Oracle® Identity Manager

Connector Guide for Sun Java System Directory

Release 9.0.3

B32373-02

March 2007

ORACLE®

Oracle Identity Manager Connector Guide for Sun Java System Directory, Release 9.0.3

B32373-02

Primary Authors: Debapriya Datta, Shiladitya Guha

Contributing Authors: Don Gosselin, Vijaykarthik Sathiyamurthy, Lyju Vadassery

Contents

Preface

Oracle Identity Manager Connector Guide for Sun Java System Directory provides information about integrating Oracle Identity Manager with Sun Java System Directory.

Note: Some parts of the product and documentation still refer to the original Thor company name and Xellerate product name and will be rebranded in future releases.

Audience

This guide is intended for users who want to deploy the Oracle Identity Manager connector for Sun Java System Directory.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. 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.

TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, seven days a week. For TTY support, call 800.446.2398.

Related Documents

For more information, refer to the following documents in the Oracle Identity Manager documentation library:

- *Oracle Identity Manager Release Notes*
- *Oracle Identity Manager Installation Guide for JBoss*
- *Oracle Identity Manager Installation Guide for Oracle Containers for J2EE*
- *Oracle Identity Manager Installation Guide for WebLogic*
- *Oracle Identity Manager Installation Guide for WebSphere*
- *Oracle Identity Manager Administrative and User Console Guide*
- *Oracle Identity Manager Administrative and User Console Customization Guide*
- *Oracle Identity Manager Design Console Guide*
- *Oracle Identity Manager Tools Reference Guide*
- *Oracle Identity Manager Audit Report Developer Guide*
- *Oracle Identity Manager Best Practices Guide*
- *Oracle Identity Manager Globalization Guide*
- *Oracle Identity Manager Glossary of Terms*

The following document is available in the Oracle Identity Manager Connector Pack documentation library:

- *Oracle Identity Manager Connector Framework Guide*

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager 9.0.3 connector documentation set, visit Oracle Technology Network at

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

What's New in the Oracle Identity Manager Connector for Sun Java System Directory?

This chapter provides an overview of the updates made to the connector and documentation for Sun Java System Directory in release 9.0.3.1 of the Oracle Identity Manager connector pack.

> **See Also:** The 9.0.3 release of this guide for information about updates that were new for the 9.0.3 release

The updates discussed in this chapter are divided into the following categories:

- Software Updates

  These include updates made to the connector software.

- Documentation-Specific Updates

  These include major changes made to the connector documentation. These changes are not related to software updates.

> **See Also:** *Oracle Identity Manager Release Notes*

Software Updates

This section discusses updates made to this release of the connector software.

Support for Siemens HiPath Slcurity DirX

Along with Sun ONE Directory Server 5.2, this release of the connector also supports Siemens HiPath Slcurity DirX 6.0 D10 as a target system. The following are changes pertaining to this functionality enhancement:

- In the "Step 1: Verifying Deployment Requirements" section on page 2-1, Siemens HiPath Slcurity DirX has been added as one of the supported target systems.
- In the "User Reconciliation Scheduled Task" section on page 2-9, the `IsIPlanetTarget` attribute has been added to the user reconciliation scheduled task definition. This attribute is used to specify whether the target system is Sun Java System Directory or Siemens HiPath Slcurity DirX.
- The "Configuring the Lookup Definition for Reconciliation with Siemens HiPath Slcurity DirX" section on page 2-10 describes the change to be made in the `AttrName.Recon.Map.iPlanet` lookup definition to enable lookup fields reconciliation on Siemens HiPath Slcurity DirX.

Documentation-Specific Updates

There are no documentation-specific updates in this release of the guide.

1

About the Connector

Oracle Identity Manager automates access rights management, security, and provisioning of IT resources. Oracle Identity Manager connectors are used to integrate Oracle Identity Manager with third-party applications. The connector for Sun Java System Directory is used to integrate Oracle Identity Manager with Sun Java System Directory.

Note: Oracle Identity Manager connectors were referred to as *resource adapters* prior to the acquisition of Thor Technologies by Oracle.

This chapter contains the following sections:

Supported Functionality

The following table lists the functions that are available with this connector.

Process Task	Type	Description
Create User	Provisioning	Creates a user
Delete User	Provisioning	Deletes a user
Enable User	Provisioning	Enables a user
Disable User	Provisioning	Disables a user
Move User	Provisioning	Moves a user from one container to another
Password Updated	Provisioning	Updates the password of a user
First Name Updated	Provisioning	Updates the first name of a user
Last Name Updated	Provisioning	Updates the last name of a user
Department Updated	Provisioning	Updates the department of a user

Process Task	Type	Description
Email ID Updated	Provisioning	Updates the e-mail address of a user
Location Updated	Provisioning	Updates the location of a user
Middle Name Updated	Provisioning	Updates the middle name of a user
Communication Language Updated	Provisioning	Updates the communication language preference of a user
Telephone Updated	Provisioning	Updates the telephone number of a user
Title Updated	Provisioning	Updates the title of the user
Organization DN Updated	Provisioning	Updates the organization DN of a user
Add User to Group	Provisioning	Adds a user to a group
Remove User from Group	Provisioning	Removes a user from a group
Add User to Role	Provisioning	Adds a user to a role
Remove User from Role	Provisioning	Removes a user from a role
Reconciliation Delete Received	Reconciliation	Deletes a user from Oracle Identity Manager if the user is deleted from Sun Java System Directory
Reconciliation Insert Received	Reconciliation	Inserts a user in Oracle Identity Manager
Reconciliation Update Received	Reconciliation	Updates user attributes, such as the first name and last name, in Oracle Identity Manager

See Also: Appendix A for information about attribute mappings between Oracle Identity Manager and Sun Java System Directory

Multilanguage Support

This release of the connector supports the following languages:

- English
- Brazilian Portuguese
- French
- German
- Italian
- Japanese
- Korean
- Simplified Chinese
- Spanish
- Traditional Chinese

See Also: *Oracle Identity Manager Globalization Guide* for information about supported special characters

Reconciliation Module

This section discusses the elements that the reconciliation module extracts from the target system to construct reconciliation event records.

Reconciliation can be divided into the following types:

- Lookup Fields Reconciliation
- User Reconciliation

Lookup Fields Reconciliation

Lookup fields reconciliation involves reconciling the fields for groups, roles, and organization.

User Reconciliation

User reconciliation involves reconciling the fields discussed in this section.

Reconciled Resource Object Fields

The following fields are reconciled:

- User ID
- First Name
- Last Name
- Middle Name
- Department
- Location
- Telephone
- Email
- Communication Language
- Title
- Organization Unit
- Server Name (IT resource)
- Group
- Role

Reconciled Xellerate User Fields

The following fields are reconciled only if reconciliation is implemented in trusted mode:

- UserID
- Password
- First Name
- Last Name
- Role

Provisioning Module

The following fields are provisioned:

- User ID
- First Name
- Last Name
- Middle Name
- Department
- Location
- Telephone
- Email
- Communication Language
- Title
- Server Name (IT resource)

Files and Directories That Comprise the Connector

The files and directories that comprise this connector are compressed in the following directory on the installation media:

`Directory Servers\Sun Java System Directory Server`

These files and directories are listed in the following table.

File in the Installation Media Directory	Description
`lib\xliIPlanet.jar`	This JAR file contains the class files required for provisioning and reconciliation.
Files in the `resources` directory	Each of these resource bundle files contains language-specific information that is used by the connector. **Note:** A **resource bundle** is a file containing localized versions of the text strings that are displayed on the user interface of Oracle Identity Manager. These text strings include GUI element labels and messages displayed on the Administrative and User Console.
`troubleshoot\TroubleShootingUtilityIPlanet.class`	This is the standalone class that interacts with the target system. This is the class that has the code required to run the test cases.
`troubleshoot\log.properties`	This file is used to specify the log level and the directory in which the log file is to be created when you run the troubleshooting utility.
`troubleshoot\TroubleShootIPlanet.properties`	This file contains the connection details that are required to connect to the target system and user details. It also contains details about the commands to be run.

File in the Installation Media Directory	Description
xml\iPlanetResourceObject.xml	This XML file contains definitions for the following components of the connector: ■ IT resource type ■ Custom process form ■ Process task and rule-generator adapters (along with their mappings) ■ Resource object ■ Provisioning process ■ Pre-populate rules ■ Reconciliation process ■ Lookup definitions
xml\iPlanetXLResourceObject.xml	This XML file contains the configuration for the Xellerate User. You must import this file only if you plan to use the connector in trusted source reconciliation mode.

Note: The files in the troubleshoot directory are used only to run tests on the connector.

The "Step 2: Copying the Connector Files" section on page 2-1 provides instructions to copy these files into the required directories.

Determining the Release Number of the Connector

To determine the release number of the connector that you have deployed:

1. Extract the contents of the xliIPlanet.jar file. For a connector that has been deployed, this file is in the following directory:

   OIM_home\xellerate\JavaTasks

2. Open the manifest.mf file in a text editor. The manifest.mf file is one of the files bundled inside the xliIPlanet.jar file.

   In the manifest.mf file, the release number of the connector is displayed as the value of the Version property.

See Also: *Oracle Identity Manager Design Console Guide*

2

Deploying the Connector

Deploying the connector involves the following steps:

- Step 1: Verifying Deployment Requirements
- Step 2: Copying the Connector Files
- Step 3: Configuring the Oracle Identity Manager Server
- Step 4: Importing the Connector XML Files
- Step 5: Configuring Reconciliation
- Step 6: Compiling Adapters
- Step 7: Configuring SSL

If you want to configure the connector for multiple installations of Sun Java System Directory, then perform the following procedure:

- Configuring the Connector for Multiple Installations of the Target System

Step 1: Verifying Deployment Requirements

The following table lists the deployment requirements for the connector.

Item	Requirement
Oracle Identity Manager	Oracle Identity Manager release 8.5.3 or later
Target systems	Sun ONE Directory Server 5.2 and Siemens HiPath Slcurity DirX 6.0 D10
Target system host platforms	The target system host platform can be any one of the following: ■ Microsoft Windows 2000 ■ Solaris 8 or 9
Target system user account	User account to which the Read, Write, Add, Delete, and Search rights have been assigned You provide the credentials of this user account while performing the procedure in the "Defining IT Resources" section on page 2-6.

Step 2: Copying the Connector Files

The connector files to be copied and the directories to which you must copy them are given in the following table.

Note: The directory paths given in the first column of this table correspond to the location of the connector files in the following directory on the installation media:

`Directory Servers\Sun Java System Directory Server`

Refer to the "Files and Directories That Comprise the Connector" section on page 1-4 for more information about these files.

Files in the Installation Media Directory	Destination Directory
`lib\xliIPlanet.jar`	*`OIM_home`*`\xellerate\JavaTasks`
Files in the `resources` directory	*`OIM_home`*`\xellerate\connectorResources`
Files in the `troubleshoot` directory	*`OIM_home`*`\xellerate\troubleshoot`
Files in the `xml` directory	*`OIM_home`*`\xellerate\iPlanet-`*`versionno`*`\xml`

Note: In the destination directory path, you must change the version number specified in the directory name `iPlanet-`*`versionno`* depending on the actual version number of the software.

While installing Oracle Identity Manager in a clustered environment, you copy the contents of the installation directory to each node of the cluster. Similarly, you must copy the `connectorResources` directory and the JAR files to the corresponding directories on each node of the cluster.

Step 3: Configuring the Oracle Identity Manager Server

Configuring the Oracle Identity Manager server involves the following procedures:

Note: In a clustered environment, you must perform this step on each node of the cluster.

- Changing to the Required Input Locale
- Clearing Content Related to Connector Resource Bundles from the Server Cache
- Enabling Logging

Changing to the Required Input Locale

Changing to the required input locale (language and country setting) involves installing the required fonts and setting the required input locale.

To set the required input locale:

Note: Depending on the operating system used, you may need to perform this procedure differently.

1. Open Control Panel.

2. Double-click **Regional Options**.
3. On the Input Locales tab of the Regional Options dialog box, add the input locale that you want to use and then switch to the input locale.

Clearing Content Related to Connector Resource Bundles from the Server Cache

Whenever you add a new resource bundle in the *OIM_home*\xellerate\connectorResources directory or make a change in an existing resource bundle, you must clear content related to connector resource bundles from the server cache.

To clear content related to connector resource bundles from the server cache:

1. In a command window, change to the *OIM_home*\xellerate\bin directory.
2. Enter one of the following commands:

   Note: You must perform Step 1 before you perform this step. If you run the command as follows, then an exception is thrown:

   OIM_home\xellerate\bin*batch_file_name*

   - On Microsoft Windows:

     ```
     PurgeCache.bat ConnectorResourceBundle
     ```

   - On UNIX:

     ```
     PurgeCache.sh ConnectorResourceBundle
     ```

   In this command, ConnectorResourceBundle is one of the content categories that you can remove from the server cache. Refer to the following file for information about the other content categories:

   OIM_home\xellerate\config\xlConfig.xml

   Note: You can ignore the exception that is thrown when you perform Step 2.

Enabling Logging

When you enable logging, Oracle Identity Manager automatically stores in a log file information about events that occur during the course of provisioning and reconciliation operations. To specify the type of event for which you want logging to take place, you can set the log level to one of the following:

- ALL

  This level enables logging for all events.

- DEBUG

  This level enables logging of information about fine-grained events that are useful for debugging.

- INFO

  This level enables logging of informational messages that highlight the progress of the application at coarse-grained level.

- WARN

  This level enables logging of information about potentially harmful situations.

- ERROR

  This level enables logging of information about error events that may still allow the application to continue running.

- FATAL

  This level enables logging of information about very severe error events that could cause the application to stop functioning.

- OFF

  This level disables logging for all events.

The file in which you set the log level and the log file path depend on the application server that you use:

- **For JBoss Application Server**

  To enable logging:

  1. In the *JBoss_home*\server\default\conf\log4j.xml file, locate the following lines:

     ```
     <category name="XELLERATE">
        <priority value="log_level"/>
     </category>
     ```

  2. In the second XML code line, replace *log_level* with the log level that you want to set. For example:

     ```
     <category name="XELLERATE">
        <priority value="INFO"/>
     </category>
     ```

  After you enable logging, log information is written to the following file:

  JBoss_home\server\default\log\server.log

- **For IBM WebSphere:**

  To enable logging:

  1. Add the following line in the *OIM_home*\xellerate\config\log.properties file:

     log4j.logger.XELLERATE=*log_level*

  2. In this line, replace *log_level* with the log level that you want to set.

     For example:

     log4j.logger.XELLERATE=INFO

  After you enable logging, log information is written to the following file:

  WebSphere_home\AppServer\logs*server_name*\startServer.log

- **For BEA WebLogic**

  To enable logging:

  1. Add the following line in the *OIM_home*\xellerate\config\log.properties file:

```
log4j.logger.XELLERATE=log_level
```

2. In this line, replace *log_level* with the log level that you want to set.

   For example:

   ```
   log4j.logger.XELLERATE=INFO
   ```

After you enable logging, log information is written to the following file:

WebLogic_home\user_projects\domains*domain_name**server_name**server_name*.log

- **For OC4J**

  To enable logging:

  1. Add the following line in the *OIM_home*\xellerate\config\log.properties file:

     ```
     log4j.logger.XELLERATE=log_level
     ```

  2. In this line, replace *log_level* with the log level that you want to set.

     For example:

     ```
     log4j.logger.XELLERATE=INFO
     ```

  After you enable logging, log information is written to the following file:

  OC4J_home\opmn\logs\default_group~home~default_group~1.log

Step 4: Importing the Connector XML Files

To import the connector XML files into Oracle Identity Manager:

1. Open the Oracle Identity Manager Administrative and User Console.
2. Click the **Deployment Management** link on the left navigation bar.
3. Click the **Import** link under Deployment Management. A dialog box for locating files is displayed.
4. Locate and open the iPlanetResourceObject.xml file, which is in the *OIM_home*\xellerate\iPlanet-*versionno*\xml directory. Details of this XML file are shown on the File Preview page.
5. Click **Add File.** The Substitutions page is displayed.
6. Click **Next.** The Confirmation page is displayed.
7. Click **Next.** The Provide IT Resource Instance Data page for the iPlanet User IT resource is displayed.
8. Specify values for the parameters of the iPlanet User IT resource. Refer to the table in the "Defining IT Resources" section on page 2-6 information about the values to be specified.
9. Click **Next**. The Provide IT Resource Instance Data page for a new instance of the LDAP Server IT resource type is displayed.
10. Click **Skip** to specify that you do not want to define another IT resource. The Confirmation page is displayed.

See Also: If you want to define another IT resource, then refer to *Oracle Identity Manager Tools Reference Guide* for instructions.

11. Click **View Selections.**

    The contents of the XML file are displayed in the Deployment Manager – Import window. You may see a cross-shaped icon along with some nodes. Remove these nodes by right-clicking each node and then selecting **Remove.**

12. Click **Import.** The connector file is imported into Oracle Identity Manager.

After you import the connector XML file, proceed to the "Step 5: Configuring Reconciliation" section on page 2-7.

Defining IT Resources

You must specify values for the `iPlanet User` IT resource parameters listed in the following table.

Parameter	Description
`Admin Id`	DN value of the user who has administrator rights on the target Sun Java System Directory server The default value is `uid=admin,ou=administrators,ou=topologymanagement,o=netscaperootAdmin`
`Admin Password`	Password of the administrator
`Server Address`	IP address of the target Sun Java System Directory server
`Port`	Port number to connect to the target Sun Java System Directory server The default value is `389`.
`Root DN`	Base DN where all the user operations are to be carried out The value can be `o=xyz`
`SSL`	Specifies whether or not an SSL connection is used for communication between Oracle Identity Manager and the target Sun Java System Directory server The value can be `true` or `false`. **Note:** It is recommended that you enable SSL to secure communication with the target system.
`Last Recon TimeStamp`	For the first reconciliation run, the time stamp value is not set. For subsequent rounds of reconciliation, the time at which the previous round of reconciliation was completed is stored in this parameter.
`Prov Attribute Lookup Code`	Name of the lookup definition that has the target attribute mappings required for provisioning The default value of this parameter is `AttrName.Prov.Map.iPlanet`
`Recon Attribute Lookup Code`	Name of the lookup definition that has the target attribute mappings required for reconciliation The default value of this parameter is `AttrName.Recon.Map.iPlanet`

Parameter	Description
`Use XL Org Structure`	If set to `true`, then the Oracle Identity Manager Organization structure is used during provisioning and reconciliation. If set to `false`, then the value of the Organization field in the process form is used for provisioning and the organization or container in the target Oracle Internet Directory is used for reconciliation.

After you specify values for these IT resource parameters, proceed to Step 9 of the procedure to import connector XML files.

Step 5: Configuring Reconciliation

Configuring reconciliation involves the following steps:

- Configuring Trusted Source Reconciliation
- Creating the Reconciliation Scheduled Tasks
- Configuring the Lookup Definition for Reconciliation with Siemens HiPath Slcurity DirX

Configuring Trusted Source Reconciliation

Note: Perform this step of the procedure only if you want to configure trusted source reconciliation. Only one connector can be configured for trusted source reconciliation. If you import the `iPlanetXLResourceObject.xml` file while you have another trusted source configured, then both connector reconciliations would stop working.

Refer to *Oracle Identity Manager Connector Framework Guide* for conceptual information about reconciliation configurations.

To configure trusted source reconciliation, you must first import the XML file for trusted source reconciliation as follows:

1. Open the Oracle Identity Manager Administrative and User Console.
2. Click the **Deployment Management** link on the left navigation bar.
3. Click the **Import** link under Deployment Management. A dialog box for locating files is displayed.
4. Locate and open the `iPlanetXLResourceObject.xml` file, which is in the *`OIM_home`*`\xellerate\iPlanet-`*`versionno`*`\xml` directory. Details of this XML file are shown on the File Preview page.
5. Click **Add File**. The Substitutions page is displayed.
6. Click **Next**. The Confirmation page is displayed.
7. Click **Import**.
8. In the message that is displayed, click **Import** to confirm that you want to import the **XML** file and then click **OK**.

Then, set the value of the `TrustedSource` reconciliation scheduled task attribute to `True` while performing the procedure described in the following section.

Creating the Reconciliation Scheduled Tasks

To create the scheduled tasks for lookup fields and user reconciliations:

1. Open the Oracle Identity Manager Design Console.
2. Expand the **Xellerate Administration** folder.
3. Select **Task Scheduler.**
4. Click **Find**. The details of the predefined scheduled tasks are displayed on two different tabs.
5. For the first scheduled task, enter a number in the **Max Retries** field. This number represents the number of times Oracle Identity Manager must attempt to complete the task before assigning the `ERROR` status to the task.
6. Ensure that the **Disabled** and **Stop Execution** check boxes are not selected.
7. In the Start region, double-click the **Start Time** field. From the date-time editor that is displayed, select the date and time at which you want the task to run.
8. In the Interval region, set the following schedule parameters:
   - To set the task to run on a recurring basis, select the **Daily**, **Weekly**, **Recurring Intervals**, **Monthly**, or **Yearly** option.

     If you select the **Recurring Intervals** option, then you must also specify the time interval at which you want the task to run on a recurring basis.
   - To set the task to run only once, select the **Once** option.
9. Provide values for the attributes of the scheduled task. Refer to the "Specifying Values for the Scheduled Task Attributes" section on page 2-8 for information about the values to be specified.

   See Also: *Oracle Identity Manager Design Console Guide* for information about adding and removing task attributes
10. Click **Save**. The scheduled task is created. The `INACTIVE` status is displayed in the **Status** field, because the task is not currently running. The task is run at the date and time that you set in Step 7.
11. Repeat Steps 5 through 10 to create the second scheduled task.

After you create both scheduled tasks, proceed to the "Step 6: Compiling Adapters" section on page 2-11.

Specifying Values for the Scheduled Task Attributes

This section provides information about the attribute values to be specified for the following scheduled tasks:

- Lookup Fields Reconciliation Scheduled Task
- User Reconciliation Scheduled Task

Lookup Fields Reconciliation Scheduled Task You must specify values for the following attributes of the lookup fields reconciliation scheduled task.

Note: Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.

Attribute	Description	Default/Sample Value
LookupCodeName	Name of the lookup definition to which values are to be reconciled	The value can be any one of the following: ■ For groups: Lookup.IPNT.UserGroup ■ For roles: Lookup.IPNT.Role
ITResourceName	Name of the IT resource for setting up a connection with the Sun Java System Directory server	iPlanet User
SearchContext	Search context to be used for searching for users	DC=mycompany,DC=com
ObjectClass	Name of the group object class	The value can be any one of the following: ■ For groups: groupOfUniqueNames ■ For roles: ldapsubentry
CodeKeyLTrimStr	String value for left-trimming the value obtained from the search If there is nothing to be trimmed, then specify the value [NONE].	cn= or uid=
CodeKeyRTrimStr	String value for right-trimming the value obtained from the search If there is nothing to be trimmed, then specify the value [NONE].	,DC=mycompany,DC=com
ReconMode	Specify REFRESH to completely refresh the existing lookup. Specify UPDATE to update the lookup with the new values.	REFRESH or UPDATE (specified in uppercase)
AttrType	Attribute type of group, role, or organization	The value can be any one of the following: ■ For groups: cn ■ For roles: cn

After you specify values for these scheduled task attributes, proceed to Step 10 of the procedure to create scheduled tasks.

User Reconciliation Scheduled Task You must specify values for the following attributes of the user reconciliation scheduled task.

Note: Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.

Attribute	Description	Default/Sample Value
ITResourceName	Name of the IT resource for setting up a connection with the Sun Java System Directory server	iPlanet User
ResourceObjectName	Name of the resource object in which users are reconciled	iPlanet User
XLDeleteUsersAllowed	If this attribute is set to True, then the Delete reconciliation event is started. Users who are deleted from the target system are removed from Oracle Identity Manager. This requires all the users on the target system to be compared with all the users in Oracle Identity Manager. If this attribute is set to False, then users deleted from the target system are not deleted from Oracle Identity Manager. **Note:** This process affects performance.	True
UserContainer	DN value from where the users are reconciled from the target system to Oracle Identity Manager	ou=user
TrustedSource	Configurable option for trusted reconciliation The value can be True or False.	False
Xellerate Type	Default Xellerate Type for the Xellerate User	End-User Administrator
Password	Default password for the Xellerate User	Dummy123
Organization	Default organization for the Xellerate User	Xellerate Users
Role	Default role for the Xellerate User	Consultant
IsIPlanetTarget	Specifies whether the target system is Sun Java System Directory or Siemens HiPath Slcurity DirX	■ For Sun Java System Directory, specify true as the value of this attribute. ■ For Siemens HiPath Slcurity DirX, do not specify any value for this attribute. Leave the field blank.

After you specify values for these scheduled task attributes, proceed to Step 10 of the procedure to create scheduled tasks.

Configuring the Lookup Definition for Reconciliation with Siemens HiPath Slcurity DirX

If you are using Siemens HiPath Slcurity DirX as the target system, then you must make the following change in the AttrName.Recon.Map.iPlanet lookup definition:

See Also: *Oracle Identity Manager Design Console Guide* for information about modifying lookup definitions

1. In the Design Console, open the `AttrName.Recon.Map.iPlanet` lookup definition.
2. In this lookup definition, search for the `ldapUserDisableAttr` code key. The current decode value of this code key is `nsaccountlock`.
3. Change the decode value to `activeEntry`.
4. Save the changes.

Step 6: Compiling Adapters

The following adapters are imported into Oracle Identity Manager when you import the connector XML file:

- `iPlanet Create User`
- `iPlanet Delete User`
- `iPlanet Modify User`
- `iPlanet Move User`
- `iPlanet Add User to Group`
- `iPlanet Remove User from Group`
- `iPlanet Add Role to User`
- `iPlanet Remove Role from User`
- `iPlanet PP String`

You must compile these adapters before you can use them to provision accounts on the target system.

To compile adapters by using the Adapter Manager form:

1. Open the Adapter Manager form.
2. To compile all the adapters that you import into the current database, select **Compile All**.

   To compile multiple (but not all) adapters, select the adapters you want to compile. Then, select **Compile Selected**.

   Note: Click **Compile Previously Failed** to recompile only those adapters that were not compiled successfully. Such adapters do not have an `OK` compilation status.

3. Click **Start.** Oracle Identity Manager compiles the selected adapters.
4. If Oracle Identity Manager is installed in a clustered environment, then copy the compiled adapters from the *`OIM_home`*`\xellerate\Adapter` directory to the same directory on each of the other nodes of the cluster. If required, overwrite the adapter files on the other nodes.

To view detailed information about an adapter:

1. Highlight the adapter in the Adapter Manager form.
2. Double-click the row header of the adapter, or right-click the adapter.
3. Select **Launch Adapter** from the shortcut menu that is displayed. Details of the adapter are displayed.

Note: To compile one adapter at a time, use the Adapter Factory form. Refer to *Oracle Identity Manager Tools Reference Guide* for information about using the Adapter Factory and Adapter Manager forms.

Step 7: Configuring SSL

Note: This is an optional step of the deployment procedure.

To enable SSL connectivity between the connector and the target Sun Java System Directory server:

1. Import the certificate from the target system into the JSDK (the JSDK that is used during installation of Oracle Identity Manager) `cacerts` keystore as follows:

   ```
   keytool -import -alias alias_name -file
   certificate_file_name_with_complete_path -keystore
   java_home\jre\lib\security\cacerts
   ```

   Here, *java_home* is the directory in which JDK is installed.

2. Restart the Oracle Identity Manager server.
3. In the `iPlanet User` IT Resource:
   - Set the `SSL` parameter value to `true`.
   - Set the `Port` parameter value to the SSL port number. Typically, this number is 636.

Configuring the Connector for Multiple Installations of the Target System

Note: Perform this procedure only if you want to configure the connector for multiple installations of Sun Java System Directory. Refer to *Oracle Identity Manager Design Console Guide* for detailed instructions on performing each step of this procedure.

To configure the connector for multiple installations of the target system:

1. Create and configure one resource object for each target system installation.

   The Resource Objects form is in the Resource Management folder. The `iPlanet User` resource object is created when you import the connector XML file. You can use this resource object as the template for creating the remaining resource objects.

2. Create and configure one IT resource for each resource object.

   The IT Resources form is in the Resource Management folder. The `iPlanet User` IT resource is created when you import the connector XML file. You can use this IT resource as the template for creating the remaining IT resources, of the same resource type.

3. Design one process form for each resource object.

   The Form Designer form is in the Development Tools folder. The following process forms are created when you import the connector XML file:

- UD_IPNT_USR (main form)
- UD_IPNT_ROL (child form for multivalue attributes)
- UD_IPNT_GRP (child form for multivalue attributes)

You can use these process forms as templates for creating the remaining process forms.

4. Create and configure one process definition for each resource object.

   The Process Definition form is in the Process Management folder. The iPlanet User process definition is created when you import the connector XML file. You can use this process definition as the template for creating the remaining process definitions.

   While creating process definitions for each target system installation, the following steps that you must perform are specific to the creation of each process definition:

   - From the **Object Name** lookup field, select the resource object that you create in Step 1.
   - From the **Table Name** lookup field, select the process form that you create in Step 3.
   - While mapping the adapter variables for the IT Resource data type, ensure that you select the IT resource that you create in Step 2 from the **Qualifier** list.

5. Configure reconciliation for each target system installation. Refer to the "Step 5: Configuring Reconciliation" section on page 2-7 for instructions. Note that only the values of the following attributes are to be changed for each reconciliation scheduled task:

   - ITResourceName
   - ResourceObjectName
   - TrustedSource

   Set the TrustedSource attribute to True for the Sun Java System Directory installation that you want to designate as a trusted source. You can designate either a single or multiple installations of Sun Java System Directory as the trusted source. For the remaining Sun Java System Directory installations, set this attribute to False.

6. If required, modify the fields to be reconciled for the Xellerate User resource object.

When you use the Administrative and User Console to perform provisioning, you can specify the IT resource corresponding to the Sun Java System Directory installation to which you want to provision the user.

3

Testing and Troubleshooting

After you deploy the connector, you must test it to ensure that it functions as expected. This chapter discusses the following topics related to connector testing:

- Running Test Cases
- Troubleshooting

Running Test Cases

You can use the troubleshooting utility to identify the cause of problems associated with connecting to the target system and performing basic operations on the target system.

To use the troubleshooting utility:

1. Set the required values in the `TroubleShootIPlanet.properties` file.

   This file is in the *`OIM_home`*`\xellerate\troubleshoot` directory. The following table describes the sections of this file in which you must provide information for running the tests.

Section	Information
Sun Java System Directory Server connection parameters	Connection parameters required to connect to the target system Refer to the "Defining IT Resources" section on page 2-6 for information about the values that you must provide.
Create User information	Values required to create a user
Modify User information	Values required to modify a user
Delete User information	DN of the user to be deleted

2. Add the following to the `CLASSPATH` environment variable:

   ```
   OIM_home\xellerate\JavaTasks\xliIPlanet.jar
   OIM_home\xellerate\lib\xlLogger.jar
   OIM_home\xellerate\ext\log4j-1.2.8.jar
   OIM_home\xellerate\lib\xlUtils.jar
   ```

3. Create an ASCII-format copy of the `TroubleShootIPlanet.properties` file as follows:

Note: You must perform this procedure every time you make a change in the contents of the `TroubleShootIPlanet.properties` file.

a. In a command window, change to the following directory:

   OIM_home\xellerate\troubleshoot

b. Enter the following command:

   ```
   native2ascii TroubleShootIPlanet.properties global.properties
   ```

   The `global.properties` is created when you run the `native2ascii` command. The contents of this file are an ASCII-format copy of the contents of the `TroubleShootIPlanet.properties` file.

4. Perform the following tests:

   - Create a user as follows:

     ```
     java -DpropertyFile=.\global.properties
     -Dlog4j.configuration=.\log.properties TroubleShootingUtilityIPlanet
     createUser
     ```

   - Modify a user as follows:

     ```
     java -DpropertyFile=.\global.properties
     -Dlog4j.configuration=.\log.properties TroubleShootingUtilityIPlanet
     modifyUser
     ```

   - Delete a user as follows:

     ```
     java -DpropertyFile=.\global.properties
     -Dlog4j.configuration=.\log.properties TroubleShootingUtilityIPlanet
     deleteUser
     ```

Troubleshooting

The following sections list solutions to some commonly encountered errors of the following types:

- Connection Errors
- Create User Errors
- Modify User Errors
- Delete User Errors
- Reconciliation Errors

Connection Errors

The following table describes solutions to commonly encountered Create User errors.

Problem Description	Solution
Oracle Identity Manager cannot establish a connection to Sun Java System Directory. **Returned Error Message:** LDAP Connection exception **Returned Error Code:** `INVALID_CONNECTION_ERROR`	■ Ensure that Sun Java System Directory is running. ■ Ensure that Oracle Identity Manager is running (that is, the database is running). ■ Ensure that all the adapters have been compiled. ■ Examine the Oracle Identity Manager record (from the IT Resources form). Verify that the specified IP address, admin ID, and admin password are correct.
Target not available **Returned Error Message:** Connection error - unable to create initial LDAP context. **Returned Error Code** `TARGET_UNAVAILABLE_ERROR`	Ensure that the specified Sun Java System Directory server connection values are correct.
Authentication error **Returned Error Messages** Connection error - unable to create Initial LDAP **Returned Error Code** `AUTHENTICATION_ERROR`	Ensure that the specified Sun Java System Directory server connection values are correct.

Create User Errors

The following table describes solutions to commonly encountered Create User errors.

Problem Description	Solution
Oracle Identity Manager cannot create a user. **Returned Error Message:** Required information missing **Returned Error Code:** `INSUFFICIENT_INFORMATION_PROVIDED`	■ Ensure that the IP address, admin ID, and admin password are correct. ■ Ensure that the following information is provided: User ID User password User container User first name User last name
Oracle Identity Manager cannot create a user. **Returned Error Message:** User already exists **Returned Error Code:** `USER_ALREADY_EXIST`	Check if a user with the specified ID already exists in Sun Java System Directory. Assign a new ID for this user, and try again.

Problem Description	Solution
Oracle Identity Manager cannot create a user. **Returned Error Message:** Connection error - unable to create initial LDAP context **Returned Error Code:** `INVALID_NAMING_ERROR`	■ Check if the specified Sun Java System Directory connection values are correct. ■ Check if an attribute value violates the schema definition.
Oracle Identity Manager cannot create a user. **Returned Error Message:** User creation failed **Returned Error Code:** `USER_CREATION_FAILED`	Check if an attribute value violates the schema definition.
The Create User operation failed because a value was being added to a nonexistent attribute. **Returned Error Message:** Attribute does not exist **Returned Error Code:** `ATTRIBUTE_DOESNOT_EXIST`	In the `AttrName.Prov.Map.iPlanet` lookup definition, check if the decode values are valid attribute names in the target system.
The Create User operation failed because an invalid value was being added. **Returned Error Message:** Invalid value specified for an attribute **Returned Error Code:** `INVALID_ATTR_VALUE_ERROR`	Check the values specified during user creation.

Modify User Errors

The following table describes solutions to commonly encountered Modify User errors.

Problem Description	Solution
Oracle Identity Manager cannot modify the attribute value of a user. **Returned Error Message:** Invalid attribute value or state **Returned Error Code:** `INVALID_ATTR_MODIFY_ERROR`	Check the specified user ID.
The Modify User operation failed because a value was being added to a nonexistent attribute. **Returned Error Message:** Attribute does not exist **Returned Error Code:** `ATTRIBUTE_DOESNOT_EXIST`	1. From the corresponding process task, get the value that is passed for `AttrName` of the connector. 2. Using the name obtained in the previous step, check in the `AttrName.Prov.Map.iPlanet` lookup definition if the decode value is a valid attribute name in the target.

Problem Description	Solution
The Modify User operation failed because an invalid value was being added. **Returned Error Message:** Invalid value specified for an attribute **Returned Error Code:** `INVALID_ATTR_VALUE_ERROR`	Check the value specified.
The Modify User operation failed because of an attempt to add a value to an attribute that does not exist in the `AttrName.Recon.Map.iPlanet` lookup definition. **Returned Error Message:** One or more attribute mappings are missing **Returned Error Code:** `ATTR_MAPPING_NOT_FOUND`	1. From the corresponding process task, get the value that is passed for `AttrName` of the connector. 2. Using the name obtained in the previous step, check if an entry has been made in the `AttrName.Recon.Map.iPlanet` lookup definition.
The operation failed because a duplicate value was being added to an attribute. **Returned Error Message:** Duplicate value **Returned Error Code:** `DUPLICATE_VALUE_ERROR`	Check the value specified.
Oracle Identity Manager cannot move a user from one container to another. **Returned Error Message:** Moving user to different container failed **Returned Error Code:** `USER_MOVE_FAILED`	Generic error. Review the log for more details.
Oracle Identity Manager cannot add a user to a security group. **Returned Error Message:** Group does not exist **Returned Error Code:** `GROUP_DOESNOT_EXIST`	The specified user security group does not exist in Sun Java System Directory. Check the group name.
Oracle Identity Manager cannot add a user to a group. **Returned Error Message:** User is already a member of this group **Returned Error Code:** `DUPLICATE_VALUE`	The user is already a member of the group.

Problem Description	Solution
Oracle Identity Manager cannot add a role to a user. **Returned Error Message:** Role does not exist **Returned Error Code:** ROLE_DOESNOT_EXIST	The specified role for the user in Oracle Identity Manager does not exist in Sun Java System Directory. Create the role in Sun Java System Directory.
Oracle Identity Manager cannot add a role to a user. **Returned Error Message:** Error while updating user info **Returned Error Code:** USER_UPDATE_FAILED	Generic error. Review the log for more details.
Oracle Identity Manager cannot add a role to a user. **Returned Error Message:** User has already been assigned this role **Returned Error Code:** DUPLICATE_VALUE	The user has already been assigned this role.
Oracle Identity Manager cannot remove a role assigned to a user. **Returned Error Message:** Removing assigned role failed **Returned Error Code:** USER_DELETE_ROLE_FAILED	Generic error. Review the log for more details.

Delete User Errors

The following table describes the solution to a commonly encountered Delete User error.

Problem Description	Solution
Oracle Identity Manager cannot delete a user. **Returned Error Message:** User does not exist in target **Returned Error Code:** USER_DOESNOT_EXIST	The specified user does not exist in Sun Java System Directory.

Reconciliation Errors

The following table describes the solution to a commonly encountered reconciliation error.

Problem Description	Solution

Oracle Identity Manager cannot reconcile users from Sun Java System Directory.
Returned Error Message:
`javax.naming.NamingException: tcUtilLDAPOperations -> : NamingException : Unable to search LDAP`
Returned Error Code:
`LDAP: error code 11 - Administrative Limit Exceeded`
	Change the Sun Java System Directory configuration as follows:
	1. Open the Sun ONE Directory Server admin console.
	2. Select **Configuration, Performance,** and **Client Control.**
	3. Set the size limit to `unlimited`.
	4. Set the look-through limit to `unlimited`.
	5. Save the changes, and restart Sun Java System Directory.

4

Known Issues

The following are known issues associated with this release of the connector:

- The user search is based on the user ID only.
- The user ID in the process form should be the same as that of the Oracle Identity Manager User login. Otherwise, reconciliation of the following operations would fail because these operations require direct API calls to update the information:
  - Enable status of user
  - Disable status of user
  - Organization update
- During provisioning, you cannot use non-English characters for the password of the user. This is because Sun Java System Directory does not support non-ASCII characters in the Password field.
- During provisioning, you cannot use non-ASCII characters for the user ID or e-mail address of the user. This is because, by default, Sun Java System Directory does not permit the entry of non-ASCII characters in the User ID and E-mail fields. If you want to enable the entry of non-ASCII characters in these fields, then you must disable the 7-bit check plug-in as follows:
  1. Open Sun ONE Directory Server.
  2. Click the **Configuration** tab.
  3. Expand **Plugins.**
  4. Select **7-bit check.**
  5. Deselect the **Enable plug-in** check box.
  6. Click **Save.**
- Some Asian languages use multibyte character sets. Because the character limit for the fields in the target system is specified in bytes, the number of Asian-language characters that you can enter in a particular field is usually less than the number of English-language characters that you can enter in the same field. The following example illustrates this limitation:

  Suppose you can enter 50 characters of English in the User Last Name field of the target system. If you were using the Japanese language, then you would not be able to enter more than 25 characters in the same field.

A

Attribute Mappings Between Oracle Identity Manager and Sun Java System Directory

The following table discusses attribute mappings between Oracle Identity Manager and Sun Java System Directory.

Oracle Identity Manager Attribute	Sun Java System Directory Attribute	Description
User ID	uid	User's login ID
First Name	givenname	First name
Last Name	sn	Last name or surname
Email	mail	E-mail address
ldapUserDisableAttr	nsaccountlock	This attribute specifies whether or not the user's account is locked. If the value is `True`, then the account is locked. If the value is `False`, then the account is not locked.
ldapOrgDNPrefix	ou	Prefix of organization entry
ldapUserDNPrefix	uid	Prefix of user entry
ldapUserUniqueAttr	uid	Unique attribute of user
Middle Name	initials	Middle name
ldapUserObjectClass	inetorgperson	User is represented by the inetOrgPerson object class
GroupName	uniquemember	This is the multivalued attribute for the group object. Its value is a list of user IDs of all the users in the group.
RoleName	nsroledn	Customized object class for role
UserGroup	groupOfUniqueNames	Group represented object class
UserRole	customOrganizationalRole	Role represented object class
ldapUserDNPrefix	uid	User ID of an entry
ldapObjectClass	objectclass	Object classes are used to group information
ldapGroupDNPrefix	cn	Common name of an entry (for example, organization, user, role, or group)
Title	title	User's title
Location	l	City of office address
Telephone	telephoneNumber	Office telephone number

Oracle Identity Manager Attribute	Sun Java System Directory Attribute	Description
Department	departmentnumber	Department name
Communication Language	preferredlanguage	Preferred language for communication
ldapPassword	userpassword	Password
ldapTargetResourceTimeStampField	modifytimestamp	Time stamp of the last modification
ldapRoleDNPrefix	cn	Common name of an entry (for example, organization, user, role, or group)
ldapRoleMemberName	nsroledn	Members to whom the role has been assigned
ldapOrgDNPrefix	ou	Common name of an entry (for example, organization, user, role, or group)
ldapUserObjectClass	inetorgperson	Object class for the user
ldapRoleObjectClass	ldapsubentry	Object class of the role
ldapOrgPersonObject	OrganizationalPerson	Required object class for the user of any organization

Index

O

P

R

S

T

U

X