

## **Oracle® Identity Manager**

Connector Guide for RSA Authentication Manager

Release 9.1.0

**E16663-03**

September 2013

Copyright © 2011, 2013 Oracle and/or its affiliates. All rights reserved.

Primary Author: Alankrita Prakash

Contributing Authors: Gowri G. R, Prakash Hulikere, Sridhar Machani, Deena Purushothaman

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

---

---

# Contents

<b>Preface</b> .....	xi
Audience .....	xi
Documentation Accessibility .....	xi
Related Documents .....	xi
Documentation Updates .....	xi
Conventions .....	xii
 <b>What's New in the Oracle Identity Manager Connector for RSA Authentication Manager?</b> .....	xiii
Software Updates .....	xiii
Documentation-Specific Updates.....	xvi
 <b>1 About the Connector</b>	
1.1 Certified Components .....	1-1
1.2 Certified Languages.....	1-2
1.3 Connector Architecture.....	1-3
1.4 Features of the Connector .....	1-4
1.4.1 Support for Reconciliation and Provisioning of RSA Authentication Manager Accounts and Tokens 1-5	
1.4.2 Mapping Standard and Custom Attributes for Reconciliation and Provisioning .....	1-5
1.4.3 Full and Incremental Reconciliation .....	1-5
1.4.4 Batched Reconciliation .....	1-5
1.4.5 Limited (Filtered) Reconciliation.....	1-5
1.4.6 Enabling and Disabling Accounts .....	1-5
1.4.7 Reconciliation of Deleted User Records .....	1-6
1.4.8 SOAP-Based Communication with the Target System .....	1-6
1.4.9 Specifying Accounts to Be Excluded from Reconciliation.....	1-6
1.4.10 Transformation and Validation of Account Data .....	1-6
1.4.11 Support for Setting a PIN and the Token Lost Attribute .....	1-6
1.5 Lookup Definitions Used During Connector Operations .....	1-6
1.5.1 Lookup Definitions Synchronized with the Target System .....	1-7
1.5.1.1 Lookup.RSA.AuthManager.Group .....	1-7
1.5.1.2 Lookup.RSA.AuthManager.IdentitySource .....	1-8
1.5.1.3 Lookup.RSA.AuthManager.SecurityDomain.....	1-8
1.5.1.4 Lookup.RSA.AuthManager.AdminRole.....	1-9

1.5.1.5	Lookup.RSA.AuthManager.LookupReconMapping .....	1-9
1.5.2	Preconfigured Lookup Definitions .....	1-10
1.6	Connector Objects Used During Reconciliation .....	1-12
1.6.1	User Attributes for Reconciliation.....	1-12
1.6.2	Token Attributes for Reconciliation.....	1-14
1.6.3	Reconciliation Rule for User Reconciliation .....	1-15
1.6.4	Reconciliation Rule for Token Reconciliation.....	1-16
1.6.5	Reconciliation Action Rules for Target Resource Reconciliation.....	1-17
1.7	Connector Objects Used During Provisioning .....	1-18
1.7.1	Provisioning Functions .....	1-19
1.7.2	User Attributes for Provisioning .....	1-19
1.7.3	Token Attributes for Provisioning .....	1-20
1.8	Roadmap for Deploying and Using the Connector .....	1-21

## 2 Deploying the Connector

2.1	Preinstallation.....	2-1
2.1.1	Files and Directories That Comprise the Connector.....	2-1
2.1.2	Determining the Release Number of the Connector .....	2-2
2.1.3	Creating a Backup of the Existing Common.jar File.....	2-3
2.1.4	Removing RSA Authentication Manager JAR Files from the IBM WebSphere Application Server Home Directory	2-4
2.2	Installation .....	2-5
2.3	Postinstallation .....	2-7
2.3.1	Changing to the Required Input Locale on the Oracle Identity Manager Host Computer	2-8
2.3.2	Clearing Content Related to Connector Resource Bundles from the Server Cache...	2-8
2.3.3	Enabling Logging.....	2-10
2.3.3.1	Enabling Logging on Oracle Identity Manager Release 9.1.0.x .....	2-10
2.3.3.2	Enabling Logging on Oracle Identity Manager Release 11.1.1 and 11.1.2.x .....	2-12
2.3.4	Modifying Dependent Lookup Query Properties for Lookup Fields on Microsoft SQL Server	2-14
2.3.5	Addressing Prerequisites for Using the Java API of RSA Authentication Manager .....	2-18
2.3.5.1	Exporting and Importing the Server Root Certificate .....	2-18
2.3.5.2	Setting the Command Client User Name and Password .....	2-22
2.3.6	Copying Target System Files to Oracle Identity Manager.....	2-22
2.3.7	Setting Values for JAVA_OPTIONS Parameters .....	2-24
2.3.7.1	Setting Values for JAVA_OPTIONS Parameters on IBM WebSphere Application Server	2-25
2.3.7.2	Setting Values for JAVA_OPTIONS Parameters on JBoss Application Server	2-25
2.3.7.3	Setting Values for JAVA_OPTIONS Parameters on Oracle Application Server.....	2-26
2.3.7.4	Setting Values for JAVA_OPTIONS Parameters on Oracle WebLogic Server.	2-27
2.3.8	Creating a Target System Account for Connector Operations.....	2-27
2.3.9	Mapping New Connection Properties.....	2-35
2.3.10	Setting Up the Configuration Lookup Definition in Oracle Identity Manager .....	2-37
2.3.11	Setting Up the Lookup.RSA.AuthManager.ExclusionList Lookup Definition .....	2-41
2.3.12	Modifying the Process Form .....	2-42

2.3.13	Configuring Connection Parameters .....	2-43
2.3.14	Creating Authorization Policies for User Management.....	2-44
2.3.14.1	Creating an Authorization Policy for Provisioning.....	2-44
2.3.14.2	Creating an Authorization Policy for Reconciliation .....	2-45
2.3.15	Configuring Request-Based Provisioning.....	2-46
2.3.15.1	Copying Predefined Request Datasets .....	2-47
2.3.15.2	Importing Request Datasets into MDS.....	2-48
2.3.15.3	Enabling the Auto Save Form Feature .....	2-49
2.3.15.4	Running the PurgeCache Utility .....	2-49
2.3.16	Configuring Oracle Identity Manager 11.1.2 or Later .....	2-49
2.3.16.1	Tagging OIM Process Form Fields.....	2-49
2.3.16.2	Creating and Activating a Sandbox .....	2-50
2.3.16.3	Creating a New UI Form .....	2-51
2.3.16.4	Creating an Application Instance.....	2-51
2.3.16.5	Publishing a Sandbox.....	2-51
2.3.16.6	Harvesting Entitlements and Sync Catalog.....	2-52
2.3.16.7	Updating an Existing Application Instance with a New Form .....	2-52
2.3.17	Localizing Field Labels in UI Forms .....	2-52

### 3 Using the Connector

3.1	Performing First-Time Reconciliation.....	3-1
3.2	Scheduled Task for Lookup Field Synchronization.....	3-2
3.3	Guidelines on Performing Reconciliation .....	3-3
3.4	Configuring Reconciliation.....	3-3
3.4.1	Full Reconciliation .....	3-3
3.4.2	Limited Reconciliation .....	3-4
3.4.3	Batched Reconciliation .....	3-5
3.4.4	Reconciliation Scheduled Tasks.....	3-5
3.4.4.1	RSA Auth Manager User Recon .....	3-5
3.4.4.2	RSA Auth Manager Token Recon .....	3-6
3.5	Configuring the Scheduled Tasks.....	3-7
3.6	Guidelines on Performing Provisioning.....	3-10
3.7	Assigning Software Tokens to Users .....	3-10
3.8	Performing Provisioning Operations in Oracle Identity Manager Release 9.1.0.x and 11.1.1.x	3-10
3.8.1	Direct Provisioning.....	3-11
3.8.2	Request-Based Provisioning.....	3-19
3.8.2.1	End User's Role in Request-Based Provisioning .....	3-19
3.8.2.2	Approver's Role in Request-Based Provisioning .....	3-20
3.8.3	Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1	3-20
3.9	Performing Provisioning Operations in Oracle Identity Manager Release 11.1.2 or Later.....	3-21

### 4 Extending the Functionality of the Connector

4.1	Determining Whether an Attribute Is an Identity Management Services or Authentication Manager Attribute	4-1
-----	---	-----

4.2	Adding New User or Token Attributes for Reconciliation.....	4-2
4.3	Adding New User or Token Attributes for Provisioning .....	4-6
4.4	Configuring Validation of Data During Reconciliation and Provisioning.....	4-10
4.5	Configuring Transformation of Data During Reconciliation .....	4-12
4.6	Modifying Field Lengths on the Process Form.....	4-13
4.7	Guideline for Importing the Connector XML File .....	4-14
4.8	Configuring the Connector for Multiple Installations of the Target System .....	4-14

## 5 Known Issues and Limitations

5.1	Known Issues.....	5-1
5.2	Limitations .....	5-1

## Index



## List of Figures

1-1	Architecture of the Connector for RSA Authentication Manager .....	1-4
1-2	Reconciliation Rule for User Reconciliation.....	1-16
1-3	Reconciliation Rule for Token Reconciliation.....	1-17
1-4	Reconciliation Action Rules for Target Resource Reconciliation.....	1-18
3-1	Create User Page .....	3-12
3-2	User Detail Page.....	3-12
3-3	Resource Profile Page .....	3-13
3-4	Step 1: Select a Resource Page.....	3-13
3-5	Step 2: Verify Resource Selection Page .....	3-14
3-6	Step 5: Provide Process Data for RSA Auth Manager User Page .....	3-16
3-7	Step 5: Provide Process Data for RSA Auth Manager Token Form Page .....	3-17
3-8	Step 5: Provide Process Data for RSA Auth Manager Role Page.....	3-17
3-9	Step 6: Verify Process Data Page .....	3-18
3-10	Resource Profile Page .....	3-18



## List of Tables

1-1	Certified Components .....	1-2
1-2	Entries in the Lookup.RSA.AuthManager.LookupReconMapping Lookup Definition .....	1-10
1-3	Preconfigured Lookup Definitions.....	1-10
1-4	Entries in the Lookup.RSA.AuthManager.UserReconAttrMap Lookup Definition.....	1-13
1-5	Entries in the Lookup.RSA.AuthManager.UserReconChildAttrMap Lookup Definition.....	1-14
1-6	Entries in the Lookup.RSA.AuthManager.TokenReconAttrMap Lookup Definition..	1-15
1-7	Action Rules for Target Resource Reconciliation.....	1-17
1-8	Supported User Provisioning Functions .....	1-19
1-9	Entries in the Lookup.RSA.AuthManager.UserAttrMap Lookup Definition.....	1-20
1-10	Entries in the Lookup.RSA.AuthManager.UserChildAttrMap Lookup Definition.....	1-20
1-11	Entries in the Lookup.RSA.AuthManager.TokenAttrMap Lookup Definition.....	1-21
2-1	Files and Directories On the Installation Media .....	2-1
2-2	Log Levels and ODL Message Type:Level Combinations .....	2-13
2-3	Child Forms .....	2-14
2-4	Entries in the Lookup.RSA.AuthManager.ITResourceMapping Lookup Definition ...	2-36
2-5	Entries in the Lookup.RSA.AuthManager.Configuration Lookup Definition .....	2-37
2-6	Parameters of the IT Resource.....	2-44
3-1	Attributes of the RSA Auth Manager Lookup Recon Scheduled Task.....	3-3
3-2	Attributes of the RSA Auth Manager User Recon Scheduled Task .....	3-6
3-3	Attributes of the RSA Auth Manager Token Recon Scheduled Task.....	3-7
3-4	Scheduled Tasks for Lookup Field Synchronization and Reconciliation .....	3-7
3-5	Fields on the User Process Form.....	3-14
3-6	Fields on the Token Process Form.....	3-16
4-1	Connector Objects and Their Associations.....	4-15



---

# Preface

This guide describes the connector that is used to integrate Oracle Identity Manager with RSA Authentication Manager.

## Audience

This guide is intended for resource administrators and target system integration teams.

## Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

### Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

## Related Documents

For information about installing and using Oracle Identity Manager, see the Oracle Identity Manager documentation library.

For generic information about connectors, see *Oracle Identity Manager Connector Concepts*.

The following Oracle Technology Network page provides links to Oracle Identity Manager documentation:

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

## Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager Connectors documentation, 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
<b>boldface</b>	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
<code>monospace</code>	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 9.1.0.7.

---

---

**Note:** Release 9.1.0.7 of the connector comes after release 9.1.0. Release numbers 9.1.0.1 through 9.1.0.6 have not been used.

---

---

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.

## Software Updates

The following sections discuss software updates:

- [Software Updates in Release 9.1.0](#)
- [Software Updates in Release 9.1.0.7](#)

### Software Updates in Release 9.1.0

The following are software updates in release 9.1.0:

- [Changes in the List of Certified Target System Versions](#)
- [Change in the Minimum Oracle Identity Manager Release Requirement](#)
- [SOAP-Based Communication with the Target System](#)
- [No Requirement for a Remote Manager](#)
- [Dedicated Support for Target Resource Reconciliation](#)
- [Transformation and Validation of Account Data](#)
- [Support for Creating Copies of Connector Objects](#)
- [Support for Mapping New Custom Attributes for Reconciliation and Provisioning](#)
- [Inclusion of Javadocs in the Connector Deployment Package](#)

- [Resolved Issues in Release 9.1.0](#)

### **Changes in the List of Certified Target System Versions**

From this release onward, the connector is certified to work with RSA Authentication Manager 7.1 (with SP3 or later).

See [Section 1.1, "Certified Components"](#) for information about the certified components.

### **Change in the Minimum Oracle Identity Manager Release Requirement**

From this release onward, Oracle Identity Manager release 9.1.0.2 BP05 is the minimum required Oracle Identity Manager release. JDK 1.5 is the minimum JDK requirement.

See [Section 1.1, "Certified Components"](#) for more information.

### **SOAP-Based Communication with the Target System**

The connector supports SSL-secured SOAP-based communication between Oracle Identity Manager and the target system.

See [Section 2.3.13, "Configuring Connection Parameters"](#) for more information.

### **No Requirement for a Remote Manager**

Earlier releases of the connector required you to install a Remote Manager on the target system host computer. From this release onward, you do not need to use a Remote Manager.

### **Dedicated Support for Target Resource Reconciliation**

The connector provides all the features required for setting up RSA Authentication Manager as a managed (target) resource of Oracle Identity Manager. You cannot use the connector to set up RSA Authentication Manager as a trusted source of Oracle Identity Manager.

See [Section 1.3, "Connector Architecture"](#) for more information.

### **Transformation and Validation of Account Data**

You can configure validation of account data that is brought into or sent from Oracle Identity Manager during reconciliation and provisioning. In addition, you can configure transformation of account data that is brought into Oracle Identity Manager during reconciliation. The following sections provide more information:

- [Section 4.4, "Configuring Validation of Data During Reconciliation and Provisioning"](#)
- [Section 4.5, "Configuring Transformation of Data During Reconciliation"](#)

### **Support for Creating Copies of Connector Objects**

The Lookup.RSA.AuthManager.Configuration lookup definition has been introduced in this release. Some of the entries in this lookup definition facilitate the use of connector objects that you create. For example, if you create a copy of the process form for users, then you can specify the details of that new process form in the Lookup.RSA.AuthManager.Configuration lookup definition.

See [Section 2.3.10, "Setting Up the Configuration Lookup Definition in Oracle Identity Manager"](#) for more information.

## Support for Mapping New Custom Attributes for Reconciliation and Provisioning

All the standard RSA Authentication Manager attributes are mapped for reconciliation and provisioning. You can also add custom attributes on the target system and then map them with Oracle Identity Manager.

See the following sections for more information:

- [Section 4.2, "Adding New User or Token Attributes for Reconciliation"](#)
- [Section 4.3, "Adding New User or Token Attributes for Provisioning"](#)

## Inclusion of Javadocs in the Connector Deployment Package

To facilitate reuse and customization of some parts of the connector code, Javadocs are included in the connector deployment package.

## Resolved Issues in Release 9.1.0

The following are issues resolved in release 9.1.0:

Bug Number	Issue	Resolution
9300135	The connector supported setting of Start Time and End Time only in hours. It did not support setting of both hours and minutes. This was because the RSA Authentication Manager 6.x API did not support specifying the time in minutes.	This issue has been resolved. The RSA Authentication Manager 7.1 API supports setting Start Time and End Time in hours and minutes. The connector uses this feature of the API.
9300198	Multiple scheduled tasks could not be configured because the RSA Authentication Manager 6.x API was not thread-safe.	This issue has been resolved. The connector includes scheduled tasks that can be run concurrently because the RSA Authentication Manager 7.1 API supports this feature.

## Software Updates in Release 9.1.0.7

The following are software updates in release 9.1.0.7:

- [Support for New Oracle Identity Manager Release](#)
- [Support for Request-Based Provisioning](#)
- [Support for Batched Reconciliation](#)
- [Support for Setting a PIN and the Token Lost Attribute](#)

## Support for New Oracle Identity Manager Release

From this release onward, the connector can be installed and used on Oracle Identity Manager 11g release 1 (11.1.1). Where applicable, instructions specific to this Oracle Identity Manager release have been added in the guide.

See [Section 1.1, "Certified Components"](#) for the full list of certified Oracle Identity Manager releases.

## Support for Request-Based Provisioning

From this release onward, the connector provides support for request-based provisioning on Oracle Identity Manager 11g release 1 (11.1.1).

See [Section 3.8.2, "Request-Based Provisioning"](#) for more information.

### Support for Batched Reconciliation

From this release onward, you can configure the connector for batched reconciliation of records from the target system.

See [Section 3.4.3, "Batched Reconciliation"](#) for more information.

### Support for Setting a PIN and the Token Lost Attribute

From this release onward, you can use the connector to set values for the following during provisioning operations:

- A PIN for a token that is assigned to a user.
- The Token Lost attribute when the token device is lost.

[Section 1.4.11, "Support for Setting a PIN and the Token Lost Attribute"](#) mentions this feature.

## Documentation-Specific Updates

The following sections discuss documentation-specific updates:

- [Documentation-Specific Updates in Release 9.1.0](#)
- [Documentation-Specific Updates in Release 9.1.0.7](#)

### Documentation-Specific Updates in Release 9.1.0

Major changes have been made in the structure of the guide. The objective of these changes is to synchronize the guide with the changes made to the connector and to improve the usability of information provided by the guide.

See [Section 1.8, "Roadmap for Deploying and Using the Connector"](#) for information about the organization of content in this guide.

In the ["Known Issues and Limitations"](#) chapter, items that have been addressed or are not applicable to this release have been removed.

### Documentation-Specific Updates in Release 9.1.0.7

The following are the documentation-specific updates in release 9.1.0.7:

- Information in [Section 2.3.6, "Copying Target System Files to Oracle Identity Manager"](#) has been modified.
- The following sections have been added:
  - [Section 2.3.12, "Modifying the Process Form"](#)
  - [Section 2.3.14, "Creating Authorization Policies for User Management"](#)
- In the "Target System" row of [Table 1–1, "Certified Components"](#), a note has been added.
- In [Section 2.3.6, "Copying Target System Files to Oracle Identity Manager,"](#) the following updates have been made:
  - The "commons-lang-2.3" file name has been changed to "commons-lang-2.2".
  - A new step for copying the ims-client-patch.jar file has been added.
  - A note has been added to the `RSA_AM_HOME/appserver/modules/com.bea.core.process_5.3.0.0.jar` file in step 1.



- A note has been added to step 2.
- The "Oracle Identity Manager" row in [Table 1–1, "Certified Components"](#) has been modified.
- A note has been added in the "Files in the DataSets directory" row of [Table 2–1, "Files and Directories On the Installation Media"](#).
- The following sections have been added:
  - [Section 2.3.16, "Configuring Oracle Identity Manager 11.1.2 or Later"](#)
  - [Section 2.3.17, "Localizing Field Labels in UI Forms"](#)
  - [Section 3.8, "Performing Provisioning Operations in Oracle Identity Manager Release 9.1.0.x and 11.1.1.x"](#)
- Instructions specific to Oracle Identity Manager release 11.1.2.x have been added in the following sections:
  - [Section 2.1.1, "Files and Directories That Comprise the Connector"](#)
  - [Section 2.1.3, "Creating a Backup of the Existing Common.jar File"](#)
  - [Section 2.2, "Installation"](#)
  - [Section 2.3.3.2, "Enabling Logging on Oracle Identity Manager Release 11.1.1 and 11.1.2.x"](#)
  - [Section 2.3.2, "Clearing Content Related to Connector Resource Bundles from the Server Cache"](#)
  - [Section 2.3.13, "Configuring Connection Parameters"](#)
  - [Section 3.5, "Configuring the Scheduled Tasks"](#)
  - [Section 4.2, "Adding New User or Token Attributes for Reconciliation"](#)
  - [Section 4.3, "Adding New User or Token Attributes for Provisioning"](#)



---

# 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 external, identity-aware applications. This guide discusses the connector that enables you to use RSA Authentication Manager as a managed (target) resource of Oracle Identity Manager.

---

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

---

In the account management (target resource) mode of the connector, information about users created or modified directly on the target system can be reconciled into Oracle Identity Manager. In addition, you can use Oracle Identity Manager to perform provisioning operations on the target system.

This chapter contains the following sections:

- [Section 1.1, "Certified Components"](#)
- [Section 1.2, "Certified Languages"](#)
- [Section 1.3, "Connector Architecture"](#)
- [Section 1.4, "Features of the Connector"](#)
- [Section 1.5, "Lookup Definitions Used During Connector Operations"](#)
- [Section 1.6, "Connector Objects Used During Reconciliation"](#)
- [Section 1.7, "Connector Objects Used During Provisioning"](#)
- [Section 1.8, "Roadmap for Deploying and Using the Connector"](#)

## 1.1 Certified Components

[Table 1–1](#) lists the deployment requirements for the connector.

**Table 1–1 Certified Components**

Item	Requirement
Oracle Identity Manager	<p>You can use one of the following releases of Oracle Identity Manager:</p> <ul style="list-style-type: none"> <li>Oracle Identity Manager release 9.1.0.2 BP05 or later</li> </ul> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>- In this guide, <b>Oracle Identity Manager release 9.1.0.x</b> has been used to denote Oracle Identity Manager release 9.1.0.2 BP05 and future releases in the 9.1.0.x series that the connector will support.</li> <li>- The connector does not support Oracle Identity Manager running on Oracle Application Server. For detailed information about certified components of Oracle Identity Manager, see the certification matrix on Oracle Technology Network at <a href="http://www.oracle.com/technetwork/documentation/oim1014-097544.html">http://www.oracle.com/technetwork/documentation/oim1014-097544.html</a></li> </ul> <ul style="list-style-type: none"> <li>Oracle Identity Manager 11g release 1 (11.1.1)</li> </ul> <p><b>Note:</b> In this guide, <b>Oracle Identity Manager release 11.1.1</b> has been used to denote Oracle Identity Manager 11g release 1 (11.1.1).</p> <ul style="list-style-type: none"> <li>Oracle Identity Manager 11g release 2 BP04 (11.1.2.0.4) or later</li> </ul> <p><b>Note:</b> In this guide, <b>Oracle Identity Manager release 11.1.2.x</b> has been used to denote Oracle Identity Manager 11g release 2 BP04 (11.1.2.0.4) or later and future releases in the 11.1.2.x series that the connector will support.</p>
Target system	RSA Authentication Manager 7.1 with SP3 or later.
JDK	<p>The JDK requirement is as follows:</p> <ul style="list-style-type: none"> <li>For Oracle Identity Manager release 9.1.0.x, use JDK 1.5 or a later release in the 1.5 series.</li> <li>For Oracle Identity Manager release 11.1.1 and 11.1.2.x, use JDK 1.6 update 18 or later or JRockit JDK 1.6 update 17 or later.</li> </ul> <p>See <a href="#">Section 2.3.7, "Setting Values for JAVA_OPTIONS Parameters"</a> if you are using JDK 1.6.</p>

## 1.2 Certified Languages

The connector supports the following languages:

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

- Spanish

**See Also:** For information about supported special characters supported by Oracle Identity Manager, see one of the following guides:

- For Oracle Identity Manager release 9.1.0.x:  
*Oracle Identity Manager Globalization Guide*
- For Oracle Identity Manager release 11.1.1 and 11.1.2.x:  
*Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*

## 1.3 Connector Architecture

During user provisioning, adapters carry provisioning data submitted through the process form to the target system. RSA APIs accept provisioning data from the adapters, carry out the required operation on the target system, and return the response from the target system to the adapters. The adapters return the response to Oracle Identity Manager.

Token provisioning operations are performed in the same manner. A separate set of Oracle Identity Manager adapters is used during token provisioning operations.

If an operation involves provisioning of an RSA Authentication Manager account, token, role, or group, then the GUID of the object created on the target system is brought back to Oracle Identity Manager. For accounts and tokens, the GUID is stored in a hidden field on the process or child form and is used during update operations.

During reconciliation, the RSA Auth Manager User Recon scheduled task establishes a connection with the target system and sends reconciliation criteria to the RSA APIs. The APIs extract user records that match the reconciliation criteria and hand them over to the scheduled task, which brings the records to Oracle Identity Manager.

---

**Note:** In Oracle Identity Manager release 11.1.1, a scheduled job is an instance of a scheduled task. In this guide, the term **scheduled task** used in the context of Oracle Identity Manager release 9.1.0.x is the same as the term **scheduled job** in the context of Oracle Identity Manager release 11.1.1 and 11.1.2.x.

See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about scheduled tasks and scheduled jobs.

---

The RSA Auth Manager User Recon scheduled task can be configured to reconcile token data. Alternatively, you can use the RSA Auth Manager Token Recon scheduled task for token reconciliation.

---

**Note:** A maximum of 3 tokens can be assigned to a user on RSA Authentication Manager. This upper limit is also applied in Oracle Identity Manager.

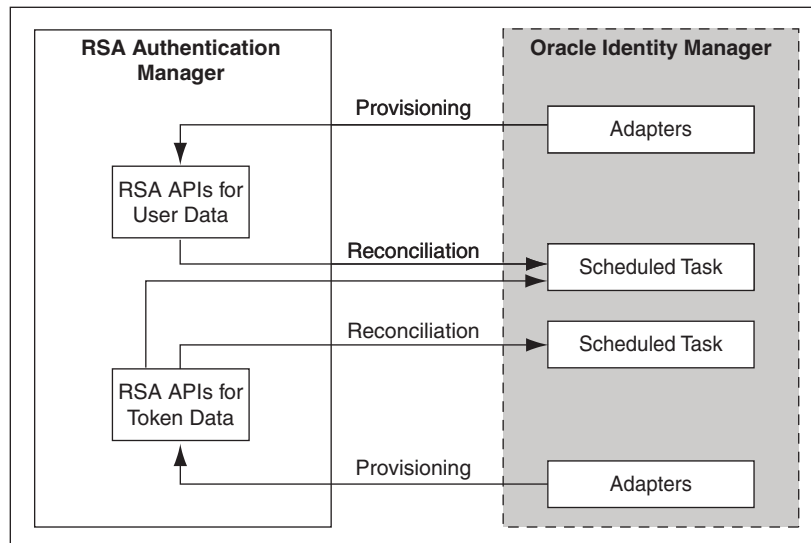
---

Each user or token record fetched from the target system is compared with RSA users or RSA tokens provisioned to OIM Users. If a match is found, then the update made to the user or token on the target system is copied to the RSA user or RSA token in Oracle

Identity Manager. If no match is found, then the user ID of the record is compared with the user ID of each OIM User. If a match is found, then data fetched from the target system user or token record is used to provision an RSA user or RSA token to the OIM User.

Figure 1–1 shows the connector integrating RSA Authentication Manager with Oracle Identity Manager.

**Figure 1–1 Architecture of the Connector for RSA Authentication Manager**



## 1.4 Features of the Connector

The following are features of the connector:

- [Section 1.4.1, "Support for Reconciliation and Provisioning of RSA Authentication Manager Accounts and Tokens"](#)
- [Section 1.4.2, "Mapping Standard and Custom Attributes for Reconciliation and Provisioning"](#)
- [Section 1.4.3, "Full and Incremental Reconciliation"](#)
- [Section 1.4.5, "Limited \(Filtered\) Reconciliation"](#)
- [Section 1.4.4, "Batched Reconciliation"](#)
- [Section 1.4.6, "Enabling and Disabling Accounts"](#)
- [Section 1.4.7, "Reconciliation of Deleted User Records"](#)
- [Section 1.4.8, "SOAP-Based Communication with the Target System"](#)
- [Section 1.4.9, "Specifying Accounts to Be Excluded from Reconciliation"](#)
- [Section 1.4.10, "Transformation and Validation of Account Data"](#)
- [Section 1.4.11, "Support for Setting a PIN and the Token Lost Attribute"](#)

### 1.4.1 Support for Reconciliation and Provisioning of RSA Authentication Manager Accounts and Tokens

You can use the connector to reconcile and provision RSA Authentication Manager accounts and tokens. The connector provides separate process forms and resource objects for user and token operations.

In RSA Authentication Manager, a user can be assigned up to 3 tokens. The connector enables the same feature in Oracle Identity Manager.

### 1.4.2 Mapping Standard and Custom Attributes for Reconciliation and Provisioning

You can create mappings for attributes that are not included in the list of default attribute mappings. These attributes can be custom attributes that you add on the target system.

See [Chapter 4, "Extending the Functionality of the Connector"](#) for more information.

### 1.4.3 Full and Incremental Reconciliation

In full reconciliation, all records are fetched from the target system to Oracle Identity Manager. In incremental reconciliation, only records that are added or modified after the last reconciliation run are fetched into Oracle Identity Manager.

You can switch from incremental to full reconciliation at any time after you deploy the connector. See [Section 3.4.1, "Full Reconciliation"](#) for more information.

### 1.4.4 Batched Reconciliation

You can break down a reconciliation run into batches by specifying the number of records that must be included in each batch.

See [Section 3.4.3, "Batched Reconciliation"](#) for more information.

### 1.4.5 Limited (Filtered) Reconciliation

To limit or filter the records that are fetched into Oracle Identity Manager during a reconciliation run, you can specify the subset of added or modified target system records that must be reconciled.

See [Section 3.4.2, "Limited Reconciliation"](#) for more information.

### 1.4.6 Enabling and Disabling Accounts

Account Start and Account Expire are two user attributes on the target system. For a particular user on the target system, if the Account Expire date is less than the current date, then the account is in the Disabled state. Otherwise, the account is in the Enabled state. When the record of this user is reconciled into Oracle Identity Manager, the user's state (RSA resource) in Oracle Identity Manager matches the user's state on the target system. In addition, through a provisioning operation, you can set the value of the Account Expire date to the current date or a date in the past.

---

**Note:** The Enabled or Disabled state of an account is not related to the Locked or Unlocked state of the account.

---

### 1.4.7 Reconciliation of Deleted User Records

The `IsDeleteAllowed` attribute of the RSA Auth Manager User Recon scheduled task is used to enable reconciliation of deleted user records. If you set the value of this attribute to `yes`, then the following events take place during a reconciliation run:

1. GUIDs of all existing users on Oracle Identity Manager are brought to the target system.
2. Each GUID brought from Oracle Identity Manager is matched against the GUIDs on the target system.
3. If a match is not found, then it is assumed that the user has been deleted on the target system. For this deleted user, the RSA Authentication Manager resource assigned to the corresponding OIM User is revoked. For each user resource that is revoked, the associated token resources are automatically revoked.

### 1.4.8 SOAP-Based Communication with the Target System

The connector supports SSL-secured SOAP-based communication between Oracle Identity Manager and the target system.

[Section 2.3.13, "Configuring Connection Parameters"](#) provides more information.

### 1.4.9 Specifying Accounts to Be Excluded from Reconciliation

You can specify a list of accounts that must be excluded from all reconciliation operations. Data from accounts whose user IDs you specify in the exclusion list is not fetched to Oracle Identity Manager during reconciliation.

See [Section 2.3.11, "Setting Up the Lookup.RSA.AuthManager.ExclusionList Lookup Definition"](#) for more information.

### 1.4.10 Transformation and Validation of Account Data

You can configure validation and transformation of account data that is brought into or sent from Oracle Identity Manager during reconciliation and provisioning. The following sections describe the procedure:

- [Section 4.4, "Configuring Validation of Data During Reconciliation and Provisioning"](#)
- [Section 4.5, "Configuring Transformation of Data During Reconciliation"](#)

### 1.4.11 Support for Setting a PIN and the Token Lost Attribute

From this release onward, you can use the connector to set the following:

- A PIN for the token that is assigned to a user.
- The Token Lost attribute when the token device is lost.

## 1.5 Lookup Definitions Used During Connector Operations

Lookup definitions used during connector operations can be categorized as follows:

- [Section 1.5.1, "Lookup Definitions Synchronized with the Target System"](#)
- [Section 1.5.2, "Preconfigured Lookup Definitions"](#)



## 1.5.1 Lookup Definitions Synchronized with the Target System

During a provisioning operation, you use a lookup field on the process form to specify a single value from a set of values. For example, you use the Identity Source lookup field to select an identity source during a provisioning operation performed through the Administrative and User Console. When you deploy the connector, lookup definitions corresponding to the lookup fields on the target system are automatically created in Oracle Identity Manager. Lookup field synchronization involves copying additions or changes made to the target system lookup fields into the lookup definitions in Oracle Identity Manager.

---

### Note:

- The target system allows you to use special characters in lookup fields. However, in Oracle Identity Manager, special characters are not supported in lookup definitions.
  - You use the RSA Auth Manager Lookup Recon scheduled task to synchronize these lookup definitions. [Section 3.2, "Scheduled Task for Lookup Field Synchronization"](#) describes this scheduled task.
- 

The following Oracle Identity Manager lookup definitions are synchronized with target system lookup fields:

- [Section 1.5.1.1, "Lookup.RSA.AuthManager.Group"](#)
- [Section 1.5.1.2, "Lookup.RSA.AuthManager.IdentitySource"](#)
- [Section 1.5.1.3, "Lookup.RSA.AuthManager.SecurityDomain"](#)
- [Section 1.5.1.4, "Lookup.RSA.AuthManager.AdminRole"](#)
- [Section 1.5.1.5, "Lookup.RSA.AuthManager.LookupReconMapping"](#)

### 1.5.1.1 Lookup.RSA.AuthManager.Group

The Lookup.RSA.AuthManager.Group lookup definition holds details of user groups defined on RSA Authentication Manager. You populate this lookup definition through lookup field synchronization performed using the RSA Auth Manager Lookup Recon scheduled task.

The following is the format of entries in this lookup definition:

- Code Key: *IT\_RESOURCE\_KEY~GROUP\_GUID*

In this format:

- *IT\_RESOURCE\_KEY* is the key assigned to the IT resource on Oracle Identity Manager.
- *GROUP\_GUID* is the GUID of the group on the target system.

- Decode: *IT\_RESOURCE\_NAME~GROUP\_NAME*

In this format:

- *IT\_RESOURCE\_NAME* is the name assigned to the IT resource on Oracle Identity Manager.
- *GROUP\_NAME* is the name of the group on the target system.

The following table shows sample entries in this lookup definition:

Code Key	Decode
1~ ims.34590df69e3714ac01625e5d14325154	RSA Server Instance~Demo Agent4 Group
1~ ims.6ddf54f39e3714ac0178e4628bbcd7f8	RSA Server Instance~Group111
1~ ims.6ddf93069e3714ac0173ec0a3d673569	RSA Server Instance~Group222

### 1.5.1.2 Lookup.RSA.AuthManager.IdentitySource

**See Also:** [Section 1.3, "Connector Architecture"](#)

In RSA Authentication Manager, an identity source can be the default internal database, an LDAP-based solution, or a database. The `Lookup.RSA.AuthManager.IdentitySource` lookup definition holds details of the identity sources configured for your target system installation.

The following is the format of entries in this lookup definition:

- Code Key: *IT\_RESOURCE\_KEY~IDENTITY\_SOURCE\_GUID*

In this format:

- *IT\_RESOURCE\_KEY* is the key assigned to the IT resource on Oracle Identity Manager.
- *IDENTITY\_SOURCE\_GUID* is the GUID of the identity source on the target system.

- Decode: *IT\_RESOURCE\_NAME~IDENTITY\_SOURCE\_NAME*

In this format:

- *IT\_RESOURCE\_NAME* is the name assigned to the IT resource on Oracle Identity Manager.
- *IDENTITY\_SOURCE\_NAME* is the name of the identity source on the target system.

The following table shows sample entries in this lookup definition:

Code Key	Decode
1~ ims.000000000000000000001000d0011000	RSA Server Instance~Internal Database

### 1.5.1.3 Lookup.RSA.AuthManager.SecurityDomain

In the RSA Authentication Manager context, security domains represent the internal business units, such as departments, of the organization. These security domains are organized in a hierarchy.

The `Lookup.RSA.AuthManager.SecurityDomain` lookup definition stores the GUID and name of these security domains.

The following is the format of entries in this lookup definition:

- Code Key: *IT\_RESOURCE\_KEY~SECURITY\_DOMAIN\_GUID*

In this format:

- `IT_RESOURCE_KEY` is the key assigned to the IT resource on Oracle Identity Manager.

- *SECURITY\_DOMAIN\_GUID* is the GUID of the security domain on the target system.
- Decode: *IT\_RESOURCE\_NAME~SECURITY\_DOMAIN\_NAME*  
In this format:
  - *IT\_RESOURCE\_NAME* is the name assigned to the IT resource on Oracle Identity Manager.
  - *SECURITY\_DOMAIN\_NAME* is the name of the security domain on the target system.

The following table shows sample entries in this lookup definition:

Code Key	Decode
1~ims.000000000000000000001000e0011000	RSA Server Instance~SystemDomain
1~ims.6de7d3c19e3714ac017cfd3c69eec20e	RSA Server Instance~Domain1
1~ims.6e3dc8939e3714ac02019a05130a8285	RSA Server Instance~Domain2

#### 1.5.1.4 Lookup.RSA.AuthManager.AdminRole

On RSA Authentication Manager, an administrative role is a collection of permissions that can be assigned to an administrator. It determines the level of control the administrator has over users, user groups, and other entities.

The Lookup.RSA.AuthManager.AdminRole lookup definition stores details of administrative roles. The following is the format of entries in this lookup definition:

- Code Key: *IT\_RESOURCE\_KEY~ROLE\_GUID*  
In this format:
  - *IT\_RESOURCE\_KEY* is the key assigned to the IT resource on Oracle Identity Manager.
  - *ROLE\_GUID* is the GUID of the role on the target system.
- Decode: *IT\_RESOURCE\_NAME~ROLE\_NAME*  
In this format:
  - *IT\_RESOURCE\_NAME* is the name assigned to the IT resource on Oracle Identity Manager.
  - *ROLE\_NAME* is the name of the role on the target system.

The following table shows sample entries in this lookup definition:

Code Key	Decode
1~ims.000000000000000000000000000000001000e0031000	RSA Server Instance~SuperAdminRole
1~ims.000000000000000000000000000000001000e0031001	RSA Server Instance~TrustedRealmAdminRole

#### 1.5.1.5 Lookup.RSA.AuthManager.LookupReconMapping

The Lookup.RSA.AuthManager.LookupReconMapping lookup definition holds the names of lookup definitions that are synchronized with the target system when you run the RSA Auth Manager Lookup Recon scheduled task.

Table 1–2 shows the entries in this lookup definition.

**Table 1–2 Entries in the Lookup.RSA.AuthManager.LookupReconMapping Lookup Definition**

Code Key	Decode
Roles Lookup	Lookup.RSA.AuthManager.AdminRole
Groups Lookup	Lookup.RSA.AuthManager.Group
Identity Source Lookup	Lookup.RSA.AuthManager.IdentitySource
Security Domain Lookup	Lookup.RSA.AuthManager.SecurityDomain

## 1.5.2 Preconfigured Lookup Definitions

[Table 1–3](#) describes the other lookup definitions that are created in Oracle Identity Manager when you deploy the connector. These lookup definitions are either prepopulated with values or values must be manually entered in them after the connector is deployed.

**Table 1–3 Preconfigured Lookup Definitions**

Lookup Definition	Description of Values	Method to Specify Values for the Lookup Definition
Lookup.RSA.AuthManager.Hours Lookup.RSA.AuthManager.Minutes	On the Administrative and User Console, these lookup definitions are used to populate the Account Start Time and Account Expire Time lookup fields of the user process form. You use these lookup fields to select the time (in hours and minutes).  <a href="#">Figure 3–6</a> shows the lookup fields for these lookup definitions on the Administrative and User Console.	You must not modify these lookup definitions.
Lookup.RSA.AuthManager.FullReconFilter	This lookup definition is used during full reconciliation.	You must not modify this lookup definition.
Lookup.RSA.AuthManager.Configuration	This lookup definition holds connector configuration entries that are used during reconciliation and provisioning.	Some of the entries in this lookup definition are preconfigured. <a href="#">Section 2.3.10, "Setting Up the Configuration Lookup Definition in Oracle Identity Manager"</a> provides information about the entries for which you can set values.
Lookup.RSA.AuthManager.Constants	This lookup definition stores values that are used internally by the connector. The connector development team can use this lookup definition to make minor configuration changes in the connector.	You must not modify this lookup definition.
Lookup.RSA.AuthManager.DateMappings	This lookup definition holds entries that are used to format date values so that they are compatible with the date format used on the target system. This lookup definition is used during provisioning.	You must not modify this lookup definition.
Lookup.RSA.AuthManager.ExclusionList	This lookup definition holds user IDs of target system accounts for which you do not want to perform reconciliation and provisioning.	You can enter user IDs in this lookup definition. See <a href="#">Section 2.3.11, "Setting Up the Lookup.RSA.AuthManager.ExclusionList Lookup Definition"</a> for more information.

**Table 1–3 (Cont.) Preconfigured Lookup Definitions**

<b>Lookup Definition</b>	<b>Description of Values</b>	<b>Method to Specify Values for the Lookup Definition</b>
Lookup.RSA.AuthManager.ITResourceMapping	The connector uses the RemoteCommandTargetBean API of the target system to establish connections with the target system. The Lookup.RSA.AuthManager.ITResourceMapping lookup definition maps some of the IT resource parameters with parameters of this API.	See <a href="#">Section 2.3.9, "Mapping New Connection Properties"</a> for information about existing entries and the procedure to add new entries in this lookup definition.
Lookup.RSA.AuthManager.UserAttrMap	This lookup definition holds mappings between the user process form fields and single-valued user attributes on the target system.	This lookup definition is preconfigured. <a href="#">Table 1–9</a> lists the default entries in it. You can add entries in this lookup definition if you want to map new target system attributes for provisioning. See <a href="#">Section 4.3, "Adding New User or Token Attributes for Provisioning"</a> for more information.
Lookup.RSA.AuthManager.UserChildAttrMap	This lookup definition holds mappings between process form fields and multivalued target system attributes. It is used during provisioning.	This lookup definition is preconfigured. <a href="#">Table 1–10</a> lists the default entries in it.
Lookup.RSA.AuthManager.UserReconChildAttrMap	This lookup definition holds mappings between resource object fields and multivalued target system attributes. It is used during reconciliation.	This lookup definition is preconfigured. <a href="#">Table 1–5</a> lists the default entries in it. You can add entries in this lookup definition if you want to map new multivalued target system attributes for provisioning.
Lookup.RSA.AuthManager.TokenAttrMap	This lookup definition holds mappings between the token process form fields and token attributes on the target system. It is used during provisioning.	This lookup definition is preconfigured. <a href="#">Table 1–11</a> lists the default entries in it. You can add entries in this lookup definition if you want to map new target system attributes for provisioning. See <a href="#">Section 4.3, "Adding New User or Token Attributes for Provisioning"</a> for more information.
Lookup.RSA.AuthManager.UserReconAttrMap	This lookup definition holds mappings between the user resource object fields and single-valued user attributes on the target system. It is used during reconciliation.	This lookup definition is preconfigured. <a href="#">Table 1–4</a> lists the default entries in it. You can add entries in this lookup definition if you want to map new target system attributes for reconciliation. See <a href="#">Section 4.2, "Adding New User or Token Attributes for Reconciliation"</a> for more information.
Lookup.RSA.AuthManager.TokenReconAttrMap	This lookup definition holds mappings between the token resource object fields and token attributes on the target system. It is used during provisioning.	This lookup definition is preconfigured. <a href="#">Table 1–8</a> lists the default entries in it. You can add entries in this lookup definition if you want to map new target system attributes for reconciliation. See <a href="#">Section 4.2, "Adding New User or Token Attributes for Reconciliation"</a> for more information.
Lookup.RSA.AuthManager.TokenTransformMapping	This lookup definition is used to configure transformation of token attribute values that are fetched from the target system during token reconciliation.	You manually create entries in this lookup definition. See <a href="#">Section 4.5, "Configuring Transformation of Data During Reconciliation"</a> for more information.

**Table 1–3 (Cont.) Preconfigured Lookup Definitions**

Lookup Definition	Description of Values	Method to Specify Values for the Lookup Definition
Lookup.RSA.AuthManager. UserTransformMapping	This lookup definition is used to configure transformation of user attribute values that are fetched from the target system during user reconciliation.	You manually create entries in this lookup definition. See <a href="#">Section 4.5, "Configuring Transformation of Data During Reconciliation"</a> for more information.
Lookup.RSA.AuthManager. TokenProvisioningValidation	This lookup definition is used to configure validation of token attribute values that are sent to the target system during provisioning.	You manually create entries in this lookup definition. See <a href="#">Section 4.4, "Configuring Validation of Data During Reconciliation and Provisioning"</a> for more information.
Lookup.RSA.AuthManager. TokenReconValidation	This lookup definition is used to configure validation of token attribute values fetched from the target system during reconciliation.	You manually create entries in this lookup definition. See <a href="#">Section 4.4, "Configuring Validation of Data During Reconciliation and Provisioning"</a> for more information.
Lookup.RSA.AuthManager. UserProvisioningValidation	This lookup definition is used to configure validation of user attribute values that are sent to the target system during provisioning.	You manually create entries in this lookup definition. See <a href="#">Section 4.4, "Configuring Validation of Data During Reconciliation and Provisioning"</a> for more information.
Lookup.RSA.AuthManager. UserReconValidation	This lookup definition is used to configure validation of user attribute values that are fetched from the target system during reconciliation.	You manually create entries in this lookup definition. See <a href="#">Section 4.4, "Configuring Validation of Data During Reconciliation and Provisioning"</a> for more information.

## 1.6 Connector Objects Used During Reconciliation

**See Also:** One of the following guides for conceptual information about reconciliation:

- For Oracle Identity Manager release 9.1.0.x: *Oracle Identity Manager Connector Concepts*
- For Oracle Identity Manager release 11.1.1 and 11.1.2.x: *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*

The following sections describe connector objects used during reconciliation:

- [Section 1.6.1, "User Attributes for Reconciliation"](#)
- [Section 1.6.2, "Token Attributes for Reconciliation"](#)
- [Section 1.6.3, "Reconciliation Rule for User Reconciliation"](#)
- [Section 1.6.4, "Reconciliation Rule for Token Reconciliation"](#)
- [Section 1.6.5, "Reconciliation Action Rules for Target Resource Reconciliation"](#)

### 1.6.1 User Attributes for Reconciliation

The Lookup.RSA.AuthManager.UserReconAttrMap lookup definition holds single-valued attribute mappings for user reconciliation. The Code Key column holds the names of resource object fields. The format of values in the Decode column is as follows:

*METHOD\_NAME;PRINCIPAL\_TYPE;ATTRIBUTE\_TYPE;RETURN\_TYPE\_OF\_METHOD;RESOURCE\_OBJECT\_FIELD\_TYPE;DTO\_ATTRIBUTE\_NAME*

In this format:

- *METHOD\_NAME* is the name of the method on the target system that fetches values from the attribute. This method belongs to one of the following APIs:

- com.rsa.admin.data.ListTokenDTO
- com.rsa.authmgr.admin.principalmgmt.data.TokenDTO

The `get` or `is` prefix of the method name is not included in the Decode value.

- *RETURN\_VALUE\_OF\_METHOD* is the data type of the values returned by the method.
- *PRINCIPAL\_TYPE* can be either `IMS` or `AM` depending on whether the attribute is an Identity Management Services attribute or an Authentication Manager attribute.

**See Also:** Target system documentation for information about differences between Identity Management Services and Authentication Manager attributes

- *RETURN\_TYPE\_OF\_METHOD* is the data type of the values fetched by the method. The return type is specified in the Javadocs for the API.
- *RESOURCE\_OBJECT\_FIELD\_TYPE* can be `Text`, `Boolean`, `Lookup`, or `Date`.
- *DTO\_ATTRIBUTE\_NAME* is the name of the attribute in the `PrincipalDTO` or `AMPrincipalDTO` API.

Table 1–4 lists the entries in this lookup definition.

**Table 1–4 Entries in the Lookup.RSA.AuthManager.UserReconAttrMap Lookup Definition**

Code Key	Decode
User ID	userID;IMS;Core;String;Text;LOGINUID
Certificate DN	certificateDN;IMS;Core;String;Text;CERTDN
Account Start Date	accountStartDate;IMS;Core;Date;Date
Account Expire Date	accountExpireDate;IMS;Core;Date;Date
Clear Incorrect Passcodes	clearBadPasscodes;AM;Core;boolean;CheckBox
Clear Windows Password	ClearWindowsLoginPassword;AM;Core;boolean;CheckBox
Identity Source	identitySourceGuid;IMS;Core;String;Lookup
Security Domain	securityDomainGuid;IMS;Core;String;Lookup
Default Shell	defaultShell;AM;Core;String;Text
User GUID	Guid;IMS;Core;String;String
Fixed Passcode Allowed	staticPasswordSet;AM;Core;boolean;CheckBox
First Name	firstName;IMS;Core;String;Text;FIRST_NAME
Last Name	lastName;IMS;Core;String;Text;LAST_NAME
Middle Name	middleName;IMS;Core;String;Text;MIDDLE_NAME



The Lookup.RSA.AuthManager.UserReconChildAttrMap lookup definition holds multivalued attribute mappings for user reconciliation. Table 1–5 lists the entries in this lookup definition.

The following is the format of entries in this lookup definition:

- Code Key: Name of the field on the resource object
- Decode: The value is in the following format:

*CHILD\_TABLE\_NAME\_IN\_RESOURCE\_OBJECT;METHOD\_NAME;RETURN\_VALUE\_OF\_METHOD;FIELD\_TYPE\_ON\_PROCESS\_FORM*

In this format:

- *CHILD\_TABLE\_NAME\_IN\_RESOURCE\_OBJECT* is the name of the child table in the resource object.
- *METHOD\_NAME* is the name of the method of the `com.rsa.admin.data.GroupDTO` or `com.rsa.admin.data.AdminRoleDTO` API on the target system that fetches values from the attribute. The `get` prefix is not included in the name of the method.
- *RETURN\_VALUE\_OF\_METHOD* is the data type of the values returned by the method.
- *FIELD\_TYPE\_ON\_PROCESS\_FORM* can be `Boolean`, `Lookup`, `Text`, or `RadioButton`, depending on the type of child form field.

**Table 1–5 Entries in the Lookup.RSA.AuthManager.UserReconChildAttrMap Lookup Definition**

Code Key	Decode
Group Name	Groups;Guid;String;Lookup
Role Name	Roles;Guid;String;Lookup

## 1.6.2 Token Attributes for Reconciliation

The Lookup.RSA.AuthManager.TokenReconAttrMap lookup definition holds single-valued attribute mappings for token reconciliation. The Code Key column holds the names of resource object fields. The format of values in the Decode column is as follows:

*METHOD\_NAME;API\_NAME;ATTRIBUTE\_TYPE;METHOD\_RETURN\_TYPE;PROCESS\_FORM\_FIELD\_TYPE*

In this format:

- *METHOD\_NAME* is the name of the method on the target system that fetches values from the attribute. This method belongs to one of the following APIs:
  - `com.rsa.admin.data.ListTokenDTO`
  - `com.rsa.authmgr.admin.principalmgt.data.TokenDTO`

The `get` or `is` prefix of the method name is not included in the Decode value.

- *API\_NAME* is either `ListTokenDTO` or `TokenDTO`.
- *ATTRIBUTE\_TYPE* can be one of the following:
  - Replace *ATTRIBUTE\_TYPE* with `Core` if the attribute is a standard RSA Authentication Manager attribute.
  - Replace *ATTRIBUTE\_TYPE* with `Extended` if the attribute is a custom attribute.



- *METHOD\_RETURN\_TYPE* is the data type of the value fetched by the method. The return type is specified in the Javadocs for the API.
- *PROCESS\_FORM\_FIELD\_TYPE* can be either `Text` or `Checkbox`.

Table 1–6 lists the entries in this lookup definition.

**Table 1–6 Entries in the Lookup.RSA.AuthManager.TokenReconAttrMap Lookup Definition**

Resource Object Field (Code Key)	RSA Authentication Manager Token Attribute (Decode)
Token Serial Number	SerialNumber;ListTokenDTO;Core;String;Text
Token GUID	Guid;ListTokenDTO;Core;String;Text
Notes	Notes;TokenDTO;Core;String;Text
Pin	Pin;TokenDTO;Core;String;Text
Token Lost	TokenLost;TokenDTO;Core;String;Text

### 1.6.3 Reconciliation Rule for User Reconciliation

**See Also:** For generic information about reconciliation matching and action rules, see one of the following guides:

- For Oracle Identity Manager release 9.1.0.x: *Oracle Identity Manager Connector Concepts*
- For Oracle Identity Manager release 11.1.1 and 11.1.2.x: *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*

The following is the process matching rule for user reconciliation:

**Rule name:** RSA AuthManager UserRecon

**Rule element:** (User Login Equals User ID) OR (User GUID Equals User GUID)

The first rule component is used to reconcile accounts that are newly created on the target system. In this rule component:

- User Login is the User ID field on the OIM User form.
- User ID is the User ID field of RSA Authentication Manager.

The second rule component is used to reconcile updates to accounts that are already reconciled from the target system. In this rule component:

- User GUID to the left of "Equals" is the User GUID of the RSA user resource assigned to the OIM User.
- User GUID to the right of "Equals" is the User GUID of the account on the target system.

After you deploy the connector, you can view the user reconciliation rule by performing the following steps:

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tools**.
3. Double-click **Reconciliation Rules**.
4. Search for **RSA AuthManager UserRecon**. Figure 1–2 shows the reconciliation rule for user reconciliation.

**Figure 1–2 Reconciliation Rule for User Reconciliation**

The screenshot shows the 'Reconciliation Rule Builder' window. At the top, the 'Name' field is 'RSA AuthManager UserRecon' and the 'Object' field is 'RSA Auth Manager User'. The 'Operator' section has 'AND' and 'OR' radio buttons, with 'OR' selected. There are checkboxes for 'Valid' and 'Active', both of which are checked. Below these, there are radio buttons for 'For User' (selected) and 'For Organization'. The 'Description' field contains 'RSA AuthManager UserRecon'. The bottom section, titled 'Rule Definition', contains a list of rule elements: 'Rule: RSA AuthManager UserRecon', 'User Login Equals User ID', and 'User GUID Equals User GUID'. On the left side of the 'Rule Definition' section, there are buttons for 'Add Rule', 'Add Rule Element', 'Delete', and 'Legend'.

## 1.6.4 Reconciliation Rule for Token Reconciliation

**See Also:** For generic information about reconciliation matching and action rules, see one of the following guides:

- For Oracle Identity Manager release 9.1.0.x: *Oracle Identity Manager Connector Concepts*
- For Oracle Identity Manager release 11.1.1 and 11.1.2.x: *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*

The following is the process matching rule for token reconciliation:

**Rule name:** RSA AuthManager TokenRecon

**Rule element:** (User Login Equals User ID) OR (User GUID Equals User GUID)

In the first rule component:

- User Login is the User ID field on the OIM User form.
- User ID is the User ID field of RSA Authentication Manager.

In the second rule component:

- User GUID to the left of "Equals" is the User GUID of the RSA token resource assigned to the OIM User.
- User GUID to the right of "Equals" is the User GUID of the resource on the target system.

This rule supports the following scenarios:

- You can provision multiple RSA Authentication Manager token resources to the same OIM User, either on Oracle Identity Manager or directly on the target system.
- You can change the user ID of a user on the target system.

This is illustrated by the following use cases:

- Use case 1: You provision an RSA account for an OIM User, and you also assign a token for the user directly on the target system.

During the next reconciliation run, application of the first rule condition helps match the resource with the record.

- Use case 2: An OIM User has an RSA token. You then change the user ID of the user on the target system.

When the first rule condition is applied, no match is found. Then, the second rule condition is applied and it is determined that a second account has been given to the user on the target system. Details of this second account are linked with the OIM User by the reconciliation engine.

After you deploy the connector, you can view the reconciliation rule for target resource reconciliation by performing the following steps:

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tools**.
3. Double-click **Reconciliation Rules**.
4. Search for **RSA AuthManager TokenRecon**. [Figure 1–3](#) shows the reconciliation rule for token reconciliation.

**Figure 1–3 Reconciliation Rule for Token Reconciliation**

The screenshot displays the 'Reconciliation Rule Builder' window. The 'Name' field is 'SA AuthManager TokenRecon'. The 'Object' is 'RSA Auth Manager Token'. The 'Operator' is set to 'OR'. The 'Valid' checkbox is checked. The 'Active' checkbox is checked. The 'For User' radio button is selected. The 'Description' is 'Token Recon Matching Rule'. The 'Rule Definition' section shows a tree structure with 'Rule: RSA AuthManager TokenRecon' at the top, followed by 'User Login Equals User ID' and 'Token Serial Number Equals Token Serial Number'. The 'Add Rule', 'Add Rule Element', 'Delete', and 'Legend' buttons are visible on the left.

## 1.6.5 Reconciliation Action Rules for Target Resource Reconciliation

[Table 1–7](#) lists the action rules for target resource reconciliation.

**Table 1–7 Action Rules for Target Resource Reconciliation**

Rule Condition	Action
No Matches Found	Assign to Administrator With Least Load
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

---

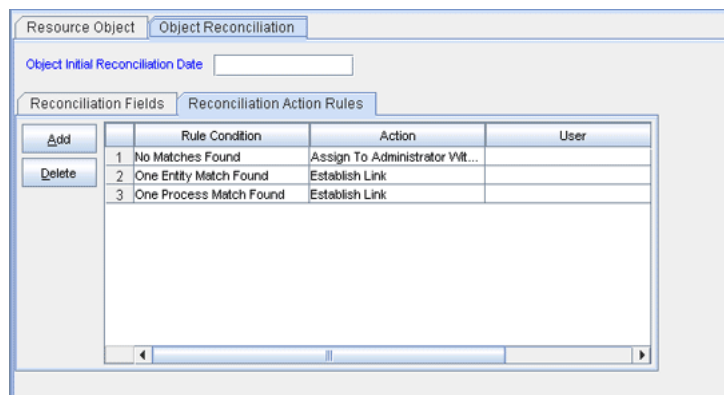
**Note:** No action is performed for rule conditions that are not predefined for this connector. You can define your own action rule for such rule conditions. For information about modifying or creating reconciliation action rules, see one of the following guides:

- For Oracle Identity Manager release 9.1.0.x: *Oracle Identity Manager Design Console Guide*
  - For Oracle Identity Manager release 11.1.1 and 11.1.2.x: *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*
- 

After you deploy the connector, you can view the reconciliation action rules for target resource reconciliation by performing the following steps:

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Resource Management**.
3. Double-click **Resource Objects**.
4. Search for and open the **RSA Auth Manager User** resource object.
5. Click the **Object Reconciliation** tab, and then click the **Reconciliation Action Rules** tab. The Reconciliation Action Rules tab displays the action rules defined for this connector. [Figure 1–4](#) shows the reconciliation action rule for target resource reconciliation.

**Figure 1–4 Reconciliation Action Rules for Target Resource Reconciliation**



## 1.7 Connector Objects Used During Provisioning

**See Also:** For conceptual information about provisioning, see one of the following guides:

- For Oracle Identity Manager release 9.1.0.x: *Oracle Identity Manager Connector Concepts*
- For Oracle Identity Manager release 11.1.1 and 11.1.2.x: *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*

The following sections describe connector objects used during provisioning:

- [Section 1.7.1, "Provisioning Functions"](#)
- [Section 1.7.2, "User Attributes for Provisioning"](#)

- [Section 1.7.3, "Token Attributes for Provisioning"](#)

## 1.7.1 Provisioning Functions

[Table 1–8](#) lists the provisioning functions that are supported by the connector. The Adapter column gives the name of the adapter that is used when the function is performed.

**Table 1–8 Supported User Provisioning Functions**

Function	Adapter
Create user	RSAMCREATEUSER
Update user	RSAMUPDATEUSER
Enable or disable user	RSAMENABLEUSER and RSAMDISABLEUSER
Assign or remove user from a group	RSAMADDGROUP and RSAMREMOVEGROUP
Add or remove role from user	RSAMADDROLE and RSAMREMOVEROLE
Delete user	RSAMDELETEUSER
Assign token to user	RSAMASSIGNTOKEN
Update token	RSAMUPDATETOKEN
Enable or disable token	RSAMENABLETOKEN and RSAMDISABLETOKEN
Revoke token from user	RSAMREVOKETOKEN
Update PIN	RSAMUPDATETOKEN
Update Token Lost	RSAMUPDATETOKEN

## 1.7.2 User Attributes for Provisioning

The Lookup.RSA.AuthManager.UserAttrMap lookup definition maps process form fields with single-valued target system attributes. The Code Key column holds the names of process form fields. The format of values in the Decode column is as follows:

*METHOD\_NAME;PRINCIPAL\_TYPE;ATTRIBUTE\_TYPE;METHOD\_INPUT\_TYPE;DTO\_ATTRIBUTE\_NAME*

In this format:

- *METHOD\_NAME* is the name of the method on the target system that fetches values from the attribute. This method belongs to one of the following APIs:

- com.rsa.admin.data.ListTokenDTO
- com.rsa.authmgr.admin.principalmgmt.data.TokenDTO

The set prefix of the method name is not included in the Decode value.

- *PRINCIPAL\_TYPE* can be either IMS or AM depending on whether the attribute is an Identity Management Services attribute or an Authentication Manager attribute.

**See Also:** Target system documentation for information about differences between Identity Management Services and Authentication Manager attributes

- *ATTRIBUTE\_TYPE* can be one of the following:
  - Replace *ATTRIBUTE\_TYPE* with Core if the attribute is a standard RSA Authentication Manager attribute.

- Replace *ATTRIBUTE\_TYPE* with *Extended* if the attribute is a custom attribute.
- *METHOD\_INPUT\_TYPE* is the data type of the value sent to the method. The return type is specified in the Javadocs for the API.
- *DTO\_ATTRIBUTE\_NAME* is the name of the attribute in the *PrincipalDTO* or *AMPrincipalDTO* API.

Table 1–9 lists the entries in this lookup definition.

**Table 1–9 Entries in the Lookup.RSA.AuthManager.UserAttrMap Lookup Definition**

Code Key	Decode
Default Shell	defaultShell;AM;Core;String
Fixed Passcode Allowed	staticPasswordSet;AM;Core;boolean
First Name	firstName;IMS;Core;String;FIRST_NAME
Last Name	lastName;IMS;Core;String;LAST_NAME
Middle Name	middleName;IMS;Core;String;MIDDLE_NAME
User ID	userId;IMS;Core;String;LOGINUID
Certificate DN	certificateDN;IMS;Core;String;CERT_DN
Password	Password;IMS;Core;String;PASSWORD
Account Start Date	accountStartDate;IMS;Core;Date;START_DATE
Account Expire Date	accountExpireDate;IMS;Core;Date;EXPIRATION_DATE
Fixed Passcode	staticPassword;AM;Core;String
Clear Incorrect Passcodes	clearBadPasscodes;AM;Core;boolean
Clear Windows Password	ClearWindowsLoginPassword;AM;Core;boolean
Identity Source	identitySourceGuid;IMS;Core;String;IDENTITY_SOURCE
Security Domain	securityDomainGuid;IMS;Core;String;OWNER_ID

The Lookup.RSA.AuthManager.UserChildAttrMap lookup definition holds multivalued attribute mappings for user reconciliation. Table 1–5 lists the entries in this lookup definition.

The following is the format of entries in this lookup definition:

Code Key: *CHILD\_FORM\_NAME*

Decode: *API\_NAME;METHOD\_NAME*

**Table 1–10 Entries in the Lookup.RSA.AuthManager.UserChildAttrMap Lookup Definition**

Code Key	Decode
UD_AMGROUP	LinkGroupPrincipalsCommand;groupGuids
UD_AMROLE	LinkAdminRolesPrincipalsCommand;adminRoleGuids

### 1.7.3 Token Attributes for Provisioning

The Lookup.RSA.AuthManager.TokenAttrMap lookup definition maps process form fields with single-valued target system attributes. The Code Key column holds the names of process form fields. The format of values in the Decode column is as follows:

*METHOD\_NAME;API\_NAME;ATTRIBUTE\_TYPE;METHOD\_INPUT\_TYPE*

In this format:

- *METHOD\_NAME* is the name of the method on the target system that fetches values from the attribute. This method belongs to one of the following APIs:
  - com.rsa.admin.data.ListTokenDTO
  - com.rsa.authmgr.admin.principalmgmt.data.TokenDTO
 The `set` prefix of the method name is not included in the Decode value.
- *API\_NAME* is either `ListTokenDTO` or `TokenDTO`.
- *ATTRIBUTE\_TYPE* can be one of the following:
  - Replace *ATTRIBUTE\_TYPE* with `Core` if the attribute is a core Identity Management Services attribute or Authentication Manager attribute.
  - Replace *ATTRIBUTE\_TYPE* with `Extended` if the attribute is an extended Identity Management Services attribute.
- *METHOD\_INPUT\_TYPE* is the data type of the value sent to the method. This data type is specified in the Javadocs for the API.

Table 1–11 lists the entries in this lookup definition.

**Table 1–11 Entries in the Lookup.RSA.AuthManager.TokenAttrMap Lookup Definition**

Code Key	Decode
Notes	Notes;TokenDTO;Core;String
Token Serial Number	SerialNumber;ListTokenDTO;Core;String
Pin	Pin;TokenDTO;Core;String
Token Lost	TokenLost;TokenDTO;Core;Boolean

## 1.8 Roadmap for Deploying and Using the Connector

The following is the organization of information in the rest of this guide:

- [Chapter 2, "Deploying the Connector"](#) describes procedures that you must perform on Oracle Identity Manager and the target system during each stage of connector deployment.
- [Chapter 3, "Using the Connector"](#) describes guidelines on using the connector and the procedure to configure reconciliation runs and perform provisioning operations.
- [Chapter 4, "Extending the Functionality of the Connector"](#) describes procedures that you can perform if you want to extend the functionality of the connector.
- [Chapter 5, "Known Issues and Limitations"](#) lists known issues and limitations associated with this release of the connector.





---

## Deploying the Connector

---

To deploy the connector, perform the procedures described in the following sections:

- [Section 2.1, "Preinstallation"](#)
- [Section 2.2, "Installation"](#)
- [Section 2.3, "Postinstallation"](#)

### 2.1 Preinstallation

This section is divided into the following topics:

- [Section 2.1.1, "Files and Directories That Comprise the Connector"](#)
- [Section 2.1.2, "Determining the Release Number of the Connector"](#)
- [Section 2.1.3, "Creating a Backup of the Existing Common.jar File"](#)
- [Section 2.1.4, "Removing RSA Authentication Manager JAR Files from the IBM WebSphere Application Server Home Directory"](#)

#### 2.1.1 Files and Directories That Comprise the Connector

[Table 2–1](#) describes the files and directories on the installation media.

**Table 2–1 Files and Directories On the Installation Media**

File in the Installation Media Directory	Description
configuration/RSAAuthManager-CI.xml	This XML file contains configuration information that is used during connector installation.
Files in the DataSets directory	These XML files specify the information to be submitted by the requester during a request-based provisioning operation. <b>Note:</b> These files will not be used if you are using Oracle Identity Manager release 11.1.2 or later.
documentation/Javadocs	This directory contains the Javadocs shipped with this connector.
lib/Common.jar	This JAR file contains the class files that are common to all connectors. During connector deployment, this file is copied into the following directory: <ul style="list-style-type: none"><li>■ For Oracle Identity Manager release 9.1.0.x: OIM_HOME/xellerate/ScheduleTask</li><li>■ For Oracle Identity Manager release 11.1.1 or 11.1.2.x: Oracle Identity Manager database</li></ul>

**Table 2–1 (Cont.) Files and Directories On the Installation Media**

File in the Installation Media Directory	Description
lib/RSAAuthManagerCommon.jar	<p>This JAR file contains the class files that is specific to this connector. During connector deployment, this file is copied into the following directory:</p> <ul style="list-style-type: none"> <li>For Oracle Identity Manager release 9.1.0.x: <i>OIM_HOME</i>/xellerate/JavaTasks</li> <li>For Oracle Identity Manager release 11.1.1 or 11.1.2.x: Oracle Identity Manager database</li> </ul>
lib/RSAAuthManager.jar	<p>This JAR file contains the class files that are used in connector operations. During connector deployment, this file is copied into the following directory:</p> <ul style="list-style-type: none"> <li>For Oracle Identity Manager release 9.1.0.x: <i>OIM_HOME</i>/xellerate/JavaTasks</li> <li>For Oracle Identity Manager release 11.1.1 or 11.1.2.x: Oracle Identity Manager database</li> </ul>
Files in the resources directory	<p>Each of these resource bundles contains language-specific information that is used by the connector. During connector deployment, this file is copied into the following directory:</p> <ul style="list-style-type: none"> <li>For Oracle Identity Manager release 9.1.0.x: <i>OIM_HOME</i>/xellerate/connectorResources</li> <li>For Oracle Identity Manager release 11.1.1 or 11.1.2.x: Oracle Identity Manager database</li> </ul> <p><b>Note:</b> A resource bundle is a file containing localized versions of the text strings that are displayed on the Administrative and User Console. These text strings include GUI element labels and messages.</p>
xml/RSA-AuthManager-ConnectorConfig.xml	<p>This XML file contains definitions of the various connector objects. These objects are created in Oracle Identity Manager when you run the Connector Installer.</p>

## 2.1.2 Determining the Release Number of the Connector

---

**Note:** If you are using Oracle Identity Manager release 9.1.0.x, then the procedure described in this section is optional.

If you are using Oracle Identity Manager release 11.1.1 to 11.1.2.x, then skip this section.

---

You might have a deployment of an earlier release of the connector. While deploying the latest release, you might want to know the release number of the earlier release. To determine the release number of the connector that has already been deployed:

1. In a temporary directory, extract the contents of the connector JAR file that is in the *OIM\_HOME*/xellerate/JavaTasks directory.
2. Open the Manifest.mf file in a text editor. The Manifest.mf file is one of the files bundled inside the connector JAR file.

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

### 2.1.3 Creating a Backup of the Existing Common.jar File

The Common.jar file is in the deployment package of each release 9.1.x connector. With each new release, code corresponding to that particular release is added to the existing code in this file. For example, the Common.jar file shipped with Connector Y on 12-July contains:

- Code specific to Connector Y
- Code included in the Common.jar files shipped with all other release 9.1.x connectors that were released before 12-July

If you have already installed a release 9.1.x connector that was released after the current release of the RSA Authentication Manager connector, then back up the existing Common.jar file, install the RSA Authentication Manager connector, and then restore the Common.jar file. The steps to perform this procedure are as follows:

---

**Caution:** If you do not perform this procedure, then your release 9.1.x connectors might not work.

---

1. Determine the release date of your existing release 9.1.x connector as follows:

- a. Extract the contents of the following file in a temporary directory:

*OIM\_HOME/xellerate/JavaTask/Common.jar*

---

**Note:** On Oracle Identity Manager release 11.1.1 and 11.1.2.x, use the Oracle Identity Manager Download JARs utility to download the Common.jar file from the database, and then extract the contents of this file into a temporary directory.

See *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for instructions about using the Download JARs utility.

---

- b. Open the Manifest.mf file in a text editor.
    - c. Note down the Build Date and Build Version values.
2. Determine the Build Date and Build Version values of the current release of the RSA Authentication Manager connector as follows:
  - a. On the installation media for the connector, extract the contents of the lib/Common.jar and then open the Manifest.mf file in a text editor.
  - b. Note down the Build Date and Build Version values.
3. If the Build Date and Build Version values for the RSA Authentication Manager connector are less than the Build Date and Build Version values for the connector that is installed, then:
  - If you are using Oracle Identity Manager release 9.1.0.x, then:
    - a. Copy the *OIM\_HOME/xellerate/JavaTasks/Common.jar* to a temporary location.
    - b. After you perform the procedure described in [Section 2.2, "Installation"](#) overwrite the new Common.jar file in the *OIM\_HOME/xellerate/JavaTasks* directory with the Common.jar file that you backed up in the preceding step.

- If you are using Oracle Identity Manager release 11.1.1 or 11.1.2.x, then run the Oracle Identity Manager Upload JARs utility to post the Common.jar file to the Oracle Identity Manager database. This utility is copied into the following location when you install Oracle Identity Manager:

---

**Note:** Before you run this utility, verify that the WL\_HOME environment variable is set to the directory in which Oracle WebLogic Server is installed.

---

**For Microsoft Windows:**

OIM\_HOME/server/bin/UploadJars.bat

**For UNIX:**

OIM\_HOME/server/bin/UploadJars.sh

When you run the utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host computer, context factory value, type of JAR file being uploaded, and the location from which the JAR file is to be uploaded. Specify 1 as the value of the JAR type.

**See Also:** *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for detailed information about the Upload JARs utility

## 2.1.4 Removing RSA Authentication Manager JAR Files from the IBM WebSphere Application Server Home Directory

---

**Note:** Perform the procedure described in this section only if your Oracle Identity Manager installation is running on IBM WebSphere Application Server.

---

Some of the following files might be present in the WEBSPHERE\_HOME/APPSERVER\_HOME/lib directory:

- com.bea.core.process\_5.3.0.0.jar
- wlfullclient.jar
- wlcipher.jar
- EccpressoAsn1.jar
- EccpressoCore.jar
- EccpressoJcae.jar

Stop the application server and then remove these files from the WEBSPHERE\_HOME/APPSERVER\_HOME/lib directory.

---

**Note:** If you run the Connector Installer while these files are present in the application server home directory, then you might encounter the following error:

java.net.MalformedURLException: no protocol: ddm-map.dtd

---

After you install the connector, you copy these JAR files back into the lib directory. The procedure is described later in this chapter.

## 2.2 Installation

---

---

### Note:

- In this guide, the term **Connector Installer** has been used to refer to the Connector Installer feature of the Oracle Identity Manager Administrative and User Console.
  - Ensure that the application server is running before you perform this procedure.
- 
- 

To run the Connector Installer:

1. Copy the contents of the connector installation media directory into the following directory:

---

---

**Note:** In an Oracle Identity Manager cluster, copy this JAR file to each node of the cluster.

---

---

- For Oracle Identity Manager release 9.1.0.x:  
OIM\_HOME/xellerate/ConnectorDefaultDirectory
  - For Oracle Identity Manager release 11.1.1 or 11.1.2.x:  
OIM\_HOME/server/ConnectorDefaultDirectory
2. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
    - For Oracle Identity Manager release 9.1.0.x:
      - a. Log in to the Administrative and User Console by using the user account described in the "Creating the User Account for Installing Connectors" section of *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.
      - b. Click **Deployment Management**, and then click **Install Connector**.
    - For Oracle Identity Manager release 11.1.1:
      - a. Log in to the Administrative and User Console by using the user account described in the "Creating the User Account for Installing Connectors" section of *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.
      - b. On the Welcome to Identity Manager Advanced Administration page, in the System Management region, click **Manage Connector**.
      - c. In the Manage Connector page, click **Install**.
    - For Oracle Identity Manager release 11.1.2.x:
      - a. Log in to Oracle Identity System Administration by using the user account described in the "Creating the User Account for Installing Connectors" section of *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

- b. In the left pane, under System Management, click **Manage Connector**.
  - c. In the Manage Connector page, click **Install**.
3. From the Connector List list, select **RSA Authentication Manager** *RELEASE\_NUMBER*. This list displays the names and release numbers of connectors whose installation files you copy into the default connector installation directory:

*OIM\_HOME*/xellerate/ConnectorDefaultDirectory

If you have copied the installation files into a different directory, then:

- a. In the **Alternative Directory** field, enter the full path and name of that directory.
  - b. To repopulate the list of connectors in the Connector List list, click **Refresh**.
  - c. From the Connector List list, select **RSA Authentication Manager**  
*RELEASE\_NUMBER*.
4. Click **Load**.
5. To start the installation process, click **Continue**.

The following tasks are performed in sequence:

- a. Configuration of connector libraries
- b. Import of the connector Target Resource user configuration XML file (by using the Deployment Manager).
- c. Compilation of adapters

On successful completion of a task, a check mark is displayed for the task. If a task fails, then an X mark and a message stating the reason for failure are displayed. Depending on the reason for failure, make the required correction and then perform one of the following steps:

- Retry the installation by clicking **Retry**.
    - Cancel the installation and begin again from Step 1.
6. If all three tasks of the connector installation process are successful, then a message indicating successful installation is displayed. In addition, a list of the steps that you must perform after the installation is displayed. These steps are as follows:
  - a. Ensuring that the prerequisites for using the connector are addressed

**Note:** At this stage, run the Oracle Identity Manager PurgeCache utility to load the server cache with content from the connector resource bundle in order to view the list of prerequisites. Refer to [Section 2.3.2, "Clearing Content Related to Connector Resource Bundles from the Server Cache"](#) for information about running the PurgeCache utility.

There are no prerequisites for some predefined connectors.

- b. Configuring the IT resource for the connector**
- Record the name of the IT resource displayed on this page. The procedure to configure the IT resource is described later in this guide.

- c. Configuring the scheduled tasks that are created when you installed the connector

---

**Note:** In Oracle Identity Manager release 11.1.1 and 11.1.2.x, a scheduled job is an instance of a scheduled task. In this guide, the term **scheduled task** used in the context of Oracle Identity Manager release 9.1.0.x is the same as the term **scheduled job** in the context of Oracle Identity Manager release 11.1.1 and 11.1.2.x.

See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about scheduled tasks and scheduled jobs.

---

Record the names of the scheduled tasks displayed on this page. The procedure to configure these scheduled tasks is described later in this guide.

When you run the Connector Installer, it copies the connector files and external code files to destination directories on the Oracle Identity Manager host computer. These files are listed in [Table 2-1](#).

---

**Note:**

- If required, revert to the earlier version of the Common.jar file. See [Section 2.1.3, "Creating a Backup of the Existing Common.jar File"](#) for more information.
  - The Connector Installer does not copy the contents of the documentation directory on the installation media. Manually copy these files to the required location.
- 

### Installing the Connector in an Oracle Identity Manager Cluster

---

**Note:** If you are using Oracle Identity Manager release 11.1.1 or 11.1.2.x then skip this section as it is not applicable.

---

While installing Oracle Identity Manager in a cluster, you must copy all the JAR files and the contents of the connectorResources directory into the corresponding directories on each node of the cluster. See [Table 2-1](#) for information about the files that you must copy and their destination locations on the Oracle Identity Manager host computer.

## 2.3 Postinstallation

The following sections discuss postinstallation procedures:

- [Section 2.3.1, "Changing to the Required Input Locale on the Oracle Identity Manager Host Computer"](#)
- [Section 2.3.2, "Clearing Content Related to Connector Resource Bundles from the Server Cache"](#)
- [Section 2.3.3, "Enabling Logging"](#)
- [Section 2.3.4, "Modifying Dependent Lookup Query Properties for Lookup Fields on Microsoft SQL Server"](#)

- [Section 2.3.5, "Addressing Prerequisites for Using the Java API of RSA Authentication Manager"](#)
- [Section 2.3.6, "Copying Target System Files to Oracle Identity Manager"](#)
- [Section 2.3.7, "Setting Values for JAVA\\_OPTIONS Parameters"](#)
- [Section 2.3.8, "Creating a Target System Account for Connector Operations"](#)
- [Section 2.3.9, "Mapping New Connection Properties"](#)
- [Section 2.3.10, "Setting Up the Configuration Lookup Definition in Oracle Identity Manager"](#)
- [Section 2.3.11, "Setting Up the Lookup.RSA.AuthManager.ExclusionList Lookup Definition"](#)
- [Section 2.3.12, "Modifying the Process Form"](#)
- [Section 2.3.13, "Configuring Connection Parameters"](#)
- [Section 2.3.14, "Creating Authorization Policies for User Management"](#)
- [Section 2.3.15, "Configuring Request-Based Provisioning"](#)
- [Section 2.3.16, "Configuring Oracle Identity Manager 11.1.2 or Later"](#)
- [Section 2.3.17, "Localizing Field Labels in UI Forms"](#)

## 2.3.1 Changing to the Required Input Locale on the Oracle Identity Manager Host Computer

---

---

**Note:** In an Oracle Identity Manager cluster, perform this procedure on each node of the cluster. Then, restart each node.

---

---

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.

## 2.3.2 Clearing Content Related to Connector Resource Bundles from the Server Cache

---

---

**Note:** In an Oracle Identity Manager cluster, perform this procedure on each node of the cluster. Then, restart each node.

---

---

When you deploy the connector, the resource bundles are copied from the resources directory on the installation media into the *OIM\_HOME/xellerate/connectorResources* directory for Oracle Identity Manager release 9.1.0.x, and Oracle Identity Manager database for Oracle Identity Manager release 11.1.1 and 11.1.2.x. Whenever you add a new resource bundle to 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, perform one of the following steps:



- If you are using Oracle Identity Manager release 9.1.0.x, then switch to the *OIM\_HOME/xellerate/bin* directory.
- If you are using Oracle Identity Manager release 11.1.1 or 11.1.2.x, then switch to the *OIM\_HOME/server/bin* directory.

---

**Note:** You must perform Step 1 before you perform Step 2. An exception is thrown if you run the command described in Step 2 as follows:

For Oracle Identity Manager release 9.1.0.x:

*OIM\_HOME/xellerate/bin/SCRIPT\_FILE\_NAME*

For Oracle Identity Manager release 11.1.1 or 11.1.2.x:

*OIM\_HOME/server/bin/SCRIPT\_FILE\_NAME*

---

## 2. Enter one of the following commands:

---

**Note:** You can use the PurgeCache utility to purge the cache for any content category. Run `PurgeCache.bat CATEGORY_NAME` on Microsoft Windows or `PurgeCache.sh CATEGORY_NAME` on UNIX. The *CATEGORY\_NAME* argument represents the name of the content category that must be purged.

For example, the following commands purge Metadata entries from the server cache:

`PurgeCache.bat MetaData`

`PurgeCache.sh MetaData`

---

- For Oracle Identity Manager release 9.1.0.x:  
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. This exception is different from the one mentioned in Step 1.

---

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

*OIM\_HOME/xellerate/config/xlconfig.xml*

- For Oracle Identity Manager release 11.1.1 or 11.1.2.x:  
On Microsoft Windows: `PurgeCache.bat All`  
On UNIX: `PurgeCache.sh All`

When prompted, enter the user name and password of an account belonging to the SYSTEM ADMINISTRATORS group. In addition, you are prompted to enter the service URL in the following format:

```
t3://OIM_HOST_NAME:OIM_PORT_NUMBER
```

In this format:

- Replace *OIM\_HOST\_NAME* with the host name or IP address of the Oracle Identity Manager host computer.
- Replace *OIM\_PORT\_NUMBER* with the port on which Oracle Identity Manager is listening.

See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about the PurgeCache utility.

## 2.3.3 Enabling Logging

Depending on the Oracle Identity Manager release you are using, perform instructions in one of the following sections:

- [Section 2.3.3.1, "Enabling Logging on Oracle Identity Manager Release 9.1.0.x"](#)
- [Section 2.3.3.2, "Enabling Logging on Oracle Identity Manager Release 11.1.1 and 11.1.2.x"](#)

### 2.3.3.1 Enabling Logging on Oracle Identity Manager Release 9.1.0.x

---

---

**Note:** In an Oracle Identity Manager cluster, perform this procedure on each node of the cluster. Then, restart each node.

---

---

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 messages that highlight the progress of the application at a 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 might 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:

#### ■ IBM WebSphere Application Server

To enable logging:

1. Add the following lines in the *OIM\_HOME/xellerate/config/log.properties* file:

```
log4j.logger.XELLERATE=log_level
log4j.logger.OIMCP.RSAM=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.OIMCP.RSAM=INFO
```

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

*WEBSPHHERE\_HOME/AppServer/logs/SERVER\_NAME/startServer.log*

#### ■ JBoss Application Server

To enable logging:

1. In the *JBOSS\_HOME/server/default/conf/jboss-log4j.xml* file, locate or add the following lines:

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

<category name="OIMCP.RSAM">
  <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="OIMCP.RSAM">
  <priority value="INFO"/>
</category>
```

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

*JBOSS\_HOME/server/default/log/server.log*

#### ■ Oracle Application Server

To enable logging:

1. Add the following lines in the *OIM\_HOME/xellerate/config/log.properties* file:

```
log4j.logger.XELLERATE=log_level
log4j.logger.OIMCP.RSAM=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.OIMCP.RSAM=INFO
```

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

*ORACLE\_HOME/opmn/logs/default\_group~home~default\_group~1.log*

#### ■ Oracle WebLogic Server

To enable logging:

1. Add the following lines in the *OIM\_HOME/xellerate/config/log.properties* file:

```
log4j.logger.XELLERATE=LOG_LEVEL
log4j.logger.OIMCP.RSAM=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.OIMCP.RSAM=INFO
```

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

*WEBLOGIC\_HOME/user\_projects/domains/DOMAIN\_NAME/SERVER\_NAME/SERVER\_NAME.log*

### 2.3.3.2 Enabling Logging on Oracle Identity Manager Release 11.1.1 and 11.1.2.x

Oracle Identity Manager uses Oracle Java Diagnostic Logging (OJDL) for logging. OJDL is based on *java.util.logger*. 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:

- *SEVERE.intValue()+100*  
This level enables logging of information about fatal errors.
- *SEVERE*  
This level enables logging of information about errors that might allow Oracle Identity Manager to continue running.
- *WARNING*  
This level enables logging of information about potentially harmful situations.
- *INFO*  
This level enables logging of messages that highlight the progress of the application.
- *CONFIG*  
This level enables logging of information about fine-grained events that are useful for debugging.
- *FINE, FINER, FINEST*  
These levels enable logging of information about fine-grained events, where *FINEST* logs information about all events.

These log levels are mapped to ODL message type and level combinations as shown in [Table 2–2](#).

**Table 2–2 Log Levels and ODL Message Type:Level Combinations**

Log Level	ODL Message Type:Level
SEVERE.intValue()+100	INCIDENT_ERROR:1
SEVERE	ERROR:1
WARNING	WARNING:1
INFO	NOTIFICATION:1
CONFIG	NOTIFICATION:16
FINE	TRACE:1
FINER	TRACE:16
FINEST	TRACE:32

The configuration file for OJDL is logging.xml, which is located at the following path:

*DOMAIN\_HOME*/config/fmwconfig/servers/*OIM\_SERVER*/logging.xml

Here, *DOMAIN\_HOME* and *OIM\_SERVER* are the domain name and server name specified during the installation of Oracle Identity Manager.

To enable logging in Oracle WebLogic Server:

1. Edit the logging.xml file as follows:

a. Add the following blocks in the file:

```
<log_handler name='rsam-handler' level='[LOG_LEVEL]'
class='oracle.core.ojdl.logging.ODLHandlerFactory'>
  <property name='logreader:' value='off' />
    <property name='path' value='[FILE_NAME]' />
    <property name='format' value='ODL-Text' />
    <property name='useThreadName' value='true' />
    <property name='locale' value='en' />
    <property name='maxFileSize' value='5242880' />
    <property name='maxLogSize' value='52428800' />
    <property name='encoding' value='UTF-8' />
  </log_handler>

<logger name="OIMCP.RSAM" level="[LOG_LEVEL]" useParentHandlers="false">
  <handler name="rsam-handler"/>
  <handler name="console-handler"/>
</logger>
```

b. Replace both occurrences of **[LOG\_LEVEL]** with the ODL message type and level combination that you require. [Table 2–2](#) lists the supported message type and level combinations.

Similarly, replace **[FILE\_NAME]** with the full path and name of the log file in which you want log messages to be recorded.

The following blocks show sample values for **[LOG\_LEVEL]** and **[FILE\_NAME]** :

```
<log_handler name='rsam-handler' level='NOTIFICATION:1'
class='oracle.core.ojdl.logging.ODLHandlerFactory'>
  <property name='logreader:' value='off' />
```

```

        <property name='path'
value='F:\MyMachine\middleware\user_projects\domains\base_domain1\servers\o
im_server1\logs\oim_server1-diagnostic-1.log' />
        <property name='format' value='ODL-Text' />
        <property name='useThreadName' value='true' />
        <property name='locale' value='en' />
        <property name='maxFileSize' value='5242880' />
        <property name='maxLogSize' value='52428800' />
        <property name='encoding' value='UTF-8' />
    </log_handler>

    <logger name="OIMCP.RSAM" level="NOTIFICATION:1" useParentHandlers="false">
        <handler name="rsam-handler" />
        <handler name="console-handler" />
    </logger>

```

With these sample values, when you use Oracle Identity Manager, all messages generated for this connector that are of a log level equal to or higher than the NOTIFICATION:1 level are recorded in the specified file.

2. Save and close the file.
3. Set the following environment variable to redirect the server logs to a file:

For Microsoft Windows:

```
set WLS_REDIRECT_LOG=FILENAME
```

For UNIX:

```
export WLS_REDIRECT_LOG=FILENAME
```

Replace **FILENAME** with the location and name of the file to which you want to redirect the output.

4. Restart the application server.

## 2.3.4 Modifying Dependent Lookup Query Properties for Lookup Fields on Microsoft SQL Server

---

### Note:

Perform the procedure described in this section only if your Oracle Identity Manager installation is running on Microsoft SQL Server.

In a clustered environment, perform this procedure on each node of the cluster. Then, restart each node.

---

In this connector, the child forms of a resource implement the dependent lookup feature of Oracle Identity Manager. [Table 2-3](#) lists the child forms shipped with this connector.

**Table 2-3** *Child Forms*

Child Form	Description
UD_AMROLE	RSA Auth Manager Role Form
UD_AMGROUP	RSA Auth Manager Group Form

By default, the queries for synchronization of lookup field values from the target system are based on Oracle Database SQL. If your Oracle Identity Manager installation is running on Microsoft SQL Server, then you must modify the lookup queries for synchronization of lookup definitions as follows:

1. To determine the field name of the **ITResourceLookupField** type from the parent form:
  - a. On the Design Console, expand **Development Tools** and double-click **Form Designer**.
  - b. Search for and open the **UD\_AMUSER** form. This is the parent form.
  - c. On the Additional Columns tab for the Parent form, search for the row containing the **ITResourceLookupField** field type and note down the value in the Name column for the row.

	Name	Variant Type	Length	Field Label	Field Type	Default Value	Order
1	UD_AMUSER_ITRESOURCE	long		Server Instance	ITResourceLookupField		1
2	UD_AMUSER_IDENTITY_SOURCE	String	255	Identity Source	LookupField		2
3	UD_AMUSER_SECURITY_DOMAIN	String	255	Security Domain	LookupField		3
4	UD_AMUSER_FIRST_NAME	String	255	First Name	TextField		4
5	UD_AMUSER_MIDDLE_NAME	String	255	Middle Name	TextField		5
6	UD_AMUSER_LAST_NAME	String	255	Last Name	TextField		6
7	UD_AMUSER_USER_ID	String	255	User ID	TextField		7
8	UD_AMUSER_PASSWORD	String	255	Password	PasswordField		8
9	UD_AMUSER_CERTIFICATE_DN	String	255	Certificate DN	TextField		9
10	UD_AMUSER_ACCOUNT_START_DATE	Date		Account Start Date	DateFieldDig		10
11	UD_AMUSER_ACCOUNT_START_HOURS	String	50	Account Start Hours	LookupField		11
12	UD_AMUSER_ACCNT_START_MINUTES	String	50	Account Start Minute	LookupField		12
13	UD_AMUSER_ACCOUNT_EXPIRE_DATE	Date		Account Expire Date	DateFieldDig		13
14	UD_AMUSER_ACCOUNT_EXPIRE_HOURS	String	50	Account Expire Hour	LookupField		14
15	UD_AMUSER_ACCNT_EXPIRE_MINUTES	String	50	Account Expire Minute	LookupField		15
16	UD_AMUSER_FIXED_PASSCODE_ALLOW	boolean	1	Fixed Passcode Allow	CheckBox		16

2. On the child forms, change the lookup field queries as follows:
  - a. Search for and open the **UD\_AMROLE** child form.
  - b. Click **Create New Version**.
  - c. Enter a version for the form, click the Save icon, and then close the dialog box.
  - d. On the Additional Columns tab, search for the lookup containing the **System Name** field label. Note down the value in the Name column.



**Form Designer**

**Table Information**

Table Name: **UD\_AMROLE** Form Type: ☒ Process ☐ Object

Description: RSA Auth Manager Role Form

Preview Form: [Button] Object Name: [Text Box]

**Version Information**

Latest Version: 1 Active Version: 1

Operations: Current Version: 1 [Dropdown] [Create New Version] [Make Version Active]

**Properties** | **Administrators** | **Usage** | **Pre-Populate** | **Default Columns** | **User Defined Fields**

Additional Columns		Child Table(s)		Object Permissions				
	Name	Variant Type	Length	Field Label	Field Type	Default Value	Order	Apply
1	UD_AMROLE_ROLENAME	String	255	Role Name	LookupField		1	

- e. Open the **Lookup Query** property for the Role Name column.

**Component Property**

Column Name: **Role Name** Column Type: **LookupField**

Property Name: **Lookup Query** Property Value: **select lkv\_encoded,lkv\_decoded from lkv lkv,lku lku where lkv.lku\_key=lku.lku\_key and lku\_type\_string\_key='Lookup.RSA.AuthManager.AdminRole' and CHARINDEX('\$Form data.UD\_AMUSER\_ITRESOURCE\$' + '~' , lkv\_encoded)>0**

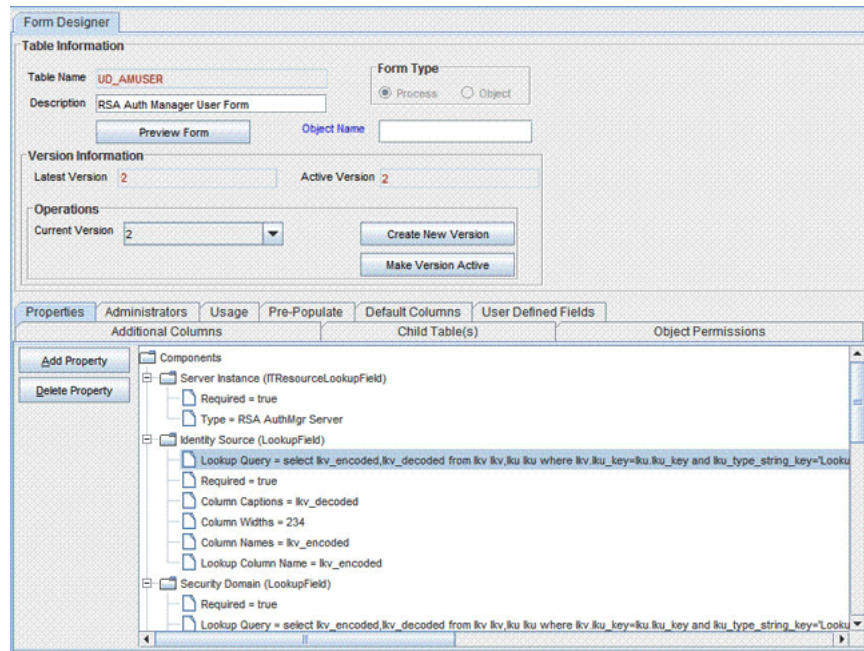
Filter Column: [Dropdown] Source: [Dropdown]

Field: [Dropdown]

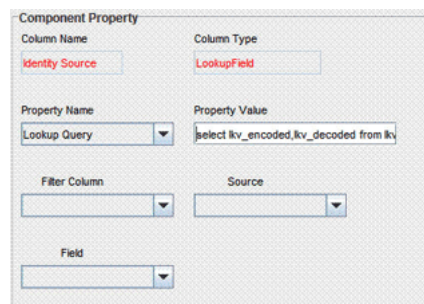
- f. Delete the contents of the **Property Value** field.
- g. Copy the following into the **Property Value** field:
- ```
select lkv_encoded,lkv_decoded from lkv lkv,lku lku where
lkv.lku_key=lku.lku_key and
lku_type_string_key='Lookup.RSA.AuthManager.AdminRole' and CHARINDEX('$Form
data.UD_AMUSER_ITRESOURCE$' + '~' , lkv_encoded)>0
```
- h. Click the Save icon and then close the dialog box.
- i. Click the Save icon to save the changes to the process form.
- j. From the **Current Version** list, select the version that you modified.
- k. Click **Make Version Active**.
- l. Click the Save icon.
- m. Perform the same procedure for the **UD\_AMGROUP** form. For this form, copy the following Microsoft SQL Server query in the Property Value field:
- ```
select lkv_encoded,lkv_decoded from lkv lkv,lku lku where
lkv.lku_key=lku.lku_key and
lku_type_string_key='Lookup.RSA.AuthManager.Group' and CHARINDEX('$Form
data.UD_AMUSER_ITRESOURCE$' + '~' , lkv_encoded)>0
```
3. For each parent form, change the lookup field queries as follows:
- a. Search for and open the **UD\_AMUSER** form.



- b. Click **Create New Version**.
- c. Enter a version for the form, click the Save icon, and then close the dialog box.
- d. On the Properties tab, double-click **Lookup Query** in the list of components.



- e. In the Edit Property dialog box, delete the contents of the **Property Value** field.



- f. Copy the following query into the **Property Value** field:  

```
select lkv_encoded, lkv_decoded from lkv lkv, lku lku where
lkv.lku_key = lku.lku_key and
lku_type_string_key = 'Lookup.RSA.AuthManager.IdentitySource' and
CHARINDEX('$Form data.UD_AMUSER_ITRESOURCE$' + '~', lkv_encoded) > 0
```
- g. Repeat Step 3 for the following forms and lookup fields:

Lookup Field and Form	Microsoft SQL Server Query
Security Domain field on UD_AMUSER	<pre>select lkv_encoded, lkv_decoded from lkv lkv, lku lku where lkv.lku_key = lku.lku_key and lku_type_string_key = 'Lookup.RSA.AuthManager.SecurityDomain' and CHARINDEX('\$Form data.UD_AMUSER_ITRESOURCE\$' + '~', , lkv_encoded) &gt; 0</pre>

**Lookup Field and Form****Microsoft SQL Server Query**

Identity source field on UD\_AMTOKEN

```
select lkv_encoded, lkv_decoded from lkv lkv, lku lku where
lkv.lku_key = lku.lku_key and
lku.type_string_key = 'Lookup.RSA.AuthManager.IdentitySource'
and CHARINDEX('$Form data.UD_AMTOKEN_ITRESOURCES$' +
'~', lkv_encoded) > 0
```

4. Associate the revised child forms with the parent forms as follows:
  - a. On the Child Tables tab, change the child form version to the version created earlier for the child forms.

The screenshot shows the 'Form Designer' window. The 'Table Information' section has 'Table Name' set to 'UD\_AMUSER' and 'Form Type' set to 'Process'. The 'Version Information' section shows 'Latest Version' and 'Active Version' both set to '2'. The 'Operations' section shows 'Current Version' set to '2'. The 'Child Table(s)' tab is selected, showing a table with columns: Parent Table, Parent Version, Child Table, and Child Version. The table contains two rows: (1, UD\_AMUSER, 2, UD\_AMROLE) and (2, UD\_AMUSER, 2, UD\_AMGROUP).

- b. Click **Make Version Active**.
- c. Click the Save icon.

## 2.3.5 Addressing Prerequisites for Using the Java API of RSA Authentication Manager

To enable the connector to work with the Java API of the target system, perform the following procedures:

- [Section 2.3.5.1, "Exporting and Importing the Server Root Certificate"](#)
- [Section 2.3.5.2, "Setting the Command Client User Name and Password"](#)

### 2.3.5.1 Exporting and Importing the Server Root Certificate

To export and then import the server root certificate:

1. On the RSA Authentication Manager computer, export the root certificate as follows:

- a. In a command window, change to the *RSA\_AM\_HOME*/appserver directory.
- b. Enter the following command:

```
jdk/jre/bin/keytool -export -keystore
RSA_AM_HOME/server/security/SERVER_NAME.jks -file am_root.cer -alias
rsa_am_ca
```

In this command:

- Replace *RSA\_AM\_HOME* with the full path of the directory in which RSA Authentication Manager is installed.
  - Replace *SERVER\_NAME* with the host name of the computer on which RSA Authentication Manager is installed.
- c. When prompted for the keystore password, press **Enter** without entering a password.

---

**Note:** Ignore the warning message. The server root certificate is exported at the path that you specify in the preceding step.

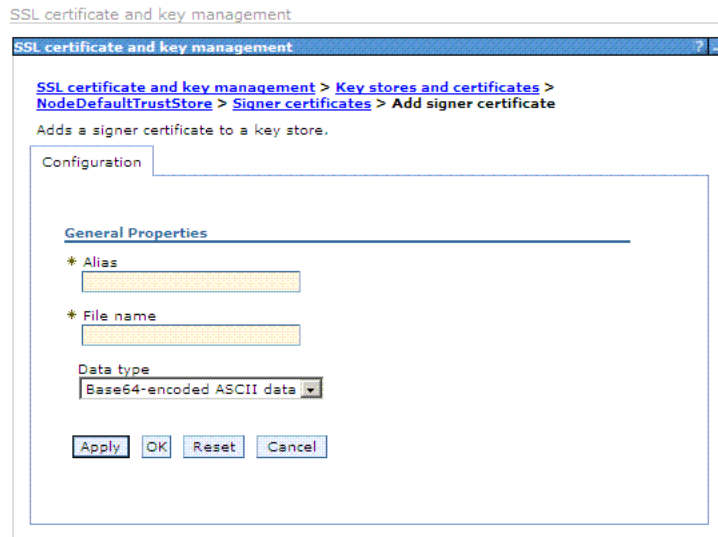
---

## 2. Import the server root certificate as follows:

- If you are using IBM Websphere Application Server, then perform the following procedure to import the certificate:
  - a. Locate the RSA Authentication Manger server root certificate file that you exported from RSA Authentication Manager, and copy it to the *WEBSPHERE\_HOME*/profiles/*SERVER\_NAME*/etc directory on the Oracle Identity Manager host computer.
  - b. Log in to the IBM WebSphere administrative console.
  - c. On the left pane, expand **Security** and select **SSL certificate and key management**.
  - d. Select **Key stores and certificates**, select **NodeDefaultTrustStore**, and then select **Signer certificates**.

Click **Add**.

The following page is displayed:

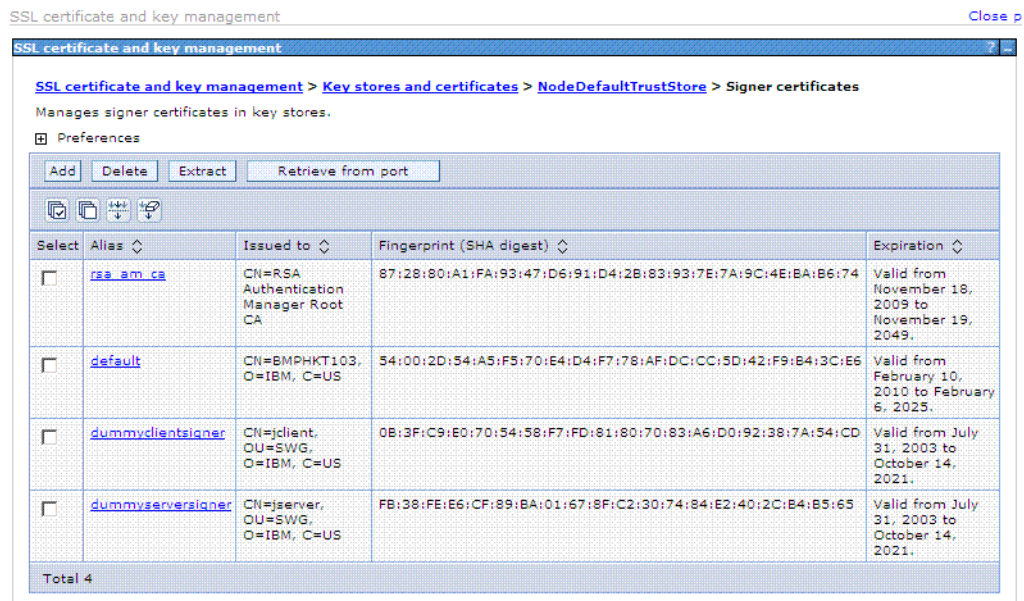


- e. In the **Alias** field, enter `rsa_am_ca`.
- f. In the **File Name** field, browse to the location where you exported the certificate.

For example: `C:\IBM\WebSphere\AppServer\profiles\AppSrv02\etc\am_root.cer`

- g. Click **OK**.

The Signer certificates should now include the new certificate you added. A page with information similar to the following is displayed:



- h. Select `rsa_am_ca`.

A page with information similar to the following is displayed:

The screenshot shows a web-based configuration interface for SSL certificates. The breadcrumb trail is: **SSL certificate and key management** > **Key stores and certificates** > **NodeDefaultTrustStore** > **Signer certificates** > **rsa\_am\_ca**. Below the breadcrumb, it says "Manages signer certificates in key stores." The "Configuration" tab is active, showing a "General Properties" section with the following fields:

Alias	rsa_am_ca
Version	3
Key size	2048
Serial number	-67068420573438650479159856395998769478
Validity period	Valid from November 18, 2009 to November 19, 2049.
Issued to	CN=RSA Authentication Manager Root CA
Issued by	CN=RSA Authentication Manager Root CA
Fingerprint (SHA digest)	87:28:80:A1:FA:93:47:D6:91:D4:2B:83:93:7E:7A:9C:4E:BA:B6:74
Signature algorithm	SHA1withRSA(1.2.840.113549.1.1.5)

At the bottom of the configuration area is a "Back" button.

- i. Click **Save**.
  - j. Restart the application server for the changes to take effect.
- If you are using JBoss Application Server, then perform the procedure described in the "Importing the Server Root Certificate (Java)" section of the RSA Authentication Manager 7.1 Developer's Guide.
  - If you are using Oracle Weblogic Server, then:
    - a. Perform the procedure described in the "Importing the Server Root Certificate (Java)" section of the RSA Authentication Manager 7.1 Developer's Guide.
    - b. Import the server root certificate into the keystore of Oracle WebLogic by running the following command:

```
keytool -import -alias ALIAS -keystore
WEBLOGIC_HOME/server/lib/DemoTrust.jks -file CERT_FILE_LOCATION
-storepass PASSWORD
```

In the preceding command, replace:

*ALIAS* with an alias for the RSA root certificate.

*CERT\_FILE\_LOCATION* with the full path and name of the certificate file.

*PASSWORD* is the password of the certificate keystore.

The following is a sample command:

```
keytool -import -alias rsa001 -keystore
D:\Oracle\Middleware\wlserver_10.3\server\lib\DemoTrust.jks -file
D:\Oracle\cert46\am_root.cer -storepass DemoTrustKeyStorePassPhrase
```

### 2.3.5.2 Setting the Command Client User Name and Password

Perform the procedure described in the "Setting the Command Client User Name and Password" section of the RSA Authentication Manager 7.1 Developer's Guide.

## 2.3.6 Copying Target System Files to Oracle Identity Manager

You must perform the following procedure to copy target system files:

1. Copy the following files from the RSA Authentication Manager installation directory into the *OIM\_HOME*/xellerate/ThirdParty directory if you are using Oracle Identity Manager release 9.1.0.x or the *OIM\_HOME*/server/ThirdParty directory if you are using Oracle Identity Manager release 11.1.1 or 11.1.2.x:

---

---

**Note:** *RSA\_AM\_HOME* is the directory in which RSA Authentication Manager is installed.

---

---

- *RSA\_AM\_HOME*/appserver/license.bea
- *RSA\_AM\_HOME*/appserver/modules/com.bea.core.process\_5.3.0.0.jar

---

---

**Note:** If you are using Oracle WebLogic Application Server, then the connector must use the JAR file that matches the one shipped with the application server.

---

---

- *RSA\_AM\_HOME*/appserver/weblogic/server/lib/wlfullclient.jar
  - *RSA\_AM\_HOME*/appserver/weblogic/server/lib/wlcipher.jar
  - *RSA\_AM\_HOME*/appserver/weblogic/server/lib/EccpressoAsn1.jar
  - *RSA\_AM\_HOME*/appserver/weblogic/server/lib/EccpressoCore.jar
  - *RSA\_AM\_HOME*/appserver/weblogic/server/lib/EccpressoJcae.jar
2. Copy the following files that are available in the *SDK\_HOME*/lib/java directory on the RSA Authentication Manager host computer to *OIM\_HOME*/xellerate/ThirdParty directory if you are using Oracle Identity Manager release 9.1.0.x or the *OIM\_HOME*/server/ThirdParty directory if you are using Oracle Identity Manager release 11.1.1 or 11.1.2.x:
    - am-client.jar
    - axis-1.3.jar
    - commons-beanutils-1.7.0.jar
    - commons-discovery-0.2.jar
    - commons-lang-2.2.jar
    - ims-client.jar
    - ims-server-o.jar
    - iScreen-1-1-0rsa-2.jar
    - iScreen-ognl-1-1-0rsa-2.jar
    - ognl-2.6.7.jar
    - spring-2.0.7.jar

---

**Note:** The SP level of SDK must match the SP level applied to the target system. For example, if RSA Authentication Manager 7.1 has been applied SP4 then SDK must be applied the same SP level, SP4.

---

3. If you are using RSA Authentication Manager 7.1 SP3 with Hot-Fix 2 or later versions, then:
  - a. Copy the `ims-client-patch.jar` file into the `OIM_HOME/xellerate/ThirdParty` directory if you are using Oracle Identity Manager release 9.1.0.x or the `OIM_HOME/server/ThirdParty` directory if you are using Oracle Identity Manager release 11.1.1 or 11.1.2.x. The `ims-client-patch.jar` file is available in the SDK directory in the RSA Auth Manager (Hot fix Upgrade) installation media.
  - b. Include the `ims-client-patch.jar` file in the classpath ahead of the `am-client.jar` and `ims-client.jar` files.
4. Depending on the application server that you are using, copy all files listed in steps 1 and 2 (except `RSA_AM_HOME/appserver/license.bea`) from the `RSA_AM_HOME/appserver` and `SDK_HOME/lib/java` directories into the following directories:

- **For IBM Websphere Application Server**

Copy the JAR files into the `WEBSphere_HOME/APPSEVER_HOME/lib` directory.

In addition, perform the following procedure:

- a. In a text editor, open the `WEBSphere_HOME/profiles/AppSrv02/bin/setupCmdLine.sh` (or `setupCmdLine.cmd`) file.
- b. In this file, search for the `WAS_CLASSPATH` variable.
- c. To the current value of the `WAS_CLASSPATH` variable, add each of the JAR files that you copied earlier in this section.

For example:

```
WAS_CLASSPATH=%WAS_HOME%\properties;%WAS_HOME%\lib\startup.jar;%WAS_HOME%\lib\bootstrap.jar;%WAS_HOME%\lib\j2ee.jar;%WAS_HOME%\lib\lmpoxy.jar;%WAS_HOME%\lib\urlprotocols.jar;%JAVA_HOME%\lib\tools.jar;%WAS_HOME%\lib\license.bea;%WAS_HOME%\lib\wlcipher.jar;%WAS_HOME%\lib\wlfclient.jar;%WAS_HOME%\lib\com.bea.core.process_5.3.0.0.jar;%WAS_HOME%\lib\EccpressoAsn1.jar;%WAS_HOME%\lib\EccpressoCore.jar;%WAS_HOME%\lib\EccpressoJcae.jar;%WAS_HOME%\lib\am-client.jar;%WAS_HOME%\lib\ims-client.jar;%WAS_HOME%\lib\spring-2.0.7.jar;%WAS_HOME%\lib\iScreen-1-1-0rsa-2.jar;%WAS_HOME%\lib\iScreen-ognl-1-1-0rsa-2.jar;%WAS_HOME%\lib\ognl-2.6.7.jar;%WAS_HOME%\lib\ims-server-o.jar;%WAS_HOME%\lib\commons-lang-2.3.jar;%WAS_HOME%\lib\axis-1.3.jar;%WAS_HOME%\lib\commons-discovery-0.2.jar;%WAS_HOME%\lib\commons-beanutils-1.7.0.jar
```

- d. Save and close the file.
- e. Restart the server for the changes to take effect.

- **For JBoss Application Server**

Copy the JAR files into the `JBoss_HOME/server/default/lib` directory of the application server installation directory. Restart the server for the changes to take effect.

- **For Oracle Application Server**

Copy the JAR files into the *ORACLE\_HOME/j2ee/home/lib* directory.

In addition, perform the following procedure:

- a. Copy the *log4j-1.2.11rsa-3.jar* and *commons-logging-1.0.4.jar* files from the *SDK\_HOME/lib/java* directory into the *ORACLE\_HOME/j2ee/home/lib* directory.
- b. Extract the contents of the *ORACLE\_HOME/j2ee/home/oc4j.jar* file into a temporary directory.
- c. In a text editor, open the *boot.xml* file. This is one of the files in the *oc4j.jar* file.
- d. Add the following lines under the `<system-class-loader>` element in the *boot.xml* file:

```
<code-source path="lib/am-client.jar"/>
<code-source path="lib/axis-1.3.jar"/>
<code-source path="lib/com.bea.core.process_5.3.0.0.jar"/>
<code-source path="lib/commons-beanutils-1.7.0.jar"/>
<code-source path="lib/commons-discovery-0.2.jar"/>
<code-source path="lib/commons-lang-2.3.jar"/>
<code-source path="lib/EccpressoAsn1.jar"/>
<code-source path="lib/EccpressoCore.jar"/>
<code-source path="lib/EccpressoJcae.jar"/>
<code-source path="lib/ims-client.jar"/>
<code-source path="lib/ims-server-o.jar"/>
<code-source path="lib/iScreen-1-1-0rsa-2.jar"/>
<code-source path="lib/iScreen-ognl-1-1-0rsa-2.jar"/>
<code-source path="lib/ognl-2.6.7.jar"/>
<code-source path="lib/spring-2.0.7.jar"/>
<code-source path="lib/wlcipher.jar"/>
<code-source path="lib/wlfullclient.jar"/>
<code-source path="lib/log4j-1.2.11rsa-3.jar"/>
<code-source path="lib/commons-logging-1.0.4.jar"/>
```

- e. Re-create the *oc4j.jar* file and copy it into the *ORACLE\_HOME/j2ee/home* directory.
- f. Restart the server for the changes to take effect.

- **For Oracle WebLogic Server**

Copy the JAR files into the *WEBLOGIC\_DOMAIN\_HOME/lib* directory.

Restart the server for the changes to take effect.

## 2.3.7 Setting Values for JAVA\_OPTIONS Parameters

*MaxMessageSize* is one of the *JAVA\_OPTIONS* parameters. You must set this parameter to a value that is high enough to handle the maximum number of user and token records that you expect the connector to process during reconciliation.

In addition, if you are using JDK 1.6, then you must set the *allowArraySyntax* *JAVA\_OPTIONS* parameter to *true*.

The procedure to configure *JAVA\_OPTIONS* parameters depends on the application server that you are using:

- [Section 2.3.7.1, "Setting Values for JAVA\\_OPTIONS Parameters on IBM WebSphere Application Server"](#)



- [Section 2.3.7.2, "Setting Values for JAVA\\_OPTIONS Parameters on JBoss Application Server"](#)
- [Section 2.3.7.3, "Setting Values for JAVA\\_OPTIONS Parameters on Oracle Application Server"](#)
- [Section 2.3.7.4, "Setting Values for JAVA\\_OPTIONS Parameters on Oracle WebLogic Server"](#)

### 2.3.7.1 Setting Values for JAVA\_OPTIONS Parameters on IBM WebSphere Application Server

To configure the `MaxMessageSize` and `allowArraySyntax` JAVA\_OPTIONS parameters on IBM WebSphere Application Server:

1. Log in to the administrative console.
2. Expand **Servers**, and click **Application servers**.
3. On the page that is displayed, click the name of the application server instance.
4. On the page that is displayed, expand **Java and Process Management**, click **Process Definition**, and then select **Java Virtual Machine**.
5. Add the following in the generic JVM arguments list:

```
-Dweblogic.MaxMessageSize= MAX_MESSAGE_SIZE
```

For example:

```
-Dweblogic.MaxMessageSize=40000000
```

6. If you are using the JDK 1.6, then you must also add the `Dsun.lang.ClassLoader.allowArraySyntax` parameter in the generic JVM arguments list:

```
-Dsun.lang.ClassLoader.allowArraySyntax=true
```

7. Click **Save**, and then restart the server for the changes to take effect.

### 2.3.7.2 Setting Values for JAVA\_OPTIONS Parameters on JBoss Application Server

To set values for the `MaxMessageSize` and `allowArraySyntax` JAVA\_OPTIONS parameters on JBoss Application Server:

1. In a text editor, open the `JBOSS_HOME/bin/run.sh` (or `run.bat`) file.
2. In this file, search for the `JAVA_OPTS` variable.

The line containing this variable would be similar to the following:

```
rem JAVA_OPTS=%JAVA_OPTS% -Dsun.rmi.dgc.client.gcInterval=3600000
-Dsun.rmi.dgc.server.gcInterval=3600000
```

3. To this line, add the `Dbea.home` and `Dweblogic` parameters as shown here:

```
set JAVA_OPTS=%JAVA_OPTS% -Dsun.rmi.dgc.client.gcInterval=3600000
-Dsun.rmi.dgc.server.gcInterval=3600000
-Dbea.home=OIM_HOME/xellerate/ThirdParty
-Dweblogic.MaxMessageSize=MAX_MESSAGE_SIZE
```

For example:

```
set JAVA_OPTS=%JAVA_OPTS% -Dsun.rmi.dgc.client.gcInterval=3600000
-Dsun.rmi.dgc.server.gcInterval=3600000
```

```
-Dbea.home=/oimserver/xellerate/ThirdParty -Dweblogic.MaxMessageSize=40000000
```

4. If you are using JDK 1.6, then you must also add the `Dsun.lang.ClassLoader.allowArraySyntax` parameter as follows:

```
set JAVA_OPTS=%JAVA_OPTS% -Dsun.rmi.dgc.client.gcInterval=3600000
-Dsun.rmi.dgc.server.gcInterval=3600000
-Dbea.home=OIM_HOME/xellerate/ThirdParty
-Dweblogic.MaxMessageSize=MAX_MESSAGE_SIZE
-Dsun.lang.ClassLoader.allowArraySyntax=true
```

For example:

```
set JAVA_OPTS=%JAVA_OPTS% -Dsun.rmi.dgc.client.gcInterval=3600000
-Dsun.rmi.dgc.server.gcInterval=3600000
-Dbea.home=/oimserver/xellerate/ThirdParty -Dweblogic.MaxMessageSize=40000000
-Dsun.lang.ClassLoader.allowArraySyntax=true
```

5. Save and close the file.
6. Restart the server for the changes to take effect.

### 2.3.7.3 Setting Values for JAVA\_OPTIONS Parameters on Oracle Application Server

To set values for the `MaxMessageSize` and `allowArraySyntax` JAVA\_OPTIONS parameters on Oracle Application Server:

1. In a text editor, open the following file:  
`ORACLE_HOME/opmn/conf/opmn.xml` file.
2. In the `opmn.xml` file, add the following in the `<data id="java-options" value="-Xrs">` tag under the `<category id="start-parameters"><ias-component id="default_group">` tag:  
`-Dweblogic.MaxMessageSize=MAX_MESSAGE_SIZE`

For example:

```
<category id="start-parameters">
<data id="java-options" value="-Xrs -DXL.HomeDir=D:\OC4J0IM\Server\xellerate
-Dlog4j.configuration=file:D:\OC4J0IM\Server\xellerate/config/log.properties
-server -XX:MaxPermSize=128M -ms512M -mx1024M -XX:AppendRatio=3
-Djava.security.policy=$ORACLE_HOME/j2ee/home/config/java2.policy
-Djava.awt.headless=true -Dhttp.webdir.enable=false
-Doraesb.home=D:\product\10.1.3.1\OracleAS_3\integration\esb
-Dhttp.proxySet=false -Doc4j.userThreads=true -Doracle.mdb.fastUndeploy=60
-Dorabpel.home=D:\product\10.1.3.1\OracleAS_3\bpel
-Xbootclasspath^/p:D:\product\10.1.3.1\OracleAS_3\bpel/lib/orabpel-boot.jar
-Dhttp.proxySet=false -Dweblogic.MaxMessageSize=40000000"/>
</category>
```

3. If you are using JDK 1.6, then you must also add the `Dsun.lang.ClassLoader.allowArraySyntax` parameter in the `opmn.xml` file as follows:

```
-Dsun.lang.ClassLoader.allowArraySyntax=true
```

4. Save and close the file.
5. Restart the server for the changes to take effect.

### 2.3.7.4 Setting Values for JAVA\_OPTIONS Parameters on Oracle WebLogic Server

To set values for the `MaxMessageSize` and `allowArraySyntax` JAVA\_OPTIONS parameters on Oracle WebLogic Server:

1. In a text editor, open the following file:

```
WEBLOGIC_HOME/user_projects/domains/DOMAIN_NAME/bin/xlStartWLS.sh (or
xlStartWLS.cmd)
```

2. Add the following to the JAVA\_OPTIONS section of the xlStartWLS file:

```
-Dweblogic.MaxMessageSize=MAX_MESSAGE_SIZE
```

For example:

```
JAVA_OPTIONS="-DXL.HomeDir=$XLHOME
-Djava.security.auth.login.config=$XLHOME/config/authwl.conf
-Dlog4j.configuration=file:$XLHOME/config/log.properties
-Djava.awt.headless=true -Doracle.jdbc.mapDateToTimestamp=false
-Dweblogic.MaxMessageSize=40000000"
```

3. If you are using the JDK 1.6, then you must also add the `Dsun.lang.ClassLoader.allowArraySyntax` parameter as follows:

```
-Dsun.lang.ClassLoader.allowArraySyntax=true
```

For example:

```
JAVA_OPTIONS="-DXL.HomeDir=$XLHOME
-Djava.security.auth.login.config=$XLHOME/config/authwl.conf
-Dlog4j.configuration=file:$XLHOME/config/log.properties
-Djava.awt.headless=true -Doracle.jdbc.mapDateToTimestamp=false
-Dweblogic.MaxMessageSize=40000000
-Dsun.lang.ClassLoader.allowArraySyntax=true"
```

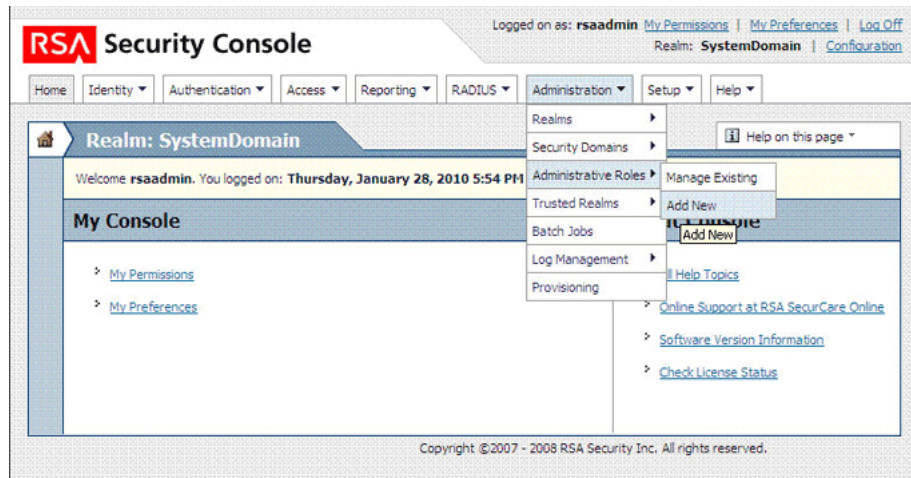
4. Save and close the file.
5. Restart the server for the changes to take effect.

## 2.3.8 Creating a Target System Account for Connector Operations

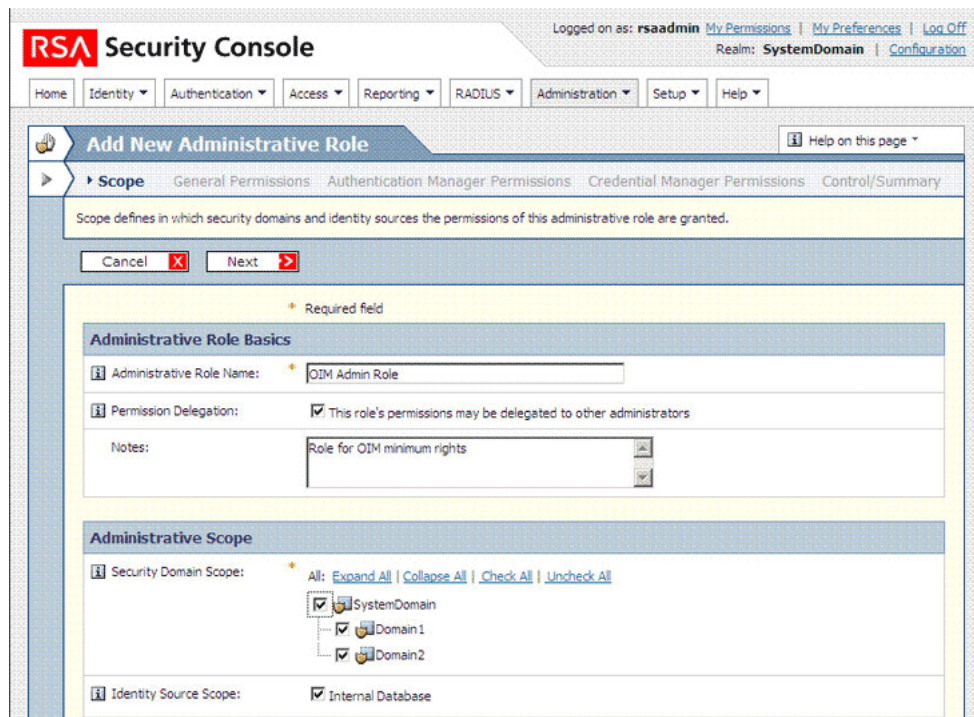
The connector uses a target system account to perform reconciliation and provisioning operations on the target system. To create this account:

1. Log in to the RSA Security Console.
2. Create a role having the permissions required for connector operations:
  - a. Expand the **Administration** list, select **Administrative Roles**, and then select **Add New**.

The following screenshot shows this page:



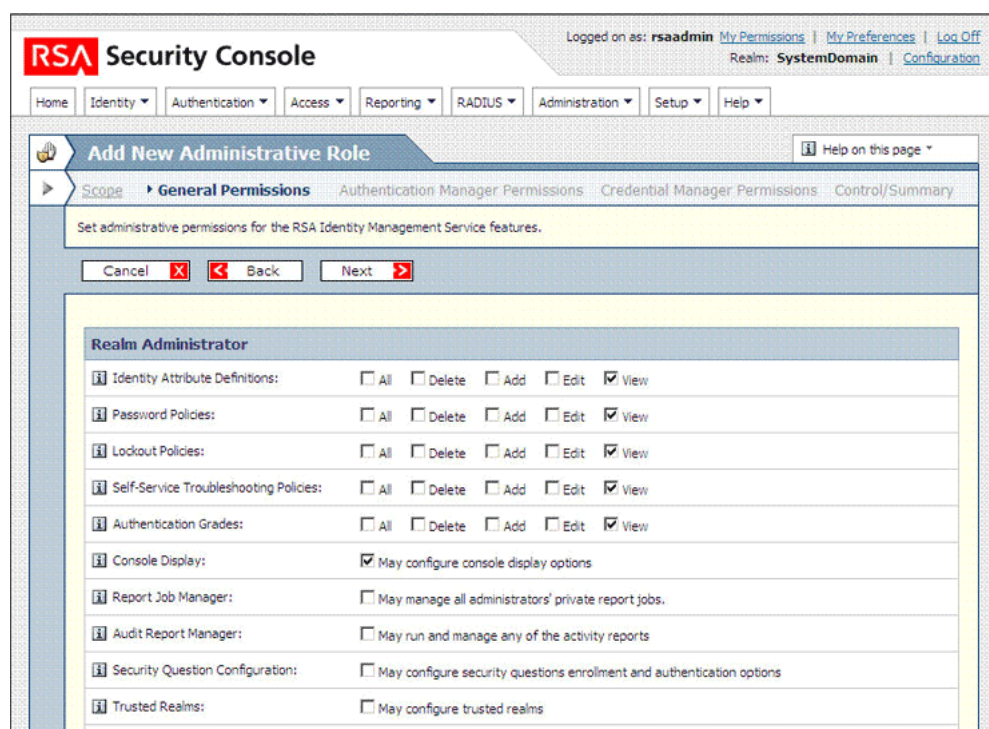
- b. In the **Administrative Role Name** field, enter a name for the role.
- c. Select the **Permission Delegation** check box.
- d. In the **Notes** field, enter a description for the role.
- e. In the Administrative Scope region:
  - Select the security domains that you want to include in the scope for connector operations.
  - Select the identity source that you want to include in the scope for connector operations.



- f. Click **Next**.
- g. In the Realm Administrator region of the General Permissions page, select the **View** check box for the following permissions:

- Identity Attribute Definitions
- Password Policies
- Lockout Policies
- Self-Service Troubleshooting Policies
- Authentication Grades
- Console Display
- SecurID Token Policies
- Offline Authentication Policies

The following screenshot shows the first part of this page:



- h. In the Manage Delegated Administration region, select the following permissions:
  - View check box for Security Domains
  - View check box for Administrative Roles
  - Assign Administrative Roles
- i. In the Manage Users region, select the **All**, **Delete**, **Add**, **Edit**, and **View** check boxes.
- j. In the Manage User Groups region, select the **Assign User Group Membership** check box.
- k. In the Manage Reports region, select the **View** check box for the Reports permission.

The following screenshot shows the second part of this page:



Administrative Roles:	<input type="checkbox"/> All <input type="checkbox"/> Delete <input type="checkbox"/> Add <input type="checkbox"/> Edit <input checked="" type="checkbox"/> View
Assign Administrative Roles:	<input checked="" type="checkbox"/> May assign administrative roles to users
<b>Manage Users</b>	
Users:	<input checked="" type="checkbox"/> All <input checked="" type="checkbox"/> Delete <input checked="" type="checkbox"/> Add <input checked="" type="checkbox"/> Edit <input checked="" type="checkbox"/> View
Reset Passwords:	<input checked="" type="checkbox"/> May reset passwords
Enable/Disable Accounts:	<input checked="" type="checkbox"/> May enable and disable accounts
Terminate Active Sessions:	<input checked="" type="checkbox"/> May terminate active user sessions
User Attribute Restriction:	<input type="checkbox"/> May manage attribute categories <input type="checkbox"/> May only access specific user attributes:
User Scope Restriction:	<input type="checkbox"/> May only manage users that match a condition:
<b>Manage User Groups</b>	
User Groups:	<input type="checkbox"/> All <input type="checkbox"/> Delete <input type="checkbox"/> Add <input type="checkbox"/> Edit <input checked="" type="checkbox"/> View
Assign User Group Membership:	<input checked="" type="checkbox"/> May assign user group membership
<b>Manage Reports</b>	
Reports:	<input type="checkbox"/> All <input type="checkbox"/> Delete <input type="checkbox"/> Add <input type="checkbox"/> Edit <input checked="" type="checkbox"/> View
Run Reports:	<input type="checkbox"/> May run and schedule report jobs
<input type="button" value="Cancel"/> <input type="button" value="Back"/> <input type="button" value="Next"/>	

Copyright ©2007 - 2008 RSA Security Inc. All rights reserved.

- i. Click **Next**.
  - m. For the SecurID Tokens permission on the Manage RSA SecurID Tokens page, select the **Edit** and **View** check boxes.
  - n. Select the check boxes for the Assign Tokens and Distribute Software Tokens permissions.
  - o. Select the **View** check box for the Token Attribute Definitions permission.
- The following screenshot shows the first part of this page:

**RSA Security Console** Logged on as: **rsaadmin** [My Permissions](#) | [My Preferences](#) | [Log Off](#)  
 Realm: **SystemDomain** | [Configuration](#)

Home Identity Authentication Access Reporting RADIUS Administration Setup Help

**Add New Administrative Role** [Help on this page](#)

Scope General Permissions **Authentication Manager Permissions** Credential Manager Permissions Control/Summary

Set administrative permissions for the RSA Identity Management Service features.

<b>Manage RSA SecurID Tokens</b>	
SecurID Tokens:	<input type="checkbox"/> All <input type="checkbox"/> Delete <input type="checkbox"/> Add <input checked="" type="checkbox"/> Edit <input checked="" type="checkbox"/> View
Reset PINs:	<input checked="" type="checkbox"/> May clear and require users to change SecurID PINs
Enable/Disable Tokens:	<input checked="" type="checkbox"/> May enable and disable SecurID tokens
Manage Token Emergency Access:	<input checked="" type="checkbox"/> May manage offline token emergency access
Manage Online Token Emergency Access:	<input checked="" type="checkbox"/> May manage online token emergency access
Resynchronize Tokens:	<input checked="" type="checkbox"/> May resynchronize SecurID Tokens
Replace Tokens:	<input type="checkbox"/> May replace assigned tokens
Assign Tokens:	<input checked="" type="checkbox"/> May assign tokens to users
Distribute Software Tokens:	<input checked="" type="checkbox"/> May distribute assigned software tokens to users
Token Attribute Definitions:	<input type="checkbox"/> All <input type="checkbox"/> Delete <input type="checkbox"/> Add <input type="checkbox"/> Edit <input checked="" type="checkbox"/> View

- p. Select the **SID-800 Smart Card Details** check box.
- q. In the Manage User Groups region, select the **View** check box for the User Group Restricted Access permission.
- r. In the Manage User Authentication Attributes region, select the following check boxes:
  - **Edit** and **View** check boxes for the Fixed Passcode permission
  - **Manage Windows Password Integration**
  - **Manage Incorrect Password Count**
  - **Edit** and **View** check boxes for the Default Shell permission
- s. In the Manage Authentication Agents region, select the **View** check box for the Authentication Agent permission.
- t. In the Trusted Realm Management region, select the following check boxes
  - **View** check box for the Trusted Users permission
  - **View** check box for the Trusted User Groups permission
  - **View** check box for the Trusted User Group Restricted Access permission

The following screenshot shows the second part of this page:

The screenshot displays a configuration interface with several sections:

- Token Attribute Definitions:**
  - ☐ All ☐ Delete ☐ Add ☐ Edit ☒ View
  - ☒ SID-800 Smart Card Details: ☒ May import and manage smart card details including PIN unlocking key
- Manage User Groups:**
  - ☐ User Group Restricted Access: ☐ All ☐ Edit ☒ View
- Manage User Authentication Attributes:**
  - ☒ Fixed Passcode: ☒ Edit ☒ View
  - ☒ Manage Windows Password Integrations: ☒ May manually clear cached copy of user's Windows credentials
  - ☒ Manage Incorrect Passcode Count: ☒ May manage incorrect passcode count
  - ☒ Default Shell: ☒ Edit ☒ View
  - ☐ Logon Aliases: ☐ Edit ☐ View
  - ☐ Manage Offline Emergency Access Passcode: ☐ May manage offline emergency access passcode
- Manage Authentication Agents:**
  - ☐ Authentication Agent: ☐ All ☐ Delete ☐ Add ☐ Edit ☒ View
  - ☐ Grant Access to Restricted Agents: ☐ May grant user groups access to restricted authentication agents
  - ☐ Manage Node Secret: ☐ May manage the shared secret between the authentication agent and the authentication manager
- Trusted Realm Management:**
  - ☐ Trusted Users: ☐ All ☐ Delete ☐ Add ☐ Edit ☒ View

- u. Select the check box in the Manage On-Demand Tokencodes region.
- v. Click **Next**.

The following screenshot shows the third part of this page:

Trusted Users:	<input type="checkbox"/> All <input type="checkbox"/> Delete <input type="checkbox"/> Add <input type="checkbox"/> Edit <input checked="" type="checkbox"/> View
Trusted User Groups:	<input type="checkbox"/> All <input type="checkbox"/> Delete <input type="checkbox"/> Add <input type="checkbox"/> Edit <input checked="" type="checkbox"/> View
Trusted User Group Restricted Access:	<input type="checkbox"/> All <input type="checkbox"/> Edit <input checked="" type="checkbox"/> View
Grant Trusted User Group Access to Trusted Users:	<input type="checkbox"/> May assign trusted used group memberships
Grant Trusted User Group Access to Agents:	<input type="checkbox"/> May grant trusted used groups access to agents

### Manage RADIUS

RADIUS Servers:	<input type="checkbox"/> All <input type="checkbox"/> Delete <input type="checkbox"/> Edit <input type="checkbox"/> View
RADIUS Clients:	<input type="checkbox"/> All <input type="checkbox"/> Delete <input type="checkbox"/> Add <input type="checkbox"/> Edit <input type="checkbox"/> View
RADIUS Profiles:	<input type="checkbox"/> All <input type="checkbox"/> Delete <input type="checkbox"/> Add <input type="checkbox"/> Edit <input type="checkbox"/> View
Assign User RADIUS Profile:	<input type="checkbox"/> May assign a RADIUS profile to a user
Assign Agent RADIUS Profile:	<input type="checkbox"/> May assign a RADIUS profile to an agent
RADIUS Realm Settings:	<input type="checkbox"/> All <input type="checkbox"/> Delete <input type="checkbox"/> Add <input type="checkbox"/> Edit <input type="checkbox"/> View
RADIUS User Attribute Definitions:	<input type="checkbox"/> All <input type="checkbox"/> Delete <input type="checkbox"/> Add <input type="checkbox"/> Edit <input type="checkbox"/> View
RADIUS User Attributes:	<input type="checkbox"/> Edit <input type="checkbox"/> View

### Manage On-Demand Tokencodes

Manage On-Demand Tokencodes:	<input checked="" type="checkbox"/> May enable and disable users for On-Demand Tokencodes and provision associated PIN
------------------------------	--

Cancel [X] Back Next

- w. On the Credential Manager Permissions page, click **Next**.

The following screenshot shows this page:

Logged on as: **rsaadmin** [My Permissions](#) | [My Preferences](#) | [Log Off](#)  
 Realm: **SystemDomain** | [Configuration](#)

Home Identity Authentication Access Reporting RADIUS Administration Setup Help

## Add New Administrative Role

Help on this page

Scope General Permissions Authentication Manager Permissions **Credential Manager Permissions** Control/Summary

Set administrative permissions for the RSA Identity Management Service features.

Cancel [X] Back Next

### Provisioning Requests

Requests:	<input type="checkbox"/> All <input type="checkbox"/> View <input type="checkbox"/> Approve <input type="checkbox"/> Distribute <input type="checkbox"/> Cancel
-----------	---

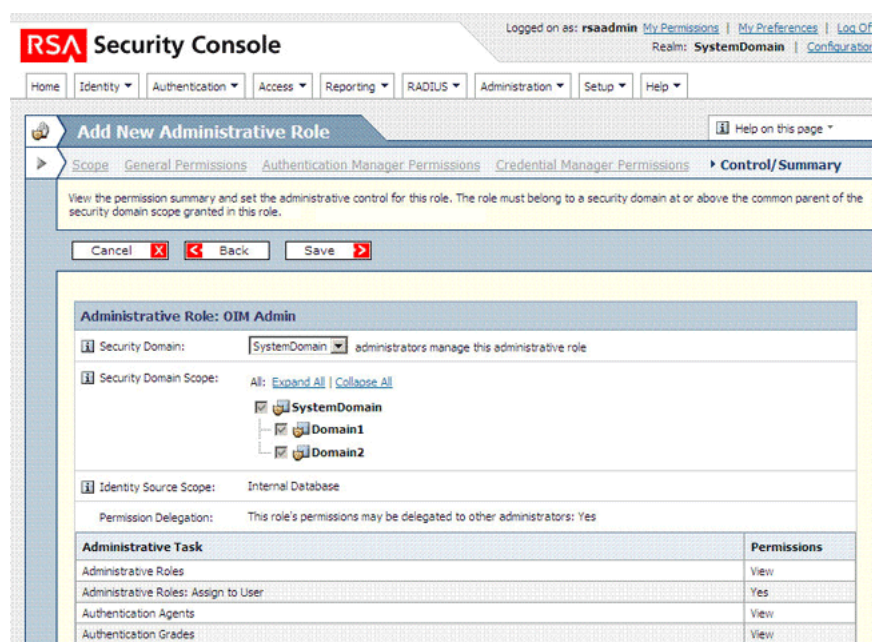
Cancel [X] Back Next

Copyright © 2007 - 2008 RSA Security Inc. All rights reserved.

- x. On the Control/Summary page, review the summary of permissions and then click **Save**.

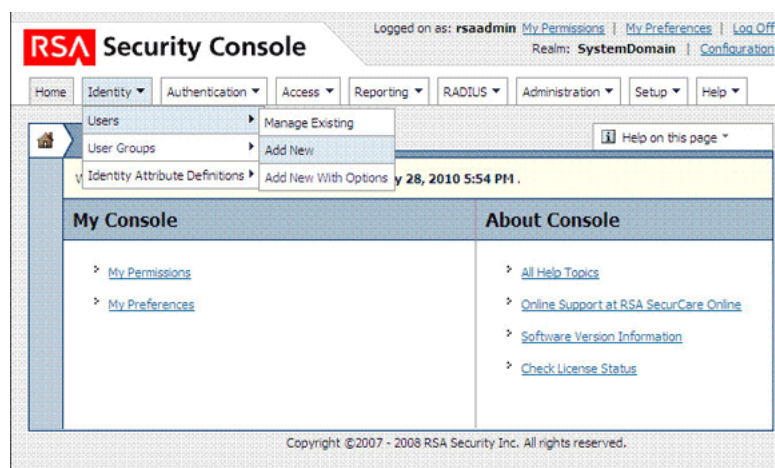
The following screenshot shows the first part of this page:





3. Create a user and assign the role to the user as follows:
  - a. Expand the Identity list, select **Users**, and then select **Add New**.

The following screenshot shows this page:



- b. On the Add New User page, enter the required values and then click **Save**.

---

#### Note:

The user ID and password that you enter on this page must be provided as the values of the Admin UserID and Admin Password IT resource parameters. [Section 2.3.13, "Configuring Connection Parameters"](#) describes these parameters.

In the Account Information region, select the No expiration date check box.

---

The following screenshot shows this page:

Logged on as: **rsaadmin** | [My Permissions](#) | [My Preferences](#) | [Log Off](#)  
 Realm: **SystemDomain** | [Configuration](#)

Home Identity Authentication Access Reporting RADIUS Administration Setup Help

### Add New User

A user represents a person or a system with a unique account within this realm.

Cancel Save Save & Add Another

\* Required field

**Administrative Control**

Identity Source: Internal Database  
 Security Domain: SystemDomain administrators manage this user

**User Basics**

First Name: OIM Admin  
 Middle Name:   
 Last Name: OIM Admin  
 User ID: oimadmin  
 Email:   
 Certificate DN:   
 Notes:

- c. Use the Search feature to open the details of the newly created user.  
 The following screenshot shows this page:

Logged on as: **rsaadmin** | [My Permissions](#) | [My Preferences](#) | [Log Off](#)  
 Realm: **SystemDomain** | [Configuration](#)

Home Identity Authentication Access Reporting RADIUS Administration Setup Help

### Users

A user represents a person or a system with a unique account within this realm.

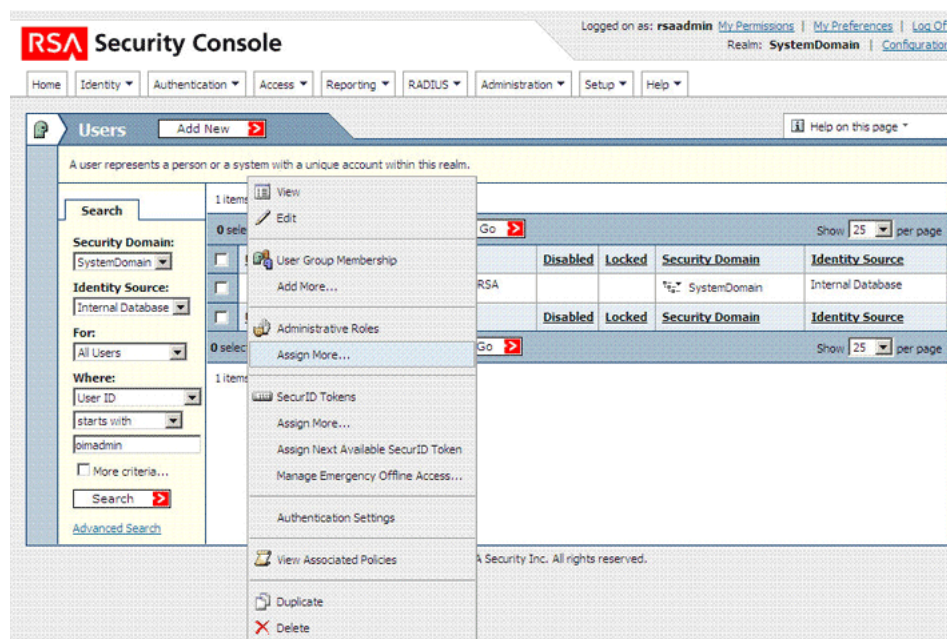
Search Enter search criteria to list users. To list all users, leave search field blank.

Security Domain: SystemDomain  
 Identity Source: Internal Database  
 For: All Users  
 Where: User ID starts with oimadmin  
☐ More criteria...  
 Search

[Advanced Search](#)

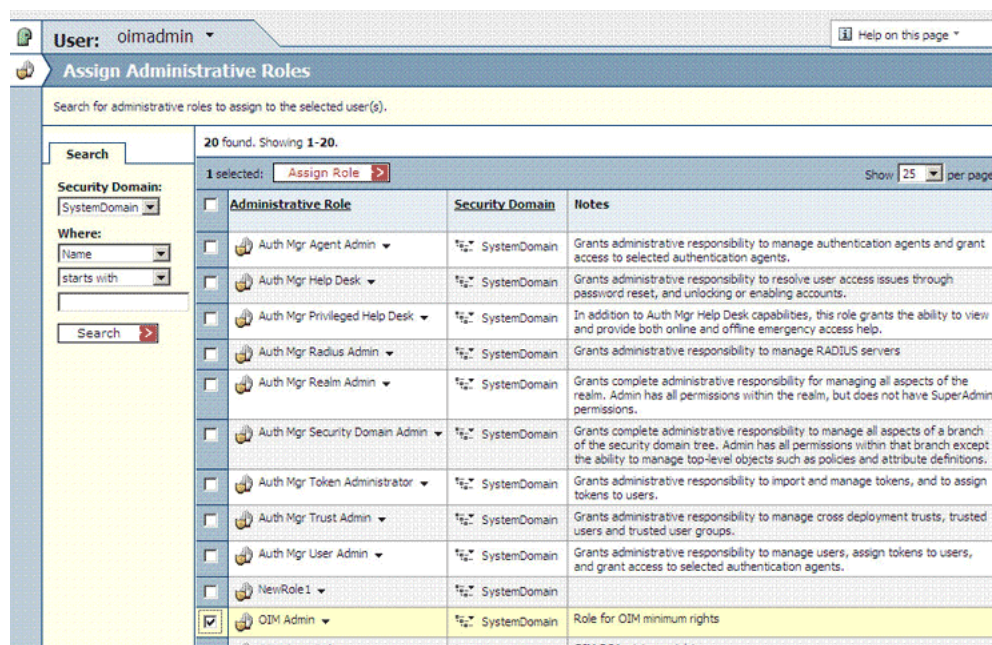
Copyright ©2007 - 2008 RSA Security Inc. All rights reserved.

- d. Click the arrow displayed next to the user name and then select **Assign More**.  
 The following screenshot shows this page:



- e. From the list of administrative roles, select the role that you create in Step 2 and then click **Assign Role**.

The following screenshot shows this page:



### 2.3.9 Mapping New Connection Properties

The connector uses the RemoteCommandTargetBean API of the target system to establish connections with the target system. The Lookup.RSA.AuthManager.ITResourceMapping lookup definition maps some of the IT resource parameters with parameters of this API. Table 2-4 shows the default entries in this lookup definition.



**Table 2–4 Entries in the Lookup.RSA.AuthManager.ITResourceMapping Lookup Definition**

Code Key/IT Resource Parameter	Decode/API Parameter
Command Client UserID	SecurityPrincipal
Command Client Password	SecurityCredentials
Provider URL	ProviderURL
JNDI Factory Class	InitialContextFactory

**Note:** See the Javadocs shipped with the target system for detailed information about connection properties used by the target system.

To meet the requirements of your operating environment, you might need to add connection properties to this default set of properties. For example, if the target system is in a clustered environment and you want to access a specific server in the cluster, then you must also provide a value for the `com.rsa.naming.pin.to.primary.server` connection property.

To map a new connection property:

1. Add the connection property as a parameter in the RSA AuthMgr Server IT resource type definition as follows:
  - a. On the Design Console, expand **Resource Management** and then click **IT Resources Type Definition**.
  - b. Search for and open the **RSA AuthMgr Server** IT resource type.
  - c. Click **Add**.

A new row is displayed in the IT Resource Type Parameter table.

The screenshot shows the 'IT Resource Type Definition' window. At the top, 'Server Type' is set to 'RSA AuthMgr Server' and 'Insert Multiple' is checked. Below this, there are two tabs: 'IT Resource Type Parameter' and 'IT Resource'. The 'IT Resource Type Parameter' tab is active, showing a table with the following data:

	Field Name	Default Field Value	Encrypted
1	Admin Password		<input checked="" type="checkbox"/>
2	Admin UserID		<input type="checkbox"/>
3	Command Client Password		<input checked="" type="checkbox"/>
4	Command Client UserID		<input type="checkbox"/>
5	Configuration Lookup	Lookup.RSA.AuthManag	<input type="checkbox"/>
6	Connect to specific node in cluster	True	<input type="checkbox"/>
7	JNDI Factory Class	weblogic.jndi.WLInitialCo	<input type="checkbox"/>
8	Provider URL		<input type="checkbox"/>

- d. In the **Field Name** column, enter a name for the parameter.
  - e. Do not enter values in any other field.
  - f. Click the Save icon.
2. Specify a value for the new parameter in the IT resource. See [Section 2.3.13, "Configuring Connection Parameters"](#) for instructions.
  3. In the `Lookup.RSA.AuthManager.ITResourceMapping` lookup definition, create a mapping between the connection property and the IT resource parameter as follows:

- a. On the Design Console, expand **Administration**, and then double-click **Lookup Definition**.
- b. Search for and open the **Lookup.RSA.AuthManager.ITResourceMapping** lookup definition.
- c. Click **Add**.
- d. In the **Code Key** column, enter the name of the IT resource parameter.  
Sample value: `Connect to specific node in cluster`
- e. In the **Decode** column, enter a value in the following format:  
Property | *PROPERTY\_NAME*  
Sample value: `Property | com.rsa.naming.pin.to.primary.server`
- f. Click the Save icon.

### 2.3.10 Setting Up the Configuration Lookup Definition in Oracle Identity Manager

[Table 2–5](#) describes the entries in the `Lookup.RSA.AuthManager.Configuration` lookup definition. You must set values for some of the entries.

---

**Note:** You must not change any of the Code Key values of this lookup definition.

---

**Table 2–5** Entries in the `Lookup.RSA.AuthManager.Configuration` Lookup Definition

Code Key	Description
Constants Lookup	This entry holds the name of the lookup definition that stores values used by the connector. The connector development team can use this lookup definition to make minor configuration changes in the connector. Default value: <code>Lookup.RSA.AuthManager.Constants</code>
Date Mappings Lookup	This entry holds the name of the lookup definition that stores entries used to format date values so that they are compatible with the date format used on the target system. This lookup definition is used during provisioning. Default value: <code>Lookup.RSA.AuthManager.DateMappings</code>
Exclusion Users Lookup	This entry holds the name of the lookup definition in which you enter user IDs of target system accounts for which you do not want to perform reconciliation and provisioning. See <a href="#">Section 2.3.11, "Setting Up the Lookup.RSA.AuthManager.ExclusionList Lookup Definition"</a> for more information. Default value: <code>Lookup.RSA.AuthManager.ExclusionList</code>
Full Recon Filter	This entry holds the name of the lookup definition that contains entries used by the connector during full reconciliation. Default value: <code>Lookup.RSA.AuthManager.FullReconFilter</code>
IT Resource Mapping	This entry holds the name of the lookup definition that maps some of the IT resource parameters with parameters of the <code>RemoteCommandTargetBean</code> API. Default value: <code>Lookup.RSA.AuthManager.ITResourceMapping</code>
Lookup Recon Mapping	This entry holds the names of lookup definitions that are synchronized with the target system when you run the RSA Auth Manager Lookup Recon scheduled task. Default value: <code>Lookup.RSA.AuthManager.LookupReconMapping</code>

**Table 2–5 (Cont.) Entries in the Lookup.RSA.AuthManager.Configuration Lookup Definition**

<b>Code Key</b>	<b>Description</b>
Target Date Format	Enter the format in which date values are stored on the target system. During reconciliation, this date format is used to validate date values fetched from the target system. Default value: <code>yyyy/MM/dd hh:mm:ss z</code>
Target TimeZone	Enter the time zone of the target system. For example, enter <code>GMT-07:00</code> if the target system is in Arizona in the United States. Default value: <code>GMT+05:30</code>
TKNFORMCOL TokenGUID	If you create a copy of the token process form, then specify the column name for the Token GUID attribute on the new token process form. Default value: <code>UD_AMTOKEN_TOKEN_GUID</code>
TKNFORMCOL TokenSerialNumber	If you create a copy of the token process form, then specify the column name for the Token Serial Number attribute on the new token process form. Default value: <code>UD_AMTOKEN_SERIAL_NUMBER</code>
TKNFORMCOL UserID	If you create a copy of the token process form, then specify the column name for the User ID attribute on the new token process form. Default value: <code>UD_AMTOKEN_USERID</code>
TKNROField TokenSerialNumber	If you create a copy of the token resource object, then specify the name of the attribute (column) in the new token resource object that holds token serial numbers. Default value: <code>Token Serial Number</code>
TKNROFIELD IdentitySource	If you create a copy of the token resource object, then specify the name of the attribute (column) in the new token resource object that holds the name of the user identity source. Default value: <code>User Identity Source</code>
TKNROFIELD TokenGuid	If you create a copy of the token resource object, then specify the name of the attribute (column) in the new token resource object that holds token GUIDs. Default value: <code>Token GUID</code>
TKNROFIELD UserId	If you create a copy of the token resource object, then specify the column name for the User ID attribute on the new token resource object. Default value: <code>User ID</code>
TKNROFIELD User GUID	If you create a copy of the token resource object, then specify the column name for the User GUID attribute on the new token resource object. Default value: <code>User Guid</code>
Token Attribute Mapping Lookup	This entry holds the name of the lookup definition that maps token process form fields with token attributes on the target system. Default value: <code>Lookup.RSA.AuthManager.TokenAttrMap</code>
Token Recon Attribute Mapping Lookup	This entry holds the name of the lookup definition that maps user process form fields with token attributes on the target system. Default value: <code>Lookup.RSA.AuthManager.TokenReconAttrMap</code>
Token SerialNumber MaxLength	Enter the maximum length of the token serial number allowed on your RSA Authentication Manager installation. Default value: <code>12</code>

**Table 2–5 (Cont.) Entries in the Lookup.RSA.AuthManager.Configuration Lookup Definition**

Code Key	Description
Token Status Provisioned	<p>The value of this entry is used to specify the state of resources created through reconciliation. You can set either <code>Provisioned</code> or <code>Enabled</code> as the value of this entry. If you set the value of this entry to, for example, <code>Enabled</code>, then resources created through reconciliation are set to the <code>Enabled</code> state.</p> <p>Default value: <code>Provisioned</code></p>
Token Transformation Mapping Lookup	<p>This entry holds the name of the lookup definition that is used to configure transformation of token attribute values fetched from the target system during token reconciliation.</p> <p>Default value: <code>Lookup.RSA.AuthManager.TokenTransformMapping</code></p>
User Attribute Mapping Lookup	<p>This entry holds the name of the lookup definition that maps user process form fields with single-valued user attributes on the target system.</p> <p>Default value: <code>Lookup.RSA.AuthManager.UserAttrMap</code></p>
User Child Attribute Mapping Lookup	<p>This entry holds the name of the lookup definition that maps user process form fields with multivalued user attributes on the target system.</p> <p>Default value: <code>Lookup.RSA.AuthManager.UserChildAttrMap</code></p>
User Recon Attribute Mapping Lookup	<p>This entry holds the name of the lookup definition that maps user resource object fields and single-valued user attributes on the target system.</p> <p>Default value: <code>Lookup.RSA.AuthManager.UserReconAttrMap</code></p>
User Recon Child Attribute Mapping Lookup	<p>This entry holds the name of the lookup definition that maps user resource object fields and multivalued user attributes on the target system.</p> <p>Default value: <code>Lookup.RSA.AuthManager.UserReconChildAttrMap</code></p>
User Status Provisioned	<p>The value of this entry is used to specify the state of resources created through reconciliation. You can set either <code>Provisioned</code> or <code>Enabled</code> as the value of this entry. If you set the value of this entry to, for example, <code>Enabled</code>, then resources created through reconciliation are set to the <code>Enabled</code> state.</p> <p>Default value: <code>Provisioned</code></p>
User Transformation Mapping Lookup	<p>This entry holds the name of the lookup definition that configures transformation of user attribute values fetched from the target system during user reconciliation.</p> <p>Default value: <code>Lookup.RSA.AuthManager.UserTransformMapping</code></p>
Use Token Transform Mapping	<p>Enter <code>yes</code> if you want to configure transformation of token attributes that are brought into Oracle Identity Manager during reconciliation. Otherwise, enter <code>no</code>.</p> <p>Default value: <code>no</code></p> <p>See <a href="#">Section 4.5, "Configuring Transformation of Data During Reconciliation"</a> for more information.</p>
Use User Transform Mapping	<p>Enter <code>yes</code> if you want to configure transformation of user attributes that are brought into Oracle Identity Manager during reconciliation. Otherwise, enter <code>no</code>.</p> <p>Default value: <code>no</code></p> <p>See <a href="#">Section 4.5, "Configuring Transformation of Data During Reconciliation"</a> for more information.</p>
Use Validation For TokenRecon	<p>Enter <code>yes</code> if you want to configure validation of token attributes that are brought into Oracle Identity Manager during reconciliation. Otherwise, enter <code>no</code>.</p> <p>Default value: <code>no</code></p> <p>See <a href="#">Section 4.4, "Configuring Validation of Data During Reconciliation and Provisioning"</a> for more information.</p>

**Table 2–5 (Cont.) Entries in the Lookup.RSA.AuthManager.Configuration Lookup Definition**

Code Key	Description
Use Validation For UserProv	<p>Enter <i>yes</i> if you want to configure validation of token attributes that are sent to RSA Authentication Manager during provisioning. Otherwise, enter <i>no</i>.</p> <p>Default value: <i>no</i></p> <p>See <a href="#">Section 4.4, "Configuring Validation of Data During Reconciliation and Provisioning"</a> for more information.</p>
Use Validation For UserRecon	<p>Enter <i>yes</i> if you want to configure validation of user attributes that are brought into Oracle Identity Manager during reconciliation. Otherwise, enter <i>no</i>.</p> <p>Default value: <i>no</i></p> <p>See <a href="#">Section 4.4, "Configuring Validation of Data During Reconciliation and Provisioning"</a> for more information.</p>
User UDF USERGUID	<p>If you create a copy of the user process form, then specify the column name of the UDF for the User GUID attribute.</p> <p>Default value: <i>USR_UDF_USERGUID</i></p>
USRFORMCOL ITResource	<p>If you create a copy of the user process form, then specify the column name for the IT Resource attribute on the new token process form.</p> <p>Default value: <i>UD_AMUSER_ITRESOURCE</i></p>
USRFORMCOL UserID	<p>If you create a copy of the user process form, then specify the column name for the User ID attribute on the new token process form.</p> <p>Default value: <i>UD_AMUSER_USER_ID</i></p>
USRROField UserGUID	<p>If you create a copy of the user resource object, then specify the column name for the User GUID attribute in the new user resource object.</p> <p>Default value: <i>User GUID</i></p>
USRROField Expire Time Hours	<p>If you create a copy of the user resource object, then specify the column name for the Expire Time Hours attribute in the new user resource object as the value of the USRROField Expire Time Hours entry. The Expire Time Hours attribute of Oracle Identity Manager is mapped to the target system attribute that holds the account expiry date and time.</p> <p>Default value: <i>Expire Time Hours</i></p>
USRROField Expire Time Mins	<p>If you create a copy of the user resource object, then specify the column name for the Expire Time Mins attribute in the new user resource object as the value of the USRROField Expire Time Mins entry. The Expire Time Mins attribute of Oracle Identity Manager is mapped to the target system attribute that holds the account expiry date and time.</p> <p>Default value: <i>Expire Time Mins</i></p>
USRFORMCOL UserGUID	<p>If you create a copy of the user process form, then specify the column name for the User GUID attribute on the new user process form.</p> <p>Default value: <i>UD_AMUSER_RSA_GUID</i></p>
USRROField IdentitySource	<p>If you create a copy of the user resource object, then specify the column name for the Identity Source attribute in the new user resource object.</p> <p>Default value: <i>User Identity Source</i></p>
USRROField Security Domain	<p>If you create a copy of the user resource object, then specify the column name for the Security Domain attribute in the new user resource object.</p> <p>Default value: <i>Security Domain</i></p>



**Table 2–5 (Cont.) Entries in the Lookup.RSA.AuthManager.Configuration Lookup Definition**

Code Key	Description
USRROField Start Time Hours	<p>If you create a copy of the user resource object, then specify the column name for the Start Time attribute in the new user resource object as the value of the USRROField Start Time Hours entry. The Start Time attribute of Oracle Identity Manager is mapped to the target system attribute that holds the account start date and time.</p> <p>Default value: <code>Start Time Hours</code></p>
USRROField Start Time Mins	<p>If you create a copy of the user resource object, then specify the column name for the Start Time attribute in the new user resource object as the value of the USRROField Start Time Mins entry. The Start Time attribute of Oracle Identity Manager is mapped to the target system attribute that holds the account start date and time.</p> <p>Default value: <code>Start Time Mins</code></p>
USRROField UserID	<p>If you create a copy of the user resource object, then specify the column name for the User ID attribute in the new user resource object.</p> <p>Default value: <code>User ID</code></p>
Validation Lookup For Token Provisioning	<p>This entry holds the name of the lookup definition that maps token process form fields with the Java validation classes that you create.</p> <p>Value: <code>Lookup.RSA.AuthManager.TokenProvisioningValidation</code></p> <p>See <a href="#">Section 4.4, "Configuring Validation of Data During Reconciliation and Provisioning"</a> for more information about this feature.</p>
Validation Lookup For Token Recon	<p>This entry holds the name of the lookup definition that maps token resource object fields with the Java validation classes that you create.</p> <p>Value: <code>Lookup.RSA.AuthManager.TokenReconValidation</code></p> <p>See <a href="#">Section 4.4, "Configuring Validation of Data During Reconciliation and Provisioning"</a> for more information about this feature.</p>
Validation Lookup For User Prov	<p>This entry holds the name of the lookup definition that maps user process form fields with the Java validation classes that you create.</p> <p>Value: <code>Lookup.RSA.AuthManager.UserProvisioningValidation</code></p> <p>See <a href="#">Section 4.4, "Configuring Validation of Data During Reconciliation and Provisioning"</a> for more information about this feature.</p>
Validation Lookup For User Recon	<p>This entry holds the name of the lookup definition that maps user resource object fields with the Java validation classes that you create.</p> <p>Value: <code>Lookup.RSA.AuthManager.UserReconValidation</code></p> <p>See <a href="#">Section 4.4, "Configuring Validation of Data During Reconciliation and Provisioning"</a> for more information about this feature.</p>

### 2.3.11 Setting Up the Lookup.RSA.AuthManager.ExclusionList Lookup Definition

In the Lookup.RSA.AuthManager.ExclusionList lookup definition, you can enter the user IDs of target system accounts for which you do not want to perform reconciliation and provisioning:

1. On the Design Console, expand **Administration** and then double-click **Lookup Definition**.
2. Search for and open the **Lookup.RSA.AuthManager.ExclusionList** lookup definition.
3. Click **Add**.
4. In the Code Key and Decode columns, enter the first user ID that you want to exclude. You must enter the same value in both columns.

---

---

**Note:** You must enter the user ID in the same case (uppercase and lowercase) in which it is stored on the target system.

---

---

5. Repeat Steps 3 and 4 for all the user IDs that you want to exclude.
6. Click the Save icon.

### 2.3.12 Modifying the Process Form

After performing lookup field synchronization, to ensure that values retrieved from the lookup fields on the target system are displayed in the lookup fields in Oracle Identity Manager, you must perform the following procedure:

1. On the Design Console, expand **Development Tools** and double-click **Form Designer**.
2. Search for and open the **UD\_AMTOKEN** form.
3. Click **Create New Version**, and then enter a version number for the new version.
4. Select the form which was created in the preceding step.
5. On the Properties tab, double-click the **Lookup Query** property.
6. In the Edit Property dialog box:
  - a. Select **Lookup Code** from the Property Name list.
  - b. Enter `Lookup.RSA.AuthManager.IdentitySource` in the **Property Value** field.
  - c. Click the Save icon.
7. Click **Make Version Active**.
8. Click the Save icon.
9. Repeat Steps 1 through 8 with the following differences:
  - While performing Step 2, search for and open the **UD\_AMROLE** form.
  - While performing Step 6.b, enter `Lookup.RSA.AuthManager.AdminRole` in the **Property Value** field.
10. Repeat Steps 1 through 8 with the following differences:
  - While performing Step 2, search for and open the **UD\_AMUSER** form.
  - While performing Step 6.b, enter `Lookup.RSA.AuthManager.IdentitySource` in the **Property Value** field.
11. Repeat Steps 1 through 8 with the following differences:
  - While performing Step 2, search for and open the **UD\_AMUSER** form.
  - While performing Step 6.b, enter `Lookup.RSA.AuthManager.SecurityDomain` in the **Property Value** field.
12. Repeat Steps 1 through 8 with the following differences:
  - While performing Step 2, search for and open the **UD\_AMGROUP** form.
  - While performing Step 6.b, enter `Lookup.RSA.AuthManager.Group` in the **Property Value** field.

## 2.3.13 Configuring Connection Parameters

The RSA Server Instance IT resource holds information used by the connector to establish a connection with the target system. This IT resource is automatically created when you run the Connector Installer. You must specify values for the IT resource parameters.

---

### Note:

The ALL USERS group has INSERT, UPDATE, and DELETE permissions on the default IT resource. This is to ensure that end users can select the IT resource during request-based provisioning. If you create another IT resource, then you must assign INSERT, UPDATE, and DELETE permissions for the ALL USERS group on the IT resource.

You must use the Administrative and User Console to configure the IT resource.

---

To specify values for the parameters of the IT resource:

1. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
  - For Oracle Identity Manager release 9.1.0.x:
    - a. Log in to the Administrative and User Console.
    - b. Expand **Resource Management**, and then click **Manage IT Resource**.
  - For Oracle Identity Manager release 11.1.1:
    - a. Log in to the Administrative and User Console.
    - b. On the Welcome to Oracle Identity Manager Self Service page, click **Advanced** in the upper-right corner of the page.
    - c. On the Welcome to Oracle Identity Manager Advanced Administration page, in the Configuration region, click **Manage IT Resource**.
  - For Oracle Identity Manager release 11.1.2.x:
    - a. Log in to Oracle Identity System Administration.
    - b. In the left pane, under Configuration, click **IT Resource**.
2. In the IT Resource Name field on the Manage IT Resource page, enter `RSA Server Instance` and then click **Search**.
3. Click the edit icon for the IT resource.
4. From the list at the top of the page, select **Details and Parameters**.
5. Specify values for the parameters of the IT resource. [Table 2–6](#) describes each parameter.

---

**Note:** Entries in this table are sorted in alphabetical order of parameter names.

---

**Table 2–6 Parameters of the IT Resource**

Parameter	Description
Admin Password	Enter the password of the target system user account that you create for connector operations See <a href="#">Section 2.3.8, "Creating a Target System Account for Connector Operations"</a> for more information.
Admin UserID	Enter the user ID of the target system user account that you create for connector operations See <a href="#">Section 2.3.8, "Creating a Target System Account for Connector Operations"</a> for more information.
Command Client Password	Enter the command client password. Setting the command client user name and password is one of the tasks in the procedure mentioned in <a href="#">Section 2.3.5, "Addressing Prerequisites for Using the Java API of RSA Authentication Manager."</a>
Command Client UserID	Enter the command client user name. Setting the command client user name and password is one of the tasks in the procedure mentioned in <a href="#">Section 2.3.5, "Addressing Prerequisites for Using the Java API of RSA Authentication Manager."</a>
Configuration Lookup	This parameter holds the name of the configuration lookup definition. Default value: <code>Lookup.RSA.AuthManager.Configuration</code>
JNDI Factory Class	This parameter holds the name of the initial context factory class on the target system. Value: <code>weblogic.jndi.WLInitialContextFactory</code> You must not change this value.
Provider URL	Enter the following value: <code>https://IP_ADDRESS or HOSTNAME:7002/ims-ws/services/CommandServer</code> <b>Note:</b> If RSA Authentication Manager is installed in a clustered environment, then replace <code>IP_ADDRESS or HOSTNAME</code> with a comma-separated list of IP addresses or host names of all the nodes of the cluster. For example: <code>https://IP_ADDRESS1 or HOSTNAME1,IP_ADDRESS2 or HOSTNAME2,...:7002</code> Sample value: <code>https://hostNode1,hostNode74,hostNode21:7002</code>

6. To save the values, click **Update**.

## 2.3.14 Creating Authorization Policies for User Management

To create authorization policies for user management, perform the procedures described in the following sections:

---

**Note:** Perform the procedure described in the following sections *only* if you are using Oracle Identity Manager release 11.1.1 or 11.1.2.x.

---

- [Section 2.3.14.1, "Creating an Authorization Policy for Provisioning"](#)
- [Section 2.3.14.2, "Creating an Authorization Policy for Reconciliation"](#)

### 2.3.14.1 Creating an Authorization Policy for Provisioning

Before you can start using the connector for provisioning operations, you must create an authorization policy as follows:

1. Log in to the Administrative and User Console.

2. On the Welcome to Identity Administration page, in the Authorization Policies page, click **Create Authorization Policy**.
3. On the Basic Policy Information page, enter values for the following fields:
  - **Policy Name:** Enter name of the authorization policy for provisioning.
  - **Description:** Enter a description of the authorization policy.
  - **Entity Name:** Select the **User Management** feature.
4. Click **Next**. The Permissions page is displayed.
5. In the Enable column, select the checkbox corresponding to the Modify User Profile permission.
6. Modify the attribute-level settings for the Modify User Profile permission as follows:
  - a. Click **Edit Attributes**.
  - b. In the Attribute Settings dialog box, from the User Attributes region, select **User GUID**, click **Save**, and then close the dialog box.
7. On the Permissions page, in the Enable column, select the checkbox corresponding to the View User Details permission.
8. Modify the attribute-level settings for the View User Details permission as follows:
  - a. Click **Edit Attributes**.
  - b. In the Attribute Settings dialog box, from the User Attributes region, select **User GUID**, click **Save**, and then close the dialog box.
9. Click **Next**. The Data Constraints page is displayed.
10. Ensure that All User is selected, and then click **Next**.
11. On the Policy Assignment page, under Assign by Rule, ensure that **Management Chain of User** is not selected to remove the assignment of the direct and indirect managers of the user to the authorization policy.
12. Assign the System Administrator role to the authorization policy as follows:
  - a. In the Assign by Role region, click **Add**.
  - b. In the Assign Roles dialog box, search for and select the **System Administrator** role, and then click **Add**. The System Administrator role is added to the table in the Policy Assignment page.
13. On the Policy Confirmation page, verify details of the policy, and then click **Finish**.  
 On the next page, a message confirming that the policy creation was successful is displayed.
14. Click **Apply** to save changes.

### 2.3.14.2 Creating an Authorization Policy for Reconciliation

To successfully use the connector for reconciliation, create an authorization policy by performing the following instructions:

1. Log in to the Administrative and User Console.
2. On the Welcome to Identity Administration page, on the left pane, click the **Authorization Policy** tab.

3. On the left pane, in the Search field, enter the name of the policy (User Management All Users Policy) as the search criterion.
4. From the search results table, select **User Management All Users Policy**.
5. From the Actions menu, select **Create Like**.
6. On the right pane, in the Basic Policy Information page, edit the Policy Name and Description fields to specify a new value, and then click **Next**. For example, enter the following values:  
  
**Policy Name:** User Management All Users Policy for RSA  
  
**Description:** Allows users with the ALL USERS role to access all user-management actions and authorization policy for the an RSA Auth Manager user.
7. On the Permissions page, in the Enable column, select the checkbox corresponding to the Modify User Profile permission .
8. Modify the attribute-level settings for the Modify User Profile permission as follows:
  - a. Click **Edit Attributes**.
  - b. In the Attribute Settings dialog box, from the User Attributes region, select **User GUID**, click **Save**, and then close the dialog box.
9. On the Permissions page, in the Enable column, select the checkbox corresponding to the View User Details permission.
10. Modify the attribute-level settings for the View User Details permission as follows:
  - a. Click **Edit Attributes**.
  - b. In the Attribute Settings dialog box, from the User Attributes region, select **User GUID**, click **Save**, and then close the dialog box.
11. On the Permissions page, in the Enable column, select the checkbox corresponding to the Search User permission, and then click **Next**.
12. On the Data Constraints page, ensure that All User is selected, and then click **Next**.
13. On the Policy Assignment page, ensure that the ALL USERS role is displayed in the table, and then click **Next**.
14. On the Policy Confirmation page, verify details of the policy, and then click **Finish**.
15. On the next page that is displayed, click **Apply** to save changes.

## 2.3.15 Configuring Request-Based Provisioning

---

---

**Note:** This step is not applicable for Oracle Identity Manager versions 11g R2 and above.

Perform the procedure described in this section only if you are using Oracle Identity Manager release 9.1.0.x or 11.1.1 and you want to configure request-based provisioning.

---

---

In request-based provisioning, an end user creates a request for a resource by using the Administrative and User Console. Administrators or other users can also create

requests for a particular user. Requests for a particular resource on the resource can be viewed and approved by approvers designated in Oracle Identity Manager.

The following are features of request-based provisioning:

- A user can be provisioned only one resource (account) on the target system.

---

**Note:** Direct provisioning allows the provisioning of multiple target system accounts on the target system.

---

- Direct provisioning cannot be used if you enable request-based provisioning.

To configure request-based provisioning, perform the following procedures:

- [Section 2.3.15.1, "Copying Predefined Request Datasets"](#)
- [Section 2.3.15.2, "Importing Request Datasets into MDS"](#)
- [Section 2.3.15.3, "Enabling the Auto Save Form Feature"](#)
- [Section 2.3.15.4, "Running the PurgeCache Utility"](#)

### 2.3.15.1 Copying Predefined Request Datasets

A request dataset is an XML file that specifies the information to be submitted by the requester during a provisioning operation. Predefined request datasets are shipped with this connector. These request datasets specify information about the default set of attributes for which the requester must submit information during a request-based provisioning operation. The following are the predefined request datasets available in the dataset directory on the installation media:

- ProvisionResourceRSA Auth Manager User.xml
- ProvisionResourceRSA Auth Manager Token.xml
- ModifyResourceRSA Auth Manager User.xml
- ModifyResourceRSA Auth Manager Token.xml

Copy these files from the installation media to any directory on the Oracle Identity Manager host computer. It is recommended that you create a directory structure as follows:

`/custom/connector/RESOURCE_NAME`

For example:

`E:\MyDatasets\custom\connector\RSA_Auth_Mgr`

---

**Note:** Until you complete the procedure to configure request-based provisioning, ensure that there are no other files or directories inside the parent directory in which you create the directory structure. In the preceding example, ensure that there are no other files or directories inside the `E:\MyDatasets` directory.

---

The directory structure to which you copy the dataset files is the MDS location into which these files are imported after you run the Oracle Identity Manager MDS Import utility. The procedure to import dataset files is described in the next section.

Depending on your requirement, you can modify the file names of the request datasets. In addition, you can modify the information in the request datasets. See

*Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information on modifying request datasets.

### 2.3.15.2 Importing Request Datasets into MDS

All request datasets must be imported into the metadata store (MDS), which can be done by using the Oracle Identity Manager MDS Import utility.

To import a request dataset definition into MDS:

1. Ensure that you have set the environment for running the MDS Import utility. See *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for detailed information about setting up the environment for MDS utilities.

---

**Note:** While setting up the properties in the `weblogic.properties` file, ensure that the value of the `metadata_from_loc` property is the parent directory of the `/custom/connector/RESOURCE_NAME` directory. For example, while performing the procedure in [Section 2.3.15.1, "Copying Predefined Request Datasets,"](#) if you copy the files to the `E:\MyDatasets\custom\connector\RSA_Auth_Mgr` directory, then set the value of the `metada_from_loc` property to `E:\MyDatasets`.

---

2. In a command window, change to the `OIM_HOME\server\bin` directory.
3. Run one of the following commands:
  - On Microsoft Windows
 

```
weblogicImportMetadata.bat
```
  - On UNIX
 

```
weblogicImportMetadata.sh
```
4. When prompted, enter the following values:
  - Please enter your username [weblogic]  
Enter the username used to log in to the WebLogic server  
Sample value: `WL_User`
  - Please enter your password [weblogic]  
Enter the password used to log in to the WebLogic server.
  - Please enter your server URL [t3://localhost:7001]  
Enter the URL of the application server in the following format:  
`t3://HOST_NAME_IP_ADDRESS:PORT`  
In this format, replace:
    - `HOST_NAME_IP_ADDRESS` with the host name or IP address of the computer on which Oracle Identity Manager is installed.
    - `PORT` with the port on which Oracle Identity Manager is listening.

The request dataset is imported into MDS at the following location:

`/custom/connector/RESOURCE_NAME`



### 2.3.15.3 Enabling the Auto Save Form Feature

To enable the Auto Save Form feature:

1. Log in to the Design Console.
2. Expand **Process Management**, and then double-click **Process Definition**.
3. Search for and open the **RSA Auth Manager User** process definition.
4. Select the **Auto Save Form** check box.
5. Click the Save icon.
6. Repeat Steps 1 through 5 with the following difference:  
While performing Step 3, search for and open the **RSA Auth Manager Token** process definition.

### 2.3.15.4 Running the PurgeCache Utility

Run the PurgeCache utility to clear content belonging to the Metadata category from the server cache. See [Section 2.3.2, "Clearing Content Related to Connector Resource Bundles from the Server Cache"](#) for instructions.

The procedure to configure request-based provisioning ends with this step.

## 2.3.16 Configuring Oracle Identity Manager 11.1.2 or Later

If you are using Oracle Identity Manager release 11.1.2.x or later, you must create additional metadata such as a UI form and an application instance, and must run entitlement and catalog synchronization jobs. In addition, you must tag some of the fields in the OIM User process form. These procedures are described in the following sections:

- [Section 2.3.16.1, "Tagging OIM Process Form Fields"](#)
- [Section 2.3.16.2, "Creating and Activating a Sandbox"](#)
- [Section 2.3.16.3, "Creating a New UI Form"](#)
- [Section 2.3.16.4, "Creating an Application Instance"](#)
- [Section 2.3.16.5, "Publishing a Sandbox"](#)
- [Section 2.3.16.6, "Harvesting Entitlements and Sync Catalog"](#)
- [Section 2.3.16.7, "Updating an Existing Application Instance with a New Form"](#)

### 2.3.16.1 Tagging OIM Process Form Fields

Some of the field on the process form in Oracle Identity Manager need additional tagging. To do so:

1. Log in to the Design Console.
2. Expand **Development Tools**, and then double-click **Form Designer**.
3. Enter UD\_AMROLE in the Table Name field and click the **Query for records** button.
4. Click **Create New Version**.
5. In the Create a New Version dialog box, specify the version name in the Label field, save the changes, and then close the dialog box.
6. From the Current Version list, select the newly created version.

7. On the Properties tab, add a property and property value to the Role Name field as follows:
  - a. Select the Role Name field, and then click **Add Property**.  
The Add Property dialog box is displayed.
  - b. From the Property Name list, select **Entitlement**.
  - c. In the Property Value field, enter `true`.
  - d. Click the Save icon and then close the dialog box.
8. Click the Save icon.
9. Click **Make Version Active**.
10. Repeat Steps 2 through 9 to add a property to the UD\_AMGROUP form with the following differences:
  - a. While performing Step 3, enter UD\_AMGROUP as the form name, instead of UD\_AMROLE.
  - b. While performing Step 7.a, select the **Group Name** field instead of Role Name.
11. Repeat Steps 2 through 9 to add a property to the UD\_AMTOKEN form with the following differences:
  - a. While performing Step 3, enter UD\_AMTOKEN as the form name, instead of UD\_AMROLE.
  - b. While performing Step 7, on the Properties tab, add the following properties:

Field	Property Name	Property Value
Server Instance	ITResource	true
Token Serial Number	AccountName	true
Token GUID	AccountId	true

12. Repeat Steps 2 through 9 to add a property to the UD\_AMUSER form with the following differences:
  - a. While performing Step 3, enter UD\_AMUSER as the form name, instead of UD\_AMROLE.
  - b. While performing Step 7, on the Properties tab, add the following properties:

Field	Property Name	Property Value
Server Instance	ITResource	true
User ID	AccountName	true
User GUID	AccountId	true

### 2.3.16.2 Creating and Activating a Sandbox

Create and activate a sandbox as follows. For detailed instructions, see the "Managing Sandboxes" section in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

1. On the upper navigation bar, click **Sandboxes**. The Manage Sandboxes page is displayed.

2. On the toolbar, click **Create Sandbox**. The Create Sandbox dialog box is displayed.
3. In the Sandbox Name field, enter a name for the sandbox. This is a mandatory field.
4. In the Sandbox Description field, enter a description of the sandbox. This is an optional field.
5. Click **Save and Close**. A message is displayed with the sandbox name and creation label.
6. Click **OK**. The sandbox is displayed in the Available Sandboxes section of the Manage Sandboxes page.
7. Select the sandbox that you created.
8. From the table showing the available sandboxes in the Manage Sandboxes page, select the newly created sandbox that you want to activate.
9. On the toolbar, click **Activate Sandbox**.  
The sandbox is activated.

### 2.3.16.3 Creating a New UI Form

Create a new UI form as follows. For detailed instructions, see the "Managing Forms" chapter in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

1. In the left pane, under Configuration, click **Form Designer**.
2. Under Search Results, click **Create**.
3. Select the resource type for which you want to create the form, for example, **RSA Auth Manager User**.
4. Enter a form name and click **Create**.

### 2.3.16.4 Creating an Application Instance

Create an application instance as follows. For detailed instructions, see the "Managing Application Instances" chapter in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

1. In the System Administration page, under Configuration in the left pane, click **Application Instances**.
2. Under Search Results, click **Create**.
3. Enter appropriate values for the fields displayed on the Attributes form and click **Save**.
4. In the Form drop-down list, select the newly created form and click **Apply**.
5. Publish the application instance to an organization to make the application instance available for requesting and subsequent provisioning to users. See the "Managing Organizations Associated With Application Instances" section in *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for detailed instructions.

### 2.3.16.5 Publishing a Sandbox

To publish the sandbox that you created in [Section 2.3.16.2, "Creating and Activating a Sandbox"](#):

1. Close all the open tabs and pages.

2. From the table showing the available sandboxes in the Manage Sandboxes page, select the sandbox that you created in [Section 2.3.16.2, "Creating and Activating a Sandbox."](#)
3. On the toolbar, click **Publish Sandbox**. A message is displayed asking for confirmation.
4. Click **Yes** to confirm. The sandbox is published and the customizations it contained are merged with the main line.

#### 2.3.16.6 Harvesting Entitlements and Sync Catalog

To harvest entitlements and sync catalog:

1. Run the scheduled jobs for lookup field synchronization.
2. Run the Entitlement List scheduled job to populate Entitlement Assignment schema from child process form table. See the "Predefined Scheduled Tasks" section in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for more information about this scheduled job.
3. Run the Catalog Synchronization Job scheduled job. See the "Predefined Scheduled Tasks" section in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for more information about this scheduled job.

#### 2.3.16.7 Updating an Existing Application Instance with a New Form

For any changes you do in the Form Designer, you must create a new UI form and update the changes in an application instance. To update an existing application instance with a new form:

1. Create a sandbox and activate it as described in [Section 2.3.16.2, "Creating and Activating a Sandbox."](#)
2. Create a new UI form for the resource as described in [Section 2.3.16.3, "Creating a New UI Form."](#)
3. Open the existing application instance.
4. In the **Form** field, select the new UI form that you created in Step 2.
5. Save the application instance.
6. Publish the sandbox as described in [Section 2.3.16.5, "Publishing a Sandbox."](#)

### 2.3.17 Localizing Field Labels in UI Forms

---

**Note:** Perform the procedure described in this section only if you are using Oracle Identity Manager release 11.1.2.x and you want to localize UI form field labels.

---

To localize field label that you add to in UI forms:

1. Log in to Oracle Enterprise Manager.
2. In the left pane, expand **Application Deployments** and then select **oracle.iam.console.identity.sysadmin.ear**.
3. In the right pane, from the Application Deployment list, select **MDS Configuration**.

4. On the MDS Configuration page, click **Export** and save the archive to the local computer.
5. Extract the contents of the archive, and open the following file in a text editor:  
`SAVED_LOCATION\xliffBundles\oracle\iam\ui\runtime\BizEditorBundle.xlf`
6. Edit the BizEditorBundle.xlf file in the following manner:

- a. Search for the following text:

```
<file source-language="en"
original="/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle.xlf"
datatype="x-oracle-adf">
```

- b. Replace with the following text:

```
<file source-language="en" target-language="LANG_CODE"
original="/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle.xlf"
datatype="x-oracle-adf">
```

In this text, replace `LANG_CODE` with the code of the language that you want to localize the form field labels. The following is a sample value for localizing the form field labels in Japanese:

```
<file source-language="en" target-language="ja"
original="/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle.xlf"
datatype="x-oracle-adf">
```

- c. Search for the application instance code. This procedure shows a sample edit for RSA application instance. The original code is:

```
<trans-unit
id="${adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBu
ndle']['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.use
rEO.UD_AMUSER_FIRST_NAME__c_description']}">
<source>First Name</source>
<target/>
</trans-unit>
<trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.RSAForm.entity.RSAFormEO.UD
_AMUSER_FIRST_NAME__c_LABEL">
<source>First Name</source>
<target/>
</trans-unit>
```

- d. Open the resource file from the connector package, for example `RSA-AuthManager_ja.properties`, and get the value of the attribute from the file, for example, `global.udf.UD_AMUSER_FIRST_NAME=\u540D`.
- e. Replace the original code shown in Step 6.c with the following:

```
<trans-unit
id="${adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBu
ndle']['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.use
rEO.UD_AMUSER_FIRST_NAME__c_description']}">
<source>First Name</source>
<target>\u540D</target>
</trans-unit>
<trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.RSAForm.entity.RSAFormEO.UD
_AMUSER_FIRST_NAME__c_LABEL">
<source>First Name</source>
```

**See Also:** The "Deploying and Undeploying Customizations" chapter in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*, for more information about exporting and importing metadata files

- f. Repeat Steps 6.a through 6.d for all attributes of the process form.
  - g. Save the file as BizEditorBundle\_ LANG\_CODE .xlf. In this file name, replace LANG\_CODE with the code of the language to which you are localizing.  
Sample file name: BizEditorBundle\_ja.xlf.
7. Repackage the ZIP file and import it into MDS.  
  
**See Also:** The "Deploying and Undeploying Customizations" chapter in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*, for more information about exporting and importing metadata files
8. Log out of and log in to Oracle Identity Manager.

---

## Using the Connector

---

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

---

This chapter is divided into the following sections:

- [Section 3.1, "Performing First-Time Reconciliation"](#)
- [Section 3.2, "Scheduled Task for Lookup Field Synchronization"](#)
- [Section 3.3, "Guidelines on Performing Reconciliation"](#)
- [Section 3.4, "Configuring Reconciliation"](#)
- [Section 3.5, "Configuring the Scheduled Tasks"](#)
- [Section 3.6, "Guidelines on Performing Provisioning"](#)
- [Section 3.7, "Assigning Software Tokens to Users"](#)
- [Section 3.8, "Performing Provisioning Operations in Oracle Identity Manager Release 9.1.0.x and 11.1.1.x"](#)
- [Section 3.8.3, "Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1"](#)
- [Section 3.9, "Performing Provisioning Operations in Oracle Identity Manager Release 11.1.2 or Later"](#)

### 3.1 Performing First-Time Reconciliation

First-time reconciliation involves synchronizing lookup definitions in Oracle Identity Manager with the lookup fields of the target system, and performing full reconciliation. In full reconciliation, all existing user records from the target system are brought into Oracle Identity Manager.

The following is the sequence of steps involved in reconciling all existing user records:

---

**Note:** In Oracle Identity Manager release 11.1.1 and 11.1.2.x, a scheduled job is an instance of a scheduled task. In this guide, the term **scheduled task** used in the context of Oracle Identity Manager release 9.1.0.x is the same as the term **scheduled job** in the context of Oracle Identity Manager release 11.1.1 or 11.1.2.x.

See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about scheduled tasks and scheduled jobs.

---

1. Perform lookup field synchronization by running the scheduled tasks provided for this operation.  
  
See [Section 3.2, "Scheduled Task for Lookup Field Synchronization"](#) for information about the attributes of the scheduled tasks for lookup field synchronization.  
  
See [Section 3.4.4, "Reconciliation Scheduled Tasks"](#) for information about running scheduled tasks.
2. Perform user and token reconciliation by running the scheduled tasks for user and token reconciliation.  
  
See [Section 3.4.4, "Reconciliation Scheduled Tasks"](#) for information about the attributes of this scheduled task.  
  
See [Section 3.4.4, "Reconciliation Scheduled Tasks"](#) for information about running scheduled tasks.

After first-time reconciliation, the Last Execution Timestamp attribute of the scheduled task is automatically set to the time stamp at which the reconciliation run began.

**See Also:** [Section 2.3.13, "Configuring Connection Parameters"](#) for information about the parameters of the IT resource

From the next reconciliation run onward, only target system user records that are added or modified after the time stamp stored in the scheduled task are considered for incremental reconciliation. These records are brought to Oracle Identity Manager when you configure and run the user reconciliation scheduled task.

## 3.2 Scheduled Task for Lookup Field Synchronization

The RSA Auth Manager Lookup Recon scheduled task is used for lookup field synchronization. [Table 3–1](#) describes the attributes of this scheduled task. The procedure to configure scheduled tasks is described later in the guide.

**See Also:** [Table 1–2](#) for the list of lookup definitions synchronized by this scheduled task



**Table 3–1 Attributes of the RSA Auth Manager Lookup Recon Scheduled Task**

Attribute	Description
IT Resource	Enter the name of the IT resource for the target system installation from which you want to reconcile user records.  Default value: <code>RSA Server Instance</code>
Scheduled Task Name	This attribute holds the name of the scheduled task. If you create a copy of the scheduled task, then enter the name of the new scheduled task as the value of the Scheduled Task Name attribute.  Value: <code>RSA Auth Manager Lookup Recon</code>

### 3.3 Guidelines on Performing Reconciliation

Apply the following guideline before you perform a reconciliation run:

If there are a large number of users or tokens to be reconciled during full reconciliation, then you might encounter the `InvalidSessionException` exception. To work around this issue, increase the Session Lifetime setting on RSA Authentication Manager as follows:

---

**Note:** In [Chapter 5, "Known Issues and Limitations,"](#) this issue has been documented as Bug 9268577.

---

1. Log in to the RSA Security Console.
2. From the Access list, select **Session Lifetimes** and then select **Manage Existing**.
3. In the Session Lifetime list, open the **Console/Command API Session Lifetime** list and select **Edit** from the list.
4. Increase the maximum lifetime value according to your requirement.
5. Save the setting.

### 3.4 Configuring Reconciliation

This section discusses the following topics related to configuring reconciliation:

- [Section 3.4.1, "Full Reconciliation"](#)
- [Section 3.4.2, "Limited Reconciliation"](#)
- [Section 3.4.4, "Reconciliation Scheduled Tasks"](#)

#### 3.4.1 Full Reconciliation

Full reconciliation involves reconciling all existing user and token records from the target system into Oracle Identity Manager. After you deploy the connector, you must first perform full reconciliation.

To perform a full reconciliation run, ensure that there are no values for the Last Execution Timestamp, CustomReconQuery, and Group attributes and then run the scheduled task. [Section 3.4.4, "Reconciliation Scheduled Tasks"](#) provides information about the procedure to set values for the scheduled task attributes.

The Last Execution Timestamp attribute of the scheduled task stores the time stamp at which a reconciliation run begins. During a reconciliation run, the scheduled task fetches only target system records that are added or modified after the time stamp

stored in the Last Execution Timestamp attribute. In other words, after a full reconciliation run, the connector automatically switches to incremental reconciliation for subsequent reconciliation runs. However, you can perform full reconciliation whenever you want to ensure that all target system records are reconciled in Oracle Identity Manager.

### 3.4.2 Limited Reconciliation

By default, all user and token 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 newly added or modified records that must be reconciled. You do this by setting a filter for reconciliation.

For this connector, you set a filter (query condition) as the value of the CustomReconQuery scheduled task attribute while performing the procedure described in [Section 3.4.4, "Reconciliation Scheduled Tasks."](#)

---

---

**Note:** In addition to the CustomReconQuery attribute, you can use the Group attribute of the scheduled task to specify the user group from which user or token records must be reconciled.

---

---

You can use the following attributes to build the filter:

- Certificate DN
- First Name
- Last Name
- Middle Name
- User ID

You can use the following comparators to build each clause in the query condition:

- =
- <>
- contains
- endsWith
- startsWith

A query condition can contain up to 3 clauses, and the clauses can be linked with the AND (&) and OR (|) operators.

The following are sample values for the CustomReconQuery attribute:

- User ID contains do

With this query condition, all records of users whose user IDs contain the string do are reconciled.

- First Name = John & Last Name endsWith oe | Last Name StartsWith Do

With this query condition, the following records are reconciled:

- Users whose first name is John and last name ends in the string oe.
- Users whose last name starts with the string Do.

- Certificate DN <> CN,OU,O

With this query condition, all records of users whose certificate DN is not equal to CN,OU,O are reconciled.

### 3.4.3 Batched Reconciliation

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

You can configure batched reconciliation to avoid such problems.

To configure batched reconciliation, you use the FullRecon Batch Size user reconciliation scheduled task attribute. This attribute is used to specify the number of records that must be included in each batch fetched from the target system.

Suppose you specify 20 as the value of the FullRecon Batch Size attribute. Suppose that 314 user records were created or modified after the last reconciliation run. These 314 records would be reconciled in batches of 20 records each.

You specify values for the FullRecon Batch Size attribute by following the instructions described in [Section 3.4.4, "Reconciliation Scheduled Tasks."](#)

### 3.4.4 Reconciliation Scheduled Tasks

When you run the Connector Installer, the scheduled tasks for user and token reconciliation are automatically created in Oracle Identity Manager.

The following sections provide information about the attributes of these reconciliation scheduled tasks:

- [Section 3.4.4.1, "RSA Auth Manager User Recon"](#)
- [Section 3.4.4.2, "RSA Auth Manager Token Recon"](#)

#### 3.4.4.1 RSA Auth Manager User Recon

[Table 3–2](#) describes the attributes of the scheduled task for user and token reconciliation.

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

**Table 3–2 Attributes of the RSA Auth Manager User Recon Scheduled Task**

Attribute	Description
CustomReconQuery	Enter the query condition that must be applied during the reconciliation run. This is one of the attributes that are used to implement limited reconciliation. <a href="#">Section 3.4.2, "Limited Reconciliation"</a> describes this feature.
Group	Enter the name of the group on the target system that you want to use for the reconciliation run. Only users or tokens from the group that you specify are considered for the reconciliation run.  This is one of the attributes that are used to implement limited reconciliation. <a href="#">Section 3.4.2, "Limited Reconciliation"</a> describes this feature.
Identity Source	Enter the name of the identity source that must be used during the reconciliation run. The identity source can be the internal database, an external database, or an LDAP solution. You must enter the name of the identity source displayed on the Identity Source page of the RSA Security Console.  Default value: Internal Database
IsDeleteAllowed	Enter <i>yes</i> to specify that users who have been deleted on the target system must be deleted from Oracle Identity Manager. Use this setting to enable reconciliation of deleted users. If you do not want to use this feature, then enter <i>no</i> as the value of the IsDeleteAllowed attribute.
IsTokenReconAllowed	Enter <i>yes</i> if you want to reconcile both users and tokens. Enter <i>no</i> if you want to reconcile only users.  When you set the value of this attribute to <i>yes</i> , during the reconciliation run, a user's record is fetched first and then the token records for that user are fetched.
IT Resource	Enter the name of the IT resource from which you want to reconcile user data.  Default value: RSA Server Instance
Last Execution Timestamp	This attribute holds the time stamp at which the last user reconciliation run started. A value is automatically entered in this attribute after each reconciliation run.  You can set the value of this attribute to 0 if you want to perform a full reconciliation run. See <a href="#">Section 3.4.1, "Full Reconciliation"</a> for more information.
Scheduled Task Name	This attribute holds the name of the scheduled task.  Default value: RSA Auth Manager User Recon  <b>Note:</b> You must not change the value of this attribute. However, if you create a copy of the scheduled task, then enter the name of the new scheduled task as the value of the Scheduled Task Name attribute.
Token Resource Object	Enter the name of the token resource object that must be used during the reconciliation run. This attribute is used only if you set the IsTokenReconAllowed attribute to <i>yes</i> .  Default value: RSA Auth Manager Token
User Resource Object	Enter the name of the user resource object that must be used during the reconciliation run.  Default value: RSA Auth Manager User
FullRecon Batch Size	Enter the number of records that must be included in each batch fetched from the target system.  If you do not want to implement batched reconciliation, then specify <i>nodata</i> .  Default value: 1000

### 3.4.4.2 RSA Auth Manager Token Recon

[Table 3–3](#) describes the attributes of the scheduled task for token reconciliation.

---

**Note:** Reconciliation of token deletion on the target system is automatically processed by this scheduled task.

---

**Table 3–3 Attributes of the RSA Auth Manager Token Recon Scheduled Task**

Attribute	Description
CustomReconQuery	Enter the query condition that must be applied during the reconciliation run. This is one of the attributes that are used to implement limited reconciliation. <a href="#">Section 3.4.2, "Limited Reconciliation"</a> describes this feature. See <a href="#">Section 3.4.1, "Full Reconciliation"</a> for information about using this attribute to perform a full reconciliation run.
Group	Enter the name of the group on the target system that you want to use for the reconciliation run. Only users or tokens from the group that you specify are considered for the reconciliation run. See <a href="#">Section 3.4.1, "Full Reconciliation"</a> for information about using this attribute to perform a full reconciliation run.
Identity Source	Enter the name of the identity source that must be used during the reconciliation run. The identity source can be the internal database, an external database, or an LDAP solution. Default value: Internal database
IT Resource	Enter the name of the IT resource from which you want to reconcile user data. Default value: RSA Server Instance
Last Execution Timestamp	This attribute holds the time stamp at which the last user reconciliation run started. A value is automatically entered in this attribute after each reconciliation run. See <a href="#">Section 3.4.1, "Full Reconciliation"</a> for information about using this attribute to perform a full reconciliation run.
Scheduled Task Name	This attribute holds the name of the scheduled task. Default value: RSA Auth Manager Token Recon <b>Note:</b> You must not change the value of this attribute. However, if you create a copy of the scheduled task, then enter the name of the new scheduled task as the value of the Scheduled Task Name attribute.
Token Resource Object	Enter the name of the token resource object that must be used during the reconciliation run. This attribute is used only if you set the IsTokenReconAllowed attribute to yes. Default value: RSA Auth Manager Token

## 3.5 Configuring the Scheduled Tasks

This section describes the procedure to configure scheduled tasks. You can apply this procedure to configure the scheduled tasks for lookup field synchronization and reconciliation.

[Table 3–4](#) lists the scheduled tasks that you must configure.

**Table 3–4 Scheduled Tasks for Lookup Field Synchronization and Reconciliation**

Scheduled Task	Description
RSA Auth Manager Lookup Recon	This scheduled task is used for lookup field synchronization.
RSA Auth Manager User Recon	This scheduled task is used for user reconciliation.
RSA Auth Manager Token Recon	This scheduled task is used for token reconciliation.

To configure a scheduled task:

1. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
  - For Oracle Identity Manager release 9.1.0.x:
    - a. Log in to the Administrative and User Console.
    - b. Expand **Resource Management**, and then click **Manage Scheduled Task**.
  - For Oracle Identity Manager release 11.1.1:
    - a. Log in to the Administrative and User Console.
    - b. On the Welcome to Oracle Identity Manager Self Service page, click **Advanced** in the upper-right corner of the page.
    - c. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Search Scheduled Jobs**.
  - For Oracle Identity Manager release 11.1.2.x:
    - a. Log in to Oracle Identity System Administration.
    - b. In the left pane, under System Management, click **Scheduler**.
2. Search for and open the scheduled task as follows:
  - If you are using Oracle Identity Manager release 9.1.0.x, then:
    - a. On the Scheduled Task Management page, enter the name of the scheduled task as the search criteria and then click **Search**.
    - b. In the search results table, click the edit icon in the Edit column for the scheduled task.
    - c. On the Scheduled Task Details page where the details of the scheduled task that you selected is displayed, click **Edit**.
  - If you are using Oracle Identity Manager release 11.1.1 or 11.1.2.x, then:
    - a. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Search Scheduled Jobs**.
    - b. On the left pane, in the Search field, enter the name of the scheduled job as the search criterion. Alternatively, you can click **Advanced Search** and specify the search criterion.
    - c. In the search results table on the left pane, click the scheduled job in the Job Name column.
3. Modify the details of the scheduled task. To do so:
  - a. If you are using Oracle Identity Manager release 9.1.0.x, then on the Edit Scheduled Task Details page, modify the following parameters, and then click **Continue**:
    - **Status**: Specify whether you want to leave the task in the enabled state. In the enabled state, the task is ready for use.
    - **Max Retries**: Enter an integer value in this 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. The default value is 1.

- **Next Start:** Use the date editor to specify the date when you want the task to run. After you select a date value in the date editor, you can modify the time value that is automatically displayed in the Next Start field.
  - **Frequency:** Specify the frequency at which you want the task to run.
- b. If you are using Oracle Identity Manager release 11.1.1 or 11.1.2.x, then on the Job Details tab, you can modify the following parameters:
- **Retries:** Enter an integer value in this field. This number represents the number of times the scheduler tries to start the job before assigning the Stopped status to the job.
  - **Schedule Type:** Depending on the frequency at which you want the job to run, select the appropriate schedule type.

---

**Note:** See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for detailed information about schedule types.

---

In addition to modifying the job details, you can enable or disable a job.

4. Specify values for the attributes of the scheduled task. To do so:

---

**Note:**

- Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.
  - Attributes of the scheduled task are discussed in [Section 3.4.4, "Reconciliation Scheduled Tasks."](#)
- 

- If you are using Oracle Identity Manager release 9.1.0.x, then on the Attributes page, select the attribute from the Attribute list, specify a value in the field provided, and then click **Update**.
  - If you are using Oracle Identity Manager release 11.1.1 or 11.1.2.x, then on the Job Details tab, in the Parameters region, specify values for the attributes of the scheduled task.
5. After specifying the attributes, perform one of the following:
- If you are using Oracle Identity Manager release 9.1.0.x, then click **Save Changes** to save the changes.

---

**Note:** The Stop Execution option is not available in the Administrative and User Console. If you want to stop a task, then click **Stop Execution** on the Task Scheduler form of the Design Console.

---

- If you are using Oracle Identity Manager release 11.1.1 or 11.1.2.x, then click **Apply** to save the changes.

---

**Note:** The Stop Execution option is available in the Administrative and User Console. You can use the Scheduler Status page to either start, stop, or reinitialize the scheduler.

---

## 3.6 Guidelines on Performing Provisioning

Apply the following guidelines while performing provisioning:

- When you try to provision a multivalued attribute, such as a role or group, if the attribute has already been set for the user on the target system, then the status of the process task is set to *Completed* in Oracle Identity Manager. If required, you can configure the task so that it shows the status *Rejected* instead of *Completed*. See *Oracle Identity Manager Design Console Guide* for information about configuring process tasks.
- The value that you enter in the Pin field must be 4 through 8 characters long and contain only numeric values.

## 3.7 Assigning Software Tokens to Users

To assign a software token to a user:

1. Import the software token file into RSA Authentication Manager. See the "Import Tokens" section in RSA Security Console Help for information about the procedure.
2. Assign the software token to the user. See [Section 3.8, "Performing Provisioning Operations in Oracle Identity Manager Release 9.1.0.x and 11.1.1.x"](#) for information about the procedure.
3. Send the software token to the user either by token file or CT-KIP. See the "Distribute Software Tokens" section in RSA Security Console Help for information about the procedure.

## 3.8 Performing Provisioning Operations in Oracle Identity Manager Release 9.1.0.x and 11.1.1.x

Provisioning a resource for an OIM User involves using Oracle Identity Manager to create an RSA Authentication Manager account or token for the user.

When you install the connector on Oracle Identity Manager release 11.1.1, the direct provisioning feature is automatically enabled. This means that the process form is enabled when you install the connector.

If you have configured the connector for request-based provisioning, then the process form is suppressed and the object form is displayed. In other words, direct provisioning is disabled when you configure the connector for request-based provisioning. If you want to revert to direct provisioning, then perform the steps described in [Section 3.8.3, "Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1."](#)

The following are types of provisioning operations:

- Direct provisioning
- Request-based provisioning
- Provisioning triggered by policy changes



**See Also:** *Oracle Identity Manager Connector Concepts* for information about the types of provisioning

This section discusses the following topics:

- [Section 3.8.1, "Direct Provisioning"](#)
- [Section 3.8.2, "Request-Based Provisioning"](#)
- [Section 3.8.3, "Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1"](#)

### 3.8.1 Direct Provisioning

To provision a resource by using the direct provisioning approach:

---

---

**Note:** This procedure describes the Create User provisioning operation. The procedure for the Update User provisioning operation is similar to this one.

---

---

1. Log in to the Administrative and User Console.
2. From the Users menu:
  - Select **Create** if you want to first create the OIM User and then provision an RSA Authentication Manager account to the user.
  - Select **Manage** if you want to provision an RSA Authentication Manager account or token to an existing OIM User.

---

---

**Note:** You must provision an account before you can provision a token to a user.

---

---

3. If you select Create, then on the Create User page, enter values for the OIM User fields and then click **Create User**. [Figure 3–1](#) shows the Create User page.

**Figure 3–1 Create User Page**

**ORACLE Identity Manager**

Welcome System Administrator HOME | LOGOUT | ABOUT

**Create User**  
You may create a new user from this page.

\* Indicates Required Field

User ID \* JDoe  
First Name \* John  
Middle Name  
Last Name \* Doe  
Status  
Organization \* Xellerate Users Clear  
User Type \* End-User  
Employee Type \* Full-Time Employee  
Manager ID Clear  
Email  
User Disabled ☐  
Password \*   
Confirm Password \*   
User Locked ☐  
Start Date   
End Date   
Provisioning Date   
Provisioned Date   
Deprovisioning Date   
Deprovisioned Date   
Change Password at next login ☐

Create User Cancel

Oracle Identity Manager 9.1.0 Copyright © 2008, Oracle Corporation.

- If you select **Manage**, then search for the OIM User and select the link for the user from the list of users displayed in the search results.
- On the User Detail page, select **Resource Profile** from the list at the top of the page. Figure 3–2 shows the User Detail page.

**Figure 3–2 User Detail Page**

**ORACLE Identity Manager**

Welcome System Administrator HOME | LOGOUT | ABOUT

**User Detail**  
This is information about the user.

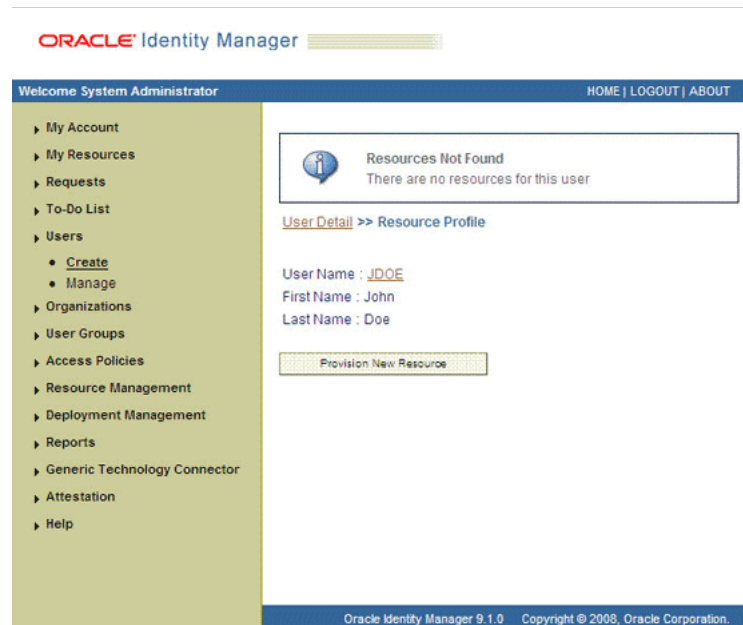
You can view additional details about this user: Select...

User ID JDoe  
First Name John  
Middle Name  
Last Name Doe  
Status Active  
Organization Xellerate Users  
User Type End-User  
Employee Type Full-Time Employee  
Manager ID  
Email  
Start Date  
End Date  
Provisioning Date  
Provisioned Date January 25, 2010  
Deprovisioning Date  
Deprovisioned Date  
Change Password at next login ☐

Edit Disable Unlock Delete Change Password

Oracle Identity Manager 9.1.0 Copyright © 2008, Oracle Corporation.

- On the Resource Profile page, click **Provision New Resource**. Figure 3–3 shows the Resource Profile page.

**Figure 3–3 Resource Profile Page**

7. On the Step 1: Select a Resource page, select **RSA Auth Manager User** from the list and then click **Continue**. Figure 3–4 shows the Step 1: Select a Resource page.

**Figure 3–4 Step 1: Select a Resource Page**

8. On the Step 2: Verify Resource Selection page, click **Continue**. Figure 3–5 shows the Step 2: Verify Resource Selection page.

**Figure 3–5 Step 2: Verify Resource Selection Page**

ORACLE Identity Manager

Welcome System Administrator HOME | LOGOUT | ABOUT

My Account  
My Resources  
Requests  
To-Do List  
Users  
    • Create  
    • Manage  
Organizations  
User Groups  
Access Policies  
Resource Management  
Deployment Management  
Reports  
Generic Technology Connector  
Attestation  
Help

Provision Resource to User  
You are provisioning to John Doe [JDOE].

Step 2: Verify Resource Selection

You have selected to provision RSA Auth Manager User to John Doe [JDOE]

Exit << Back Continue >>

Oracle Identity Manager 9.1.0 Copyright © 2008, Oracle Corporation.

9. On the Step 5: Provide Process Data for RSA Auth Manager User Details page, enter the details of the account that you want to create on the target system and then click **Continue**.

Table 3–5 describes the fields on the user process form.

**Table 3–5 Fields on the User Process Form**

Field	Description
Server Instance	Select the IT resource representing the target system installation on which you want to perform the provisioning operation.
Identity Source	Select the identity source in which you want to perform the provisioning operation.
Security Domain	Select the security domain in which you want to perform the provisioning operation.
First Name	Enter the first name of the user.
Middle Name	Enter the middle name of the user.
Last Name	Enter the last name of the user.
User ID	Enter a user ID for the user.
Password	Enter a password for the user.
Certificate DN	Enter the subject line of the certificate issued to the user for authentication.
Account Start Date	Select the date from which the account must be activated. This field is used in conjunction with the Account Start Hours and Account Start Minutes fields.
Account Start Hours	Select the time (in hours) at which the account must be activated. This field is used in conjunction with the Account Start Date and Account Start Minutes field.
Account Start Minutes	Select the time (in minutes) at which the account must be activated. This field is used in conjunction with the Account Start Date and Account Start Hours field.

**Table 3–5 (Cont.) Fields on the User Process Form**

Field	Description
Account Expire Date	<p>Select the date at which the account must be closed.</p> <p>This field is used in conjunction with the Account Expire Hours and Account Expire Minutes fields.</p>
Account Expire Hours	<p>Select the time (in hours) at which the account must be closed.</p> <p>This field is used in conjunction with the Account Expire Date and Account Expire Minutes field.</p>
Account Expire Minutes	<p>Select the time (in minutes) at which the account must be closed.</p> <p>This field is used in conjunction with the Account Expire Date and Account Expire Hours field.</p>
Fixed Passcode Allowed	<p>Select this check box if you want to allow the user to use a fixed passcode.</p> <p>For authentication purposes, a passcode is an alternative to a password. A user enters a passcode along with the PIN displayed on the token. With a fixed passcode, a user need not use the PIN.</p>
Fixed Passcode	<p>Enter the passcode. The value entered in this field is accepted only if you select the Fixed Passcode Allowed check box.</p>
Clear Incorrect Passcode	<p>Select this check box if you want to clear the count of previous incorrect authentication attempts stored in RSA Authentication Manager. This check box is used only for Update User operations.</p> <p>A policy defined in RSA Authentication Manager specifies the number of incorrect authentication attempts after which the user is locked out of the system. As the administrator, you can select the Clear Incorrect Passcode check box to clear the count and unlock the user.</p>
Clear Windows Passcode	<p>As part of an offline authentication policy, if Microsoft Windows password integration is enabled, then Microsoft Windows passwords of users are stored in RSA Authentication Manager. For authentication, users only need their Windows user name and RSA SecurID passcode.</p> <p>If you select the Clear Windows Passcode check box, then the saved copy of the user's Windows password is deleted and the user has to reenter the Windows password at next logon.</p>
Default Shell	<p>If RSA Authentication Manager is running on a UNIX platform, then use the Default Shell field to specify a default shell or home directory for the user. The specified directory must exist on the target system for the operation to succeed.</p> <p>Sample value: /bin/jdoe</p>

Figure 3–6 shows the user details added.

**Figure 3–6 Step 5: Provide Process Data for RSA Auth Manager User Page**

Provision Resource to User  
You are provisioning to John Doe jdoe@...

Step 5: Provide Process Data  
RSA Auth Manager User Form

**Prepopulate**

\* Indicates required field

Server Instance  [Clear](#)

Identity Source  [Clear](#)

Security Domain

First Name  John

Middle Name  Simon

Last Name  Doe

User ID  jdoe

Password  \*\*\*\*\*

Certificate DN

Account Start Date  January 25, 2010 [Clear](#)

Account Start Hours  12AM [Clear](#)

Account Start Minutes  00 Mins [Clear](#)

Account Expire Date  January 25, 2012 [Clear](#)

Account Expire Hours  11PM [Clear](#)

Account Expire Minutes  59 Mins [Clear](#)

Fixed Passcode Allowed ☒

Fixed Passcode  \*\*\*\*

Clear Incorrect Passcodes ☐

Clear Windows Password ☐

Default Shell  /bin/jdoe

**Back** **Continue >>**

If you are performing a token provisioning operation, then enter values for the fields listed in [Table 3–6](#).

**Table 3–6 Fields on the Token Process Form**

Field	Description
Server Instance	Select the IT resource representing the target system installation on which you want to perform the provisioning operation.
User ID	Enter a user ID for the user.
User Identity Source	Select the identity source in which you want to perform the provisioning operation.
Token Serial Number	Enter the serial number of the token that you want to assign to the user.
Notes	Enter comments for this operation.
Pin	Enter the Pin for the token.
Token Lost	Select this field if the token device assigned to the user is lost. Otherwise, deselect this field.

[Figure 3–7](#) shows the same page for tokens.

**Figure 3–7 Step 5: Provide Process Data for RSA Auth Manager Token Form Page**

Welcome System Administrator

HOME | LOGOUT | ABOUT

Provision Resource to User  
You are provisioning to Test4win Test4win [TEST4WIN].

Step 5: Provide Process Data

RSA Auth Manager Token Form

Prepopulate

\* Indicates required field

Server Instance \* RSA Server Instance Clear

User ID \* TEST4WIN

User Identity Source \* 141~ims.0000000000000000 Clear

Token Serial Number \* 000108600421

Notes Token for test

Pin \*\*\*\*

Token Lost ☐

Exit Continue >>

Oracle Identity Manager 9.1.0 Copyright © 2008, Oracle Corporation.

- On the Step 5: Provide Process Data page, search for and select a role for the user on the target system and then click **Continue**. Figure 3–8 shows this page. The page for selecting a group for the user is similar to this page.

**Figure 3–8 Step 5: Provide Process Data for RSA Auth Manager Role Page**

ORACLE Identity Manager

Welcome System Administrator

HOME | LOGOUT | ABOUT

Provision Resource to User  
You are provisioning to John Doe [JDOE].

Step 5: Provide Process Data

RSA Auth Manager Role Form

Prepopulate

\* Indicates required field

Role Name \* Clear

Add

Exit << Back Continue >>

Oracle Identity Manager 9.1.0 Copyright © 2008, Oracle Corporation.

- On the Step 6: Verify Process Data page, verify the data that you have provided and then click **Continue**.

Figure 3–9 shows the Step 6: Verify Process Data page for the user resource.



**Figure 3–9 Step 6: Verify Process Data Page**

**Step 6: Verify Process Data**

You have selected to provision RSA Auth Manager User to John Doe [JDOE].

**RSA Auth Manager User Form** [Edit](#)

Server Instance	RSA Server Instance
Identity Source	RSA Server Instance-Internal Database
Security Domain	RSA Server Instance-SystemDomain
First Name	John
Middle Name	Simon
Last Name	Doe
User ID	JDOE
Password	*****
Certificate DN	
Account Start Date	January 25, 2010
Account Start Hours	12AM
Account Start Minutes	00 Mins
Account Expire Date	January 25, 2012
Account Expire Hours	11PM
Account Expire Minutes	59 Mins
Fixed Passcode Allowed	1
Fixed Passcode	*****
Clear Incorrect Passcodes	0
Clear Windows Password	0
Default Shell	/bin/jdoe

The Resource Profile page is displayed. [Figure 3–10](#) shows this page. The resource that you provisioned is displayed on this page.

**Figure 3–10 Resource Profile Page**

**ORACLE Identity Manager**

Welcome System Administrator [HOME](#) | [LOGOUT](#) | [ABOUT](#)

[User Detail >> Resource Profile](#)

User Name : [JDOE](#)  
 First Name : John  
 Last Name : Doe

Results 1-1 of 1

Resource Name	Status	Description	Request ID	Resource Form	Process Form	Enable	Disable	Revoke
<a href="#">RSA Auth Manager User</a>	Provisioned	26			<a href="#">View</a> <a href="#">Edit</a>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

[Provision New Resource](#)

First | Previous | Next | Last

Oracle Identity Manager 9.1.0 Copyright © 2008, Oracle Corporation.



## 3.8.2 Request-Based Provisioning

---

**Note:** The information provided in this section is applicable only if you are using Oracle Identity Manager release 11.1.1.

---

A request-based provisioning operation involves both end users and approvers. Typically, these approvers are in the management chain of the requesters. The following sections discuss the steps to be performed by end users and approvers during a request-based provisioning operation:

---

**Note:** The procedures described in these sections are built on an example in which the end user raises or creates a request for provisioning a target system account. This request is then approved by the approver.

---

- [Section 3.8.2.1, "End User's Role in Request-Based Provisioning"](#)
- [Section 3.8.2.2, "Approver's Role in Request-Based Provisioning"](#)

### 3.8.2.1 End User's Role in Request-Based Provisioning

The following steps are performed by the end user in a request-based provisioning operation:

**See Also:** *Oracle Fusion Middleware User's Guide for Oracle Identity Manager* for detailed information about these steps

1. Log in to the Administrative and User Console.
2. On the Welcome page, click **Self-Service** in the upper-right corner of the page.
3. On the Welcome to Identity Manager Self Service page, in the Request region, click **Create Request**.
4. On the Request Beneficiary page, select **Request for Others**, and then click **Next**.
5. From the Request Template list, select **Provision Resource**, and then click **Next**.
6. On the Select Users page, specify a search criterion in the fields to search for the user that you want to provision the resource, and then click **Search**. A list of users that match the search criterion you specify is displayed in the Available Users list.
7. From the **Available Users** list, select the user to whom you want to provision the resource.

If you want to create a provisioning request for more than one user, then from the **Available Users** list, select users to whom you want to provision the account.

8. Click **Move** or **Move All** to include your selection in the Selected Users list, and then click **Next**.
9. On the Select Resources page, click the arrow button next to the Resource Name field to display the list of all available resources.
10. From the Available Resources list, select one of the following, move it to the Selected Resources list, and then click **Next**:
  - If you want to provision an RSA Authentication Manager account, then select **RSA Auth Manager User**.

- If you want to provisioning an RSA Authentication Manager token, then select **RSA Auth Manager Token**.

---

**Note:** The RSA Auth Manager User has to be provisioned before RSA Auth Manager Token.

---

11. On the Resource Details page, enter details of the resource to be provisioned, and then click **Next**.
12. On the Justification page, you can specify values for the following fields, and then click **Finish**.

- Effective Date
- Justification

On the resulting page, a message confirming that your request has been sent successfully is displayed along with the Request ID.

13. If you click the request ID, then the Request Details page is displayed.
14. To view details of the approval, on the Request Details page, click the **Request History** tab.

### 3.8.2.2 Approver's Role in Request-Based Provisioning

The following are steps performed by the approver in a request-based provisioning operation:

The following are steps that the approver can perform:

1. Log in to the Administrative and User Console.
2. On the Welcome page, click **Self-Service** in the upper-right corner of the page.
3. On the Welcome to Identity Manager Self Service page, click the **Tasks** tab.
4. On the **Approvals** tab, in the first section, you can specify a search criterion for request task that is assigned to you.
5. From the search results table, select the row containing the request you want to approve, and then click **Approve Task**.

A message confirming that the task was approved is displayed.

## 3.8.3 Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1

---

**Note:** It is assumed that you have performed the procedure described in [Section 2.3.15, "Configuring Request-Based Provisioning."](#)

---

**On Oracle Identity Manager release 11.1.1, if you want to switch from request-based provisioning to direct provisioning, then:**

1. Log in to the Design Console.
2. Disable the Auto Save Form feature as follows:
  - a. Expand **Process Management**, and then double-click **Process Definition**.
  - b. Search for and open the **RSA Auth Manger User** process definition.

- c. Deselect the **Auto Save Form** check box.
  - d. Click the Save icon.
  - e. Repeat Steps 2.a through 2.d with the following difference:  
While performing Step 2.b, search for and open the **RSA Auth Manager Token** process definition.
3. If the Self Request Allowed feature is enabled, then:
- a. Expand **Resource Management**, and then double-click **Resource Objects**.
  - b. Search for and open the **RSA Auth Manager User** resource object.
  - c. Deselect the **Self Request Allowed** check box.
  - d. Click the Save icon.
  - e. Repeat Steps 3.a through 3.d with the following difference:  
While performing Step 3.c, search for and open the **RSA Auth Manager Token** resource object.

**On Oracle Identity Manager release 11.1.1, if you want to switch from direct provisioning back to request-based provisioning, then:**

- 1. Log in to the Design Console.
- 2. Enable the Auto Save Form feature as follows:
  - a. Expand **Process Management**, and then double-click **Process Definition**.
  - b. Search for and open the **RSA Auth Manager User** process definition.
  - c. Select the **Auto Save Form** check box.
  - d. Click the Save icon.
  - e. Repeat Steps 2.a through 2.d with the following difference:  
While performing Step 2.b search for and open the **RSA Auth Manager Token** process definition.
- 3. If you want to enable end users to raise requests for themselves, then:
  - a. Expand **Resource Management**, and then double-click **Resource Objects**.
  - b. Search for and open the **RSA Auth Manager User** resource object.
  - c. Select the **Self Request Allowed** check box.
  - d. Click the Save icon.
  - e. Repeat Steps 3.a through 3.d with the following difference:  
While performing Step 3.b search for and open the **RSA Auth Manager Token** process definition.

## 3.9 Performing Provisioning Operations in Oracle Identity Manager Release 11.1.2 or Later

To perform provisioning operations in Oracle Identity Manager release 11.1.2 or later:

- 1. Log in to Oracle Identity Administrative and User console.
- 2. Create a user. See the "Managing Users" chapter in *Oracle Fusion Middleware User's Guide for Oracle Identity Manager* for more information about creating a user.

3. On the Account tab, click **Request Accounts**.
4. In the Catalog page, search for and add to cart the application instance created in [Section 2.3.16.4, "Creating an Application Instance"](#) and then click **Checkout**.
5. Specify value for fields in the application form and then click **Ready to Submit**.
6. Click **Submit**.
7. If you want to provision entitlements, then:
  - a. On the Entitlements tab, click **Request Entitlements**.
  - b. In the Catalog page, search for and add to cart the entitlement, and then click **Checkout**.
  - c. Click **Submit**.

---

## Extending the Functionality of the Connector

---

This chapter discusses the following optional procedure:

---

**Note:** These sections describe optional procedures. Perform a procedure only if you want to address the business requirement stated at the start of the section.

---

- [Section 4.1, "Determining Whether an Attribute Is an Identity Management Services or Authentication Manager Attribute"](#)
- [Section 4.2, "Adding New User or Token Attributes for Reconciliation"](#)
- [Section 4.3, "Adding New User or Token Attributes for Provisioning"](#)
- [Section 4.4, "Configuring Validation of Data During Reconciliation and Provisioning"](#)
- [Section 4.5, "Configuring Transformation of Data During Reconciliation"](#)
- [Section 4.6, "Modifying Field Lengths on the Process Form"](#)
- [Section 4.7, "Guideline for Importing the Connector XML File"](#)
- [Section 4.8, "Configuring the Connector for Multiple Installations of the Target System"](#)

### 4.1 Determining Whether an Attribute Is an Identity Management Services or Authentication Manager Attribute

Some of the sections in this chapter describe procedures to map new attributes for reconciliation and provisioning. One of the steps of these procedures is to create an entry in the lookup definition that holds the mapping between target system and Oracle Identity Manager attributes. The Decode value of these lookup definitions contains a setting that requires you to specify whether the attribute is an Identity Management Services or Authentication Manager attribute.

To determine if an attribute is an Identity Management Services or Authentication Manager attribute:

1. Log in to the RSA Security Console.
2. From the Identity list, select **Users** and then select **Manage Existing**.
3. Use the Search feature to display details of either a single user or all users.
4. For any user in the list of users displayed, click the arrow next to the user ID.

5. From the menu displayed:
  - Select **View** to display the list of Identity Management Services attributes.
  - Select **Authentication Setting** to display the list of Authentication Manager attributes.

## 4.2 Adding New User or Token Attributes for Reconciliation

---

**Note:**

- You must ensure that new attributes you add for reconciliation contain only string-format data. Binary data must not be brought into Oracle Identity Manager natively.
  - Only single-valued attributes can be mapped for reconciliation.
  - For Oracle Identity Manager release 11.1.2.x, you must create a new UI form to see this new attribute. See [Section 2.3.16.3, "Creating a New UI Form"](#) for more information.
- 

By default, the attributes listed in [Table 1–4](#) and [Table 1–6](#) are mapped for reconciliation between Oracle Identity Manager and the target system. If required, you can add new attributes for reconciliation.

### Summary of the procedure to add a new user or token attribute for reconciliation

1. Add the new attribute on the process form.
2. Add the attribute to the list of reconciliation fields in the resource object.
3. Create a reconciliation field mapping for the attribute in the process definition.
4. Create an entry for the field in the lookup definition that holds attribute mappings.

### To add a new user or token attribute for reconciliation:

---

**Note:**

See *Oracle Identity Manager Design Console Guide* for detailed information about the steps of this procedure.

If you have already added an attribute for provisioning, then you need not repeat steps performed as part of that procedure.

---

1. Log in to the Oracle Identity Manager Design Console.
2. Add the new attribute on the process form as follows:
  - a. Expand **Development Tools**, and double-click **Form Designer**.
  - b. If you want to add a user attribute, then search for and open the **UD\_AMUSER** process form.  
  
If you want to add a token attribute, then search for and open the **UD\_AMTOKEN** process form.
  - c. Click **Create New Version**, and then click **Add**.
  - d. Enter the details of the field.

For example, if you are adding the Country field, enter UD\_AMUSER\_COUNTRY in the Name field and then enter other details such as Variable Type, Length, Field Label, and Field Type.

- e. Click the Save icon, and then click **Make Version Active**. The following screenshot shows the new field added to the process form:

	Name	Variable Type	Length	Field Label	Field Type	Default Value	Order	Application
8	UD_AMUSER_ACCOUNT_EXPIRE_DATE	Date		Account Expire Date	UserEntry		13	
9	UD_AMUSER_ACCOUNT_EXPIRE_HRS	String	50	Account Expire Hour	LookupField		14	
10	UD_AMUSER_CLR_INCORCT_PASSCD	boolean	1	Clear Incorrect Pass	CheckBox		18	
11	UD_AMUSER_FIXED_PASSCODE	String	255	Fixed Passcode	PasswordField		17	
12	UD_AMUSER_ITRESOURCE	long		Server Instance	ITResourceLoo		1	
13	UD_AMUSER_FIRST_NAME	String	255	First Name	TextField		4	
14	UD_AMUSER_SECURITY_DOMAIN	String	255	Security Domain	LookupField		3	
15	UD_AMUSER_MIDDLE_NAME	String	255	Middle Name	TextField		5	
16	UD_AMUSER_LAST_NAME	String	255	Last Name	TextField		6	
17	UD_AMUSER_CERTIFICATE_DN	String	255	Certificate DN	TextField		9	
18	UD_AMUSER_VWINDOWS_PWD_INTG	boolean	1	Clear Windows Pas	CheckBox		19	
19	UD_AMUSER_ACCOUNT_START_HOUR	String	50	Account Start Hours	LookupField		11	
20	UD_AMUSER_FXD_PASSCODE_ALLOW	boolean	1	Fixed Passcode Allo	CheckBox		16	
21	UD_AMUSER_ACCNT_EXPIRE_MINS	String	50	Account Expire Mini	LookupField		15	
22	UD_AMUSER_COUNTRY	String	255	Country	TextField		21	

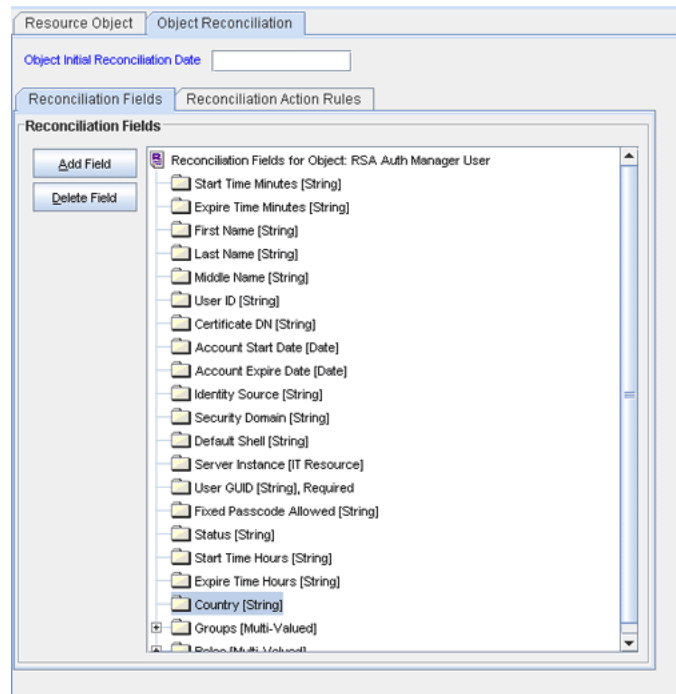
3. Add the new attribute to the list of reconciliation fields in the resource object as follows:

- a. Expand **Resource Management**, and double-click **Resource Objects**.
- b. Search for and open either the **RSA Auth Manager User** or the **RSA Auth Manager Token** resource object.
- c. On the Object Reconciliation tab, click **Add Field**.
- d. Enter the details of the field.

For example, enter Country in the **Field Name** field and select **String** from the Field Type list.

Later in this procedure, you enter the field name as the Code value of the entry that you create in the lookup definition for reconciliation.

- e. Click the Save icon. The following screenshot shows the new reconciliation field added to the resource object:



- f. If you are using Oracle Identity Manager release 11.1.1 or 11.1.2.x, then click **Create Reconciliation Profile**. This copies changes made to the resource object into the MDS.
4. Create a reconciliation field mapping for the new attribute in the process definition as follows:
  - a. Expand **Process Management**, and double-click **Process Definition**.
  - b. Search for and open either the **RSA Auth Manager User** or the **RSA Auth Manager Token** process definition.
  - c. On the **Reconciliation Field Mappings** tab of the **RSA Auth Manager User** process definition, click **Add Field Map**.
  - d. From the **Field Name** list, select the field that you want to map.
  - e. Double-click the **Process Data Field** field, and then select the column for the attribute. For example, select **UD\_AMUSER\_COUNTRY**.
  - f. Click the Save icon. The following screenshot shows the new reconciliation field mapped to a process data field in the process definition:



The screenshot shows the 'Process Definition' window for 'RSA Auth Manager User'. The 'Form Assignment' section shows 'Table Name' as 'UD\_AMUSER'. The 'Reconciliation Field Mappings' tab is active, displaying a list of mappings. On the left, there are buttons for 'Add Field Map', 'Add Table Map', and 'Delete Map'. The list of mappings includes:

- Expire Time Minutes [String] = UD\_AMUSER\_ACCOUNT\_EXPIRE\_MINUTES
- First Name [String] = UD\_AMUSER\_FIRST\_NAME
- Last Name [String] = UD\_AMUSER\_LAST\_NAME
- Middle Name [String] = UD\_AMUSER\_MIDDLE\_NAME
- User ID [String] = UD\_AMUSER\_USER\_ID, <KEY>
- Certificate DN [String] = UD\_AMUSER\_CERTIFICATE\_DN
- Account Start Date [Date] = UD\_AMUSER\_ACCOUNT\_START\_DATE
- Account Expire Date [Date] = UD\_AMUSER\_ACCOUNT\_EXPIRE\_DATE
- Identity Source [String] = UD\_AMUSER\_IDENTITY\_SOURCE
- Security Domain [String] = UD\_AMUSER\_SECURITY\_DOMAIN
- Default Shell [String] = UD\_AMUSER\_DEFAULT\_SHELL
- Server Instance [IT Resource] = UD\_AMUSER\_ITRESOURCE
- User GUID [String] = UD\_AMUSER\_RSA\_GUID, <KEY>
- Fixed Passcode Allowed [String] = UD\_AMUSER\_FIXED\_PASSCODE\_ALLOW
- Status [String] = OIM\_OBJECT\_STATUS
- Start Time Hours [String] = UD\_AMUSER\_ACCOUNT\_START\_HOURS
- Expire Time Hours [String] = UD\_AMUSER\_ACCOUNT\_EXPIRE\_HOURS
- Country [String] = UD\_AMUSER\_COUNTRY

At the bottom of the list, there is a note: 'Role: Multi-Valued = Table UD\_AMUSER'.

5. Create an entry for the field in the lookup definition for reconciliation as follows:

- Expand **Administration**.
- Double-click **Lookup Definition**.
- Search for and open either the **Lookup.RSA.AuthManager.UserReconAttrMap** or the **Lookup.RSA.AuthManager.TokenReconAttrMap** lookup definition.
- Click **Add** and enter the Code Key and Decode values for the field. The Code Key value must be the name of the field in the resource object. Enter the Decode value in the following format:

```
METHOD_NAME;PRINCIPAL_TYPE;ATTRIBUTE_TYPE;RETURN_TYPE_OF_METHOD;RESOURCE_OBJECT_FIELD_TYPE;DTO_ATTRIBUTE_NAME
```

See [Section 1.6.1, "User Attributes for Reconciliation"](#) for information about this format.

- Click the Save icon. The following screenshot shows the entry added to the lookup definition:

	Code Key ▼	Decode
1	Account Expire Date	accountExpireDate;IMS;Core;Date;Date
2	Account Start Date	accountStartDate;IMS;Core;Date;Date
3	Certificate DN	certificateDN;IMS;Core;String;Text;CERTDN
4	Country	Country;IMS;Extended;String;Text
5	Default Shell	defaultShell;AM;Core;String;Text
6	First Name	firstName;IMS;Core;String;Text;FIRST_NAME
7	Fixed Passcode Allowed	staticPasswordSet;AM;Core;boolean;CheckBox
8	Identity Source	identitySourceGuid;IMS;Core;String;Lookup
9	Last Name	lastName;IMS;Core;String;Text;LAST_NAME
10	Middle Name	middleName;IMS;Core;String;Text;MIDDLE_NAME
11	Security Domain	securityDomainGuid;IMS;Core;String;Lookup
12	User GUID	Guid;IMS;Core;String;String
13	User ID	userId;IMS;Core;String;Text;LOGINUID

### 4.3 Adding New User or Token Attributes for Provisioning

By default, the attributes listed in [Table 1–9](#) and [Table 1–11](#) are mapped for provisioning between Oracle Identity Manager and the target system. If required, you can map additional attributes for provisioning.

---

#### Note:

- Only single-valued attributes can be mapped for provisioning.
  - For Oracle Identity Manager release 11.1.2.x, you must create a new UI form to see this new attribute. See [Section 2.3.16.3, "Creating a New UI Form"](#) for more information.
- 

#### Summary of the procedure to add a new user or token attribute for provisioning

1. Add the new attribute on the process form.
2. Create an entry for the attribute in the lookup definition that holds attribute mappings.
3. Create a task to enable update of the attribute during provisioning operations.

#### To add a new user or token attribute for provisioning:

---

**Note:** See *Oracle Identity Manager Design Console Guide* for detailed information about the steps of this procedure.

If you have already added an attribute for reconciliation, then you need not repeat steps performed as part of that procedure.

---

1. Log in to the Oracle Identity Manager Design Console.
2. Add the new attribute on the process form as follows:
  - a. Expand **Development Tools**, and double-click **Form Designer**.

- b. If you want to add a user attribute, then search for and open the **UD\_AMUSER** process form.

If you want to add a token attribute, then search for and open the **UD\_AMTOKEN** process form.

- c. Click **Create New Version**, and then click **Add**.
- d. Enter the details of the attribute.

For example, if you are adding the Country field, enter **UD\_AMUSER\_COUNTRY** in the Name field, and then enter the rest of the details of this field.

- e. Click the Save icon, and then click **Make Version Active**. The following screenshot shows the new field added to the process form:

Name	Variant Type	Length	Field Label	Field Type	Default Value	Order	Application
UD_AMUSER_ACCOUNT_EXPIRE_DATE	Date	50	Account Expire Date	LookupField		13	
UD_AMUSER_ACCOUNT_EXPIRE_HRS	String	50	Account Expire Hour	LookupField		14	
UD_AMUSER_CLR_INCORCT_PASSCD	boolean	1	Clear Incorrect Pass	CheckBox		18	
UD_AMUSER_FIXED_PASSCODE	String	255	Fixed Passcode	PasswordField		17	
UD_AMUSER_ITRESOURCE	long		Server Instance	ITResourceLoo		1	
UD_AMUSER_FIRST_NAME	String	255	First Name	TextField		4	
UD_AMUSER_SECURITY_DOMAIN	String	255	Security Domain	LookupField		3	
UD_AMUSER_MIDDLE_NAME	String	255	Middle Name	TextField		5	
UD_AMUSER_LAST_NAME	String	255	Last Name	TextField		6	
UD_AMUSER_CERTIFICATE_DN	String	255	Certificate DN	TextField		9	
UD_AMUSER_WINDOWS_PWD_INTG	boolean	1	Clear Windows Pas	CheckBox		19	
UD_AMUSER_ACCOUNT_START_HOUR	String	50	Account Start Hours	LookupField		11	
UD_AMUSER_FXD_PASSCODE_ALLOW	boolean	1	Fixed Passcode Allo	CheckBox		16	
UD_AMUSER_ACNT_EXPIRE_MINS	String	50	Account Expire Mini	LookupField		15	
UD_AMUSER_COUNTRY	String	255	Country	TextField		21	

3. Create an entry for the attribute in the lookup definition for provisioning as follows:

- a. Expand **Administration**.
- b. Double-click **Lookup Definition**.
- c. Search for and open either the **Lookup.RSA.AuthManager.UserAttrMap** or the **Lookup.RSA.AuthManager.TokenAttrMap** lookup definition.
- d. Click **Add** and then enter the Code Key and Decode values for the attribute.

See [Section 1.7.2, "User Attributes for Provisioning"](#) for information about the format of the value to be entered in the Decode column.

For example, enter **Country** in the **Code Key** column and then enter **Country;IMS;Extended;String** in the **Decode** column. The following screenshot shows the entry added to the lookup definition:

	Code Key	Decode
1	Default Shell	defaultShell;AM;Core;String
2	Fixed Passcode Allowed	staticPasswordSet;AM;Core;boolean
3	First Name	firstName;IMS;Core;String;FIRST_NAME
4	Last Name	lastName;IMS;Core;String;LAST_NAME
5	Middle Name	middleName;IMS;Core;String;MIDDLE_NAME
6	User ID	userId;IMS;Core;String;LOGINUID
7	Certificate DN	certificateDN;IMS;Core;String;CERT_DN
8	Password	Password;IMS;Core;String;PASSWORD
9	Account Start Date	accountStartDate;IMS;Core;Date;START_DATE
10	Account Expire Date	accountExpireDate;IMS;Core;Date;EXPIRATION_DATE
11	Fixed Passcode	staticPassword;AM;Core;String
12	Clear Incorrect Passcodes	clearBadPasscodes;AM;Core;boolean
13	Clear Windows Password	ClearWindowsLoginPassword;AM;Core;boolean
14	Identity Source	identitySourceGuid;IMS;Core;String;IDENTITY_SOURCE
15	Security Domain	securityDomainGuid;IMS;Core;String;OWNER_ID
16	Country	Country;IMS;Extended;String

4. Create a task to enable update of the attribute during provisioning operations.

If you do not perform this procedure, then you will not be able to modify the value of the attribute after you set a value for it during the Create User provisioning operation.

To enable the update of the attribute during provisioning operations, add a process task for updating the attribute:

**See Also:** *Oracle Identity Manager Design Console Guide* for detailed information about these steps

- a. Expand **Process Management**, and double-click **Process Definition**.
- b. Search for and open either the **RSA Auth Manager User** or the **RSA Auth Manager Token** process definition.
- c. Click **Add**.
- d. On the General tab of the Creating New Task dialog box, enter a name and description for the task and then select the following:
  - Conditional
  - Required for Completion
  - Allow Cancellation while Pending
  - Allow Multiple Instances
- e. Click the Save icon. The following screenshot shows the new task added to the process definition:

- f. On the Integration tab of the Creating New Task dialog box, click **Add**.
- g. In the Handler Selection dialog box, select **Adapter**, click **adpRSAMUPDATEUSER**, and then click the Save icon.

The list of adapter variables is displayed on the Integration tab. The following screenshot shows the list of adapter variables:

Map	Mapped (Y/N)	Name	Description
1	N	pParentFormProc...	Parent Form Process Instance Key
2	N	sITResourceUDField	IT Resource UDField
3	N	sUserGuid	GUID of the user
4	N	sIdSourceGuid	GUID of user identity source
5	N	sDomainGuid	GUID of user security domain
6	N	sAttributeName	Name of the modified attribute
7	N	Adapter return val...	Return variable

- h. To create the mapping for the first adapter variable:  
Double-click the number of the first row.  
In the Edit Data Mapping for Variable dialog box, enter the following values:  
**Variable Name:** pParentFormProcessInstanceKey  
**Map To:** Process Data  
**Qualifier:** Process Instance  
Click the Save icon.
- i. To create mappings for the remaining adapter variables, use the data given in the following table:

Variable Number	Variable Name	Map To	Qualifier
Second	sITResourceUDField	Literal	String For Example: UD_AMUSER_ITRESOURCE

Variable Number	Variable Name	Map To	Qualifier
Third	sUserGuid	Process Data	User GUID
Fourth	sIdSourceGuid	Process Data	Identity Source
Fifth	sDomainGuid	Process Data	Security Domain
Sixth	sAttributeName	Literal	String For Example: Country
Seventh	Adapter return value	Response Code	Not applicable

- j. Click the Save icon in the Editing Task dialog box, and then close the dialog box.
- k. Click the Save icon to save changes to the process definition.

## 4.4 Configuring Validation of Data During Reconciliation and Provisioning

You can configure validation of reconciled and provisioned data according to your requirements. For example, you can validate data fetched from the First Name attribute to ensure that it does not contain the at sign (@). In addition, you can validate data entered in the First Name field on the process form so that the at sign (@) is not sent to the target system during provisioning operations.

For data that fails the validation check, the following message is displayed or recorded in the log file:

Value returned for field *FIELD\_NAME* is false.

To configure validation of data:

1. Write code that implements the required validation logic in a Java class.

This validation class must implement the `oracle.iam.connectors.common.validate.Validator` interface and the `validate` method.

**See Also:** The Javadocs shipped with the connector for more information about this interface

The following sample validation class checks if the value in the First Name attribute contains the at sign (@):

```
public boolean validate(HashMap hmUserDetails,
    HashMap hmEntitlementDetails, String field) {
    /*
     * You must write code to validate attributes. Parent
     * data values can be fetched by using hmUserDetails.get(field)
     * For child data values, loop through the
     * ArrayList/Vector fetched by hmEntitlementDetails.get("Child Table")
     * Depending on the outcome of the validation operation,
     * the code must return true or false.
     */
    /*
     * In this sample code, the value "false" is returned if the field
     * contains the number sign (#). Otherwise, the value "true" is
     * returned.
     */
}
```



```

        boolean valid=true;
        String sFirstName=(String) hmUserDetails.get(field);
        for(int i=0;i<sFirstName.length();i++){
            if (sFirstName.charAt(i) == '#'){
                valid=false;
                break;
            }
        }
        return valid;
    }
}

```

2. Create a JAR file to hold the Java class.
3. Copy the JAR file into the JavaTasks or ScheduleTask directory.
4. If you created the Java class for validating a user or token attribute for reconciliation, then:
  - a. Log in to the Design Console.
  - b. Search for and open one of the following lookup definitions:
    - For a user attribute, open **Lookup.RSA.AuthManager.UserReconValidation**.
    - For a token attribute, open **Lookup.RSA.AuthManager.TokenReconValidation**.
  - c. In the **Code Key** column, enter the resource object field name. In the **Decode** column, enter the class name.
  - d. Save the changes to the lookup definition.
  - e. Search for and open the **Lookup.RSA.AuthManager.Configuration** lookup definition.
  - f. Set the value of one of the following entries to **yes** :
    - For a user attribute, set **Use Validation For UserRecon** to **yes**.
    - For a token attribute, set **Use Validation For TokenRecon** to **yes**.
  - g. Save the changes to the lookup definition.
5. If you created the Java class for validating an attribute for provisioning, then:
  - a. Log in to the Design Console.
  - b. Search for and open one of the following lookup definitions:
    - For a user attribute, open **Lookup.RSA.AuthManager.UserProvisioningValidation**.
    - For a token attribute, open **Lookup.RSA.AuthManager.TokenProvisioningValidation**.
  - c. In the **Code Key** column, enter the process form field name. In the **Decode** column, enter the class name.
  - d. Save the changes to the lookup definition.
  - e. Search for and open the **Lookup.RSA.AuthManager.Configuration** lookup definition.
  - f. Set the value of one of the following entries to **yes** :
    - For a user attribute, set **Use Validation For UserProv** to **yes**.

- For a token attribute, set **Use Validation For TokenProv** to yes.
- g. Save the changes to the lookup definition.

## 4.5 Configuring Transformation of Data During Reconciliation

You can configure transformation of reconciled single-valued user data according to your requirements. For example, you can use First Name and Last Name values to create a value for the Full Name field in Oracle Identity Manager.

To configure transformation of single-valued user data fetched during reconciliation:

1. Write code that implements the required transformation logic in a Java class.

This transformation class must implement the `oracle.iam.connectors.common.transform.Transformation` interface and the `transform` method.

**See Also:** The Javadocs shipped with the connector for more information about this interface

The following sample transformation class creates a value for the Full Name attribute by using values fetched from the First Name and Last Name attributes of the target system:

```
package oracle.iam.connectors.common.transform;

import java.util.HashMap;

public class TransformAttribute implements Transformation {

    /**
     Description:Abstract method for transforming the attributes

     param hmUserDetails<String,Object>

     HashMap containing parent data details

     param hmEntitlementDetails <String,Object>

     HashMap containing child data details

     */
    public Object transform(HashMap hmUserDetails, HashMap
hmEntitlementDetails,String sField) {
        /**
         * You must write code to transform the attributes.
         Parent data attribute values can be fetched by
         using hmUserDetails.get("Field Name").
         *To fetch child data values, loop through the
         * ArrayList/Vector fetched by hmEntitlementDetails.get("Child
Table")
         * Return the transformed attribute.
         */
        String sFirstName= (String)hmUserDetails.get("First Name");
        String sLastName= (String)hmUserDetails.get("Last Name");
        String sFullName=sFirstName+"."+sLastName;
        return sFullName;
    }
}
```



2. Create a JAR file to hold the Java class.
3. Copy the JAR file into the JavaTasks or ScheduleTask directory.
4. If you created the Java class for transforming an attribute for reconciliation, then:
  - a. Log in to the Design Console.
  - b. Search for and open one of the following lookup definitions:
    - For a token attribute, open **Lookup.RSA.AuthManager.TokenTransformMapping**.
    - For a user attribute, open **Lookup.RSA.AuthManager.UserTransformMapping**.
  - c. In the **Code Key** column, enter the resource object field name. In the **Decode** column, enter the class name.
  - d. Save the changes to the lookup definition.
  - e. Search for and open the **Lookup.RSA.AuthManager.Configuration** lookup definition.
  - f. Depending on whether you are applying the transformation to a user or token attribute, set either the **Use Token Transform Mapping** or the **Use User Transform Mapping** entry to **yes**.
  - g. Save the changes to the lookup definition.

## 4.6 Modifying Field Lengths on the Process Form

You might want to modify the lengths of fields (attributes) on the process form. For example, if you use the Japanese locale, then you might want to increase the lengths of process form fields to accommodate multibyte data from the target system.

If you want to modify the length of a field on the process form, then:

1. Log in to the Design Console.
2. Expand **Development Tools**, and double-click **Form Designer**.
3. Search for and open the **UD\_AMUSER** process form.

---

**Note:** If you want to change field lengths on the token process form, then open the **UD\_AMTOKEN** form. The remaining steps of the procedure are the same for both process forms.

---

4. Click **Create New Version**.
5. Enter a label for the new version, click the Save icon, and then close the dialog box.
6. From the **Current Version** list, select the version that you create.
7. Modify the length of the required field.
8. Click the Save icon.
9. Click **Make Version Active**.

## 4.7 Guideline for Importing the Connector XML File

---

**Note:** This section describes a guideline that you must apply if you are planning to create (or modify) and then import the connector XML file on an Oracle Identity Manager installation running on IBM WebSphere Application Server.

---

When you install the connector, you copy JAR files from the RSA Authentication Manager home directory to the application server home directory. You might encounter an error if you try to run the Deployment Manager or Connector Installer without first removing these JAR files from the application server home directory. [Section 2.1.4, "Removing RSA Authentication Manager JAR Files from the IBM WebSphere Application Server Home Directory"](#) describes this issue. To avoid this issue:

1. Perform the procedure described in [Section 2.1.4, "Removing RSA Authentication Manager JAR Files from the IBM WebSphere Application Server Home Directory."](#)
2. Import the revised connector XML file by using the Deployment Manager. Alternatively, if you have created a deployment package using the modified connector XML file, then run the Connector Installer.
3. Perform the procedure described in [Section 2.3.6, "Copying Target System Files to Oracle Identity Manager."](#)

## 4.8 Configuring the Connector for Multiple Installations of the Target System

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

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

To meet the requirement posed by such a scenario, you can create copies of connector objects, such as the IT resource and resource object.

The decision to create a copy of a connector object might be based on a requirement. For example, an IT resource can hold connection information for one target system installation. Therefore, it is mandatory to create a copy of the IT resource for each target system installation.

With some other connector objects, you do not need to create copies at all. For example, a single attribute-mapping lookup definition can be used for all installations of the target system.

All connector objects are linked. For example, a scheduled task holds the name of the IT resource. Similarly, the IT resource holds the name of the configuration lookup definition (Lookup.RSA.AuthManager.Configuration). If you create a copy of an object, then you must specify the name of the copy in associated connector objects. [Table 4–1](#) lists associations between connector objects whose copies can be created and the other objects that reference these objects. When you create a copy of a connector object, use this information to change the associations of that object with other objects.

---

**Note:** If you create a copy of a connector object, then you must set a unique name for it.

---

**Table 4–1** *Connector Objects and Their Associations*

Connector Object	Name	Referenced By	Comments on Creating a Copy
IT resource	RSA Server Instance	RSA Auth Manager Lookup Recon (scheduled task) RSA Auth Manager User Recon (scheduled task) RSA Auth Manager Token Recon (scheduled task)	Create a copy of the IT resource. See <a href="#">Section 2.3.13, "Configuring Connection Parameters"</a> for more information.
Resource objects	RSA Auth Manager User (user resource object) RSA Auth Manager Token (token resource object)	RSA Auth Manager User Recon (scheduled task) RSA Auth Manager Token Recon (scheduled task)	If you are reconciling the same set of attributes from all installations of the target system, then you need not create a copy of the resource object. In other words, create copies of the resource object only if there are differences in attributes between the various installations of the target system. See <a href="#">Section 3.4.4, "Reconciliation Scheduled Tasks"</a> for more information.
Process definition	RSA Auth Manager User	NA	Create copies of this process definition only if there are difference in attributes between the installations of the target system.
Attribute Mapping Lookup Definition	Lookup.RSA.AuthManager.UserAttrMap Lookup.RSA.AuthManager.UserChildAttrMap Lookup.RSA.AuthManager.UserReconAttrMap Lookup.RSA.AuthManager.UserReconChildAttrMap Lookup.RSA.AuthManager.TokenAttrMap Lookup.RSA.AuthManager.TokenReconAttrMap	NA	Create copies of this process definition only if there are difference in attributes between the installations of the target system. See the following sections for more information: <a href="#">Section 1.6, "Connector Objects Used During Reconciliation"</a> <a href="#">Section 1.7, "Connector Objects Used During Provisioning"</a>
Process form	UD_AMUSER	NA	It is optional to create a copy of a process form. If you are provisioning different sets of attributes, then you need to create a copy of this connector object.
Configuration lookup definition	Lookup.RSA.AuthManager.Configuration	RSA Server Instance (IT resource)	Create copies of this lookup definition only if you want to use a different set of configuration values for the various installations of the target system. See <a href="#">Section 2.3.10, "Setting Up the Configuration Lookup Definition in Oracle Identity Manager"</a> for more information.

**When you configure reconciliation:**

To reconcile data from a particular target system installation, specify the name of the IT resource for that target system installation as the value of the scheduled task attribute that holds the IT resource name. For example, you enter the name of the IT resource as the value of the IT resource attribute of the RSA Auth Manager User Recon and RSA Auth Manager Token Recon scheduled tasks.

**When you perform provisioning operations:**

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

---

## Known Issues and Limitations

This chapter is divided into the following sections:

- [Section 5.1, "Known Issues"](#)
- [Section 5.2, "Limitations"](#)

### 5.1 Known Issues

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

- **Bug 7207232**

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.

- **Bug 9268577**

If there are a large number users or tokens to be reconciled during full reconciliation, then the `InvalidSessionException` exception might be encountered.

See [Section 3.3, "Guidelines on Performing Reconciliation"](#) for information about a workaround to this issue.

### 5.2 Limitations

The following are connector limitations arising from features of the target system:

- In the earlier release of the target system, the next token code mode could be set through an administrative API. RSA Authentication Manager 7.1 does not support this feature.
- In RSA Authentication Manager 7.1, a group assignment change for a user updates neither the group record nor the user record. Therefore, incremental reconciliation does not bring the updated user record into Oracle Identity Manager.
- On the target system, the Lock User and Unlock User operations can be performed only through the application of lockout policies defined on the target system. The connector does not provide a UI option for these features.

- The connector does not support fetching of the emergency access token code if the token is lost

---

---

# Index

## A

---

adapters, 1-19  
AMPrincipalDTO API, 1-13, 1-20  
assigning software tokens, 3-10  
attributes, adding new, 4-2

## C

---

certified components, 1-1  
certified languages, 1-2  
changing input locale, 2-8  
clearing server cache, 2-8  
common.jar file, 2-1, 2-3, 2-7  
communication modes  
    SOAP-based, 2-44  
connector files and directories, 2-1  
connector functionality, extending, 4-1  
Connector Installer, 2-5  
connector operations, target system account, 2-27  
connector release number, determining, 2-2

## D

---

determining release number of connector, 2-2  
disabling accounts, 1-5

## E

---

enabling accounts, 1-5  
enabling logging, 2-10  
exclusion list, 1-6, 1-10, 2-37, 2-41  
extending connector functionality, 4-1

## F

---

field lengths, modifying, 4-13  
files and directories of the connector  
    *See* connector files and directories  
filtered reconciliation, 1-5, 3-4  
full reconciliation, 1-5, 1-10

## I

---

Identity Management Services attributes, 1-13, 1-19, 1-21  
incremental reconciliation, 1-5

input locale, changing, 2-8  
installation  
    preinstallation, 2-1  
installing connector, 2-1  
issues, 5-1  
IT resources, 2-43  
IT resources, parameters, 2-43

## J

---

Java API, 2-18  
JAVA\_OPTIONS parameters, 2-24

## K

---

known issues, 5-1

## L

---

limitations, 5-1  
limited reconciliation, 1-5, 3-4  
ListTokenDTO API, 1-13, 1-14, 1-15, 1-19, 1-21  
logging enabling, 2-10  
lookup definitions  
    Lookup.RSA.AuthManager.AdminRole, 1-9, 1-10  
    Lookup.RSA.AuthManager.Configuration, 1-10, 2-37, 2-44, 4-11, 4-13, 4-14, 4-15  
    Lookup.RSA.AuthManager.Constants, 1-10, 2-37  
    Lookup.RSA.AuthManager.DateMappings, 1-10, 2-37  
    Lookup.RSA.AuthManager.FullReconFilter, 1-10, 2-37  
    Lookup.RSA.AuthManager.Group, 1-7, 1-10, 2-16  
    Lookup.RSA.AuthManager.Hours, 1-10  
    Lookup.RSA.AuthManager.IdentitySource, 1-8, 1-10  
    Lookup.RSA.AuthManager.ITResourceMapping, 1-11, 2-35, 2-36, 2-37  
    Lookup.RSA.AuthManager.LookupReconMapping, 1-9, 2-37  
    Lookup.RSA.AuthManager.Minutes, 1-10  
    Lookup.RSA.AuthManager.SecurityDomain, 1-8, 1-10  
    Lookup.RSA.AuthManager.TokenAttrMap, 1-11, 1-20, 2-38, 4-7, 4-15  
    Lookup.RSA.AuthManager.TokenProvisioningVali





- 3-2, 3-7, 4-15
- RSA Auth Manager Token Recon, 1-3, 3-6, 3-7, 4-15, 4-16
- RSA Auth Manager User Recon, 1-3, 1-6, 3-5, 3-7, 4-15, 4-16
- scheduled tasks attributes, 3-5
- server cache, clearing, 2-8
- SOAP-based communication, 2-44
- software tokens, assigning, 3-10
- standard target system attributes, 4-6
- supported
  - releases of Oracle Identity Manager, 1-2
  - target systems, 1-2

## **T**

---

- target resource reconciliation, 1-1
  - reconciliation action rules, 1-17
- target system account for connector operations, 2-27
- target system, multiple installations, 4-14
- target systems supported, 1-2
- token reconciliation rule, 1-16
- TokenDTO API, 1-13, 1-14, 1-15, 1-19, 1-21
- transformation, 1-6, 1-11, 1-12, 2-39, 4-12

## **U**

---

- user reconciliation rule, 1-15

## **V**

---

- validation, 1-6, 1-12, 2-39, 2-40, 2-41, 4-10

