

Oracle® Identity Manager

Connector Guide for RSA Authentication Manager

Release 9.0.3

B32366-01

February 2007

Oracle Identity Manager Connector Guide for RSA Authentication Manager, Release 9.0.3

B32366-01

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

Primary Authors: Debapriya Datta, Shiladitya Guha

Contributing Authors: Don Gosselin, Lyju Vadassery

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

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

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

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

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

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

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

Contents

Preface	v
Audience	v
Documentation Accessibility	v
Related Documents	vi
Documentation Updates	vi
Conventions	vi
What's New in the Oracle Identity Manager Connector for RSA Authentication Manager?	vii
Software Updates	vii
Documentation-Specific Updates.....	viii
1 About the Connector	
Supported Functionality	1-1
Multilanguage Support	1-4
Reconciliation Module	1-4
Reconciling Multivalue Attribute Groups.....	1-4
Provisioning Module	1-5
RSA Authentication Manager User Provisioning	1-5
RSA Authentication Manager Token Provisioning.....	1-5
Files and Directories That Comprise the Connector	1-5
Determining the Release Number of the Connector	1-7
2 Deploying the Connector	
Step 1: Verifying Deployment Requirements	2-1
Step 2: Configuring the Target System	2-2
Setting Up the Remote Manager	2-2
Configuring Strong Authentication Between Oracle Identity Manager and the Remote Manager 2-4	
Configuring SSL Client (Oracle Identity Manager Server) Authentication	2-4
Step 3: Copying the Connector Files	2-6
Step 4: Configuring the Oracle Identity Manager Server	2-7
Changing to the Required Input Locale.....	2-7
Clearing Content Related to Connector Resource Bundles from the Server Cache	2-7
Enabling Logging	2-8

Step 5: Importing the Connector XML Files	2-10
Defining IT Resources	2-11
IT Resource: ACE Remote Manager.....	2-11
IT Resource: ACE Server Remote	2-11
Step 6: Configuring Reconciliation	2-12
Configuring Trusted Source Reconciliation	2-12
Installing Software Tokens	2-13
Creating Scheduled Tasks.....	2-14
Enabling Reconciliation in Oracle Identity Manager Release 9.0.1	2-15
Step 7: Compiling Adapters	2-15
Configuring the Connector for Multiple Installations of the Target System	2-16

3 Testing and Troubleshooting

Running Connector Tests.....	3-1
Troubleshooting.....	3-4

4 Known Issues

Index

Preface

Oracle Identity Manager Connector Guide for RSA Authentication Manager provides information about integrating Oracle Identity Manager with RSA Authentication Manager.

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 RSA Authentication Manager.

Documentation Accessibility

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

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

TTY Access to Oracle Support Services

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

Related Documents

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

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

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

- *Oracle Identity Manager Connector Framework Guide*

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager 9.0.3 connector documentation set, visit Oracle Technology Network at

<http://www.oracle.com/technology/documentation/index.html>

Conventions

The following text conventions are used in this document.

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

What's New in the Oracle Identity Manager Connector for RSA Authentication Manager?

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

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

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

- [Software Updates](#)
These include updates made to the connector software.
- [Documentation-Specific Updates](#)
These include major changes made to the connector documentation. These changes are not related to software updates.

See Also: *Oracle Identity Manager Release Notes*

Software Updates

This section discusses the following software updates implemented in this release of the connector.

Enhancement in the Multilanguage Support Feature

In addition to the three languages supported by the earlier release, this release of the connector supports seven new languages. All the supported languages are listed in the "[Multilanguage Support](#)" section on page 1-4.

RSA APIs do not support certain characters of the Japanese, Simplified Chinese, Traditional Chinese, Korean, and French languages. An item pertaining to this limitation of the target system has been added in the Known Issues list in [Chapter 4](#).

Reconciling Multivalued Attribute Groups

The "[Reconciling Multivalued Attribute Groups](#)" section on page 1-4 provides information about this functionality.

Support for OC4J

Earlier releases of the connector supported the following application servers:

- JBoss Application Server
- BEA WebLogic
- IBM WebSphere

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

Correction in Commands for ACE 5.0, 5.2, and 6.0

The commands for ACE 5.0, 5.2, and 6.0 have been changed in the following sections:

- Step 4 of the "[Setting Up the Remote Manager](#)" section on page 2-2
- The "[Running Connector Tests](#)" section on page 3-1

Addition of Configuration File

The configuration file that is added in the XML directory is mentioned in "[Files and Directories That Comprise the Connector](#)" section on page 1-5.

New Scheduled Task Attributes

The "[Creating Scheduled Tasks](#)" section on page 2-14, provides descriptions for the following attributes that have been added in the scheduled task definition:

- IsTrusted
- IsDeleteAllowed

Documentation-Specific Updates

- The following IT resource parameters have been moved from the "IT Resource: ACE Remote Manager" section to the "[IT Resource: ACE Server Remote](#)" section on page 2-11:
 - Target Locale: Country
 - Target Locale: Language
- In the "[Enabling Logging](#)" section on page 2-8, instructions for each of the application servers that are supported by this release of the connector have been added.
- In the "[Step 7: Compiling Adapters](#)" section on page 2-15, the instruction about restarting the node has been removed from Step 4 of the procedure to compile adapters.
- All content pertaining to RSA Authentication Manager 6.0.2 has been removed.

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 RSA Authentication Manager is used to integrate Oracle Identity Manager with RSA Authentication Manager.

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

This chapter contains the following sections:

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

Supported Functionality

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

Function	Type	Description
Create User	Provisioning	Creates a user
Delete User	Provisioning	Deletes a user This function would not run if the user to be deleted is an administrator.
Enable Token	Provisioning	Enables a disabled token
Disable Token	Provisioning	Disables an existing token

Function	Type	Description
Assign SecurID Tokens to Users	Provisioning	<p>Assigns a token to a user</p> <p>While assigning a software token to the user, the Type of Algorithm field must be filled in the process form.</p> <ul style="list-style-type: none"> ■ If SID is selected in the Type of Algorithm field, then values must be specified for the following fields in the process form: <ul style="list-style-type: none"> - Software Token File Name: This is the name of the RSA SecurID software token file in which user and token information is saved. You must enter the file name with the full directory path and ensure that the extension is <code>.sdtid</code>. - Encryption Key Type - Copy Protection Flag - Password Usage and Interpretation Method - Password - Encryption Key Type - Password Usage and Interpretation Method - Password <p>Note: If these combinations do not matter, then you can accept the default options.</p> ■ If AES is specified in the Type of Algorithm field, then: <p>You must enter a value in the Software Token File Name field of the process form. This is the name of the RSA SecurID software token file in which user and token information is saved. You must enter the file name with the full directory path and ensure that the extension is <code>.sdtid</code>.</p> <p>The Password field is optional.</p> <p>The following fields can be ignored:</p> <ul style="list-style-type: none"> - Encryption Key Type - Copy Protection Flag - Password Usage and Interpretation Method
Revoke SecurID Tokens from Users	Provisioning	Revokes a token from a user

Function	Type	Description
Assign Users to RSA Authentication Manager Groups	Provisioning	<p>Assigns a user to a group</p> <p>You must ensure that the following prerequisites are met before you use this function:</p> <ul style="list-style-type: none"> Valid groups exist in RSA Authentication Manager. The required lookup codes (corresponding to valid group names) are added in the <code>UD_Lookup.ACE_Group</code> lookup definition. For example, for a group called <code>Managers</code> defined in ACE DB, the following entry must be added as the lookup code: <p>Code Key: <code>Managers</code></p> <p>Decode: <code>Managers</code></p> <p>Lang: <code>en</code></p> <p>Country: <code>US</code></p>
Remove Users from RSA Authentication Manager Groups	Provisioning	<p>Removes a user from a group</p> <p>You must ensure that the following prerequisites are met before you use this function:</p> <ul style="list-style-type: none"> Valid groups exist in ACE DB. This function is run only after the Assign Users to RSA Authentication Manager Groups function has been run.
Set Token PIN	Provisioning	Updates the configuration of a token according to a change in the PIN attribute
Set PIN to Next Token Code Mode	Provisioning	Sets the PIN to the next token code mode in RSA Authentication Manager
Track Lost Tokens	Provisioning	Updates the configuration of a token according to a change in the Track Lost attribute
Test Login	Provisioning	<p>Verifies the login for a new user to whom a token has been assigned</p> <p>You must ensure that the following prerequisites are met before you use this function:</p> <ul style="list-style-type: none"> An agent host is defined in the RSA Authentication Manager database. The user for whom the Test Login function is to be implemented is enabled on this agent host. After this is done, the RSA Authentication Manager is restarted (Broker as well as Authentication Server). <p>For software token types, you must enter the passcode, instead of the token code, in the Current Token Code field in the process form.</p> <p>The passcode can be viewed by using the software token application, which is installed on the Oracle Identity Manager server.</p> <p>See Also: The "Installing Software Tokens" section on page 2-13 for more information</p>
Update User ID	Provisioning	Updates the configuration of a user according to a change in the User ID attribute

Multilanguage Support

This release of the connector supports the following languages:

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

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

Reconciliation Module

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

- Default Login
- First Name
- Last Name
- Group Name
- Group Login
- Token Serial Number
- Type of Token

Reconciling Multivalue Attribute Groups

The following are features related to the reconciliation of multivalue attribute groups:

- Group names that include the names of sites are entered in the *group_name@domain_name* format. In Oracle Identity Manager 9.0.3, you can choose not to include the domain name while creating or updating the name of a group. Similarly, regardless of whether or not the name of a group in the target system includes a domain name, it is reconciled in Oracle Identity Manager.

Note: The term "domain name" in the Oracle Identity Manager context is the same as "site name" in RSA Authentication Manager.

- When a user is deleted from a group in ACE, the group is also deleted from the user's ACE process child table.

Provisioning Module

This section discusses the fields that are provisioned.

RSA Authentication Manager User Provisioning

The following fields are provisioned:

- Default Login
- First Name
- Last Name
- Group Login
- Group Name

RSA Authentication Manager Token Provisioning

The following fields are provisioned:

- Token Serial Number
- PIN
- Current Token Code
- Lifetime (hours)
- Number of Digits
- Type of Token
- Copy Protection Flag
- Password
- Password Usage and Interpretation Method
- Software Token File Name
- Encryption Key Type
- Type of Algorithm

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:

Security Applications\RSA Authentication Manager

These files and directories are listed in the following table.

File in the Installation Media Directory	Description
lib\xliACE.jar	This file contains the Java classes that are required for provisioning in RSA Authentication Manager.
remotePackage\config\xl.policy	This file contains the security configuration that is required for the RMI server codebase for running calls on RSA Authentication Manager for reconciliation.
remotePackage\lib\ACE50\ACEUser.dll	This file contains the shared library that is required to support provisioning in RSA ACE Server 5.0.

File in the Installation Media Directory	Description
remotePackage\lib\ACE52\ACEUser.dll	This file contains the shared library that is required to support provisioning in RSA ACE Server 5.2.
remotePackage\lib\ACE52Sol\libACEUser.so	This file contains the shared library that is required to support provisioning in RSA Authentication Manager.
remotePackage\lib\AuthMgr60\ACEUser.dll	This file contains the shared library that is required to support provisioning in RSA Authentication Manager 6.0.
remotePackage\lib\AuthMgr60Sol\libACEUser.so	This file contains the shared library that is required to support provisioning in RSA Authentication Manager 6.0, on Solaris.
remotePackage\lib\xliACE.jar	This file contains the Java classes that are required for provisioning in RSA Authentication Manager.
remotePackage\scripts\AuthMgrImportXLCert.bat	This file contains the script for importing the required security certificate into the remote manager keystore (.xlkeystore).
remotePackage\scripts\AuthMgrImportXLCert.sh	This file contains the script for importing the required security certificate into the remote manager keystore (.xlkeystore) on Solaris.
remotePackage\tests\config\xl.policy	This file contains the security configuration required for the RMI server codebase to run test calls on RSA Authentication Manager.
remotePackage\tests\lib\xliACETestServer.jar	This file contains the Java classes that are required to run the RMI server for running test calls on RSA Authentication Manager.
remotePackage\tests\logs	This directory is used by the connector test suite to log the results of the tests. The log files are created in this directory.
remotePackage\tests\scripts\runTestServer.bat	This file contains the script that is required to run the RMI server for running test calls on RSA Authentication Manager.
remotePackage\tests\scripts\runTestServer.sh	This file contains the script that is required to run the RMI server for running test calls on RSA Authentication Manager, on Solaris.
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\AuthMgrImportRMCert.bat	This file contains the script for importing the required security certificate in the Oracle Identity Manager server keystore (.xlkeystore).
scripts\AuthMgrImportRMCert.sh	This file contains the script for importing the required security certificate in the Oracle Identity Manager server keystore (.xlkeystore) on Solaris.
tests\config\config.properties	This file contains the properties required by the RMI client for running test calls from the Oracle Identity Manager server.

File in the Installation Media Directory	Description
tests\lib\xliACETestClient.jar	This file contains the Java classes required to run the RMI client for running test calls from the Oracle Identity Manager server.
tests\logs	This directory is used by the connector test suite to log the results of the tests. The log files are created in this directory.
tests\scripts\runTestClient.bat	This file contains the script required to run the RMI client for running test calls from the Oracle Identity Manager Server, for Microsoft Windows.
tests\scripts\runTestClient.sh	This file contains the script required to run the RMI client for running test calls from the Oracle Identity Manager Server, for Solaris.
xml\xliAuthMgrScheduledTask_DM.xml	This file contains definitions for the components required for reconciliation.
xml\xliAuthMgrToken_DM.xml	This file contains definitions for the following ACE Token components of the connector: <ul style="list-style-type: none"> ■ ACE Token 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\xliAuthMgrTrusted.xml	This file contains configuration parameters for the Xellerate User. You must import this file only if you plan to use the connector in trusted source reconciliation mode.
xml\xliAuthMgrUser_DM.xml	This file contains definitions for the following ACE User components of the connector: <ul style="list-style-type: none"> ■ 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

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 2-6 provides instructions to copy these files into the required directories.

Determining the Release Number of the Connector

To determine the release number of the connector that you have deployed:

1. Extract the contents of the `xliACE.jar` file. For a connector that has been deployed, this file is in the following directory:

`OIM_home\xellerate\JavaTasks`

2. Open the `manifest.mf` file in a text editor. The `manifest.mf` file is one of the files bundled inside the `xliACE.jar` file.

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

See Also: *Oracle Identity Manager Design Console Guide*

Deploying the Connector

Deploying the connector involves the following steps:

- [Step 1: Verifying Deployment Requirements](#)
- [Step 2: Configuring the Target System](#)
- [Step 3: Copying the Connector Files](#)
- [Step 4: Configuring the Oracle Identity Manager Server](#)
- [Step 5: Importing the Connector XML Files](#)
- [Step 6: Configuring Reconciliation](#)
- [Step 7: Compiling Adapters](#)

If you want to configure the connector for multiple installations of RSA Authentication Manager, then perform the following procedure:

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

Step 1: Verifying Deployment Requirements

The following table lists the deployment requirements for the connector.

Item	Requirement
Oracle Identity Manager	Oracle Identity Manager release 8.5.3 or later
Target system	The target system can be any one of the following: <ul style="list-style-type: none"> ■ RSA Authentication Manager 6.0 ■ RSA ACE Server 5.2 ■ RSA ACE Server 5.0
Target system host platforms	The target system host platform can be any one of the following: <ul style="list-style-type: none"> ■ Microsoft Windows 2000 Server for RSA ACE Server 5.0 and RSA ACE Server 5.2 ■ Microsoft Windows 2003 Server for RSA Authentication Manager 6.0 and RSA ACE Server 5.2 ■ Solaris 9 for RSA Authentication Manager 6.0 and RSA ACE Server 5.2 ■ Red Hat Advanced Server 2.1 for RSA Authentication Manager 6.0 and RSA ACE Server 5.2

Item	Requirement
Other systems	<ul style="list-style-type: none"> ▪ JDK The version of JDK on which Oracle Identity Manager server is running must be installed on the ACE server. ▪ RSA SecurID software token application See Also: The "Step 6: Configuring Reconciliation" section on page 2-12 for more information about the RSA SecurID software token
Remote manager node user account	<p>In Host mode, no credentials are required.</p> <p>In Remote mode, any remote node user account would suffice.</p> <p>Refer to the "Defining IT Resources" section on page 2-11 for details.</p>

Step 2: Configuring the Target System

Configuring the target system involves the following steps:

- [Setting Up the Remote Manager](#)
- [Configuring Strong Authentication Between Oracle Identity Manager and the Remote Manager](#)
- [Configuring SSL Client \(Oracle Identity Manager Server\) Authentication](#)

Setting Up the Remote Manager

To set up the remote manager on the RSA Authentication Manager server:

Note: For Solaris, you must create an ACE administrator as a preinstallation requirement for RSA Authentication Manager. This administrator is the file owner of the RSA Authentication Manager installation. Use this ACE administrator account to install the remote manager.

1. Create the `AuthManager` directory on the RSA Authentication Manager server.
2. From the installation media directory, copy the `remotePackage` directory into the `AuthManager` directory.

For Solaris 9

Log in to the Solaris server by using the user credentials of the RSA Authentication Manager File Owner that was created as a preinstallation requirement for RSA Authentication Manager. Then, create the directory into which you copy the `remotePackage` directory.

Note: If you copy files from Microsoft Windows to Solaris, all data transfer from the FTP client must be performed in binary mode. In addition, after copying files to the Solaris server, you must check the files for the ^M character pattern.

You must also perform required operations, such as `dos2unix`. As described earlier, copy all the files while using the ACE administrator credentials.

3. To update the class files, copy the `lib\xliACE.jar` file from the installation media directory to the `xl_remote\xlremote\JavaTasks` directory.

Note: From this point onward in the guide, the full path of the `remotePackage` directory on the RSA Authentication Manager server is referred to as `xl_remote`.

4. Update the library files as follows:

On Microsoft Windows:

Use a text editor to open the following file:

```
xl_remote\xlremote\remotemanager.bat
```

In this file, depending on the version of Authentication Manager that you are using, set one of the following as the first line of the file:

For ACE 5.0:

```
set PATH=authmgr_home\lib\ACE50;%PATH%
```

For ACE 5.2:

```
set PATH=authmgr_home\lib\ACE52;%PATH%
```

For RSA Authentication Manager 6.0:

```
set PATH=authmgr_home\lib\AuthMgr60;%PATH%
```

On Solaris 9:

For ACE 5.0:

Update the `xl_remote/xlremote/remotemanager.sh` file by adding the following lines:

```
AUTHMGR_HOME=authmgr_home
export AUTHMGR_HOME
ACE_INSTALL=ace_installation
export ACE_INSTALL
USR_ACE=$ACE_INSTALL/prog
export USR_ACE
VAR_ACE=$ACE_INSTALL/data
export VAR_ACE
DLC=$ACE_INSTALL/rdbms
export DLC
PROPATH=$ACE_INSTALL/prog/proapi/adbapi.pl:$ACE_INSTALL/prog/proapi/sdproapi.pl
:$ACE_INSTALL/prog/protrig:$ACE_INSTALL/prog
export PROPATH
```

Note: In the third line, *ace_installation* is the directory in which RSA ACE Server 5.0 is installed.

For RSA ACE 5.2, add the following line:

```
LD_LIBRARY_PATH=$ACE_INSTALL/prog:$AUTHMGR_HOME/lib/ACE52Sol
```

For RSA Authentication Manager 6.0, add the following line:

```
LD_LIBRARY_PATH=$ACE_INSTALL/prog:$AUTHMGR_HOME/lib/AuthMgr60Sol
```

Then, add the following line:

```
export LD_LIBRARY_PATH
```

5. For RSA ACE Server 5.0, copy the *ace_installation*\AuthManager\utils\toolkit\apidemon.exe file into the *xl_remote*\xlremote directory.

Here, *ace_installation* is the directory in which RSA ACE Server 5.0 is installed.

Configuring Strong Authentication Between Oracle Identity Manager and the Remote Manager

To configure strong authentication between Oracle Identity Manager and the remote manager, you must import the required certificate from the remote manager keystore to the Oracle Identity Manager server keystore as follows:

1. From the Oracle Identity Manager server, copy the *OIM_home*\xellerate\config\xlserver.cert file to the *AuthManager_home*\scripts\config directory on the RSA Authentication Manager server.
2. Use a text editor to open the *authmgr_home*\scripts\AuthMgrImportXLCert.bat file. Here, *authmgr_home* is the directory in which RSA Authentication Manager is installed.

In this file, set the following parameters:

```
set JAVA_HOME=jdk_home
set XL_REMOTE=xl_remote
```

For Solaris 9, set the following parameters in the *authmgr_home*/scripts/AuthMgrImportXLCert.sh file:

```
export XL_REMOTE=xl_remote
export JAVA_HOME=jdk_home
```

3. Run the AuthMgrImportXLCert.bat file.

For Solaris 9, run the AuthMgrImportXLCert.sh file.

Configuring SSL Client (Oracle Identity Manager Server) Authentication

To configure SSL client (Oracle Identity Manager server) authentication:

1. Open the *xl_remote*\xlremote\config\xlconfig.xml file.

2. In the <RMSecurity> section of this file, change the value of the <ClientAuth> element to true.

The following is a code block from the `xlconfig.xml` file:

```
<RMSecurity>
  <RMIOverSSL>true</RMIOverSSL>
  <SSLPort>12345</SSLPort>
  <SSLContextAlgorithm>TLS</SSLContextAlgorithm>
  <KeyManagerFactory>SunX509</KeyManagerFactory>
  <BindingPort>12346</BindingPort>
  <ServiceName>RManager</ServiceName>
  <LoggerConfigFilePath>log.conf</LoggerConfigFilePath>
  <ClientAuth>true</ClientAuth>
</RMSecurity>
```

Multiple Oracle Identity Manager Servers Communicating with a Single Remote Manager

If a setup involves more than one Oracle Identity Manager server communicating with a single remote manager, then you must address the considerations described in this section.

The `OIM_home\xellerate\config\xlserver.cert` certificate for any Oracle Identity Manager installation would have the same `dname` value. If you import this certificate from one Oracle Identity Manager installation into the target system remote manager keystore, then you cannot directly use the same certificate from another installation for the same purpose and in the same manner.

Therefore, if one Oracle Identity Manager installation is already configured with a particular remote manager and the same is needed for another Oracle Identity Manager installation, then you must first create a certificate with a different DN for the second installation before you can use this new certificate with the remote manager.

Enter the following commands in the specified order.

1. Generate a new key pair by entering the following command:

```
jdk_home\jre\bin\keytool -genkey -alias xell2 -keyalg DSA -keysize 1024 -dname
"CN=Customer1, OU=Customer, O=Customer, L=City, ST=NY, C=US" -validity 3650
-keypass xellerate -keystore OIM_home\xellerate\config\xlkeystore -storepass
xellerate -storetype jks -provider sun.security.provider.Sun
```

When you run this command, ensure that the `dname` value specified in the preceding command, is not the same as the default value of `dname`, for the existing certificates in the Oracle Identity Manager keystore:

```
OIM_home\xellerate\config\xlkeystore
```

The default value is as follows:

```
CN=Customer, OU=Customer, O=Customer, L=City, ST=NY, C=US
```

2. Create a certificate request by entering the following command:

```
jdk_home\jre\bin\keytool -certreq -alias xell2 -file
OIM_home\xellerate\config\xell1.csr -keypass xellerate -keystore
OIM_home\xellerate\config\xlkeystore -storepass xellerate -storetype jks
-provider sun.security.provider.Sun
```

3. Export the certificate to a file by entering the following command:

```
jdk_home\jre\bin\keytool -export -alias xell2 -file
OIM_home\xellerate\config\xlserver1.cert -keypass xellerate -keystore
OIM_home\xellerate\config\xlkeystore -storepass xellerate -storetype jks
-provider sun.security.provider.Sun
```

This command creates the following security certificate:

```
OIM_home\xellerate\config\xlserver1.cert
```

This is the certificate that you must use for configuration purposes.

4. Import the certificate into the remote manager keystore by entering the following command:

```
jdk_home\jre\bin\keytool -import -trustcacerts -alias xel2trusted -noprompt
-keystore OIM_home\xellerate\config\xlkeystore -file
OIM_home\xellerate\config\xlserver1.cert -storepass xellerate
```

For configuring strong authentication between another Oracle Identity Manager Server installation and the remote manager, use the `OIM_home\xellerate\config\xlserver1.cert` file instead of the `xlserver.cert` file.

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:

Security Applications\RSA Authentication Manager

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
lib\xliACE.jar	OIM_home\xellerate\JavaTasks OIM_home\xellerate\ScheduleTask
Directories and files in the remotePackage directory	OIM_home\xellerate\XLIntegrations\AuthManager\remotePackage Note: You do not need to copy this directory if you already performed the procedure described in the " Setting Up the Remote Manager " section on page 2-2.
Files in the resources directory	OIM_home\xellerate\connectorResources
Directories and files in the scripts directory	OIM_home\xellerate\XLIntegrations\AuthManager\scripts
Directories and files in the tests directory	OIM_home\xellerate\XLIntegrations\AuthManager\tests
Files in the xml directory	OIM_home\xellerate\XLIntegrations\AuthManager\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 performing the following procedures:

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

- [Changing to the Required Input Locale](#)
- [Clearing Content Related to Connector Resource Bundles from the Server Cache](#)
- [Enabling Logging](#)

Changing to the Required Input Locale

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

To set the required input locale:

Note: Depending on the operating system used, you may need to perform this procedure differently.

1. Open Control Panel.
2. Double-click **Regional Options**.
3. On the Input Locales tab of the Regional Options dialog box, add the input locale that you want to use and then switch to the input locale.

Clearing Content Related to Connector Resource Bundles from the Server Cache

Whenever you add a new resource bundle file in the `OIM_home\xellerate\connectorResources` directory or make a change in an existing resource bundle file, you must clear content related to connector resource bundles from the server cache.

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

1. In a command window, change to the `OIM_home\xellerate\bin` directory.
2. Enter one of the following commands:

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

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

- On Microsoft Windows:
`PurgeCache.bat ConnectorResourceBundle`
- On UNIX:
`PurgeCache.sh ConnectorResourceBundle`

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

`OIM_home\xellerate\config\xlConfig.xml`

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

Enabling Logging

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

- ALL
This level enables logging for all events.
- DEBUG
This level enables logging of information about fine-grained events that are useful for debugging.
- INFO
This level enables logging of informational messages that highlight the progress of the application at coarse-grained level.
- WARN
This level enables logging of information about potentially harmful situations.
- ERROR
This level enables logging of information about error events that may still allow the application to continue running.
- FATAL
This level enables logging of information about very severe error events that could cause the application to stop functioning.
- OFF
This level disables logging for all events.

The file in which you set the log level and the log file path depend on the application server that you use:

- **For JBoss Application Server**
To enable logging:
 1. In the `JBoss_home\server\default\conf\log4j.xml` file, locate the following lines:

```
<category name="XELLERATE">
  <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="XELLERATE">
  <priority value="INFO"/>
</category>
```

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

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

- **For IBM WebSphere:**

To enable logging:

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

```
log4j.logger.XELLERATE=log_level
```

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

For example:

```
log4j.logger.XELLERATE=INFO
```

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

```
WebSphere_home\AppServer\logs\server_name\startServer.log
```

- **For BEA WebLogic**

To enable logging:

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

```
log4j.logger.XELLERATE=log_level
```

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

For example:

```
log4j.logger.XELLERATE=INFO
```

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

```
WebLogic_home\user_projects\domains\domain_name\server_name\server_name.log
```

- **For OC4J**

To enable logging:

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

```
log4j.logger.XELLERATE=log_level
```

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

For example:

```
log4j.logger.XELLERATE=INFO
```

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

```
OC4J_home\opmn\logs\default_group~home~default_group~1.log
```

Step 5: Importing the Connector XML Files

To import the connector XML files into Oracle Identity Manager:

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 `xliAuthMgrUser_DM.xml` file, which is in the `OIM_home\xellerate\XLIIntegrations\AuthManager\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 ACE Remote Manager IT resource is displayed.
8. Specify values for the parameters of the ACE Remote Manager IT resource. Refer to the table in the "[IT Resource: ACE Remote Manager](#)" section on page 2-11 for information about the values to be specified.
9. Click **Next**. The Provide IT Resource Instance Data page for a new instance of the Remote Manager IT resource type is displayed.
10. Click **Skip** to specify that you do not want to define another IT resource. The Provide IT Resource Instance Data page for the ACE Server Remote IT resource is displayed.

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

11. Specify values for the parameters of the ACE Server Remote IT resource. Refer to the table in the "[IT Resource: ACE Server Remote](#)" section on page 2-11 for information about the values to be specified.
12. Click **Next**. The Provide IT Resource Instance Data page for a new instance of the ACE Server IT resource type is displayed.
13. 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.

14. Click **View Selections**.

The contents of the XML file are displayed on the Import page. You may see a cross-shaped icon along with some nodes. Remove these nodes by right-clicking each node and then selecting **Remove**.

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

16. Perform this procedure again to import the remaining connector XML files in the following order:

Note: The IT resources that you define while importing the `xliAuthMgrUser_DM.xml` file are the same as those that you would need to define when you import the `xliAuthMgrToken_DM.xml` file. Therefore, you do not need to define these IT resources again when you import the `xliAuthMgrToken_DM.xml` file.

```
xliAuthMgrToken_DM.xml
xliAuthMgrScheduledTask_DM.xml
```

These files are in the `OIM_home\xellerate\XLIIntegrations\AuthManager\xml` directory.

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

After you import the connector XML files, proceed to the ["Step 6: Configuring Reconciliation"](#) section on page 2-12.

Defining IT Resources

This section provides information about defining the following IT resources.

IT Resource: ACE Remote Manager

You must specify values for the `ACE Remote Manager` IT resource parameters listed in the following table.

Parameter	Description
<code>service name</code>	Remote manager service name <code>RManager</code>
<code>url</code>	Remote manager URL For example: <code>rmi://10.1.1.114:12346</code>

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

IT Resource: ACE Server Remote

You must specify values for the `ACE Server Remote` IT resource parameters listed in the following table.

Parameter	Description
<code>ACEAdminMode</code>	Admin mode through which the connector connects to RSA Authentication Manager for provisioning and reconciliation The value can be <code>Host</code> or <code>Remote</code> .

Parameter	Description
ACEAdminPassCode	Admin passcode, which is required only when the admin mode is Remote This value is encrypted after it is saved. Sample value: 123456 This value is encrypted after it is saved.
ACEAdminUserId	Admin user ID, which is required when the admin mode is either Remote or Host.
Target Locale: Country	Country code Default value: US Note: You must specify the value in uppercase.
Target Locale: Language	Language code You can select one of the following: <ul style="list-style-type: none"> ▪ English: en ▪ Japanese: jp ▪ French: fr Note: You must specify the value in lowercase.

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

Step 6: Configuring Reconciliation

Configuring reconciliation involves performing the following procedures:

- [Configuring Trusted Source Reconciliation](#)
- [Installing Software Tokens](#)
- [Creating Scheduled Tasks](#)
- [Enabling Reconciliation in Oracle Identity Manager Release 9.0.1](#)

Configuring Trusted Source Reconciliation

Note: Perform this step of the procedure only if you want to configure trusted source reconciliation. Only one connector can be configured for trusted source reconciliation. If you import the `xliAuthMgrTrusted.xml` file while you have another trusted source configured, then both connector reconciliations would stop working.

Refer to *Oracle Identity Manager Connector Framework Guide* for conceptual information about reconciliation configurations.

To configure trusted source reconciliation, you must first import the XML file for trusted source reconciliation as follows:

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 `xliAuthMgrTrusted.xml` file, which is in the `OIM_home\xellerate\XLIntegrations\AuthManager\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**.

Then, set the value of the `IsTrusted` reconciliation scheduled task attribute to `True` while performing the procedure described in the following section.

Installing Software Tokens

When you use this connector to run provisioning functions that are specific to software tokens, you must provide the required input parameters, such as the Token Code.

You can determine the values of these token-specific parameters only after the RSA Software Token application is installed on the Oracle Identity Manager server or on a user computer other than the Oracle Identity Manager server.

If you are using RSA SecurID software tokens, then:

1. Download RSA SecurID Token for Windows Desktops 3.0.5 from <http://www.rsasecurity.com/node.asp?id=1162>
2. Install the file on the Oracle Identity Manager server.
3. Copy the RSA SecurID software token file to an appropriate location on the Oracle Identity Manager server. The file to be copied is in the RSA Authentication Manager installation directory. The format of the directory path where you copy this file can be as follows:

```
target_dir_location\Token1File\
```

Note: While assigning a software token to an ACE user, you must specify the name and complete location of this file (in the `db_file_location\file_name.sdtid` format) in the Software Token File Name process form field.

4. Import the `.sdtid` file into the RSA SecurID Token software application as follows:
 - a. Click **Start**, and then select **Programs**.
 - b. Click **RSA SecurID Software Token**, and select the subcategory **RSA SecurID Software Token**.

The token screen is displayed.

- c. Click the **File** menu, and then select **Import Tokens**. In the dialog box that is displayed, select the `.sdtid` file mentioned in Step 3.

For example:

```
target_dir_location\Token1File\file_name.sdtid
```

- d. Select the token serial number, and click **Transfer Selected Tokens to Hard Drive**. The software token is imported.
- e. On the screen that is displayed, click **View** and then select **Advanced View**.
- f. On the screen that is displayed, click **View** and then select **Token View** to view the software token number.

Creating Scheduled Tasks

To create the reconciliation 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 task 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, set 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 to run the task 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 following table for information about the values to be specified.

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

Attribute	Description	Sample Value
IsTrusted	Specifies whether or not reconciliation must be performed in trusted mode	True or False
Server	Name of the IT resource	ACE Server Remote
Target System Recon - Resource Object name	Name of the target system resource object corresponding to the RSA Authentication Manager User	Auth Manager User
Target System Recon - Token Resource Object name	Name of the target system resource object corresponding to the RSA Authentication Manager User	Auth Manager Token
Trusted Source Recon - Resource Object name	Name of the trusted source Resource Object	Xellerate User

Attribute	Description	Sample Value
IsDeleteAllowed	Specifies whether or not the users who have been deleted in the target system should be deleted in Oracle Identity Manager	True or False

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.

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

Step 7: Compiling Adapters

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

- ACE ASSIGN TO GROUP
- ACE DELETE USER
- ACE CREATE USER
- ACE PrePop DefLogin
- ACE PrePop FirstName
- ACE PrePop GrpLogin
- ACE PrePop LastName
- ACE ASSIGN TOKEN
- ACE REMOVE TOKEN
- ACE DISABLE TOKEN
- ACE SET PIN
- ACE SET PIN TO NTC
- ACE TRACK LOST TOKEN
- ACE ENABLE TOKEN
- ACE TEST LOGIN

You must compile these adapters before you can use them to provision accounts on the target system.

To compile adapters by using the Adapter Manager form:

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

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

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

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

To view detailed information about an adapter:

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

Note: To compile one adapter at a time, use the Adapter Factory form. Refer to *Oracle Identity Manager Tools Reference Guide* for information about using the Adapter Factory and Adapter Manager forms.

Configuring the Connector for Multiple Installations of the Target System

Note: Perform this procedure only if you want to configure the connector for multiple installations of RSA Authentication Manager. Refer to *Oracle Identity Manager Design Console Guide* for detailed instructions on performing each step of this procedure.

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

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

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

2. Configure reconciliation for each target system installation. Refer to the "[Step 6: Configuring Reconciliation](#)" section on page 2-12 for instructions. Note that you need to modify only the attributes that are used to specify the IT resource and to

specify whether or not the target system installation is to be set up as a trusted source.

You can designate either a single or multiple installations of RSA Authentication Manager as the trusted source.

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

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

Testing and Troubleshooting

After you deploy the connector, you must test it to ensure that it functions as expected. This chapter discusses the following topics related to connector testing:

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

Running Connector Tests

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

To use the troubleshooting utility:

1. For RSA ACE Server 5.0:

On the target server, copy the `ace_installation\AuthManager\utils\toolkit\apidemon.exe` file to the `authmgr_home\tests\scripts` directory.

For all other versions of RSA ACE server, on the target server, add the following lines in the `authmgr_home\tests\scripts\runTestServer.bat` file:

```
set JAVA_HOME=jdk_home
set AUTHMGR_HOME=authmgr_home
set XL_REMOTE=xl_remote
```

For RSA ACE 5.0, add the following line:

```
set PATH=authmgr_home\lib\ACE50;%PATH%
```

For RSA ACE 5.2, add the following line:

```
set PATH=authmgr_home\lib\ACE52;%PATH%
```

For RSA Authentication Manager 6.0, add the following line:

```
set PATH=authmgr_home\lib\AuthMgr60;%PATH%
```

For Solaris 9, update the following file:

```
authmgr_home\tests\scripts\runTestServer.sh
```

In this file, change the values specified for the following variables:

```
export AUTHMGR_HOME=authmgr_home
export ACE_INSTALL=ace_install
export XL_REMOTE=xl_remote
```

2. Run the `runTestServer.bat` script.

The `runTestServer.bat` script runs an RMI server on the RSA Authentication Manager. Therefore, when you run this script, you must pass a port number as an argument as shown in the following example:

```
runTestServer 1001
```

For Solaris 9, run the `runTestServer.sh` script as follows:

```
./runTestServer.sh 1001
```

3. Use the information in the following table to change the default attribute values in the `config.properties` file.

This file is in the `authmgr_home\tests\config` directory.

Attribute	Description	Sample Values
Computer name	Computer name or IP address of the computer on which RSA Authentication Manager is running	10.1.1.114
port	Port at which the RMI server is listening	1001
passwd	RMI password This password must be the same as the one provided in the RMI server. It is the value of the <code>pw</code> property set in <code>authmgr_home\tests\scripts\runTestServer</code> . For example, <code>-Dpw=yourpassword</code>	yourpassword
adminMode	Administration mode for RSA Authentication Manager (host or remote)	Host
admin	User ID part of the remote administrator credentials for RSA Authentication Manager	jdoe
passcode	Passcode part of the remote administrator credentials for RSA Authentication Manager	1234
action	Action to be tested The value can be any one of the following: <ul style="list-style-type: none"> ■ addUser ■ deleteUser ■ assignToken ■ revokeToken ■ enableToken ■ disableToken ■ setPin ■ assignUsertogroup ■ removeUserfromgroup ■ settoNextTokenMode ■ trackLostToken ■ testLogin ■ issueSoftwareToken ■ deploySoftwareToken 	createUser
userID	User ID	jdoe

Attribute	Description	Sample Values
firstName	First name	Jane
lastName	Last name	Doe
group	Group name	John Doe and Sons
groupLogin	Group login	jdoeGrp
tokenSerialNumber	Token serial number	10473824
pin	Token PIN	1234
currentTokenCode	Token code	796563
number	Number of token codes to be generated	2
lifetime	Number of hours until emergency access mode expires	24
digits	Number of digits in the token code to be generated	6
loggerfile	Log file name with path	..\logs\Test_ACE.log
loggerlevel	Logger level: DEBUG, FATAL, WARN, INFO, or ERROR	DEBUG
RevokeFlag	Revoke token flag	1
fileName	Name of the software token file	C:\SoftToken\soft18.sdtid
key	Encryption key type	1
protect	Copy protection flag	0
method	Password usage and interpretation method	0
password	Password (maximum 8 characters)	welcome1
rangeMode	Criteria used to deploy AES type software tokens	2
endRange	Ending token serial number	The value must be the same as that in the tokenSerialNumber field
logFile	Name of the log file containing the status of the deployment operation	<i>filename.log</i>
overOption	Overwrites the output of a previously generated XML file	1
closeOption	Closing option of the XML file	Do not specify a value for this attribute

4. Update the following file on the Oracle Identity Manager server:

```
OIM_home\xellerate\XLIntegrations\AuthManager\tests\scripts\runTestClient.bat
```

In this file, add the following lines:

```
XELLERATE_HOME\xellerate=OIM_home\xellerate
JAVA_HOME=jdk_home
```

Run the `runTestClient.bat` file.

For Solaris:

Update the following file:

`OIM_home/xellerate/XLIntegrations/AuthManager/tests/scripts/runTestClient.sh`

Add the following lines:

`XELLERATE_HOME/xellerate=OIM_home/xellerate`
`JAVA_HOME=jdk_home`

Run the `runTestClient.sh` file.

After the script is run, the output is written to a log file. The log file is located in the following directory:

`OIM_home\xellerate\XLIntegrations\AuthManager\tests\logs`

The following are sample contents of this log file:

```
03 Dec 2004 16:52:45 INFO Constructor: ..\logs\Test_ACE.log DEBUG
03 Dec 2004 16:52:45 INFO You want to add a user!!
03 Dec 2004 16:52:45 INFO result-->ACE_USERCREATION_SUCCESS
```

Troubleshooting

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

Problem Description	Solution
Process definition: ACEUser Process task: Create User Returned Error Message: Access Denied. Check admin credentials. Returned Error Code: ACE_AUTHORIZED_ACCESS_FAIL	Check the administrator credentials specified in the IT resource definition.
Process definition: ACEUser Process task: Create User Returned Error Message: Unable to communicate with Authentication Server, RSA ACE Authentication Server not running Returned Error Code: ACE_AUTHORIZATION_ENGINE_FAIL	Start the service for RSA ACE Authentication Server.
Process definition: ACEUser Process task: Create User Returned Error Message: Failed to Connect to server DB, RSA ACE Broker not running Returned Error Code: ACE_SERVERDBCONNECT_FAIL	Start the service for RSA ACE Broker.

Problem Description	Solution
<p>Process definition: ACEUser Process task: Create User</p> <p>Returned Error Message User already exists in the DB</p> <p>Returned Error Code ACE_USERCREATION_ALREADYEXISTSINDB_FAIL</p>	<p>Check the user ID that you have specified. A user with this ID already exists in ACE.</p>
<p>Process definition: ACEUser Process task: Delete User</p> <p>Returned Error Message: Access Denied. Check admin credentials.</p> <p>Returned Error Code: ACE_AUTHORIZED_ACCESS_FAIL</p>	<p>Check the administrator credentials specified in the IT resource definition.</p>
<p>Process definition: ACEUser Process task: Delete User</p> <p>Returned Error Message: Unable to communicate with Authentication Server, RSA ACE Authentication Server not running</p> <p>Returned Error Code: ACE_AUTHORIZATION_ENGINE_FAIL</p>	<p>Start the service for RSA ACE Authentication Server.</p>
<p>Process definition: ACEUser Process task: Delete User</p> <p>Returned Error Message: Failed to connect to server DB, RSA ACE Broker not running</p> <p>Returned Error Code: ACE_SERVERDBCONNECT_FAIL</p>	<p>Start the service for RSA ACE Broker.</p>
<p>Process definition: ACEUser Process task: Delete User</p> <p>Returned Error Message: User is invalid</p> <p>Returned Error Code: ACE_USERDELETIONINVALIDUSER_FAIL</p>	<p>Check the user ID that you have specified. A user with this ID does not exist in ACE.</p>
<p>Process definition: ACEUser Process task: Delete User</p> <p>Returned Error Message: User is invalid</p> <p>Returned Error Code: ACE_USERDELETIONISADMIN_FAIL</p>	<p>Check the user ID that you have specified. The user with this ID is an administrator. If you still want to delete it, then you must first revoke the administrator role.</p>

Problem Description	Solution
<p>Process definition: ACEUser Process task: Assign users to ACE groups Returned Error Message: Access denied, check admin credentials Returned Error Code: ACE_AUTHORIZED_ACCESS_FAIL</p>	<p>Check the administrator credentials specified in the IT resource definition.</p>
<p>Process definition: ACEUser Process task: Assign users to ACE groups Returned Error Message: Unable to communicate with Authentication Server, RSA ACE Authentication Server not running Returned Error Code: ACE_AUTHORIZATION_ENGINE_FAIL</p>	<p>Start the service for RSA ACE Authentication Server.</p>
<p>Process definition: ACEUser Process task: Assign users to ACE groups Returned Error Message: Failed to Connect to server DB, RSA ACE Broker not running Returned Error Code: ACE_SERVERDBCONNECT_FAIL</p>	<p>Start the service for RSA ACE Broker.</p>
<p>Process definition: ACEUser Process task: Assign users to ACE groups Returned Error Message: User is invalid Returned Error Code: ACE_ADDTOGRP_ASSIGNGROUPSINVALIDUSER_FAIL</p>	<p>Check the user ID that you have specified. A user with this ID does not exist in ACE.</p>
<p>Process definition: ACEUser Process task: Assign users to ACE groups Returned Error Message: Group is invalid Returned Error Code: ACE_ADDTOGRP_ASSIGNGROUPSINVALIDGROUP_FAIL</p>	<p>Check the group name that you have specified. A group with this name does not exist in ACE.</p>
<p>Process definition: ACEUser Process task: Remove users from ACE groups Returned Error Message: Access Denied. Check admin credentials. Returned Error Code: ACE_AUTHORIZED_ACCESS_FAIL</p>	<p>Check the administrator credentials specified in the IT resource definition.</p>

Problem Description	Solution
<p>Process definition: ACEUser Process task: Remove users from ACE groups</p> <p>Returned Error Message: Unable to communicate with Authentication Server, RSA ACE Authentication Server not running</p> <p>Returned Error Code: ACE_AUTHORIZATION_ENGINE_FAIL</p>	<p>Start the service for RSA ACE Authentication Server.</p>
<p>Process definition: ACEUser Process task: Remove users from ACE groups</p> <p>Returned Error Message: Failed to connect to server DB, RSA ACE Broker not running</p> <p>Returned Error Code: ACE_SERVERDBCONNECT_FAIL</p>	<p>Start the service for RSA ACE Broker.</p>
<p>Process definition: ACEUser Process task: Remove users from ACE groups</p> <p>Returned Error Message: User is invalid</p> <p>Returned Error Code: ACE_REMFRMGRP_ASSIGNGROUPSINVALIDUSER_FAIL</p>	<p>Check the user ID that you have specified. A user with this ID does not exist in ACE.</p>
<p>Process definition: ACEUser Process task: Remove users from ACE groups</p> <p>Returned Error Message: Group is invalid</p> <p>Returned Error Code: ACE_REMFRMGRP_ASSIGNGROUPSINVALIDGROUP_FAIL</p>	<p>Check the group name that you have specified. A group with this name does not exist in ACE.</p>
<p>Process definition: ACE Token Process task: Assign SecurID tokens to users</p> <p>Returned Error Message: Access Denied. Check admin credentials.</p> <p>Returned Error Code: ACE_AUTHORIZED_ACCESS_FAIL</p>	<p>Check the administrator credentials specified in the IT resource definition.</p>
<p>Process definition: ACE Token Process task: Assign SecurID tokens to users</p> <p>Returned Error Message: Unable to communicate with Authentication Server, RSA ACE Authentication Server not running</p> <p>Returned Error Code: ACE_AUTHORIZATION_ENGINE_FAIL</p>	<p>Start the service for RSA ACE Authentication Server.</p>

Problem Description	Solution
<p>Process definition: ACE Token</p> <p>Process task: Assign SecurID tokens to users</p> <p>Returned Error Message:</p> <p>Failed to Connect to server DB, RSA ACE Broker not running</p> <p>Returned Error Code:</p> <p>ACE_SERVERDBCONNECT_FAIL</p>	<p>Start the service for RSA ACE Broker.</p>
<p>Process definition: ACE Token</p> <p>Process task: Assign SecurID tokens to users</p> <p>Returned Error Message:</p> <p>Token Serial Number is Invalid</p> <p>Returned Error Code:</p> <p>ACE_ASSIGN_TOKENSNOINVALID_FAIL</p>	<p>Check the token serial number that you have specified. A token with this serial number does not exist in ACE.</p>
<p>Process definition: ACE Token</p> <p>Process task: Assign SecurID tokens to users</p> <p>Returned Error Message:</p> <p>Token is already assigned</p> <p>Returned Error Code:</p> <p>ACE_TOKENALREADYASSIGNED_FAIL</p>	<p>Check the token serial number that you have specified. A token with this serial number is already assigned to another user in ACE.</p>
<p>Process definition: ACE Token</p> <p>Process task: Assign SecurID tokens to users</p> <p>Returned Error Message:</p> <p>Maximum number of users already assigned to this user</p> <p>Returned Error Code:</p> <p>ACE_TOKENMAXALREADYASSIGNED_FAIL</p>	<p>Check the user to whom you have assigned the token. The maximum number (three) of SecurID tokens has already been assigned to this user in ACE.</p>
<p>Process definition: ACE Token0</p> <p>Process task: Disable Token</p> <p>Returned Error Message:</p> <p>Access Denied. Check admin credentials.</p> <p>Returned Error Code:</p> <p>ACE_AUTHORIZED_ACCESS_FAIL</p>	<p>Check the administrator credentials specified in the IT resource definition.</p>
<p>Process definition: ACE Token</p> <p>Process task: Disable Token</p> <p>Returned Error Message:</p> <p>Unable to communicate with Authentication Server, RSA ACE Authentication Server not running</p> <p>Returned Error Code:</p> <p>ACE_AUTHORIZATION_ENGINE_FAIL</p>	<p>Start the service for RSA ACE Authentication Server.</p>

Problem Description	Solution
<p>Process definition: ACE Token</p> <p>Process task: Disable Token</p> <p>Returned Error Message:</p> <p>Failed to Connect to server DB, RSA ACE Broker not running</p> <p>Returned Error Code:</p> <p>ACE_SERVERDBCONNECT_FAIL</p>	<p>Start the service for RSA ACE Broker.</p>
<p>Process definition: ACE Token</p> <p>Process task: Disable Token</p> <p>Returned Error Message:</p> <p>Token Serial Number is Invalid</p> <p>Returned Error Code:</p> <p>ACE_DISABLE_TOKENSNOINVALID</p>	<p>Check the token serial number that you have specified. A token with this serial number does not exist in ACE.</p>
<p>Process definition: ACE Token</p> <p>Process task: Disable Token</p> <p>Returned Error Message:</p> <p>Token is not assigned</p> <p>Returned Error Code:</p> <p>ACE_DISABLE_TOKENNOTASSIGNED_FAIL</p>	<p>Check the token serial number that you have specified. A token with this serial number is not assigned to any user in ACE.</p>
<p>Process definition: ACE Token</p> <p>Process task: Enable Token</p> <p>Returned Error Message:</p> <p>Access Denied, check admin credentials</p> <p>Returned Error Code:</p> <p>ACE_AUTHORIZED_ACCESS_FAIL</p>	<p>Check the administrator credentials specified in the IT resource definition.</p>
<p>Process definition: ACE Token</p> <p>Process task: Enable Token</p> <p>Returned Error Message:</p> <p>Unable to communicate with Authentication Server, RSA ACE Authentication Server not running</p> <p>Returned Error Code:</p> <p>ACE_AUTHORIZATION_ENGINE_FAIL</p>	<p>Start the service for RSA ACE Authentication Server.</p>
<p>Process definition: ACE Token</p> <p>Process task: Enable Token</p> <p>Returned Error Message:</p> <p>Failed to Connect to server DB, RSA ACE Broker not running</p> <p>Returned Error Code:</p> <p>ACE_SERVERDBCONNECT_FAIL</p>	<p>Start the service for RSA ACE Broker.</p>

Problem Description	Solution
<p>Process definition: ACE Token Process task: Enable Token Returned Error Message: Token Serial Number is Invalid Returned Error Code: ACE_ENABLE_TOKENSNOINVALID_FAIL</p>	<p>Check the token serial number that you have specified. A token with this serial number does not exist in ACE.</p>
<p>Process definition: ACE Token Process task: Enable Token Returned Error Message: Token is not assigned Returned Error Code: ACE_ENABLE_TOKENNOTASSIGNED_FAIL</p>	<p>Check the token serial number that you have specified. A token with this serial number is not assigned to any user in ACE.</p>
<p>Process definition: ACE Token Process task: Set PIN Updated Returned Error Message: Access Denied, please check admin credentials Returned Error Code: ACE_AUTHORIZED_ACCESS_FAIL</p>	<p>Check the administrator credentials specified in the IT resource definition.</p>
<p>Process definition: ACE Token Process task: Set PIN Updated Returned Error Message: Unable to communicate with Authentication Server, RSA ACE Authentication Server not running Returned Error Code: ACE_AUTHORIZATION_ENGINE_FAIL</p>	<p>Start the service for RSA ACE Authentication Server.</p>
<p>Process definition: ACE Token Process task: Set PIN Updated Returned Error Message: Failed to Connect to server DB, RSA ACE Broker not running Returned Error Code: ACE_SERVERDBCONNECT_FAIL</p>	<p>Start the service for RSA ACE Broker.</p>
<p>Process definition: ACE Token Process task: Set PIN Updated Returned Error Message: Token Serial Number is Invalid Returned Error Code: ACE_SETPIN_TOKENSNOINVALID_FAIL</p>	<p>Check the token serial number that you have specified. A token with this serial number does not exist in ACE.</p>

Problem Description	Solution
<p>Process definition: ACE Token Process task: Set PIN Updated Returned Error Message: PINs Do Not Match Returned Error Code: ACE_PINMATCH_FAIL</p>	<p>Check the PIN that you have specified and then reentered. The PINs do not match.</p>
<p>Process definition: ACE Token Process task: Set PIN to NTC Updated Returned Error Message: Access Denied, please check admin credentials Returned Error Code: ACE_AUTHORIZED_ACCESS_FAIL</p>	<p>Check the administrator credentials specified in the IT resource definition.</p>
<p>Process definition: ACE Token Process task: Set PIN to NTC Updated Returned Error Message: Unable to communicate with Authentication Server, RSA ACE Authentication Server not running Returned Error Code: ACE_AUTHORIZATION_ENGINE_FAIL</p>	<p>Start the service for RSA ACE Authentication Server.</p>
<p>Process definition: ACE Token Process task: Set PIN to NTC Updated Returned Error Message: Failed to Connect to server DB, RSA ACE Broker not running Returned Error Code: ACE_SERVERDBCONNECT_FAIL</p>	<p>Start the service for RSA ACE Broker.</p>
<p>Process definition: ACE Token Process task: Set PIN to NTC Updated Returned Error Message: Token Serial Number is Invalid Returned Error Code: ACE_SETPINTONTC_TOKENSNOINVALID_FAIL</p>	<p>Check the token serial number that you have specified. A token with this serial number does not exist in ACE.</p>
<p>Process definition: ACE Token Process task: Set PIN to NTC Updated Returned Error Message: Current Token Code is Invalid Returned Error Code: ACE_CURRENTTOKENCODEINVALID_FAIL</p>	<p>Check the token code that you have specified. It is invalid. Ensure that the token code does not change until the API call reaches RSA Authentication Manager.</p>

Problem Description	Solution
<p>Process definition: ACE Token Process task: Set PIN to NTC Updated Returned Error Message: Token is not assigned Returned Error Code: ACE_SETPINTONTC_TOKENNOTASSIGNED_FAIL</p>	<p>Check the token serial number that you have specified. A token with this serial number is not assigned to any user in ACE.</p>
<p>Process definition: ACE Token Process task: Set Lost Updated Returned Error Message: Access Denied, check admin credentials Returned Error Code: ACE_AUTHORIZED_ACCESS_FAIL</p>	<p>Check the administrator credentials specified in the IT resource definition.</p>
<p>Process definition: ACE Token Process task: Set Lost Updated Returned Error Message: Unable to communicate with Authentication Server, RSA ACE Authentication Server not running Returned Error Code: ACE_AUTHORIZATION_ENGINE_FAIL</p>	<p>Start the service for RSA ACE Authentication Server.</p>
<p>Process definition: ACE Token Process task: Set Lost Updated Returned Error Message: Failed to Connect to server DB, RSA ACE Broker not running Returned Error Code: ACE_SERVERDBCONNECT_FAIL</p>	<p>Start the service for RSA ACE Broker.</p>
<p>Process definition: ACE Token Process task: Set Lost Updated Returned Error Message: Token Serial Number is Invalid Returned Error Code: ACE_TRACKLOST_TOKENSNOINVALID_FAIL</p>	<p>Check the token serial number that you have specified. A token with this serial number does not exist in ACE.</p>
<p>Process definition: ACE Token Process task: Test Login Updated Returned Error Message: Access Denied, please check admin credentials Returned Error Code: ACE_AUTHORIZED_ACCESS_FAIL</p>	<p>Check the administrator credentials specified in the IT resource definition.</p>

Problem Description	Solution
<p>Process definition: ACE Token Process task: Test Login Updated</p> <p>Returned Error Message: Unable to communicate with Authentication Server, RSA ACE Authentication Server not running</p> <p>Returned Error Code: ACE_AUTHORIZATION_ENGINE_FAIL</p>	<p>Start the service for RSA ACE Authentication Server.</p>
<p>Process definition: ACE Token Process task: Test Login Updated</p> <p>Returned Error Message: Failed to Connect to server DB, RSA ACE Broker not running</p> <p>Returned Error Code: ACE_SERVERDBCONNECT_FAIL</p>	<p>Start the service for RSA ACE Broker.</p>
<p>Process definition: ACE Token Process task: Test Login Updated</p> <p>Returned Error Message: Token Serial Number is Invalid</p> <p>Returned Error Code: ACE_TESTLOGININVALIDUSER_FAIL</p>	<p>Check the token serial number that you have specified. A token with this serial number does not exist in ACE.</p>
<p>Process definition: ACE Token Process task: Test Login Updated</p> <p>Returned Error Message: Current Token Code is Invalid</p> <p>Returned Error Code: ACE_CURRENTTOKENCODEMISSING_FAIL</p>	<p>Check if you have entered the token code.</p>
<p>Process definition: ACE Token Process task: Test Login Updated</p> <p>Returned Error Message: Passcode is invalid</p> <p>Returned Error Code: ACE_INVALID_PASSCODE</p>	<p>Check the token code that you have specified. It is invalid. Ensure that the token code does not change until the API call reaches the RSA Authentication Manager.</p>
<p>Process definition: ACE Token Process task: Revoke SecurID tokens from users</p> <p>Returned Error Message: Access Denied, please check admin credentials</p> <p>Returned Error Code: ACE_AUTHORIZED_ACCESS_FAIL</p>	<p>Check the administrator credentials specified in the IT resource definition.</p>

Problem Description	Solution
<p>Process definition: ACE Token Process task: Revoke SecurID tokens from users</p> <p>Returned Error Message: Unable to communicate with Authentication Server, RSA ACE Authentication Server not running</p> <p>Returned Error Code: ACE_AUTHORIZATION_ENGINE_FAIL</p>	<p>Start the service for RSA ACE Authentication Server.</p>
<p>Process definition: ACE Token Process task: Revoke SecurID tokens from users</p> <p>Returned Error Message: Failed to Connect to server DB, RSA ACE Broker not running</p> <p>Returned Error Code: ACE_SERVERDBCONNECT_FAIL</p>	<p>Start the service for RSA ACE Broker.</p>
<p>Process definition: ACE Token Process task: Revoke SecurID tokens from users</p> <p>Returned Error Message: Token Serial Number is Invalid</p> <p>Returned Error Code: ACE_UNASSIGN_TOKENSNOINVALID_FAIL</p>	<p>Check the token serial number that you have specified. A token with this serial number does not exist in ACE.</p>
<p>Process definition: ACE Token Process task: Revoke SecurID tokens from users</p> <p>Returned Error Message: Token is not assigned</p> <p>Returned Error Code: ACE_UNASSIGN_TOKENNOTASSIGNED_FAIL</p>	<p>Check the token serial number that you have specified. A token with this serial number is not assigned to any user in ACE.</p>

Known Issues

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

- RSA Authentication Manager APIs for extracting the group membership of user accounts are also exposed with the standard set, `Sd_ListGroupMembership`. Although this API is not used with the XL OOTB released connector, if you intend to extend the OOTB connector to use the same API, then keep in mind the following limitation:

If there is a delimiter character (for example, a comma) in the default shell, then it would result in incorrect output from the API (which is comma separated).

Therefore, you must make the required changes to handle such exceptional cases.

- While creating a user in RSA Authentication Manager, you must not enter special characters in the Default Login field. If you enter special characters in this field, then reconciliation would not work because Oracle Identity Manager does not support special characters in the User ID field.
- Some Asian languages use multibyte character sets. If the character limit for the fields in the target system is specified in bytes, then the number of Asian-language characters that you can enter in a particular field may be less than the number of English-language characters that you can enter in the same field. The following example illustrates this limitation:

Suppose you can enter 50 characters of English in the User Last Name field of the target system. If you were using the Japanese language and if the character limit for the target system fields were specified in bytes, then you would not be able to enter more than 25 characters in the same field.

- The connector does not support the use of security certificates that contain non-English characters.
- The following limitation applies to the use of the Japanese, Simplified Chinese, Traditional Chinese, Korean, and French languages:

RSA APIs do not support certain characters of the character sets of these languages. The provisioning or reconciliation operation fails if any of the field values submitted during the operation contains any one of the unsupported characters at the start of the field value. However, the operation does not fail if unsupported characters appear at any place other than the start of the field value

Refer to your RSA documentation for information about the characters of these languages that are not supported.

Attribute Mappings Between Oracle Identity Manager and RSA Authentication Manager

The following table discusses attribute mappings between Oracle Identity Manager and RSA Authentication Manager.

Oracle Identity Manager Attribute	RSA Authentication Manager Attribute	Description
Group Login	chLogin	Login ID of this user when logged in as a member of a specific group If a group login ID is not defined, the user's regular default login is used.
Group Name	chName	Name of the group
Token Serial Number	chSerialNum	Serial number
Pin	Pin	Sets a PIN for a specified token that is assigned to a user
Set Pin	bCreatePIN	Specifies whether or not users can create their own PINs The value can be <code>True</code> or <code>False</code> .
Curent Token Code	Not mapped to an attribute in RSA Authentication Manager DB	Token code that is displayed on the token device There is no designated field in the target to store it.
Set PIN to NTC	iNextTCodeStatus	Specifies that the next autogenerated token code must be taken as the PIN for the user
Lifetime (Hours)	datePWExpires	Date on which the password expires
Number of Digits	iNumDigits	Number of digits returned in the password generated for emergency access after a token is set to the <code>LOST</code> state
Set Lost	bLost	Specifies whether or not the token device is lost The default is <code>NOT LOST</code> .
Type of Token	iType	Token type The token can be a hardware token device or a software token authenticator.
Copy Protection Flag	bSoftID_CopyProtected	Specifies whether or not copy protection is enabled The value can be <code>True</code> or <code>False</code> .

Oracle Identity Manager Attribute	RSA Authentication Manager Attribute	Description
Password	chOTPPasswordsSB	Password to be provided by the RSA Authentication Manager administrator in order to access an RSA SecurID software token XML file If there is no password associated with the file, then an empty string can be passed.
Password Usage and Interpretation Method	method	Password usage and interpretation method The value can be any one of the following: <ul style="list-style-type: none"> ■ 0: No password ■ 1: Static password ■ 2: Default login ■ 3: Default login appended to static password
Software Token File Name	Not mapped to an attribute in RSA Authentication Manager DB	Software token file name path There is no designated field in the target to store/represent it.
Encryption Key Type	iTokenVersion	Version of the token algorithm
Type of Algorithm	iSeedSizeType	Specifies the algorithm type The value can be any one of the following: <ul style="list-style-type: none"> ■ SID: For 64-bit encryption ■ AES: For 128-bit encryption
First Name	chFirstName	First name
Last Name	chLastName	Last name
Default Login	chDefaultLogin	Default login ID

Index

A

Adapter Factory form, 2-16
Adapter Manager form, 2-16
adapters, compiling, 2-15
Administrative and User Console, 2-10, 2-12
attributes mappings, A-1

C

changing input locale, 2-7
clearing server cache, 2-7
compiling adapters, 2-15
configuring
 connector for multiple installations of the target system, 2-16
 Oracle Identity Manager server, 2-7
 reconciliation, 2-12
 trusted source reconciliation, 2-12
connector files and directories
 copying, 2-6
 description, 1-5
 destination directories, 2-6
 installation directory, 1-5, 2-6
connector testing, 3-1
connector version number, determining, 1-7
connector XML files
 See XML files
creating scheduled tasks, 2-12

D

defining
 IT resources, 2-11
 scheduled tasks, 2-12
deployment requirements, 2-1
Design Console, 2-14
determining version number of connector, 1-7

E

enabling logging, 2-8
errors, 3-4

F

files and directories of the connector

See connector files and directories
functionality supported, 1-1
functions available, 1-1

G

globalization features, 1-4

I

importing connector XML files, 2-10
input locale, changing, 2-7
issues, 4-1
IT resources defining, 2-11

L

limitations, 4-1
logging enabling, 2-8

M

mapping between attributes of target system and Oracle Identity Manager, A-1
multilanguage support, 1-4

O

Oracle Identity Manager Administrative and User Console, 2-10, 2-12
Oracle Identity Manager Design Console, 2-14
Oracle Identity Manager Release 9.0.1, 2-15
Oracle Identity Manager server, configuring, 2-7

P

problems, 3-4
process tasks, 1-1
provisioning
 fields, 1-5
 functions, 1-1
 module, 1-5

R

reconciliation
 configuring, 2-12

- enabling in Oracle Identity Manager Release
 - 9.0.1, 2-15
- functions, 1-1
- module, 1-4
- trusted source, 2-12

requirements for deploying connector, 2-1

S

- scheduled tasks
 - creating, 2-12
 - defining, 2-14
- server cache, clearing, 2-7
- software tokens, installing, 2-13
- supported
 - languages, 1-4
 - Oracle Identity Manager versions, 2-1
 - target systems, 2-1

T

- target system, multiple installations, 2-16
- target systems supported, 2-1
- testing the connector, 3-1
- troubleshooting, 3-4
- trusted source reconciliation, 2-12

U

- user attribute mappings, A-1

V

- version number of connector, determining, 1-7

X

- XML files, importing, 2-10