Oracle® Identity Manager

Connector Guide for UNIX SSH

Release 9.0.4

E10176-01

May 2007

ORACLE®

Oracle Identity Manager Connector Guide for UNIX SSH, Release 9.0.4

E10176-01

Primary Authors: Debapriya Datta, Shiladitya Guha

Contributing Authors: Tehmurasp Ghyara, Don Gosselin, Lyju Vadassery

Contents

Preface

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

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

Audience

This guide is intended for users who want to deploy the Oracle Identity Manager connector for UNIX SSH.

Documentation Accessibility

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

http://www.oracle.com/accessibility/

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

TTY Access to Oracle Support Services

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

Related Documents

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

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

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

- *Oracle Identity Manager Connector Framework Guide*

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager Connector Pack Release 9.0.4 documentation library, visit Oracle Technology Network at

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

Conventions

The following text conventions are used in this document:

Convention	Meaning
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 the 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 of the Oracle Identity Manager connector pack.

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

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

- Software Updates

  These include updates made to the connector software.

- Documentation-Specific Updates

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

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

Software Updates

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

Enabling Logging

By following the instructions in the "Enabling Logging" section on page 2-19, you can configure the generation of log information that is specific to the target system.

Partial Reconciliation

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

Batched Reconciliation

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

Separate Scheduled Tasks for Trusted and Nontrusted Source Reconciliation

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

Timeout Support

This release of the connector provides timeout support for provisioning and reconciliation. In the "Defining IT Resources" section on page 2-21, the IT resource parameters that are used to implement this feature are described.

Testing Utility

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

- Files and Directories That Comprise the Connector on page 1-5
- Step 3: Copying the Connector Files on page 2-17
- Chapter 4, "Testing and Troubleshooting"

Changes in the Connector Files

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

Changes in the Supported Target Systems List

In the "Step 1: Verifying Deployment Requirements" section on page 2-1, the list of supported target systems has been modified. This release of the connector also supports.

Adding Custom Attributes

This release of the connector supports the adding of custom attributes for reconciliation and provisioning. This feature is described in the "Adding Custom Attributes for Reconciliation" section on page 3-6 and the "Adding Custom Attributes for Provisioning" section on page 3-10.

Documentation-Specific Updates

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

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

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.

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

This chapter contains the following sections:

Reconciliation Module

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

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

The following target system attributes are reconciled:

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

- GECOS
- Password Change Time
- Account Expiry Date

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

Reconciled Xellerate User Fields

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

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

Provisioning Module

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

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

For this target system, the following fields are provisioned:

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

Supported Functionality

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

Function	Type	Description
Create User	Provisioning	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 Account field must be populated only when the UNIX server is configured in trusted mode. ■ Before populating the Skeleton directory field, data must be populated in the Home Directory field and the Create Home Directory check box must also be selected. ■ While specifying a value in the GECOS field, ensure that there are no spaces.
Delete User	Provisioning	Deletes a user
Update User UID	Provisioning	Updates user properties according to a change in the User UID attribute
Update User Group	Provisioning	Updates user properties according to a change in the User Group attribute
Update User Password Change Time	Provisioning	Updates user properties according to a change in the User Password Change Time attribute
Update Shell	Provisioning	Updates user properties according to a change in the Shell attribute
Update Home Directory	Provisioning	Updates user properties according to a change in the Home Directory attribute
Update Account Expiry Date	Provisioning	Updates user properties according to a change in the Account Expiry Date attribute
Update User GECOS	Provisioning	Updates user properties according to a change in the User GECOS attribute
Set Password	Provisioning	Updates user properties according to a change in the Password attribute The changed password must conform to the password policy requirements of the target system.
Update Secondary Group Names	Provisioning	Updates user properties according to a change in the Secondary Group Names attribute Do not update the User Login field when you update the Secondary Group Names value. When you specify the secondary group name for the first time and then run this function, the primary group name is assigned the same value as the secondary group name. However, after the value of the primary group name is changed, you cannot set the secondary group name to the same value. On Solaris, the value of the Secondary Group Names field in the User Defined process form must always be different from the value of the Primary Group Name field.
Update Inactive Days	Provisioning	Updates user properties according to a change in the Update Inactive Days attribute This function is not supported on AIX 5.2.

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

Multilanguage Support

The connector supports the following languages:

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

Note: 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

Files and Directories That Comprise the Connector

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

`Operating Systems/UNIX/UNIX SSH`

These files and directories are listed in the following table.

File in the Installation Media Directory	Description
`ext/sshfactory.jar`	This file contains the JSCAPE libraries. These libraries are used to open an SSH session with the target server.
`lib/xliSSH.jar`	This file contains the Java classes that are required to support provisioning and reconciliation in SSH.
Files in the `resources` directory	Each of these resource bundle files contains language-specific information that is used by the connector. **Note:** A **resource bundle** is a file containing localized versions of the text strings that are displayed on the user interface of Oracle Identity Manager. These text strings include GUI element labels and messages displayed on the Administrative and User Console.
`scripts/privateKeyGen.sh`	This file is used to generate the private key in SSH.
`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.
`test/config/log.properties`	This file is used to specify the log level and the directory in which the log file is to be created when you run the testing utility.
`test/config/userAttribute_NonAIX_prov.properties`	This file contains the parameters required for dynamic provisioning on non-AIX platforms.
`test/config/userAttribute_AIX_prov.properties`	This file contains the parameters required for dynamic provisioning on AIX platform.
`test/config/userAttribute_NonAIX_recon.properties`	This file contains the parameters required for dynamic reconciliation on non-AIX platforms.
`test/config/userAttribute_AIX_recon.properties`	This file contains the parameters required for dynamic reconciliation on AIX platform.
`test/lib/xliSSHTest.jar`	This file contains the Java classes that are required to run the client for running test calls from the Oracle Identity Manager server.
`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.

File in the Installation Media Directory	Description
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 ■ Nontrusted source reconciliation schedule task
xml/XellSSHUser.xml	This XML file contains the configuration for the Xellerate 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.

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

The "Step 3: Copying the Connector Files" section on page 2-17 provides instructions to copy these files into the required directories.

Determining the Release Number of the Connector

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

Before Deployment

To determine the release number of a connector:

1. Extract the contents of the `xliSSH.jar` file. This file is in the following directory on the installation media:

   `Operating Systems/UNIX/UNIX SSH/lib`

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.

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

After Deployment

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

See Also: *Oracle Identity Manager Design Console Guide*

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

2

Deploying the Connector

Deploying the connector involves the following steps:

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

Step 1: Verifying Deployment Requirements

The following table lists the deployment requirements for the connector.

Item	Requirement
Oracle Identity Manager	Oracle Identity Manager release 8.5.3 or later
Target systems	The target system can be any one of the following: ■ Solaris 8 - 10 ■ HP-UX 11.11 (trusted/nontrusted) ■ Linux (Red Hat Advanced Server 2.1, Red Hat Enterprise Linux 3.x, or Red Hat Linux 4.x) ■ AIX 4.3, AIX 5.1 - 5.3
External code	JSCAPE SSH/SSH Libraries (SSH factory)
Other systems	OpenSSH, OpenSSL, operating system patches (HP-UX), and SUDO software (only if the SUDO Admin mode is required)
Target system user account	root or sudo user You provide the credentials of this user account while performing the procedure in the "Defining IT Resources" section on page 2-21. 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 (en_US) supported by the target system	The target system must support en_US character encoding standards such as UTF-8 and iso8859. Use the following command to check the en_US character encoding standards that the target system supports: `locale -a` **Note:** If the target system does not support any of the en_US character encoding standards, then you must install the en_US language pack.

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	-

Step 2: Configuring the Target System

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

- Platform-Specific Configuration Steps
- Installing External Software
- Public Key Authentication (SSH Key Generation)

Platform-Specific Configuration Steps

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

- Configuration Steps for Solaris and Linux
- Configuration Steps for AIX
- Configuration Steps for HP-UX

Configuration Steps for Solaris and Linux

Perform the following steps for Solaris and Linux environments:

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

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

   The same file name with the path must be inserted in the Passwd Mirror File/User Mirror File attribute of the reconciliation scheduled task.

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

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

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

Configuration Steps for AIX

Perform the following steps for AIX environments:

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

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

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

Configuration Steps for HP-UX

Perform the following steps for HP-UX environments:

1. Log in as root and then run the following command:
2. Select **Auditing and Security** and **System Security Policies.** A message is displayed asking if you want to switch to the trusted mode.
3. Click **OK.**

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

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

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

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

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

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

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

Installing External Software

This section describes the procedure to install external software.

Installing OpenSSH

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

For Solaris 8

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

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

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

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

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

a. `prngd-0.9.25-sol8-sparc-local.gz` (optional)

b. `tcp_wrappers-7.6-sol8-sparc-local.gz` (optional, but recommended)

c. `zlib-1.2.1-sol8-sparc-local.gz`

d. `openssl-0.9.7g-sol8-sparc-local.gz`

e. `openssh-4.1p1-sol8-sparc-local.gz`

2. Create a group with the name `sshd` and group ID `27`. Add a user with the name `sshadmin` to this group.

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

```
PermitRootLogin yes
```

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

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

For Solaris 9

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

http://www.sunfreeware.com/

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

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

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

You must install these packages in the following order:

a. `prngd-0.9.25-sol9-sparc-local.gz`

b. `tcp_wrappers-7.6-sol9-sparc-local.gz`

c. `zlib-1.2.1-sol9-sparc-local.gz`

d. `openssl-0.9.7d-sol9-sparc-local.gz`

e. `openssh-3.9p1-sol9-sparc-local.gz`

2. Create a group with the name `sshd` and group ID `27`. Add a user with the name `sshadmin` to this group.

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

```
PermitRootLogin yes
```

> **Note:** Implement this change only if it does not violate local security policies. If Public Key Authentication is enabled, then you can change the value of `PermitRootLogin` to `without-password`.
>
> Instead of using the root account, if you can use a user account with sudo privileges, then you do not need to perform this step.

For Solaris 10

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

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

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

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

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

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

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

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

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

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

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

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

```
PermitRootLogin yes
```

> **Note:** Implement this change only if it does not violate local security policies. If Public Key Authentication is enabled, then you can change the value of `PermitRootLogin` to `without-password`.
>
> Instead of using the root account, if you can use a user account with sudo privileges, then you do not need to perform this step.

For Linux

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

For AIX

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

1. Download and install OpenSSL.

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

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

   Then, enter the following command to install OpenSSL:

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

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

2. Download and install PRNG.

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

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

   Then, enter the following command to install PRNG:

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

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

3. Download and install OpenSSH.

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

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

   Then, enter the following commands to install openSSH:

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

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

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

```
PermitRootLogin yes
```

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

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

Installing and Configuring SUDO

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

For Solaris

1. If SUDO is not installed on the Solaris server, then first download it.
   - For Solaris 9, download the `sudo-1.6.8p4-sol9-sparc-local.gz` file from

     http://www.sunfreeware.com/programlistsparc9.html#sudo
   - For Solaris10, download the `sudo-1.6.8p9-sol9-sparc-local.gz` file from

     http://www.sunfreeware.com/programlistsparc9.html#sudo
   - For Solaris 8, download the `sudo-1.6.8p9-sol8-sparc-local.gz` file from

     http://www.sunfreeware.com/programlistsparc8.html#sudo
2. Use the following command to install SUDO:

```
pkgadd -d filename_with_full_path
```

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

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

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

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

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

   This connector uses the following commands:

   - `useradd`
   - `usermod`

- passwd
- cat
- diff
- userdel

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

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

For information about customizing the sudoers file, refer to

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

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

```
Defaults timestamp_timeout=0
```

This is a prerequisite for this connector to work successfully.

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

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

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

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

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

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

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

For HP-UX

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

http://hpux.cs.utah.edu

Enter the following command to install SUDO:

```
swinstall -s filename_with_full_path
```

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

OIM_home/Xellerate/XLIntegrations/SSH/config/

For example, if you have a group named 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
- passwd
- cat
- diff
- userdel

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

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

For information about customizing the sudoers file, refer to

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

---

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

   ```
   Defaults timestamp_timeout=0
   ```

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

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

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

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

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

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

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

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

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

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

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

For AIX

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

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

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

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

3. Enter the following command to install SUDO:

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

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

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

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

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

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

   This connector uses the following commands:

   - mkuser
   - chuser
   - passwd
   - cat
   - diff
   - usermod
   - rmuser

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

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

   For information about customizing the sudoers file, refer to

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

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

   ```
   Defaults timestamp_timeout=0
   ```

   This is a prerequisite for this connector to work successfully.

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

For Red Hat Advanced Server 2.1

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

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

   Then, enter the following command to install SUDO:

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

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

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

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

   1. Enter the following command:

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

   2. Make the required changes in the `sudoers` file.
   3. Enter the following command:

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

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

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

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

   The commands that this connector uses are:

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

- userdel

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

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

For information about customizing the sudoers file, refer to

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

---

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

```
Defaults timestamp_timeout=0
```

This is a prerequisite for this connector to work successfully.

4. Create a SUDO user as follows:

   a. Enter the following command:

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

   In this command:

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

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

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

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

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

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

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

   Then, enter the following command to install SUDO:

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

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

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

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

1. Enter the following command:

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

2. Make the required changes in the `sudoers` file.
3. Enter the following command:

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

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

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

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

This connector uses the following commands:

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

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

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

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

`http://www.courtesan.com/sudo/man/sudoers.html`

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

   ```
   Defaults timestamp_timeout=0
   ```

   This is a prerequisite for this connector to work successfully.

4. Create a SUDO user as follows:

   a. Enter the following command:

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

      In this command:

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

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

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

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

Public Key Authentication (SSH Key Generation)

This section discusses the following topics:

- Configuring Public Key Authentication
- Configuring SSH Public Key Authentication

Configuring Public Key Authentication

To configure Public Key Authentication:

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

   For Solaris or Linux:

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

   For HP-UX:

   ```
   dos2ux privateKeyGen.sh
   ```

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

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

   - id_rsa: This is a private key file.
   - authorized_keys: This file lists public keys that can be used to log in.

5. When the keys are generated successfully, edit the sshd_config file for Public Key Authentication and test login.
6. After successfully testing login, copy the id_rsa file to the following directory:

   OIM_home/Xellerate/XLIntegrations/SSH/Config

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

Configuring SSH Public Key Authentication

To configure SSH Public Key Authentication:

For Solaris

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

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

> **Note:** Change the value of `PermitRootLogin` to `yes` only if it does not violate local security policies. If Public Key Authentication is enabled, then you can change the value of `PermitRootLogin` to `without-password`.
>
> Instead of using the root account, if you can use a user account with sudo privileges, then you do not need to perform this step.

2. To restart the SSH server, enter the following commands:
   - `/etc/init.d/sshd stop`
   - `/etc/init.d/sshd start`
3. To test login:

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

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

For HP-UX

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

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

> **Note:** Change the value of `PermitRootLogin` to `yes` only if it does not violate local security policies. If Public Key Authentication is enabled, then you can change the value of `PermitRootLogin` to `without-password`.
>
> Instead of using the root account, if you can use a user account with sudo privileges, then you do not need to perform this step.

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

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

3. To test login, enter the following command:

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

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

For Linux

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

```
mkdir /.ssh
```

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

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

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

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

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

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

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

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

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

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

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

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

For AIX

1. The first step of this procedure depends on the version of AIX that you are using:
   - For AIX 4.3, use the `/etc/openssh/sshd_config` file to set the following parameters:

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

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

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

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

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

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

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

3. To restart the SSH server, enter the following commands:
   - `/opt/ssh/sbin/sshd` (For AIX 4.3)
   - `/usr/sbin/sshd` (For AIX 5.2)
4. To test the login, enter the following command:

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

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

Note: This release of the connector does not support Public Key Authentication provisioning if it is implemented through the SUDO Admin mode. The Public Key Authentication used for system access is available for the root user. This point is also mentioned in the Known Issues list in Chapter 5.

Step 3: Copying the Connector Files

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

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

`Operating Systems/UNIX/UNIX SSH`

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

File in the Installation Media Directory	Destination Directory
`ext/sshfactory.jar`	*OIM_home*`/xellerate/ThirdParty`
`lib/xliSSH.jar`	*OIM_home*`/xellerate/JavaTasks`
`lib/xliSSH.jar`	*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: While installing Oracle Identity Manager in a clustered environment, you copy the contents of the installation directory to each node of the cluster. Similarly, you must copy the `connectorResources` directory and the JAR files to the corresponding directories on each node of the cluster.

Step 4: Configuring the Oracle Identity Manager Server

Configuring the Oracle Identity Manager server involves the following procedures:

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

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

Changing to the Required Input Locale

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

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

Clearing Content Related to Connector Resource Bundles from the Server Cache

While performing the instructions described in the "Step 3: Copying the Connector Files" section on page 2-17, you copy files from the `resources` directory on the installation media into the *`OIM_home`*`/xellerate/connectorResources` directory. Whenever you add a new resource bundle in the `connectorResources` directory or make a change in an existing resource bundle, you must clear content related to connector resource bundles from the server cache.

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

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

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

   `OIM_home``/xellerate/bin/`*`batch_file_name`*

2. Enter one of the following commands:

   - On Microsoft Windows:

     ```
     PurgeCache.bat ConnectorResourceBundle
     ```

   - On UNIX:

     ```
     PurgeCache.sh ConnectorResourceBundle
     ```

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

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

OIM_home`/xellerate/config/xlConfig.xml`

Enabling Logging

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

- `ALL`

  This level enables logging for all events.

- `DEBUG`

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

- `INFO`

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

- `WARN`

  This level enables logging of information about potentially harmful situations.

- `ERROR`

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

- `FATAL`

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

- `OFF`

  This level disables logging for all events.

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

- **BEA WebLogic**

  To enable logging:

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

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

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

     For example:

     `log4j.logger.Adapter.TELNETSSH=INFO`

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

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

- **IBM WebSphere**

  To enable logging:

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

     log4j.logger.Adapter.TELNETSSH=*log_level*

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

     For example:

     log4j.logger.Adapter.TELNETSSH=INFO

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

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

- **JBoss Application Server**

  To enable logging:

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

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

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

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

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

  JBoss_home/server/default/log/server.log

- **OC4J**

  To enable logging:

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

     log4j.logger.Adapter.TELNETSSH=*log_level*

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

     For example:

     log4j.logger.Adapter.TELNETSSH=INFO

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

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

Step 5: Importing the Connector XML Files

To import the connector XML files:

1. Open the Oracle Identity Manager Administrative and User Console.
2. Click the **Deployment Management** link on the left navigation bar.
3. Click the **Import** link under Deployment Management. A dialog box for locating files is displayed.
4. Locate and open the `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 server Solaris` IT resource is displayed.
8. Specify values for the parameters of the `SSH server Solaris` IT resource. Refer to the table in the "Defining IT Resources" section on page 2-21 for information about the values to be specified.
9. Click **Next.** The Provide IT Resource Instance Data page for a new instance of the `SSH Server` IT resource type is displayed.
10. Click **Skip** to specify that you do not want to define another IT resource. The Confirmation page is displayed.

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

11. Click **View Selections**.

    The contents of the XML file are displayed on the Import page. You *may* see a cross-shaped icon along with some nodes. 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.

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

Defining IT Resources

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

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

Parameter	Description
Admin Password/Private file Pwd	Password of the administrator dead_line (for root/non-SUDO) or jdoe Here, jdoe is the SUDO user password, for the SUDO Admin mode. **Note:** For the SUDO Admin mode, the private key is not supported. You must not specify a value for this mode. If a private key is used, then the Private Key PassPhrase must be provided as the value of this 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 $
Login Prompt	You can ignore this parameter. This parameter is not used for SSH.
Password Prompt	You can ignore this parameter. This parameter is not used for SSH.
Whether Trusted System (HP-UX)	YES (for trusted HP-UX System) or NO (for nontrusted HP-UX system)
Whether SUDO Admin Mode	NO (for root) or YES (for SUDO Admin mode)
Target Locale	Target locale (language and country) For the locale that you want to use, you can specify a value similar to the following: ■ en_US for English ■ ja_JP for Japanese ■ fr_FR for French **Note:** You must not make any change (uppercase or lowercase) in the value that you specify.
Supported Character Encoding (en_US) - Target	Encoding format for the en_US target locale The default value is UTF-8. **Note:** You can check which en_US encoding formats the target system supports by using the following command: locale -a

Parameter	Description
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

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

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

Configuring Reconciliation

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

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

Partial Reconciliation

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

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

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

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

Batched Reconciliation

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

You can configure batched reconciliation to avoid these problems.

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

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

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

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

- `BatchSize`: 20
- `NumberOfBatches`: 10

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

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

Configuring System Properties

To configure system properties:

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

Configuring Trusted Source Reconciliation

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

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

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 configure trusted source reconciliation:

1. Open the Oracle Identity Manager Administrative and User Console.
2. Click the **Deployment Management** link on the left navigation bar.
3. Click the **Import** link under Deployment Management. A dialog box for locating files is displayed.
4. Locate and open the `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**.

Creating the Reconciliation Scheduled Tasks

To create 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.

Specifying Values for the Scheduled Task Attributes

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

- `SSH UserTrusted Reconciliation task` (Scheduled task for trusted source reconciliation)
- `SSH User Non Trusted Reconciliation task` (Scheduled task for nontrusted source reconciliation)

The following table describes the attributes of both scheduled tasks.

Note:

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

Attribute	Description	Sample Value
`Server`	Name of the IT resource	`SSH server Solaris`

Attribute	Description	Sample Value

Passwd Mirror File/User Mirror File	Name 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.
		/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.
		/etc/shadow1

IsTrusted	Specifies whether or not reconciliation is to be carried out in trusted mode	Specify Yes for trusted source reconciliation. Specify No for nontrusted source reconciliation.
Target System Recon - Resource Object name	Name of the target system resource object	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
Date Format	Format in which date values sent from the target system are to be saved during reconciliation The value that you specify must be the same as the value specified in the "Configuring System Properties" section on page 3-2.	yyyy/MM/dd hh:mm:ss z

Attribute	Description	Sample Value
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.
NumOfBatches	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
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.

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

Enabling Reconciliation in Oracle Identity Manager Release 9.0.1

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

See Also: *Oracle Identity Manager Design Console Guide*

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

Adding Custom Attributes for Reconciliation

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

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

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

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

1. Open the following file in the *OIM_home*/xellerate/XLIntegrations/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:

   Connector_Attribute=OIM_Server_Attribute

   For example:

   maxage=Users.AccountExpiryDate

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

   For non-AIX platforms:

   OIM_Server_Attribute=Target_Server_Attribute_index

   For example:

   Users.DefaultShell=6

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

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

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

   b. Click **Query for Records**.

   c. On the Resource Objects Table tab, double-click the 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. Modify the process definition to include the mapping between the newly added attribute and the corresponding reconciliation field as follows:

a. Open the Process Definition form. This 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.

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

Configuring Provisioning

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

This section discusses the following topics related to configuring provisioning:

- Compiling Adapters
- Adding Custom Attributes for Provisioning

Compiling Adapters

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

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

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

- SSH Disable User
- SSH GECOS Updated
- SSH Set Password
- SSH Default Shell Updated
- SSH Password Change Time Updated
- SSH Create User
- SSH Delete User
- SSH Home Directory Updated
- SSH Primary Group Name Updated
- SSH Account Expiry Date Updated
- SSH User UID Updated
- SSH Secondary Group Name Updated
- SSH Inactive Days Updated
- SSH User Login Updated
- SSH Enable User
- SSH Prepopulate User Login
- SSH Prepopulate End Date

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

To compile adapters by using the Adapter Manager form:

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

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

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

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

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

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

To view detailed information about an adapter:

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

Adding Custom Attributes for Provisioning

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

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

See Also: *Oracle Identity Manager Design Console Guide*

1. Modify the attribute entries in the following file:

   For the AIX platform:

   OIM_home/xellerate/XLIntegrations/SSH/config/userAttribute_AIX_prov.properties

   For non-AIX platforms:

   OIM_home/xellerate/XLIntegrations/SSH/config/userAttribute_NonAIX_prov.properties

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

   OimAttributeName=TargetAttributeName

   For example:

   homeDir=-d

2. Add a new column in the process form.
   a. Open the process form. This form is in the Development Tools folder of the Oracle Identity Manager Design Console.
   b. Click **Create New Version**.
   c. In the Create a New Version dialog box, specify the version name in the **Label** field, save the changes, and then close the dialog box.
   d. From the **Current Version** list, select the newly created version.
   e. On the Additional Columns tab, click **Add**.
   f. Specify the new field name and other values.
3. Add a new variable in the variable list.

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

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

c. On the Adapter Factory Table tab, double-click the **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 Status (Literal)" parameter:

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

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

iii. In the **Value** field, enter **Status**.

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

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

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

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

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

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

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

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

d. In the Edit Set Variable Task Parameters dialog box, select **input** from the **Variable Name** list, select **Adapter Task** from the **Operand Type** list, and the

Operand Qualifier as the Adapter Task that you have created in the previous step. Then, click **Save**.

6. Map the process form columns and adapter variables for the Create User process task as follows:
   a. Open the Process Definition form. This form is in the Process Management folder of the Design Console.
   b. Click the **Query for Records** icon.
   c. On the Process Definition Table tab, double-click the **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.

Configuring the Connector for Multiple Installations of the Target System

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

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

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

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

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

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

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

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

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

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

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, you must set the required values in the `config.properties` file. This file is in the *`OIM_home`*`/xellerate/XLIntegrations/SSH/test/config/config.properties` directory.

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

Attribute	Description	Default Attribute (Sample Value)
`hostname`	IP address of the target server on which SSH provisioning is to be performed	`10.1.1.114`
`loginPrompt`	Default login prompt of the target server	`login`
`passwordPrompt`	Default password prompt of the target server	`Password`
`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	`dead_line`
`admin`	UNIX server administrator credentials for the SSH server	`root`
`action`	Action to be tested The value can be one of the following: ■ `CREATE` ■ `MODIFY` ■ `DELETE`	`CREATE`
`userName`	User attribute	jdoe
`uID`	New user UID for the user identified by `UserName`	`12548`

Attribute	Description	Default Attribute (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

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

For UNIX:

OIM_home/xellerate/XLIntegrations/SSH/test/scripts/SSH.sh

For Microsoft Windows:

OIM_home/xellerate/XLIntegrations/SSH/test/scripts/SSH.bat

5

Known Issues

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

- This connector does not support logins that differ by case only. It also requires all logins to be distinct considering that their values are automatically converted to uppercase by Oracle Identity Manager.

  For example, the user logins `jdoe` and `JDOE` would be considered different in a UNIX server. However, from Oracle Identity Manager, the input would always be passed as `JDOE`, because user ID values are stored only in uppercase in Oracle Identity Manager.

- During provisioning, the data in the User Defined form fields must not contain the shell prompt character. Because there is a variation in shell prompt character depending on the target UNIX server, it should be checked in the target system.
- During provisioning, the maximum permitted date value for account expiry is `31/12/2099.`
- Suppose that a user on the UNIX server is disabled. If the Set Password function is run on this user account, then the account is automatically reenabled.
- During reconciliation, the Group Name field is reconciled as a number and not as the exact name because it is stored directly as the group ID in the target system.
- During reconciliation, the user login field is successfully reconciled only if the user ID does not exceed 32 characters.
- During reconciliation with the trusted option set to `YES` in the IT resource, the value for the `Shadow Mirror File` attribute must not be NULL or blank.
- While creating an IT resource, the user name provided for `Admin UserId` must be that of an active user in the target system. This means that the user must not be locked or disabled.
- When you configure an IT resource for an SSH user account and then directly provision it to a user, the Create User Task function is rejected. The user account is not created on the target system. The following message is displayed:

  "`SSH_USERCREATION_NOTCONNECTED_FAIL not able to connect successfully to the Target System Server`".

- On AIX 5.2, while providing data in the GECOS field, ensure that there are no spaces. If there are spaces in this field, then the Update User Login function would not work.
- The Update Secondary Group Names and Update User Login functions do not work simultaneously.
- The Update Inactive Days function does not work on AIX 5.2.

- Oracle Identity Manager does not support special characters in the User ID field on HP-UX, Solaris, and Linux target systems. If a user were created with special characters in the User Login field, then reconciliation would not work.
- The Enable User function is not supported by the HP-UX (trusted) target system.
- The connector has been tested and certified only for RSA keys, and not DSA. In addition, this connector has been tested and certified for only single key configuration and not multiple keys.
- Public Key Authentication provisioning is not supported by this connector if it is implemented through the SUDO Admin mode. Refer to the "Step 2: Configuring the Target System" section on page 2-2 for more details.
- This release of the connector does not support all the shell types that are available on various operating systems. For information about the supported shell types, refer to the table at the end of the "Step 1: Verifying Deployment Requirements" section on page 2-1.
- The entry of multibyte characters is not supported in some fields. Refer to Appendix A for more information about this known issue.

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, group are separated by commas, with no intervening whitespace between group names.
Password	passwd	Password
Reenter Password	Reenter Password	Password reentered for confirmation
User Login	login	New login name, specified as a string of printable characters It cannot contain a colon (`:`) or a newline (`\n`) character.
User UID	uid	Numeric value of the user ID This value must be unique and nonnegative. The default is to use the smallest ID value greater than 99 and greater than the number used for any other user. Values between 0 and 99 are typically reserved for system accounts.
Primary Group Name	initial group	The group name or number of the user's initial login group.
Default Shell	shell	User's login shell
GECOS	comment	Generally, a short description of the login It is used as the field for the user's full name. This information is stored in the user's `/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

Index

S

T

U

V

X