Oracle® Identity Manager

Connector Guide for UNIX SSH

Release 9.0.4

E10447-06

July 2009

Oracle Identity Manager Connector Guide for UNIX SSH, Release 9.0.4

E10447-06

Primary Author: Alankrita Prakash

Contributing Authors: Debapriya Datta, Devanshi Mohan, Lyju Vadassery

Contents

3 Configuring the Connector

4 Testing and Troubleshooting

5 Known Issues

A Attribute Mappings Between Oracle Identity Manager and UNIX SSH

B Privileges Required for Performing Provisioning and Reconciliation

C Sample Transformation Class

Index

Preface

This guide provides information about Oracle Identity Manager Connector for UNIX SSH.

Audience

This guide is intended for resource administrators and target system integration teams.

Documentation Accessibility

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

Deaf/Hard of Hearing Access to Oracle Support Services

To reach Oracle Support Services, use a telecommunications relay service (TRS) to call Oracle Support at 1.800.223.1711. An Oracle Support Services engineer will handle technical issues and provide customer support according to the Oracle service request process. Information about TRS is available at `http://www.fcc.gov/cgb/consumerfacts/trs.html`, and a list of phone numbers is available at `http://www.fcc.gov/cgb/dro/trsphonebk.html`.

Related Documents

For information about installing and using Oracle Identity Manager, see the Oracle Identity Manager documentation library.

For generic information about connectors, see *Oracle Identity Manager Connector Concepts*.

The following Oracle Technology Network page provides links to Oracle Identity Manager documentation:

`http://www.oracle.com/technology/documentation/oim.html`

Documentation Updates

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

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

Conventions

The following text conventions are used in this document:

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

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

This chapter provides an overview of the updates made to the software and documentation for the UNIX SSH connector in release 9.0.4.7.

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

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

- Software Updates

  This section describes updates made to the connector software.

- Documentation-Specific Updates

  This section describes major changes made to this guide. These changes are not related to software updates.

Software Updates

The following sections discuss updates made from release 9.0.4 to the current release of the connector:

- Software Updates in Release 9.0.4.2
- Software Updates in Release 9.0.4.3
- Software Updates in Release 9.0.4.4
- Software Updates in Release 9.0.4.5
- Software Updates in Release 9.0.4.6
- Software Updates in Release 9.0.4.7

Software Updates in Release 9.0.4.2

The following are software updates in release 9.0.4.2:

- In Step 2 of the "Installing and Configuring SUDO" section for Solaris, the `usermod` command has been added to the list of commands used by the target system.
- In the "Enabling Logging" section, the name of the adapter for this connector has been changed from `ADAPTERS.TELNETSSH` to `OIMCP.TELNETSSH`.

- In the "Compiling Adapters" section, the `SSH updateHomeDir` adapter has been added to the list of adapters.
- In the IT resource definition, the following parameters have been removed:
  - `Login Prompt`
  - `Password Prompt`
  - `Target Locale`
  - `Supported Character Encoding (en_US) - Target`

  The following scheduled task attributes have been converted into IT resource parameters:
  - `Passwd Mirror File/User Mirror File`
  - `Shadow Mirror File`
  - `Target Date Format`
- The following table lists issues resolved in release 9.0.4.2:

Bug Number	Issue	Resolution
6375896	Target resource reconciliation threw exceptions when users were reconciled from Linux using a SUDO admin user.	Target resource reconciliation issues related to Linux used in the SUDO mode have been resolved.
6609731	The `Supported Character Encoding` and `Target Locale` IT resource parameters were not used by the connector.	The `Supported Character Encoding` and `Target Locale` IT resource parameters have been removed.
6642345	The connection retry feature of the connector was not working correctly.	Issues related to the connection retry feature have been resolved.
6680047	If a connection retry attempt was made, then previous sessions were not released and new sessions were established each time.	Connectivity issues related to session leakage have been resolved.
6728741	An incorrect response was received from the connector if the username value was greater than 8 characters and the Create Home directory check box was checked.	The responses received from the connector have been corrected.
6742869	A user could not be provisioned if there were spaces in value of the GECOS field.	Spaces are now allowed in the GECOS field.
6766705 and 6801405	The status of the resource object stayed at `Provisioned` even when provisioning tasks were rejected.	Issues related to the resource object status and response during provisioning have been resolved.
6786399	The connector was unable to handle responses from target systems running a non-English locale.	Responses from target systems running a non-English locale are now handled correctly.
6801537	During reconciliation, temporary files were created in the `/etc` directory.	During reconciliation, temporary files are now created in the `/tmp` folder.

Bug Number	Issue	Resolution
6837471	A user could not be provisioned with spaces in the values of any of the user attributes.	Spaces are now allowed in many of the user attributes.
5180204	On AIX computers, the connector was not able to reconcile a large number of records.	Issues related to the reconciliation of a large number of users on AIX have been resolved.
5502324	Date format parsing errors were encountered during reconciliation.	The date format parsing error that was encountered during the user reconciliation has been resolved.
5503100	The message displayed when the user name had multibyte characters during a Create User provisioning operation was incorrect.	The message displayed when the user name has multibyte characters during a Create User provisioning operation has been modified.
5647992	On Linux, Solaris, and AIX computers, the Home Directory attribute could not be updated.	The Home Directory attribute is updated correctly on Linux, Solaris, and AIX targets.
5180227	The IT Resources contained two redundant parameters, `Login Prompt` and `Password Prompt`.	The `Login Prompt` and `Password Prompt` IT resource parameters have been deleted.
6604117	The Password and Confirm Password fields on the process form were not encrypted.	The Password and Confirm Password fields have been modified to accept encrypted values.
6310073	During provisioning, if user creation on the target system failed at some stage, then the user was not cleaned up from the target system although the status of the resource was `Provisioning`. When this happened, another user with the same name could not be provisioned.	During provisioning, if the user is not created properly on the target, then the user is deleted from the target system and the resource object status is set to `Provisioning`.

Software Updates in Release 9.0.4.3

The following are software updates in release 9.0.4.3:

- The `Primary Group Name` field on the process form has been converted into a lookup field. During a provisioning operation, you can now select a primary group instead of entering the name of the group. The `TelnetSSHGroupLookupReconTask` scheduled task has been added to reconcile (synchronize) the values in the lookup definition with primary group names in the target system.
- The name of the target resource reconciliation scheduled task has been changed from `SSH User Non Trusted Reconciliation task` to `SSH Target Resource User Reconciliation Task`.
- The level of detail has been increased for data logged when you set the log level to `DEBUG`. With this log level, it is now easier to track down the cause of an error recorded in the log file.
- The following table lists issues resolved in release 9.0.4.3:

Bug Number	Issue	Resolution
7121688	On AIX 5.3, the `SSH_USERUID_SIZE_FAIL` or `SSH_USER_FAIL` exception was thrown if you tried to update the User Login attribute through a provisioning operation.	This issue has been resolved. You can now update the User Login attribute through a provisioning operation. **Note:** The Update User Login provisioning operation is not supported by default on AIX 4.x and 5.1. However, if you upgrade these versions of AIX to support the useradd, usermod, and userdel commands, then you can perform the Update User Login provisioning operation.
7143460	During a reconciliation run on AIX, the `ArrayIndexOutofBounds` exception was thrown if the number of deleted records fetched from the target system was more than the number of newly created or updated records fetched from the target system.	This issue has been resolved. An exception is not thrown if the number of deleted records fetched from the target system is more than the number of newly created or updated records fetched from the target system.
7143486	If a reconciliation run ended in an exception, then the connection with the target system was not closed.	This issue has been resolved. The connection with the target system is closed even if a reconciliation run ends in an exception.

Software Updates in Release 9.0.4.4

The following are software updates in release 9.0.4.4:

- Using the Connector Installer

Using the Connector Installer

From Oracle Identity Manager release 9.1.0 onward, the Administrative and User Console provides the Connector Installer feature. This feature can be used to automate the connector installation procedure.

See "Installing the Connector on Oracle Identity Manager Release 9.1.0 or Later" on page 2-18 for details.

Software Updates in Release 9.0.4.5

The following are software updates in release 9.0.4.5:

- Support for Role-Based Access Control (RBAC) on Solaris
- Resolved Issues in Release 9.0.4.5

Support for Role-Based Access Control (RBAC) on Solaris

In earlier releases, you had to provide the credentials of the root or sudo user for letting Oracle Identity Manager communicate with the Solaris target system. This release supports the role-based access control (RBAC) feature of Solaris. From this release onward, Oracle Identity Manager can communicate with Solaris by using a user account to which you assign the minimum required privileges.

See "Creating a Target System User Account for Connector Operations" on page 2-3 for more information.

The following are some of the changes made in the IT resource:

- The `Whether SUDO Admin Mode` parameter has been renamed to `Sudo Or RBAC`.

- Descriptions of the `Admin UserId` and `Admin Password/Private file Pwd` parameters have been modified.
- The `RBAC Role Name` and `RBAC Role Passwd` parameters have been added.

See the "Deploying the Connector" chapter for information about these parameters.

Resolved Issues in Release 9.0.4.5

The following table lists issues resolved in release 9.0.4.5:

Bug Number	Issue	Resolution
5503263	The "Create Home Directory" field is a check box on the Administrative and User Console. If you selected this check box, the numeral 1 was displayed on the page that summarizes input you provide during provisioning operations.	The check box has been changed to a radio button. If you select the "Create Home Directory" option, then the word "Yes" is displayed on the page that summarizes input. If you do not select the option, then the word "No" is displayed.
7133380	A user for whom an SSH account was created on AIX through a provisioning operation was forced to change the password at first login.	Password change at first login is not enforced for newly created SSH accounts on AIX.
7225692	To stop a scheduled task, you use the Stop Execution option in the Design Console. This option did not work in earlier releases.	You can now use the Stop Execution option to stop scheduled tasks. **Note:** When you stop a batched reconciliation run, reconciliation stops at the end of the batch being reconciled.
7345302	During a provisioning operation, the home directory was not created if you specified an invalid path on the target system host computer. However, the status of the process task was Completed.	If an invalid home directory path is specified, then the "Invalid Home directory" error message is displayed on the Administrative and User Console.
7347256	An error was thrown when a user connected to an HP-UX target system was updated through a provisioning operation performed on Oracle Identity Manager. The response from the target system was not correctly parsed and displayed as an error message on the Administrative and User Console.	The "User currently in use" message is displayed if you try to update any attribute of a user who is currently logged in to the target system.

Software Updates in Release 9.0.4.6

The following table lists issues resolved in release 9.0.4.6:

Bug Number	Issue	Resolution
7478452	You use the IT resource to specify the credentials of the SUDO user that you want to use for connector operations. If this SUDO user did not have the required permissions, then the target system did not allow you to perform Disable User provisioning operations. This is expected behavior. However, the status of the user was set to Disabled on Oracle Identity Manager even though the status of the user on the target system remained unchanged.	This issue has been resolved. If the SUDO user does not have the permissions required to disable users on the target system, then an appropriate message is displayed on the Administrative and User Console.
7503701	The target system does not allow you to delete a user who is logged in to the system. This is expected behavior. However, even when the target system did not allow the deletion of a user, the status of the user (resource) on Oracle Identity Manager was changed to Deleted (Revoked).	This issue has been resolved. If the target system does not allow the deletion of a user, then an appropriate message is displayed as the outcome of the Delete User provisioning operation. The item describing this issue has been removed from the "Known Issues" chapter.

Software Updates in Release 9.0.4.7

The following are software updates in release 9.0.4.7:

- Support for New Target System
- Resolved Issues

Support for New Target System

From this release onward, the connector adds support for Oracle Enterprise Linux 5.2 as a target system.

This target system is mentioned in "Verifying Deployment Requirements" on page 2-1.

Resolved Issues

The following table lists issues resolved in release 9.0.4.7:

Bug Number	Issue	Resolution
7520249	During reconciliation, you could not transform values of the target system field before they were stored in Oracle Identity Manager.	This issue has been resolved. You can now transform the values of the target system fields before they are stored in Oracle Identity Manager. See the "Transforming Data Reconciled Into Oracle Identity Manager" chapter in the connector guide for more information.
7563415	During reconciliation, the Group Name field was reconciled as a number and not as the exact name because it was stored directly as the group ID in the target system.	This issue has been resolved. During reconciliation, the exact name of the Group Name field is reconciled.
8341984	In the Create User process task, the default value of the Map To variable was IT Resource. This value was incorrect.	This issue has been resolved. The `Map To` variable in the Create User process task displays the correct default value. The default value of Map To variable is now `Process Data`.

Bug Number	Issue	Resolution
8396795	During connector deployment, the lib/xliSSH.jar file on the installation media was not automatically copied into the *OIM_HOME*/xellerate/ScheduleTask directory.	This issue has been resolved. The lib/xliSSH.jar file is now automatically copied to the *OIM_HOME*/xellerate/ScheduleTask directory.

Documentation-Specific Updates

The following sections discuss documentation-specific updates made from release 9.0.4 to the current release of the connector:

- Documentation-Specific Updates in Releases 9.0.4.1 Through 9.0.4.4
- Documentation-Specific Updates in Release 9.0.4.5
- Documentation-Specific Updates in Release 9.0.4.6
- Documentation-Specific Updates in Release 9.0.4.7

Documentation-Specific Updates in Releases 9.0.4.1 Through 9.0.4.4

The following documentation-specific updates have been made in releases 9.0.4.1 through 9.0.4.4:

- Changes have been made in the following sections:
  - Adding Custom Attributes for Reconciliation
  - Adding Custom Attributes for Provisioning
- In the "Known Issues" chapter, the following items have been added:
  - "The Update User Login function is not supported on most versions of AIX."
  - A reconciliation run stops if the scheduled task code encounters target system user data containing the character or characters that are same as the shell prompt of the target system.
- From the "Known Issues" chapter, the following item has been removed:

  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`".

Documentation-Specific Updates in Release 9.0.4.5

The following are documentation-specific updates in release 9.0.4.5:

- In the "Deploying the Connector" chapter, the `Protocol` parameter has been added in the table that describes the IT resource parameters.
- In the "Known Issues" chapter:
  - Bug numbers have been added for all the known issues.
  - The following guidelines have been moved from the "Known Issues" chapter to other parts of this guide:

    - 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 on 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 maximum permitted date value for account expiry is 31/12/2099.

  - The following point has been removed from the "Known Issues" chapter:

    - The Update Secondary Group Names and Update User Login functions do not work simultaneously.

Documentation-Specific Updates in Release 9.0.4.6

At some places in this guide, corrections have been made to address some documentation issues.

Documentation-Specific Updates in Release 9.0.4.7

The following are documentation-specific updates in release 9.0.4.7:

- Changes have been made in the following sections:
  - Verifying Deployment Requirements
  - Installing OpenSSH
  - Installing and Configuring SUDO
  - Configuring SSH Public Key Authentication
  - Scheduled Tasks for Trusted Source and Target Resource Reconciliation
- Section 3.4, "Transforming Data Reconciled Into Oracle Identity Manager" has been added
- The following point has been removed from the "Known Issues" chapter:

  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.
- The following appendixes have been added:
  - Appendix B, "Privileges Required for Performing Provisioning and Reconciliation"
  - Appendix C, "Sample Transformation Class"
- In the "Verifying Deployment Requirements" section, changes have been made in the "Target systems" row.

1 About the Connector

Oracle Identity Manager automates access rights management, security, and provisioning of IT resources. Oracle Identity Manager connectors are used to integrate Oracle Identity Manager with third-party applications. The connector for SSH is used to integrate Oracle Identity Manager with target systems running AIX, HP-UX, Linux, and Solaris, using the SSH protocol.

This chapter contains the following sections:

- Reconciliation Module
- Provisioning Module
- Supported Functionality
- Multilanguage Support
- Files and Directories on the Installation Media
- Determining the Release Number of the Connector

> **Note:** In this guide, the term *Oracle Identity Manager server* refers to the computer on which Oracle Identity Manager is installed.

1.1 Reconciliation Module

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

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

The following target system attributes are reconciled:

- User Login

Note: The 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 on 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.

- 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.

1.1.1 Reconciled Xellerate User (OIM User) Fields

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

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

1.2 Provisioning Module

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

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

For this target system, the following fields are provisioned:

- User Login
- Password
- Secondary Group Names

- User UID
- Primary Group Name
- Default Shell
- GECOS
- Home Directory
- Account Expiry Date

> **Note:** During provisioning, the maximum permitted date value for account expiry is 31-Dec-2099.

- Password Change Time
- Create Home Directory
- Skeleton Directory
- Inactive Days

1.3 Supported Functionality

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

Function	Type	Description
Create User	Provisioning	Creates a user When you use this function, in the User Defined process form: ■ 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 Days 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.
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 **Note:** The home directory specified for a user should not contain spaces.
Update Account Expiry Date	Provisioning	Updates user properties according to a change in the Account Expiry Date attribute **Note:** During provisioning, the maximum permitted date value for account expiry is 31-Dec-2099.

Function	Type	Description
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 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 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.
Trusted Reconciliation for User	Reconciliation	Creates OIM 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

1.4 Multilanguage Support

The connector supports the following languages:

- Arabic
- Chinese Simplified
- Chinese Traditional
- Danish
- English
- French
- German

- Italian
- Japanese
- Korean
- Portuguese (Brazilian)
- Spanish

Note: However, the connector does not support the entry of multibyte characters in some of the fields. Appendix A, "Attribute Mappings Between Oracle Identity Manager and UNIX SSH" provides information about the fields in which multibyte characters are not supported.

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

1.5 Files and Directories on the Installation Media

The files and directories on the installation media are listed and described in Table 1–1.

Table 1–1 Files and Directories on the Installation Media

File in the Installation Media Directory	Description
`configuration/UNIX SSH-CI.xml`	This XML file contains configuration information that is used during connector installation.
`ext/sshfactory.jar`	This file contains the JSCAPE libraries. These libraries are used to open an SSH session with the target server. During connector deployment, this file is copied into the following directories: *OIM_HOME*/xellerate/ThirdParty
`lib/xliSSH.jar`	This file contains the Java classes that are required to support provisioning and reconciliation in SSH. During connector deployment, this file is copied into the following directories: *OIM_HOME*/xellerate/JavaTasks *OIM_HOME*/xellerate/ScheduleTask
Files in the `resources` directory	Each of these resource bundles contains language-specific information that is used by the connector. During connector deployment, these resource bundles are copied into the following directory: *OIM_HOME*/xellerate/connectorResources **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.
`scripts/sudoers`	This file contains the SUDO user specifications and configurations.
`test/config/config.properties`	This file is used to specify the parameters and settings required to connect to the target system by using the testing utility.

Table 1–1 (Cont.) Files and Directories on the Installation Media

File in the Installation Media Directory	Description
`test/config/log.properties`	This file is used to specify the log level and the directory in which the log file is to be created when you run the testing utility.
`config/userAttribute_NonAIX_prov.properties`	This file contains the parameters required for dynamic provisioning on non-AIX platforms.
`config/userAttribute_AIX_prov.properties`	This file contains the parameters required for dynamic provisioning on AIX platform.
`config/userAttribute_NonAIX_recon.properties`	This file contains the parameters required for dynamic reconciliation on non-AIX platforms.
`config/userAttribute_AIX_recon.properties`	This file contains the parameters required for dynamic reconciliation on AIX platform.
`test/scripts/SSH.bat` `test/scripts/SSH.sh`	This file contains the script required to run the client for running test calls from the Oracle Identity Manager server.
`xml/SSHNonTrustedUser.xml`	This XML file contains definitions for the following SSH User components of the connector: ■ IT resource type ■ IT resource ■ Resource object ■ Process definition ■ Process tasks ■ Adapters ■ Process form ■ Reconciliation scheduled task
`xml/XellSSHUser.xml`	This XML file contains the configuration for the Xellerate User (OIM User) and the definition of the trusted source reconciliation schedule task. You must import this file only if you plan to use the connector for trusted source reconciliation.

1.6 Determining the Release Number of the Connector

You might have a deployment of an earlier release of the connector. While deploying the latest release, you might want to know the release number of the earlier release. To determine the release number of the connector that has already been deployed:

1. In a temporary directory, extract the contents of the following JAR file:

   OIM_HOME`/xellerate/JavaTasks/xliSSH.jar`

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.

2 Deploying the Connector

Deploying the connector involves the following steps:

- Verifying Deployment Requirements
- Configuring the Target System
- Depending on the release of Oracle Identity Manager that you use, perform the procedures described in one of the following sections:
  - Installing the Connector on Oracle Identity Manager Release 9.1.0 or Later
  - Installing the Connector on Oracle Identity Manager Release 8.5.3.1 Through 9.0.3.x
- Configuring the Oracle Identity Manager Server

2.1 Verifying Deployment Requirements

The following table lists the deployment requirements for the connector.

Item	Requirement
Oracle Identity Manager	Oracle Identity Manager release 8.5.3.1 or later
Target systems	The target system can be any one of the following operating systems that support SSH 2.0: ■ HP-UX 11.11, 11.20 ■ IBM AIX 5L Version 5.2, 5.3 ■ Oracle Enterprise Linux 5.2 ■ Red Hat Enterprise Linux AS 2.1, 3, 4.x, Red Hat Enterprise Linux ES 3, 4.x ■ Solaris 8, 9, 10
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 configuring the IT resource. The procedure is described later in this guide. If you do not use a target system user account of the specified type, then an error message similar to the following would be displayed when Oracle Identity Manager tries to exchange data with the target system: `SSH_USER_NORIGHTS_FAIL`

Item	Requirement
Character encoding supported by the target system	The target system must support the default C (POSIX) locale. Use the following command to check the locale that the target system supports: `locale -a`

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

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

2.2 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)

2.2.1 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

2.2.1.1 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. Create a passwd mirror file on the target server by using a command similar to the following:

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

   You can specify any destination directory and file name when you run the command. While configuring the IT resource, you specify the name and path of this file as the value of the `Passwd Mirror File/User Mirror File` parameter of the IT resource for Solaris and Linux.

   > **Note:** The administrator account whose credentials you provide as part of the IT resource definition must have read and write permissions on this file.

3. Create a shadow mirror file on the target server by using a command similar to the following:

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

   You can specify any destination directory and file name when you run the command. While configuring the IT resource, you specify the name and path of this file as the value of the `Shadow Mirror File` parameter of the IT resource.

   > **Note:** The administrator account whose credentials you provide as part of the IT resource definition must have read and write permissions on this file.

4. For Solaris only:

   If you want to create and use a target system account with the minimum privileges required for connector operations, then perform the procedure described in "Creating a Target System User Account for Connector Operations" on page 2-3.

2.2.1.1.1 Creating a Target System User Account for Connector Operations Oracle Identity Manager uses a target system account for performing reconciliation and provisioning operations. On all supported target systems, this account must be either the root user or sudo user. On Solaris, the role-based access control (RBAC) feature can be applied to create an account and assign to it the minimum privileges required for connector operations. This is an alternative to the use of the root user and sudo user.

> **Note:** You use the IT resource to specify whether or not you want to use an RBAC user. Parameters of the IT resource are described later in this chapter.

To create a user account with the minimum required privileges:

1. Run the following command to create a role for the user.

   ```
   roleadd -d /export/home/ROLE_NAME -m ROLE_NAME
   ```

   In this command, replace *`ROLE_NAME`* with the name that you want to assign to the role, for example, `OIMRole`.

2. Run the following command to assign a password to the role:

   ```
   passwd ROLE_NAME
   ```

   At the prompt, enter a password for the role.

   > **See Also:** Appendix B, "Privileges Required for Performing Provisioning and Reconciliation" for information about the privileges required to run the commands that are used for provisioning and reconciliation

3. Create a profile for the user as follows:

   a. Open the `/etc/security/prof_attr` file in a text editor and insert the following line in the file:

      ```
      PROFILE_NAME:::Oracle Identity Manager Profile:
      ```

In this line, replace *PROFILE_NAME* with the name that you want to assign to the profile, for example, `OIMProf`.

b. Save and close the file.

4. Add execution attribute entries in the `/etc/security/exec_attr` file. Each entry defines a task to be run and the uid that the role will assume when running the task.

   Open the `/etc/security/exec_attr` file in a text editor, and insert the following lines:

   > **Note:** There are seven fields in this file, and the colon (:) is used as the delimiting character.
   >
   > On Solaris 10, the value `suser` can be replaced with `solaris`.
   >
   > Some of the entries contain `euid`. These instances of `euid` can be replaced with `uid`.

```
PROFILE_NAME:suser:cmd:::/usr/sbin/usermod:uid=0
PROFILE_NAME:suser:cmd:::/usr/sbin/useradd:uid=0
PROFILE_NAME:suser:cmd:::/usr/sbin/userdel:uid=0
PROFILE_NAME:suser:cmd:::/usr/bin/passwd:uid=0
PROFILE_NAME:suser:cmd:::/usr/bin/cat:euid=0
PROFILE_NAME:suser:cmd:::/usr/bin/diff:euid=0
PROFILE_NAME:suser:cmd:::/usr/bin/sort:euid=0
PROFILE_NAME:suser:cmd:::/usr/bin/rm:uid=0
PROFILE_NAME:suser:cmd:::/usr/bin/grep:euid=0
PROFILE_NAME:suser:cmd:::/usr/bin/egrep:euid=0
PROFILE_NAME:suser:cmd:::/bin/echo:euid=0
PROFILE_NAME:suser:cmd:::/bin/sed:euid=0
```

5. Run the following command to associate the profile with the role:

```
rolemod -P PROFILE_NAME ROLE_NAME
```

6. Run the following command to create the user:

```
useradd -d /export/home/USER_NAME -m USER_NAME
```

7. Run the following command to assign a password to the user:

```
passwd USER_NAME
```

8. Run the following command to grant the role to the user:

```
usermod -R ROLE_NAME USER_NAME
```

9. To verify the changes that you have made, open the `/etc/user_attr` file in a text editor and verity that the following entries are present in the file:

```
ROLE_NAME::::type=role;profiles=PROFILE_NAME
USER_NAME::::type=normal;roles=ROLE_NAME
```

2.2.1.2 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. Create a user mirror file on the server by using a command similar to the following:

   ```
   > /etc/mainUserFile1
   ```

   You can specify any destination directory and file name when you run the command. While configuring the IT resource, you specify the name and path of this file as the value of the `Passwd Mirror File/User Mirror File (AIX)` parameter of the IT resource for AIX.

   > **Note:**
   >
   > - The administrator account whose credentials you provide as part of the IT resource definition must have read and write permissions on this file.
   > - For AIX, first-time reconciliation involves reconciliation of all the users present in the target system. This functionality is different from that of other target systems. On other target systems, records of all existing users are fetched from the target system only if you have created the passwd mirror file and the shadow mirror file as empty files.
   > - The Update User Login provisioning operation is not supported by default on AIX 4.x and 5.1. However, if you upgrade these versions of AIX to support the useradd, usermod, and userdel commands, then you can perform the Update User Login provisioning operation.

2.2.1.3 Configuration Steps for HP-UX

Perform the following steps for HP-UX environments:

1. If you want to switch to HP-UX Trusted mode, then:

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

   ```
   /usr/bin/sam

   /usr/sbin/sam
   ```

   b. Select **Auditing and Security** and then select **System Security Policies.** A message is displayed asking if you want to switch to the trusted mode.

   c. Click **Yes.** The following message is displayed:

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

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

3. Create a passwd mirror file on the target server by using a command similar to the following:

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

   You can specify any destination directory and file name when you run the command. While configuring the IT resource, you specify the name and path of this file as the value of the `Passwd Mirror File/User Mirror File` parameter of the IT resource for HP-UX.

> **Note:** The administrator account whose credentials you provide as part of the IT resource definition must have read and write permissions on this file.

4. Create a shadow mirror file on the target server by using a command similar to the following:

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

   You can specify any destination directory and file name when you run the command. While configuring the IT resource, you specify the name and path of this file as the value of the `Shadow Mirror File` parameter of the IT resource.

   > **Note:** The administrator account whose credentials you provide as part of the IT resource definition must have read and write permissions on this file.

2.2.2 Installing External Software

This section describes the procedure to install external software.

2.2.2.1 Installing OpenSSH

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

For Solaris 8 and 9

1. If SSH is not installed on the Solaris server, then install the appropriate OpenSSH.
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/ssh_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 from the installation media.

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 from the installation media:

1. Install OpenSSL.
2. Install PRNG.
3. Install OpenSSH.
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.

2.2.2.2 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 install it from the installation media.
2. 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`
- `userdel`
- `passwd`
- `sh`
- `cat`
- `diff`
- `sort`
- `rm`
- `grep`
- `echo`

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

> **Caution:** Do not use the `NOPASSWD: ALL` option for any SUDO user or group. The connector will not work correctly if the `NOPASSWD: ALL` is set.
>
> 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 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.

4. 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
```

5. 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
```

6. 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 from the installation media.

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

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

   For example, if you have a group named mqm 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:

   ```
   %mqm 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 mqm.

   This connector uses the following commands:

   - useradd
   - usermod
   - userdel
   - passwd
   - sh
   - cat
   - diff
   - sort
   - rm
   - grep
   - echo
   - modprpw (/usr/lbin/modprpw)

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

   > **Caution:** Do not use the NOPASSWD: ALL option for any SUDO user or group. The connector will not work correctly if the NOPASSWD: ALL is set.
   >
   > 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 from the installation media.

2. 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`
   - `rmuser`
   - `lsuser`
   - `sh`
   - `cat`
   - `diff`
   - `sort`

- rm
- grep
- echo
- sed
- usermod

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

Caution: Do not use the NOPASSWD: ALL option for any SUDO user or group. The connector will not work correctly if the NOPASSWD: ALL is set.

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 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.

4. 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. from the installation media.

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.

This connector uses the following commands:

- `useradd`
- `usermod`
- `userdel`
- `passwd`
- `sh`
- `cat`
- `diff`
- `sort`
- `rm`
- `grep`
- `echo`
- `chage`

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

> **Caution:** Do not use the `NOPASSWD: ALL` option for any SUDO user or group. The connector will not work correctly if the `NOPASSWD: ALL` is set.
>
> 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 from the installation media.

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`
- `userdel`
- `passwd`
- `sh`
- `cat`
- `diff`
- `sort`
- `rm`
- `grep`
- `echo`
- `chage`

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

Caution: Do not use the `NOPASSWD: ALL` option for any SUDO user or group. The connector will not work correctly if the `NOPASSWD: ALL` is set.

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
   ```

2.2.3 Public Key Authentication (SSH Key Generation)

This section discusses the following topics:

- Configuring Public Key Authentication
- Configuring SSH Public Key Authentication

2.2.3.1 Configuring Public Key Authentication

To configure Public Key Authentication:

Note: If Public Key Authentication is used, then an RBAC user for a Solaris target mode and the SUDO user for the remaining target systems cannot be used.

---

1. Copy `scripts/privateKeyGen.sh` from the installation media directory to any directory on the target system 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.

2.2.3.2 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:

   ```
   ssh-keygen -q -f $HOME /.ssh/id_rsa -t rsa
   cd $HOME/.ssh
   cat id_rsa.pub >> authorized_keys
   chmod 700 authorized_keys
   ```

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

   ```
   OIM_HOME/xellerate/XLIntegrations/SSH/config
   ```

5. 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:

   > **Note:** The account used to run the OIM application server on UNIX should have the ownership of the id_rsa file.

   ```
   ssh -i OIM_HOME/xellerate/XLIntegratrions/SSH/config/id_rsa root - i
   lhost_ip_address
   ```

6. When you configure the IT resource, 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 5.

2.3 Installing the Connector on Oracle Identity Manager Release 9.1.0 or Later

> **Note:** In this guide, the term **Connector Installer** has been used to refer to the Connector Installer feature of the Oracle Identity Manager Administrative and User Console.

Installing the connector on Oracle Identity Manager release 9.1.0 or later involves the following procedures:

- Running the Connector Installer
- Configuring the IT Resource

2.3.1 Running the Connector Installer

To run the Connector Installer:

1. Copy the contents of the connector installation media into the following directory:

   ```
   OIM_HOME/xellerate/ConnectorDefaultDirectory
   ```

2. Log in to the Administrative and User Console by using the user account described in the "Creating the User Account for Installing Connectors" section of *Oracle Identity Manager Administrative and User Console*.
3. Click **Deployment Management**, and then click **Install Connector**.
4. From the Connector List list, select **UNIX SSH *RELEASE_NUMBER***. This list displays the names and release numbers of connectors whose installation files you copy into the default connector installation directory:

   ```
   OIM_HOME/xellerate/ConnectorDefaultDirectory
   ```

   If you have copied the installation files into a different directory, then:

   a. In the **Alternative Directory** field, enter the full path and name of that directory.

   b. To repopulate the list of connectors in the Connector List list, click **Refresh**.

   c. From the Connector List list, select **UNIX SSH *RELEASE_NUMBER***.
5. Click **Load**.
6. To start the installation process, click **Continue**.

   The following tasks are performed in sequence:

   a. Configuration of connector libraries

   b. Import of the connector Target Resource user configuration XML file (by using the Deployment Manager). If you want to import the target system as a trusted source for reconciliation, then see "Configuring the Target System As a Trusted Source" on page 3-3.

   c. Compilation of adapters

   On successful completion of a task, a check mark is displayed for the task. If a task fails, then an X mark and a message stating the reason for failure are displayed. Depending on the reason for the failure, make the required correction and then perform one of the following steps:

- Retry the installation by clicking **Retry.**
- Cancel the installation and begin again from Step 1.

7. If all three tasks of the connector installation process are successful, then a message indicating successful installation is displayed. In addition, a list of the steps that you must perform after the installation is displayed. These steps are as follows:

   a. Ensuring that the prerequisites for using the connector are addressed

   > **Note:** At this stage, run the `PurgeCache` utility to load the server cache with content from the connector resource bundle in order to view the list of prerequisites. Refer to "Clearing Content Related to Connector Resource Bundles from the Server Cache" on page 2-25 for information about running the `PurgeCache` utility.
   >
   > There are no prerequisites for some predefined connectors.

   b. Configuring the IT resource for the connector

   Record the name of the IT resource displayed on this page. The procedure to configure the IT resource is described later in this guide.

   c. Configuring the scheduled tasks that are created when you installed the connector

   Record the names of the scheduled tasks displayed on this page. The procedure to configure these scheduled tasks is described later in this guide.

When you run the Connector Installer, it copies the connector files and external code files to destination directories on the Oracle Identity Manager host computer. These files are listed in Table 1–1.

Installing the Connector in an Oracle Identity Manager Cluster

While installing Oracle Identity Manager in a clustered environment, you must copy all the JAR files and the contents of the `connectorResources` directory into the corresponding directories on each node of the cluster. See "Files and Directories on the Installation Media" on page 1-5 for information about the files that you must copy and their destination locations on the Oracle Identity Manager server.

2.3.2 Configuring the IT Resource

> **Note:** Perform this procedure if you are installing the connector on Oracle Identity Manager release 9.1.0 or later.

You must specify values for the parameters of the `SSH` IT resource as follows:

1. Log in to the Administrative and User Console.
2. Expand **Resource Management.**
3. Click **Manage IT Resource**.
4. In the IT Resource Name field on the Manage IT Resource page, enter `SSH` and then click **Search**.
5. Click the edit icon for the IT resource.
6. From the list at the top of the page, select **Details and Parameters**.

7. Specify values for the parameters of the IT resource. The following table describes each parameter:

Parameter	Description and Sample Value
`Admin UserId`	User ID of the administrator `root` or `jdoe` Here, `jdoe` can be the SUDO user ID, for the SUDO Admin mode. Alternatively, on Solaris, it can be the user ID of the account to which you assign the minimum privileges required to perform connector operations. See "Creating a Target System User Account for Connector Operations" on page 2-3 for more information.
`Admin Password/Private file Pwd`	Password of the administrator **Note:** For the SUDO Admin mode, the private key is not supported. Specify a password for this mode as the value of the parameter. If a private key is used, then enter the private key passphrase as the value of the parameter. For the Solaris target system, if an RBAC user is used, then enter the RBAC user's password as the value of the parameter.
`Server IP Address`	Server IP address
`Port`	The port at which the SSH service is running on the server Default value: `22`
`Private Key`	Private key file name with full path **Note:** For SUDO Admin administrator, this parameter must be left blank.
`Server OS`	Specify one of the following: ■ `AIX` ■ `HP-UX` ■ `SOLARIS` ■ `LINUX`
`Shell Prompt`	# or $
`Whether Trusted System (HP-UX)`	`YES` (for trusted HP-UX System) or `NO` (for non-trusted HP-UX system)
`Sudo Or RBAC`	Enter one of the following values: ■ `None`: Specifies the root user. ■ `Sudo`: Specifies the sudo user. ■ `RBAC`: Specifies the RBAC user. See "Creating a Target System User Account for Connector Operations" on page 2-3 for more information.
`Max Retries`	Number of times that the connector must retry connecting to the target server if the connection fails Default value: `2`
`Delay`	Delay (in milliseconds) before the connector attempts to retry connecting to the target system, if the connection fails Default value: `10000`
`Timeout`	Value of the timeout (in milliseconds) for the connection to the target server Default value: `20000`

Parameter	Description and Sample Value

`Passwd Mirror File/User Mirror File`	Name and full path of the password mirror file/user mirror file
	The SUDO user must have read and write permissions on this file.
	For example, suppose you run the following command to view the permissions on the mirror file:
	`$ ls -ltr passwd1`
	The command generates the following output:
	`-rwxr--r-- 1 janedoe mqm 9972 Mar 11 20:35 passwd1`
	In this output, `janedoe` is the SUDO user.
	Sample value for this attribute: `/etc/passwd1`

`Shadow Mirror File`	Name of the shadow mirror file
	The SUDO user must have read and write permissions on this file.
	For example, suppose you run the following command to view the permissions on the mirror file:
	`$ ls -ltr shadow1`
	The command generates the following output:
	`-rwxr--r--  1 janedoe mqm 9972     Mar 11 20:35 shadow1`
	In this output, `janedoe` is the SUDO user.
	Note:
	This attribute is not required on AIX.
	The value of this attribute must not be null or blank, even for an HP-UX trusted system. However, the reconciliation process on an HP-UX trusted system ignores this attribute.
	Sample value: `/etc/shadow1`

`Target Date Format`	This parameter is used to specify the date format of the target UNIX computer. The default value for this parameter is: `MMddhhmmyy` This parameter is used for user reconciliation.
`Protocol`	Default value: `SSH` Do not change this default value.
`RBAC Role Name`	If you specify RBAC as the value of the `Sudo Or RBAC` parameter, then enter the name of the role assigned to the RBAC user. Otherwise, do not specify a value for this parameter. See "Creating a Target System User Account for Connector Operations" on page 2-3 for more information.
`RBAC Role Passwd`	If you specify RBAC as the value of the `Sudo Or RBAC` parameter, then enter the password of the role assigned to the RBAC user. Otherwise, do not specify a value for this parameter. See "Creating a Target System User Account for Connector Operations" on page 2-3 for more information.

8. To save the values, click **Save**.

2.4 Installing the Connector on Oracle Identity Manager Release 8.5.3.1 Through 9.0.3.x

Installing the connector on any Oracle Identity Manager release between releases 8.5.3.1 and 9.0.3.x involves the following procedures:

- Copying the Connector Files

- Importing the Connector XML Files

2.4.1 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.

> **See Also:** "Files and Directories on the Installation Media" section on page 1-5 for more information about these files

File in the Installation Media Directory	Destination Directory
Files in the `config` directory	*OIM_HOME*/xellerate/XLIntegrations/SSH/config
`ext/sshfactory.jar`	*OIM_HOME*/xellerate/ThirdParty
`lib/xliSSH.jar`	*OIM_HOME*/xellerate/JavaTasks *OIM_HOME*/xellerate/ScheduleTask
Files in the `resources` directory	*OIM_HOME*/xellerate/connectorResources
Files in the `scripts` directory	*OIM_HOME*/xellerate/XLIntegrations/SSH/scripts
Files and directories in the `test` directory	*OIM_HOME*/xellerate/XLIntegrations/SSH
Files in the `xml` directory	*OIM_HOME*/xellerate/XLIntegrations/SSH/xml

> **Note:** In a clustered environment, copy the JAR files and the contents of the `connectorResources` directory to the corresponding directories on each node of the cluster.

2.4.2 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 opening files is displayed.
4. Locate and open the `SSHNonTrustedUser.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` IT resource is displayed.
8. Specify values for the parameters of the `SSH` IT resource. Refer to the following table for information about the values to be specified:

Parameter	Description and Sample Value
`Admin UserId`	User ID of the administrator `root` or `jdoe` Here, `jdoe` can be the SUDO user ID, for the SUDO Admin mode. Alternatively, on Solaris, it can be the user ID of the account to which you assign the minimum privileges required to perform connector operations. See "Creating a Target System User Account for Connector Operations" on page 2-3 for more information.
`Admin Password/Private file Pwd`	Password of the administrator **Note:** For the SUDO Admin mode, the private key is not supported. Specify a password for this mode as the value of the parameter. If a private key is used, then enter the private key passphrase as the value of the parameter. For the Solaris target system, if an RBAC user is used, then enter the RBAC user's password as the value of the parameter.
`Server IP Address`	Server IP address
`Port`	The port at which the SSH service is running on the server Default value: `22`
`Private Key`	Private key file name with full path **Note:** For SUDO Admin administrator, this parameter must be left blank.
`Server OS`	Specify one of the following: ■ `AIX` ■ `HP-UX` ■ `SOLARIS` ■ `LINUX`
`Shell Prompt`	`#` or `$`
`Whether Trusted System (HP-UX)`	`YES` (for trusted HP-UX System) or `NO` (for non-trusted HP-UX system)
`Sudo Or RBAC`	Enter one of the following values: ■ `None`: Specifies the root user. ■ `Sudo`: Specifies the sudo user. ■ `RBAC`: Specifies the RBAC user. See "Creating a Target System User Account for Connector Operations" on page 2-3 for more information.
`Max Retries`	Number of times that the connector must retry connecting to the target server if the connection fails Default value: `2`
`Delay`	Delay (in milliseconds) before the connector attempts to retry connecting to the target system, if the connection fails Default value: `10000`
`Timeout`	Value of the timeout (in milliseconds) for the connection to the target server Default value: `20000`

Parameter	Description and Sample Value
`Passwd Mirror File/User Mirror File`	Name of the password mirror file/user mirror file. The user must have read and write permissions on this file. The sample value for this parameter is: `/etc/passwd1` This parameter is used for user reconciliation.

`Shadow Mirror File`	Name of the shadow mirror file
	The SUDO user must have read and write permissions on this file.
	For example, suppose you run the following command to view the permissions on the mirror file:
	`$ ls -ltr shadow1`
	The command generates the following output:
	`-rwxr--r--  1 janedoe mqm 9972     Mar 11 20:35 shadow1`
	In this output, `janedoe` is the SUDO user.
	Note:
	This attribute is not required on AIX.
	The value of this attribute must not be null or blank, even for an HP-UX trusted system. However, the reconciliation process on an HP-UX trusted system ignores this attribute.
	Sample value: `/etc/shadow1`

`Target Date Format`	This parameter is used to specify the date format of the target UNIX computer. The default value for this parameter is: `MMddhhmmyy` This parameter is used for user reconciliation.
`Protocol`	Default value: `SSH` Do not change this default value.
`RBAC Role Name`	If you specify RBAC as the value of the `Sudo Or RBAC` parameter, then enter the name of the role assigned to the RBAC user. Otherwise, do not specify a value for this parameter.
`RBAC Role Passwd`	If you specify RBAC as the value of the `Sudo Or RBAC` parameter, then enter the password of the role assigned to the RBAC user. Otherwise, do not specify a value for this parameter.

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 Administrative and User Console Guide* for instructions.

11. Click **View Selections**.

    The contents of the XML file are displayed on the Import page. You *may* see a cross-shaped icon along with some nodes. These nodes represent Oracle Identity Manager entities that are redundant. Before you import the connector XML file, you must remove these entities by right-clicking each node and then selecting **Remove**.

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

2.5 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

2.5.1 Changing to the Required Input Locale

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

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

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

While performing the instructions described in the "Copying the Connector Files" section on page 2-22, you copy files from the `resources` directory on the installation media into the *`OIM_HOME`*`/xellerate/connectorResources` directory. Whenever you add a new resource bundle in the `connectorResources` directory or make a change in an existing resource bundle, you must clear content related to connector resource bundles from the server cache.

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

1. In a command window, change to the *`OIM_HOME`*`/xellerate/bin` directory.

> **Note:** You must perform Step 1 before you perform Step 2. An exception is thrown if you run the command described in Step 2 as follows:
>
> *`OIM_HOME`*`/xellerate/bin/`*`batch_file_name`*

2. Enter one of the following commands:

   - On Microsoft Windows:

     ```
     PurgeCache.bat ConnectorResourceBundle
     ```

   - On UNIX:

     ```
     PurgeCache.sh ConnectorResourceBundle
     ```

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

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

```
OIM_HOME/xellerate/config/xlConfig.xml
```

2.5.3 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 messages that highlight the progress of the application at a 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 allow the application to continue running.

- `FATAL`

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

- `OFF`

  This level disables logging for all events.

The file in which you set the log level depends on the application server that you use:

- **BEA WebLogic Server**

  To enable logging:

  1. Add the following line in the *OIM_HOME*`/xellerate/config/log.properties` file:

     ```
     log4j.logger.OIMCP.TELNETSSH=log_level
     ```

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

     For example:

     ```
     log4j.logger.OIMCP.TELNETSSH=INFO
     ```

  After you enable logging, log information is displayed on the server console.

- **IBM WebSphere Application Server**

  To enable logging:

1. Add the following line in the *OIM_HOME*/xellerate/config/log.properties file:

   ```
   log4j.logger.OIMCP.TELNETSSH=log_level
   ```

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

   For example:

   ```
   log4j.logger.OIMCP.TELNETSSH=INFO
   ```

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

```
WEBSPHERE_HOME/AppServer/logs/SERVER_NAME/SystemOut.log
```

- **JBoss Application Server**

  To enable logging:

  1. In the *JBOSS_HOME*/server/default/conf/log4j.xml file, add the following lines if they are not already present in the file:

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

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

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

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

  ```
  JBOSS_HOME/server/default/log/server.log
  ```

- **Oracle Application Server**

  To enable logging:

  1. Add the following line in the *OIM_HOME*/xellerate/config/log.properties file:

     ```
     log4j.logger.OIMCP.TELNETSSH=log_level
     ```

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

     For example:

     ```
     log4j.logger.OIMCP.TELNETSSH=INFO
     ```

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

  ```
  ORACLE_HOME/opmn/logs/default_group~home~default_group~1.log
  ```

3

Configuring the Connector

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

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

- Configuring Reconciliation
- Configuring Provisioning
- Configuring the Connector for Multiple Installations of the Target System
- Transforming Data Reconciled Into Oracle Identity Manager

3.1 Configuring Reconciliation

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

- Partial Reconciliation
- Batched Reconciliation
- Configuring System Properties
- Configuring the Target System As a Trusted Source
- Configuring the Reconciliation Scheduled Tasks
- Enabling Reconciliation in Oracle Identity Manager Release 9.0.1
- Adding Custom Attributes for Reconciliation

3.1.1 Partial Reconciliation

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

Creating a filter involves specifying a value for the UserNameFilter scheduled task attribute, which will be used in the query SELECT criteria to retrieve the records to be reconciled. For example, if you specify the value JDoe for this attribute, then all target system user records with the user name JDoe are reconciled.

While deploying the connector, follow the instructions in the "Specifying Values for the Scheduled Task Attributes" section on page 3-4 to specify a value for this attribute.

3.1.2 Batched Reconciliation

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

You can configure batched reconciliation to avoid these problems.

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

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

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

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

- BatchSize: 20
- NumberOfBatches: 10

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

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

3.1.3 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**.

3.1.4 Configuring the Target System As a Trusted Source

While configuring the connector, the target system can be designated as a trusted source or target resource. If you designate the target system as a **trusted source**, then during a reconciliation run:

- For each newly created user on the target system, an OIM User is created.
- Updates made to each user on the target system are propagated to the corresponding OIM User.

If you designate the target system as a **target resource**, then during a reconciliation run:

- For each account created on the target system, a resource is assigned to the corresponding OIM User.
- Updates made to each account on the target system are propagated to the corresponding resource.

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

Configuring trusted source reconciliation involves the following steps:

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

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

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

To import the XML file for trusted source reconciliation:

1. Open the Oracle Identity Manager Administrative and User Console.
2. Click the **Deployment Management** link on the left navigation bar.
3. Click the **Import** link under Deployment Management. A dialog box for opening files is displayed.
4. Locate and open the `XellSSHUser.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 **Import**.
8. In the message that is displayed, click **Import** to confirm that you want to import the **XML** file and then click **OK**.

3.1.5 Configuring the Reconciliation Scheduled Tasks

> **Note:** If you want to run full reconciliation at any time after first-time reconciliation, then run the following commands on the target system before you run the scheduled tasks:
>
> ```
> > etc/passwd1
> > etc/shadow1
> ```

To configure the reconciliation scheduled task:

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

     If you select the **Recurring Intervals** option, then you must also specify the time interval at which you want the task to run on a recurring basis.
   - To set the task to run only once, select the **Once** option.
9. Provide values for the user-configurable attributes of the scheduled task. Refer to the "Specifying Values for the Scheduled Task Attributes" section on page 3-4 for information about the values to be specified.

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

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

3.1.5.1 Specifying Values for the Scheduled Task Attributes

You must specify values for the attributes of the following user reconciliation scheduled tasks:

- Scheduled Tasks for Trusted Source and Target Resource Reconciliation
- Scheduled Task for Lookup Field Reconciliation

3.1.5.1.1 Scheduled Tasks for Trusted Source and Target Resource Reconciliation

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

- `SSH User Trusted Source Reconciliation Task` (Scheduled task for trusted source reconciliation)
- `SSH User Target Resource Reconciliation Task` (Scheduled task for target resource reconciliation)

The following table describes the attributes of both scheduled tasks.

Note:

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

Attribute	Description	Sample Value
`Server`	Name of the IT resource	`SSH LINUX`
`IsTrusted`	Specifies whether or not reconciliation is to be carried out in trusted mode	Specify `Yes` for trusted source reconciliation. Specify `No` for target resource reconciliation.
`Target System Recon - Resource Object name`	Name of the target system resource object	`SSH User`
`Trusted Source Recon - Resource Object name`	Name of the trusted source resource object	Default value: `Xellerate User` Specify `false` (in lowercase) if you do not want to configure trusted source reconciliation
`BatchSize`	Number of records in each batch that is reconciled If you do not want to implement batched reconciliation, then specify `nodata`. **See Also:** The "Batched Reconciliation" section on page 3-2	The default value is 1000.
`NoOfBatches`	Number of batches to be reconciled The number of records in each batch is specified by the `BatchSize` attribute. **See Also:** The "Batched Reconciliation" section on page 3-2	Specify `All` if you want to reconcile all the batches. This is the default value. Specify an integer value if you want to reconcile only a fixed number of batches

Attribute	Description	Sample Value
`UserNameFilter`	This is a filter attribute. Use this attribute to specify the user name (User Login) for which you want to reconcile user records. If you do not want to use this filter attribute, then specify `Nodata`. **See Also:** The "Partial Reconciliation" section on page 3-1	The value can be either the user name or `Nodata`. The default value is `Nodata`.
`TransformLookupName`	This is a lookup attribute. Use this attribute to specify the lookup name used for the transformation class map that is stored in the lookup tables. This attribute is valid only when the `UseTransformMapping` attribute is set to `Yes`.	`Lookup.Reconciliation.TransformationMap`
`UseTransformMapping`	Specifies whether or not the transform mappings accessed by the `TransformLookupName` attribute must be used.	Enter `Yes` if you want the transform mappings accessed by the `TransformLookupName` attribute to be used. Otherwise, enter `No`. The default value is `No`.

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

3.1.5.1.2 Scheduled Task for Lookup Field Reconciliation

The following are attributes of the `TelnetSSHGroupLookupReconTask` scheduled task for lookup field reconciliation.

Attribute	Description
`Server`	Name of the IT resource
`Lookup Field Name`	Enter `UD_Lookup_SSH_PrimaryGroupNames`.
`Exclusion List`	Enter a comma-delimited list of the names of groups on the target system that you do not want to reconcile.

3.1.6 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**.

3.1.7 Adding Custom Attributes for Reconciliation

> **Note:**
>
> - In this section, the term "attribute" refers to the identity data fields that store user data.
>
> - You need not perform this procedure if you do not want to add custom attributes for reconciliation.

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

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

1. Open the following file in the `*OIM_HOME*/xellerate/XLIntegrations/SSH/config` directory:

   For AIX:

   ```
   userAttribute_AIX_recon.properties
   ```

   For non-AIX platforms:

   ```
   userAttribute_NonAIX_recon.properties
   ```

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

   For AIX:

   ```
   Target_System_Attribute=OIM_Server_Attribute
   ```

   For example:

   ```
   maxage=Users.AccountExpiryDate
   ```

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

   For non-AIX platforms:

   ```
   OIM_Server_Attribute=Target_System_Attribute_index
   ```

   For example:

   ```
   Users.DefaultShell=6
   ```

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

3. In the resource object definition, add a reconciliation field corresponding to the new attribute as follows:

a. Open the Resource Objects form. This form is in the Resource Management folder.

b. Click **Query for Records**.

c. On the Resource Objects Table tab, double-click the `SSH User` resource object to open it for editing.

d. On the Object Reconciliation tab, click **Add Field** to open the Add Reconciliation Field dialog box.

e. Specify a value for the field name.

   For AIX:

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

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

   For non-AIX platforms:

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

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

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

   For example: `String`

g. Save the values that you enter, and then close the dialog box.

h. If required, repeat Steps d through g to map more fields.

4. Add a new field in the process form.

   a. Open the `UD_SSH` process form. This form is in the Development Tools folder of the Oracle Identity Manager Design Console.

   b. Click **Create New Version**.

   c. In the Create a New Version dialog box, specify the version name in the **Label** field, save the changes, and then close the dialog box.

   d. From the **Current Version** list, select the newly created version.

   e. On the Additional Columns tab, click **Add**.

   f. Specify the new field name and other values. For the example described in Step 3 in the connector guide, you enter the value `UD_SSH_DEFAULTSHELL`.

   g. Click **Make Version Active** and then save the changes.

5. Modify the provisioning process to include the mapping between the newly added attribute and the corresponding reconciliation field as follows:

   a. Open the `SSH User` provisioning process. The provisioning process form is in the Process Management folder.

   b. On the Reconciliation Field Mappings tab, click **Add Field Map** to open the Add Reconciliation Field Mapping dialog box.

   c. Enter the required values, save the values that you enter, and then close the dialog box.

For the example described in Step 3 in the connector guide, you enter the values `Users.DefaultShell [String]` and `UD_SSH_DEFAULTSHELL`.

d. If required, repeat Steps b and c to map more fields.

3.2 Configuring Provisioning

As mentioned earlier in this guide, provisioning involves creating or modifying a user's account information on the target system through Oracle Identity Manager.

This section discusses the following topics related to configuring provisioning:

- Compiling Adapters
- Adding Custom Attributes for Provisioning

3.2.1 Compiling Adapters

> **Note:** You must perform the procedure described in this section if you want to use the provisioning features of Oracle Identity Manager for this target system.
>
> You need not perform the procedure to compile adapters if you have performed the procedure described in "Installing the Connector on Oracle Identity Manager Release 9.1.0 or Later" on page 2-18.

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

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

- `SSH Create User`
- `SSH Delete User`
- `SSH Set Password`
- `SSH Enable User`
- `SSH Disable User`
- `SSH Prepopulate User Login`
- `SSH updateDateField`
- `SSH updateIntField`
- `SSH updateStrField`
- `SSH updateHomeDir`

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

To compile adapters by using the Adapter Manager form:

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

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

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

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

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

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

To view detailed information about an adapter:

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

3.2.2 Adding Custom Attributes for Provisioning

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

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

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

1. Modify the attribute entries in the following file:

   For the AIX platform:

   ```
   OIM_HOME/xellerate/XLIntegrations/SSH/config/userAttribute_AIX_prov.properties
   ```

   For non-AIX platforms:

   ```
   OIM_HOME/xellerate/XLIntegrations/SSH/config/userAttribute_NonAIX_prov.properti
   es
   ```

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

   ```
   OimAttributeName=TargetAttributeName
   ```

   For example:

```
homeDir=-d
```

2. Add a new column in the process form.

   > **Note:** If you have already performed Step 4 of the "Adding Custom Attributes for Reconciliation" section on page 3-7, then directly proceed to Step 3.

   a. Open the process form. This form is in the Development Tools folder of the Oracle Identity Manager Design Console.

   b. Click **Create New Version**.

   c. In the Create a New Version dialog box, specify the version name in the **Label** field, save the changes, and then close the dialog box.

   d. From the **Current Version** list, select the newly created version.

   e. On the Additional Columns tab, click **Add**.

   f. Specify the new field name and other values.

   g. Click **Make Version Active** and save the changes.

3. Add a new variable in the variable list.

   a. Open the Adapter Factory form. This form is in the Development Tools folder of the Oracle Identity Manager Design Console.

   b. Click the **Query for Records** icon.

   c. On the Adapter Factory Table tab, double-click the **adpSSHCREATEUSER** adapter from the list.

   d. On the Variable List tab, click **Add**.

   e. In the Add a Variable dialog box, specify the required values and then save and close the dialog box.

4. Define an additional adapter task for the newly added variable in the `adpSSHCREATEUSER` adapter.

   a. On the Adapter Tasks tab of the Adapter Factory form, click **Add**.

   b. In the Adapter Task Selection dialog box, select **Functional Task**, select **Java** from the list of functional task types, and then click **Continue**.

   c. In the Object Instance Selection dialog box, select **Persistent Instance** and then click **Continue**.

   d. In the Add an Adapter Factory Task dialog box, specify the task name, select the **setProperty** method from the **Method** list, and then click **Save**.

   e. Map the application method parameters, and then save and close the dialog box. To map the application method parameters:

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

   i. From the **Map to** list, select **Literal**.

   ii. From the **Name** list, select **Return variable**.

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

   i. From the **Map to** list, select **Adapter Variables**.

ii. From the **Name** list, select **Input**.

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

i. From the **Map to** list, select **Literal**.

ii. From the **Name** list, select **String**.

iii. In the **Value** field, specify the name that is to the left of the equal sign in the line that you uncomment or add while performing Step 1.

For example, if you uncomment the `homeDir=-d` line in Step 1, then you must specify `homeDir` as the attribute name.

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

i. From the **Map to** list, select **Adapter Variables**.

ii. From the **Name** list, select the newly added adapter variable.

f. Repeat Steps b through g to create more adapter tasks.

5. Create an additional adapter task to set the input variable.

   a. Open the Adapter Factory form. This form is in the Development Tools folder in the Oracle Identity Manager Design Console.

   b. On the Adapter Tasks tab, click **Add**.

   c. In the Adapter Task Selection dialog box, select **Logic Task**, select **SET VARIABLE** from the list, and then click **Continue**.

   d. In the Edit Set Variable Task Parameters dialog box, select **input** from the **Variable Name** list, select **Adapter Task** from the **Operand Type** list, and the Operand Qualifier as the Adapter Task that you have created in the previous step. Then, click **Save**.

6. Map the process form columns and adapter variables for the Create User process task as follows:

   a. Open the Process Definition form. This form is in the Process Management folder of the Design Console.

   b. Click the **Query for Records** icon.

   c. On the Process Definition Table tab, double-click the **SSH User** process.

   d. On the Tasks tab, double-click the **Create User** task.

   e. In the Closing Form dialog box, click **Yes**.

   f. On the Integration tab of the Editing Task Columns Create User dialog box, map the unmapped variables, and then save and close the dialog box. To map an unmapped variable:

   i. Double-click the row in which **N** is displayed in the Status column. The value `N` signifies that the variable is not mapped.

   ii. From the **Map to** list in the Edit Data Mapping for Variables dialog box, select **Process Data**.

   iii. From the **Qualifier** list, select the name of the variable.

   Repeat Steps i through iii for all unmapped variables.

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

3.3 Configuring the Connector for Multiple Installations of the Target System

Note: Perform this procedure only if you want to configure the connector for multiple installations of the target system.

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

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

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

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

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

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

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

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

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

When you use the Administrative and User Console to perform provisioning, you can specify the IT resource corresponding to the target system installation to which you want to provision the user.

3.4 Transforming Data Reconciled Into Oracle Identity Manager

This section discusses the `TransformLookupName` and `UseTransformMapping` attributes of the scheduled tasks for target resource and trusted source reconciliation, `SSH User Target Resource Reconciliation Task` and `SSH User Trusted Source Reconciliation Task`.

During reconciliation, you may want to transform the values of some target system fields before they are stored in Oracle Identity Manager. Appending a number at the end of the user ID is an example of a data transformation.

The `TransformLookupName` and `UseTransformMapping` attributes provide a method for implementing such transformations. To use these attributes

1. Identify the fields that you want to transform.

2. Create the Java file containing the code implementation of the transformation that must be performed during reconciliation. See Appendix C, "Sample Transformation Class" for information about creating a transformation class.

3. Compile the Java file. While compiling the file, you must reference the `xliSSH.jar` file in the *`OIM_HOME`*`/xellerate/ScheduleTask` directory.

4. Create JAR files containing the code to implement the required transformations on the fields.

5. Copy the JAR files into the following directory:

   `OIM_HOME``/xellerate/ScheduleTask`

6. In the `Lookup.Reconciliation.TransformationMap` lookup definition, add an entry for the transformation. In the Code Key column, enter the name of the reconciliation field (in the resource object) on which you want the transformation to be performed. In the Decode column, enter the name of the class file. For example:

   > **Note:** You can use this lookup definition for both UNIX SSH and SSH Telnet.

   Code Key: `First Name`

   Decode: `AppendNumber`

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

7. While configuring the `SSH User Target Resource Reconciliation Task` and `SSH User Trusted Source Reconciliation Task` scheduled tasks by performing the procedure described in "Scheduled Tasks for Trusted Source and Target Resource Reconciliation" on page 3-5:

   - Enter the name of the lookup definition as the value of the `TransformLookupName` attribute.
   - Enter `Yes` as the value of the `UseTransformMapping` attribute to specify that you want transformations to be applied. If you enter `No` as the value, then the transformations are not applied.

4 Testing and Troubleshooting

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

Before you use the testing utility, copy the files in the `test` directory on the installation media to the *`OIM_HOME`*`/xellerate/XLIntegrations/SSH` directory.

Set the required values in the `config.properties` file. This file is in the *`OIM_HOME`*`/xellerate/XLIntegrations/SSH/config/config.properties` directory.

Use the information in the following table to modify the default attributes of the `config.properties` file.

Attribute	Description	Default/Sample Value
`hostname`	IP address of the target server on which user provisioning is to be performed	`10.1.1.114`
`shellPrompt`	Default shell prompt of the target server: # for Solaris, Linux, and HP-UX $ for AIX	`#`
`port`	Port at which the SSH server is listening	`22`
`osType`	Operating system type of the UNIX server Accepted values are `SOLARIS`, `LINUX`, `HP-UX`, and `AIX`.	`SOLARIS`
`adminpassword`	Admin user password	`password1`
`admin`	UNIX server administrator credentials for the SSH server	`root`
`action`	Action to be tested The value can be one of the following: ■ `CONNECT` ■ `CREATE` ■ `CHANGEPASSWORD` ■ `MODIFY` ■ `DELETE` ■ `DISABLE` ■ `ENABLE` ■ `ENABLETRUSTED` (only for HP-UX trusted mode)	`CREATE`
`userName`	User attribute	jdoe

Attribute	Description	Default/Sample Value
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.
Max Retries	Number of times that the UNIX SSH connector should retry connecting to the target server if the connection fails	2
Delay	Delay (in milliseconds) before the connector attempts to retry connecting to the target system, in case the connection fails	2000
Timeout	Value of the timeout (in milliseconds) for the connection to the target server	10000
passwdMirrorFilePath	This parameter is used to specify the passwd mirror file path for reconciliation.	/etc/passwd1
shadowMirrorFilePath	This parameter is used to specify the shadow mirror file path for reconciliation.	/etc/shadow1
targetDateFormat	This parameter is used to specify the date format of the target UNIX computer.	MMddhhmmyy

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

For UNIX:

```
OIM_HOME/xellerate/XLIntegrations/SSH/scripts/SSH.sh
```

For Microsoft Windows:

```
OIM_HOME\xellerate\XLIntegrations\SSH\scripts\SSH.bat
```

5 Known Issues

The following is the known issue associated with this release of the connector:

- **Bug 6923238**

  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.

  A reconciliation run stops if the scheduled task code encounters target system user data containing the character or characters that are same as the shell prompt of the target system.

A

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, groups are separated by commas, with no intervening whitespace between group names.
Password	passwd	Password
Reenter Password	Reenter Password	Password reentered for confirmation
User Login	login	New login name, specified as a string of printable characters It cannot contain a colon (`:`) or a newline (`\n`) 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 `/etc/passwd` file entry. **Note:** The entry of multibyte characters is supported for this attribute.

Oracle Identity Manager Attribute	UNIX SSH Attribute	Description
Home Directory	home directory	Login directory of the new user The default directory name is obtained by appending the login name to the default home directory. For example, if the login name is `jdoe`, then the default home directory is `/home/jdoe`. **Note:** The entry of multibyte characters is supported for this attribute.
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	Specifies the skeleton directory that contains information that can be copied to the new login's home directory An existing directory must be specified. The system provides a skeleton directory, `/etc/skel`, that can be used for this purpose. **Note:** The entry of multibyte characters is supported for this attribute.
Inactive Days	inactive days	Number of days after a password has expired before the account is disabled

B

Privileges Required for Performing Provisioning and Reconciliation

This appendix lists the privileges required for successful provisioning operations and reconciliation runs.

This appendix includes the following topics:

- Privileges Required for Running Commands on Non-AIX
- Privileges Required for Running Commands on HP-UX
- Privileges Required for Running Commands on AIX

B.1 Privileges Required for Running Commands on Non-AIX

Users must have privileges to run the following commands:

```
usermod, useradd, userdel, passwd, chage
```

In addition, the users must have execute permissions for the following commands:

```
sed, cat, diff, sort, rm, grep, egrep, echo, /usr/bin/sh,
/bin/sh
```

Users must have read and write permissions on the `/etc` and `/tmp` directories.

B.2 Privileges Required for Running Commands on HP-UX

Users must have privileges to execute the `modprpw` command.

In addition, users must have read and write permissions on the `/etc` and `/tmp` directories.

B.3 Privileges Required for Running Commands on AIX

User must have privileges to execute the following commands:

```
mkuser, chuser, rmuser, lsuser, /usr/bin/usermod, /usr/chuser
```

In addition, the users must have execute permissions for the following commands:

```
/usr/bin/bdiff, sh, cat, /usr/bin/sort, /usr/bin/rm,
/usr/bin/grep, /bin/echo, /bin/sed, command.
```

Users must have read and write permissions on the `/ (root)` and `/tmp` directory.

C

Sample Transformation Class

When you use this connector, you can transform reconciled data according to your requirements. This feature has been described in "Transforming Data Reconciled Into Oracle Identity Manager" on page 3-13, along with the discussion on the `TransformLookupName` and `UseTransformMapping` attributes.

If you want to transform the value of a target system field that is fetched during reconciliation, then the first step is to implement the required transformation logic in a Java class. This transformation class must implement the com.thortech.xl.schedule.telnetssh.tasks.AttributeTransformer interface and the transform method.

The following is a sample transformation class:

```
package com.thortech.xl.schedule.telnetssh.tasks;
import java.util.Hashtable;
import com.thortech.util.logging.Logger;
import com.thortech.xl.integration.telnetssh.util.TelnetSSHConstants;
public class AppendTransformer implements AttributeTransformer
{
/**
 * sample transformation method
 *  it appends '123' to the key if present in the data to be reconciled
 *  @param sKeyToBeTransformed - key to be transformed for example: Users.GECOS
 *  @paramhtReconData - hash table of the data to be reconciled
*/
public Hashtable transform(String sKeyToBeTransformed, Hashtable htReconData)
{
if(htReconData != null && sKeyToBeTransformed != null ) {
if(htReconData.get(sKeyToBeTransformed) != null) {
String sValue = (String)htReconData.get(sKeyToBeTransformed) ;
sValue+="123";
htReconData.put(sKeyToBeTransformed, sValue);
}
}
return htReconData;
}
}
```

The method defined in this class accepts the value of the field to be transformed, appends the string 123 to it, and returns the transformed string value.

Index