

# **Oracle® Identity Manager**

Connector Guide for UNIX Telnet

Release 9.0.4

**E10177-01**

May 2007

Copyright © 1991, 2007, Oracle. All rights reserved.

Primary Authors: Debapriya Datta, Shiladitya Guha

Contributing Authors: Don Gosselin, Lyju Vadassery

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software--Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

Oracle, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

---

---

# Contents

<b>Preface</b> .....	v
Audience .....	v
Documentation Accessibility .....	v
Related Documents .....	vi
Documentation Updates .....	vi
Conventions .....	vi
 <b>What's New in the Oracle Identity Manager Connector for UNIX Telnet?</b> .....	vii
Software Updates .....	vii
Documentation-Specific Updates .....	viii
 <b>1 About the Connector</b>	
<b>Reconciliation Module</b> .....	1-1
Reconciled Xellerate User Fields .....	1-2
<b>Provisioning Module</b> .....	1-2
<b>Supported Functionality</b> .....	1-3
<b>Multilanguage Support</b> .....	1-4
<b>Files and Directories That Comprise the Connector</b> .....	1-5
<b>Determining the Release Number of the Connector</b> .....	1-6
Before Deployment .....	1-6
After Deployment .....	1-6
 <b>2 Deploying the Connector</b>	
<b>Step 1: Verifying Deployment Requirements</b> .....	2-1
<b>Step 2: Configuring the Target System</b> .....	2-2
Configuration Steps for Solaris and Linux .....	2-2
Configuration Steps for AIX .....	2-3
Configuration Steps for HP-UX .....	2-3
<b>Step 3: Copying the Connector Files</b> .....	2-3
<b>Step 4: Configuring the Oracle Identity Manager Server</b> .....	2-4
Changing to the Required Input Locale .....	2-4
Clearing Content Related to Connector Resource Bundles from the Server Cache .....	2-4
Enabling Logging .....	2-5
<b>Step 5: Importing the Connector XML Files</b> .....	2-7
Defining IT Resources .....	2-8

### **3 Configuring the Connector**

<b>Configuring Reconciliation</b> .....	3-1
Partial Reconciliation .....	3-1
Batched Reconciliation .....	3-2
Configuring System Properties .....	3-2
Configuring Trusted Source Reconciliation .....	3-3
Configuring the Reconciliation Scheduled Tasks.....	3-3
Specifying Values for the Scheduled Task Attributes .....	3-4
Enabling Reconciliation in Oracle Identity Manager Release 9.0.1 .....	3-6
Adding Custom Attributes for Reconciliation.....	3-6
<b>Configuring Provisioning</b> .....	3-8
Compiling Adapters .....	3-8
Adding Custom Attributes for Provisioning .....	3-9
<b>Configuring the Connector for Multiple Installations of the Target System</b> .....	3-12

### **4 Testing and Troubleshooting**

### **5 Known Issues**

### **A Attribute Mappings Between Oracle Identity Manager and UNIX Telnet**

### **Index**

---

---

# Preface

*Oracle Identity Manager Connector Guide for UNIX Telnet* provides information about integrating Oracle Identity Manager with target systems running AIX, HP-UX, Linux, and Solaris, using the Telnet protocol.

---

---

**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 UNIX Telnet.

## 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 Connector Pack Release 9.0.4 documentation library, 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
<b>boldface</b>	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
<code>monospace</code>	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 UNIX Telnet?

This chapter provides an overview of the updates made to the software and documentation for the UNIX Telnet connector in release 9.0.4 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.

### Enabling Logging

By following the instructions in the "[Enabling Logging](#)" section on page 2-5, you can configure the generation of log information that is specific to the target system.

### Partial Reconciliation

You can customize the reconciliation process by specifying the subset of added or modified target system records that must be reconciled. This feature is described in the "[Partial Reconciliation](#)" section on page 3-1.

### Batched Reconciliation

In this release of the connector, user reconciliation scheduled task is added with attributes such as `BatchSize` and `NumberOfBatches`. By specifying values for these attributes, you can reconcile users in various batches. These attributes are discussed in the "[Batched Reconciliation](#)" section on page 3-2.

### **Configuring Trusted Source Reconciliation**

From this release onward, you can configure trusted source reconciliation for this target system by importing the `XellTelnetUser.xml` file. The procedure is described in the "[Configuring Trusted Source Reconciliation](#)" section on page 3-3.

### **Separate Scheduled Tasks for Trusted and Nontrusted Source Reconciliation**

In this release of the connector, there are separate user reconciliation scheduled tasks for trusted and nontrusted source reconciliation. In the "[Specifying Values for the Scheduled Task Attributes](#)" section on page 3-4, the attributes of these scheduled tasks are described.

### **Timeout Support**

This release of the connector provides timeout support for provisioning and reconciliation. In the "[Defining IT Resources](#)" section on page 2-8, the IT resource parameters that are used to implement this feature are described.

### **Testing Utility**

The testing utility has been added in this release of the connector. You will find information about the files that constitute this utility and the procedure to use it in the following sections of this guide:

- [Files and Directories That Comprise the Connector](#) on page 1-5
- [Step 3: Copying the Connector Files](#) on page 2-3
- [Chapter 4, "Testing and Troubleshooting"](#)

### **Changes in the Connector Files**

The "[Files and Directories That Comprise the Connector](#)" section on page 1-5 reflects the changes made to the connector files and directories.

### **Adding Custom Attributes**

This release of the connector supports the adding of custom attributes for reconciliation and provisioning. This feature is described in the "[Adding Custom Attributes for Reconciliation](#)" section on page 3-6 and the "[Adding Custom Attributes for Provisioning](#)" section on page 3-9.

## **Documentation-Specific Updates**

The following documentation-specific updates have been made in this release of the guide:

- Instructions in the "[Files and Directories That Comprise the Connector](#)" section on page 1-5 have been revised.
- Some of the content from the Chapter 2 in earlier releases of this guide has been moved to [Chapter 3](#).



---

## 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 Telnet is used to integrate Oracle Identity Manager with target systems running AIX, HP-UX, Linux, and Solaris, using the Telnet protocol.

---

**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:

- [Reconciliation Module](#)
- [Provisioning Module](#)
- [Supported Functionality](#)
- [Multilanguage Support](#)
- [Files and Directories That Comprise the Connector](#)
- [Determining the Release Number of the Connector](#)

### Reconciliation Module

**Reconciliation** involves duplicating in Oracle Identity Manager additions of and modifications to user accounts on the target system. It is an automated process initiated by a scheduled task that you configure.

**See Also:** The "Deployment Configurations of Oracle Identity Manager" section in *Oracle Identity Manager Connector Framework Guide* for conceptual information about reconciliation configurations

The following target system attributes are reconciled:

- User Login
- User UID
- Primary Group Name
- Default Shell
- Home Directory

- GECOS
- Password Change Time
- Account Expiry Date

---

**Note:** For a trusted configuration (such as the HP-UX trusted mode), the Password Change Time and Account Expiry Date fields are not reconciled.

---

## Reconciled Xellerate User Fields

The following target system fields are reconciled only if trusted source reconciliation is implemented:

- User ID
- First Name
- Last Name
- Organization
- User Type
- Employee Type

## Provisioning Module

**Provisioning** involves creating or modifying a user's account information on the target system through Oracle Identity Manager. You use the Administrative and User Console to perform provisioning operations.

**See Also:** The "Deployment Configurations of Oracle Identity Manager" section in *Oracle Identity Manager Connector Framework Guide* for conceptual information about provisioning

For this target system, the following fields are provisioned:

- User Login
- Password
- Secondary Group Names
- User UID
- Primary Group Name
- Default Shell
- GECOS
- Home Directory
- Account Expiry Date
- Password Change Time
- Create Home Directory
- Skeleton Directory
- Inactive Days

## Supported Functionality

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

Function	Type	Description
Create User	Provisioning	<p>Creates a user</p> <p>When you use this function, in the User Defined process form:</p> <ul style="list-style-type: none"> <li>On Solaris, the value in the Secondary Group Names field must be different from the value in the Primary Group Name field.</li> <li>On HP-UX, the Inactive Account field must be populated only when the UNIX server is configured in trusted mode.</li> <li>Before populating the Skeleton directory field, data must be populated in the Home Directory field and the Create Home Directory check box must also be selected.</li> <li>While specifying a value in the GECOS field, ensure that there are no spaces.</li> </ul>
Delete User	Provisioning	Deletes a provisioned user on the UNIX server
Update User UID	Provisioning	Updates user properties according to a change in the User UID attribute
Update User Group	Provisioning	Updates user properties according to a change in the User Group attribute
Update User Password Change Time	Provisioning	Updates user properties according to a change in the User Password Change Time attribute
Update Shell	Provisioning	Updates user properties according to a change in the Shell attribute
Update Home Directory	Provisioning	Updates user properties according to a change in the Home Directory attribute
Update Account Expiry Date	Provisioning	Updates user properties according to a change in the Account Expiry Date attribute
Update User GECOS	Provisioning	Updates user properties according to a change in the User GECOS attribute
Set Password	Provisioning	<p>Updates user properties according to a change in the Password attribute</p> <p>The changed password must conform to the password policy requirements of the target system.</p>
Update Secondary Group Names	Provisioning	<p>Updates user properties according to a change in the Secondary Group Names attribute</p> <p>Do not update the User Login field when you update the Secondary Group Names value.</p> <p>When you specify the secondary group name for the first time and then run this function, the primary group name is assigned the same value as the secondary group name. However, after the value of the primary group name is changed, you cannot set the secondary group name to the same value.</p> <p>On Solaris, the value of the Secondary Group Names field in the User Defined process form must always be different from the value of the Primary Group Name field.</p>
Update Inactive Days	Provisioning	<p>Updates user properties according to a change in the Update Inactive Days attribute</p> <p>This function is not supported on AIX 5.2.</p>

Function	Type	Description
Update User Login	Provisioning	<p>Updates user properties according to a change in the User Login attribute</p> <p>Do not update the Secondary Group Names field when you update the User Login field.</p> <p>On AIX 5.2, if the User GECOS value contains spaces, then this function does not work.</p>
Disable User	Provisioning	<p>Disables an existing user on the UNIX server</p> <p><b>Note:</b> Suppose that a user on the UNIX server is disabled. If the Set Password function is run on this user account, then the account is automatically reenabled.</p>
Enable User	Provisioning	<p>Enables a disabled existing user on the UNIX server</p> <p>Before running this function, the Set Password function must be run.</p> <p>This function is not supported on an HP-UX (trusted) server.</p>
Trusted Reconciliation for User	Reconciliation	Creates Xellerate User accounts corresponding to the reconciled user accounts from the UNIX server
Create User	Reconciliation	Reconciles user accounts from the UNIX server
Update User	Reconciliation	Updates the attributes of previously reconciled user accounts from the UNIX server
Delete User	Reconciliation	Reconciles user accounts that have been deleted from the UNIX server

## Multilanguage Support

The connector supports the following languages:

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

---

**Note:** The connector does not support the entry of multibyte characters in some of the fields. [Appendix A, "Attribute Mappings Between Oracle Identity Manager and UNIX Telnet"](#) provides information about the fields in which multibyte characters are not supported.

---

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

## 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:

Operating Systems/UNIX/UNIX Telnet

These files and directories are listed in the following table.

File in the Installation Media Directory	Description
ext/sshfactory.jar	This file contains the JScape libraries. These libraries are used to open an Telnet session with the target server.
lib/xliTelnet.jar	This file contains the Java classes that are required to support provisioning and reconciliation in Telnet.
Files in the resources directory	Each of these resource bundle files contains language-specific information that is used by the connector.  <b>Note:</b> A <b>resource bundle</b> 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.
test/config/config.properties	This file is used to specify the parameters and settings required to connect to the target system by using the testing utility.
test/config/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 testing utility.
test/config/userAttribute_NonAIX_prov.properties	This file contains the parameters required for dynamic provisioning on non-AIX platforms.
test/config/userAttribute_AIX_prov.properties	This file contains the parameters required for dynamic provisioning on AIX platform.
test/config/userAttribute_NonAIX_recon.properties	This file contains the parameters required for dynamic reconciliation on non-AIX platforms.
test/config/userAttribute_AIX_recon.properties	This file contains the parameters required for dynamic reconciliation on AIX platform.
test/lib/xliTelnetTest.jar	This file contains the Java classes required to run the client for running test calls from the Oracle Identity Manager server.
test/scripts/Telnet.bat test/scripts/telnet.sh	This file contains the script required to run the client for running test calls from the Oracle Identity Manager server.
xml/TelnetNonTrustedUser.xml	This file contains definitions for the following Telnet User components of the connector: <ul style="list-style-type: none"> <li>■ Telnet User IT resource type</li> <li>■ Custom process form</li> <li>■ Process task and rule generator adapters (along with their mappings)</li> <li>■ Resource object</li> <li>■ Provisioning process</li> <li>■ Pre-populate rules that are used with this connector</li> </ul>
xml/XellTelnetUser.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 `test` directory are used only to run tests on the connector.

---

---

The "[Step 3: Copying the Connector Files](#)" section on page 2-3 provides instructions to copy these files into the required directories.

## Determining the Release Number of the Connector

You can use any one of the following methods to determine the release number of the connector.

### Before Deployment

To determine the release number of a connector:

1. Extract the contents of the `xliTelnet.jar` file. This file is in the following directory on the installation media:  
  
`Operating Systems/UNIX/UNIX Telnet/lib`
2. Open the `manifest.mf` file in a text editor. The `manifest.mf` file is one of the files bundled inside the `xliTelnet.jar` file.

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

---

---

**Note:** If you maintain a copy of the `xliTelnet.jar` file after deployment, you can use this method to determine the release number of the connector at any stage. After you deploy the connector, it is recommended that you use the "After Deployment" method, which is described in the following section.

---

---

### After Deployment

To determine the release number of a connector that has already been deployed:

**See Also:** *Oracle Identity Manager Design Console Guide*

1. Open the Oracle Identity Manager Design Console.
2. In the Form Designer, open the process form. The release number of the connector is the value of the **Version** field.

---

## Deploying the Connector

Deploying the connector involves the following steps:

- [Step 1: Verifying Deployment Requirements](#)
- [Step 2: Configuring the Target System](#)
- [Step 3: Copying the Connector Files](#)
- [Step 4: Configuring the Oracle Identity Manager Server](#)
- [Step 5: Importing the Connector XML Files](#)

### 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	The target system can be any one of the following: <ul style="list-style-type: none"><li>■ Solaris 8 - 10</li><li>■ HP-UX 11.11 (trusted/nontrusted)</li><li>■ Linux (Red Hat Advanced Server 2.1, Red Hat Enterprise Linux 3.x, or Red Hat Linux 4.x)</li><li>■ AIX 4.3, AIX 5.1 - 5.3</li></ul>
External code	JSCAPE Telnet/SSH Libraries (SSH factory)
Other systems	Operating system patches (HP-UX)
Target system user account	root <p>You provide the credentials of this user account while performing the procedure in the <a href="#">"Defining IT Resources"</a> section on page 2-8.</p> <p>If you do not provide the credentials of this user account, then the "Insufficient rights or privileges" message is displayed when Oracle Identity Manager tries to communicate with the target system.</p>

Item	Requirement
Character encoding (en_US) supported by the target system	<p>The target system must support en_US character encoding standards such as UTF-8 and iso8859.</p> <p>Use the following command to check the en_US character encoding standards that the target system supports:</p> <pre>locale -a</pre> <p><b>Note:</b> If the target system does not support any of the en_US character encoding standards, then you must install the en_US language pack.</p>

The supported shell types for various operating systems are given in the following table.

Solaris	HP-UX	Linux	AIX
sh	csch	ksh	csch
csch	ksh	bash	ksh
-	sh	sh	sh
-	-	csch	-

## Step 2: Configuring the Target System

This section provides instructions to configure the target system on the following platforms:

- [Configuration Steps for Solaris and Linux](#)
- [Configuration Steps for AIX](#)
- [Configuration Steps for HP-UX](#)

### Configuration Steps for Solaris and Linux

Perform the following steps for Solaris and Linux environments:

1. Ensure that the `/etc/passwd` and `/etc/shadow` files are available on the UNIX server.
2. Ensure that a `passwd` mirror file is created on the target server by using a command similar to the following:

```
cp /etc/passwd /etc/passwd1
```

The same file name with the path must be inserted in the `Password Mirror File/User Mirror File (AIX)` attribute of the reconciliation scheduled task.

3. Ensure that a `shadow` mirror file is created on the target server by using a command similar to the following:

```
cp /etc/shadow /etc/shadow1
```

The name and path of this file must be specified for the `Shadow Mirror File` attribute of the reconciliation scheduled task.



## Configuration Steps for AIX

Perform the following steps for AIX environments:

1. Ensure that the `/etc/passwd` and `/etc/security/user` files are available on the server.
2. Ensure that a user mirror file is created on the server by using a command similar to the following:

```
lsuser -c -a id pgrp gecost home shell expires maxage ALL |
tr '#' ' ' > /mainUserFile1
```

The name and path of this file must be specified for the `Passwd Mirror File/User Mirror File (AIX)` attribute of the scheduled task for reconciliation.

## Configuration Steps for HP-UX

Perform the following steps for HP-UX environments:

1. Log in as root and then run the following command:

```
/usr/bin/sam
```

2. Select **Auditing and Security** and **System Security Policies**. A message is displayed asking if you want to switch to the trusted mode.
3. Click **OK**.

If the following message is displayed, then skip the next step:

```
System changed successfully to trusted system
```

4. Ensure that the `/etc/passwd` and `/etc/shadow` directories are available on the target server.

If the shadow file does not exist, then follow the installation instructions at

<http://docs.hp.com/en/5991-0909/index.html>

All the patches are available in the HP patch database, which you can download from

<http://www5.itrc.hp.com/>

## Step 3: 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:

Operating Systems/UNIX/UNIX Telnet

Refer to the "[Files and Directories That Comprise the Connector](#)" section on page 1-5 for more information about these files.

---

---

File in the Installation Media Directory	Destination Directory
ext/sshfactory.jar	<i>OIM_home</i> /xellerate/ThirdParty
lib/xliTelnet.jar	<i>OIM_home</i> /xellerate/JavaTasks
lib/xliTelnet.jar	<i>OIM_home</i> /xellerate/ScheduleTask
Files in the resources directory	<i>OIM_home</i> /xellerate/connectorResources
Files in the test directory	<i>OIM_home</i> /xellerate/XLIntegrations/Telnet
Files in the xml directory	<i>OIM_home</i> /xellerate/XLIntegrations/Telnet/xml

---

**Note:** 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 4: 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.

You may require the assistance of the system administrator to change to the required input locale.

### Clearing Content Related to Connector Resource Bundles from the Server Cache

While performing the instructions described in the "[Step 3: Copying the Connector Files](#)" section on page 2-3, you copy files from the `resources` directory on the installation media into the *OIM\_home*/xellerate/connectorResources directory. Whenever you add a new resource bundle in the `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.

---

**Note:** You must perform Step 1 before you perform Step 2. If you run the command described in Step 2 as follows, then an exception is thrown:

---

```
OIM_home\xellerate\bin\batch_file_name
```

---

**2. Enter one of the following commands:**

- On Microsoft Windows:

```
PurgeCache.bat ConnectorResourceBundle
```

- On UNIX:

```
PurgeCache.sh ConnectorResourceBundle
```

---

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

---

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
```

## 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 depends on the application server that you use:

- **BEA WebLogic**

To enable logging:

1. Add the following line in the *OIM\_home/xellerate/config/log.properties* file:  

```
log4j.logger.Adapter.TELNETSSH=log_level
```
2. In this line, replace *log\_level* with the log level that you want to set.

For example:

```
log4j.logger.Adapter.TELNETSSH=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*

- **IBM WebSphere**

To enable logging:

1. Add the following line in the *OIM\_home/xellerate/config/log.properties* file:  

```
log4j.logger.Adapter.TELNETSSH=log_level
```
2. In this line, replace *log\_level* with the log level that you want to set.

For example:

```
log4j.logger.Adapter.TELNETSSH=INFO
```

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

*WebSphere\_home/AppServer/logs/server\_name/startServer.log*

- **JBoss Application Server**

To enable logging:

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

```
<category name="Adapter.TELNETSSH">  
  <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="Adapter.TELNETSSH">  
  <priority value="INFO"/>  
</category>
```

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

*JBoss\_home/server/default/log/server.log*

- **OC4J**

To enable logging:

1. Add the following line in the `OIM_home/xellerate/config/log.properties` file:  
`log4j.logger.Adapter.TELNETSSH=log_level`
2. In this line, replace `log_level` with the log level that you want to set.

For example:

```
log4j.logger.Adapter.TELNETSSH=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 5: Importing the Connector XML Files

To import the connector XML files into Oracle Identity Manager:

---

**Note:** If you do not import the connector files in the specified order, then the connector may not work.

---

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 `TelnetNonTrustedUser.xml` file, which is in the `OIM_home/xellerate/XLIntegrations/Telnet/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 `Telnet server-Solaris` IT resource is displayed.
8. Specify values for the parameters of the `Telnet server-Solaris` IT resource. Refer to the table in the ["Defining IT Resources"](#) section on page 2-8 for information about the values to be specified.
9. Click **Next**. The Provide IT Resource Instance Data page for a new instance of the `TELNET 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 on the Import page. You *may* see a cross-shaped icon along with some nodes. These nodes represent Oracle Identity Manager entities that are redundant. Before you import the connector XML file, you must remove these entities by right-clicking each node and then selecting **Remove**.

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

13. Perform the same procedure to import the `XLITelnetSchedulerTask_DM.xml` file, which is in the `OIM_home/xellerate/XLIntegrations/Telnet/xml` directory.

After you import the connector XML files, proceed to the next chapter.

## Defining IT Resources

You must specify values for the Telnet server- Solaris IT resource parameters listed in the following table.

Parameter	Description
Admin UserId	User ID of the administrator root
Admin Password	Password of the administrator dead_line
Server IP Address	Server IP address
Port	The port at which the Telnet service is running on the server Default value: 22
Server OS	Specify one of the following: <ul style="list-style-type: none"> <li>■ AIX</li> <li>■ HP-UX</li> <li>■ SOLARIS</li> <li>■ LINUX</li> </ul>
Shell Prompt	# or \$
Login Prompt	Login prompt that is displayed when you log in to the server login:
Password Prompt	Password prompt that is displayed when you log in to the server Password:
Whether Trusted System (HP-UX)	YES (for trusted HP-UX System) or NO (for nontrusted HP-UX system)
Target Locale	Target locale The following are sample values: <ul style="list-style-type: none"> <li>■ en_US for English</li> <li>■ ja_JP for Japanese</li> <li>■ fr_FR for French</li> </ul> <b>Note:</b> You must not make any change (uppercase or lowercase) in the value that you specify.

Parameter	Description
Supported Character Encoding (en_US) - Target	Encoding format for the en_US target locale The default value is UTF-8. <b>Note:</b> You can check which en_US encoding formats the target system supports by using the following command: <code>locale -a</code>
Max Retries	Number of times that the UNIX Telnet connector should retry connecting to the target server if the connection fails Default value: 2
Delay	Delay (in milliseconds) before the connector attempts to retry connecting to the target system, in case the connection fails Default value: 10000
Timeout	Value of the timeout (in milliseconds) for the connection to the target server Default value: 20000

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





---

## Configuring the Connector

After you deploy the connector, you must configure it to meet your requirements. This chapter discusses the following connector configuration procedures:

---

**Note:** These sections provide both conceptual and procedural information about configuring the connector. It is recommended that you read the conceptual information before you perform the procedures.

---

- [Configuring Reconciliation](#)
- [Configuring Provisioning](#)
- [Configuring the Connector for Multiple Installations of the Target System](#)

### Configuring Reconciliation

As mentioned earlier in this guide, reconciliation involves duplicating in Oracle Identity Manager additions of and modifications to user accounts on the target system. This section discusses the following topics related to configuring reconciliation:

- [Partial Reconciliation](#)
- [Batched Reconciliation](#)
- [Configuring System Properties](#)
- [Configuring Trusted Source Reconciliation](#)
- [Configuring the Reconciliation Scheduled Tasks](#)
- [Enabling Reconciliation in Oracle Identity Manager Release 9.0.1](#)
- [Adding Custom Attributes for Reconciliation](#)

### Partial Reconciliation

By default, all target system records that are added or modified after the last reconciliation run are reconciled during the current reconciliation run. You can customize this process by specifying the subset of added or modified target system records that must be reconciled. You do this by creating filters for the reconciliation module.

Creating a filter involves specifying a value for the `UserNameFilter` scheduled task attribute, which will be used in the query SELECT criteria to retrieve the records to be

reconciled. For example, if you specify the value `JDoe` for this attribute, then all target system user records with the user name `JDoe` are reconciled.

While deploying the connector, follow the instructions in the ["Specifying Values for the Scheduled Task Attributes"](#) section on page 3-4 to specify values for these attributes and the logical operator that you want to apply.

## Batched Reconciliation

During a reconciliation run, all changes in the target system records are reconciled into Oracle Identity Manager. Depending on the number of records to be reconciled, this process may require a large amount of time. In addition, if the connection breaks during reconciliation, then the process would take longer to complete.

You can configure batched reconciliation to avoid these problems.

To configure batched reconciliation, you must specify values for the following user reconciliation scheduled task attributes:

- **BatchSize:** Use this attribute to specify the number of records that must be included in each batch. The default value is 1000.
- **NumberOfBatches:** Use this attribute to specify the total number of batches that must be reconciled. The default value is `All`.

If you specify a value other than `All`, then some of the newly added or modified user records may not get reconciled during the current reconciliation run. The following example illustrates this:

Suppose you specify the following values while configuring the scheduled tasks:

- **BatchSize:** 20
- **NumberOfBatches:** 10

Suppose that 314 user records were created or modified after the last reconciliation run. Of these 314 records, only 200 records would be reconciled during the current reconciliation run. The remaining 114 records would be reconciled during the next reconciliation run.

You specify values for the `BatchSize` and `NumberOfBatches` attributes by following the instructions described in the ["Specifying Values for the Scheduled Task Attributes"](#) section on page 3-4.

## Configuring System Properties

To configure system properties:

1. Open the Oracle Identity Manager Design Console.
2. Navigate to the System Configuration page.
3. Check if there is an entry for "Default date format." If this entry is not there, then perform Step 4.
4. Add a new entry in the Server category:
  - **Name:** `Default date format`
  - **Keyword:** `XL.DefaultDateFormat`
  - **Value:** `yyyy/MM/dd hh:mm:ss z`
5. Click **Save**.

## Configuring Trusted Source Reconciliation

While configuring the connector, the target system can be designated as a trusted source or a target resource. If you designate the target system as a **trusted source**, then both newly created and modified user accounts are reconciled in Oracle Identity Manager. If you designate the target system as a **target resource**, then only modified user accounts are reconciled in Oracle Identity Manager.

---

**Note:** You can skip this section if you do not want to designate the target system as a trusted source for reconciliation.

---

Configuring trusted source reconciliation involves the following steps:

1. Import the XML file for trusted source reconciliation, `XellTelnetUser.xml`, by using the Deployment Manager. This section describes the procedure to import the XML file.

---

**Note:** Only one target system can be designated as a trusted source. If you import the `XellTelnetUser.xml` file while you have another trusted source configured, then both connector reconciliations would stop working.

---

2. Specify values for the attributes of the `TELNET User Trusted Reconciliation task` scheduled task. This procedure is described later in this guide.

To import the XML file for trusted source reconciliation:

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 `XellTelnetUser.xml` file, which is in the `OIM_home/xellerate/XLIntegrations/Telnet/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**.

## Configuring the Reconciliation Scheduled Tasks

When you perform the procedure described in the ["Step 5: Importing the Connector XML Files"](#) section on page 2-7, the scheduled tasks for lookup fields, trusted source user, and nontrusted user reconciliations are automatically created in Oracle Identity Manager. To configure these scheduled tasks:

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.
5. 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 user-configurable attributes of the scheduled task. Refer to the ["Specifying Values for the Scheduled Task Attributes"](#) section on page 3-4 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.

After you create the scheduled task, proceed to the ["Enabling Reconciliation in Oracle Identity Manager Release 9.0.1"](#) section on page 3-6.

### Specifying Values for the Scheduled Task Attributes

Depending on whether you want to implement trusted or nontrusted source reconciliation, you must specify values for the attributes of one of the following user reconciliation scheduled tasks:

- TELNET User Trusted Reconciliation task (Scheduled task for trusted source reconciliation)
- TELNET User Non Trusted Reconciliation task (Scheduled task for nontrusted source reconciliation)

The following table describes the attributes of both scheduled tasks.

---

**Note:**

- Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.
  - Values (either default or user-defined) must be assigned to all the attributes. If even a single attribute value were left empty, then reconciliation would not be performed.
-

Attribute	Description	Sample Value
Server	Name of the IT Resource	Telnet server-Solaris
Passwd Mirror File/User Mirror File	Name of the password mirror file/user mirror file	/etc/passwd1
Shadow Mirror File	Name of the shadow mirror file <b>Note:</b> This attribute is not required on AIX. The value of this attribute must not be null or blank, even for an HP-UX trusted system. However, the reconciliation process on an HP-UX trusted system ignores this attribute.	/etc/shadow1
IsTrusted	Specifies whether or not reconciliation is to be carried out in trusted mode	Specify Yes for trusted source reconciliation.  Specify No for nontrusted source reconciliation.
Target System Recon - Resource Object name	Name of the target system resource object	Telnet User
Trusted Source Recon - Resource Object name	Name of the trusted source resource object	Default value: Xellerate User  Specify false (in lowercase) if you do not want to configure trusted source reconciliation
Date Format	Format in which date values sent from the target system are to be saved during reconciliation  The value that you specify must be the same as the value specified in the <a href="#">"Configuring System Properties"</a> section on page 3-2.	yyyy/MM/dd hh:mm:ss z
BatchSize	Number of records in each batch that is reconciled  If you do not want to implement batched reconciliation, then specify nodata .  <b>See Also:</b> The <a href="#">"Batched Reconciliation"</a> section on page 3-2	The default value is 1000.
NumOfBatches	Number of batches to be reconciled  The number of records in each batch is specified by the BatchSize attribute.  <b>See Also:</b> The <a href="#">"Batched Reconciliation"</a> section on page 3-2	Specify All if you want to reconcile all the batches. This is the default value.  Specify an integer value if you want to reconcile only a fixed number of batches

Attribute	Description	Sample Value
UserNameFilter	<p>This is a filter attribute. Use this attribute to specify the user name (User Login) for which you want to reconcile user records.</p> <p>If you do not want to use this filter attribute, then specify Nodata .</p> <p><b>See Also:</b> The "<a href="#">Partial Reconciliation</a>" section on page 3-1</p>	<p>The value can be either the user name or Nodata .</p> <p>The default value is Nodata .</p>

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

## Enabling Reconciliation in Oracle Identity Manager Release 9.0.1

If you are using Oracle Identity Manager release 9.0.1, then you must perform the following procedure to enable reconciliation:

**See Also:** *Oracle Identity Manager Design Console Guide*

1. Open the Process Definition form for the Telnet User. This form is in the Process Management folder.
2. Click the **Reconciliation Field Mappings** tab.
3. For each field that is of the IT resource type:
  - a. Double-click the field to open the Edit Reconciliation Field Mapping window for that field.
  - b. Deselect **Key Field for Reconciliation Matching**.

## Adding Custom Attributes for Reconciliation

---

**Note:** In this section, the term "attribute" refers to the identity data fields that store user data.

---

By default, the attributes listed in the "[Reconciliation Module](#)" section on page 1-1 are mapped for reconciliation between Oracle Identity Manager and the target system. If required, you can map additional attributes for reconciliation as follows:

---

**Note:** You need not perform this procedure if you do not want to add custom attributes for reconciliation.

---

**See Also:** *Oracle Identity Manager Design Console* for detailed instructions on performing the following steps

1. Open the following file in the `OIM_home/xellerate/XLIntegrations/Telnet/config` directory:

For AIX users:

`userAttribute_AIX_recon.properties`

For non-AIX users:

```
userAttribute_NonAIX_recon.properties
```

2. At the end of this file, some of the attribute definitions are preceded by comment characters. You can uncomment the definition of an attribute to make it a part of the list of reconciliation attributes. If required, you can also add new attributes in this file. The format that you must use is as follows:

**For AIX:**

```
Connector_Attribute=OIM_Server_Attribute
```

For example:

```
maxage=Users.AccountExpiryDate
```

In this example, `AccountExpiryDate` is the reconciliation field and `maxage` is the equivalent server command parameter. As a standard, the prefix `"Users."` is added at the start of all reconciliation field names.

**For non-AIX platforms:**

```
OIM_Server_Attribute=Target_Server_Attribute_index
```

For example:

```
Users.DefaultShell=6
```

In this example, `DefaultShell` is the reconciliation field and `6` is the equivalent server Target Server Attributes index. As a standard, the prefix `"Users."` is added at the start of all reconciliation field names.

3. In the resource object definition, add a reconciliation field corresponding to the new attribute as follows:
  - a. Open the Resource Objects form. This form is in the Resource Management folder.
  - b. Click **Query for Records**.
  - c. On the Resource Objects Table tab, double-click the `Telnet User` resource object to open it for editing.
  - d. On the Object Reconciliation tab, click **Add Field** to open the Add Reconciliation Field dialog box.
  - e. Specify a value for the field name.

**For AIX:**

You must specify the name that is to the right of the equal sign in the line that you uncomment or add while performing Step 2.

For example, if you uncomment the `maxage=Users.AccountExpiryDate` line in Step 2, then you must specify `Users.AccountExpiryDate` as the attribute name.

**For non-AIX platforms:**

You must specify the name that is to the left of the equal sign in the line that you uncomment or add while performing Step 2.

For example, if you uncomment the `Users.DefaultShell=6` line in Step 2, then you must specify `Users.DefaultShell` as the attribute name.

- f. From the **Field Type** list, select a data type for the field.

For example: String

- [illegible]

## Configuring Provisioning

As mentioned earlier in this guide, provisioning involves creating or modifying a user's account information on the target system through Oracle Identity Manager. Refer to the ["Supported Functionality"](#) section on page 1-3 for a listing of the provisioning functions that are available with this connector.

This section discusses the following topics related to configuring provisioning:

- Compiling Adapters
- Adding Custom Attributes for Provisioning

## Compiling Adapters

**Note:** You must perform this procedure if you want to use the provisioning features of the connector.

Adapters are used to implement provisioning functions. The following adapters are imported into Oracle Identity Manager when you import the connector XML file:

**See Also:** The "Supported Functionality" section on page 1-3 for a listing of the provisioning functions that are available with this connector

- Telnet Disable User
- Telnet Delete User
- Telnet Default Shell Updated
- Telnet Create User
- Telnet Set Password
- Telnet User UID Updated
- Telnet GECOS Updated
- Telnet Home Directory Updated
- Telnet Primary Group Name Updated



- Telnet Account Expiry Date Updated
- Telnet Password Change Time Updated
- Telnet Secondary Group Names Updated
- Telnet Inactive Days Updated
- Telnet User Login Updated
- Telnet Enable User
- Telnet Prepopulate User Login
- Telnet Prepopulate End Date

You must compile these adapters before they can be used in provisioning operations.

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.

If you want to compile one adapter at a time, then use the Adapter Factory form.

**See Also:** *Oracle Identity Manager Tools Reference Guide* for information about using the Adapter Factory and Adapter Manager forms

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.

## Adding Custom Attributes for Provisioning

---

**Note:** In this section, the term "attribute" refers to the identity data fields that store user data.

---

By default, the attributes listed in the "[Provisioning Module](#)" section on page 1-2 are mapped for provisioning between Oracle Identity Manager and the target system. If required, you can map additional attributes for provisioning as follows:

**See Also:** *Oracle Identity Manager Design Console Guide*

1. Modify the attribute entries in the following file:

For the AIX platform:

```
OIM_home/xellerate/XLIntegrations/Telnet/config/userAttribute_AIX_prov.properties
```

For non-AIX platforms:

```
OIM_home/xellerate/XLIntegrations/Telnet/config/userAttribute_NonAIX_prov.properties
```

If required, you can add new attributes in this file. The format that you must use is as follows:

```
OimAttributeName=TargetAttributeName
```

For example:

```
homeDir=-d
```

2. Add a new column in the process form.
  - a. Open the process form. This form is in the Development Tools folder of the Oracle Identity Manager Design Console.
  - b. Click **Create New Version**.
  - c. In the Create a New Version dialog box, specify the version name in the **Label** field, save the changes, and then close the dialog box.
  - d. From the **Current Version** list, select the newly created version.
  - e. On the Additional Columns tab, click **Add**.
  - f. Specify the new field name and other values.
3. Add a new variable in the variable list.
  - a. Open the Adapter Factory form. This form is in the Development Tools folder of the Oracle Identity Manager Design Console.
  - b. Click the **Query for Records** icon.
  - c. On the Adapter Factory Table tab, double-click the **adpTELNETCREATEUSER** adapter from the list.
  - d. On the Variable List tab, click **Add**.
  - e. In the Add a Variable dialog box, specify the required values and then save and close the dialog box.
4. Define an additional adapter task for the newly added variable in the adpTELNETCREATEUSER adapter.
  - a. On the Adapter Tasks tab of the Adapter Factory form, click **Add**.
  - b. In the Adapter Task Selection dialog box, select **Functional Task**, select **Java** from the list of functional task types, and then click **Continue**.

- c. In the Object Instance Selection dialog box, select **Persistent Instance** and then click **Continue**.
  - d. In the Add an Adapter Factory Task dialog box, specify the task name, select the **setProperty** method from the **Method** list, and then click **Save**.
  - e. Map the application method parameters, and then save and close the dialog box. To map the application method parameters:
 

For the "Output: String Return variable (Adapter Variable)" parameter:

    - i. From the **Map to** list, select **Literal**.
    - ii. From the **Name** list, select **Return variable**.

For the "Input: String input (Adapter Variable)" parameter:

    - i. From the **Map to** list, select **Adapter Variables**.
    - ii. From the **Name** list, select **Input**.

For the "Input: String Status (Literal)" parameter:

    - i. From the **Map to** list, select **Literal**.
    - ii. From the **Name** list, select **String**.
    - iii. In the **Value** field, enter **Status**.

For the "Input: String Status (Adapter Variable)" parameter:

    - i. From the **Map to** list, select **Adapter Variables**.
    - ii. From the **Name** list, select **Status**.
  - f. Repeat Steps b through g to create more adapter tasks.
5. Create an additional adapter task to set the input variable.
    - a. Open the Adapter Factory form. This form is in the Development Tools folder in the Oracle Identity Manager Design Console.
    - b. On the Adapter Tasks tab, click **Add**.
    - c. In the Adapter Task Selection dialog box, select **Logic Task**, select **SET VARIABLE** from the list, and then click **Continue**.
    - d. In the Edit Set Variable Task Parameters dialog box, select **input** from the **Variable Name** list, select **Adapter Task** from the **Operand Type** list, and the Operand Qualifier as the Adapter Task that you have created in the previous step. Then, click **Save**.
  6. Map the process form columns and adapter variables for the Create User process task as follows:
    - a. Open the Process Definition form. This form is in the Process Management folder of the Design Console.
    - b. Click the **Query for Records** icon.
    - c. On the Process Definition Table tab, double-click the **TELNET User** process.
    - d. On the Tasks tab, double-click the **Create User** task.
    - e. In the Closing Form dialog box, click **Yes**.
    - f. On the Integration tab of the Editing Task Columns Create User dialog box, map the unmapped variables, and then save and close the dialog box. To map an unmapped variable:

- i. Double-click the row in which N is displayed in the Status column. The value N signifies that the variable is not mapped.
- ii. From the **Map to** list in the Edit Data Mapping for Variables dialog box, select **Process Data**.
- iii. From the **Qualifier** list, select the name of the variable.

Repeat Steps i through iii for all unmapped variables.

Repeat Steps 1 through 6 if you want to add more attributes.

## 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 the target system.

---

You may want to configure the connector for multiple installations of the target system. The following example illustrates this requirement:

The Tokyo, London, and New York offices of Acme Multinational Inc. have their own installations of the target system. The company has recently installed Oracle Identity Manager, and they want to configure Oracle Identity Manager to link all the installations of the target system.

To meet the requirement posed by such a scenario, you must configure the connector for multiple installations of the target system.

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

**See Also:** *Oracle Identity Manager Design Console Guide* for detailed instructions on performing each step of this procedure

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

The IT Resources form is in the Resource Management folder. An 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.

2. Configure reconciliation for each target system installation. Refer to the ["Configuring Reconciliation"](#) section on page 3-1 for instructions. Note that you only need to modify the attributes that are used to specify the IT resource and to specify whether or not the target system installation is to be set up as a trusted source.
3. 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 target system installation to which you want to provision the user.

## Testing and Troubleshooting

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

Before you use the testing utility, you must set the required values in the `config.properties` file. This file is in the `OIM_home/xellerate/XLIntegrations/Telnet/test/config/config.properties` directory. Use the information in the following table to modify the default attributes of the `config.properties` file.

Attribute	Description	Default Attribute (Sample Value)
hostname	IP address of the target server on which Telnet provisioning is to be performed	10.1.1.114
loginPrompt	Login prompt of the target server Default login	login
passwordPrompt	Password prompt of the UNIX server Default password	Password
shellPrompt	Default shell prompt of the UNIX server: # for Solaris, Linux, and HP-UX \$ for AIX	#
Port	Port at which the Telnet server is listening	22
Os Type	Operating system type of the UNIX server Accepted values are SOLARIS, LINUX, HP-UX, and AIX.	SOLARIS
adminpassword	Admin user password	dead_line
Admin	UNIX server administrator credentials for the Telnet server	root
Action	Action to be tested The value can be any of the following: <ul style="list-style-type: none"> <li>■ CREATE</li> <li>■ MODIFY</li> <li>■ DELETE</li> </ul>	CREATE
UserName	User attribute	jdoe
UID	New user UID for the user identified by UserName	12548

---

Attribute	Description	Default Attribute (Sample Value)
Max Retries	Number of times that the UNIX Telnet connector should retry connecting to the target server if the connection fails	2
Delay	Delay (in milliseconds) before the connector attempts to retry connecting to the target system, in case the connection fails	2000
Timeout	Value of the timeout (in milliseconds) for the connection to the target server	10000

After you specify values in the `config.properties` file, run the following script:

For UNIX:

```
OIM_home/xellerate/XLIntegrations/Telnet/test/scripts/telnet.sh
```

For Microsoft Windows:

```
OIM_home\xellerate\XLIntegrations\Telnet\test\scripts\Telnet.bat
```

---

## Known Issues

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

- This connector does not support logins that differ by case only. It also requires all logins to be distinct considering that their values are automatically converted to uppercase by Oracle Identity Manager.  
  
For example, the user logins `jdoe` and `JDOE` would be considered different in a UNIX server. However, from Oracle Identity Manager, the input would always be passed as `JDOE`, because user ID values are stored only in uppercase in Oracle Identity Manager.
- During provisioning, the data in the User Defined form fields must not contain the shell prompt character. Because there is a variation in shell prompt character depending on the target UNIX server, it should be checked in the target system.
- During provisioning, the maximum permitted date value for account expiry is `31/12/2099`.
- Suppose that a user on the UNIX server is disabled. If the Set Password function is run on this user account, then the account is automatically reenabled.
- During reconciliation, the Group Name field is reconciled as a number and not as the exact name because it is stored directly as the group ID in the target system.
- During reconciliation, the user login field is successfully reconciled only if the user ID does not exceed 32 characters.
- During reconciliation with the trusted option set to YES in the IT resource, the value for the `Shadow Mirror File` attribute must not be NULL or blank.
- While creating an IT resource, the user name provided for `Admin UserId` must be that of an active user in the target system. This means that the user must not be locked or disabled.
- When you configure an IT resource for a Telnet user account and then directly provision it to a user, the Create User Task function is rejected. The user account is not created on the target system. The following message is displayed:  
  
`"TELNET_USERCREATION_NOTCONNECTED_FAIL not able to connect successfully to the Target System Server"`.
- On AIX 5.2, while providing data in the GECOS field, ensure that there are no spaces. If there are spaces in this field, then the Update User Login function would not work.
- The Update Secondary Group Name and Update User Login functions do not work simultaneously.
- The Update Inactive Days function does not work on AIX 5.2.

- 
- Oracle Identity Manager does not support special characters in the User ID field on HP-UX, Solaris, and Linux target systems. If a user were created with special characters in the User Login field, then reconciliation would not work.
  - The Enable User function is not supported by the HP-UX (trusted) target system.
  - This release of the connector does not support all the shell types that are available on various operating systems. For information about the supported shell types, refer to the table at the end of the "[Step 1: Verifying Deployment Requirements](#)" section on page 2-1.
  - The entry of multibyte characters is not supported in some fields. Refer to [Appendix A](#) for more information about this known issue.



## Attribute Mappings Between Oracle Identity Manager and UNIX Telnet

The following table discusses attribute mappings between Oracle Identity Manager and UNIX Telnet.

**Note:** The entry of multibyte characters is supported for only some of the attributes listed in this table.

Oracle Identity Manager Attribute	UNIX Telnet Attribute	Description
Secondary Group Names	supplementary groups	List of supplementary groups, of which the user is also a member  In the value specified, groups are separated by commas, with no intervening whitespace between group names.
Password	passwd	Password
Reenter Password	Reenter Password	Password reentered for confirmation
User Login	login	New login name, specified as a string of printable characters It cannot contain a colon (:) or a newline (\n).
User UID	uid	Numeric value of the user ID  This value must be unique and nonnegative. The default is to use the smallest ID value greater than 99 and greater than the number used for any other user. Values between 0 and 99 are typically reserved for system accounts.
Primary Group Name	initial group	The group name or number of the user's initial login group.
Default Shell	shell	User's login shell
GECOS	comment	Generally, a short description of the login  It is used as the field for the user's full name. This information is stored in the user's <code>/etc/passwd</code> file entry.  <b>Note:</b> The entry of multibyte characters is supported for this attribute.

Oracle Identity Manager		
Attribute	UNIX Telnet Attribute	Description
Home Directory	home directory	<p>Login directory of the new user</p> <p>The default directory name is obtained by appending the login name to the default home directory. For example, if the login name is <code>jdoe</code>, then the default home directory is <code>/home/jdoe</code>.</p> <p><b>Note:</b> The entry of multibyte characters is supported for this attribute.</p>
Account Expiry Date	expire date	Date on which the user account is disabled
Password Change Time	maxdays	Maximum number of days for which a password is valid
Create Home Directory		If the Create Home Directory option is not selected, then the user home directory is not created.
Skeleton Directory	skeleton directory	<p>Specifies the skeleton directory that contains information that can be copied to the new login's home directory</p> <p>An existing directory must be specified. The system provides a skeleton directory, <code>/etc/skel</code>, that can be used for this purpose.</p> <p><b>Note:</b> The entry of multibyte characters is supported for this attribute.</p>
Inactive Days	inactive days	Number of days after a password has expired before the account is disabled

---

---

# Index

## A

---

Adapter Manager form, 3-9  
adapters, compiling, 3-8  
additional files, 2-1  
Administrative and User Console, 2-7, 3-3  
attributes mappings, A-1

## C

---

changing input locale, 2-4  
clearing server cache, 2-4  
compiling adapters, 3-8  
configuring  
    connector for multiple installations of the target  
        system, 3-12  
    Oracle Identity Manager server, 2-4  
configuring connector, 3-1  
configuring provisioning, 3-8  
connector configuration, 3-1  
connector files and directories  
    copying, 2-3  
    description, 1-5  
    destination directories, 2-3  
    installation directory, 1-5, 1-6, 2-3  
connector version number, determining, 1-6  
creating scheduled tasks, 3-3

## D

---

defining  
    scheduled tasks, 3-3  
deployment  
    requirements, 2-1  
Design Console, 3-2, 3-3  
determining version number of connector, 1-6

## E

---

enabling logging, 2-5  
external code files, 2-1

## F

---

files  
    additional, 2-1  
    external code, 2-1

*See also* XML files

*See* XML files

functionality supported, 1-3  
functions available, 1-3

## G

---

globalization features, 1-4

## I

---

importing connector XML files, 2-7  
input locale, changing, 2-4  
issues, 5-1

## L

---

limitations, 5-1  
logging enabling, 2-5

## M

---

mapping between attributes of target system and  
    Oracle Identity Manager, A-1  
connector XML files  
    *See* XML files  
files and directories of the connector  
    *See* connector files and directories  
multilanguage support, 1-4

## O

---

Oracle Identity Manager Administrative and User  
    Console, 2-7, 3-3  
Oracle Identity Manager Design Console, 3-2, 3-3  
Oracle Identity Manager Release 9.0.1, 3-6  
Oracle Identity Manager server, configuring, 2-4

## P

---

process tasks, 1-3  
provisioning  
    functions, 1-3

## R

---

reconciliation

- enabling in Oracle Identity Manager Release 9.0.1, 3-6
- functions, 1-3
- module, 1-1
- requirements for deploying, 2-1

## **S**

---

- scheduled tasks
  - defining, 3-3
- server cache, clearing, 2-4
- supported
  - languages, 1-4
  - releases of Oracle Identity Manager, 2-1
  - target systems, 2-1

## **T**

---

- target system, multiple installations, 3-12
- target systems supported, 2-1
- testing, 4-1
- troubleshooting, 4-1

## **U**

---

- user attribute mappings, A-1

## **V**

---

- version number of connector, determining, 1-6

## **X**

---

- XML files, importing, 2-7