Oracle® Identity Manager

Connector Guide for RSA Authentication Manager

Release 9.0.4

E10168-01

May 2007

ORACLE®

Oracle Identity Manager Connector Guide for RSA Authentication Manager, Release 9.0.4

E10168-01

Primary Authors: Debapriya Datta, Shiladitya Guha

Contributing Authors: Don Gosselin, Lyju Vadassery

Contents

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 Connector Pack Release 9.0.4 documentation library, visit Oracle Technology Network at

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

Conventions

The following text conventions are used in this document.

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that 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 software and documentation for the RSA Authentication Manager connector in release 9.0.4 of the Oracle Identity Manager connector pack.

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

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

- Software Updates

  These include updates made to the connector software.

- Documentation-Specific Updates

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

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

Software Updates

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

New Target System Identity Attributes for Reconciliation and Provisioning

In the "Reconciliation Module" section on page 1-1 and the "Provisioning Module" section on page 1-2, the Key Value and Data Value identity attributes have been added.

New Supported Provisioning Functions

In the "Supported Functionality" section on page 1-3, the following provisioning functions have been added:

- Add key-data pairs to user extension data
- Update key-data pairs in user extension data
- Delete key-data pairs from user extension data

In the "Compiling Adapters" section on page 3-5, the following adapters have been added for these functions:

- ACE ADD USER EXTENSION DATA TO USER

- ACE UPDATE USER EXTENSION DATA FOR USER
- ACE DEL USER EXTENSION DATA TO USER

Changes in List of Supported Target Systems

From this release onward:

- RSA ACE Server 5.0 has been desupported. All information pertaining to this target system has been removed from the guide.
- RSA Authentication Manager 6.1 is supported. Information pertaining to this target system has been added at the required places in the guide.

Partial Reconciliation

The `CustomReconQuery` parameter has been added to the IT resource definition. You can use this parameter to customize the query that the reconciliation module uses to determine the records to be retrieved from the target system. The `CustomReconQuery` parameter is explained in the following sections:

- IT Resource: ACE Server Remote on page 2-12
- Partial Reconciliation on page 3-1
- Testing Partial Reconciliation on page 4-5

Changes to the List of Supported Target System Host Platforms

In the "Step 1: Verifying Deployment Requirements" section on page 2-1, the information on supported target system host platform has been modified. This release of the connector also supports Microsoft Windows 2000 Server for RSA ACE Server 5.2 and Solaris 9 for RSA Authentication Manager 6.0. This release of the connector does not support Solaris 8 for RSA Ace Server 5.2 as a target system host platform.

Enabling Logging

By following the instructions in the "Enabling Logging" section on page 2-8, you can configure the generation of log information that is specific to the target system.

New Adapters

In the "Compiling Adapters" section on page 3-5, the following adapters have been added:

- `ACE ADD USER EXTENSION DATA TO USER`
- `ACE UPDATE USER EXTENSION DATA FOR USER`
- `ACE DEL USER EXTENSION DATA TO USER`

Changes in the Known Issues

In the Known Issues list in Chapter 5, the following point has been removed:

"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."

Documentation-Specific Updates

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

- In the "Supported Functionality" section on page 1-3, the "Update User ID" provisioning function has been removed from the list of supported functions.
- In the "Files and Directories That Comprise the Connector" section on page 1-6, the row for the following files has been removed:

  `remotePackage/lib/AuthMgr60Sol/libACEUser.so`

- Instructions in the "Determining the Release Number of the Connector" section on page 1-9 have been revised.
- In the "Step 1: Verifying Deployment Requirements" section on page 2-1, the content related to RSA Authentication Manager versions 5.0 and 6.0 hosted on Solaris has been removed.
- The "Setting Up the Remote Manager as a Trusted Source for Reconciliation" has been renamed to "Configuring Strong Authentication Between the Remote Manager and the Oracle Identity Manager Server" and moved on page 2-5.
- The content related to RSA Authentication Manager versions 5.0 and 6.0 hosted on Solaris has been removed from the following sections:
  - Step 1: Verifying Deployment Requirements on page 2-1
  - Files and Directories That Comprise the Connector on page 1-6
  - Setting Up the Remote Manager on page 2-2
  - Running Connector Tests on page 4-1
- Some of the content from the Chapter 2 of the earlier release of this guide has been moved to Chapter 3.

1

About the Connector

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

Note: At some places in this guide, RSA Authentication Manager has been referred to as the *target system.*

Reconciliation Module

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

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

Reconciled Resource Object Fields

The following target system fields are reconciled:

- Default Login
- First Name

- Last Name
- Group Name
- Group Login
- Key Value
- Data Value
- Token Serial Number
- Type of Token

Reconciled Xellerate User Fields

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

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

Reconciliation of 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

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

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

For this target system, provisioning is divided into the following types:

- RSA Authentication Manager User Provisioning

- RSA Authentication Manager Token Provisioning

RSA Authentication Manager User Provisioning

In this provisioning type, you can specify values for the following fields:

- Default Login
- First Name
- Last Name
- Group Login
- Group Name
- Key Value
- Data Value

RSA Authentication Manager Token Provisioning

In this provisioning type, you can specify values for the following fields:

- 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

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	Assigns a token to a user While assigning a software token to the user, the **Type of Algorithm** field must be filled in the process form. ■ If `SID` is selected in the Type of Algorithm field, then values must be specified for the following fields in the process form: - 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 `.sdtid`. - Encryption Key Type - Copy Protection Flag - Password Usage and Interpretation Method - Password - Encryption Key Type - Password Usage and Interpretation Method - Password **Note:** If these combinations do not matter, then you can accept the default options. ■ If `AES` is specified in the Type of Algorithm field, then: 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 `.sdtid`. The Password field is optional. The following fields can be ignored: - 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	Assigns a user to a group You must ensure that the following prerequisites are met before you use this function: ▪ Valid groups exist in RSA Authentication Manager. ▪ The required lookup codes (corresponding to valid group names) are added in the `UD_Lookup.ACE_Group` lookup definition. For example, for a group called `Managers` defined in ACE DB, the following entry must be added as the lookup code: **Code Key:** `Managers` **Decode:** `Managers` **Lang:** `en` **Country:** `US`
Remove Users from RSA Authentication Manager Groups	Provisioning	Removes a user from a group You must ensure that the following prerequisites are met before you use this function: ▪ 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	Verifies the login for a new user to whom a token has been assigned You must ensure that the following prerequisites are met before you use this function: ▪ 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). For software token types, you must enter the passcode, instead of the token code, in the Current Token Code field in the process form. The passcode can be viewed by using the software token application, which is installed on the Oracle Identity Manager server. **See Also:** The "Installing Software Tokens" section on page 3-6 for more information
Add key-data pairs to user extension data	Provisioning	Adds a key-data pair to user extension data Before you use this function, you must ensure that the following prerequisite is met: User must not have user extension data with the same key before provisioning to the target system.

Function	Type	Description
Update key-data pairs in user extension data	Provisioning	Update a key-data pair in user extension data Before you use this function, you must ensure that the following prerequisites are met: ■ User must have user extension data with the same key value before provision to the target system. ■ You must not change the key value. Only the data value needs to be change before provisioning.
Delete key-data pairs from user extension data	Provisioning	Delete a key-data pair user extension data Before you use this function, you must ensure that the following prerequisite is met: User must have user extension data with the same key value before provisioning to the target system.

See Also: Appendix A, "Attribute Mappings Between Oracle Identity Manager and RSA Authentication Manager"

Multilanguage Support

The connector supports the following languages:

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

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

Files and Directories That Comprise the Connector

The files and directories that comprise this connector are 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.

File in the Installation Media Directory	Description
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/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/AuthMgr61/ACEUser.dll	This file contains the shared library that is required to support provisioning in RSA Authentication Manager 6.1, on Microsoft Windows.
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.

File in the Installation Media Directory	Description
tests/config/config.properties	This file contains the properties required by the RMI client for running test calls from the Oracle Identity Manager server.
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: ■ 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: ■ 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

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

Before Deployment

To determine the release number of a connector before you deploy it:

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

   `Security Applications/RSA Authentication Manager/lib`

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.

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

After Deployment

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

See Also: *Oracle Identity Manager Design Console Guide*

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

2

Deploying the Connector

Deploying the connector involves the following steps:

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

Step 1: Verifying Deployment Requirements

The following table lists the deployment requirements for the connector.

Item	Requirement
Oracle Identity Manager	Oracle Identity Manager release 8.5.3 or later
Target system	The target system can be any one of the following: ■ RSA Authentication Manager 6.1 ■ RSA Authentication Manager 6.0 ■ RSA ACE Server 5.2
Target system host platforms	The target system host platform can be any one of the following: ■ Microsoft Windows 2003 Server for RSA Authentication Manager 6.0, RSA Authentication Manager 6.1, and RSA ACE Server 5.2 ■ Microsoft Windows 2000 Server for RSA ACE Server 5.2 ■ Solaris 9 for RSA Authentication Manager 6.0 and RSA ACE Server 5.2
Other systems	■ 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 "Installing Software Tokens" section on page 3-6 for more information about the RSA SecurID software token

Item	Requirement
Remote manager node user account	In Host mode, no credentials are required. In Remote mode, any remote node user account would suffice. Refer to the "Defining IT Resources" section on page 2-12 for details. If the specified type of user account is not used, then the following error message is displayed when connector operations are attempted: `Access denied, check administrator credentials`

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 5.2:

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

   For RSA Authentication Manager 6.0:

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

   For RSA Authentication Manager 6.1:

   ```
   set PATH=authmgr_home/lib/AuthMgr61;%PATH%
   ```

   On Solaris 9:

   For RSA ACE 5.2, add the following lines:

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

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:

```
XL_REMOTE=xl_remote
export XL_REMOTE
JAVA_HOME=jdk_home
export JAVA_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\/ellerate/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.

Configuring Strong Authentication Between the Remote Manager and the Oracle Identity Manager Server

To set up the remote manager as a trusted source for Oracle Identity Manager:

1. On the RSA Authentication Manager server, copy the *xl_remote*/xlremote/config/xlserver.cert file into the following directory:

OIM_home/xellerate/XLIntegrations/AuthManager/scripts/config

2. Use a text editor to open the following file:

OIM_home/xellerate/XLIntegrations/AuthManager/scripts/AuthMgrImportRMCert.bat

In this file, edit the following lines to specify the path to the JDK and Oracle Identity Manager installation directories:

set JAVA_HOME = *jdk_home*
set XELLERATE_HOME = *OIM_home*

For Oracle Identity Manager installed on Solaris 8 or Red Hat Advanced Server 2.1, open the following file in a text editor:

OIM_home/xellerate/XLIntegrations/AuthManager/scripts/AuthMgrImportRMCert.sh

In this file, edit the following lines to specify the path to the JDK and Oracle Identity Manager installation directories:

```
JAVA_HOME = jdk_home
export JAVA_HOME
XELLERATE_HOME = OIM_home
export XELLERATE_HOME
```

3. Run the `AuthMgrImportRMCert.bat` file.

   For Oracle Identity Manager installed on Solaris 8 or Red Hat Linux AS 2.1, run the `AuthMgrImportRMCert.sh` 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 1-6 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

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

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.

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

Clearing Content Related to Connector Resource Bundles from the Server Cache

While performing the instructions described in the "Step 3: Copying the Connector Files" section on page 2-6, you copy files from the `resources` directory on the installation media into the *`OIM_home`*`/xellerate/connectorResources` directory. Whenever you add a new resource bundle in the `connectorResources` directory or make a change in an existing resource bundle, you must clear content related to connector resource bundles from the server cache.

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

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

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

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

2. Enter one of the following commands:

   - On Microsoft Windows:

     ```
     PurgeCache.bat ConnectorResourceBundle
     ```

   - On UNIX:

     ```
     PurgeCache.sh ConnectorResourceBundle
     ```

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

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

OIM_home`/xellerate/config/xlConfig.xml`

Enabling Logging

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

- `ALL`

  This level enables logging for all events.

- `DEBUG`

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

- `INFO`

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

- `WARN`

  This level enables logging of information about potentially harmful situations.

- `ERROR`

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

- `FATAL`

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

- `OFF`

  This level disables logging for all events.

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

- **BEA WebLogic**

  To enable logging:

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

     ```
     log4j.logger.XELLERATE=log_level
     log4j.logger.XL_INTG.RSA_ACE=log_level
     ```

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

     For example:

```
log4j.logger.XELLERATE=INFO
log4j.logger.XL_INTG.RSA_ACE=INFO
```

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

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

- **IBM WebSphere**

  To enable logging:

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

     ```
     log4j.logger.XELLERATE=log_level
     log4j.logger.XL_INTG.RSA_ACE=log_level
     ```

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

     For example:

     ```
     log4j.logger.XELLERATE=INFO
     log4j.logger.XL_INTG.RSA_ACE=INFO
     ```

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

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

- **JBoss Application Server**

  To enable logging:

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

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

     <category name="XL_INTG.RSA_ACE">
        <priority value="log_level"/>
     </category>
     ```

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

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

     <category name="XL_INTG.RSA_ACE">
        <priority value="INFO"/>
     </category>
     ```

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

  JBoss_home/server/default/log/server.log

- **OC4J**

  To enable logging:

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

```
log4j.logger.XELLERATE=log_level
log4j.logger.XL_INTG.RSA_ACE=log_level
```

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

   For example:

   ```
   log4j.logger.XELLERATE=INFO
   log4j.logger.XL_INTG.RSA_ACE=INFO
   ```

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

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

Enabling Logging for the Remote Manager

To enable logging for the Remote Manager:

1. Add the following lines in the *RemoteManager_home*/xlremote/config/log.properties file:

   ```
   log4j.rootLogger=WARN,stdout,logfile
   log4j.appender.logfile.File=log_file_path_and_name
   log4j.logger.XELLERATE=log_level
   log4j.logger.XL_INTG.RSA_ACE=log_level
   ```

2. In these lines, replace *log_file_path_and_name* with the full path and name of the log file and *log_level* with the log level that you want to set.

   For example:

   ```
   log4j.rootLogger=WARN,stdout,logfile
   log4j.appender.logfile.File=c:/rm_rsa_ace_connector.log
   log4j.logger.XELLERATE=INFO
   log4j.logger.XL_INTG.RSA_ACE=INFO
   ```

After you enable logging, log information is written to the file that you specify as the value of the the log4j.appender.logfile.File attribute.

Step 5: Importing the Connector XML Files

As mentioned in the "Files and Directories That Comprise the Connector" section on page 1-6, the connector XML file contains definitions of the components of the connector. By importing the connector XML file, you create these components in Oracle Identity Manager.

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/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 **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 2-12 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 2-12 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. These nodes represent Oracle Identity Manager entities that are redundant. Before you import the connector XML file, you must remove these entities by right-clicking each node and then selecting **Remove**.
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/XLIntegrations/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 next chapter.

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
`service name`	Remote manager service name `RManager`
`url`	Remote manager URL For example: `rmi://10.1.1.114:12346`

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
`ACEAdminMode`	Admin mode through which the connector connects to RSA Authentication Manager for provisioning and reconciliation The value can be `Host` or `Remote`.
`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: ■ English: `en` ■ Japanese: `jp` ■ French: `fr` **Note:** You must specify the value in lowercase.

Parameter	Description
`CustomReconQuery`	Query condition on which reconciliation must be based If you specify a query condition for this parameter, then the target system records are searched based on the query condition. If you want to reconcile all the target system records, then do not specify a value for this parameter. The query can be composed with the AND (&) and OR (|) logical operators. Sample value: `First Name=John&Last Name=Doe` For more information about this parameter, refer to the "Partial Reconciliation" section on page 3-1.

After you specify values for these IT resource parameters, proceed to Step 12 of the procedure to import connector XML files.

3

Configuring the Connector

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

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

- Configuring Reconciliation
- Configuring Provisioning
- Configuring the Connector for Multiple Installations of the Target System

> **Note:** This chapter provides both conceptual and procedural information about customizing the connector. It is recommended that you read the conceptual information before you perform the procedures.

Configuring Reconciliation

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

- Partial Reconciliation
- Configuring Trusted Source Reconciliation
- Configuring the Reconciliation Scheduled Tasks

Partial Reconciliation

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

For this connector, you create a filter by specifying values for the `CustomReconQuery` IT resource parameter while performing the procedure described in the "Defining IT Resources" section on page 2-12.

The following are the attributes that you can use to build the query condition:

- User ID
- First Name
- Last Name
- Group

The following are sample query conditions:

- `First Name=John&Last Name=Doe`

  With this query condition, records of users whose first name is `John` and last name is `Doe` are reconciled.

- `First Name=John&Last Name=Doe|Group=contractors`

  With this query condition, records of users who meet either of the following conditions are reconciled:

  – The user's first name is `John` or last name is `Doe`.

  – The user belongs to the `contractors` group.

If you do not specify values for the `CustomReconQuery` parameter, then all the records in the target system are compared with existing Oracle Identity Manager records during reconciliation.

The following are guidelines to be followed while specifying a value for the `CustomReconQuery` parameter:

- You must not include unnecessary blank spaces between operators and values in the query condition.

  A query condition with spaces separating values and operators would yield different results as compared to a query condition that does not contain spaces between values and operators. For example, the output of the following query conditions would be different:

  ```
  First Name=John&Last Name=Doe
  ```

  ```
  First Name= John&Last Name= Doe
  ```

  In the second query condition, the reconciliation engine would look for first name and last name values that contain a space at the start.

- You must not include special characters other than the equal sign (=), ampersand (&), and vertical bar (|) in the query condition.

  Note: An exception is thrown if you include special characters other than the equal sign (=), ampersand (&), and vertical bar (|).

You specify a value for the `CustomReconQuery` parameter while performing the procedure described in the "Defining IT Resources" section on page 2-12.

Configuring Trusted Source Reconciliation

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

Manager. If you designate the target system as a **target resource**, then only modified user accounts are reconciled in Oracle Identity Manager.

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

Configuring trusted source reconciliation involves the following steps:

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

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

2. Set the `IsTrusted` scheduled task attribute to `True`. You specify a value for this attribute while configuring the user reconciliation scheduled task, which is described later in this guide.

To import the XML file for trusted source reconciliation:

1. Open the Oracle Identity Manager Administrative and User Console.
2. Click the **Deployment Management** link on the left navigation bar.
3. Click the **Import** link under Deployment Management. A dialog box for 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**.

After you import the XML file for trusted source reconciliation, you must set the value of the `IsTrusted` reconciliation scheduled task attribute to `True`. This procedure is described in the "Configuring the Reconciliation Scheduled Tasks" section on page 3-3.

Configuring the Reconciliation Scheduled Tasks

When you perform the procedure described in the "Step 5: Importing the Connector XML Files" section on page 2-10, the scheduled tasks for lookup fields and user reconciliations are automatically created in Oracle Identity Manager. To configure the 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`
`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.

Stopping Reconciliation

Suppose the User Reconciliation Scheduled Task for the connector is running and user records are being reconciled. If you want to stop the reconciliation process:

1. Perform Steps 1 through 4 of the procedure to configure reconciliation scheduled tasks.
2. Select the **Stop Execution** check box in the task scheduler.
3. Click **Save**.

Configuring Provisioning

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

This section discusses the following topics related to configuring provisioning:

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

- Compiling Adapters
- Installing Software Tokens

Compiling Adapters

Adapters are used to implement provisioning functions. 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
- ACE ADD USER EXTENSION DATA TO USER
- ACE UPDATE USER EXTENSION DATA FOR USER
- ACE DEL USER EXTENSION DATA TO USER

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

To compile adapters by using the Adapter Manager form:

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

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

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

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

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

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

To view detailed information about an adapter:

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

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.

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.

You may want to configure the connector for multiple installations of RSA Authentication Manager. The following example illustrates this requirement:

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

To meet the requirement posed by such a scenario, you must configure the connector for multiple installations of RSA Authentication Manager.

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

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

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

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

2. Configure reconciliation for each target system installation. Refer to the "Configuring Reconciliation" section on page 3-1 for instructions. Note that you 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.

4

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 testing 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 testing utility:

1. For all supported 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 5.2, 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 RSA Authentication Manager 6.1, add the following line:

   ```
   set PATH=authmgr_home/lib/AuthMgr61;%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:

   ```
   AUTHMGR_HOME=authmgr_home
   export AUTHMGR_HOME
   ACE_INSTALL=ace_installation_home
   export ACE_INSTALL
   XL_REMOTE=xl_remote
   export 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. The properties file must be converted to ASCII format for multilanguage support using the native2ascii tool on command console as follows:

   ```
   native2ascii src.properties dest.properties
   ```

   For example:

   ```
   native2ascii config1.properties config.properties
   ```

4. 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 pw property set in *authmgr_home*/tests/scripts/ runTestServer. For example, -Dpw=yourpassword	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

Attribute	Description	Sample Values
action	Action to be tested The value can be any one of the following: ■ addUser ■ deleteUser ■ assignToken ■ revokeToken ■ enableToken ■ disableToken ■ setPin ■ assignUsertogroup ■ removeUserfromgroup ■ settoNextTokenMode ■ trackLostToken ■ testLogin ■ issueSoftwareToken ■ deploySoftwareToken ■ addUserExtensionData ■ updateUserExtensionData ■ removeUserExtensionData ■ aceRecon	createUser
userID	User ID	jdoe
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

Attribute	Description	Sample Values
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	*filename*.log
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
userExtensionData_KeyValue	Key value for user extension data	EMPID EMAIL
userExtensionData_DataValue	Data value for user extension data	416451 test123@nabd.com
customQuery	Custom reconciliation query to run partial user reconciliation	First Name=Test &Group=Group1

5. 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
```

Testing Partial Reconciliation

To test query-based reconciliation, you can specify the following types of query conditions as values for the the `CustomReconQuery` parameter:

- Simple query with user attributes

  Value assigned to the `CustomReconQuery` parameter: `last name = Doe`

  The users with last name `Doe` are reconciled.

- Query consisting of '&', '|', and multiple groups
  - Value assigned to the `CustomReconQuery` parameter: `first name=John&last name=Doe&group=a,b,c`

    The users with first name `John`, last name `Doe`, and who also belong to all the groups `a`, `b`, and `c` are reconciled.
  - Value assigned to the `CustomReconQuery` parameter: `first name = John|last name = Doe|group=a,b,c`

    The users with first name as `John`, last name as `Doe`, and who belong to the groups `a`, `b`, and `c` are reconciled.

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 administrator 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:** Could not communicate with authentication server, RSA ACE authentication server is 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:** Could not connect to RSA ACE database, RSA ACE Broker is not running **Returned Error Code:** `ACE_SERVERDBCONNECT_FAIL`	Start the service for RSA ACE Broker.

Problem Description	Solution
Process definition: ACEUser Process task: Create User **Returned Error Message** User already exists in database **Returned Error Code** `ACE_USERCREATION_ALREADYEXISTSINDB_FAIL`	Check the user ID that you have specified. A user with this ID already exists in ACE.
Process definition: ACEUser Process task: Delete User **Returned Error Message:** Access denied, check administrator credentials **Returned Error Code:** `ACE_AUTHORIZED_ACCESS_FAIL`	Check the administrator credentials specified in the IT resource definition.
Process definition: ACEUser Process task: Delete User **Returned Error Message:** Could not 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: Delete User **Returned Error Message:** Could not connect to RSA ACE database, RSA ACE Broker is not running **Returned Error Code:** `ACE_SERVERDBCONNECT_FAIL`	Start the service for RSA ACE Broker.
Process definition: ACEUser Process task: Delete User **Returned Error Message:** User does not exist **Returned Error Code:** `ACE_USERDELETIONINVALIDUSER_FAIL`	Check the user ID that you have specified. A user with this ID does not exist in ACE.
Process definition: ACEUser Process task: Delete User **Returned Error Message:** User is an administrator **Returned Error Code:** `ACE_USERDELETIONISADMIN_FAIL`	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.

Problem Description	Solution
Process definition: ACEUser Process task: Assign users to ACE groups **Returned Error Message:** Access denied, check administrator credentials **Returned Error Code:** ACE_AUTHORIZED_ACCESS_FAIL	Check the administrator credentials specified in the IT resource definition.
Process definition: ACEUser Process task: Assign users to ACE groups **Returned Error Message:** Could not communicate with authentication server, RSA ACE authentication server is not running **Returned Error Code:** ACE_AUTHORIZATION_ENGINE_FAIL	Start the service for RSA ACE Authentication Server.
Process definition: ACEUser Process task: Assign users to ACE groups **Returned Error Message:** Could not connect to RSA ACE database, RSA ACE Broker is not running **Returned Error Code:** ACE_SERVERDBCONNECT_FAIL	Start the service for RSA ACE Broker.
Process definition: ACEUser Process task: Assign users to ACE groups **Returned Error Message:** User does not exist **Returned Error Code:** ACE_ADDTOGRP_ASSIGNGROUPSINVALIDUSER_FAIL	Check the user ID that you have specified. A user with this ID does not exist in ACE.
Process definition: ACEUser Process task: Assign users to ACE groups **Returned Error Message:** Group does not exist **Returned Error Code:** ACE_ADDTOGRP_ASSIGNGROUPSINVALIDGROUP_FAIL	Check the group name that you have specified. A group with this name does not exist in ACE.
Process definition: ACEUser Process task: Remove users from ACE groups **Returned Error Message:** Access denied, check administrator credentials **Returned Error Code:** ACE_AUTHORIZED_ACCESS_FAIL	Check the administrator credentials specified in the IT resource definition.

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

Problem Description	Solution
Process definition: ACE Token Process task: Assign SecurID tokens to users **Returned Error Message:** Could not connect to RSA ACE database, RSA ACE Broker is not running **Returned Error Code:** ACE_SERVERDBCONNECT_FAIL	Start the service for RSA ACE Broker.
Process definition: ACE Token Process task: Assign SecurID tokens to users **Returned Error Message:** Token Serial Number is invalid **Returned Error Code:** ACE_ASSIGN_TOKENSNOINVALID_FAIL	Check the token serial number that you have specified. A token with this serial number does not exist in ACE.
Process definition: ACE Token Process task: Assign SecurID tokens to users **Returned Error Message:** Token is already assigned **Returned Error Code:** ACE_TOKENALREADYASSIGNED_FAIL	Check the token serial number that you have specified. A token with this serial number is already assigned to another user in ACE.
Process definition: ACE Token Process task: Assign SecurID tokens to users **Returned Error Message:** Maximum number of tokens already assigned to this user **Returned Error Code:** ACE_TOKENMAXALREADYASSIGNED_FAIL	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.
Process definition: ACE Token0 Process task: Disable Token **Returned Error Message:** Access denied, check administrator credentials **Returned Error Code:** ACE_AUTHORIZED_ACCESS_FAIL	Check the administrator credentials specified in the IT resource definition.
Process definition: ACE Token Process task: Disable Token **Returned Error Message:** Could not communicate with authentication server, RSA ACE authentication server is not running **Returned Error Code:** ACE_AUTHORIZATION_ENGINE_FAIL	Start the service for RSA ACE Authentication Server.

Problem Description	Solution
Process definition: ACE Token Process task: Disable Token **Returned Error Message:** Could not connect to RSA ACE database, RSA ACE Broker is not running **Returned Error Code:** ACE_SERVERDBCONNECT_FAIL	Start the service for RSA ACE Broker.
Process definition: ACE Token Process task: Disable Token **Returned Error Message:** Token Serial Number is invalid **Returned Error Code:** ACE_DISABLE_TOKENSNOINVALID	Check the token serial number that you have specified. A token with this serial number does not exist in ACE.
Process definition: ACE Token Process task: Disable Token **Returned Error Message:** Token is not assigned **Returned Error Code:** ACE_DISABLE_TOKENNOTASSIGNED_FAIL	Check the token serial number that you have specified. A token with this serial number is not assigned to any user in ACE.
Process definition: ACE Token Process task: Enable Token **Returned Error Message:** Access denied, check administrator credentials **Returned Error Code:** ACE_AUTHORIZED_ACCESS_FAIL	Check the administrator credentials specified in the IT resource definition.
Process definition: ACE Token Process task: Enable Token **Returned Error Message:** Could not communicate with authentication server, RSA ACE authentication server is not running **Returned Error Code:** ACE_AUTHORIZATION_ENGINE_FAIL	Start the service for RSA ACE Authentication Server.
Process definition: ACE Token Process task: Enable Token **Returned Error Message:** Could not connect to RSA ACE database, RSA ACE Broker is not running **Returned Error Code:** ACE_SERVERDBCONNECT_FAIL	Start the service for RSA ACE Broker.

Problem Description	Solution
Process definition: ACE Token Process task: Enable Token **Returned Error Message:** Token Serial Number is invalid **Returned Error Code:** ACE_ENABLE_TOKENSNOINVALID_FAIL	Check the token serial number that you have specified. A token with this serial number does not exist in ACE.
Process definition: ACE Token Process task: Enable Token **Returned Error Message:** Token is not assigned **Returned Error Code:** ACE_ENABLE_TOKENNOTASSIGNED_FAIL	Check the token serial number that you have specified. A token with this serial number is not assigned to any user in ACE.
Process definition: ACE Token Process task: Set PIN Updated **Returned Error Message:** Access denied, check administrator credentials **Returned Error Code:** ACE_AUTHORIZED_ACCESS_FAIL	Check the administrator credentials specified in the IT resource definition.
Process definition: ACE Token Process task: Set PIN Updated **Returned Error Message:** Could not communicate with authentication server, RSA ACE authentication server is not running **Returned Error Code:** ACE_AUTHORIZATION_ENGINE_FAIL	Start the service for RSA ACE Authentication Server.
Process definition: ACE Token Process task: Set PIN Updated **Returned Error Message:** Could not connect to RSA ACE database, RSA ACE Broker is not running **Returned Error Code:** ACE_SERVERDBCONNECT_FAIL	Start the service for RSA ACE Broker.
Process definition: ACE Token Process task: Set PIN Updated **Returned Error Message:** Token Serial Number is invalid **Returned Error Code:** ACE_SETPIN_TOKENSNOINVALID_FAIL	Check the token serial number that you have specified. A token with this serial number does not exist in ACE.

Problem Description	Solution
Process definition: ACE Token Process task: Set PIN Updated **Returned Error Message:** PINS do not match **Returned Error Code:** ACE_PINMATCH_FAIL	Check the PIN that you have specified and then reentered. The PINs do not match.
Process definition: ACE Token Process task: Set PIN to NTC Updated **Returned Error Message:** Access denied, check administrator credentials **Returned Error Code:** ACE_AUTHORIZED_ACCESS_FAIL	Check the administrator credentials specified in the IT resource definition.
Process definition: ACE Token Process task: Set PIN to NTC Updated **Returned Error Message:** Could not communicate with authentication server, RSA ACE authentication server is not running **Returned Error Code:** ACE_AUTHORIZATION_ENGINE_FAIL	Start the service for RSA ACE Authentication Server.
Process definition: ACE Token Process task: Set PIN to NTC Updated **Returned Error Message:** Could not connect to RSA ACE database, RSA ACE Broker is not running **Returned Error Code:** ACE_SERVERDBCONNECT_FAIL	Start the service for RSA ACE Broker.
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	Check the token serial number that you have specified. A token with this serial number does not exist in ACE.
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	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.

Problem Description	Solution
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	Check the token serial number that you have specified. A token with this serial number is not assigned to any user in ACE.
Process definition: ACE Token Process task: Set Lost Updated **Returned Error Message:** Access denied, check administrator credentials **Returned Error Code:** ACE_AUTHORIZED_ACCESS_FAIL	Check the administrator credentials specified in the IT resource definition.
Process definition: ACE Token Process task: Set Lost Updated **Returned Error Message:** Could not communicate with authentication server, RSA ACE authentication server is not running **Returned Error Code:** ACE_AUTHORIZATION_ENGINE_FAIL	Start the service for RSA ACE Authentication Server.
Process definition: ACE Token Process task: Set Lost Updated **Returned Error Message:** Could not connect to RSA ACE database, RSA ACE Broker is not running **Returned Error Code:** ACE_SERVERDBCONNECT_FAIL	Start the service for RSA ACE Broker.
Process definition: ACE Token Process task: Set Lost Updated **Returned Error Message:** Token Serial Number is invalid **Returned Error Code:** ACE_TRACKLOST_TOKENSNOINVALID_FAIL	Check the token serial number that you have specified. A token with this serial number does not exist in ACE.
Process definition: ACE Token Process task: Test Login Updated **Returned Error Message:** Access denied, check administrator credentials **Returned Error Code:** ACE_AUTHORIZED_ACCESS_FAIL	Check the administrator credentials specified in the IT resource definition.

Problem Description	Solution
Process definition: ACE Token Process task: Test Login Updated **Returned Error Message:** Could not communicate with authentication server, RSA ACE authentication server is not running **Returned Error Code:** ACE_AUTHORIZATION_ENGINE_FAIL	Start the service for RSA ACE Authentication Server.
Process definition: ACE Token Process task: Test Login Updated **Returned Error Message:** Could not connect to RSA ACE database, RSA ACE Broker is not running **Returned Error Code:** ACE_SERVERDBCONNECT_FAIL	Start the service for RSA ACE Broker.
Process definition: ACE Token Process task: Test Login Updated **Returned Error Message:** User does not exist **Returned Error Code:** ACE_TESTLOGININVALIDUSER_FAIL	Check the token serial number that you have specified. A token with this serial number does not exist in ACE.
Process definition: ACE Token Process task: Test Login Updated **Returned Error Message:** Current token code is missing **Returned Error Code:** ACE_CURRENTTOKENCODEMISSING_FAIL	Check if you have entered the token code.
Process definition: ACE Token Process task: Test Login Updated **Returned Error Message:** Passcode is invalid **Returned Error Code:** ACE_INVALID_PASSCODE	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.
Process definition: ACE Token Process task: Revoke SecurID tokens from users **Returned Error Message:** Access denied, check administrator credentials **Returned Error Code:** ACE_AUTHORIZED_ACCESS_FAIL	Check the administrator credentials specified in the IT resource definition.

Problem Description	Solution
Process definition: ACE Token Process task: Revoke SecurID tokens from users **Returned Error Message:** Could not 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: ACE Token Process task: Revoke SecurID tokens from users **Returned Error Message:** Could not connect to RSA ACE database, RSA ACE Broker is not running **Returned Error Code:** `ACE_SERVERDBCONNECT_FAIL`	Start the service for RSA ACE Broker.
Process definition: ACE Token Process task: Revoke SecurID tokens from users **Returned Error Message:** Token Serial Number is invalid **Returned Error Code:** `ACE_RESCIND_TOKENSNOINVALID_FAIL`	Check the token serial number that you have specified. A token with this serial number does not exist in ACE.
Process definition: ACE Token Process task: Revoke SecurID tokens from users **Returned Error Message:** Token is not assigned **Returned Error Code:** `ACE_UNASSIGN_TOKENNOTASSIGNED_FAIL`	Check the token serial number that you have specified. A token with this serial number is not assigned to any user in ACE.

5

Known Issues

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

- 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.
- The connector does not support the use of security certificates that contain non-English characters.
- 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 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.

  See Also: For more information about the characters not supported in provisioning and reconciliation, refer to the metalink note 421232.1 in the metalink Web site at https://metalink.oracle.com.

A

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 `True` or `False`.
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 `LOST` state
Set Lost	bLost	Specifies whether or not the token device is lost The default is `NOT LOST`.
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 `True` or `False`.

Oracle Identity Manager Attribute	RSA Authentication Manager Attribute	Description
Password	chOTPasswordsSB	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: ■ 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: ■ 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

S

T

U

X