Oracle® Identity Manager

Connector Guide for RSA Authentication Manager

Release 9.0.1

B31132-01

June 2006

ORACLE®

Oracle Identity Manager Connector Guide for RSA Authentication Manager, Release 9.0.1

B31132-01

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

Audience

This guide is intended for users who want to deploy the Oracle Identity Manager connector for 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 set:

- *Oracle Identity Manager Release Notes*
- *Oracle Identity Manager Installation and Upgrade Guide for JBoss*
- *Oracle Identity Manager Installation and Upgrade Guide for WebLogic*
- *Oracle Identity Manager Installation and Upgrade Guide for WebSphere*
- *Oracle Identity Manager Administrative and User Console Guide*
- *Oracle Identity Manager Administrative and User Console Customization Guide*
- *Oracle Identity Manager Design Console Guide*
- *Oracle Identity Manager Tools Reference Guide*
- *Oracle Identity Manager Audit Report Developer Guide*
- *Oracle Identity Manager Best Practices Guide*
- *Oracle Identity Manager Connector Framework Guide*
- Connector guides for various third-party applications

Documentation Updates

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

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

Conventions

The following text conventions are used in this document.

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

1

About the Connector

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

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

This chapter contains the following sections:

Supported Functionality

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 provisioned 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 the following fields must be filled in the process form: **Software Token File Name:** This is 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 the following fields must be filled in the process form: **Software Token File Name:** This is 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 Authorization Manager groups	Provisioning	Assigns user to a group You must ensure that the following prerequisites are met before you use this function: ■ Valid groups must exist in RSA Authentication Manager. ■ Correct lookup codes (corresponding to valid group names) must be 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 Authorization Manager groups	Provisioning	Removes user from a group You must ensure that the following prerequisites are met before you use this function: ■ Valid groups must exist in ACE DB. ■ This function can be run only after the Assign Users to ACE/Server 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 logging in for a created user with a token assigned You must ensure that the following prerequisites are met before you use this function: ■ An agent host must be in the database. ■ The user (for whom the Test Login function is to be implemented) must be enabled on this agent host. ■ After this is done, the RSA Authentication Manager must be 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 on 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:** "Software Tokens" on page 2-9 for more information
Update User ID	Provisioning	Updates the configuration of a user according to a change in the User Id attribute

Reconciliation Module

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

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

Provisioning Module

This section discusses the fields that are provisioned.

RSA Authentication Manager User Provisioning

The following fields are provisioned:

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

RSA Authentication Manager Token Provisioning

The following fields are provisioned:

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

Files and Directories That Comprise the Connector

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

`Security Applications\RSA Authentication Manager\RSA Authentication Manager Rev 4.1.0.zip`

These files and directories are listed in the following table.

File Name with Path	Description
`xml\xliAuthMgrUser_DM.xml`	This file contains 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
`xml\xliAuthMgrToken_DM.xml`	This file contains 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\xliAuthMgrScheduledTask_DM.xml`	This file contains the components required for reconciliation.
`lib\xliACE.jar`	This file contains the Java classes that are required for provisioning in RSA Authentication Manager.
`remotePackage\lib\ACE50\ACEUser.dll`	This file contains the shared library that is required to support provisioning in RSA Authentication Manager.
`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\AuthMgr60\ACEUser.dll`	This file contains the shared library that is required to support provisioning in RSA Authentication Manager 6.0.
`remotePackage\lib\ACE52Sol\libACEUser.so`	This file contains the shared library that is required to support provisioning in RSA Authentication Manager.
`remotePackage\lib\AuthMgr60Sol\libACEUser.so`	This file contains the shared library that is required to support provisioning in RSA Authentication Manager 6.0 installed on Solaris.
`remotePackage\scripts\AuthMgrImportXLCert.bat`	This file contains the script for importing the required security certificate in the remote manager keystore (`.xlkeystore`).
`remotePackage\scripts\AuthMgrImportXLCert.sh`	This file contains the script for importing the required security certificate in the remote manager keystore (`.xlkeystore`) on Solaris.

File Name with Path	Description
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\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.
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.
scripts\AuthMgrImportXLCert.bat	This file contains the script for importing the required security certificate in the Oracle Identity Manager server keystore (.xlkeystore).
scripts\AuthMgrImportXLCert.sh	This file contains the script for importing the required security certificate in the Oracle Identity Manager server keystore (.xlkeystore) on Solaris.
tests\config\config.properties	This file contains the properties required by the RMI client for running test calls from the Oracle Identity Manager server.
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\scripts\runTestClient.bat	This file contains the script required to run the RMI client for running test calls from the Oracle Identity Manager Server.
docs\B31132_01.pdf docs\html	These are PDF and HTML versions of this guide, which provides instructions to deploy the connector.

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

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

2

Deploying the Connector

Deploying the connector involves the following steps:

Step 1: Verifying Deployment Requirements

The following table lists the deployment requirements for the connector.

Item	Requirement
Oracle Identity Manager	Oracle Identity Manager release 8.5.3 or later
Target system	The target system can be any one of the following: ■ RSA Authentication Manager 6.0.2 ■ RSA Authentication Manager 6.0 ■ RSA ACE Server 5.2 ■ RSA ACE Server 5.0
Target system host platforms	The target system host platform can be any one of the following: ■ Microsoft Windows 2000 Server for RSA ACE Server 5.0 and RSA ACE Server 5.2 ■ Microsoft Windows 2003 Server for RSA Authentication Manager 6.0.2, RSA Authentication Manager 6.0, and RSA ACE Server 5.2 ■ Solaris 9 for RSA Authentication Manager 6.0.2, RSA Authentication Manager 6.0, and RSA ACE Server 5.2
Infrastructure requirements	JDK The version of JDK on which Oracle Identity Manager server is running must be installed on the ACE server.
External applications	RSA SecurID software token application **See Also:** The "Step 5: Configuring Reconciliation" section on page 2-8 for more information about this requirement.

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

You must set up a remote manager on the RSA Authentication Manager server in a directory such as *XL_REMOTE*.

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 the same ACE admin credentials to install the remote manager.

---

1. Create the *authmgr_home* directory in the RSA Authentication Manager. From the installation media directory, copy the `remotePackage` directory into the *authmgr_home* 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 *authmgr_home* 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 admin credentials.

   ---

2. To update the class files, copy the *authmgr_home*`\lib\xliACE.jar` file to the *XL_REMOTE*`\xlremote\JavaTasks` directory.
3. Update the library files by editing the following file:

   XL_REMOTE`\xlremote\remotemanager.bat`

   In this file, depending on your system environment, set one of the following parameters as the first line of the file:

   For ACE 5.2:

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

   For ACE 5.0:

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

For RSA Authentication Manager 6.0:

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

For Solaris 9:

Update the file by adding the following lines:

XL_REMOTE/xlremote/remotemanager.sh

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

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

For RSA Authentication Manager 6.0 and 6.0.2, add the following line:

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

For RSA ACE 5.2, add the following line:

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

Then, add the following line:

```
export LD_LIBRARY_PATH
```

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

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

Configuring Strong Authentication Between Oracle Identity Manager and the Remote Manager

To configure strong authentication between Oracle Identity Manager and the remote manager:

1. From the Oracle Identity Manager server, copy the *xellerate_home*\xellerate\config\xlserver.cert file to the *authmgr_home*\scripts\config\ directory in the RSA Authentication Manager.
2. Open the following file:

   authmgr_home\scripts\AuthMgrImportXLCert.bat

In this file, set the following parameters:

```
set JAVA_HOME=JDK_HOME
set XL_REMOTE=XL_REMOTE
```

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

```
export XL_REMOTE=XL_REMOTE
export JAVA_HOME=JDK_HOME
```

3. Run the AuthMgrImportXLCert.bat file.

   For Solaris 9, run the AuthMgrImportXLCert.sh file.

Configuring SSL Client (Oracle Identity Manager Server) Authentication

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

1. Open the *XL_REMOTE*\xlremote\config\xlconfig.xml file.
2. In the <RMSecurity> section of this file, change the value of the <ClientAuth> element to true.

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

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

Multiple Oracle Identity Manager Servers Communicating with a Single Remote Manager

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

The *xellerate_home*\xellerate\config\xlserver.cert certificate for any Oracle Identity Manager installation would have the same dname value. If you have imported 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 remote manager.

Enter the following commands in the specified order. You must provide the corresponding values of *JDK_HOME* and *xellerate_home* in these commands.

1. First 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 xellerate_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 same as the default value of dname, for the existing certificates in the Oracle Identity Manager keystore:

```
xellerate_home\xellerate\config\.xlkeystore
```

The default value is as follows:

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

2. Second command

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

3. Third command

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

This command creates the following security certificate:

```
xellerate_home\xellerate\config\xlserver1.cert
```

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

4. Fourth command

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

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

Step 3: Copying the Connector Files

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

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

```
Collaboration and Messaging Applications\IBM Lotus Notes Domino\IBM
Lotus Notes Domino Rev 1.0.0.zip
```

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

File in the Installation Media Directory	Destination Directory

The following files in the `xml` directory:
`xliAuthMgrUser_DM.xml`
`xliAuthMgrToken_DM.xml`
`xliAuthMgrScheduledTask_DM.xml`
	xellerate_home`\xellerate\XLIntegrations\AuthManager\xml`

`lib\xliACE.jar`	*xellerate_home*`\xellerate\JavaTasks` *xellerate_home*`\xellerate\ScheduleTask`

For Microsoft Windows, copy the following file:
`scripts\AuthMgrImportXLCert.bat`
 	
For Solaris, copy the following file:
`scripts\AuthMgrImportXLCert.sh`
	xellerate_home`\xellerate\XLIntegrations\AuthManager\scripts`

The following contents of the `tests` directory:
`config\config.properties`
`lib\xliACETestClient.jar`
`scripts\runTestClient.bat`
	xellerate_home`\xellerate\XLIntegrations\AuthManager\tests`

The following contents of the `docs` directory:
`B31132_01.pdf`
`html`
	xellerate_home`\xellerate\XLIntegrations\AuthManager\docs`

Note: Instructions to copy the contents of the `remotePackage` installation media directory have been covered in the "Step 2: Configuring the Target System" section on page 2-2.

Step 4: Importing the Connector XML Files

To import the connector XML files into Oracle Identity Manager:

1. Open the Oracle Identity Manager Administrative and User Console.
2. Click the **Deployment Management** link on the left navigation bar.
3. Click the **Import** link under Deployment Management. A dialog box for locating files is displayed.
4. Locate and open the `xliAuthMgrUser_DM.xml` file, which is in the *xellerate_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 2-7 for information about the values to be specified.

9. Click **Next.** The Provide IT Resource Instance Data page for a new instance of the `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 2-8 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. You must remove these nodes. To do this, right-click each such node and then select **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:

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

    These files are in the *xellerate_home*`\xellerate\XLIntegrations\AuthManager\xml` directory.

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

Defining IT Resources

This section provides information about the IT resources defined in the `xliAuthMgrUser_DM.xml` file.

IT Resource: ACE Remote Manager

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

Parameter Name	Parameter Description
`service name`	`RManager`
`url`	`rmi://10.1.1.114:12346`

IT Resource: ACE Server - Remote

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

Parameter Name	Parameter Description
`ACEAdminMode`	`Host`
`ACEAdminPassCode`	`123456` This value is encrypted after it is saved.
`ACEAdminUserId`	`jdoe`

Step 5: Configuring Reconciliation

You can use the RSA Authentication Manager connector to perform reconciliation in trusted mode. The prerequisite steps to implement this are as follows:

1. Open the Resource Object form.
2. Search for the Xellerate User.
3. On the Object Reconciliation tab, add reconciliation fields as required. Add all those reconciliation fields that would be needed to provide input for the mandatory fields in the Xellerate User form, such as User Login and First Name. Although the Password field is a mandatory field, it can be ignored.
4. Open the Process Definition form.
5. Search for the Xellerate User.
6. On the Reconciliation Field Mappings tab, add the reconciliation field mappings as required. Ensure that mappings to all mandatory fields of the User Defined process form are present.
7. Open the Reconciliation Rules form.
8. Create a new rule for Object Xellerate User, with a rule element as required.
9. After you create the rule, select the Active check box.

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

1. In RSA Authentication Manager, copy the *XL_REMOTE*`\xlremote\config\xlserver.cert` file to the following directory:

   xellerate_home`\xellerate\XLIntegrations\AuthManager\scripts\config\`

2. Open the following file in a text editor:

   xellerate_home`\xellerate\XLIntegrations\AuthManager\scripts\AuthMgrImportRMCert.bat`

   In this file, configure the following entries:

   ```
   set JAVA_HOME = jdk_home
   set XELLERATE_HOME = xellerate_home
   ```

   For Oracle Identity Manager installed on Solaris 9 or Red Hat Linux AS 2.1, open the following file in a text editor:

   xellerate_home`/xellerate/XLIntegrations/AuthManager/scripts/AuthMgrImportRMCert.sh`

In this file, configure the following entries:

```
export JAVA_HOME = jdk_home
export XELLERATE_HOME = xellerate_home
```

3. Run the `AuthMgrImportRMCert.bat` file.

   For Oracle Identity Manager installed on Solaris 9 or Red Hat Linux AS 2.1, run the `AuthMgrImportRMCert.sh` file.

Software Tokens

Using this connector, for running provisioning functions that are specific to software tokens, you would need to provide the required input parameters, such as the Token Code.

You can determine all such token-specific parameters only after RSA Software Token application is installed on the Oracle Identity Manager server desktop or user desktop, other than the Oracle Identity Manager server.

If you are using RSA SecurID software tokens, then:

1. Download the 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. To import the `.sdtid` file into the RSA SecurID Token software application:
   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.

Defining Scheduled Tasks

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

1. Open the Oracle Identity Design Console.
2. Expand the **Xellerate Administration** folder.
3. Select **Task Scheduler.**
4. Click **Find**. The details of the predefined scheduled tasks are displayed on two different tabs.
5. Enter a number in the **Max Retries** field. This number represents the number of times Oracle Identity Manager attempts to complete the task before assigning the `ERROR` status to the task.
6. Ensure that the **Disabled** and **Stop Execution** check boxes are cleared.
7. In the Start region, double-click the **Start Time** field. From the date-time editor that is displayed, set the date and time at which you want the task to run.
8. Specify that you want the task to run on a recurring basis by selecting the **Recurring Intervals** option.
9. In the Interval region, set the following schedule parameters:
   - To set the task to run on a recurring basis, select the **Daily**, **Weekly**, **Recurring Intervals**, **Monthly**, or **Yearly** option.

     If you select the **Recurring Intervals** option, then you must almost specify the time interval at which you want to run the task on a recurring basis.
   - To set the task to run only once, select the **Once** option.
10. Provide values for the user-configurable attributes of the scheduled task. Refer to the 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 Name	Description	Sample Value
`Server`	Name of the IT Resource	`ACE Server Remote`
`Target System Recon - Resource Object name`	Name of the target system resource object	`Auth Manager User`
`Target System Recon - Token Resource Object name`	Name of the target system resource object	`Auth Manager Token`
`Trusted Source Recon - Resource Object name`	Name of the trusted source Resource Object	`Xellerate User`

11. Click **Save**. The scheduled task is created. The `INACTIVE` status is displayed in the **Status** field, because the task is not currently running. The task is run at the date and time that you set in Step 7.
12. Repeat Step 5 through 11 to define the second scheduled task.

Step 6: Compiling Adapters

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

- ACE ASSIGN TO GROUP
- ACE DELETE USER
- ACEASSIGNTOGROUP
- 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

To compile adapters by using the Adapter Manager form:

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

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

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

3. Click **Start.** Oracle Identity Manager compiles the adapters that you specify.

To view detailed information about an adapter:

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

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

Security Considerations

You must address the following security considerations before you start using the connector:

- There must be a trust relationship between Oracle Identity Manager and the remote manager. To achieve this, you must import the required certificate from the remote manager keystore to the Oracle Identity Manager server keystore.
- The remote manager provides the Client Authentication feature of SSL. This feature has been used in this connector to provide additional security. You must perform the prerequisite configuration steps described in Chapter 2, "Deploying the Connector" to enable this security feature.

3

Testing the Connector

After you deploy the connector, you must test it to ensure that it functions as expected.

> **Note:** In earlier releases of this guide, the connector was referred to as the *integration.*

This chapter contains the following sections:

Running Connector Tests

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

You can use the troubleshooting utility to directly use the connector for identifying the cause of problems associated with connecting to the target system server and performing basic operations on the target system.

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

After you specify the required values in the `config.properties` file, perform the following steps to run the test cases:

1. For RSA ACE Server 5.0:

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

   For all other versions of RSA ACE server:

   Update the following file on the target server:

   `authmgr_home``\tests\scripts\runTestServer.bat`

   In this file, add the following lines:

   ```
   set JAVA_HOME=JAVA_HOME
   set AUTHMGR_HOME=authmgr_home
   set XL_REMOTE=XL_REMOTE
   ```

For RSA ACE 5.0, add the following line:

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

For RSA ACE 5.2, add the following line:

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

For RSA Authentication Manager 6.0, add the following line:

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

For Solaris 9, update the following file:

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

In this file, add the following lines:

```
export AUTHMGR_HOME=authmgr_home
export ACE_INSTALL=ACE_INSTALL
export XL_REMOTE=XL_REMOTE
```

2. Run the `runTestServer.bat` script.

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

   For example:

   ```
   runTestServer 1001
   ```

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

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

3. On the Oracle Identity Manager server, use the following table to modify the default attributes of the config.properties file.

   This file is in the *xellerate_home*`\xellerate\XLIntegrations\AuthManager\tests\config\` directory.

Name	Description	Default 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. Check for the value of the `pw` property set in *authmgr_home*`\tests\scripts\runTestServer.` For example, `-Dpw=yourpassword.`	`yourpassword`
`adminMode`	Administration mode for the RSA Authentication Manager (host or remote)	`Host`
`admin`	Remote administration credentials for the RSA Authentication Manager and admin ID	`jdoe`
`passcode`	Remote administration credentials for the RSA Authentication Manager and the passcode for the admin ID	`1234`

Name	Description	Default 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	createUser
userID	User ID	jdoe
firstName	Represents the user attributes and first name	Jane
lastName	Represents the user attributes and last name	Doe
group	Represents the group attributes and group name	John Doe and Sons
groupLogin	Represents the group attributes and group login	jdoeGrp
tokenSerialNumber	Represents the token attributes and token Serial Number.	10473824
pin	Represents the token attributes and token PIN	1234
currentTokenCode	Represents the token attributes and token code	796563
number	Represents the token attributes and number of token codes to generate	2
lifetime	Represents the token attributes and the number of hours until emergency access mode expires.	24
digits	Represents the token attributes and the number of digits in the token code to be generated	6
loggerfile	Represents the log file name with path	..\logs\Test_ACE.log
loggerlevel	Represents the Logger properties and Logger level: DEBUG, FATAL, WARN, INFO, or ERROR	DEBUG
RevokeFlag	Revoke Token Flag	1
fileName	Software token file name	C:\SoftToken\soft18.sdtid
key	Encryption key type	1
protect	Copy protection flag	0
method	Password usage and interpretation method	0

Name	Description	Default 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 deployment operation	*filename*.log
overOption	Overwrites the output of a previously generated XML file	1
closeOption	Closing option of XML File	Leave this blank

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

   xellerate_home\xellerate\XLIntegrations\AuthManager\tests\scripts\runTestClient.bat

   In this file, add the following lines:

   XELLERATE_HOME\xellerate=*xellerate_home*\xellerate
   JAVA_HOME=*jdk_home*

   Run the runTestClient.bat file.

   For Solaris:

   Update the following file:

   xellerate_home/xellerate/XLIntegrations/AuthManager/tests/scripts/runTestClient.sh

   Add the following lines:

   XELLERATE_HOME/xellerate=*xellerate_home*/xellerate
   JAVA_HOME=*jdk_home*

   Run the runTestClient.sh file.

5. After the script is run, you must get the relevant output in a log file. The log file is located in the following directory:

   xellerate_home\xellerate\XLIntegrations\AuthManager\tests\logs\

   The following are sample contents of this file:

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

Troubleshooting

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

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

Problem Description	Solution
Process definition: ACEUser Process task: Delete User **Returned Error Message:** Failed to connect to serv DB, RSA ACE Broker 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 is invalid **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 invalid **Returned Error Code:** ACE_USERDELETIONISADMIN_FAIL	Check the user ID that you have specified. A user with this ID is an administrator. If you still want to delete it, revoke the Admin role.
Process definition: ACEUser Process task: Assign users to ACE groups **Returned Error Message:** Access denied, check admin credentials **Returned Error Code:** ACE_AUTHORIZED_ACCESS_FAIL	Check the admin credentials specified in the IT resource definition.
Process definition: ACEUser Process task: Assign users to ACE groups **Returned Error Message:** Unable to communicate with Authentication Server, RSA ACE Authentication Server not running **Returned Error Code:** ACE_AUTHORIZATION_ENGINE_FAIL	Start the service for RSA ACE Authentication Server.
Process definition: ACEUser Process task: Assign users to ACE groups **Returned Error Message:** Failed to Connect to serv DB, RSA ACE Broker not running **Returned Error Code:** ACE_SERVERDBCONNECT_FAIL	Start the service for RSA ACE Broker.

Problem Description	Solution
Process definition: ACEUser Process task: Assign users to ACE groups **Returned Error Message:** User is invalid **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 is invalid **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 admin credentials. **Returned Error Code:** ACE_AUTHORIZED_ACCESS_FAIL	Check the admin credentials specified in the IT resource definition.
Process definition: ACEUser Process task: Remove users from ACE groups **Returned Error Message:** Unable to communicate with Authentication Server, RSA ACE Authentication Server not running **Returned Error Code:** ACE_AUTHORIZATION_ENGINE_FAIL	Start the service for RSA ACE Authentication Server.
Process definition: ACEUser Process task: Remove users from ACE groups **Returned Error Message:** Failed to connect to serv DB, RSA ACE Broker 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 is invalid **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.

Problem Description	Solution
Process definition: ACEUser Process task: Remove users from ACE groups **Returned Error Message:** Group is invalid **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 admin credentials. **Returned Error Code:** ACE_AUTHORIZED_ACCESS_FAIL	Check the admin credentials specified in the IT resource definition.
Process definition: ACE Token Process task: Assign SecurID tokens to users **Returned Error Message:** Unable to communicate with Authentication Server, RSA ACE Authentication Server not running **Returned Error Code:** ACE_AUTHORIZATION_ENGINE_FAIL	Start the service for RSA ACE Authentication Server.
Process definition: ACE Token Process task: Assign SecurID tokens to users **Returned Error Message:** Failed to Connect to serv DB, RSA ACE Broker 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.

Problem Description	Solution
Process definition: ACE Token Process task: Assign SecurID tokens to users **Returned Error Message:** Maximum number of users already assigned to this user **Returned Error Code:** ACE_TOKENMAXALREADYASSIGNED_FAIL	Check the user to whom you have assigned the token. The maximum number (3) is already assigned to this user in ACE.
Process definition: ACE Token Process task: Disable Token **Returned Error Message:** Access Denied. Check admin credentials. **Returned Error Code:** ACE_AUTHORIZED_ACCESS_FAIL	Check the admin credentials specified in the IT resource definition.
Process definition: ACE Token Process task: Disable Token **Returned Error Message:** Unable to communicate with Authentication Server, RSA ACE Authentication Server not running **Returned Error Code:** ACE_AUTHORIZATION_ENGINE_FAIL	Start the service for RSA ACE Authentication Server.
Process definition: ACE Token Process task: Disable Token **Returned Error Message:** Failed to Connect to serv DB, RSA ACE Broker 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.

Problem Description	Solution
Process definition: ACE Token Process task: Enable Token **Returned Error Message:** Access Denied, check admin credentials **Returned Error Code:** ACE_AUTHORIZED_ACCESS_FAIL	Check the admin credentials specified in the IT resource definition.
Process definition: ACE Token Process task: Enable Token **Returned Error Message:** Unable to communicate with Authentication Server, RSA ACE Authentication Server not running **Returned Error Code:** ACE_AUTHORIZATION_ENGINE_FAIL	Start the service for RSA ACE Authentication Server.
Process definition: ACE Token Process task: Enable Token **Returned Error Message:** Failed to Connect to serv DB, RSA ACE Broker not running **Returned Error Code:** ACE_SERVERDBCONNECT_FAIL	Start the service for RSA ACE Broker.
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, please check admin credentials **Returned Error Code:** ACE_AUTHORIZED_ACCESS_FAIL	Check the admin credentials specified in the IT resource definition.

Problem Description	Solution
Process definition: ACE Token Process task: Set Pin Updated **Returned Error Message:** Unable to communicate with Authentication Server, RSA ACE Authentication Server not running **Returned Error Code:** ACE_AUTHORIZATION_ENGINE_FAIL	Start the service for RSA ACE Authentication Server.
Process definition: ACE Token Process task: Set Pin Updated **Returned Error Message:** Failed to Connect to serv DB, RSA ACE Broker 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.
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, please check admin credentials **Returned Error Code:** ACE_AUTHORIZED_ACCESS_FAIL	Check the admin credentials specified in the IT resource definition.
Process definition: ACE Token Process task: Set Pin to NTC Updated **Returned Error Message:** Unable to communicate with Authentication Server, RSA ACE Authentication Server not running **Returned Error Code:** ACE_AUTHORIZATION_ENGINE_FAIL	Start the service for RSA ACE Authentication Server.

Problem Description	Solution
Process definition: ACE Token Process task: Set Pin to NTC Updated **Returned Error Message:** Failed to Connect to serv DB, RSA ACE Broker 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 the RSA Authentication Manager.
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 token 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 admin credentials **Returned Error Code:** ACE_AUTHORIZED_ACCESS_FAIL	Check the admin credentials specified in the IT resource definition.
Process definition: ACE Token Process task: Set Lost Updated **Returned Error Message:** Unable to communicate with Authentication Server, RSA ACE Authentication Server not running **Returned Error Code:** ACE_AUTHORIZATION_ENGINE_FAIL	Start the service for RSA ACE Authentication Server.

Problem Description	Solution
Process definition: ACE Token Process task: Set Lost Updated **Returned Error Message:** Failed to Connect to serv DB, RSA ACE Broker 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, please check admin credentials **Returned Error Code:** ACE_AUTHORIZED_ACCESS_FAIL	Check the admin credentials specified in the IT resource definition.
Process definition: ACE Token Process task: Test Login Updated **Returned Error Message:** Unable to communicate with Authentication Server, RSA ACE Authentication Server not running **Returned Error Code:** ACE_AUTHORIZATION_ENGINE_FAIL	Start the service for RSA ACE Authentication Server.
Process definition: ACE Token Process task: Test Login Updated **Returned Error Message:** Failed to Connect to serv DB, RSA ACE Broker 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:** Token Serial Number is Invalid **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.

Problem Description	Solution
Process definition: ACE Token Process task: Test Login Updated **Returned Error Message:** Current Token Code is Invalid **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, please check admin credentials **Returned Error Code:** ACE_AUTHORIZED_ACCESS_FAIL	Check the admin credentials specified in the IT resource definition.
Process definition: ACE Token Process task: Revoke SecurID tokens from users **Returned Error Message:** Unable to communicate with Authentication Server, RSA ACE Authentication Server not running **Returned Error Code:** ACE_AUTHORIZATION_ENGINE_FAIL	Start the service for RSA ACE Authentication Server.
Process definition: ACE Token Process task: Revoke SecurID tokens from users **Returned Error Message:** Failed to Connect to serv DB, RSA ACE Broker 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_UNASSIGN_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: 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.

4

Known Issues

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

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

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

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

- While creating a user in RSA Authentication Manager, you must not enter special characters in the Default Login field. If you enter special characters in this field, then reconciliation would not work because Oracle Identity Manager does not support special characters in the User ID field.

Index