Oracle® Identity Manager

Connector Guide for UNIX Telnet

Release 9.0.1

B31141-01

June 2006

ORACLE®

Oracle Identity Manager Connector Guide for UNIX Telnet, Release 9.0.1

B31141-01

Primary Authors: Debapriya Datta, Shiladitya Guha

Contributing Authors: Don Gosselin, Lyju Vadassery

Contents

3 Testing the Connector

4 Known Issues

Index

Preface

Oracle Identity Manager Connector Guide for UNIX Telnet provides information about integrating Oracle Identity Manager with UNIX Telnet.

Note: This is a transitional release following Oracle's acquisition of Thor Technologies. Some parts of the product and documentation still refer to the original Thor company name and Xellerate product name and will be rebranded in future releases.

Audience

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

Documentation Accessibility

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

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

TTY Access to Oracle Support Services

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

Related Documents

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

- *Oracle Identity Manager Release Notes*
- *Oracle Identity Manager Installation and Upgrade Guide for JBoss*
- *Oracle Identity Manager Installation and Upgrade Guide for WebLogic*
- *Oracle Identity Manager Installation and Upgrade 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 Connector Framework Guide*
- Connector guides for various third-party applications

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager 9.0.1 connector documentation set, visit Oracle Technology Network at

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

Conventions

The following text conventions are used in this document:

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

1

About the Telnet Connector

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

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

This chapter contains the following sections:

Supported Functionality

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

Function	Type	Description
Create User	Provisioning	Creates a user in UNIX server with the input values provided ▪ 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 should only be populated 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 "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 provisioned user in UNIX server
Update User UID	Provisioning	Updates the configuration of a user in UNIX server according to a change in the User UID attribute

Function	Type	Description
Update User Group	Provisioning	Updates the configuration of a user in UNIX server according to a change in the Group attribute
Update User Password Change Time	Provisioning	Updates the configuration of a user in UNIX server according to a change in the Password Change Time attribute
Update Shell	Provisioning	Updates the configuration of a user in UNIX server according to a change in the Shell attribute
Update Home Directory	Provisioning	Updates the configuration of a user in UNIX server according to a change in the Home Directory attribute
Update User Account Expiration Date	Provisioning	Updates the configuration of a user in UNIX server according to a change in the Account Expiration Date attribute
Update User GECOS	Provisioning	Updates the configuration of a user in UNIX server according to a change in the GECOS attribute
Set Password	Provisioning	Updates the configuration of a user in UNIX server according to a change in the Password attribute
Update Secondary Group Name	Provisioning	Updates the configuration of a user in UNIX server according to a change in the Secondary Group Name attribute Do not update the User Login field when you update the Secondary Group Names value. On Solaris, the value of the Secondary Group Names field must always be different from the value of the Primary Group Name field.
Update Inactive Days	Provisioning	Updates the configuration of a user in UNIX server for attribute: Update Inactive Days. This function does not work on AIX 5.2
Update User Login	Provisioning	Updates the configuration of a user in UNIX server 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 in UNIX server
Enable User	Provisioning	Enables a disabled existing user in 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 with respect 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

Reconciliation Module

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

- User Login
- User UID
- Primary Group Name

- Default Shell
- Home Directory
- GECOS
- Password Change Time
- Account Expiry Date

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

Provisioning Module

The following fields are provisioned:

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

Files and Directories That Comprise the Connector

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

```
Operating Systems\UNIX\Unix Telnet Rev 4.1.0.zip
```

These files and directories are listed in the following table.

File in the Installation Media Directory	Description
xml/XLITelnet_DM.xml	This file contains the following Telnet User components of the connector: ■ Telnet User IT resource type ■ Custom process form ■ Process task and rule generator adapters (along with their mappings) ■ Resource object ■ Provisioning process ■ Pre-populate rules that are used with this connector
xml/XLITelnetSchedulerTask_DM.xml	This file contains the scheduled task for reconciliation.
xml/XLITelnet_Trusted_DM.xml	This file contains the following Telnet User components for the Telnet connector for Trusted system (HP-UX): ■ Telnet User IT resource type ■ Custom process form ■ Process task and rule-generator connectors (along with their mappings) ■ Resource object ■ Provisioning process ■ Pre-populate rules that are used with this connector
lib/801/xliTelnet.jar	This file contains the Java classes that are required to connect to the target system through Telnet, for Oracle Identity Manager 8.0.1.
ext/sshfactory.jar	This file contains the JSCAPE libraries. These libraries are used to open an SSH session with the target server.
tests/	This is the test suite for the Telnet connector.
tests/config/config.properties	This file specifies the properties required by the client for running test calls from the Oracle Identity Manager server.
tests/lib/xliTelnetTest.jar	This file contains the Java classes required to run the client for running test calls from the Oracle Identity Manager server.
tests/scripts/telnet.bat	This file contains the script required to run the client for running test calls from the Oracle Identity Manager server.
docs/B31141_01.pdf docs/html	These are PDF and HTML versions of this guide, which provides instructions to deploy the connector.

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

The "Step 3: Copying the Connector Files" section on page 2-5 provides instructions to copy these files into the required directories.

2

Deploying the Connector

Deploying the connector involves the following steps:

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, Solaris 9, Solaris 10 ■ HP-UX 11.11 (trusted or nontrusted) ■ Linux (RedHat Linux AS 2.1, RedHat Linux AS 3.x, or RedHat Linux AS 4.1) ■ AIX 4.3 or AIX 5.2
Target system host platforms	The target system host platform can be any one of the following: ■ Solaris 8, Solaris 9, or Solaris 10 ■ HP-UX 11.11 (trusted or nontrusted) ■ Linux (RedHat Linux AS 2.1, RedHat Linux AS 3.x, or RedHat Linux AS 4.1) ■ AIX 5.2 or AIX 4.3
External code	JSCAPE Telnet/SSH Libraries (SSH factory)
Other systems	Operating system patches (HP-UX, as described later in this guide)

Step 2: Configuring the Target System

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

Platform-Specific Configuration Steps

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

For Solaris and Linux

Perform the following steps for Solaris and Linux environments:

1. Ensure that the `/etc/passwd` and `/etc/shadow` directories 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 (AIX)` task 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 scheduled task for reconciliation.

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 > /mainUserFile1
   tr '#' ' ' < /mainUserFile1 > /mainUserFileTemp1
   cat /mainUserFileTemp1 > /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.

For HP-UX

Note: If you are using an HP-UX configuration, then start from Step 1. Otherwise, go to Step 5.

1. Log in as root by specifying the user name as `sam`.
2. Click **Enter.**
3. Select to **Auditing and Security** and **System Security Policies.** A message is displayed asking if you want to convert from the system to the trusted mode.
4. Click **OK.**

   If the following message is displayed, then skip Step 5:

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

5. 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://www.software.hp.com/portal/swdepot/displayInstallInfo.do?productNumber=ShadowPassword`

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

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

Installing Required and Optional Enablement Patches

The ShadowPW includes new files to support shadow passwords.

The following are required patches:

PHNE_23502, PHCO_24402, PHCO_25526, PHCO_25568, PHCO_27036, PHCO_27038, PHCO_27040, PHCO_27041, PHCO_27042, PHCO_27064, PHCO_28192, PHCO_28194, and PHCO_30402

Do not install a corequisite patch if it is superseded by another patch.

Apply the following guidelines when you install these patches:

- When CDE is present, it is very important to install both patch PHSS_26492 and PHSS_26493.
- Patch PHCO_28193 must be installed only if UUCP is present.
- Patch PHCO_28176 must be installed only if the `/usr/lbin/tsconvert` command is present.
- Patch PHCO_27035 defines the prototypes of new APIs.
- Patch PHCO_27909 updates the main pages.
- If necessary, patch PHCO_23578 updates the Software Distributor.
- An optional patch is not installed if the underlying product is removed from the system. For example, if UUCP has been removed, then patch PHCO_28193 is not installed.

> **Note:** If UUCP is installed, then in order to ensure correct functioning of the `uucp` command in shadow mode, you must also install patch PHCO_28193.

Installing the Shadow Password Bundle

To install the bundle:

1. Log in as root.
2. Download the `ShadowPassword.depot` file to the `/tmp` directory.
3. Verify that the file has been downloaded by using the `swlist` command as follows:

   ```
   swlist -d @ complete_path/ShadowPassword.depot
   ```

   The following is sample output of the `swlist` command:

   ```
   # Initializing...
   # Contacting target localhost...
   #
   # Target: localhost:/tmp/ShadowPassword.depot
   # Bundle(s):
   #
   ShadowPassword  B.11.11.02  HP-UX 11.11 Shadow Password Bundle
   ```

   Note: When you use the `swlist` and `swinstall` commands, you must specify the complete path in the source depot.

4. Create a backup of the system before installing the product.
5. On a standalone system, run the `swinstall` command to install the product as follows:

   ```
   swinstall -x autoreboot=true -s complete_path/ShadowPassword.depot \*
   ```

6. Verify that the `ShadowPW.SHADOW` file set is installed by using the `swlist` command as follows:

   ```
   # swlist -l fileset complete_path/ShadowPW.SHADOW
   ```

   The following is sample output of this command

   ```
   # Initializing...
   # Contacting target "localhost"...
   #
   # Target: localhost:/
   #
   ShadowPW.SHADOW  B.11.11.02 HP-UX 11.11 Shadow Password Enablement
   ```

   After the patches are installed, the system can be converted to use shadow passwords by running the `pwconv` command. This command converts the entries in the `/etc/passwd` file to the appropriate format in the `/etc/shadow` file.
7. Reboot the system. Remember to keep the shadow password handy.

Uninstalling the Shadow Password Bundle

To disable the shadow passwords and switch back to standard passwords:

1. Log in as root.
2. Run `pwunconv`.

   Caution: If you skip this step, then the system may become unbootable in the multiuser mode.

3. Reboot the system.
4. Ensure that the `/etc/shadow` file does not exist and that passwords are in the `/etc/password` file.

   You can do this by running the `swremove Shadow` command.
5. From the Shadow Password bundle, remove the enabling patches that were installed but are no longer needed. This is an optional step.
6. Ensure that a password mirror file is created on the server by running 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 (AIX)` attribute of the scheduled task for reconciliation.
7. Ensure that a shadow mirror file is created on the server by running a command similar to the following:

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

   The same file name with the path must be inserted in the `Shadow Mirror File` attribute of the scheduled task for reconciliation.

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. The directory paths given in the first column of this table correspond to the location of these files on the installation media.

See Also: "Files and Directories That Comprise the Connector" on page 1-3

File in the Installation Media Directory	Destination Directory
The following files in the `xml` directory: ■ `XLITelnet_DM.xml` ■ `XLITelnetSchedulerTask_DM.xml` ■ `XLITelnet_Trusted_DM.xml`	`xellerate_home/xellerate/xml`
`lib/801/xliTelnet.jar`	*xellerate_home*`/xellerate/XLIntegrations/Telnet/lib/801`
`lib/xliTelnet.jar`	*xellerate_home*`/xellerate/JavaTasks`
`lib/xliTelnet.jar`	*xellerate_home*`/xellerate/ScheduleTask`
`ext/sshfactory.jar`	*xellerate_home*`/xellerate/ext`
The following files in the tests directory: ■ `config/config.properties` ■ `lib/xliTelnetTest.jar` ■ `scripts/telnet.bat`	*xellerate_home*`/xellerate/tests`
`docs/B31141_01.pdf` `docs/html`	*xellerate_home*`/xellerate/docs`

Step 4: Importing the Connector Files

To import the connector files:

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

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

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

11. Click **View Selections.**

    The contents of the XML file are displayed in the Deployment Manager – Import window. You may see a cross-shaped icon along with some nodes. You must remove these nodes. To do this, right-click each such node and then select **Remove.**
12. Click **Import.** The connector file is imported into Oracle Identity Manager.
13. Perform the same procedure to import the `XLITelnetSchedulerTask_DM.xml` file, which is in the *`xellerate_home`*`/xellerate/XLIntegrations/Telnet/xml` directory.
14. If you plan to use the connector in trusted source reconciliation mode, then perform the same procedure to import the XLITelnet_Trusted_DM.xml file. This file is in the *`xellerate_home`*`/xellerate/XLIntegrations/Telnet/xml` directory.

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

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

Defining IT Resources

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

Parameter Name	Parameter Description
`Admin UserId`	`root`
`Admin Password`	`dead_line`
`Server IP Address`	`10.1.1.61`
`Port`	`23`
`Server OS`	AIX, HP-UX, SOLARIS, or LINUX
`Shell Prompt`	# or $
`Login Prompt`	`login`
`Password Prompt`	Password
`Whether Trusted System (HP-UX)`	`YES` (for trusted HP-UX System) or `NO` (for nontrusted HP-UX system)

Step 5: Configuring Reconciliation

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

- Adding Prerequisites for Reconciliation
- Defining Scheduled Tasks

Adding Prerequisites for Reconciliation

This section consists of the following:

- Configuring System Properties
- Configuring Trusted Source Reconciliation Oracle Identity Manager Entities

Configuring System Properties

To configure system properties:

1. Open the Oracle Identity Manager Design Console.
2. Navigate to the System Configuration page.
3. Add a new entry in the Server category:
   - Name: `Default date format`
   - Keyword: `XL.DefaultDateFormat`
   - Value: `MMM dd, yyyy 'at' hh:mm:ss z`
4. Click **Save**.

Configuring Trusted Source Reconciliation Oracle Identity Manager Entities

This procedure involves the following steps:

1. Open the Resource Object form, and search for the Xellerate User. On the Object Reconciliation tab, add the required reconciliation fields. Add all the reconciliation fields that would be needed to provide input for mandatory fields in the Xellerate User form. For example, fields like User Login and First Name. Only one mandatory field, Password, can be ignored. All the mandatory fields of the User Defined process form must be mapped.
2. Open the Process Definition form, and search for the Xellerate User. On the Reconciliation Field Mappings tab, add the required reconciliation field mappings. All the mandatory fields of the user defined process form should be mapped.
3. Open the Reconciliation Rules form, and create a new rule for the Xellerate User resource object, with a rule element.
4. After creating the rule, select the Active check box.

Defining Scheduled Tasks

Configuring reconciliation involves creating scheduled tasks for User reconciliations. To create a scheduled task:

1. Open the Oracle Identity Design Console.
2. Expand the **Xellerate Administration** folder.
3. Select **Task Scheduler.**
4. Click **Find**. The details of the predefined scheduled tasks are displayed on two different tabs.
5. Enter a number in the **Max Retries** field. This number represents the number of times Oracle Identity Manager attempts to complete the task before assigning the `ERROR` status to the task.
6. Ensure that the **Disabled** and **Stop Execution** check boxes are cleared.
7. In the Start region, double-click the **Start Time** field. From the date-time editor that is displayed, set the date and time at which you want the task to run.
8. Specify that you want the task to run on a recurring basis by selecting the **Recurring Intervals** option.
9. 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 almost specify the time interval at which you want to run the task on a recurring basis.
   - To set the task to run only once, select the **Once** option.
10. Provide values for the user-configurable attributes of the scheduled task. Refer to the appropriate table in the "Specifying Attributes for the Scheduled Task Attributes" section on page 2-9 for information about the values to be specified.

    See Also: *Oracle Identity Manager Design Console Guide* for information about adding and removing task attributes

11. 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.
12. Repeat Steps 5 through 11 to define the second scheduled task.

After you create both scheduled tasks, proceed to the "Step 6: Compiling Adapters" section on page 2-10.

Specifying Attributes for the Scheduled Task Attributes

You must specify values for the following attributes of the reconciliation scheduled task.

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

Attribute	Description	Sample Value
Server	Name of the IT Resource	Telnet server-Solaris

Passwd Mirror File/User Mirror File	Name of the passwd mirror file/user mirror file
	This attribute is used only on AIX. 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: The value of this attribute must not be null or blank, even for a trusted system. However, the reconciliation process ignores it.
		/etc/shadow1

Target System Recon - Resource Object name	Name of the target system resource object	Telnet User

Attribute	Description	Sample Value
Trusted Source Recon - Resource Object name	Name of the trusted source resource object	Xellerate User

After you specify values for these task attributes, go to Step 11 of the procedure to create scheduled tasks.

Step 6: Compiling Adapters

The following adapters are imported into Oracle Identity Manager when you import the connector XML file. You must compile these adapters before you can use them to provision accounts on the target system.

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

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 the **Compile All** option.

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

   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 adapters that match the criteria you specified in Step 2.

To view detailed information about an adapter:

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

3

Testing the Connector

After you deploy the connector, you must test it to ensure that it functions as expected. Tests that you can run on the connector can be divided into the following high-level categories:

This chapter contains the following sections:

Running Connector Tests

This section discusses test cases that you can perform by using the troubleshooting utility.

You can use the troubleshooting utility to directly use the connector to identify the cause of problems associated with connecting to the Oracle Identity Manager server and performing basic operations on the server.

Before you can use the troubleshooting utility, you must set the required values in the `config.properties` file. This file is in the *`xellerate_home`*`/xellerate/XLIntegrations/Telnet/tests/config/config.properties` directory.

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

Name	Description	Default Attribute (Sample Values)
`hostname`	IP address of the UNIX server on which Telnet provisioning is to be performed	`10.1.1.114`
`loginPrompt`	Login prompt of the UNIX server Default login	`login`
`passwordPrompt`	Password prompt of the UNIX server Default password	`Password`
`shellPrompt`	Default shell prompt of the UNIX server: # for Solaris, Linux, and HP-UX $ for AIX	`#`
`Port`	Port at which the Telnet server is listening	`23`

Name	Description	Default Attribute (Sample Values)
Os Type	Operating system type of the UNIX server Accepted values are SOLARIS, LINUX, HP-UX, and AIX.	SOLARIS
adminpassword	Admin user password	dead_line
Admin	UNIX server administrator credentials for the Telnet server	root
Action	Action to be tested The values can be any of the following: ■ CREATE ■ MODIFY ■ DELETE	CREATE
UserName	User attribute	jdoe
UID	New user UID for the above user	12548

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

xellerate_home/xellerate/XLIntegrations/Telnet/tests/scripts/telnet.bat

Troubleshooting

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

Problem Description	Solution
Process definition: TELNET User Process task: Create User **Returned Error Message:** Not able to connect successfully to the UNIX server **Returned Error Code:** TELNET_USERCREATION_NOTCONNECTED_FAIL	Check if the UNIX server is running and accessible. In addition, check the admin credentials entered in the IT Resource.
Process definition: TELNET User Process task: Create User **Returned Error Message:** User does not have creation rights on the UNIX server **Returned Error Code:** TELNET_USERCREATION_NORIGHTS_FAIL	Check the admin credentials entered in the IT Resource.

Problem Description	Solution
Process definition: TELNET User Process task: Create User **Returned Error Message:** Oracle Identity Manager is not able to create a user successfully due to a missing password file **Returned Error Code:** `TELNET_USERCREATION_MISSINGPASSWDFILE_FAIL`	Check the availability of the `/etc/passwd` file on the UNIX server.
Process definition: TELNET User Process task: Create User **Returned Error Message:** User name already exists on the UNIX server **Returned Error Code:** `TELNET_USERCREATION_USEREXISTS_FAIL`	Check the user name that you have entered. A user with the same name already exists on the UNIX server.
Process definition: TELNET User Process task: Create User **Returned Error Message:** User ID already exists and is unique or specified user ID is out of range **Returned Error Code:** `TELNET_USERCREATION_USERID_FAIL`	Check the user ID that you have entered. Another user may have the same user ID on the UNIX server or the value of the user ID may be out of range.
Process definition: TELNET User Process task: Create User **Returned Error Message:** User name too long **Returned Error Code:** `TELNET_USERCREATION_NAMEFORMAT_FAIL`	Check the user name that you have entered.
Process definition: TELNET User Process task: Create User **Returned Error Message:** User ID already exists and is unique or specified user ID is out of range **Returned Error Code:** `TELNET_USERCREATION_USERID_FAIL`	Check the user ID that you have entered. Another user may have the same ID on the UNIX server or the value of the user ID may be out of range.
Process definition: TELNET User Process task: Create User **Returned Error Message:** Group name or ID mismatch **Returned Error Code:** `TELNET_USERCREATION_NOGROUP_FAIL`	Check the primary group name that you have entered. The group name entered should exist on the UNIX server. In addition, spaces are not allowed in the group name.

Problem Description	Solution
Process definition: TELNET User Process task: Create User **Returned Error Message:** Missing default shell **Returned Error Code:** TELNET_USERCREATION_NOSHELL_FAIL	Check the default shell that you have specified. The default shell specified should be installed on the UNIX server.
Process definition: TELNET User Process task: Create User **Returned Error Message:** Wrong expiry date **Returned Error Code:** TELNET_USERCREATION_DATERANGE_FAIL	Check the date selected.
Process definition: TELNET User Process task: Create User **Returned Error Message:** Wrong password change time **Returned Error Code:** TELNET_USERCREATION_WRONGCHANGETIME_FAIL	Check the password change time that you have entered.
Process definition: TELNET User Process task: Create User **Returned Error Message:** Wrong GECOS data **Returned Error Code:** TELNET_USERCREATION_GECOSFORMAT_FAIL	Check the GECOS data that you have entered. Spaces are not allowed.
Process definition: TELNET User Process task: Create User **Returned Error Message:** Wrong Home Directory **Returned Error Code:** TELNET_USERCREATION_HOMEDIR_FAIL	Check the home directory that you have specified.
Process definition: TELNET User Process task: Create User **Returned Error Message:** Wrong Home Directory **Returned Error Code:** TELNET_USERCREATION_SETPASSWORD_FAIL	Check the password, and reenter the password data.

Problem Description	Solution
Process definition: TELNET User Process task: Delete User **Returned Error Message:** Not able to connect to the UNIX server **Returned Error Code:** `TELNET_USERDELETION_NOTCONNECTED_FAIL`	Check if the UNIX server is running and accessible. In addition, check the admin credentials specified in the IT Resource.
Process definition: TELNET User Process task: Delete User **Returned Error Message:** Oracle Identity Manager administrator does not have deletion rights on the UNIX server **Returned Error Code:** `TELNET_USERDELETION_NORIGHTS_FAIL`	Check the admin credentials specified in the IT Resource.
Process definition: TELNET User Process task: Delete User **Returned Error Message:** User does not exist on the UNIX server **Returned Error Code:** `TELNET_USERDELETION_NOUSER_FAIL`	Check if the particular user exists on the UNIX server.
Process definition: TELNET User Process task: GECOS Updated **Returned Error Message:** Not able to connect to the UNIX server **Returned Error Code:** `TELNET_UPDATEGECOS_NOTCONNECTED_FAIL`	Check if the UNIX server is running and accessible. In addition, check the admin credentials specified in the IT Resource.
Process definition: TELNET User Process task: GECOS Updated **Returned Error Message:** Oracle Identity Manager administrator does not have deletion rights on the UNIX server **Returned Error Code:** `TELNET_UPDATEGECOS_NORIGHTS_FAIL`	Check the admin credentials specified in the IT Resource.
Process definition: TELNET User Process task: GECOS Updated **Returned Error Message:** User does not exist on the UNIX server **Returned Error Code:** `TELNET_UPDATEGECOS_NOUSER_FAIL`	Check if the particular user exists on the UNIX server.

Problem Description	Solution
Process definition: TELNET User Process task: GECOS Updated **Returned Error Message:** Update user GECOS failed due to data format or size **Returned Error Code:** `TELNET_UPDATEGECOS_FORMAT_FAIL`	Check the GECOS data that you have entered. Spaces are not allowed.
Process definition: TELNET User Process task: Password Change Time Updated **Returned Error Message:** Not able to connect to the target system **Returned Error Code:** `TELNET_UPDATECHANGETIME_NOTCONNECTED_FAIL`	Check if the UNIX server is running and accessible. In addition, check the admin credentials specified in the IT Resource.
Process definition: TELNET User Process task: Password Change Time Updated **Returned Error Message:** Oracle Identity Manager administrator does not have deletion rights on the UNIX server **Returned Error Code:** `TELNET_UPDATECHANGETIME_NORIGHTS_FAIL`	Check the admin credentials specified in the IT Resource.
Process definition: TELNET User Process task: Password Change Time Updated **Returned Error Message:** User does not exist on the UNIX server **Returned Error Code:** `TELNET_UPDATECHANGETIME_NOUSER_FAIL`	Check if the user exists on the UNIX server.
Process definition: TELNET User Process task: Password Change Time Updated **Returned Error Message:** Update password change time failed due to wrong change time format **Returned Error Code:** `TELNET_UPDATECHANGETIME_WRONGCHANGETIME _FAIL`	Check the Password change time data that you have specified.

Problem Description	Solution
Process definition: TELNET User Process task: Home Directory Updated **Returned Error Message:** Not able to connect to the UNIX server **Returned Error Code:** `TELNET_UPDATEHOMEDIR_NOTCONNECTED_FAIL`	Check if the UNIX server is running and accessible. In addition, check the admin credentials specified in the IT Resource.
Process definition: TELNET User Process task: Home Directory Updated **Returned Error Message:** Oracle Identity Manager administrator does not have deletion rights on the UNIX server **Returned Error Code:** `TELNET_UPDATEHOMEDIR_NORIGHTS_FAIL`	Check the admin credentials specified in the IT Resource.
Process definition: TELNET User Process task: Home Directory Updated **Returned Error Message:** User does not exist on the UNIX server **Returned Error Code:** `TELNET_UPDATEHOMEDIR_NOUSER_FAIL`	Check if the user exists on the UNIX server.
Process definition: TELNET User Process task: Home Directory Updated **Returned Error Message:** Update user home directory failed due to wrong directory **Returned Error Code:** `TELNET_UPDATEHOMEDIR_INVALIDDIR_FAIL`	Check the Home Directory that you have specified.
Process definition: TELNET User Process task: Default Shell Updated **Returned Error Message:** Not able to connect to the UNIX server **Returned Error Code:** `TELNET_UPDATESHELL_NOTCONNECTED_FAIL`	Check if the UNIX server is running and accessible. In addition, check the admin credentials specified in the IT Resource.
Process definition: TELNET User Process task: Default Shell Updated **Returned Error Message:** Oracle Identity Manager administrator does not have deletion rights on the UNIX server **Returned Error Code:** `TELNET_UPDATESHELL_NORIGHTS_FAIL`	Check the admin credentials specified in the IT Resource.

Problem Description	Solution
Process definition: TELNET User Process task: Default Shell Updated **Returned Error Message:** User does not exist on the UNIX server **Returned Error Code:** TELNET_UPDATESHELL_NOUSER_FAIL	Check if the user exists on the UNIX server.
Process definition: TELNET User Process task: Default Shell Updated **Returned Error Message:** Update user shell failed as the specified shell does not exist **Returned Error Code:** TELNET_UPDATESHELL_NOTEXIST_FAIL	Check the default shell that you have entered. The default shell specified should be installed on the UNIX server.
Process definition: TELNET User Process task: User UID Updated **Returned Error Message:** Not able to connect to the UNIX server **Returned Error Code:** TELNET_UPDATEUID_NOTCONNECTED_FAIL	Check if the UNIX server is running and accessible. In addition, check the admin credentials specified in the IT Resource.
Process definition: TELNET User Process task: User UID Updated Returned Error Message: Oracle Identity Manager administrator does not have deletion rights on the UNIX server **Returned Error Code:** TELNET_UPDATEUID_NORIGHTS_FAIL	Check the admin credentials specified in the IT Resource.
Process definition: TELNET User Process task: User UID Updated **Returned Error Message:** User does not exist on the UNIX server **Returned Error Code:** TELNET_UPDATEUID_NOUSER_FAIL	Check if the user exists on the UNIX server.
Process definition: TELNET User Process task: User UID Updated **Returned Error Message:** User UID already exists and unique **Returned Error Code:** TELNET_UPDATEUID_UNIQUE_FAIL	Check the user UID that you have specified. Another user may have the same UID on the UNIX server.

Problem Description	Solution
Process definition: TELNET User Process task: User UID Updated **Returned Error Message:** Specified user UID is too long **Returned Error Code:** `TELNET_UPDATEUID_SIZE_FAIL`	Check the user UID that you have entered. The value specified is out of the acceptable range.
Process definition: TELNET User Process task: Account Expiry Date Updated **Returned Error Message:** Not able to connect to the UNIX server **Returned Error Code:** `TELNET_UPDATEEXPDATE_NOTCONNECTED_FAIL`	Check whether the UNIX server is running and accessible. In addition, check the admin credentials specified in the IT Resource.
Process definition: TELNET User Process task: Account Expiry Date Updated **Returned Error Message:** Oracle Identity Manager administrator does not have deletion rights on the UNIX server **Returned Error Code:** `TELNET_UPDATEEXPDATE_NORIGHTS_FAIL`	Check the admin credentials specified in the IT Resource.
Process definition: TELNET User Process task: Account Expiry Date Updated **Returned Error Message:** User does not exist on the UNIX server **Returned Error Code:** `TELNET_UPDATEEXPDATE_NOUSER_FAIL`	Check if the user exists on the UNIX server.
Process definition: TELNET User Process task: Account Expiry Date Updated **Returned Error Message:** User expiry date not updated due to wrong date **Returned Error Code:** `TELNET_UPDATEEXPDATE_DATERANGE_FAIL`	Check the account expiry date that you have specified.
Process definition: TELNET User Process task: Primary Group Name Updated **Returned Error Message:** Not able to connect to the UNIX server **Returned Error Code:** `TELNET_UPDATEGROUP_NOTCONNECTED_FAIL`	Check if the UNIX server is running and accessible. In addition, check the admin credentials specified in the IT Resource.

Problem Description	Solution
Process definition: TELNET User Process task: Primary Group Name Updated **Returned Error Message:** Oracle Identity Manager administrator does not have deletion rights on the UNIX server **Returned Error Code:** TELNET_UPDATEGROUP_NORIGHTS_FAIL	Check the admin credentials specified in the IT Resource.
Process definition: TELNET User Process task: Primary Group Name Updated **Returned Error Message:** User does not exist on the UNIX server **Returned Error Code:** TELNET_UPDATEGROUP_NOUSER_FAIL	Check if the user exists on the UNIX server.
Process definition: TELNET User Process task: Primary Group Name Updated **Returned Error Message:** Group name or group ID does not exist on the UNIX server **Returned Error Code:** TELNET_UPDATEGROUP_NOGROUP_FAIL	Check the primary group name that you have specified.
Process definition: TELNET User Process task: Password Updated **Returned Error Message:** Not able to connect to the UNIX server **Returned Error Code:** TELNET_SETPASSWORD_NOTCONNECTED_FAIL	Check if the UNIX server is running and accessible. In addition, check the admin credentials specified in the IT Resource.
Process definition: TELNET User Process task: Password Updated **Returned Error Message:** Oracle Identity Manager administrator does not have deletion rights on the UNIX server **Returned Error Code:** TELNET_SETPASSWORD_NORIGHTS_FAIL	Check the admin credentials specified in the IT Resource.
Process definition: TELNET User Process task: Password Updated **Returned Error Message:** User does not exist on the UNIX server **Returned Error Code:** TELNET_SETPASSWORD_NOUSER_FAIL	Check if the user exists on the UNIX server.

Problem Description	Solution
Process definition: TELNET User Process task: Password Updated **Returned Error Message:** Group name or group ID does not exist on the UNIX server **Returned Error Code:** `TELNET_SETPASSWORD_MISMATCH_FAIL`	The password specified and the one entered again for confirmation must match.
Process definition: TELNET User Process task: Password Updated **Returned Error Message:** Group name or group id does not exist on the UNIX server **Returned Error Code:** `TELNET_SETPASSWORD_SIZE_FAIL`	Enter the password according to the policy defined on the UNIX server.
Process definition: TELNET User Process task: Secondary Group Name Updated **Returned Error Message:** User does not exist on the UNIX server **Returned Error Code:** `TELNET_ UPDATESECONDARYGROUP_NOUSER_FAIL`	Check if the user exists on the UNIX server.
Process definition: TELNET User Process task: Secondary Group Name Updated **Returned Error Message:** Oracle Identity Manager administrator does not have deletion rights on the UNIX server **Returned Error Code:** `TELNET_ UPDATESECONDARYGROUP_NORIGHTS_FAI L`	Check the admin credentials specified in the IT Resource.
Process definition: TELNET User Process task: Secondary Group Name Updated **Returned Error Message:** Group name or group ID does not exist on the UNIX server **Returned Error Code:** `TELNET_UPDATESECONDARYGROUP_NOGRO UP_FAIL`	Check the secondary group names that you have specified.

Problem Description	Solution
Process definition: TELNET User Process task: Secondary Group Name Updated **Returned Error Message:** Oracle Identity Manager is not able to connect successfully to the UNIX server **Returned Error Code:** `TELNET_UPDATESECONDARYGROUP_NOTCONNECTED_FAIL`	Check if the UNIX server is running and accessible. In addition, check the admin credentials specified in the IT Resource.
Process definition: TELNET User Process task: Inactive Days Updated **Returned Error Message:** Oracle Identity Manager administrator does not have update rights in Target System **Returned Error Code:** `TELNET_UPDATEINACTIVEDAYS_NORIGHTS_FAIL`	Check the admin credentials specified in the IT Resource.
Process definition: TELNET User Process task: Inactive Days Updated **Returned Error Message:** Oracle Identity Manager is not able to connect successfully to the target system **Returned Error Code:** `TELNET_UPDATEINACTIVEDAYS_NOTCONNECTED_FAIL`	Check if the UNIX server is running and accessible. In addition, check the admin credentials specified in the IT Resource.
Process definition: TELNET User Process task: Inactive Days Updated **Returned Error Message:** User does not exist on the target system **Returned Error Code:** `TELNET_UPDATEINACTIVEDAYS_NOUSER_FAIL`	Check if the user exists on the UNIX server.
Process definition: TELNET User Process task: Inactive Days Updated **Returned Error Message:** Invalid numeric number **Returned Error Code:** `TELNET_UPDATEINACTIVEDAYS_INVALID_NUMERIC_ARGUMENT_FAIL`	Check if the value specified in the Inactive Days field is numeric.

Problem Description	Solution
Process definition: TELNET User Process task: User Login Updated **Returned Error Message:** Oracle Identity Manager is not able to connect successfully to the Target System **Returned Error Code:** `TELNET_UPDATELOGINCLASS_NOTCONNECTED_FAIL`	Check if the UNIX server is running and accessible. In addition, check the admin credentials specified in the IT Resource.
Process definition: TELNET User Process task: User Login Updated **Returned Error Message:** Oracle Identity Manager administrator does not have update rights in Target System **Returned Error Code:** `TELNET_UPDATELOGINCLASS_NORIGHTS_FAIL`	Check the secondary group names that you have specified.
Process definition: TELNET User Process task: User Login Updated **Returned Error Message:** User does not exist on the target system **Returned Error Code:** `TELNET_UPDATELOGINCLASS_NOUSER_FAIL`	Check if the user exists on the UNIX server.
Process definition: TELNET User Process task: Disable User **Returned Error Message:** Oracle Identity Manager is not able to connect successfully to the target system **Returned Error Code:** `TELNET_DISABLEUSER_NOTCONNECTED_FAIL`	Check if the UNIX server is running and accessible. In addition, check the admin credentials specified in the IT Resource.
Process definition: TELNET User Process task: Disable User **Returned Error Message:** Oracle Identity Manager administrator does not have update rights in target system **Returned Error Code:** `TELNET_DISABLEUSER_NORIGHTS_FAIL`	Check the admin credentials specified in the IT Resource.
Process definition: TELNET User Process task: Disable User **Returned Error Message:** User does not exist on the target system **Returned Error Code:** `TELNET_DISABLEUSER_NOUSER_FAIL`	Check if the user exists on the UNIX server.

Problem Description	Solution
Process definition: TELNET User Process task: Enable User **Returned Error Message:** Oracle Identity Manager is not able to connect successfully to the target system **Returned Error Code:** `TELNET_ENABLEUSER_NOTCONNECTED_FAIL`	Check if the UNIX server is running and accessible. In addition, check the admin credentials specified in the IT Resource.
Process definition: TELNET User Process task Enable User **Returned Error Message:** Oracle Identity Manager is not able to connect successfully to the target system **Returned Error Code:** `TELNET_ENABLEUSER_NOTCONNECTED_FAIL`	Check the admin credentials specified in the IT Resource.
Process definition: TELNET User Process task: Enable User **Returned Error Message:** User does not exist on the target system **Returned Error Code:** `TELNET_ENABLEUSER_NOUSER_FAIL`	Check if the user exists on the UNIX server.

Note:

The following run-time exception message is displayed when:

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

Run-time exception message:

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

4

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 would get 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 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 provisioning, the data in the User Defined form fields must not contain the shell prompt character. As there is a variation in shell prompt character based on the relevant target Unix Server, it should be checked in the target.
- During reconciliation with the trusted option set to `YES` in the IT Resource, the value for the `Shadow Mirror File` task 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.
- During provisioning, the maximum permitted date value for account expiry is `31/12/2099.`
- After configuring an IT Resource for a Telnet user account and then directly provisioning it to a user, the Create User Task function is rejected. The user account is not created on the target system. The following message is displayed:

  "`TELNET_USERCREATION_NOTCONNECTED_FAIL not able to connect successfully to the Target System Server`".
- On AIX 5.2, while providing data in the GECOS field, ensure that there are no spaces. If there are spaces in this field, then the Update User Login function would not work.
- The Update Secondary Group Name and Update User Login functions do not work simultaneously.
- The Update Inactive Days function does not work on AIX 5.2.

- Oracle Identity Manager does not support special characters in the User ID field on HP-UX, Solaris, and Linux target systems. If a user were created with special characters in the User Login field, then reconciliation would not work.
- The Enable User function is not supported by the HP-UX (trusted) target system.

Index