

Oracle® Identity Manager

Connector Guide for UNIX SSH

Release 9.0.3

B32374-01

February 2007

Oracle Identity Manager Connector Guide for UNIX SSH, Release 9.0.3

B32374-01

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

Primary Authors: Debapriya Datta, Shiladitya Guha

Contributing Authors: Tehmurasp Ghyara, 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

Preface	v
Audience	v
Documentation Accessibility	v
Related Documents	vi
Documentation Updates	vi
Conventions	vi
What's New in the Oracle Identity Manager Connector for UNIX SSH?	vii
Software Updates	vii
Documentation-Specific Updates.....	viii
1 About the Connector	
Supported Functionality	1-1
Multilanguage Support.....	1-3
Reconciliation Module.....	1-3
Provisioning Module.....	1-4
Files and Directories That Comprise the Connector	1-4
Determining the Release Number of the Connector.....	1-5
2 Deploying the Connector	
Step 1: Verifying Deployment Requirements.....	2-1
Step 2: Configuring the Target System.....	2-2
Platform-Specific Configuration Steps.....	2-2
Configuration Steps for Solaris and Linux.....	2-2
Configuration Steps for AIX.....	2-3
Configuration Steps for HP-UX	2-3
Installing External Software	2-3
Installing OpenSSH	2-3
Installing and Configuring SUDO.....	2-7
Public Key Authentication (SSH Key Generation).....	2-14
Configuring Public Key Authentication.....	2-14
Configuring SSH Public Key Authentication	2-14
Step 3: Copying the Connector Files.....	2-17
Step 4: Configuring the Oracle Identity Manager Server.....	2-18
Changing to the Required Input Locale.....	2-18

Clearing Content Related to Connector Resource Bundles from the Server Cache	2-18
Enabling Logging	2-19
Step 5: Importing the Connector XML Files.....	2-20
Defining IT Resources	2-21
Step 6: Configuring Reconciliation.....	2-23
Adding Prerequisites for Reconciliation.....	2-23
Configuring System Properties.....	2-23
Configuring Trusted Source Reconciliation Oracle Identity Manager Entities	2-23
Defining Scheduled Tasks.....	2-24
Specifying Values for the Scheduled Task Attributes	2-25
Enabling Reconciliation in Oracle Identity Manager Release 9.0.1	2-26
Step 7: Compiling Adapters	2-26
Configuring the Connector for Multiple Installations of the Target System	2-27

3 Testing and Troubleshooting

Running Connector Tests.....	3-1
Troubleshooting.....	3-2

4 Known Issues

A Attribute Mappings Between Oracle Identity Manager and UNIX SSH

Index

Preface

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

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 9.0.2 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.
<i>italic</i>	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 displays on the screen, or text that you enter.

What's New in the Oracle Identity Manager Connector for UNIX SSH?

This chapter provides an overview of the updates made to the connector and documentation for UNIX SSH in release 9.0.3 of the Oracle Identity Manager connector pack.

See Also: The 9.0.2 release of this guide for information about updates that were new for the 9.0.2 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.

Enhancement in the Multilanguage Support Feature

In addition to the three languages supported by the earlier release, this release of the connector supports seven new languages. All the supported languages are listed in the "[Multilanguage Support](#)" section on page 1-3.

Support for OC4J

Earlier releases of the connector supported the following application servers:

- JBoss Application Server
- BEA WebLogic
- IBM WebSphere

This release of the connector also supports Oracle Containers for J2EE (OC4J).

Incorporation of Multilanguage Support

This connector does not support the entry of multibyte characters in some fields. Information about this limitation has been added in the following parts of the guide:

- [Chapter 4, "Known Issues"](#)
- [Appendix A, "Attribute Mappings Between Oracle Identity Manager and UNIX SSH"](#)

Documentation-Specific Updates

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

- In the "[Supported Functionality](#)" section on page 1-1, the following function has been added to the list of supported functions:

```
Delete User (Reconciliation)
```

- In [Chapter 2](#), a Note explaining alternatives to changing the value of `PermitRootLogin` to `yes` in the `/etc/ssh/sshd_config` file has been added at the required places.
- In the "[Step 1: Verifying Deployment Requirements](#)" section on page 2-1, information about supported shell types for various operating systems has been added.

This point is also listed as a limitation in the Known Issues list in [Chapter 4](#).

- In the "[Specifying Values for the Scheduled Task Attributes](#)" section on page 2-11, changes have been made in the descriptions of the following attributes:

```
Passwd Mirror File/User Mirror File
```

```
Shadow Mirror File
```

- In the "[Step 7: Compiling Adapters](#)" section on page 2-26, the instruction about restarting the node has been removed from Step 4 of the procedure to compile adapters.
- Instructions to enable logging are given in the "[Enabling Logging](#)" section on page 2-19.
- [Appendix A](#) provides information about attribute mappings between Oracle Identity Manager and UNIX SSH.

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 SSH is used to integrate Oracle Identity Manager with target systems running AIX, HP-UX, Linux, and Solaris , using the SSH 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:

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

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"> ■ On Solaris, the value in the Secondary Group Names field must be different from the value in the Primary Group Name field. ■ On HP-UX, the Inactive Account field must be populated only when the UNIX server is configured in trusted mode. ■ 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. ■ While specifying a value in the GECOS field, ensure that there are no spaces.

Function	Type	Description
Delete User	Provisioning	Deletes a user
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	Updates user properties according to a change in the Password attribute The changed password must conform to the password policy requirements of the target system.
Update Secondary Group Names	Provisioning	Updates user properties according to a change in the Secondary Group Names attribute Do not update the User Login field when you update the Secondary Group Names value. 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. 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.
Update Inactive Days	Provisioning	Updates user properties according to a change in the Update Inactive Days attribute This function is not supported on AIX 5.2.
Update User Login	Provisioning	Updates user properties according to a change in the User Login attribute Do not update the Secondary Group Names field when you update the User Login field. On AIX 5.2, if the User GECOS value contains spaces, then this function does not work.
Disable User	Provisioning	Disables an existing user on the UNIX server Note: 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.
Enable User	Provisioning	Enables a disabled existing user on the UNIX server Before running this function, the Set Password function must be run. This function is not supported on an HP-UX (trusted) server.

Function	Type	Description
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

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

The reconciliation module extracts the following elements from the target system to construct reconciliation event records:

- 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.

Provisioning Module

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

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 SSH

These files and directories are listed in the following table.

File in the Installation Media Directory	Description
config\sudoers	This file contains the SUDO user specifications and configurations.
ext\sshfactory.jar	This file contains the JScape libraries. These libraries are used to open an SSH session with the target server.
lib\xliSSH.jar	This file contains the Java classes that are required to support provisioning in SSH.
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.
scripts\privateKeyGen.sh	This file is used to generate the private key in SSH.
tests\config\config.properties	This file specifies the properties required by the client for running test calls from the Oracle Identity Manager server.

File in the Installation Media Directory	Description
tests\lib\xliSSHTest.jar	This file contains the Java classes that are required to run the client for running test calls from the Oracle Identity Manager server.
tests\logs	This directory is used by the connector test suite to log the results of the tests. The log files are created in this directory.
tests\scripts\SSH.bat tests\scripts\SSH.sh	This file contains the script required to run the client for running test calls from the Oracle Identity Manager server.
xml\XLISSH_DM.xml	This XML file contains definitions for the following SSH User components of the connector: <ul style="list-style-type: none"> ■ SSH User IT resource type ■ Custom process form ■ Process task and rule-generator adapters (along with their mappings) ■ Resource object ■ Provisioning process ■ Pre-populate rules that are used with this connector
xml\XLISSH_Trusted_DM.xml	This file contains definitions for the following SSH User components of the connector for a trusted system (HP-UX): <ul style="list-style-type: none"> ■ SSH User IT resource type ■ Custom process form ■ Process task and rule-generator adapters (along with their mappings) ■ Resource object ■ Provisioning process ■ Pre-populate rules that are used with this connector
xml\XLISSHSchedulerTask_DM.xml	This file contains the definition of the scheduled task for reconciliation.

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

The "[Step 3: Copying the Connector Files](#)" section on page 2-17 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 xliSSH.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 `xliSSH.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*

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 6: Configuring Reconciliation](#)
- [Step 7: Compiling Adapters](#)

If you want to configure the connector for multiple installations of UNIX SSH, 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	The target system can be any one of the following: <ul style="list-style-type: none"> ■ Solaris 8, Solaris 9, or Solaris 10 ■ HP-UX 11.11 (trusted/nontrusted) ■ Linux (Red Hat Advanced Server 2.1, Red Hat Enterprise Linux 3.x, or Red Hat Linux 4.x) ■ AIX 4.3 or AIX 5.2
External code	JSCAPE SSH/SSH Libraries (SSH factory)
Other systems	OpenSSH, OpenSSL, operating system patches (HP-UX), and SUDO software (only if the SUDO Admin mode is required)
Target system user account	root or sudo user You provide the credentials of this user account while performing the procedure in the " Defining IT Resources " section on page 2-21.

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>Note: 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

Configuring the target system involves the steps described in the following sections:

- [Platform-Specific Configuration Steps](#)
- [Installing External Software](#)
- [Public Key Authentication \(SSH Key Generation\)](#)

Platform-Specific Configuration Steps

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` 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 '#' ' ' > /etc/mainUserFile1
```

The name and path of this file must be specified for the `Password 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:
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/>

Installing External Software

This section describes the procedure to install external software.

Installing OpenSSH

Follow these steps to install OpenSSH on Solaris 9 or HP-UX.

For Solaris 8

1. If SSH is not installed on the Solaris server, then install the appropriate OpenSSH. For Solaris 8, you can download the packages listed in this section from

<http://www.sunfreeware.com/openssh8.html>

If the GCC compiler is not installed, then you must install the packages in the following file:

```
libgcc-3.3-sol8-sparc-local.gz
```

The following packages are included in this file. You must install these packages in the specified order:

- a. `prngd-0.9.25-sol8-sparc-local.gz` (optional)
 - b. `tcp_wrappers-7.6-sol8-sparc-local.gz` (optional, but recommended)
 - c. `zlib-1.2.1-sol8-sparc-local.gz`
 - d. `openssl-0.9.7g-sol8-sparc-local.gz`
 - e. `openssh-4.1p1-sol8-sparc-local.gz`
2. Create a group with the name `sshd` and group ID 27. Add a user with the name `sshadmin` to this group.
 3. To enable root logins, change the value of `PermitRootLogin` in the `/etc/ssh/sshd_config` file as follows:

```
PermitRootLogin yes
```

Note: Implement this change only if it does not violate local security policies. If Public Key Authentication is enabled, then you can change the value of `PermitRootLogin` to `without-password`.

Instead of using the root account, if you can use a user account with `sudo` privileges, then you do not need to perform this step.

For Solaris 9

1. If SSH is not installed on the Solaris server, then install the appropriate OpenSSH. For Solaris 9, you can download the packages listed in this section from

<http://www.sunfreeware.com/>

Note: If the GCC compiler is not installed, then install the following packages:

```
libgcc-3.4.1-sol9-sparc-local.gz
```

```
libiconv-1.8-sol9-sparc-local.gz
```

You must install these packages in the following order:

- a. `prngd-0.9.25-sol9-sparc-local.gz`
 - b. `tcp_wrappers-7.6-sol9-sparc-local.gz`
 - c. `zlib-1.2.1-sol9-sparc-local.gz`
 - d. `openssl-0.9.7d-sol9-sparc-local.gz`
 - e. `openssh-3.9p1-sol9-sparc-local.gz`
2. Create a group with the name `sshd` and group ID 27. Add a user with the name `sshadmin` to this group.

3. To enable root logins, change the value of `PermitRootLogin` in the `/etc/ssh/sshd_config` file as follows:

```
PermitRootLogin yes
```

Note: Implement this change only if it does not violate local security policies. If Public Key Authentication is enabled, then you can change the value of `PermitRootLogin` to `without-password`.

Instead of using the root account, if you can use a user account with sudo privileges, then you do not need to perform this step.

For Solaris 10

By default, OpenSSH is installed on Solaris 10. If it is not installed, then install the OpenSSH server from the operating system installation CD. To enable SSH on Solaris 10, make the following changes in the `/etc/ssh/sshd_config` file:

1. Remove the comment character from the `Host *` line.
2. To enable root logins, change the value of `PermitRootLogin` in the `/etc/ssh/sshd_config` file as follows:

```
PermitRootLogin yes
```

Note: Implement this change only if it does not violate local security policies. If Public Key Authentication is enabled, then you can change the value of `PermitRootLogin` to `without-password`.

Instead of using the root account, if you can use a user account with sudo privileges, then you do not need to perform this step.

For HP-UX

If SSH is not installed on the UNIX server, then install the appropriate OpenSSH:

1. For HP-UX 11.11, download and install the appropriate patch from

<http://www4.itrc.hp.com/>

For HP-UX B.11.11, download the file, `PHCO_33711.depot` for `hpux_800_11.11_11300132-patch.tgz`. Use the following command to install it:

```
swinstall -x autoreboot=true -x patch_match_target=true -s /tmp/PHCO_33711.depot
```

2. Download and install OpenSSH. You can download the `T1471AA_A.03.81.002_HP-UX_B.11.11_32+64.depot` file from

<http://software.hp.com/portal/swdepot/displayProductInfo.do?productNumber=T1471AA>

After the patch is successfully installed, use the following command to install openSSH.

```
swinstall -s /tmp/T1471AA_A.03.81.002_HP-UX_B.11.11_32+64.depot
```

After this is installed, the HP-UX Secure Shell daemon (`sshd`) is automatically preconfigured and started.

3. Create a group with the name `sshd`.

4. Add a user with the name `sshadmin` to this group.
5. To enable root logins, change the value of `PermitRootLogin` in the `/etc/ssh/sshd_config` file as follows:

```
PermitRootLogin yes
```

Note: Implement this change only if it does not violate local security policies. If Public Key Authentication is enabled, then you can change the value of `PermitRootLogin` to `without-password`.

Instead of using the root account, if you can use a user account with sudo privileges, then you do not need to perform this step.

For Linux

By default, OpenSSH is installed on Red Hat Advanced Server 2.1 and Red Hat Enterprise Linux 3. If it is not installed, then install the OpenSSH server from the operating system installation CD.

For AIX

If SSH is not installed on the AIX 5.2 server, then perform the following steps:

1. Download and install OpenSSL.

Download the `openssl-0.9.7d-aix5.1.ppc.rpm` file from

<http://www-1.ibm.com/servers/aix/products/aixos/linux/download.html>

Then, enter the following command to install OpenSSL:

```
geninstall -d /root/download R: openssl-0.9.7d-2.aix5.1.ppc.rpm
```

In this command, `/root/download` is the location on the AIX server where the `openssl-0.9.7d-2.aix5.1.ppc.rpm` file is stored.

2. Download and install PRNG.

Download the `prngd-0.9.23-3.aix4.3.ppc.rpm` file from

<http://www-1.ibm.com/servers/aix/products/aixos/linux/download.html>

Then, enter the following command to install PRNG:

```
geninstall -d /root/download R: prngd-0.9.23-3.aix4.3.ppc.rpm
```

In this command, `/root/download` is the location on the AIX server where the `prngd-0.9.23-3.aix4.3.ppc.rpm` file is stored.

3. Download and install OpenSSH.

Download the `openssh-3.8.1p1_52.tar.gz` file from

<http://www-1.ibm.com/servers/aix/products/aixos/linux/download.html>

Then, enter the following commands to install openSSH:

```
gunzip /root/download/openssh-3.8.1p1_52.tar.gz
tar -xvf /root/download/openssh-3.8.1p1_52.tar
geninstall -I"Y" -d /root/download I:openssh.base
```

In these commands, `/root/download` is the location on the AIX server where the `openssh-3.8.1p1_52.tar.gz` file is stored.

4. To enable root logins, change the value of `PermitRootLogin` in the `/etc/ssh/sshd_config` file as follows:

```
PermitRootLogin yes
```

Note: Implement this change only if it does not violate local security policies. If Public Key Authentication is enabled, then you can change the value of `PermitRootLogin` to `without-password`.

Instead of using the root account, if you can use a user account with sudo privileges, then you do not need to perform this step.

Installing and Configuring SUDO

If you want to use the SSH connector in the SUDO Admin mode, then perform the following steps to install and configure SUDO:

For Solaris

1. If SUDO is not installed on the Solaris server, then first download it.
 - For Solaris 9, download the `sudo-1.6.8p4-sol9-sparc-local.gz` file from
<http://www.sunfreeware.com/programlistsparc9.html#sudo>
 - For Solaris10, download the `sudo-1.6.8p9-sol9-sparc-local.gz` file from
<http://www.sunfreeware.com/programlistsparc9.html#sudo>
 - For Solaris 8, download the `sudo-1.6.8p9-sol8-sparc-local.gz` file from
<http://www.sunfreeware.com/programlistsparc8.html#sudo>
2. Use the following command to install SUDO:

```
pkgadd -d filename_with_full_path
```

3. Edit the `sudoers` file on the Solaris server to customize it according to your requirements. This file is located in the following directory:

```
/usr/local/etc/
```

For example, if a group named `mqm` exists on the Solaris server, and you require all members of the group to act as SUDO users with all possible privileges, then the `sudoers` file must contain a line similar to the following:

```
%mqm ALL= (ALL) ALL
```

This is only a sample configuration. If you require some other group members or individual users to be SUDO users with specific privileges, then you must edit this file as you did for the sample value `mqm`.

This connector uses the following commands:

- `useradd`
- `usermod`

- passwd
- cat
- diff

Therefore, the SUDO user must have privileges to run these commands.

Note: Do not use the `NOPASSWD: ALL` option for any SUDO user or group.

For information about customizing the `sudoers` file, refer to

<http://www.courtesan.com/sudo/man/sudoers.html>

4. Edit the same `sudoers` file so that every time a command is run in SUDO Admin mode, the SUDO user is prompted for the password. Add the following line under the `# Defaults` specification header:

```
Defaults timestamp_timeout=0
```

This is a prerequisite for this connector to work successfully.

5. Log in to the Solaris computer as root, and enter the following commands:

```
chmod 440 /usr/local/etc/sudoers
chgrp root /usr/local/etc/sudoers
chmod 4111 /usr/local/bin/sudo
```

6. Create a SUDO user. The SUDO user must be created according to the constraints specified in the `sudoers` file.

The SUDO user must always be created with its home directory by using a command similar to the following:

```
useradd -g group_name -d /export/home/directory_name -m user_name
```

7. In the sudo user's `.profile` file, which is created in the sudo user's home directory, add the following lines to set the value of the `PATH` environment variable:

```
PATH=/usr/sbin:/usr/local/bin:/usr/local/etc:/var/adm/sw/products:$PATH
export PATH
```

For HP-UX

1. If SUDO is not installed on the HP-UX server, then install the appropriate SUDO. For HP-UX, download the `sudo-1.6.8p6-sd-11.11.depot.gz` file from

<http://hpux.cs.utah.edu>

Enter the following command to install SUDO:

```
swinstall -s filename_with_full_path
```

2. Edit the `sudoers` file to customize it according to your requirements. This file is located in the following directory:

```
OIM_home/Xellerate/XLIntegrations/SSH/config/
```

For example, if you have a group named `mcm` on the HP-UX server and you want all members of the group to act as SUDO users with all possible privileges, then the `sudoers` file must contain the following line:

```
%mcm ALL= (ALL) ALL
```

This is only a sample configuration. If you want to make SUDO users with specific privileges out of other group members or individual users, then edit this file as you did for the sample value `mcm`.

This connector uses the following commands:

- `useradd`
- `usermod`
- `passwd`
- `cat`
- `diff`

Therefore, the SUDO user must have the privileges required to run these commands.

Note: Do not use the `NOPASSWD: ALL` option for any SUDO user or group.

For information about customizing the `sudoers` file, refer to

<http://www.courtesan.com/sudo/man/sudoers.html>

3. Edit the same `sudoers` file so that every time a command is run in SUDO Admin mode, the SUDO user is prompted for a password. Add the following line under the `# Defaults` specification header:

```
Defaults timestamp_timeout=0
```

This is an essential prerequisite for the connector to work successfully.

4. Copy the `sudoers` file that you edited into the `/etc` directory of the target system. After copying the file, enter the following command:

```
dos2ux /etc/sudoers > /etc/sudoers1
```

Then, change the name of the file from `sudoers1` to `sudoers`.

5. Log in as `root`, and enter the following commands on the HP-UX computer:

```
chmod 440 /etc/sudoers
chgrp root /etc/sudoers
chmod 4111 /usr/local/bin/sudo
```

6. Create a SUDO user. The SUDO user should be created according to the constraints specified in the `sudoers` file.

The SUDO user should always be created with its home directory by using a command similar to the following:

```
useradd -g group_name -d /home/directory_name -m user_name
```

In addition, in the `.profile` file, which is created in the home directory, add the following lines to set the appropriate `PATH`:

```
PATH=/usr/sbin:/usr/local/bin:/usr/local/etc:/var/adm/sw/products:$PATH
export PATH
```

For AIX

1. If SUDO is not installed on AIX 5.2, then install the appropriate SUDO AIX 5.2 version `sudo-1.6.7p5-2.aix5.1.ppc.rpm` file from

<http://www-1.ibm.com/servers/aix/products/aixos/linux/download.html>

2. If RPM Package Manager is not installed on the AIX 5.2 server, then install it from

<http://www-1.ibm.com/servers/aix/products/aixos/linux/altlic.html>

3. Enter the following command to install SUDO:

```
rpm -I /root/download/sudo-1.6.7p5-2.aix5.1.ppc.rpm
```

In this command, `/root/download` is the location on the AIX server where the `sudo-1.6.7p5-2.aix5.1.ppc.rpm` file is stored.

4. Edit the `sudoers` file, which is in the `/etc` directory on the AIX server, to customize the file according to your requirements.

For example, if you have a group named `mqm` in the AIX server and require all members of the group to act as SUDO users with all possible privileges, then the `sudoers` file must contain the following line:

```
%mqm ALL= (ALL) ALL
```

This is only a sample configuration. If you need other group members or individual users to be SUDO users with specific privileges, then edit this file as was done for the sample value `mqm`.

This connector uses the following commands:

- `mkuser`
- `chuser`
- `passwd`
- `cat`
- `diff`
- `usermod`

Therefore, the SUDO user must have the privileges required to run these commands.

Note: Do not use the `NOPASSWD: ALL` option for any SUDO user or group.

For information about customizing the `sudoers` file, refer to

<http://www.courtesan.com/sudo/man/sudoers.html>

5. Edit the same `sudoers` file to configure the system, so that every time a command is run through SUDO Admin mode, the SUDO user is prompted for a password. Add the following line under the `# Defaults` specification header:

```
Defaults timestamp_timeout=0
```

This is a prerequisite for this connector to work successfully.

6. Create a SUDO user. The SUDO user should be created according to the constraints specified in the `sudoers` file.

For Red Hat Advanced Server 2.1

1. If SUDO is not installed on the Red Hat Advanced Server 2.1 server, then install the appropriate SUDO. To do this, first download the `sudo-1.6.7p5-1.i686.rpm` file from

<http://rpmfind.net/linux/rpm2html/search.php?query=sudo&submit=Search>

Then, enter the following command to install SUDO:

```
rpm -i /root/download/sudo-1.6.7p5-1.i686.rpm
```

In this command, `/root/download` is the location on the Linux server where the `sudo-1.6.7p5-1.i686.rpm` file is stored.

2. Use the `visudo` command to edit and customize the `/etc/sudoers` file according to your requirements.

Note: If you cannot use the `visudo` command to edit the `sudoers` file, then:

1. Enter the following command:

```
chmod 777 /etc/sudoers
```

2. Make the required changes in the `sudoers` file.

3. Enter the following command:

```
chmod 440 /etc/sudoers
```

For example, if you have a group named `mqm` on the Linux server and require all members of the group to act as SUDO users with all possible privileges, then the `sudoers` file must contain the following line:

```
mqm ALL= (ALL) ALL
```

This example is only a sample configuration. If you need other group members or individual users to be SUDO users with specific privileges, then edit this file as was done for the sample value `mqm`.

The commands that this connector uses are:

- `useradd`
- `usermod`
- `passwd`
- `cat`
- `diff`

Therefore, the SUDO user must have the privileges required to run these commands.

Note: Do not use the `NOPASSWD: ALL` option for any SUDO user or group.

For information about customizing the `sudoers` file, refer to

<http://www.courtesan.com/sudo/man/sudoers.html>

3. Edit the same `sudoers` file to configure the system, so that every time a command is run in SUDO Admin mode, the SUDO user is prompted for a password. Under the `# Defaults` specification header, add the following line:

```
Defaults timestamp_timeout=0
```

This is a prerequisite for this connector to work successfully.

4. Create a SUDO user as follows:

- a. Enter the following command:

```
useradd -g group_name -d /home/directory_name -m user_name
```

In this command:

- *group_name* is the SUDO users group for which there is an entry in the `/etc/sudoers` file.

- *directory_name* is the name of the directory in which you want to create the default directory for the user.

- b. In the `.bash_profile` file, which is created in the `/home/directory_name` directory, add the following lines to set the `PATH` environment variable:

```
PATH=/usr/sbin:$PATH
export PATH
```

For Red Hat Enterprise Linux 3.x and Red Hat Linux 4.x

1. If SUDO is not installed on the Red Hat Enterprise Linux 3.x or 4.x server, then install the appropriate SUDO. For Linux Advanced Server 3.0 and 4.1, download the `sudo-1.6.7p5-1.i686.rpm` file from

<http://rpmfind.net/linux/rpm2html/search.php?query=sudo&submit=Search>

Then, enter the following command to install SUDO:

```
rpm -i /root/download/sudo-1.6.7p5-1.i686.rpm
```

In this command, `/root/download` is the location on the Linux server where the `sudo-1.6.7p5-1.i686.rpm` file is stored.

2. Use the `visudo` command to edit and customize the `/etc/sudoers` file according to your requirements.

Note: If you cannot use the `visudo` command to edit the `sudoers` file, then:

1. Enter the following command:

```
chmod 777 /etc/sudoers
```

2. Make the required changes in the `sudoers` file.

3. Enter the following command:

```
chmod 440 /etc/sudoers
```

For example, if you have a group named `mqm` on the Linux server and want all of the members of the group to act as SUDO users with all possible privileges, then the `sudoers` file must contain the following line:

```
%mqm ALL= (ALL) ALL
```

This is only a sample configuration. If you want some other group members or individual users to be SUDO users with specific privileges, you must edit this file as was done for the sample value `mqm`.

This connector uses the following commands:

- `useradd`
- `usermod`
- `passwd`
- `cat`
- `diff`

Therefore, the SUDO user must have the privileges required to run these commands.

Note: Do not use the `NOPASSWD: ALL` option for any SUDO user or group.

For information about customizing the `sudoers` file, refer to

<http://www.courtesan.com/sudo/man/sudoers.html>

3. Edit the same `sudoers` file to configure the system, so that every time a command is run in SUDO Admin mode, the SUDO user is prompted for a password. Under the `# Defaults` specification header, add the following line:

```
Defaults timestamp_timeout=0
```

This is a prerequisite for this connector to work successfully.

4. Create a SUDO user as follows:

- a. Enter the following command:

```
useradd -g group_name -d /home/directory_name -m user_name
```

In this command:

- `group_name` is the SUDO users group for which there is an entry in the `/etc/sudoers` file.

- *directory_name* is the name of the directory in which you want to create the default directory for the user.

- b. In the `.bash_profile` file, which is created in the `/home/directory_name` directory, add the following lines to set the `PATH` environment variable:

```
PATH=/usr/sbin:$PATH
export PATH
```

Public Key Authentication (SSH Key Generation)

This section discusses the following topics:

- [Configuring Public Key Authentication](#)
- [Configuring SSH Public Key Authentication](#)

Configuring Public Key Authentication

To configure Public Key Authentication:

1. Copy `SSH/scripts/privateKeyGen.sh` to any directory on the server.
2. Open this script file in a text editor and specify a working directory path other than the default value given in the file.
3. If required, enter the following command:

For Solaris or Linux:

```
dos2unix privateKeyGen.sh privateKeyGen.sh
```

For HP-UX:

```
dos2ux privateKeyGen.sh
```

4. Run the `privateKeyGen.sh` script on the UNIX server. Provide a secure pass phrase when prompted.

When these commands are run, the following files are created in the `$HOME/.ssh` directory:

- `id_rsa`: This is a private key file.
 - `authorized_keys`: This file lists public keys that can be used to log in.
5. When the keys are generated successfully, edit the `sshd_config` file for Public Key Authentication and test login.
 6. After successfully testing login, copy the `id_rsa` file to the following directory:

```
OIM_home/Xellerate/XLIntegrations/SSH/Config
```

Note: This release of the connector has been tested and certified only for RSA keys, and not DSA. In addition, this connector has been tested and certified for only single key configuration and not multiple keys.

Configuring SSH Public Key Authentication

To configure SSH Public Key Authentication:

For Solaris

1. Set the following parameters in the `/etc/ssh/sshd_config` file:

```
PubKeyAuthorization yes
PasswordAuthentication no
PermitRootLogin yes
```

Note: Change the value of `PermitRootLogin` to `yes` only if it does not violate local security policies. If Public Key Authentication is enabled, then you can change the value of `PermitRootLogin` to `without-password`.

Instead of using the root account, if you can use a user account with sudo privileges, then you do not need to perform this step.

2. To restart the SSH server, enter the following commands:

```
■ /etc/init.d/sshd stop
■ /etc/init.d/sshd start
```

3. To test login:

```
ssh -i /.ssh/id_rsa -l root server_IP_address
```

This command prompts you for the passkey before setting up the connection.

For HP-UX

1. Uncomment the following lines in the `/etc/ssh/sshd_config` file:

```
PermitRootLogin yes
PubkeyAuthentication yes
AuthorizedKeysFile .ssh/authorized_keys
```

Note: Change the value of `PermitRootLogin` to `yes` only if it does not violate local security policies. If Public Key Authentication is enabled, then you can change the value of `PermitRootLogin` to `without-password`.

Instead of using the root account, if you can use a user account with sudo privileges, then you do not need to perform this step.

2. To restart the SSH Server, enter the following command:

```
/opt/ssh/sbin/sshd
```

3. To test login, enter the following command:

```
ssh -i /.ssh/id_rsa -l root server_IP_address
```

When prompted, enter the passkey to connect to the server.

For Linux

1. Enter the following commands at the UNIX server prompt:

```
mkdir /.ssh
chmod 700 /.ssh
ssh-keygen -q -f /.ssh/id_rsa -t rsa
chmod 700 /.ssh/*
```

You are prompted to enter a passphrase when you enter these commands. You can press **Enter** if you do not want to use a passphrase.

2. Add the following line in the `/etc/ssh/sshd_config` file:

```
AuthorizedKeysFile      /.ssh/id_rsa.pub
```

3. Enter the following commands to restart the UNIX server:

```
/etc/init.d/sshd stop  
/etc/init.d/sshd start
```

4. To check if you can connect to the target system using the SSH protocol, directly from the command prompt and without using a password, enter the following command:

```
#ssh -l root -i /.ssh/id_rsa host_ip_address
```

5. Copy the `/.ssh/id_rsa` file to the following directory:

```
OIM_home/xellerate/XLIntegrations/SSH/config
```

6. When you perform the procedure described in the ["Defining IT Resources"](#) section on page 2-21, provide the name and full path of the `id_rsa` file as the value of the `Private Key` parameter:

```
OIM_home/xellerate/XLIntegrations/SSH/config/id_rsa
```

For AIX

1. The first step of this procedure depends on the version of AIX that you are using:

- For AIX 4.3, use the `/etc/openssh/sshd_config` file to set the following parameters:

```
export PATH=$PATH: /usr/local/bin  
Installation path: /etc/openssh/  
sshd -- /usr/local/bin/
```

- For AIX 5.2, use the `/etc/ssh/sshd_config` file to set the following parameters:

```
export PATH=$PATH: /usr/sbin  
Installation path: /etc/ssh/  
sshd -- /usr/sbin/
```

2. Open the `/etc/ssh/sshd_config` file, and uncomment the following lines:

```
AuthorizedKeysFile .ssh/authorized_keys  
PermitRootLogin yes  
PubkeyAuthentication yes
```

Note: Change the value of `PermitRootLogin` to `yes` only if it does not violate local security policies. If `Public Key Authentication` is enabled, then you can change the value of `PermitRootLogin` to `without-password`.

Instead of using the root account, if you can use a user account with `sudo` privileges, then you do not need to perform this step.

3. To restart the SSH server, enter the following commands:

- /opt/ssh/sbin/sshd (For AIX 4.3)
 - /usr/sbin/sshd (For AIX 5.2)
4. To test the login, enter the following command:
- ```
ssh -i /.ssh/id_rsa -l root server_IP_address
```

When prompted, enter the passkey to connect to the server.

---



---

**Note:** This release of the connector does not support Public Key Authentication provisioning if it is implemented through the SUDO Admin mode. The Public Key Authentication used for system access is available for the root user. This point is also mentioned in the Known Issues list in [Chapter 4](#).

---



---

## 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 SSH

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

---



---

| File in the Installation Media Directory | Destination Directory                                 |
|------------------------------------------|-------------------------------------------------------|
| config\sudoers                           | <i>OIM_home</i> /xellerate/XLIntegrations/SSH/config  |
| ext\sshfactory.jar                       | <i>OIM_home</i> /xellerate/ThirdParty                 |
| lib\xliSSH.jar                           | <i>OIM_home</i> /xellerate/JavaTasks                  |
| lib\xliSSH.jar                           | <i>OIM_home</i> /xellerate/ScheduleTask               |
| Files in the resources directory         | <i>OIM_home</i> /xellerate/connectorResources         |
| scripts\privateKeyGen.sh                 | <i>OIM_home</i> /xellerate/XLIntegrations/SSH/scripts |
| Files in the tests directory             | <i>OIM_home</i> /xellerate/XLIntegrations/SSH/tests   |
| Files in the xml directory               | <i>OIM_home</i> /xellerate/XLIntegrations/SSH/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.

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 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 depends on the application server that you use:

- **For JBoss Application Server**

In the `JBoss_home\server\default\conf\log4j.xml` file, add the following lines of XML code:

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

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 = "WARN"/>
</category>
```

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

```
JBoss_home\server\default\log\server.log
```

- **For IBM WebSphere**

Add the following line in the

*OIM\_home*\xellerate\config\log.properties file:

```
log4j.logger.Adapter.TELNETSSH=log_level
```

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
```

- **For BEA WebLogic**

Add the following line in the

*OIM\_home*\xellerate\config\log.properties file:

```
log4j.logger.Adapter.TELNETSSH=log_level
```

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
```

- **For OC4J**

Add the following line in the

*OIM\_home*\xellerate\config\log.properties file:

```
log4j.logger.Adapter.TELNETSSH=log_level
```

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:

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 `XLISSH_DM.xml` file, which is in the `OIM_home/xellerate/XLIntegrations/SSH/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 SSH server Solaris IT resource is displayed.
8. Specify values for the parameters of the SSH server Solaris IT resource. Refer to the table in the "[Defining IT Resources](#)" section on page 2-21 for information about the values to be specified.
9. Click **Next**. The Provide IT Resource Instance Data page for a new instance of the SSH 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. Remove these nodes 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 `XLISSH_SchedulerTask_DM.xml` file, which is in the `OIM_home/xellerate/XLIntegrations/SSH/xml` directory.
14. If you plan to use the connector in trusted source reconciliation mode, then perform the same procedure to import the `XLISSH_Trusted_DM.xml` file. This file is in the `OIM_home/xellerate/XLIntegrations/SSH/xml` directory.

---

**Caution:** Only one connector can be configured for trusted source reconciliation. If you import the `XLISSH_Trusted_DM.xml` file while you have another trusted source configured, then both connector reconciliations would stop working.

---

After you import the connector XML file, proceed to the "[Step 6: Configuring Reconciliation](#)" section on page 2-23.

## Defining IT Resources

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

Parameter	Description
Admin UserId	User ID of the administrator root or jdoe Here, jdoe is the SUDO user ID, for the SUDO Admin mode.

Parameter	Description
Admin Password/Private file Pwd	<p>Password of the administrator</p> <p>dead_line (for root/non-SUDO) or jdoe</p> <p>Here, jdoe is the SUDO user password, for the SUDO Admin mode.</p> <p><b>Note:</b></p> <p>For the SUDO Admin mode, the private key is not supported. You must not specify a value for this mode.</p> <p>If a private key is used, then the Private Key PassPhrase must be provided as the value of this parameter.</p>
Server IP Address	Server IP address
Port	<p>The port at which the SSH service is running on the server</p> <p>Default value: 22</p>
Private Key	<p>Private key file name with full path</p> <p><b>Note:</b> For SUDO Admin administrator, this parameter must be left blank.</p>
Server OS	<p>Specify one of the following:</p> <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	You can ignore this parameter. This parameter is not used for SSH.
Password Prompt	You can ignore this parameter. This parameter is not used for SSH.
Whether Trusted System (HP-UX)	YES (for trusted HP-UX System) or NO (for nontrusted HP-UX system)
Whether SUDO Admin Mode	NO (for root) or YES (for SUDO Admin mode)
Target Locale	<p>Target locale (language and country)</p> <p>You can specify any one of the following values:</p> <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> <p><b>Note:</b> You must not make any change (uppercase or lowercase) in the value that you specify.</p>
Supported Character Encoding (en_US) - Target	<p>Encoding format for the en_US target locale</p> <p>The default value is UTF-8.</p> <p><b>Note:</b> You can check which en_US encoding formats the target system supports by using the following command:</p> <pre>locale -a</pre>

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

## Step 6: Configuring Reconciliation

This section describes the following steps involved in configuring the Oracle Identity Manager server:

- [Adding Prerequisites for Reconciliation](#)
- [Defining Scheduled Tasks](#)
- [Enabling Reconciliation in Oracle Identity Manager Release 9.0.1](#)

### Adding Prerequisites for Reconciliation

This section discusses the following topics:

- [Configuring System Properties](#)
- [Configuring Trusted Source Reconciliation Oracle Identity Manager Entities](#)

#### 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 Oracle Identity Manager Entities

---



---

**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 configure trusted source reconciliation for this connector 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.

---



---

This procedure involves the following steps:

1. Open the Oracle Identity Manager Design Console.
2. In the Resource Object form:
  - a. Search for the Xellerate User.



## Specifying Values for the Scheduled Task Attributes

You must specify values for the following attributes of the 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	Sample Value
Server	Name of the IT resource	SSH server Solaris
Passwd Mirror File/User Mirror File	<p>Name of the password mirror file/user mirror file</p> <p>The SUDO user must have read and write permissions on this file.</p> <p>For example, suppose you run the following command to view the permissions on the mirror file:</p> <pre>\$ ls -ltr passwd1</pre> <p>The command generates the following output:</p> <pre>-rwxr--r-- 1 janedoe mqm 9972 Mar 11 20:35 passwd1</pre> <p>In this output, janedoe is the SUDO user.</p>	/etc/passwd1
Shadow Mirror File	<p>Name of the shadow mirror file</p> <p>The SUDO user must have read and write permissions on this file.</p> <p>For example, suppose you run the following command to view the permissions on the mirror file:</p> <pre>\$ ls -ltr shadow1</pre> <p>The command generates the following output:</p> <pre>-rwxr--r-- 1 janedoe mqm 9972 Mar 11 20:35 shadow1</pre> <p>In this output, janedoe is the SUDO user.</p> <p><b>Note:</b></p> <p>This attribute is not required on AIX.</p> <p>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.</p>	/etc/shadow1
Target System Recon - Resource Object name	Name of the target system resource object	SSH User

Attribute	Description	Sample Value
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 2-23.	yyyy/MM/dd hh:mm:ss z

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 SSH 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**.

## Step 7: Compiling Adapters

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

- SSH Disable User
- SSH GECOS Updated
- SSH Set Password
- SSH Default Shell Updated
- SSH Password Change Time Updated
- SSH Create User
- SSH Delete User
- SSH Home Directory Updated
- SSH Primary Group Name Updated
- SSH Account Expiry Date Updated

- SSH User UID Updated
- SSH Secondary Group Name Updated
- SSH Inactive Days Updated
- SSH User Login Updated
- SSH Enable User
- SSH Prepopulate User Login
- SSH Prepopulate End Date

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.

---

---

## 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 UNIX SSH. 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 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 "[Step 6: Configuring Reconciliation](#)" section on page 2-23 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.

You can designate either a single or multiple installations of UNIX SSH as the 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 UNIX SSH installation to which you want to provision the user.

---



---

## 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 Connector Tests](#)
- [Troubleshooting](#)

### Running Connector Tests

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.

Before you use the troubleshooting utility, you must set the required values in the `config.properties` file. This file is in the `OIM_home/xellerate/XLIntegrations/SSH/tests/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)
<code>hostname</code>	IP address of the target server on which SSH provisioning is to be performed	<code>10.1.1.114</code>
<code>loginPrompt</code>	Default login prompt of the target server	<code>login</code>
<code>passwordPrompt</code>	Default password prompt of the target server	<code>Password</code>
<code>shellPrompt</code>	Default shell prompt of the target server: # for Solaris, Linux, and HP-UX \$ for AIX	<code>#</code>
<code>port</code>	Port at which the SSH server is listening	<code>22</code>
<code>osType</code>	Operating system type of the UNIX server Accepted values are <code>SOLARIS</code> , <code>LINUX</code> , <code>HP-UX</code> , and <code>AIX</code> .	<code>SOLARIS</code>
<code>adminpassword</code>	Admin user password	<code>dead_line</code>
<code>admin</code>	UNIX server administrator credentials for the SSH server	<code>root</code>

Attribute	Description	Default Attribute (Sample Value)
action	Action to be tested The value can be one 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
privateKey	Key for Public Key authentication	The value can be blank, or it can be the name and path of the private key file.
sudoFlag	Sudo Admin Mode flag	The value is YES for the SUDO Admin mode. It must be NO if the SUDO Admin mode is not used.

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

For UNIX:

```
OIM_home/xellerate/XLIntegrations/SSH/tests/scripts/SSH.sh
```

For Microsoft Windows:

```
OIM_home/xellerate/XLIntegrations/SSH/tests/scripts/SSH.bat
```

## Troubleshooting

The following table lists solutions to some commonly encountered issues associated with the connector.

Problem Description	Solution
Process definition: SSH User Process task: Create User <b>Returned Error Message:</b> Not able to connect successfully to the UNIX server <b>Returned Error Code:</b> SSH_USERCREATION_NOTCONNECTED_FAIL	Check if the UNIX server is running and accessible. In addition, check the admin credentials entered in the IT resource.

<b>Problem Description</b>	<b>Solution</b>
<p>Process definition: SSH User Process task: Create User</p> <p><b>Returned Error Message:</b> User does not have creation rights on the UNIX server</p> <p><b>Returned Error Code:</b> SSH_USERCREATION_NORIGHTS_FAIL</p>	<p>Check the admin credentials entered in the IT resource.</p>
<p>Process definition: SSH User Process task: Create User</p> <p><b>Returned Error Message:</b> Oracle Identity Manager is not able to create a user successfully due to a missing password file</p> <p><b>Returned Error Code:</b> SSH_USERCREATION_MISSINGPASSWDFILE_FAIL</p>	<p>Check the availability of the <code>/etc/passwd</code> file on the UNIX server.</p>
<p>Process definition: SSH User Process task: Create User</p> <p><b>Returned Error Message:</b> User name already exists on the UNIX server</p> <p><b>Returned Error Code:</b> SSH_USERCREATION_USEREXISTS_FAIL</p>	<p>Check the user name that you have entered. A user with the same name already exists on the UNIX server.</p>
<p>Process definition: SSH User Process task: Create User</p> <p><b>Returned Error Message:</b> User ID already exists and is unique or specified user ID is out of range</p> <p><b>Returned Error Code:</b> SSH_USERCREATION_USERID_FAIL</p>	<p>Check the user ID that you have entered. Another user may have the same user ID on the UNIX server or the value of the user ID may be out of range.</p>
<p>Process definition: SSH User Process task: Create User</p> <p><b>Returned Error Message:</b> User name too long</p> <p><b>Returned Error Code:</b> SSH_USERCREATION_NAMEFORMAT_FAIL</p>	<p>Check the user name that you have entered.</p>
<p>Process definition: SSH User Process task: Create User</p> <p><b>Returned Error Message:</b> User ID already exists and is unique or specified user ID is out of range</p> <p><b>Returned Error Code:</b> SSH_USERCREATION_USERID_FAIL</p>	<p>Check the user ID that you have entered. Another user may have the same ID on the UNIX server or the value of the user ID may be out of range.</p>

<b>Problem Description</b>	<b>Solution</b>
Process definition: SSH User Process task: Create User <b>Returned Error Message:</b> Group name or ID mismatch <b>Returned Error Code:</b> SSH_USERCREATION_NOGROUP_FAIL	Check the primary group name that you have entered. The group name entered should exist on the UNIX server. In addition, spaces are not allowed in the group name.
Process definition: SSH User Process task: Create User <b>Returned Error Message:</b> Missing default shell <b>Returned Error Code:</b> SSH_USERCREATION_NOSHELL_FAIL	Check the default shell that you have specified. The default shell specified should be installed on the UNIX server.
Process definition: SSH User Process task: Create User <b>Returned Error Message:</b> Wrong expiry date <b>Returned Error Code:</b> SSH_USERCREATION_DATERANGE_FAIL	Check the date selected.
Process definition: SSH User Process task: Create User <b>Returned Error Message:</b> Wrong password change time <b>Returned Error Code:</b> SSH_USERCREATION_WRONGCHANGETIME_FAIL	Check the password change time that you have entered.
Process definition: SSH User Process task: Create User <b>Returned Error Message:</b> Wrong GECOS data <b>Returned Error Code:</b> SSH_USERCREATION_GECOSFORMAT_FAIL	Check the GECOS data that you have entered. Spaces are not allowed.
Process definition: SSH User Process task: Create User <b>Returned Error Message:</b> Wrong Home Directory <b>Returned Error Code:</b> SSH_USERCREATION_HOMEDIR_FAIL	Check the home directory that you have specified.

<b>Problem Description</b>	<b>Solution</b>
Process definition: SSH User Process task: Create User <b>Returned Error Message:</b> Wrong Home Directory <b>Returned Error Code:</b> SSH_USERCREATION_SETPASSWORD_FAIL	Check the password that you specify.
Process definition: SSH User Process task: Delete User <b>Returned Error Message:</b> Not able to connect to the UNIX server <b>Returned Error Code:</b> SSH_USERDELETION_NOTCONNECTED_FAIL	Check if the UNIX server is running and accessible. In addition, check the admin credentials specified in the IT resource.
Process definition: SSH User Process task: Delete User <b>Returned Error Message:</b> Oracle Identity Manager administrator does not have deletion rights on the UNIX server <b>Returned Error Code:</b> SSH_USERDELETION_NORIGHTS_FAIL	Check the admin credentials specified in the IT resource.
Process definition: SSH User Process task: Delete User <b>Returned Error Message:</b> User does not exist on the UNIX server <b>Returned Error Code:</b> SSH_USERDELETION_NOUSER_FAIL	Check if the particular user exists on the UNIX server.
Process definition: SSH User Process task: GECOS Updated <b>Returned Error Message:</b> Not able to connect to the UNIX server <b>Returned Error Code:</b> SSH_UPDATEGECOS_NOTCONNECTED_FAIL	Check if the UNIX server is running and accessible. In addition, check the admin credentials specified in the IT resource.
Process definition: SSH User Process task: GECOS Updated <b>Returned Error Message:</b> Oracle Identity Manager administrator does not have deletion rights on the UNIX server <b>Returned Error Code:</b> SSH_UPDATEGECOS_NORIGHTS_FAIL	Check the admin credentials specified in the IT resource.

<b>Problem Description</b>	<b>Solution</b>
<p>Process definition: SSH User                      Process task: GECOS Updated</p> <p><b>Returned Error Message:</b>                      User does not exist on the UNIX server</p> <p><b>Returned Error Code:</b>                      SSH_UPDATEGECOS_NOUSER_FAIL</p>	<p>Check if the particular user exists on the UNIX server.</p>
<p>Process definition: SSH User                      Process task: GECOS Updated</p> <p><b>Returned Error Message:</b>                      Update user GECOS failed due to data format or size</p> <p><b>Returned Error Code:</b>                      SSH_UPDATEGECOS_FORMAT_FAIL</p>	<p>Check the GECOS data that you have entered. Spaces are not allowed.</p>
<p>Process definition: SSH User                      Process task: Password Change Time Updated</p> <p><b>Returned Error Message:</b>                      Not able to connect to the target system</p> <p><b>Returned Error Code:</b>                      SSH_UPDATECHANGETIME_NOTCONNECTED_FAIL</p>	<p>Check if the UNIX server is running and accessible. In addition, check the admin credentials specified in the IT resource.</p>
<p>Process definition: SSH User                      Process task: Password Change Time Updated</p> <p><b>Returned Error Message:</b>                      Oracle Identity Manager administrator does not have deletion rights on the UNIX server</p> <p><b>Returned Error Code:</b>                      SSH_UPDATECHANGETIME_NORIGHTS_FAIL</p>	<p>Check the admin credentials specified in the IT resource.</p>
<p>Process definition: SSH User                      Process task: Password Change Time Updated</p> <p><b>Returned Error Message:</b>                      User does not exist on the UNIX server</p> <p><b>Returned Error Code:</b>                      SSH_UPDATECHANGETIME_NOUSER_FAIL</p>	<p>Check if the user exists on the UNIX server.</p>

<b>Problem Description</b>	<b>Solution</b>
<p>Process definition: SSH User            Process task: Password Change Time Updated</p> <p><b>Returned Error Message:</b>            Update password change time failed due to wrong change time format</p> <p><b>Returned Error Code:</b>            SSH_UPDATECHANGETIME_WRONGCHANGETIME_FAIL</p>	<p>Check the Password Change Time value that you have specified.</p>
<p>Process definition: SSH User            Process task: Home Directory Updated</p> <p><b>Returned Error Message:</b>            Not able to connect to the UNIX server</p> <p><b>Returned Error Code:</b>            SSH_UPDATEHOMEDIR_NOTCONNECTED_FAIL</p>	<p>Check if the UNIX server is running and accessible. In addition, check the admin credentials specified in the IT resource.</p>
<p>Process definition: SSH User            Process task: Home Directory Updated</p> <p><b>Returned Error Message:</b>            Oracle Identity Manager administrator does not have deletion rights on the UNIX server</p> <p><b>Returned Error Code:</b>            SSH_UPDATEHOMEDIR_NORIGHTS_FAIL</p>	<p>Check the admin credentials specified in the IT resource.</p>
<p>Process definition: SSH User            Process task: Home Directory Updated</p> <p><b>Returned Error Message:</b>            User does not exist on the UNIX server</p> <p><b>Returned Error Code:</b>            SSH_UPDATEHOMEDIR_NOUSER_FAIL</p>	<p>Check if the user exists on the UNIX server.</p>
<p>Process definition: SSH User            Process task: Home Directory Updated</p> <p><b>Returned Error Message:</b>            Update user home directory failed due to wrong directory</p> <p><b>Returned Error Code:</b>            SSH_UPDATEHOMEDIR_INVALIDDIR_FAIL</p>	<p>Check the Home Directory that you have specified.</p>
<p>Process definition: SSH User            Process task: Default Shell Updated</p> <p><b>Returned Error Message:</b>            Not able to connect to the UNIX server</p> <p><b>Returned Error Code:</b>            SSH_UPDATESHELL_NOTCONNECTED_FAIL</p>	<p>Check if the UNIX server is running and accessible. In addition, check the admin credentials specified in the IT resource.</p>

<b>Problem Description</b>	<b>Solution</b>
<p>Process definition: SSH User                      Process task: Default Shell Updated</p> <p><b>Returned Error Message:</b>                      Oracle Identity Manager administrator does not have deletion rights on the UNIX server</p> <p><b>Returned Error Code:</b>                      SSH_UPDATESHELL_NORIGHTS_FAIL</p>	<p>Check the admin credentials specified in the IT resource.</p>
<p>Process definition: SSH User                      Process task: Default Shell Updated</p> <p><b>Returned Error Message:</b>                      User does not exist on the UNIX server</p> <p><b>Returned Error Code:</b>                      SSH_UPDATESHELL_NOUSER_FAIL</p>	<p>Check if the user exists on the UNIX server.</p>
<p>Process definition: SSH User                      Process task: Default Shell Updated</p> <p><b>Returned Error Message:</b>                      Update user shell failed because the specified shell does not exist</p> <p><b>Returned Error Code:</b>                      SSH_UPDATESHELL_NOTEXIST_FAIL</p>	<p>Check the default shell that you have entered. The default shell specified should be installed on the UNIX server.</p>
<p>Process definition: SSH User                      Process task: User UID Updated</p> <p><b>Returned Error Message:</b>                      Not able to connect to the UNIX server</p> <p><b>Returned Error Code:</b>                      SSH_UPDATEUID_NOTCONNECTED_FAIL</p>	<p>Check if the UNIX server is running and accessible. In addition, check the admin credentials specified in the IT resource.</p>
<p>Process definition: SSH User                      Process task: User UID Updated</p> <p><b>Returned Error Message:</b>                      Oracle Identity Manager administrator does not have deletion rights on the UNIX server</p> <p><b>Returned Error Code:</b>                      SSH_UPDATEUID_NORIGHTS_FAIL</p>	<p>Check the admin credentials specified in the IT resource.</p>
<p>Process definition: SSH User                      Process task: User UID Updated</p> <p><b>Returned Error Message:</b>                      User does not exist on the UNIX server</p> <p><b>Returned Error Code:</b>                      SSH_UPDATEUID_NOUSER_FAIL</p>	<p>Check if the user exists on the UNIX server.</p>

<b>Problem Description</b>	<b>Solution</b>
<p>Process definition: SSH User            Process task: User UID Updated  <b>Returned Error Message:</b>            User UID already exists and unique  <b>Returned Error Code:</b>            SSH_UPDATEUID_UNIQUE_FAIL</p>	<p>Check the user UID that you have specified. Another user may have the same UID on the UNIX server.</p>
<p>Process definition: SSH User            Process task: User UID Updated  <b>Returned Error Message:</b>            Specified user UID is too long  <b>Returned Error Code:</b>            SSH_UPDATEUID_SIZE_FAIL</p>	<p>Check the user UID that you have specified. The value specified is out of the acceptable range.</p>
<p>Process definition: SSH User            Process task: Account Expiry Date Updated  <b>Returned Error Message:</b>            Not able to connect to the UNIX server  <b>Returned Error Code:</b>            SSH_UPDATEEXPDATE_NOTCONNECTED_FAIL</p>	<p>Check whether the UNIX server is running and accessible. In addition, check the admin credentials specified in the IT resource.</p>
<p>Process definition: SSH User            Process task: Account Expiry Date Updated  <b>Returned Error Message:</b>            Oracle Identity Manager administrator does not have deletion rights on the UNIX server  <b>Returned Error Code:</b>            SSH_UPDATEEXPDATE_NORIGHTS_FAIL</p>	<p>Check the admin credentials specified in the IT resource.</p>
<p>Process definition: SSH User            Process task: Account Expiry Date Updated  <b>Returned Error Message:</b>            User does not exist on the UNIX server  <b>Returned Error Code:</b>            SSH_UPDATEEXPDATE_NOUSER_FAIL</p>	<p>Check if the user exists on the UNIX server.</p>
<p>Process definition: SSH User            Process task: Account Expiry Date Updated  <b>Returned Error Message:</b>            User expiry date not updated due to wrong date  <b>Returned Error Code:</b>            SSH_UPDATEEXPDATE_DATERANGE_FAIL</p>	<p>Check the account expiry date that you have specified.</p>

Problem Description	Solution
<p>Process definition: SSH User                      Process task: Primary Group Name Updated  <b>Returned Error Message:</b>                      Not able to connect to the UNIX server  <b>Returned Error Code:</b>                      SSH_UPDATEGROUP_NOTCONNECTED_FAIL</p>	<p>Check if the UNIX server is running and accessible. In addition, check the admin credentials specified in the IT resource.</p>
<p>Process definition: SSH User                      Process task: Primary Group Name Updated  <b>Returned Error Message:</b>                      Oracle Identity Manager administrator does not have deletion rights on the UNIX server  <b>Returned Error Code:</b>                      SSH_UPDATEGROUP_NORIGHTS_FAIL</p>	<p>Check the admin credentials specified in the IT resource.</p>
<p>Process definition: SSH User                      Process task: Primary Group Name Updated  <b>Returned Error Message:</b>                      User does not exist on the UNIX server  <b>Returned Error Code:</b>                      SSH_UPDATEGROUP_NOUSER_FAIL</p>	<p>Check if the user exists on the UNIX server.</p>
<p>Process definition: SSH User                      Process task: Primary Group Name Updated  <b>Returned Error Message:</b>                      Group name or group ID does not exist on the UNIX server  <b>Returned Error Code:</b>                      SSH_UPDATEGROUP_NOGROUP_FAIL</p>	<p>Check the primary group name that you have specified.</p>
<p>Process definition: SSH User                      Process task: Password Updated  <b>Returned Error Message:</b>                      Not able to connect to the UNIX server  <b>Returned Error Code:</b>                      SSH_SETPASSWORD_NOTCONNECTED_FAIL</p>	<p>Check if the UNIX server is running and accessible. In addition, check the admin credentials specified in the IT resource.</p>
<p>Process definition: SSH User                      Process task: Password Updated  <b>Returned Error Message:</b>                      Oracle Identity Manager administrator does not have deletion rights on the UNIX server  <b>Returned Error Code:</b>                      SSH_SETPASSWORD_NORIGHTS_FAIL</p>	<p>Check the admin credentials specified in the IT resource.</p>

<b>Problem Description</b>	<b>Solution</b>
<p>Process definition: SSH User</p> <p>Process task: Password Updated</p> <p><b>Returned Error Message:</b></p> <p>User does not exist on the UNIX server</p> <p><b>Returned Error Code:</b></p> <p>SSH_SETPASSWORD_NOUSER_FAIL</p>	<p>Check if the user exists on the UNIX server.</p>
<p>Process definition: SSH User</p> <p>Process task: Password Updated</p> <p><b>Returned Error Message:</b></p> <p>Group name or group ID does not exist on the UNIX server</p> <p><b>Returned Error Code:</b></p> <p>SSH_SETPASSWORD_MISMATCH_FAIL</p>	<p>The password specified and the one entered again for confirmation must match.</p>
<p>Process definition: SSH User</p> <p>Process task: Password Updated</p> <p><b>Returned Error Message:</b></p> <p>Group name or group ID does not exist on the UNIX server</p> <p><b>Returned Error Code:</b></p> <p>SSH_SETPASSWORD_SIZE_FAIL</p>	<p>Enter the password according to the policy defined on the UNIX server.</p>
<p>Process definition: SSH User</p> <p>Process task: Secondary Group Name Updated</p> <p><b>Returned Error Message:</b></p> <p>User does not exist on the UNIX server</p> <p><b>Returned Error Code:</b></p> <p>SSH_UPDATESECONDARYGROUP_NOUSER_FAIL</p>	<p>Check if the user exists on the UNIX server.</p>
<p>Process definition: SSH User</p> <p>Process task: Secondary Group Name Updated</p> <p><b>Returned Error Message:</b></p> <p>Oracle Identity Manager administrator does not have deletion rights on the UNIX server</p> <p><b>Returned Error Code:</b></p> <p>SSH_UPDATESECONDARYGROUP_NORIGHTS_FAIL</p>	<p>Check the admin credentials specified in the IT resource.</p>

<b>Problem Description</b>	<b>Solution</b>
<p>Process definition: SSH User</p> <p>Process task: Secondary Group Name Updated</p> <p><b>Returned Error Message:</b></p> <p>Group name or group ID does not exist on the UNIX server</p> <p><b>Returned Error Code:</b></p> <p>SSH_UPDATESECONDARYGROUP_NOGROUP_FAIL</p>	<p>Check the secondary group names that you specify.</p>
<p>Process definition: SSH User</p> <p>Process task: Secondary Group Name Updated</p> <p><b>Returned Error Message:</b></p> <p>Oracle Identity Manager is not able to connect successfully to the UNIX server</p> <p><b>Returned Error Code:</b></p> <p>SSH_UPDATESECONDARYGROUP_NOTCONNECTED_FAIL</p>	<p>Check if the UNIX server is running and accessible. In addition, check the admin credentials specified in the IT resource.</p>
<p>Process definition: SSH User</p> <p>Process task: Inactive Days Updated</p> <p><b>Returned Error Message:</b></p> <p>Oracle Identity Manager administrator does not have update rights in Target System</p> <p><b>Returned Error Code:</b></p> <p>SSH_UPDATEINACTIVEDAYS_NORIGHTS_FAIL</p>	<p>Check the admin credentials specified in the IT resource.</p>
<p>Process definition: SSH User</p> <p>Process task: Inactive Days Updated</p> <p><b>Returned Error Message:</b></p> <p>Oracle Identity Manager is not able to connect successfully to the target system</p> <p><b>Returned Error Code:</b></p> <p>SSH_UPDATEINACTIVEDAYS_NOTCONNECTED_FAIL</p>	<p>Check if the UNIX server is running and accessible. In addition, check the admin credentials specified in the IT resource.</p>
<p>Process definition: SSH User</p> <p>Process task: Inactive Days Updated</p> <p><b>Returned Error Message:</b></p> <p>User does not exist on the target system</p> <p><b>Returned Error Code:</b></p> <p>SSH_UPDATEINACTIVEDAYS_NOUSER_FAIL</p>	<p>Check if the user exists on the UNIX server.</p>

<b>Problem Description</b>	<b>Solution</b>
<p>Process definition: SSH User            Process task: Inactive Days Updated</p> <p><b>Returned Error Message:</b>            Invalid numeric number</p> <p><b>Returned Error Code:</b>            SSH_UPDATEINACTIVEDAYS_INVALID_NUMERIC_ARGUMENT_FAIL</p>	<p>Check if the value specified in the Inactive Days field is numeric.</p>
<p>Process definition: SSH User            Process task: User Login Updated</p> <p><b>Returned Error Message:</b>            Oracle Identity Manager is not able to connect successfully to the target system</p> <p><b>Returned Error Code:</b>            SSH_UPDATELOGINCLASS_NOTCONNECTED_FAIL</p>	<p>Check if the UNIX server is running and accessible. In addition, check the admin credentials specified in the IT resource.</p>
<p>Process definition: SSH User            Process task: User Login Updated</p> <p><b>Returned Error Message:</b>            Oracle Identity Manager administrator does not have update rights in target system</p> <p><b>Returned Error Code:</b>            SSH_UPDATELOGINCLASS_NORIGHTS_FAIL</p>	<p>Check the secondary group names that you have specified.</p>
<p>Process definition: SSH User            Process task: User Login Updated</p> <p><b>Returned Error Message:</b>            User does not exist on the target system</p> <p><b>Returned Error Code:</b>            SSH_UPDATELOGINCLASS_NOUSER_FAIL</p>	<p>Check if the user exists on the UNIX server.</p>
<p>Process definition: SSH User            Process task: Disable User</p> <p><b>Returned Error Message:</b>            Oracle Identity Manager is not able to connect successfully to the target system</p> <p><b>Returned Error Code:</b>            SSH_DISABLEUSER_NOTCONNECTED_FAIL</p>	<p>Check if the UNIX server is running and accessible. In addition, check the admin credentials specified in the IT resource.</p>
<p>Process definition: SSH User            Process task: Disable User</p> <p><b>Returned Error Message:</b>            Oracle Identity Manager administrator does not have update rights on the target system</p> <p><b>Returned Error Code:</b>            SSH_DISABLEUSER_NORIGHTS_FAIL</p>	<p>Check the admin credentials specified in the IT resource.</p>

<b>Problem Description</b>	<b>Solution</b>
Process definition: SSH User Process task: Disable User <b>Returned Error Message:</b> User does not exist on the target system <b>Returned Error Code:</b> SSH_DISABLEUSER_NOUSER_FAIL	Check if the user exists on the UNIX server.
Process definition: SSH User Process task: Enable User <b>Returned Error Message:</b> Oracle Identity Manager is not able to connect successfully to the target system <b>Returned Error Code:</b> SSH_ENABLEUSER_NOTCONNECTED_FAIL	Check if the UNIX server is running and accessible. In addition, check the admin credentials specified in the IT resource.
Process definition: SSH User Process task Enable User <b>Returned Error Message:</b> Oracle Identity Manager is not able to connect successfully to the target system <b>Returned Error Code:</b> SSH_ENABLEUSER_NOTCONNECTED_FAIL	Check the admin credentials specified in the IT resource.
Process definition: SSH User Process task: Enable User <b>Returned Error Message:</b> User does not exist on the target system <b>Returned Error Code:</b> SSH_ENABLEUSER_NOUSER_FAIL	Check if the user exists on the UNIX server.

---



---

**Note:**

The following run-time exception message is displayed when:

- The credentials in the IT resource are incorrect.
- The number of concurrent connections to the target system exceeds the permitted value. For example, if a target system accepts only two concurrent connections, then the third connection is not allowed and the error message is displayed.

Run-time exception message:

```

Java.lang.RuntimeException:Exceeded
timeout of 120000ms while waiting..
at com.jscape.inet.telnet.TelnetTask$TelnetTaskMonitor.run (Unknown
Source)

```

---



---

---

---

## 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 an SSH 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:  

```
"SSH_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 Names 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.
  - The connector has been tested and certified only for RSA keys, and not DSA. In addition, this connector has been tested and certified for only single key configuration and not multiple keys.
  - Public Key Authentication provisioning is not supported by this connector if it is implemented through the SUDO Admin mode. Refer to the "[Step 2: Configuring the Target System](#)" section on page 2-2 for more details.
  - 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 SSH

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

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

Oracle Identity Manager Attribute	UNIX SSH Attribute	Description
Secondary Group Names	supplementary groups	List of supplementary groups, of which the user is also a member  In the value specified, group 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) character.
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.

---

<b>Oracle Identity Manager</b>		
<b>Attribute</b>	<b>UNIX SSH Attribute</b>	<b>Description</b>
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 Factory form, 2-27  
Adapter Manager form, 2-27  
adapters, compiling, 2-26  
additional files, 2-1  
Administrative and User Console, 2-20  
attributes mappings, A-1

## C

---

changing input locale, 2-18  
clearing server cache, 2-18  
compiling adapters, 2-26  
configuring

- connector for multiple installations of the target system, 2-27
- Oracle Identity Manager server, 2-18
- reconciliation, 2-23

connector files and directories

- copying, 2-17
- description, 1-4
- destination directories, 2-17
- installation directory, 1-4, 2-17

connector testing, 3-1  
connector version number, determining, 1-5  
creating scheduled tasks, 2-23

## D

---

defining

- IT resources, 2-21
- scheduled tasks, 2-23

deployment

- requirements, 2-1

Design Console, 2-23, 2-24  
determining version number of connector, 1-5

## E

---

enabling logging, 2-19  
errors, 3-2  
external code files, 2-1

## F

---

files

additional, 2-1  
external code, 2-1  
*See also* XML files  
functionality supported, 1-1  
functions available, 1-1

## G

---

globalization features, 1-3

## I

---

importing connector XML files, 2-20  
input locale, changing, 2-18  
issues, 4-1  
IT resources

- defining, 2-21

## L

---

limitations, 4-1  
logging enabling, 2-19

## 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, 1-3

## O

---

Oracle Identity Manager Administrative and User Console, 2-20  
Oracle Identity Manager Design Console, 2-23, 2-24  
Oracle Identity Manager Release 9.0.1, 2-26  
Oracle Identity Manager server, configuring, 2-18

## P

---

problems, 3-2  
process tasks, 1-1  
provisioning

- functions, 1-1

## **R**

---

reconciliation  
  adding prerequisites for, 2-23  
  configuring, 2-23  
  enabling in Oracle Identity Manager Release  
    9.0.1, 2-26  
  functions, 1-1  
  module, 1-3  
  scheduled tasks, 2-24  
  trusted source, 2-21  
requirements for deploying, 2-1

## **S**

---

scheduled tasks, 2-24  
  defining, 2-23  
server cache, clearing, 2-18  
supported  
  languages, 1-3  
  releases of Oracle Identity Manager, 2-1  
  target systems, 2-1

## **T**

---

target system, multiple installations, 2-27  
target systems supported, 2-1  
testing the connector, 3-1  
troubleshooting, 3-2  
trusted source reconciliation, 2-21

## **U**

---

user attribute mappings, A-1

## **V**

---

version number of connector, determining, 1-5

## **X**

---

XML files, importing, 2-20