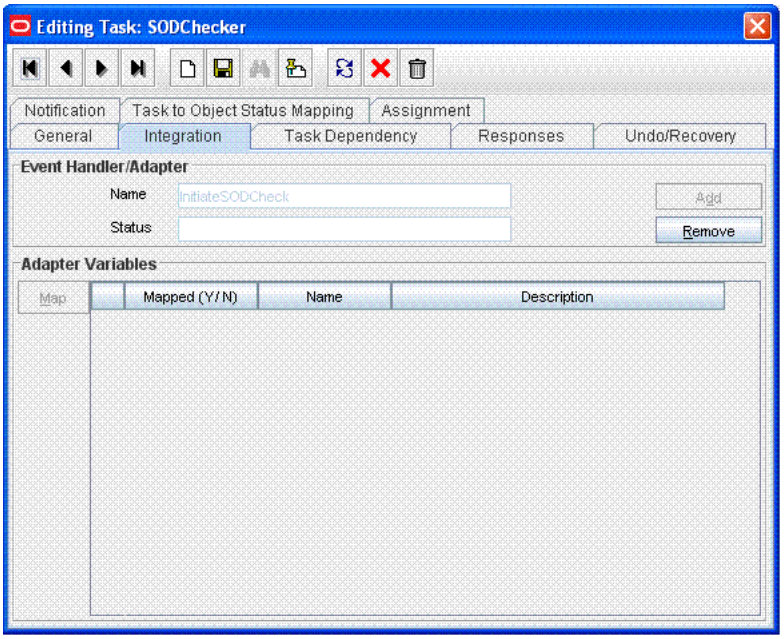
– Add a new task with a name starting with SODChecker (for example, SODChecker1). The task must be non-conditional and must be set to `Required for Completion`.

The following screenshot displays a sample SODChecker task:



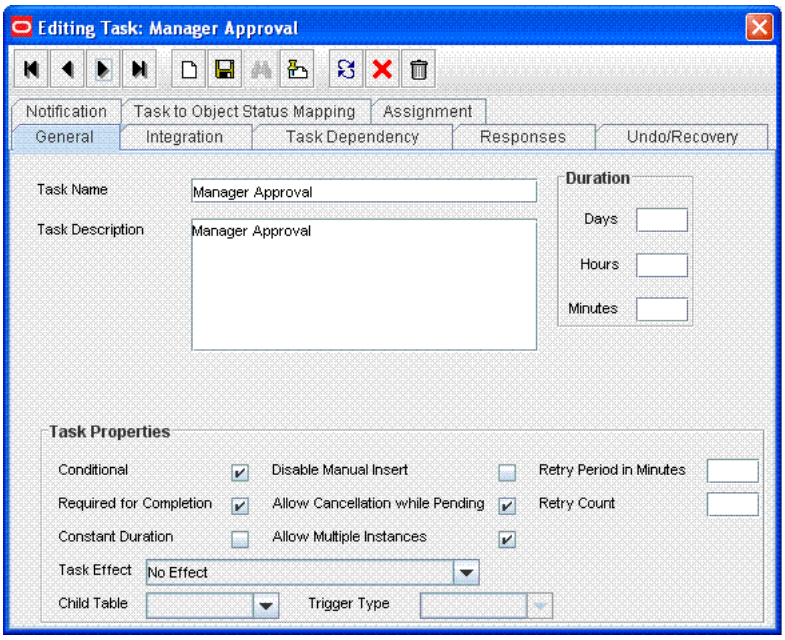
– Attach the InitiateSODCheck process task adapter to this task.

  This is shown in the following screenshot:

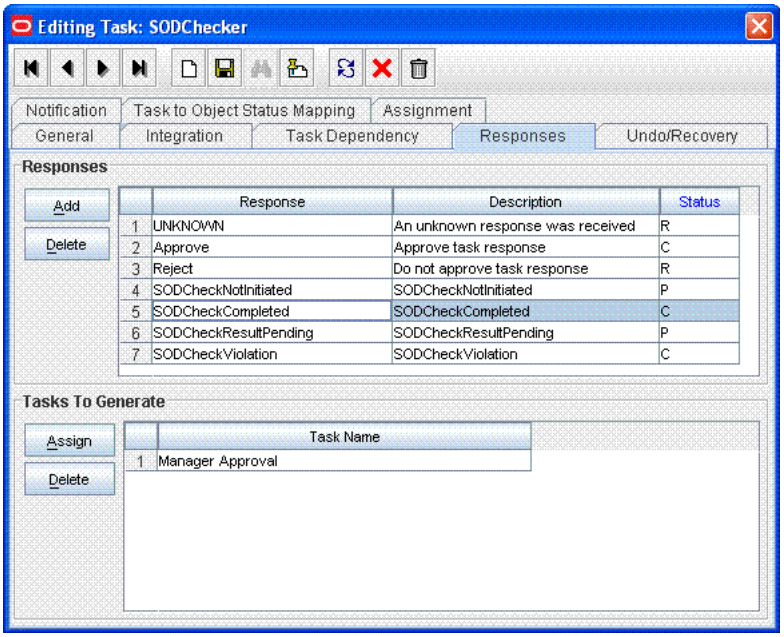


– Attach a human approval task to the workflow. This task must be conditional and marked as `Required for Completion`. The generation of this task will depend on the completion of the SODChecker task.

  The following screenshot shows the human approval task to the workflow:



In addition, the human approval task must be generated when the SODCheckCompleted response code is received. The following screenshot shows a Manager Approval task attached as a task to be generated on completion of the SODChecker task:



– Attach the following response codes to the SODChecker task:

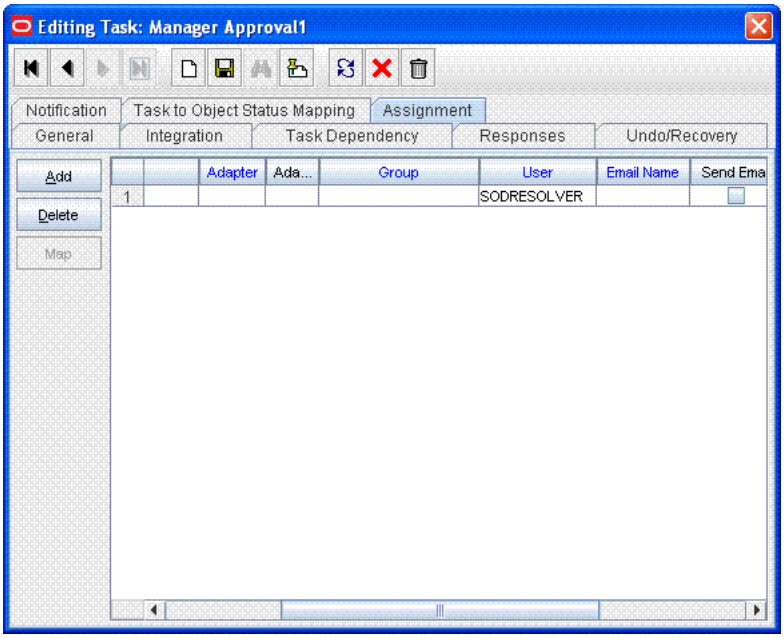
Response Code	Task Status	Description
SODCheckResultPending	P	The SoD validation process is initiated and results are awaited. **Note:** This response code is for an SoD engine that returns responses asynchronously.

Response Code	Task Status	Description
SODCheckCompleted	C	The SoD validation process results have been returned, and the response shows that there is no SoD violation.
SODCheckViolation	C	The SoD validation process results have been returned, and the response shows that there is an SoD violation.
SODCheckNotInitiated	C	The SoD validation process has not been initiated because SoD has not been enabled in Oracle Identity Manager.

– Add a human approval task (for example, Manager Approval1) similar to the one described earlier. Assign this task to a user (for example, SODResolver).

Note: The SODResolver user can be any user in your Oracle Identity Manager installation. You must ensure that the SODResolver user has permissions to modify the object form entitlement data. This can be achieved by adding the SODResolver user to a group that has read/write permissions on the object form.

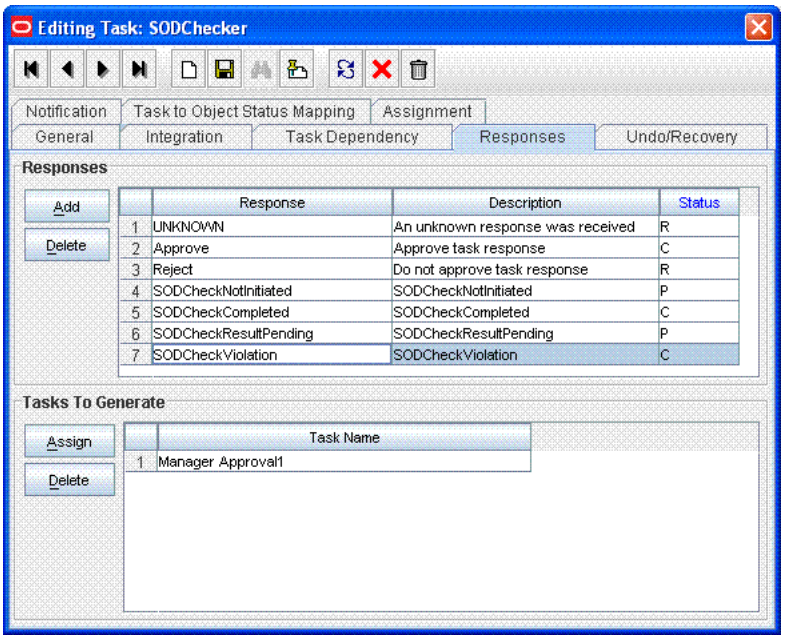
The following screenshot shows the second approval task assigned to the SODResolver user:



Note: Two approval tasks are required to enable the introduction of two separate approvers. Depending on the SoD validation process results, an approver can be selected.

– Attach the second approval task as a task to be generated in the event that an SoD validation process encounters a violation.

The following screenshot shows the second approval task attached as a task to be generated in the event that a violation is encountered:



According to this workflow, if the SoD validation process is successfully completed, then the system administrator is assigned the approval task. However, if a violation is encountered, then the approval task is assigned to the user identified by SODResolver. This user is expected to resolve the conflict by removing one of the conflicting entitlements.

Alternatively, in your operating environment, you might want to reject the provisioning request if a violation is encountered. This can be achieved by mapping the SODCheckViolation response code to the Cancelled (X) task status. In the event that a violation is encountered, the SODChecker task is canceled and provisioning does not proceed further.

5. The process task adapter attached to the SoDChecker task triggers the SoD validation process by calling the SoD Invocation Library (SIL) synchronous/asynchronous API.

Note: The registration of Oracle Identity Manager, SoD engine, and target system must be completed before any SIL call is triggered, because their reference IDs must be passed to the SIL APIs.

The adapter initiates one of the following forms of SoD analysis:

– Synchronous SoD Analysis

  The adapter immediately returns the results and SoDCheckStatus is set to `SoDCheckCompleted` in the parent object form. If there are no violations, then the adapter sets the SODChecker task to `Completed`. The SoDChecker can then approve the request. If there is a violation, then the `SODCheckViolation` response code is returned.

– Asynchronous SoD Analysis

  The adapter sets SoDCheckStatus to `SoDResultPending` in the parent object form and sets the task status to `Pending`. The adapter does not provide results in a single API call. You must run a scheduled task to call the SIL API for collecting results. This scheduled task looks for process tasks that are

awaiting approval, are of SoD Type (prefixed with `SODChecker`), and for which the corresponding `SoDCheckStatus` in the parent object form is `SoDResultPending`. For each such task, the scheduled task retrieves the tracking ID value and invokes the SoD framework library to retrieve SoD results. If the SoD result is available, the `SoDCheckStatus` is updated to `SoDCheckCompleted`. In addition, the `SoDCheckResult` and the `SoDCheckViolation` fields are updated appropriately with the returned values and the task is either completed or rejected based on the outcome.

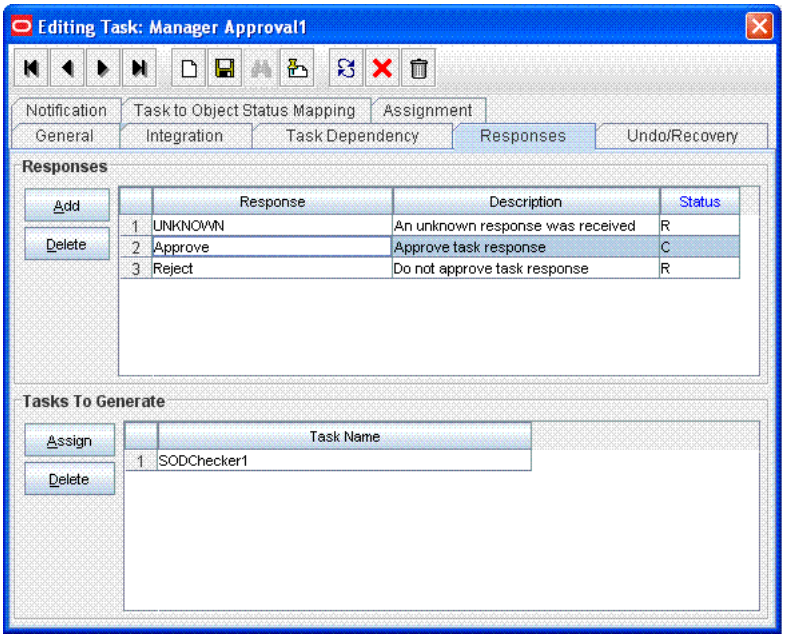
Multilevel Approval

A multilevel approval system may be required if you want to allow the first approver to modify entitlement data before granting approval. In this case, either the SODResolver user must be trusted to provide nonconflicting entitlements or SoD validation must be rerun after the SODResolver user has approved the request.

To implement multilevel approval:

1. Create a task whose name starts with SODChecker (for example SODChecker1), same as the SODChecker task that you created earlier. This task must be generated on completion of the Manager Approval1 task.

   The following screenshot shows a sample SODChecker task:



2. Attach an approval task (Manager Approval2) that is triggered on completion of SODChecker1. This is similar to the way in which the Manager Approval task is triggered on completion of SODChecker.

   In this case, there will be two tasks and two levels of approval:

   Note: The multilevel approval approach can be extended to any number of levels. However, the final approver must not modify the data.

   - **SODChecker:** Non-Conditional, Required for Completion, and attach InitiateSODCheck Adapter

Manager Approval: Conditional, Required for Completion, and generated on completion of SODChecker when the response code is `SODCheckCompleted`

Manager Approval1: Conditional, Required for Completion, and generated on completion of SODChecker when the response code is `SODCheckViolation`

- **SODChecker1:** Conditional, Required for Completion, and generated on completion of Manager Approval1

  Manager Approval2: Conditional, Required for Completion, and generated on completion of SODChecker1

13.4.4.2 Modifying the Provisioning Workflow for SoD

Each process definition has a process task attached to provision entitlements to a user. The SoD validation process must be performed before triggering this task and immediately after inserting *all* data in the child table that holds entitlements on the target system. Therefore, you must hold this process task until the SoD validation process is completed after inserting the data in child tables. To achieve this, you create a Holder task that precedes the provisioning of an entitlement to a user.

The Holder task is added to prevent provisioning of a resource to a user before the SoD validation process is completed. User entitlements are provisioned only if this task is complete. The task is completed when the SoD engine validates that SoD policies or rules are not violated by the assignment of the entitlements.

If an SoD validation process has been performed before human approval, then the SoD validation process need not be performed again even if the SoD validation process is enabled at the provisioning level. Whether the SoD validation process needs to be performed or not can be assessed by checking the following before the SoD validation process at the provisioning level:

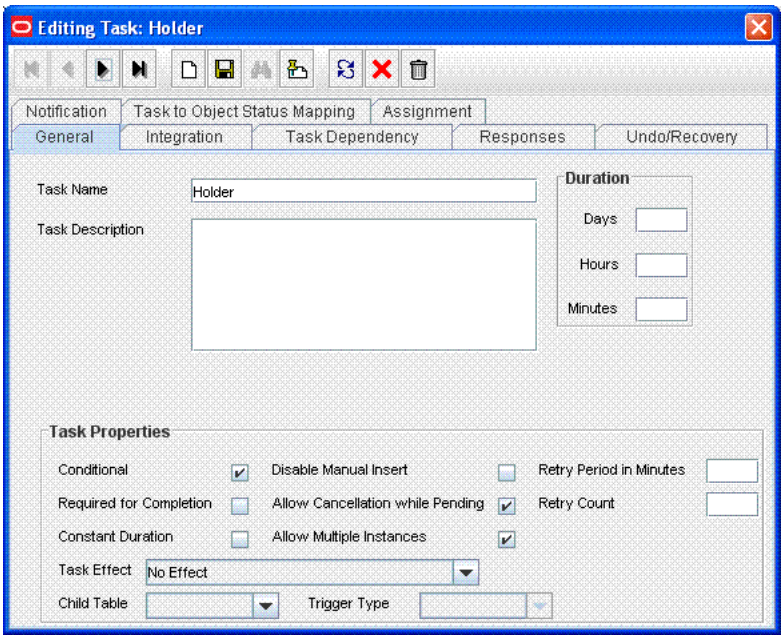
- Is the provisioning related to a request?
- If yes, is the SoDCheckStatus field set to `SoDCheckCompleted`?
- If yes, then do not perform the SoD validation process during entitlement provisioning.

> **Note:** The SoD validation process will be performed again only when the process child form is edited to add, update, or remove entitlements.

To modify the provisioning workflow for SoD validation:

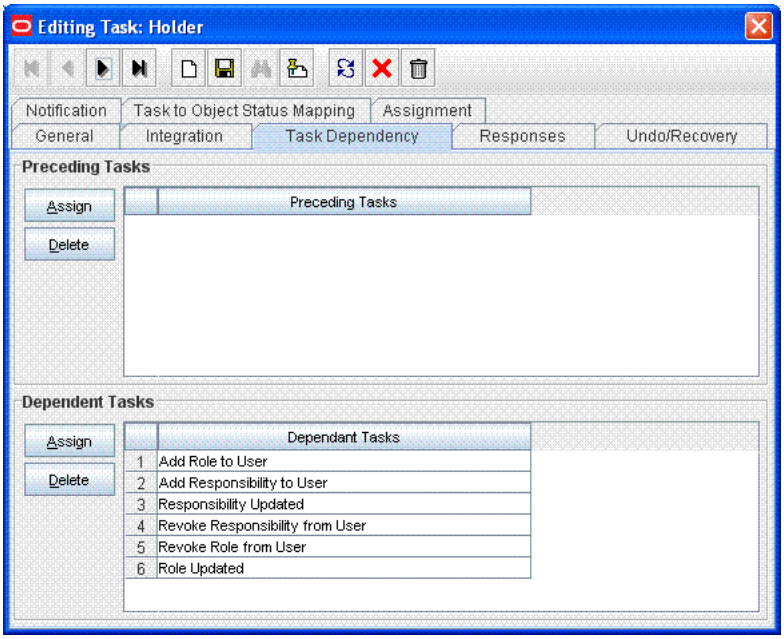
1. Add a Holder task to the provisioning workflow. This task must be made conditional and the Allow Multiple instances option must be selected.

   The following screenshot shows this Holder task:

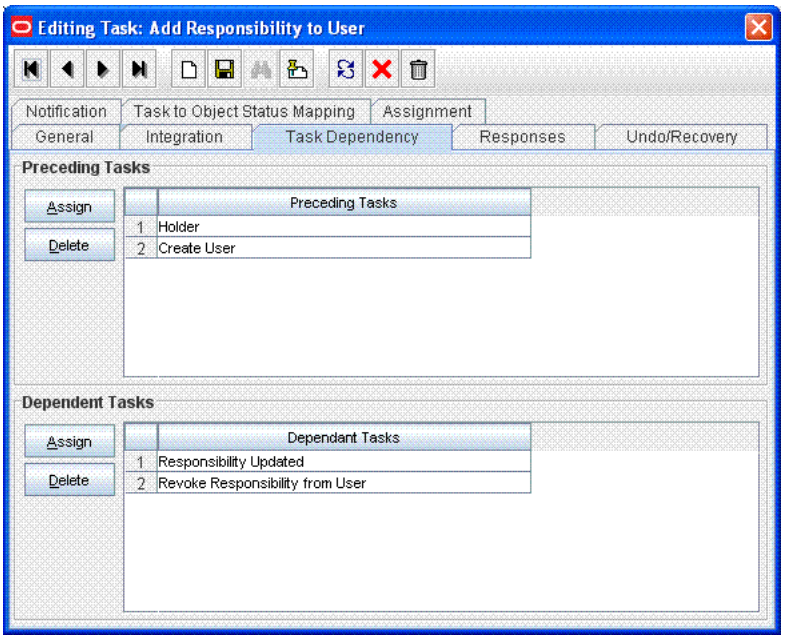


2. Make the connector insert, update, and revoke entitlement tasks dependent on the Holder task.

   The following screenshot shows all entitlement tasks of the Oracle e-Business User Management connector dependent on the Holder task:

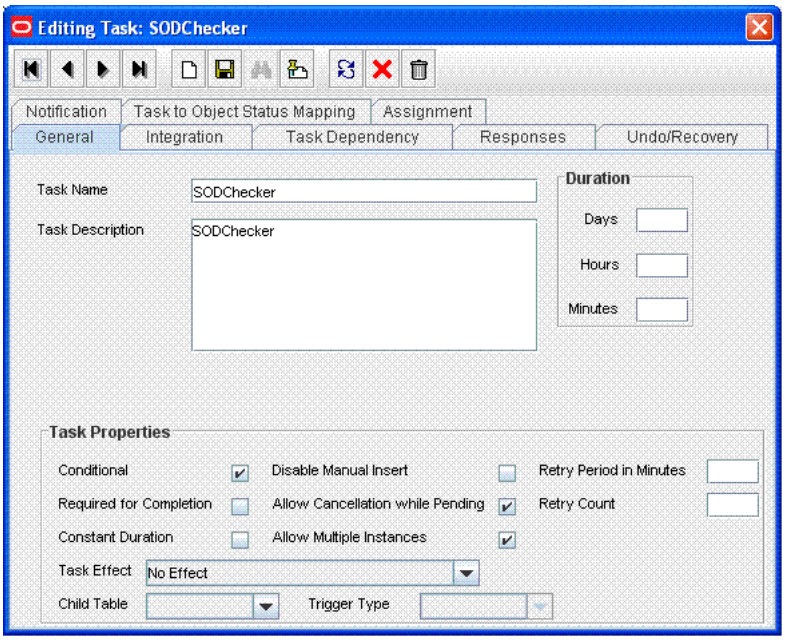


   The following screenshot shows the Holder task as a preceding task of the Add Responsibility to User task:



3. Add the SODChecker task (any task whose name starts with SODChecker). This task must be made conditional.

   The following screenshot shows the SODChecker task:



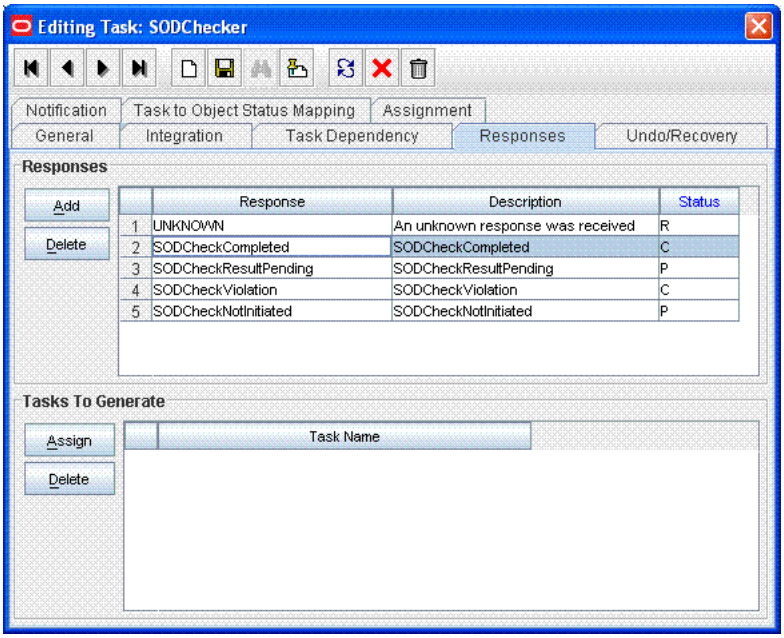
4. Attach the InitiateSODCheck process task adapter to the SoDChecker task.

   Attach the following response codes to the SODChecker task:

Response Code	Task Status	Description
SODCheckResultPending	P	The SoD validation process is initiated and results are awaited. **Note:** This response code is for an SoD engine that returns responses asynchronously.

Response Code	Task Status	Description
SODCheckCompleted	C	The SoD validation process results have been returned, and the response shows that there is no SoD violation.
SODCheckViolation	C	The SoD validation process results have been returned, and the response shows that there is an SoD violation.
SODCheckNotInitiated	C	The SoD validation process has not been initiated because SoD has not been enabled in Oracle Identity Manager.

The following screenshot shows these response codes:



13.4.5 Marking Child Process Form Tables That Hold Entitlement Data

Child process form tables can hold different types of multivalued data, for example, role data, profile data, and address information. You must mark the child process form tables holding entitlement data that you want to use for SoD operations. See Section 14.4, "Marking Entitlement Attributes on Child Process Forms" for information.

13.4.6 Registering the New Target System

To register the new target system, perform the procedure described in the following sections:

1. See Section 13.3.5.2, "Running the Registration Script and Providing Registration Information" for information on rerunning the registration script. In this run of the script, do not enter values for service components that have already been registered.
2. See Section 13.3.5.3, "Recording the Names of the System Types" for information on entering data about the new target system in the SILConfig.xml file.

13.5 Creating SIL Providers

Note:

Perform the procedure described in this section only if you want to use an SoD engine other than Oracle Application Access Controls Governor and SAP GRC. You must also perform the procedures given in Section 13.4, "Configuring Connectors for SoD" if you are using a target system other than Oracle e-Business Suite, SAP CUA, and SAP R3.

You must install the SoD engine before you begin creating the SIL provider.

You can perform this procedure either before or at any time after first-time implementation of SoD in Oracle Identity Manager.

The following is a summary of the procedure to create a SIL provider:

1. Follow instructions given in Section 13.5.1, "Addressing Prerequisites".
2. Create Java class implementations of the interfaces for the SIL provider. See Section 13.5.2, "Implementing the Interfaces for the Provider" for instructions.
3. Add entries in the registration XML file for the new SoD engine. See Section 13.5.3, "Modifying the Registration XML File for the New SoD Engine" for instructions.
4. Register the new SoD engine. See Section 13.5.4, "Registering the New SIL Provider" for instructions.

13.5.1 Addressing Prerequisites

Ensure that the following prerequisites are addressed:

1. Load entitlement data from the target system to the SOD engine. You can use any ETL utility to perform this step. For details, see vendor documentation for the SoD engine.
2. On the SoD engine, create policy definitions or risk definitions by using the data loaded from the target system.
3. Deploy the Oracle Identity Manager connector for the target system. See the connector documentation for more information.

13.5.2 Implementing the Interfaces for the Provider

Create Java implementations of the following service components:

See Also: The Javadocs shipped with this release of Oracle Identity Manager

- CallBackIdMOper
- SoDAnalysisExecutionOper
- SoDDataValidationOper

13.5.3 Modifying the Registration XML File for the New SoD Engine

Enter the details of the transformation layer in the registration.xml file as follows:

1. Open the registration.xml file in a text editor. This file is in the *SIL_HOME*/registrationXML directory.
2. Add a SystemType element for the SoD engine.

   See Also: The SystemType elements for Oracle Application Access Controls Governor and SAP GRC in the registration.xml file

3. Save and close the registration.xml file.

13.5.4 Registering the New SIL Provider

To register the new SIL provider, perform the procedure described in the following sections:

1. See Section 13.3.5.2, "Running the Registration Script and Providing Registration Information" for information on rerunning the registration script. In this run of the script, do not enter values for service components that have already been registered.
2. See Section 13.3.5.3, "Recording the Names of the System Types" for information on entering data about the new target system in the SILConfig.xml file.

14

Using Entitlement Data

An entitlement granted to an account on a target system enables the account owner (user) to perform a specific task or function. An entitlement can be a role, responsibility, or group membership. For example, if user Richard is granted the Inventory Analyst role on a target system, then Richard can use that entitlement to access and generate inventory-related reports from the target system.

In Oracle Identity Manager, there is one process form for each account (resource) provisioned to an OIM User. Entitlement data is stored in child process forms of the process form. In the example described earlier, the process form for Richard's account on the target system has a child process form that holds Inventory Manager role data.

Attributes that constitute entitlement data stored on a child process form may vary from one target system to another. In addition, different types of entitlements, such as roles and responsibilities, may have different attributes. For example, Target System A contains the following role data attributes:

- Role Name
- Role Description
- Start Date
- End Date

The same target system can have a different set of attributes for responsibility data:

- Responsibility ID
- Date Assigned
- Proxy User
- Escalation User

You can mark or highlight the attribute that uniquely identifies an entitlement on a target system. For the sample role and responsibility data attributes listed earlier, the Role Name and Responsibility ID attributes uniquely identify the role and responsibility entitlements on Target System A. By marking attributes that uniquely identify entitlements, you enable the capture of entitlement data that can be used by other identity management solutions and also displayed in reports.

This chapter discusses the following sections:

- Available Entitlements and Assigned Entitlements
- Entitlement Data Capture Process
- Configuring the Oracle Application Server Installation to Use This Feature
- Marking Entitlement Attributes on Child Process Forms

- Configuring Scheduled Tasks for Working with Entitlement Data
- Disabling the Capture of Modifications to Assigned Entitlements
- Entitlement-Related Reports
- Archiving Data Stored in the ENT_ASSIGN_HIST Table

14.1 Available Entitlements and Assigned Entitlements

A target system can have a set of entitlements defined and ready for assignment to accounts (users) on the target system. When you integrate this target system with Oracle Identity Manager, you can import (synchronize) entitlement data from the target system into the LKV table on Oracle Identity Manager.

Note: If you use a predefined connector to integrate the target system, then you can use scheduled tasks to fetch entitlement data into this table.

Entitlements in the LKV table are available for assignment to accounts. In this guide, these entitlements are called available entitlements.

During a provisioning operation, you select the entitlement that you want to assign from a lookup field on the child process form. In this guide, entitlements assigned to accounts are called assigned entitlements. Data about assigned entitlements is stored in child process form tables.

14.2 Entitlement Data Capture Process

After you mark the entitlement attribute in each child process form, the following processes take place:

- Capture of Data About Available Entitlements
- Capture of Data About Assigned Entitlements

14.2.1 Capture of Data About Available Entitlements

The following steps describe how data about available entitlements is captured:

Note: You must mark the entitlement attribute in each child process form to enable the process described in these steps. The procedure is described later in this chapter.

---

1. Data about available entitlements is stored in the LKV table through synchronization with the target system.
2. You schedule and run the Entitlement List scheduled task.
3. The scheduled task identifies the entitlement attribute from the UD_ tables.
4. The scheduled task copies data about available entitlements from the LKV table to the ENT_LIST table.

14.2.2 Capture of Data About Assigned Entitlements

This section describes how data about assigned entitlements is captured.

Note: You must mark the entitlement attribute in each child process form UD_ table to enable the process described in these steps. The procedure is described later in this chapter.

To perform first-time synchronization of assigned entitlements:

1. You schedule the Entitlement Assignments scheduled task to run once.
2. The scheduled task identifies the entitlement attribute from the child process form (UD_) tables.
3. The scheduled task creates INSERT, UPDATE, and DELETE triggers on each UD_ table.
4. The scheduled task copies data about assigned entitlements from the UD_ tables to the ENT_ASSIGN table.

Note: The ENT_ASSIGN table holds data about entitlement currently assigned to resources (users). When an entitlement is revoked, the record for that entitlement is moved out of this table to history data. Details are given in the "Entitlement Updations" section.

To perform incremental synchronization of assigned entitlements:

1. When a change is made to assigned entitlements through provisioning operations or reconciliation, the INSERT, UPDATE, or DELETE trigger copies the added, modified, or deleted row from the UD_ table to a staging table.
2. You configure and run the Entitlement Updations scheduled task.
3. For each record in the staging (ENT_ASSIGN_DELTA) table, the action taken by the scheduled task depends on the type of operation that was performed to the assigned entitlement:

Note: The type of operation (INSERT, UPDATE, or DELETE) is one of the data items stored in the staging table.

- **Event:** The entitlement was newly assigned to the account.

  Action: A new record is created (copied from the staging table) in the `ENT_ASSIGN` table.

- **Event:** An existing entitlement was modified.

  Action: The existing record is copied from the ENT_ASSIGN table into the ENT_ASSIGN_HIST table. The existing record is deleted from the ENT_ASSIGN table. A record corresponding to the newly modified entitlement is created in the ENT_ASSIGN table.

- **Event:** An existing entitlement was revoked.

  Action: The existing record is copied from the ENT_ASSIGN table into the ENT_ASSIGN_HIST table. The existing record is deleted from the ENT_ASSIGN table.

14.3 Configuring the Oracle Application Server Installation to Use This Feature

If your Oracle Identity Manager installation is running on Oracle Application Server and if you want to work with entitlement data, then:

1. In a text editor, open the opmn.xml file.
2. In this file, search for the following block of code:

```
<process-type id="home" module-id="OC4J" status="enabled">
     <module-data>
     <category id="start-parameters">
     <data id="oc4j-options" value="-userThreads"/>
     <data id="java-options"
value="-DXL.HomeDir=/home/testoc4j/OIM9102/xlserver/xellerate
-Dlog4j.configuration=file:/home/testoc4j/OIM9102/xlserver/xellerate/config/lo
g.properties -server -XX:PermSize=128M -XX:MaxPermSize=256M -ms512M -mx1024M
-XX:AppendRatio=3 -XX:AppendRatio=3
-Djava.security.policy=$ORACLE_HOME/j2ee/home/config/java2.policy
-Djava.awt.headless=true -Dhttp.webdir.enable=false"/>
</category>
```

3. Add the following line in this block of code as shown here:

```
<process-type id="home" module-id="OC4J" status="enabled">
     <module-data>
     <category id="start-parameters">
     <data id="oc4j-options" value="-userThreads"/>
     <data id="java-options"
value="-DXL.HomeDir=/home/testoc4j/OIM9102/xlserver/xellerate
-Dlog4j.configuration=file:/home/testoc4j/OIM9102/xlserver/xellerate/config/lo
g.properties -server -XX:PermSize=128M -XX:MaxPermSize=256M -ms512M -mx1024M
-XX:AppendRatio=3 -XX:AppendRatio=3
-Djava.security.policy=$ORACLE_HOME/j2ee/home/config/java2.policy
-Djava.awt.headless=true -Dhttp.webdir.enable=false"/>
<data id="oc4j-options" value="-userThreads"/>
</category>
```

4. Save and close the file.

14.4 Marking Entitlement Attributes on Child Process Forms

You must mark the entitlement attribute in the child process form UD_ table for resources for which you want to capture entitlement data. Suppose there are 15 target systems in your operating environment. If you want to capture entitlement data from 12 of 15 resources, then you must mark the entitlement attribute in those 12 resources.

Apply the following guidelines while performing the procedure described in this section:

- On a child process form, only one attribute holding entitlement data can be marked.
- The attribute that you mark must be of the LookupField type and its property must be one of the following:
  - Lookup code
  - Lookup query

    The Lookup query must satisfy the following conditions:

* The query uses the LKU and LKV tables
* The Lookup code in the query is from the LKU table
* The LKV_ENCODED column value is used for saving
* The LKV_DECODED column value is used for display purposes

To mark a field as an entitlement in a child process form:

1. Log in to the Design Console.
2. Expand **Development Tools**, and then double-click **Form Designer**.
3. Search for and open the child form on which you want to mark an entitlement.

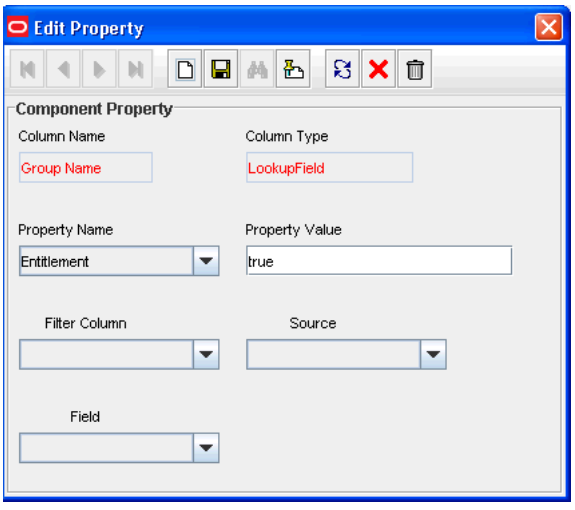
   For example, you might want to mark an entitlement on the UD_ADUSRC child form.
4. Click **Create New Version**.
5. Enter a label for the new version, click the Save icon, and then close the dialog box.
6. From the **Current Version** list, select the version that you create.
7. On the Properties tab, select the field that you want to mark as an entitlement and then click **Add Property**.
8. From the Property Name list in the Add Property dialog box, select **Entitlement**.

   Note: You can set Entitlement as the property of a field only if the column type is set to LookupField and the property name is set to Lookup Code.

9. In the **Property Value** field, enter `true`.

   You need not specify values for any of the other fields in the dialog box.

   The following screenshot shows the Edit Property dialog box for the lookup field:



10. Click the Save icon and then close the dialog box.
11. If you want to enable the capture of Start Date and End Date values for the entitlement, then:

Note: You can enable the capture of the Start Date and End Date values only if the column type for both fields is DateFieldDlg.

a. On the Properties tab, select the **Start Date** field and then click **Add Property**.

b. From the Property Name list in the Add Property dialog box, select **Entitlement Valid From**.

c. In the Property Value field, enter `true`.

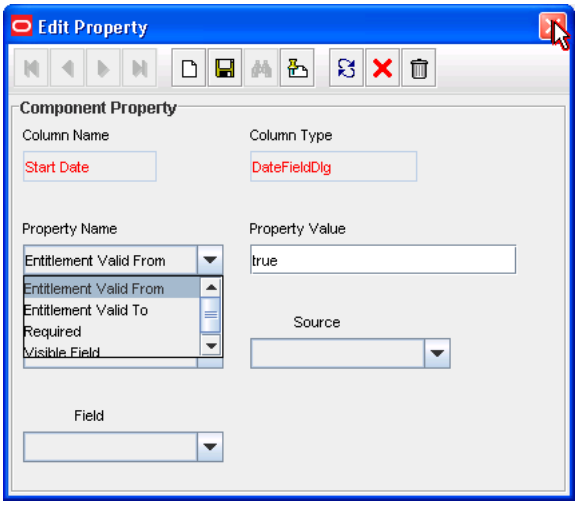
d. Click the Save icon and then close the dialog box.

e. On the Properties tab, select the **End Date** field and then click **Add Property**.

f. From the Property Name list in the Add Property dialog box, select **Entitlement Valid To**.

g. In the Property Value field, enter `true`.

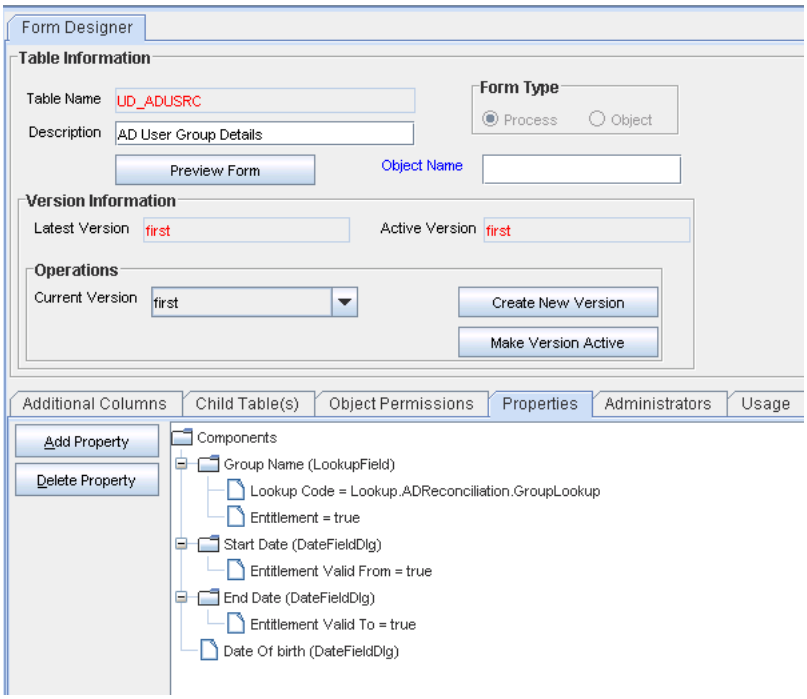
The following screenshot shows the Edit Property dialog box for the Start Date field:



h. Click the Save icon, and then close the dialog box.

12. Click the Save icon to save the changes made to the child process form.

The following screenshot shows the Properties tab of the child process form:



Note: Marking Start Date and End Date are optional.

13. Click **Make Version Active**.

14.5 Configuring Scheduled Tasks for Working with Entitlement Data

You configure the following scheduled tasks for working with entitlement data:

- Entitlement List
- Entitlement Assignments
- Entitlement Updations

14.5.1 Entitlement List

The Entitlement List scheduled task identifies the entitlement attribute from the child process form table and then copies entitlement data from the LKV table into the ENT_LIST table. A record created in the ENT_LIST table corresponds to an entitlement defined on a particular target system.

You must set a schedule for this task depending on how frequently new entitlements are defined on the target systems in your operating environment. In addition, you must run this scheduled task when new target systems are integrated with Oracle Identity Manager. In other words, you must run this task each time you mark a new entitlement. After the connector scheduled tasks fetch lookup field data from the target system into the LKV table, you can run the Entitlement List scheduled task to copy that entitlement data into the ENT_LIST table.

This scheduled task also handles updates to or deletion of entitlements from the target system. For example, if the Senior Accounts Analyst role is removed from the target system, then the connector scheduled task removes the entry for that role from the

LKV table. When the Entitlement List scheduled task is run, it marks the row containing the role in the ENT_LIST table as a deleted row.

14.5.2 Entitlement Assignments

The Entitlement Assignments scheduled task is used for copying data about assigned entitlements into the ENT_ASSIGN table for the first time. This task identifies the entitlement attribute from the child process form table, and then copies data about assigned entitlements from the child process form table into the ENT_ASSIGN table. A record created in the ENT_ASSIGN table corresponds to an entitlement assigned to a particular user on a particular target system.

In addition, it creates INSERT, UPDATE, and DELETE triggers on the child process form tables from which it copies entitlement data. See "Capture of Data About Assigned Entitlements" for information about the function of these triggers.

You can use the RECORDS_TO_PROCESS_IN_BATCH attribute of this scheduled task to specify the number of records in each batch. The default batch size is 5000.

You must run this scheduled task the first time you start using entitlement data and whenever you mark a new child process form field as an entitlement.

14.5.3 Entitlement Updations

The Entitlement Updations scheduled task updates the ENT_ASSIGN table with changes to entitlement assignment data in the child process form tables. Triggers created by the Entitlement Assignments scheduled task copy changes made to entitlement assignment data into a staging table. The Entitlement Updations scheduled task processes data in the staging table and makes the required changes to data in the ENT_ASSIGN table.

14.6 Disabling the Capture of Modifications to Assigned Entitlements

You can manually disable incremental synchronization of assigned entitlement data in the ENT_ASSIGN table. In other words, you can disable the capture of modifications to assigned entitlements. To achieve this, you create and run an SQL script to drop the following triggers created on the child process form tables:

Note: These triggers are created by the Entitlement Assignments scheduled task.

- The OIU_U_TRG trigger created on the OIU table
- The following triggers created on the UD_ tables:
  - *UD_TABLE_NAME*_I_TRG
  - *UD_TABLE_NAME*_D_TRG
  - *UD_TABLE_NAME*_U_TRG

After you run the script, modifications to assigned entitlements are not copied into the staging table.

14.7 Entitlement-Related Reports

The following predefined reports provide data about assigned entitlements:

Note:

You must be a member of the ADMINISTRATORS group to be able to view these reports.

Duplicate assignments of the same entitlement to a particular user are suppressed in the reports because they are not copied to the ENT_ tables. For example, if user John Doe has been assigned the Sales Superintendent role twice on a target system, then the reports show only one instance of this entitlement.

- Entitlement Access List
- Entitlement Access List History
- User Resource Entitlement
- User Resource Entitlement History

14.7.1 Entitlement Access List

The Entitlement Access List report lists users who are currently assigned the entitlements that you specify while generating the report. The report provides basic information about the entitlements and the list of users to whom the entitlements are assigned.

14.7.2 Entitlement Access List History

The Entitlement Access List History report lists users who had been assigned the entitlements that you specify while generating the report. The report provides basic information about the entitlements and the list of users to whom the entitlements were assigned.

14.7.3 User Resource Entitlement

The User Resource Entitlement report lists the current entitlements of users whom you specify while generating the report. The report displays basic user information and entitlement details.

14.7.4 User Resource Entitlement History

The User Resource Entitlement History report lists details of past entitlements assigned to users whom you specify while generating the report. The report displays basic user information and entitlement details.

14.8 Archiving Data Stored in the ENT_ASSIGN_HIST Table

Note: The utility described in this section can be used only if your Oracle Identity Manager installation is using Oracle Database.

Oracle Identity Manager does not automatically remove data from the ENT_ASSIGN_HIST table. Over a period of time, the gradual increase in the size of this table might have an adverse impact on the performance of the Oracle Identity

Manager database. You can use the Entitlement Archival utility to archive and remove data from the ENT_ASSIGN_HIST table.

Note: Data archived by the Entitlement Archival utility cannot be accessed by generating the reports listed in the "Entitlement-Related Reports" section.

The following sections describe the procedure to run the Entitlement Archival utility:

- Creating a Tablespace to Store Archived Entitlement Data
- Running the Entitlement Archival Utility

14.8.1 Creating a Tablespace to Store Archived Entitlement Data

Note: The procedure described in this section is a one-time activity. The tablespace that you create is used for all subsequent runs of the Entitlement Archival utility.

You must create a tablespace to store archived entitlement data. You can use the oim_archival_tablespace_setup.sql script to create the tablespace. This script is in the *OIM_HOME*/xellerate/db/oracle/Utilities/EntitlementArchival directory.

Note: The default size of the datafile created for the OIM_TASK_ARCH tablespace is 3 GB, which can hold approximately 1 million records. To meet your requirements, you might want to add more space to the default datafile of Oracle Identity Manager or create a datafile.

To create a tablespace in the Oracle Identity Manager database:

1. Connect to the Oracle Identity Manager database as SYSDBA.
2. Run the oim_archival_tablespace_setup.sql script.

   The script prompts for the following information:

   - Name (with complete path) of the datafile
   - User name of an Oracle Identity Manager database account: The utility uses this account for archive operations.

14.8.2 Running the Entitlement Archival Utility

Note: It is recommended that you run the Entitlement Archival utility outside business hours.

To run the Entitlement Archival utility:

1. Ensure that the Oracle Identity Manager database is available. In addition, verify that the Oracle Identity Manager database is not open for transactions with other sessions.

2. Create a backup of the ENT_ASSIGN_HIST table.
3. To check the last updated statistics of the active entitlement history table and their indexes, run the following query:

   SELECT table_name, last_analyzed FROM user_tables;

4. Stop Oracle Identity Manager.
5. On Linux and UNIX platforms, to set execution permission for the oim_Entitlement_archival.sh file and to ensure that the file is a valid Linux and UNIX text file:

   In a command window, switch to to the following directory:

   OIM_HOME/xellerate/db/oracle/Utilities/EntitlementArchival

   Run the following commands:

   ```
   chmod 755 FULL_PATH/oim_Entitlement_archival.sh
   dos2unix FULL_PATH/oim_Entitlement_archival.sh
   ```

6. On Linux and UNIX platforms, run the FULL_PATH/oim_Entitlement_archival.sh file.

   On Microsoft Windows platforms, run the FULL_PATH\oim_Entitlement_archival.bat file.

7. When you run the script, you are prompted for the following information:

   Oracle home

   Your response: Press the Enter key to accept the default Oracle home directory. Alternatively, provide the full path of the Oracle home directory.

   Oracle SID

   Your response: Enter y accept the default Oracle SID. Alternatively, provide the Oracle SID.

   Oracle port number

   Your response: Enter the port number at which Oracle Database is running.

   Database user password

   Your response: Enter the password of the database account that you create for the utility.

   Date in YYYYMMDD format

   Enter the end date limit for records that you want to archive. All tasks with dates equal to or earlier than the specified date are archived.

   Batch size

   Enter a batch size for the archive operation. The default batch size is 10000.

   Archive action

   Enter one of the following numbers:

   Enter 1 to archive and then purge entitlement data.

   Enter 2 to purge entitlement data without archiving it.

   Enter 3 to quit.

   At the end of the archive run, the Archival Complete message is displayed.

8. See the log file created in the following directory for information about the archive run:

   OIM_HOME/xellerate/db/oracle/Utilities/EntitlementArchival/logs_*YYYYMMDD_hhmi*

15

Bulk Load Utility

Oracle Identity Manager may be one among many repositories of user data in your organization. When you start using Oracle Identity Manager, you might want to load data from the other repositories into Oracle Identity Manager. The Bulk Load utility offers a solution to this requirement.

The Bulk Load utility is aimed at automating the process of loading a large amount of data into Oracle Identity Manager. It helps reduce the downtime involved in loading data. You can use this utility either immediately after you install Oracle Identity Manager or at any time during the production lifetime of Oracle Identity Manager.

The Bulk Load utility can use either CSV files or database tables as the source of data. Data imported into Oracle Identity Manager is automatically converted into OIM Users or accounts provisioned to OIM Users.

This document is divided into the following sections:

- Features of the Bulk Load Utility
- Installing the Bulk Load Utility
- Temporary Tables Used During a Bulk Load Operation
- Loading OIM User Data
- Loading Account Data

15.1 Features of the Bulk Load Utility

The following are features of the bulk load utility:

- The utility is compatible with Oracle Identity Manager release 9.1.0 and later.
- Data can be loaded into Oracle Identity Manager either as OIM Users or as accounts allocated (provisioned) to OIM Users.
- Data can be loaded from a single or multiple CSV files or a database table.

> **Note:** You cannot use the utility to load data into a remote Oracle Identity Manager database.

- Data can be loaded from a single or multiple trusted sources.
- Data can be loaded into either an empty Oracle Identity Manager repository or an Oracle Identity Manager repository that already contains data about OIM Users and resources. In other words, user data can be loaded at any time, either

immediately after Oracle Identity Manager installation or when the system is already in production.

- Exceptions generated during user data loading are handled, and records that fail the loading process can be retried.
- Audit snapshots can be generated after a bulk load operation.
- After bulk loading of OIM User data, password change at first login is enforced because a dummy password is used during the operation.

Note: You cannot use the utility to encrypt user attributes. In other words, if a user field in Oracle Identity Manager is encrypted, then the utility cannot be used to encrypt data that is loaded into that field.

15.2 Installing the Bulk Load Utility

To install the utility:

1. Copy the following directory from the installation package into a directory on the Oracle Identity Manager database host computer:

   InstallServer/Xellerate/db/oracle/Utilities/oimbulkload

   Note: You cannot use the utility to load data to a remote database.

2. Extract the contents of the ZIP file.

   The oimbulkload directory is created when you extract the contents of the ZIP file. The following directories are created inside this directory:

   - sqls: This directory contains SQL scripts used during bulk load operations.
   - scripts: This directory contains the .sh and .bat scripts used during bulk load operations.
   - csv_files: If you are going to use a single or multiple CSV files as the input source, then the CSV files must be stored in this directory.
   - lib: The directory contains the oimBulkLoad.jar and ojdbc5.jar files. These files are used by the utility during bulk load operations.

     Sample Data: This directory contains the following sample CSV files:

     – For OIM User load operations:

       master.txt

       OIDusers.csv

       HRusers.csv

     – For account load operations:

       parentAD.csv

       childAD.csv

   - Logs_ *YYYYMMDD_hhmi*: The log directory contains the log files that store the summary of the bulk load operation. This directory is created at run time.

The following sections provide additional information about the utility and bulk load operations:

- Scripts That Constitute the Utility
- Options Offered by the Utility

15.2.1 Scripts That Constitute the Utility

The following are the main scripts that constitute the utility:

- **oim_blkld.bat and oim_blkld.sh**

  This script contains the code to perform bulk load operations. When it is run, this script calls other scripts and stored procedures.

- **oim_blkld_setup.sql**

  This script is used to add a datafile in the Oracle Identity Manager tablespace. The "Creating a Datafile in the Oracle Identity Manager Tablespace" section of this document provides more information.

15.2.2 Options Offered by the Utility

When you run the bulk load utility, it prompts you to select one of the following options:

> **Note:** The utility prompts for more input depending on the option you select.

- Load User Data

  You select this option if you want the utility to load OIM User data. In other words, data is imported into the USR table of Oracle Identity Manager. In addition, you can select the input source, CSV files or database tables, for the data that you want to load.

- Load Account Data

  You select this option if you want the utility to load account data. In other words, data is imported into the relevant UD_ tables of Oracle Identity Manager. In addition, you can select the input source, CSV files or database tables, for the data that you want to load.

- Generate Audit Snapshot

  You select this option if you want the utility to generate an audit snapshot of data that you have loaded.

15.3 Temporary Tables Used During a Bulk Load Operation

The following temporary tables are used during a bulk load operation:

- **OIM_BLKLD_TMP_*SUFFIX***

  If you are using a CSV file as the input source, then the utility automatically creates the OIM_BLKLD_TMP_*SUFFIX* table and first loads data from the CSV file into this table. The suffix for the table name is determined as follows:

  - The first 6 characters of the file name are taken into account.
  - Special characters in the file name and the file extension (.csv) are ignored while determining the first 6 characters.

- A unique number is appended to the first 6 characters.
- For example, if the name of the file is acc_Data.csv, then the table that is created during the bulk load operation is named `oim_blkld_tmp_accDat1`.

If there are multiple CSV files, then one table is created for each file. Because the first six characters of each CSV file name are appended to the table name, you must ensure that the first six characters of each file's name are unique. This guideline is explained later in this document.

Note: if you are using a database table as the input source, then you can specify any name for the table. You provide the name of this table as one of the input parameters of the utility.

- **OIM_BLKLD_EX_*SUFFIX***

  The OIM_BLKLD_EX_*SUFFIX* table is used to hold data records that fail (are not loaded into Oracle Identity Manager) during a bulk load operation. One OIM_BLKLD_EX_SUFFIX table is created for each OIM_BLKLD_TMP_*SUFFIX* table. The EXCEPTION_MSG column of the table stores the reason for failure of each record in the table.

  If you are using CSV files as the input source, then the first six characters of the CSV file name are added as a suffix to the table name. For example, if the name of the CSV file is usrdt120508.csv, then the name of the table is OIM_BLKLD_EX_ usrdt1. If there are multiple CSV files, then one temporary table is created for each CSV file.

  Note: If there are multiple CSV files, then you must ensure that the first six characters of each CSV file name are unique.

- **OIM_BLKLD_LOG**

  During a bulk load operation, the utility inserts progress and error messages in the OIM_BLKLD_LOG table. You can query this table to monitor the progress of a bulk load operation. This procedure is described in detail later in this document.

15.4 Loading OIM User Data

The following is a summary of the steps involved in loading OIM User data:

1. If required, create a tablespace for the temporary tables used during the bulk load operation.
2. If required, create a datafile in the Oracle Identity Manager tablespace.
3. Create the OIM User whose password will be used as the default password for all OIM Users created during the bulk load operation.
4. Create the input source for the bulk load operation.

   If you want to use a database table as the input source, then create the table and copy user data into the table.

   If you want to use CSV files as the input source, then create the CSV files and copy user data into the files. In addition, create a master.txt file containing the names of the files in the sequence in which you want to load data from them.

5. Determine values for the input parameters of the utility.
6. Stop Oracle Identity Manager.
7. Run the oim_blkld script.
8. Monitor the progress of the bulk load operation.
9. Determine the outcome of the bulk load operation.
10. If required, reload data that was not loaded during the first run.
11. Restart Oracle Identity Manager.
12. Verify the outcome of the bulk load operation.
13. Gather performance data from the operation.
14. Remove temporary tables and files created during the operation.
15. Generate an audit snapshot.

The following sections provide detailed information about the steps involved in loading OIM User data:

- Creating a Tablespace for Temporary Tables
- Creating a Datafile in the Oracle Identity Manager Tablespace
- Setting a Default Password for OIM Users Added by the Utility
- Creating the Input Source for the Bulk Load Operation
- Determining Values for the Input Parameters of the Utility
- Running the Utility
- Monitoring the Progress of the Operation
- Handling Exceptions Recorded During the Operation
- Fixing Exceptions and Reloading Data Records
- Verifying the Outcome of the Bulk Load Operation
- Gathering Performance Data from the Bulk Load Operation
- Cleaning Up After a Bulk Load Operation
- Generating an Audit Snapshot

15.4.1 Creating a Tablespace for Temporary Tables

As mentioned in "Temporary Tables Used During a Bulk Load Operation", temporary database tables are used during the bulk load operation. It is recommended that you create a tablespace to accommodate these temporary tables instead of using the default tablespace of the Oracle Identity Manager database.

Follow the instructions in the database documentation to create a tablespace.

15.4.2 Creating a Datafile in the Oracle Identity Manager Tablespace

The default size of the datafile in the Oracle Identity Manager tablespace created during Oracle Identity Manager installation is 500 MB. You may need to add space to this datafile to accommodate the data that you are going to load. The alternative is to create a datafile.

To create a datafile in the Oracle Identity Manager tablespace:

1. Start a SQL*Plus session.
2. Connect to the Oracle Identity Manager database as SYSDBA.
3. Run the oim_blkld_setup.sql script. The script will prompt for the following:
   - Name of the Oracle Identity Manager tablespace
   - Full path and name for the datafile to be added in the Oracle Identity Manager tablespace
   - Oracle Identity Manager database user name

15.4.3 Setting a Default Password for OIM Users Added by the Utility

The utility does not encrypt passwords that it assigns to OIM Users created during the bulk load operation. Instead, it assigns the password of an existing OIM User to all OIM Users that are created during the operation.

Note: Each OIM User is required to change the password at first login.

When you run the utility, it prompts for the login name of the existing OIM User whose password you want to use as the default password for the new OIM Users. Before you run the utility, create this OIM User as follows:

> **See Also:** *Oracle Identity Manager Administrative and User Console Guide* for detailed information about creating OIM Users

1. Log in to the Oracle Identity Manager Administrative and User Console as a user with Create User privileges.
2. On the left navigation pane, click **Users** and then click **Create**.
3. Specify values for the following fields:
   - User ID
   - First Name
   - Last Name
   - Organization: Select **Xellerate Users**.
   - Password
   - Confirm Password
4. Click **Create User**.

15.4.4 Creating the Input Source for the Bulk Load Operation

Depending on the input source that you want to use, apply the guidelines given in one of the following sections:

- Using CSV Files As the Input Source
- Creating Database Tables As the Input Source

15.4.4.1 Using CSV Files As the Input Source

If you want to use CSV files as the input source for the bulk load operation, then apply the following guidelines while creating the CSV files:

- The CSV files must be placed in the oimbulkload/csv_files directory.
- The first line in the CSV file is called the control line. This line must contain a comma-separated list of column names of the USR table in the Oracle Identity Manager database.

  Note: Ensure that the Password column or any other encrypted column is not included in the list of columns. As mentioned earlier in this document, the utility assigns the password of an existing OIM User that you specify to all OIM Users that it loads into Oracle Identity Manager.

- From the second line onward, the file must contain values for the columns in the control line. The order of columns in the first line and the values in the rest of the lines must be the same.

  The following are sample contents of a CSV file:

```
USR_LOGIN,USR_FIRST_NAME,USR_LAST_NAME
john_doe, John, Doe
jane_doe, Jane, Doe
richard_roe, Richard, Roe
```

- If the value in any column contains a comma, then that value must be enclosed in double quotation marks (").
- The CSV file must contain values for all columns that are designated as mandatory in the USR table.
- Each row in the CSV file must have a unique value for the USR_LOGIN column in the USR table. If there are multiple files, you must ensure that USR_LOGIN values are unique across the CSV files. This check for uniqueness of USR_LOGIN values must also cover existing OIM Users in Oracle Identity Manager.

  Ensuring that USR_LOGIN values are unique can be a time-consuming exercise. As an alternative, you can first perform the bulk load operation, fix USR_LOGIN values that are not unique, and then retry the loading operation for the modified user records. This is possible because the utility checks for uniqueness of USR_LOGIN values at run time and copies records that fail this check into the OIM_BLKLD_EX table. Later in this document, there are instructions on retrying the bulk load operation for records that are not loaded during the first run.
- If you want to include an organization name in each user record, then add ORG_NAME in the control line and enter the organization name for each user from the second line onward.

  Note: All organization names listed under the ORG_NAME column in the CSV file must exist in Oracle Identity Manager.

- If you want to include a manager name in each user record, then add MANAGER_NAME in the control line and enter the USR_LOGIN value of the manager for each user from the second line onward.

The utility looks up the USR_LOGIN values for managers after all user data, from all CSV files, is loaded into Oracle Identity Manager. If a USR_LOGIN value given in the MANAGER_NAME column does not exist in Oracle Identity Manager, then the lookup for that user record fails and the record is copied into the exception table, OIM_BLKLD_EX. At the end of the bulk load operation, you can perform the procedure described in "Fixing Exceptions and Reloading Data Records" to reload user records that fail the first run.

- Note that the following default values are inserted into Oracle Identity Manager if the CSV file does not contain values for these columns:

  ORG_NAME: `Xellerate Users`

  USR_TYPE: `End-User`

  USR_STATUS: `Active`

  USR_EMP_TYPE: `Full-Time`

- Create a master TXT file containing the names of the CSV files containing user data to be loaded. You can specify any name for the file, for example, master.txt. Save the master file in the oimbulkload/csv_files directory.

  If you want to load multiple CSV files, then enter the name of each data CSV file on a separate line in the master file. Order the list of CSV file names in the sequence in which you want the utility to load data from the files. For example, suppose you have created three data CSV files, London_Users.csv, NewYork_Users.csv, and Tokyo_Users.csv. In the master file, you enter the names of the data CSV files in the following order:

  ```
  Tokyo_Users.csv
  London_Users.csv
  NewYork_Users.csv
  ```

  When you run the utility, data is loaded in this order.

15.4.4.2 Creating Database Tables As the Input Source

If you want to use a database table as the input source for loading OIM User data, then apply the following guidelines while creating the database table:

- Create the table in the Oracle Identity Manager database.
- The table must contain the following primary key column:

  OIM_BLKLD_USRSEQ NUMBER(19)

  The utility uses this column as the primary key. If required, you can use a database sequence to populate this column.

- The rest of the columns must be the same as the ones in the USR table that you want to use. In other words, ignore optional USR_ columns that you do not want to include in the table that you create.

  Note: The USR_LOGIN column is a mandatory column.

- Note that the following default values are inserted into Oracle Identity Manager if the table does not contain values for these columns:

  ORG_NAME: `Xellerate Users`

  USR_TYPE: `End-User`

USR_STATUS: `Active`

USR_EMP_TYPE: `Full-Time`

Table 15–1 shows the structure of a sample database table.

Table 15–1 Structure of a Sample Database Table

Name	Null?	Type
USR_LOGIN	NOT NULL	VARCHAR2(256)
USR_FIRST_NAME		VARCHAR2(80)
USR_LAST_NAME		VARCHAR2(80)
. . .	. . .	. . .
OIM_BLKLD_USRSEQ	NOT NULL	NUMBER(19)

15.4.5 Determining Values for the Input Parameters of the Utility

The following are input parameters of the utility:

- Oracle Home

  Value of the ORACLE_HOME environment variable on the host computer for the Oracle Identity Manager database

- Oracle SID

  SID of the Oracle Identity Manager database. In an Oracle RAC environment, you run the utility on one of the nodes. Provide the SID of that node.

- Port Number

  Port on which the Oracle Identity Manager database is running. In an Oracle RAC environment, you run the utility on one of the nodes. Provide the port number of that node.

- OIM DB User

  Database login ID of the Oracle Identity Manager database user

- OIM DB Pwd

  Password of the Oracle Identity Manager database user

- IP Address

  IP address of the computer on which you run the utility. In an Oracle RAC environment, you run the utility on one of the nodes. Provide the IP address of that node.

- Master file name

  Name of the file containing names of the CSV data files to be loaded

  This parameter is used only if the input source is a single or multiple CSV files. You place the master file and CSV data files in the oimbulkload/csv_files directory. See "Using CSV Files As the Input Source" for more information.

- Tmp table name

  Name of the temporary table to be used as the input source

  This parameter is used only if the input source for the bulk load operation is a database table. See "Creating Database Tables As the Input Source" for more information.

- Control Line

  Comma-separated list of names of columns to be loaded from the database table into Oracle Identity Manager

  This parameter is used only if the input source for the bulk load operation is a database table.

- Tablespace Name

  Name of the tablespace in which temporary tables are to be created during the bulk load operation

  See "Creating a Tablespace for Temporary Tables" for more information.

- Date format

  Date format used by date columns in the CSV files

  This parameter is used only if the input source is a single or multiple CSV files.

- Batch Size

  Number of user records that must be processed by the utility as a single transaction

  The batch size can influence the performance of the bulk load operation. The default value of this parameter is 10000.

- Debug Flag

  You can specify Y or N as the value of this parameter. If this parameter is set to Y, then the utility records detailed information about events that occur during the bulk load operation. See "Data Recorded During the Operation" for more information.

- User ID for default password

  Login name of the OIM User that you create by performing the procedure described in "Setting a Default Password for OIM Users Added by the Utility".

15.4.6 Running the Utility

> **Note:** If there are name conflicts with existing tables, then the utility overwrites existing temporary tables at the start of each run. If required, rename temporary database tables created during an earlier run of the utility.

To run the utility:

1. Stop Oracle Identity Manager.
2. Run one of the following scripts on the computer on which the Oracle Identity Manager database is configured:
   - On UNIX computers:

     OIMBulkload/script/oim_blkld.sh
   - On Microsoft Windows computers:

     OIMBulkload\script\oim_blkld.bat
3. From the main menu, select **Load User data**.

4. From the second menu:
   - Select **CSV File** if you are using CSV files as the input source.
   - Select **DB Table** if you are using a database table as the input source.
5. When prompted, provide values for the input parameters described earlier in this document.
6. Monitor the performance of the operation by following the steps given in "Monitoring the Progress of the Operation".

15.4.7 Monitoring the Progress of the Operation

The following sections provide information that you can apply to monitor the progress of the operation:

- Data Recorded During the Operation
- Querying the OIM_BLKLD_LOG Table for Progress and Error Messages

15.4.7.1 Data Recorded During the Operation

During the bulk load operation, the utility inserts progress and error messages in the OIM_BLKLD_LOG table. Data in this table is not deleted at the start of a new bulk load operation. One of the columns in this table holds the time stamp at which messages are recorded in the table.

Table 15–2 describes the structure of the OIM_BLKLD_LOG table.

Table 15–2 Structure of the OIM_BLKLD_LOG Table

Name	Null?	Type	Description
MSG_SEQ_NO	NOT NULL	NUMBER(19)	This column stores the number that denotes the order in which messages are inserted in this table. The column is populated using the OIM_BLKLD_LOG_SEQ sequence. You can use this column to query for messages in the order in which they are recorded in the table.
MODULE	NOT NULL	VARCHAR2(20)	This column stores one of the following values: USER: This value indicates that the message has been recorded while loading OIM User data. ACCOUNT: This value indicates that the message has been recorded while loading account data.
LOG_LEVEL	NOT NULL	VARCHAR2(20)	This column stores one of the following values: ERROR DEBUG PROGRESS_MSG

LOAD_SOURCE	NOT NULL	VARCHAR2(40)	This column indicates the source of data for the bulk load operation during which the row was inserted. The value can be one of the following:
			`CSV File: filename`
			`DB Table`

MSG	NOT NULL	VARCHAR2(4000)	This column stores a message corresponding to the value stored in the LOG_LEVEL column.

Table 15–2 (Cont.) Structure of the OIM_BLKLD_LOG Table

Name	Null?	Type	Description
CREATE_DATE		DATE	This column holds the time stamp at which the record was created. The format for entries in this column is as follows: yyyy/mm/dd hh24:mi:ss For example: 2008/06/23 21:49:16:32

15.4.7.2 Querying the OIM_BLKLD_LOG Table for Progress and Error Messages

During the bulk load operation, you can query the OIM_BLKLD_LOG table for information about the progress of the operation. For example, you can run the following query to see progress messages generated during the bulk load operation to load OIM User data:

```
SELECT MSG FROM OIM_BLKLD_LOG
WHERE MODULE = 'USER' AND LOG_LEVEL = 'PROGRESS_MSG'
ORDER BY MSG_SEQ_NO;
```

Errors encountered during the bulk load operation can be viewed by querying the OIM_BLKLD_LOG table. The following is an example of the query to retrieve error messages:

```
SELECT MSG FROM OIM_BLKLD_LOG
WHERE MODULE = 'USER' AND LOG_LEVEL = 'ERROR'
ORDER BY MSG_SEQ_NO;
```

15.4.8 Handling Exceptions Recorded During the Operation

At the end of a bulk load operation, the utility records statistics related to the operation in the following file:

oimbulkload/logs_*YYYYMMDD_hhmm*/oim_blkld_user_load_summary.log

To determine if there were exceptions during the operation, open this log file and look for the number against the Number of Records Rejected label. If the number of rejected records is greater than zero, then exceptions were thrown during the operation. User records that are rejected by the utility are recorded in the exception table (OIM_BLKLD_EX_*SUFFIX*). For each rejected record, the EXCEPTION_MSG column in the OIM_BLKLD_EX_*SUFFIX* table stores information about the reason the record could not be loaded.

Example 15–1 shows sample statistics recorded in the log file at the end of a bulk load operation to store OIM User data.

Example 15–1 Sample Log File Generated After Loading OIM User Data

```
**************************************************************

Processing File: u10.csv
==============================================================
U S E R   L O A D   S T A T I S T I C S   F O R   F I L E : u10.csv
==============================================================
Start Time:   08-AUG-08 11.44.12.228000 AM
End Time:     08-AUG-08 11.44.13.368000 AM
Number of Records Processed:  10
Number of Records Loaded:     8
Number of Records Rejected:   2
==============================================================
```

```
The name of the TMP table used during the load:
OIM_BLKLD_TMP_U101

The name of the Exception table used during the load:
OIM_BLKLD_EX_U101

*****************************************************************
Processing File: u10b.csv

=================================================================
U S E R    L O A D    S T A T I S T I C S    F O R    F I L E : u10b.csv
=================================================================
Start Time:   08-AUG-08 11.44.15.368000 AM
End Time:     08-AUG-08 11.44.15.540000 AM
Number of Records Processed:  16
Number of Records Loaded:     15
Number of Records Rejected:   1
=================================================================
The name of the TMP table used during the load:
OIM_BLKLD_TMP_U10B2

The name of the Exception table used during the load:
OIM_BLKLD_EX_U10B2
=================================================================

=================================================================
Time taken in re-building indexes and enabling FK constraints
=================================================================
Start time:      08-AUG-08 11.44.15.556000 AM
End Time:        08-AUG-08 11.46.50.586000 AM
=================================================================
```

In this sample, the number of rejected records is 2. If the log file shows that any records were rejected by the utility, then see "Fixing Exceptions and Reloading Data Records" for information about retrying the load operation for these records.

> **Note:** At the end of each bulk load operation, it is recommended that you create a backup of the exception tables.

15.4.9 Fixing Exceptions and Reloading Data Records

As mentioned earlier, errors encountered during the bulk load operation can be viewed by querying the OIM_BLKLD_LOG table. The following is an example of the query to retrieve error messages:

```
SELECT MSG FROM OIM_BLKLD_LOG
WHERE MODULE = 'USER' AND LOG_LEVEL = 'ERROR'
ORDER BY MSG_SEQ_NO;
```

An exception table OIM_BLKLD_EX_*SUFFIX* is created for each data table used as the input source during the bulk load operation. Records that do not meet the criteria for the operation are copied into this exception table. The suffix appended to the name of each exception table is the same as suffix appended to the name of the corresponding data table.

To reload rejected records:

1. Create a backup of the exception table in which rejected records are stored.

Note: Although this is an optional step, it is recommended that you create a backup.

2. Review each record in the exception table, and fix errors in the data based on the message recorded in the EXCEPTION_MSG column.
3. After you fix errors in all the rejected records in an exception table, rename the table to OIM_BLKLD_TMP_*SUFFIX* and then use it as the input source.
4. Load records from the OIM_BLKLD_TMP_*SUFFIX* table by running the utility. See "Running the Utility" for more information.
5. Repeat Steps 1 through 4 until the Number of Records Rejected label in the oim_blkld_account_load_summary.log file shows the value 0.
6. Restart Oracle Identity Manager.

15.4.10 Verifying the Outcome of the Bulk Load Operation

To verify the outcome of the bulk load operation, check if you are able to perform the following steps for one of the OIM User added by the utility:

See Also: *Oracle Identity Manager Administrative and User Console Guide* for detailed information about these procedures

- Log in as the OIM User. The system should prompt you to change the password.
- Provision a resource for the OIM User.
- Add the OIM User to a group.
- Modify the account profile of the OIM User.
- Revoked the resource provisioned to the OIM User.
- Unassign the OIM User from the group to which the user was added earlier.
- Modify the account profile again to restore the profile to its original state.
- Check if the User Resource Access report (an operational report) and the User Resource Access History report can be generated for the user.
- Create an Attestation and check its status using the Diagnostic Dashboard.

15.4.11 Gathering Performance Data from the Bulk Load Operation

As mentioned earlier in this document, the following log file is created during the bulk load operation:

oimbulkload/logs_*YYYYMMDD_hhmm*/oim_blkld_account_load_summary.log

Data recorded in this file can be used to collate performance-related information about the bulk load operation. The following information can be collected after the bulk load operation:

- Start time
- Input source
- Number of records in the system before the load
- Number of records successfully loaded

- Number of records rejected
- Total time taken

You can use this information during future runs of the utility. If you want to retain information about the bulk load operation, then move this file to a permanent location.

15.4.12 Cleaning Up After a Bulk Load Operation

If you do not want to save the results of a bulk load operation, then:

- Remove the OIM_BLKLD_TMP_*SUFFIX*, OIM_BLKLD_EX_*SUFFIX*, and OIM_BLKLD_LOG tables.
- Remove any files that you created or used during the operation.
- If you created a tablespace for the operation, then remove the tablespace.
- See "Gathering Performance Data from the Bulk Load Operation" before you remove log files created in the logs_*timestamp* directory.

> **Note:** At this point, you can restart Oracle Identity Manager if you have not already done so.

15.4.13 Generating an Audit Snapshot

If required, you can generate an audit snapshot of Oracle Identity Manager data after a bulk load operation. The utility uses the audit utility shipped with Oracle Identity Manager release 9.1.0. Internally, the GenerateSnapshot script is called when you run the audit utility. Similarly, the GenerateSnapshot script is called when you select the option to generate an audit snapshot.

> **Note:** Oracle Identity Manager must be up and running when you run the audit utility.

Before you generate an audit snapshot:

1. Open the *OIM_HOME*/bin/GenerateSnapshot.sh (or GenerateSnapshot.bat) file in a text editor.
2. In this file, search for the following line:
   - In the GenerateSnapshot.bat file:

     SET XEL_HOME=..
   - In the GenerateSnapshot.sh file:

     XEL_HOME=..
3. Replace this line with the following line:
   - In the GenerateSnapshot.bat file:

     SET XEL_HOME=<*Full path of the OIM_HOME directory*>
   - In the GenerateSnapshot.sh file:

     XEL_HOME=<*Full path of the OIM_HOME directory*>
4. Save and close the file.

See *Oracle Identity Manager Audit Report Developer's Guide* for information about the procedure to generate audit snapshots.

15.5 Loading Account Data

The following is a summary of the steps involved in loading account data:

1. If required, create a tablespace for the temporary tables used during the bulk load operation.
2. If required, create a datafile in the Oracle Identity Manager tablespace.
3. Create the input source for the bulk load operation.

   If you want to use a database table as the input source, then create the table and copy account data into the table.

   If you want to use CSV files as the input source, then create the CSV files and copy account data into the files.
4. Determine values for the input parameters of the utility.
5. Stop Oracle Identity Manager.
6. Run the oim_blkld script.
7. Monitor the progress of the bulk load operation.
8. Determine the outcome of the bulk load operation.
9. If required, reload data that was not loaded during the first run.
10. Restart Oracle Identity Manager.
11. Verify the outcome of the bulk load operation.
12. Gather performance data from the operation.
13. Remove temporary tables and files created during the operation.
14. Generate an audit snapshot.

Requirements and Features of the Bulk Load Operation for Account Data

The following are requirements and features of the bulk load operation for account data:

- Reconciliation must be set up and you should be able to test reconciliation by importing a few accounts from the target system.
- Only accounts for which there are corresponding OIM Users can be loaded.
- A target system that requires multiple IT resources is not supported.
- Duplicate accounts cannot be detected during a bulk load operation. If there are multiple entries for the same account in the input source, then multiple accounts are created for the corresponding OIM User.
- For a particular target system, if there are multiple provisioning processes/process forms in Oracle Identity Manager, then the utility uses the default provisioning process for the resource object.
- Information about the stage up to which earlier bulk load operations progressed is not stored. In other words, the utility cannot resume a bulk load operation. You must backup the Oracle Identity Manager database before a bulk load operation. If you want to retry a bulk load operation, you must first restore the database and then rerun the procedure.

The following sections provide detailed information about the steps involved in loading account data:

- Creating a Tablespace for Temporary Tables
- Creating a Datafile in the Oracle Identity Manager Tablespace
- Creating the Input Source for the Bulk Load Operation
- Determining Values for the Input Parameters of the Utility
- Running the Utility
- Monitoring the Progress of the Operation
- Handling Exceptions Recorded During the Operation
- Fixing Exceptions and Reloading Data Records
- Verifying the Outcome of the Bulk Load Operation
- Gathering Performance Data from the Bulk Load Operation
- Cleaning Up After a Bulk Load Operation
- Generating an Audit Snapshot

15.5.1 Creating a Tablespace for Temporary Tables

As mentioned in "Temporary Tables Used During a Bulk Load Operation", temporary database tables are used during the bulk load operation. It is recommended that you create a tablespace to accommodate these temporary tables instead of using the default tablespace of the Oracle Identity Manager database.

Follow the instructions in the database documentation to create a tablespace.

15.5.2 Creating a Datafile in the Oracle Identity Manager Tablespace

The default size of the datafile in the Oracle Identity Manager tablespace created during Oracle Identity Manager installation is 500 MB. You may need to add space to this datafile to accommodate the data that you are going to load. The alternative is to create a datafile.

To create a datafile in the Oracle Identity Manager tablespace:

1. Start a SQL*Plus session.
2. Connect to the Oracle Identity Manager database as SYSDBA.
3. Run the oim_blkld_setup.sql script. The script will prompt for the following:
   - Name of the Oracle Identity Manager tablespace
   - Full path and name for the datafile to be added in the Oracle Identity Manager tablespace
   - Oracle Identity Manager database user name

15.5.3 Creating the Input Source for the Bulk Load Operation

Depending on the input source that you want to use, apply the guidelines given in one of the following sections:

- Using CSV Files As the Input Source
- Creating Database Tables As the Input Source

15.5.3.1 Using CSV Files As the Input Source

If you want to use CSV files as the input source for the bulk load operation, then apply the following guidelines while creating the CSV files:

- The CSV files must be placed in the oimbulkload/csv_files directory.
- The first line in the CSV file is called the control line. This line must contain a comma-separated list of column names in the account (UD_*) table into which you want to load the account data.

  Note: Ensure that the Password column or any other encrypted column is not included in the list of columns.

- From the second line onward, the file must contain values for the columns in the control line. The order of columns in the first line and the values in the rest of the lines must be the same.
- If the value in any column contains a comma, then that value must be enclosed in double quotation marks (").
- The CSV file must contain values for all columns that are designated as mandatory in the account table.
- If you want to load account data into parent and child tables, then you must create one parent CSV file and one child CSV file for each child table. For example if you are loading data into one parent table and three child tables, then you must create one parent CSV file and three child CSV files.
- If you want to load account data into parent and child tables, then at least one column must be the same in both tables. This column corresponds to the link attribute between the parent and child CSV files. The following example illustrates this:

  The following are sample contents of a parent CSV file:

```
UD_ADUSER_UID,UD_ADUSER_ORGNAME,UD_ADUSER_FNAME,UD_ADUSER_LNAME,UD_ADUSER_MNAME
,UD_ADUSER_FULLNAME
jdoe,Finance,John,Doe,M,John M Doe
rroe,Accounting,Richard,Roe,,Richard Roe
```

  The following are sample contents of a child CSV file:

```
UD_ADUSER_UID,UD_ADUSRC_GROUPNAME
jdoe,group1
jdoe,group2
jdoe,group3
rroe,group1
rroe,group2
```

  The UD_ADUSER_UID column is common to both the parent file and the child file.

15.5.3.2 Creating Database Tables As the Input Source

If you want to use a database table as the input source for loading account data, then apply the following guidelines while creating the database table:

- Create the table in the Oracle Identity Manager database.
- The table must contain the following primary key column:

OIM_BLKLD_USRSEQ NUMBER(19)

The utility uses this column as the primary key. If required, you can use a database sequence to populate this column.

- The rest of the columns must be the same as the ones in the account (UD_) table that you want to use. In other words, ignore optional UD_ columns that you do not want to include in the table that you create.

Table 15–3 shows the structure of a sample parent table.

Table 15–3 Structure of a Sample Database Table

Name	Null?	Type
UD_ADUSER_UID		VARCHAR2(20)
UD_ADUSER_ORGNAME		VARCHAR2(256)
UD_ADUSER_FNAME		VARCHAR2(80)
UD_ADUSER_LNAME		VARCHAR2(80)
UD_ADUSER_MNAME		VARCHAR2(80)
UD_ADUSER_FULLNAME		VARCHAR2(240)
OIM_BLKLD_SEQ	NOT NULL	NUMBER(19)

Table 15–4 shows the structure of a sample child table.

Table 15–4 Structure of a Sample Child Database Table

Name	Null?	Type
UD_ADUSER_UID		VARCHAR2(20)
UD_ADUSER_ORGNAME		VARCHAR2(256)
UD_ADUSRC_GROUPNAME		VARCHAR2(32)
OIM_BLKLD_SEQ	NOT NULL	NUMBER(19)

15.5.4 Determining Values for the Input Parameters of the Utility

The following are input parameters of the utility:

- Oracle Home

  Value of the ORACLE_HOME environment variable on the host computer for the Oracle Identity Manager database

- Oracle SID

  SID of the Oracle Identity Manager database. In an Oracle RAC environment, you run the utility on one of the nodes. Provide the SID of that node.

- Port Number

  Port on which the Oracle Identity Manager database is running. In an Oracle RAC environment, you run the utility on one of the nodes. Provide the port number of that node.

- OIM DB User

  Database login ID of the Oracle Identity Manager database user

- OIM DB Pwd

Password of the Oracle Identity Manager database user

- IP Address

  IP address of the computer on which you run the utility. In an Oracle RAC environment, you run the utility on one of the nodes. Provide the IP address of that node.

- Object name (OBJ_NAME)

  Name of the resource object corresponding to the account data to be loaded

- CSV file names

  Names of the CSV files to be used as the input source

  This parameter is used only if the input source is CSV files. See "Using CSV Files As the Input Source" for more information. If you are loading data from parent and child CSV file, then use a comma-delimited list to enter the names of the files. The name of the parent CSV file must be provided first, and it must be followed by the names of the child CSV files.

- Tmp table name

  Name of the temporary table to be used as the input source

  This parameter is used only if the input source for the bulk load operation is a database table. See "Creating Database Tables As the Input Source" for more information.

- Control Line

  Comma-separated list of names of columns to be loaded from the database table into Oracle Identity Manager

  This parameter is used only if the input source for the bulk load operation is a database table.

- Tablespace Name

  Name of the tablespace in which temporary tables are to be created during the bulk load operation

  See "Creating a Tablespace for Temporary Tables" for more information.

- Date format

  Date format used by date columns in the CSV files

  This parameter is used only if the input source is a single or multiple CSV files.

- Batch Size

  Number of user records that must be processed by the utility as a single transaction

  The batch size can influence the performance of the bulk load operation. The default value of this parameter is 10000.

- Debug Flag

  You can specify Y or N as the value of this parameter. If this parameter is set to Y, then the utility records detailed information about events that occur during the bulk load operation. See "Data Recorded During the Operation" for more information.

- IT Resource Name

Name of the IT resource created for the target system

15.5.5 Running the Utility

Note: If there are name conflicts with existing tables, then the utility overwrites existing temporary tables at the start of each run. If required, rename temporary database tables created during an earlier run of the utility.

To run the utility:

1. Stop Oracle Identity Manager.
2. Run one of the following scripts on the computer on which the Oracle Identity Manager database is configured:
   - On UNIX computers:

     OIMBulkload/script/oim_blkld.sh
   - On Microsoft Windows computers:

     OIMBulkload\script\oim_blkld.bat
3. From the main menu, select **Load User data**.
4. From the second menu:
   - Select **CSV File** if you are using CSV files as the input source.
   - Select **DB Table** if you are using a database table as the input source.
5. When prompted, provide values for the input parameters described earlier in this document.
6. Monitor the performance of the operation by following the steps given in "Monitoring the Progress of the Operation".

15.5.6 Monitoring the Progress of the Operation

The following sections provide information that you can apply to monitor the progress of the operation:

- Data Recorded During the Operation
- Querying the OIM_BLKLD_LOG Table for Progress and Error Messages

15.5.6.1 Data Recorded During the Operation

During the bulk load operation, the utility inserts progress and error messages in the OIM_BLKLD_LOG table. Data in this table is not deleted at the start of a new bulk load operation. One of the columns in this table holds the time stamp at which messages are recorded in the table.

Table 15–5 describes the structure of the OIM_BLKLD_LOG table.

Table 15–5 Structure of the OIM_BLKLD_LOG Table

Name	Null?	Type	Description
MSG_SEQ_NO	NOT NULL	NUMBER(19)	This column stores the number that denotes the order in which messages are inserted in this table. The column is populated using the OIM_BLKLD_LOG_SEQ sequence. You can use this column to query for messages in the order in which they are recorded in the table.
MODULE	NOT NULL	VARCHAR2(20)	This column stores one of the following values: USER: This value indicates that the message has been recorded while loading OIM User data. ACCOUNT: This value indicates that the message has been recorded while loading account data.
LOG_LEVEL	NOT NULL	VARCHAR2(20)	This column stores one of the following values: ERROR DEBUG PROGRESS_MSG
LOAD_SOURCE	NOT NULL	VARCHAR2(40)	This column indicates the source of data for the bulk load operation during which the row was inserted. The value can be one of the following: CSV File: <filename> DB Table
MSG	NOT NULL	VARCHAR2(4000)	This column stores a message corresponding to the value stored in the LOG_LEVEL column.
CREATE_DATE		DATE	This column holds the time stamp at which the record was created. The format for entries in this column is as follows: yyyy/mm/dd hh24:mi:ss For example: 2008/06/23 21:49:16:32

15.5.6.2 Querying the OIM_BLKLD_LOG Table for Progress and Error Messages

During the bulk load operation, you can query the OIM_BLKLD_LOG table for information about the progress of the operation. For example, you can run the following query to see progress messages generated during the bulk load operation to load account data:

```
SELECT MSG FROM OIM_BLKLD_LOG
WHERE MODULE = 'ACCOUNT' AND LOG_LEVEL = 'PROGRESS_MSG'
ORDER BY MSG_SEQ_NO;
```

For example, you can run the following query to see progress messages generated during the bulk load operation to load account data:

```
SELECT MSG FROM OIM_BLKLD_LOG
WHERE MODULE = 'ACCOUNT' AND LOG_LEVEL = 'PROGRESS_MSG'
ORDER BY MSG_SEQ_NO;
```

Errors encountered during the bulk load operation can be viewed by querying the OIM_BLKLD_LOG table. The following is an example of the query to retrieve error messages:

```
SELECT MSG FROM OIM_BLKLD_LOG
WHERE MODULE = 'ACCOUNT' AND LOG_LEVEL = 'ERROR'
ORDER BY MSG_SEQ_NO;
```

15.5.7 Handling Exceptions Recorded During the Operation

At the end of a bulk load operation, the utility records statistics related to the operation in the following file:

oimbulkload/logs_*YYYYMMDD_hhmm*/oim_blkld_account_load_summary.log

To determine if there were exceptions during the operation, open this log file and look for the number against the Number of Records Rejected label. If the number of rejected records is greater than zero, then exceptions were thrown during the operation. User records that are rejected by the utility are recorded in the exception table (OIM_BLKLD_EX_*SUFFIX*). For each rejected record, the EXCEPTION_MSG column in the OIM_BLKLD_EX_*SUFFIX* table stores information about the reason the record could not be loaded.

Example 15–2 shows sample statistics recorded in the log file at the end of a bulk load operation to store account data.

Example 15–2 Sample Log File Generated After Loading Account Data

```
============================================================
A C C O U N T   L O A D   S T A T I S T I C S
============================================================
Start Time:   22-JUL-08 03.59.30.206000 PM
End Time:     22-JUL-08 04.03.21.126000 PM
Number of Records Processed:  100026
Number of Records Loaded:     100000
Number of Records Rejected:   26
============================================================

The names of the TMP tables used during the load:
OIM_BLKLD_TMP_P100001
OIM_BLKLD_TMP_C100002
The names of the Exception tables used during the load:
OIM_BLKLD_EX_P100001
OIM_BLKLD_EX_C100002
```

In this sample, the number of rejected records is 26. If the log file shows that any records were rejected by the utility, then see "Fixing Exceptions and Reloading Data Records" for information about retrying the load operation for these records.

Note: At the end of each bulk load operation, it is recommended that you create a backup of the exception tables.

15.5.8 Fixing Exceptions and Reloading Data Records

Note: If you want to load data from CSV files for multiple target systems, then you can apply one of the following approaches:

- **Approach 1:** Run the utility for all the sets of CSV files, and then perform the procedure described in this section.
- **Approach 2:** Run the utility for one set of CSV files, and perform the procedure described in this section. Then, repeat this procedure for the next set of CSV files.

As mentioned earlier, errors encountered during the bulk load operation can be viewed by querying the OIM_BLKLD_LOG table. The following is an example of the query to retrieve error messages:

```
SELECT MSG FROM OIM_BLKLD_LOG
WHERE MODULE = 'ACCOUNT' AND LOG_LEVEL = 'ERROR'
ORDER BY MSG_SEQ_NO;
```

An exception table OIM_BLKLD_EX_*SUFFIX* is created for each data table used as the input source during the bulk load operation. Records that do not meet the criteria for the operation are copied into this exception table. The suffix appended to the name of each exception table is the same as suffix appended to the name of the corresponding data table.

To reload rejected records:

1. Create a backup of the exception table in which rejected records are stored.

   Note: Although this is an optional step, it is recommended that you create a backup.

2. Review each record in the exception table, and fix errors in the data based on the message recorded in the EXCEPTION_MSG column.
3. After you fix errors in all the rejected records in an exception table, rename the table to OIM_BLKLD_TMP_*SUFFIX* and then use it as the input source.
4. Load records from the OIM_BLKLD_TMP_*SUFFIX* table by running the utility. See "Running the Utility" for more information.
5. Repeat Steps 1 through 4 until the Number of Records Rejected label in the oim_blkld_account_load_summary.log file shows the value 0.
6. Restart Oracle Identity Manager.

15.5.9 Verifying the Outcome of the Bulk Load Operation

To verify the outcome of the bulk load operation, check if you are able to perform the following steps for one of the OIM Users for whom an account has been added by the utility:

See Also: *Oracle Identity Manager Administrative and User Console Guide* for detailed information about these procedures

- Log in as the OIM User, and check if the newly created account is displayed in the resource profile of the user.
- Log in to the target system by using the credentials of the newly created account.

15.5.10 Gathering Performance Data from the Bulk Load Operation

As mentioned earlier in this document, the following log file is created during the bulk load operation:

oimbulkload/logs_*YYYYMMDD_hhmm*/oim_blkld_account_load_summary.log

Data recorded in this file can be used to collate performance-related information about the bulk load operation. The following information can be collected after the bulk load operation:

- Start time
- Input source
- Number of records in the system before the load
- Number of records successfully loaded
- Number of records rejected
- Total time taken

You can use this information during future runs of the utility. If you want to retain information about the bulk load operation, then move this file to a permanent location.

15.5.11 Cleaning Up After a Bulk Load Operation

If you do not want to save the results of a bulk load operation, then:

- Remove the OIM_BLKLD_TMP_*SUFFIX*, OIM_BLKLD_EX_*SUFFIX*, and OIM_BLKLD_LOG tables.
- Remove files that you created or used during the operation.
- If you created a tablespace for the operation, then remove the tablespace.
- See "Sect1: Gathering Performance Data from the Bulk Load Operation" before you remove log files created in the logs_*timestamp* directory.

Note: At this point, you can restart Oracle Identity Manager if you have not already done so.

15.5.12 Generating an Audit Snapshot

If required, you can generate an audit snapshot of Oracle Identity Manager data after a bulk load operation. The utility uses the audit utility shipped with Oracle Identity Manager release 9.1.0. Internally, the GenerateSnapshot script is called when you run the audit utility. Similarly, the GenerateSnapshot script is called when you select the option to generate an audit snapshot.

Note: Oracle Identity Manager must be up and running when you run the audit utility.

Before you generate an audit snapshot:

1. Open the *OIM_HOME*/bin/GenerateSnapshot.sh (or GenerateSnapshot.bat) file in a text editor.
2. In this file, search for the following line:
   - In the GenerateSnapshot.bat file:

     SET XEL_HOME=..
   - In the GenerateSnapshot.sh file:

     XEL_HOME=..
3. Replace this line with the following line:
   - In the GenerateSnapshot.bat file:

     SET XEL_HOME=<*Full path of the OIM_HOME directory*>

- In the GenerateSnapshot.sh file:

  XEL_HOME=<*Full path of the OIM_HOME directory*>

4. Save and close the file.

See *Oracle Identity Manager Audit Report Developer's Guide* for information about the procedure to generate audit snapshots.

A

Reference for Design Console Users

In the previous release, this appendix described the Design Console actions and adapter task mapping information. From the current release onward, you will find this information in the "Design Console Actions" and the "Adapter Mapping Information" sections in the *Oracle Identity Manager Reference*.

B

Sample SPML Messages

This appendix lists some sample SOAP SPML messages that are supported by the SPML Web service. These SPML messages are embedded in a SOAP request.

Add Request

The following sample contains an Add Request operation to create a user with the user ID `John Doe` and subscribe him to two groups, Groups 5 and Groups 6:

```
<addRequest returnData="everything" xmlns="urn:oasis:names:tc:SPML:2:0"
xmlns:dsml="urn:oasis:names:tc:DSML:2:0:core">
    <data>
           <dsml:attr name="objectclass">
                 <dsml:value>Users</dsml:value>
           </dsml:attr>
          <dsml:attr name="Users.User ID">
                 <dsml:value>John Doe</dsml:value>
           </dsml:attr>
            <dsml:attr name="Users.First Name">
                  <dsml:value>John</dsml:value>
            </dsml:attr>
            <dsml:attr name="Users.Last Name">
                   <dsml:value>Doe</dsml:value>
             </dsml:attr>
             <dsml:attr name="Organizations.Organization Name">
                    <dsml:value>Xellerate Users</dsml:value>
             </dsml:attr>
             <dsml:attr name="Users.Xellerate Type">
                     <dsml:value>End-User</dsml:value>
             </dsml:attr>
             <dsml:attr name="Users.Role">
                      <dsml:value>Full-Time</dsml:value>
              </dsml:attr>
              <dsml:attr name="Users.Password">
                      <dsml:value>welcome</dsml:value>
                </dsml:attr>
        </data>
   <capabilityData capabilityURI="urn:oasis:names:tc:SPML:2:0:reference"
mustUnderstand="true">
        <reference typeOfReference="memberOf"
xmlns="urn:oasis:names:tc:SPML:2:0:reference">
                  <toPsoID ID="Groups:5" />
         </reference>
         <reference typeOfReference="memberOf"
xmlns="urn:oasis:names:tc:SPML:2:0:reference">
                   <toPsoID ID="Groups:6" />
         </reference>
```

```
      </capabilityData>
</addRequest>
```

The following sample contains the success response for the preceding Add Request operation:

```
<addResponse status="success">
<pso>
<psoID ID="Users:7"/>
<data>
<attr name="Users.User ID">
<value>John Doe</value>
</attr>
<attr name="Users.Key">
<value>7</value>
</attr>
<attr name="Users.Last Name">
<value>Doe</value>
</attr>
<attr name="Users.First Name">
<value>John</value>
</attr>
<attr name="Users.Xellerate Type">
<value>End-User</value>
</attr>
<attr name="Users.Creation Date">
<value>2007-08-28 12:42:32.147</value>
</attr>
<attr name="Users.Updated By">
<value>1</value>
</attr>
<attr name="Users.Update Date">
<value>2007-08-28 12:42:36.38</value>
</attr>
<attr name="Users.Status">
<value>Active</value>
</attr>
<attr name="Users.Disable User">
<value>0</value>
</attr>
<attr name="Users.Lock User">
<value>0</value>
</attr>
<attr name="Organizations.Key">
<value>1</value>
</attr>
<attr name="Users.Role">
<value>Full-Time</value>
</attr>
<attr name="Organizations.Organization Name">
<value>Xellerate Users</value>
</attr>
<attr name="Users.Provisioned Date">
<value>2007-08-28 12:42:32.147</value>
</attr>
<attr name="Users.Change Password At Next Logon">
<value>1</value>
</attr>
<attr name="objectclass">
<value>Users</value>
</attr>
```

```
</data>
<capabilityData capabilityURI="urn:oasis:names:tc:SPML:2:0:reference"
mustUnderstand="true">
<reference typeOfReference="memberOf">
<toPsoID ID="Groups:5"/>
</reference>
<reference typeOfReference="memberOf">
<toPsoID ID="Groups:6"/>
</reference>
</capabilityData>
</pso>
</addResponse>
```

The following sample contains the failure response for the Add Request operation in case the user with the user ID already exists:

```
<addResponse status="failure" error="alreadyExists">
<errorMessage>
exception=tcDuplicateUserException;errorMessage=Duplicate_User
</errorMessage>
</addResponse>
```

The following sample contains an Add Request operation to create a group and subscribe it to two groups Groups:4 and Groups:5. The request is also to assign the group to two administrator groups Groups:7 and Groups:8.

```
<addRequest returnData="everything" xmlns="urn:oasis:names:tc:SPML:2:0"
xmlns:dsml="urn:oasis:names:tc:DSML:2:0:core">
<data>
<dsml:attr name="objectclass">
<dsml:value>Groups</dsml:value>
</dsml:attr>
<dsml:attr name="Groups.Group Name">
<dsml:value>Add Group40</dsml:value>
</dsml:attr>
</data>
<capabilityData capabilityURI="urn:oasis:names:tc:SPML:2:0:reference"
mustUnderstand="true">
<reference typeOfReference="memberOf"
xmlns="urn:oasis:names:tc:SPML:2:0:reference">
<toPsoID ID="Groups:4" />
                                                              </reference>
                                <reference typeOfReference="memberOf"
xmlns="urn:oasis:names:tc:SPML:2:0:reference">
                                          <toPsoID ID="Groups:5" />
                                </reference>
<reference typeOfReference="administrator"
xmlns="urn:oasis:names:tc:SPML:2:0:reference">
            <toPsoID ID="Groups:7" />
</reference>
<reference typeOfReference="administrator"
xmlns="urn:oasis:names:tc:SPML:2:0:reference">
            <toPsoID ID="Groups:8" />
</reference>
              </capabilityData>
</addRequest>
```

The following sample contains the success response for the preceding Add Request operation to create a group:

```
<addResponse status="success">
```

```
<pso>
<psoID ID="Groups:11"/>
<data>
<attr name="Groups.Key">
<value>11</value>
</attr>
<attr name="Groups.Group Name">
<value>Add Group40</value>
</attr>
<attr name="Groups.Updated By">
<value>1</value>
</attr>
<attr name="Groups.Update Date">
<value>2007-08-28 15:22:04.953</value>
</attr>
<attr name="Groups.Creation Date">
<value>2007-08-28 15:22:04.953</value>
</attr>
<attr name="Groups.Created By">
<value>1</value>
</attr>
<attr name="objectclass">
<value>Groups</value>
</attr>
</data>
<capabilityData capabilityURI="urn:oasis:names:tc:SPML:2:0:reference"
mustUnderstand="true">
<reference typeOfReference="memberOf">
<toPsoID ID="Groups:4"/>
</reference>
<reference typeOfReference="memberOf">
<toPsoID ID="Groups:5"/>
</reference>
<reference typeOfReference="administrator">
<toPsoID ID="Groups:1"/>
</reference>
<reference typeOfReference="administrator">
<toPsoID ID="Groups:7"/>
</reference>
<reference typeOfReference="administrator">
<toPsoID ID="Groups:8"/>
</reference>
</capabilityData>
</pso>
</addResponse>
```

The following sample contains the failure response for the preceding operation in case the group already exists:

```
<addResponse status="failure" error="alreadyExists">
<errorMessage>exception=Duplicate_Group</errorMessage>
</addResponse>
```

Modify Request

The following sample contains a Modify Request operation to unsubscribe a user from two groups and subscribe him to two new groups, Groups:4 and Groups:5:

```
<modifyRequest returnData="everything" xmlns="urn:oasis:names:tc:SPML:2:0"
xmlns:dsml="urn:oasis:names:tc:DSML:2:0:core">
<psoID ID="Users:31"></psoID>
```

```
    <modification modificationMode="add">
             <capabilityData capabilityURI="urn:oasis:names:tc:SPML:2:0:reference"
mustUnderstand="true">
                    <reference typeOfReference="memberOf"
xmlns="urn:oasis:names:tc:SPML:2:0:reference">
                                <toPsoID ID="Groups:4" />
                    </reference>
                     <reference typeOfReference="memberOf"
xmlns="urn:oasis:names:tc:SPML:2:0:reference">
                                <toPsoID ID="Groups:5"/>
                     </reference>
              </capabilityData>
</modification>
<modification modificationMode="delete">
            <capabilityData capabilityURI="urn:oasis:names:tc:SPML:2:0:reference"
mustUnderstand="true">
                      <reference typeOfReference="memberOf"
xmlns="urn:oasis:names:tc:SPML:2:0:reference">
                               <toPsoID ID="Groups:6"/>
                      </reference>
                     <reference typeOfReference="memberOf"
xmlns="urn:oasis:names:tc:SPML:2:0:reference">
                             <toPsoID ID="Groups:7"/>
                      </reference>
           </capabilityData>
   </modification>
</modifyRequest>
```

The following sample contains the success response for the preceding Modify Request operation:

```
<modifyResponse status="success">
<pso>
<psoID ID="Users:31"/>
<data>
<attr name="Users.User ID">
<value>John Doe</value>
</attr>
<attr name="Users.Key">
<value>7</value>
</attr>
<attr name="Users.Last Name">
<value>Doe</value>
</attr>
<attr name="Users.First Name">
<value>John</value>
</attr>
<attr name="Users.Xellerate Type">
<value>End-User</value>
</attr>
<attr name="Users.Creation Date">
<value>2007-08-28 12:42:32.147</value>
</attr>
<attr name="Users.Updated By">
<value>1</value>
</attr>
<attr name="Users.Update Date">
<value>2007-08-28 12:42:36.38</value>
</attr>
<attr name="Users.Status">
<value>Active</value>
```

```
</attr>
<attr name="Users.Disable User">
<value>0</value>
</attr>
<attr name="Users.Lock User">
<value>0</value>
</attr>
<attr name="Organizations.Key">
<value>1</value>
</attr>
<attr name="Users.Role">
<value>Full-Time</value>
</attr>
<attr name="Organizations.Organization Name">
<value>Xellerate Users</value>
</attr>
<attr name="Users.Provisioned Date">
<value>2007-08-28 12:42:32.147</value>
</attr>
<attr name="Users.Change Password At Next Logon">
<value>1</value>
</attr>
</data>
<capabilityData capabilityURI="urn:oasis:names:tc:SPML:2:0:reference"
mustUnderstand="true">
<reference typeOfReference="memberOf">
<toPsoID ID="Groups:3"/>
</reference>
<reference typeOfReference="memberOf">
<toPsoID ID="Groups:4"/>
</reference>
<reference typeOfReference="memberOf">
<toPsoID ID="Groups:5"/>
</reference>
</capabilityData>
</pso>
</modifyResponse>
```

The following sample contains the failure response for the preceding operation in case the user is not available:

```
<modifyResponse status="failure" error="noSuchIdentifier">
<errorMessage>
exception=OIMSpmlException;errorMessage=NO_USER_ID_DEFINED
</errorMessage>
</modifyResponse>
```

The following sample contains a Modify Request operation that modifies the group Groups:36 and its group references by adding two more group membership (Groups:7 and Groups:8) and a group administrator (Groups:9). It also deletes an existing group membership (Groups:10) and an administrator reference (Groups:11).

```
<modifyRequest returnData="everything" xmlns="urn:oasis:names:tc:SPML:2:0"
xmlns:dsml="urn:oasis:names:tc:DSML:2:0:core">
       <psoID ID="Groups:36"></psoID>
        <modification>
                   <dsml:modification name="Groups.Group Name" operation="add">
                           <dsml:value>Changed</dsml:value>
                   </dsml:modification>
          </modification>
          <modification modificationMode="add">
```

```
                  <capabilityData
capabilityURI="urn:oasis:names:tc:SPML:2:0:reference" mustUnderstand="true">
                           <reference typeOfReference="memberOf"
xmlns="urn:oasis:names:tc:SPML:2:0:reference">
                                        <toPsoID ID="Groups:7"/>
                            </reference>
                            <reference typeOfReference="memberOf"
xmlns="urn:oasis:names:tc:SPML:2:0:reference">
                                        <toPsoID ID="Groups:8"/>
                           </reference>
                          <reference typeOfReference="administrator"
xmlns="urn:oasis:names:tc:SPML:2:0:reference">
                                       <toPsoID ID="Groups:9"/>
                           </reference>
                 </capabilityData>
          </modification>
          <modification modificationMode="delete">
                <capabilityData
capabilityURI="urn:oasis:names:tc:SPML:2:0:reference" mustUnderstand="true">
                      <reference typeOfReference="administrator"
xmlns="urn:oasis:names:tc:SPML:2:0:reference">
                                  <toPsoID ID="Groups:10"/>
                      </reference>
                       <reference typeOfReference="memberOf"
xmlns="urn:oasis:names:tc:SPML:2:0:reference">
                               <toPsoID ID="Groups:11"/>
                       </reference>
                </capabilityData>
           </modification>
</modifyRequest>
```

The following sample contains the success response for the preceding Modify Request operation:

```
<modifyResponse status="success">
<pso>
<psoID ID="Groups:36"/>
<data>
<attr name="Groups.Key">
<value>36</value>
</attr>
<attr name="Groups.Group Name">
<value>Changed</value>
</attr>
<attr name="Groups.Updated By">
<value>1</value>
</attr>
<attr name="Groups.Update Date">
<value>2007-08-29 21:00:51.657</value>
</attr>
<attr name="Groups.Creation Date">
<value>2007-08-27 15:22:43.97</value>
</attr>
<attr name="Groups.Created By">
<value>1</value>
</attr>
</data>
<capabilityData capabilityURI="urn:oasis:names:tc:SPML:2:0:reference"
mustUnderstand="true">
<reference typeOfReference="memberOf">
```

```
<toPsoID ID="Groups:7"/>
</reference>
<reference typeOfReference="memberOf">
<toPsoID ID="Groups:8"/>
</reference>
<reference typeOfReference="administrator">
<toPsoID ID="Groups:1"/>
</reference>
<reference typeOfReference="administrator">
<toPsoID ID="Groups:9"/>
</reference>
</capabilityData>
</pso>
</modifyResponse>
```

The following sample contains the failure response for the preceding operation in case the group ID is missing:

```
<modifyResponse status="failure" error="noSuchIdentifier">
<errorMessage>
exception=OIMSpmlException;errorMessage=GROUP_NOT_FOUND
</errorMessage>
</modifyResponse>
```

Add Request With Date Format

The following sample Add Request operation adds a user by assigning some start date and end date attribute. The date format should assume the format- yyyy-mm-dd HH:MM:SS.sss.

```
<addRequest returnData="everything" xmlns="urn:oasis:names:tc:SPML:2:0"
xmlns:dsml="urn:oasis:names:tc:DSML:2:0:core">
    <data>
 <dsml:attr name="objectclass">
         <dsml:value>Users</dsml:value>
</dsml:attr>
<dsml:attr name="Users.User ID">
    <dsml:value>John Doe</dsml:value>
</dsml:attr>
<dsml:attr name="Users.First Name">
    <dsml:value>John</dsml:value>
</dsml:attr>
<dsml:attr name="Users.Last Name">
    <dsml:value>Doe</dsml:value>
</dsml:attr>
<dsml:attr name="Organizations.Organization Name">
    <dsml:value>Xellerate Users</dsml:value>
</dsml:attr>
<dsml:attr name="Users.Xellerate Type">
    <dsml:value>End-User</dsml:value>
</dsml:attr>
<dsml:attr name="Users.Manager Login">
    <dsml:value>Jane Doe</dsml:value>
</dsml:attr>
<dsml:attr name="Users.Role">
    <dsml:value>Full-Time</dsml:value>
</dsml:attr>
<dsml:attr name="Users.Password">
    <dsml:value>welcome</dsml:value>
</dsml:attr>
```

```
<dsml:attr name="Users.Start Date">
    <dsml:value>2007-06-18 00:00:00.000</dsml:value>
</dsml:attr>
<dsml:attr name="Users.End Date">
    <dsml:value>2017-06-18 00:00:00.000</dsml:value>
</dsml:attr>
  </data>
</addRequest>
```

The following sample contains the success response for the preceding Add Request operation:

```
<addResponse status="success">
<pso>
<psoID ID="Users:8"/>
<data>
<attr name="Users.User ID">
<value>John Doe</value>
</attr>
<attr name="Users.Key">
<value>8</value>
</attr>
<attr name="Users.Last Name">
<value>Doe</value>
</attr>
<attr name="Users.First Name">
<value>John</value>
</attr>
<attr name="Users.Manager Key">
<value>4</value>
</attr>
<attr name="Users.Manager Login">
<value>John</value>
</attr>
<attr name="Users.Manager First Name">
<value>John</value>
</attr>
<attr name="Users.Manager Last Name">
<value>Doe</value>
</attr>
<attr name="Users.Xellerate Type">
<value>End-User</value>
</attr>
<attr name="Users.Creation Date">
<value>2007-08-29 21:27:03.39</value>
</attr>
<attr name="Users.Updated By">
<value>1</value>
</attr>
<attr name="Users.Update Date">
<value>2007-08-29 21:27:06.937</value>
</attr>
<attr name="Users.Status">
<value>Active</value>
</attr>
<attr name="Users.Disable User">
<value>0</value>
</attr>
<attr name="Users.Lock User">
<value>0</value>
</attr>
```

```
<attr name="Organizations.Key">
<value>1</value>
</attr>
<attr name="Users.Role">
<value>Full-Time</value>
</attr>
<attr name="Organizations.Organization Name">
<value>Xellerate Users</value>
</attr>
<attr name="Users.Start Date">
<value>2007-06-18 00:00:00.0</value>
</attr>
<attr name="Users.End Date">
<value>2017-06-18 00:00:00.0</value>
</attr>
<attr name="Users.Provisioning Date">
<value>2007-06-18 00:00:00.0</value>
</attr>
<attr name="Users.Provisioned Date">
<value>2007-08-29 21:27:03.39</value>
</attr>
<attr name="Users.Change Password At Next Logon">
<value>1</value>
</attr>
<attr name="objectclass">
<value>Users</value>
</attr>
</data>
<capabilityData capabilityURI="urn:oasis:names:tc:SPML:2:0:reference"
mustUnderstand="true">
<reference typeOfReference="memberOf">
<toPsoID ID="Groups:3"/>
</reference>
</capabilityData>
</pso>
</addResponse>
```

The following sample contains the failure response for the preceding operation in case the user already exists:

```
<addResponse status="failure" error="alreadyExists">
<errorMessage>
exception=tcDuplicateUserException;errorMessage=Duplicate_User
</errorMessage>
</addResponse>
```

Index

A

Adapter Variables, 3-3
Adapters, 1-2, 3-1
Adding the Trust Relation, 2-2
asynchronous SoD validation process, 13-20, 13-27, 13-29, 13-33
Attaching Pre-Populate Adapters, 7-2
Attaching Process Task Adapters to Process Tasks, 4-3
Attaching Task Assignment Adapters to Process Tasks, 5-2

C

Compiling Adapters, 9-1
Create a Remote Task, 3-10
Create a Response, 3-25
Create a Stored Procedure Task, 3-12
Create a Utility Task, 3-14
Create an Oracle Identity Manager API Task, 3-16
Creating Adapter Tasks, 3-5
custom SoD engine, 13-3, 13-35

D

Delete a Response, 3-26
Deleting Adapter Tasks, 3-24
Disabling Adapters, 3-2

E

Entity Adapters, 3-26
Execution Schedule, 1-3
Exporting and Importing Adapters, 10-1

H

How a Process Task Adapter Works, 4-2

I

include data for capability element, 12-5
Installing the Remote Manager, 2-2
Integration Problem, 1-1

M

Managing Entities, 8-1
Mapping Rule Generator Adapter Variables, 6-2
Modify a Response, 3-25
Modify an Adapter Variable, 3-4
Modifying Adapter Tasks, 3-22

O

OAACG SIL Provider, 13-2
Oracle Application Access Controls Governor, 13-1, 13-2, 13-6, 13-9, 13-14, 13-18, 13-21, 13-22, 13-23, 13-35, 13-36
Oracle e-Business Suite, 13-1, 13-6, 13-14, 13-21, 13-35
Oracle e-Business User Management, 13-2, 13-23, 13-32
Oracle Identity Manager Design Console Guide, 1-2
Oracle Identity Manager Solution, 1-1

P

Post-install Configuration, 11-1
preconfigured SoD connectors
  Oracle e-Business User Management, 13-2, 13-23, 13-32
  SAP CUA connector, 13-2
  SAP User Management connector, 13-2, 13-23
Pre-Populate Adapters, 7-1

R

Removing Process Task Adapters from Process Tasks, 4-6
Removing Rule Generators from Form Fields, 6-5
Removing Task Assignment Adapters from Process Tasks, 5-5
Resources, 1-4
Responses, 1-4

S

SAP CUA, 13-1, 13-2, 13-14, 13-21, 13-23, 13-35
SAP GRC, 13-1, 13-2, 13-6, 13-19, 13-21, 13-35, 13-36
SAP GRC SIL Provider, 13-2
SAP R/3, 13-1, 13-6, 13-14

SAP User Management connector, 13-2, 13-23
Scheduling Rule Generators, 3-26
segregation of duties, 13-1
SIL, 13-1, 13-29
SIL provider, 13-3
SIL providers, 13-2, 13-4, 13-9, 13-23, 13-35
  OAACG, 13-2
  SAP, 13-2
SILConfig.xml, 13-10, 13-11, 13-13, 13-16, 13-34, 13-36
SoD, 13-1
SoD engines
  Oracle Application Access Controls Governor, 13-1, 13-2, 13-6, 13-9, 13-14, 13-18, 13-21, 13-22, 13-23, 13-35, 13-36
  SAP GRC, 13-1, 13-2, 13-6, 13-19, 13-21, 13-35, 13-36
SoD target systems
  Oracle e-Business Suite, 13-1, 13-6, 13-14, 13-21, 13-35
  SAP CUA, 13-1, 13-14, 13-21, 13-23, 13-35
  SAP R/3, 13-1, 13-6, 13-14
SPML requests, B-1
SSL, configuring for SoD validation, 13-10, 13-17
synchronous SoD validation process, 13-20, 13-29

T

Tabs of the Adapter Factory Form, 1-3

U

Usage Lookup, 1-4

V

Variable List, 1-4

W

Working with Responses, 3-24