# Oracle® Identity Manager

Connector Guide for RSA Authentication Manager

Release 9.1.0

**E16663-02**

June 2011

Oracle Identity Manager Connector Guide for RSA Authentication Manager, Release 9.1.0

E16663-02

Primary Author: Alankrita Prakash

Contributing Authors: Prakash Hulikere, Sridhar Machani

# Contents

**Preface** ..... xi

Audience ..... xi
Documentation Accessibility ..... xi
Related Documents ..... xi
Documentation Updates ..... xi
Conventions ..... xii

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

Software Updates ..... xiii
Documentation-Specific Updates ..... xvi

**1 About the Connector**

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 ....................................... 2-2
2.1.4 Removing RSA Authentication Manager JAR Files from the IBM WebSphere Application Server Home Directory 2-4
2.2 Installation ............................................................................................................... 2-4
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 ............................................................................................... 2-9
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 .......................... 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 .................................... 2-21
2.3.6 Copying Target System Files on Oracle Identity Manager ........................................ 2-21
2.3.7 Setting Values for JAVA_OPTIONS Parameters ........................................................ 2-23
2.3.7.1 Setting Values for JAVA_OPTIONS Parameters on IBM WebSphere Application Server 2-24
2.3.7.2 Setting Values for JAVA_OPTIONS Parameters on JBoss Application Server 2-24
2.3.7.3 Setting Values for JAVA_OPTIONS Parameters on Oracle Application Server ......... 2-25
2.3.7.4 Setting Values for JAVA_OPTIONS Parameters on Oracle WebLogic Server . 2-26
2.3.8 Creating a Target System Account for Connector Operations .................................. 2-26
2.3.9 Mapping New Connection Properties ........................................................................ 2-34
2.3.10 Setting Up the Configuration Lookup Definition in Oracle Identity Manager ....... 2-36
2.3.11 Setting Up the Lookup.RSA.AuthManager.ExclusionList Lookup Definition ....... 2-40
2.3.12 Modifying the Process Form ............................................................................ 2-41

2.3.13 Configuring Connection Parameters .......... 2-42
2.3.14 Creating Authorization Policies for User Management.......... 2-43
2.3.14.1 Creating an Authorization Policy for Provisioning.......... 2-43
2.3.14.2 Creating an Authorization Policy for Reconciliation .......... 2-44
2.3.15 Configuring Request-Based Provisioning.......... 2-45
2.3.15.1 Copying Predefined Request Datasets .......... 2-46
2.3.15.2 Importing Request Datasets into MDS.......... 2-47
2.3.15.3 Enabling the Auto Save Form Feature .......... 2-47
2.3.15.4 Running the PurgeCache Utility .......... 2-48

## 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 .......... 3-2
3.4 Configuring Reconciliation.......... 3-3
3.4.1 Full Reconciliation .......... 3-3
3.4.2 Limited Reconciliation .......... 3-3
3.4.3 Batched Reconciliation.......... 3-4
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.......... 3-9
3.7 Assigning Software Tokens to Users .......... 3-9
3.8 Performing Provisioning Operations.......... 3-10
3.8.1 Direct Provisioning.......... 3-10
3.8.2 Request-Based Provisioning.......... 3-18
3.8.2.1 End User's Role in Request-Based Provisioning.......... 3-18
3.8.2.2 Approver's Role in Request-Based Provisioning.......... 3-19
3.9 Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1 3-19

## 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 ........ 3-11
3–2 User Detail Page........ 3-11
3–3 Resource Profile Page........ 3-12
3–4 Step 1: Select a Resource Page........ 3-12
3–5 Step 2: Verify Resource Selection Page ........ 3-13
3–6 Step 5: Provide Process Data for RSA Auth Manager User Page ........ 3-15
3–7 Step 5: Provide Process Data for RSA Auth Manager Token Form Page........ 3-16
3–8 Step 5: Provide Process Data for RSA Auth Manager Role Page........ 3-16
3–9 Step 6: Verify Process Data Page ........ 3-17
3–10 Resource Profile Page........ 3-17

## 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 ........ 2-12
2–3 Child Forms ........ 2-14
2–4 Entries in the Lookup.RSA.AuthManager.ITResourceMapping Lookup Definition ........ 2-35
2–5 Entries in the Lookup.RSA.AuthManager.Configuration Lookup Definition ........ 2-36
2–6 Parameters of the IT Resource ........ 2-43
3–1 Attributes of the RSA Auth Manager Lookup Recon Scheduled Task ........ 3-2
3–2 Attributes of the RSA Auth Manager User Recon Scheduled Task ........ 3-5
3–3 Attributes of the RSA Auth Manager Token Recon Scheduled Task ........ 3-6
3–4 Scheduled Tasks for Lookup Field Synchronization and Reconciliation ........ 3-7
3–5 Fields on the User Process Form ........ 3-13
3–6 Fields on the Token Process Form ........ 3-15
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 |
|---|---|
| **boldface** | Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary. |
| *italic* | Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values. |
| `monospace` | Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter. |

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

This chapter provides an overview of the updates made to the software and documentation for the RSA Authentication Manager connector in release 9.1.0.7.

> **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 11*g* 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 11*g* 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 on 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"

# 1 About the Connector

Oracle Identity Manager automates access rights management, security, and provisioning of IT resources. Oracle Identity Manager connectors are used to integrate Oracle Identity Manager with 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 | You can use one of the following releases of Oracle Identity Manager:<br>■ Oracle Identity Manager release 9.1.0.2 BP05 or later<br>**Note:**<br>- In this guide, **Oracle Identity Manager release 9.1.0.*x*** 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.<br>- 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<br>`http://www.oracle.com/technetwork/documentation/oim1014-097544.html`<br>■ Oracle Identity Manager 11*g* release 1 (11.1.1)<br>**Note:** In this guide, **Oracle Identity Manager release 11.1.1** has been used to denote Oracle Identity Manager 11*g* release 1 (11.1.1). |
| JDK | The JDK requirement is as follows:<br>■ For Oracle Identity Manager release 9.1.0.*x*, use JDK 1.5 or a later release in the 1.5 series.<br>■ For Oracle Identity Manager release 11.1.1, use JDK 1.6 update 18 or later or JRockit JDK 1.6 update 17 or later.<br>See Section 2.3.7, "Setting Values for JAVA_OPTIONS Parameters" if you are using JDK 1.6. |
| Target system | RSA Authentication Manager 7.1 with SP3 or later |

## 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:

  *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.

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

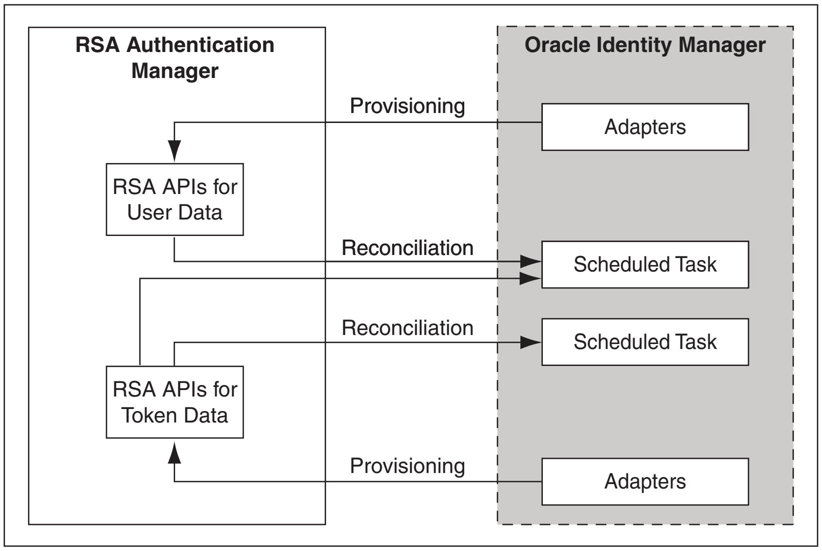
The RSA Auth Manager User Recon scheduled task can be configured to reconcile token data. Alternatively, you can use the RSA Auth Manager Token Recon scheduled task for token reconciliation.

**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.000000000000000000001000e0031000 | RSA Server Instance~SuperAdminRole |
| 1~ ims.000000000000000000001000e0031001 | 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<br>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).<br>Figure 3–6 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. Section 2.3.10, "Setting Up the Configuration Lookup Definition in Oracle Identity Manager" 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 Section 2.3.11, "Setting Up the Lookup.RSA.AuthManager.ExclusionList Lookup Definition" 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.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 Section 2.3.9, "Mapping New Connection Properties" 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. Table 1–9 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 Section 4.3, "Adding New User or Token Attributes for Provisioning" 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. Table 1–10 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. Table 1–5 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. Table 1–11 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 Section 4.3, "Adding New User or Token Attributes for Provisioning" 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. Table 1–4 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 Section 4.2, "Adding New User or Token Attributes for Reconciliation" 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. Table 1–8 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 Section 4.2, "Adding New User or Token Attributes for Reconciliation" 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 Section 4.5, "Configuring Transformation of Data During Reconciliation" 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 Section 4.5, "Configuring Transformation of Data During Reconciliation" 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 Section 4.4, "Configuring Validation of Data During Reconciliation and Provisioning" 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 Section 4.4, "Configuring Validation of Data During Reconciliation and Provisioning" 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 Section 4.4, "Configuring Validation of Data During Reconciliation and Provisioning" 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 Section 4.4, "Configuring Validation of Data During Reconciliation and Provisioning" 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: *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.principalmgt.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: *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.

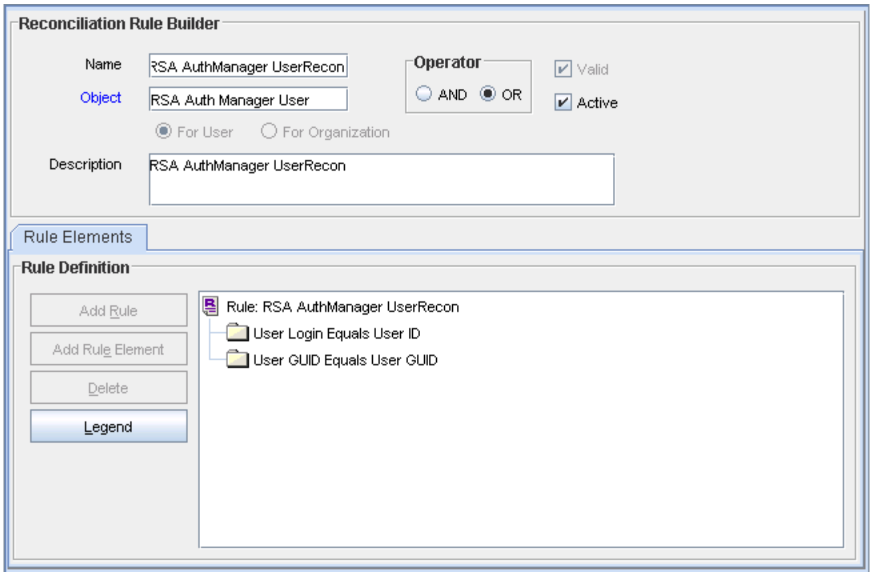
The second rule component is used to reconcile updates to accounts that are already reconciled from the target system. In this rule component:

- 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*



Reconciliation Rule Builder

Name: RSA AuthManager UserRecon

Object: RSA Auth Manager User

● For User ○ For Organization

Description: RSA AuthManager UserRecon

Operator: ○ AND ● OR

☑ Valid

☑ Active

Rule Definition

Rule: RSA AuthManager UserRecon
- User Login Equals User ID
- User GUID Equals User GUID

## 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: *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.

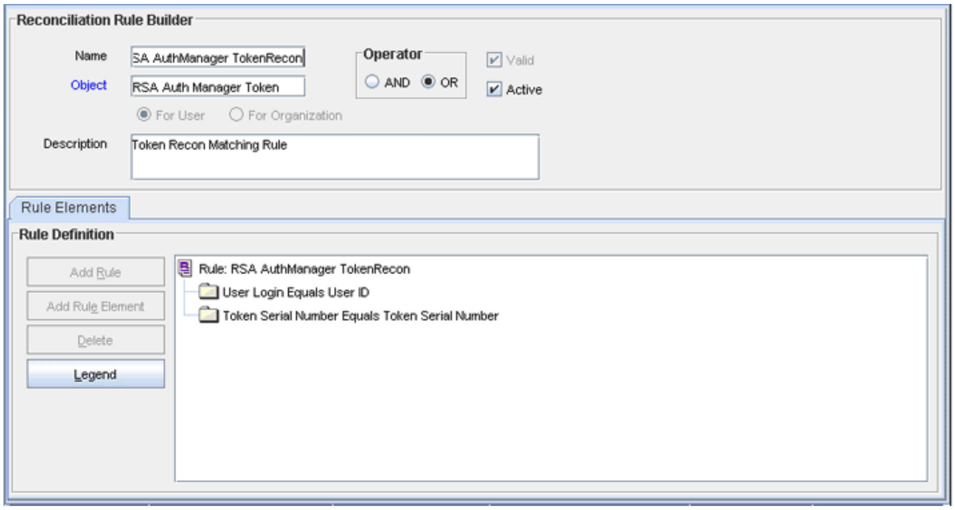
- Use case 2: An OIM User has an RSA token. You then change the user ID of the user on the target system.

  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***



Reconciliation Rule Builder

Name: SA AuthManager TokenRecon

Object: RSA Auth Manager Token

● For User ○ For Organization

Operator: ○ AND ● OR

☑ Valid

☑ Active

Description: Token Recon Matching Rule

Rule Elements

Rule Definition

Rule: RSA AuthManager TokenRecon
- User Login Equals User ID
- Token Serial Number Equals Token Serial Number

## 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***

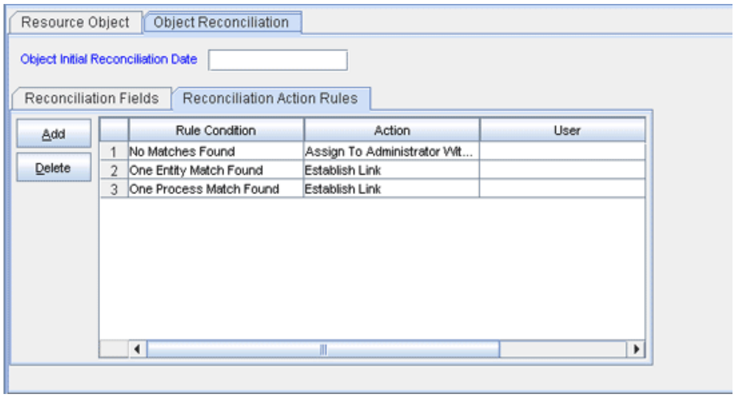
| Rule Condition | Action |
|---|---|
| No Matches Found | Assign to Administrator With Least Load |
| One Entity Match Found | Establish Link |
| One Process Match Found | Establish Link |

> **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: *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***



| | Rule Condition | Action | User |
|---|---|---|---|
| 1 | No Matches Found | Assign To Administrator Wit... | |
| 2 | One Entity Match Found | Establish Link | |
| 3 | One Process Match Found | Establish Link | |

## 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: *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.principalmgt.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.principalmgt.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.

# 2 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. |
| 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:<br>*OIM_HOME*/xellerate/ScheduleTask |
| lib/RSAAuthManagerCommon.jar | This JAR file contains the class files that is specific to this connector. During connector deployment, this file is copied into the following directory:<br>*OIM_HOME*/xellerate/JavaTasks |

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

| File in the Installation Media Directory | Description |
|---|---|
| lib/RSAAuthManager.jar | This JAR file contains the class files that are used in connector operations. During connector deployment, this file is copied into the following directory:<br>*OIM_HOME*/xellerate/JavaTasks |
| Files in the resources directory | 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:<br>*OIM_HOME*/xellerate/connectorResources<br>**Note:** 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. |
| xml/RSA-AuthManager-ConnectorConfig.xml | This XML file contains definitions of the various connector objects. These objects are created in Oracle Identity Manager when you run the Connector Installer. |

## 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, 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, 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 11g Release 1 (11.1.1)* 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, 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:
     *OIM_HOME*/server/ConnectorDefaultDirectory

2. 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 the following guide:

   - For Oracle Identity Manager release 9.1.0.*x*:

     *Oracle Identity Manager Administrative and User Console Guide*

   - For Oracle Identity Manager release 11.1.1:

     *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager*

3. 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*:

     Click **Deployment Management**, and then click **Install Connector**.

   - For Oracle Identity Manager release 11.1.1:

     On the Welcome to Identity Manager Advanced Administration page, in the System Management region, click **Install Connector**.

4. 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***.

5. Click **Load**.

6. 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.

7. 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 Identiy 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, 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.
   >
   > 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

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 on 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"

### 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. 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, 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:
   >
   > ```
   > 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:

  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"

#### 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:

  *WEBSPHERE_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

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

Oracle Identity Manager release 11.1.1 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.

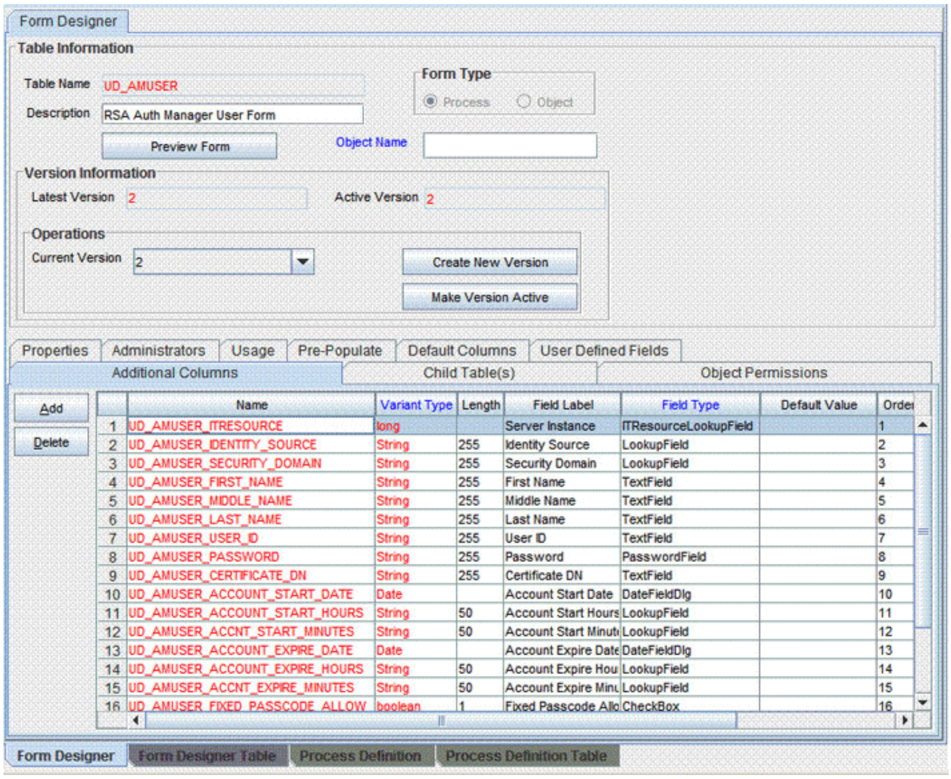


Table Name: UD_AMUSER

Description: RSA Auth Manager User Form

Form Type: ● Process ○ Object

Object Name:

Latest Version: 2

Active Version: 2

Current Version: 2

| | 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 | DateFieldDlg | | 10 |
| 11 | UD_AMUSER_ACCOUNT_START_HOURS | String | 50 | Account Start Hours | LookupField | | 11 |
| 12 | UD_AMUSER_ACCNT_START_MINUTES | String | 50 | Account Start Minut | LookupField | | 12 |
| 13 | UD_AMUSER_ACCOUNT_EXPIRE_DATE | Date | | Account Expire Date | DateFieldDlg | | 13 |
| 14 | UD_AMUSER_ACCOUNT_EXPIRE_HOURS | String | 50 | Account Expire Hou | LookupField | | 14 |
| 15 | UD_AMUSER_ACCNT_EXPIRE_MINUTES | String | 50 | Account Expire Minu | LookupField | | 15 |
| 16 | UD_AMUSER_FIXED_PASSCODE_ALLOW | boolean | 1 | Fixed Passcode Allo | 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.

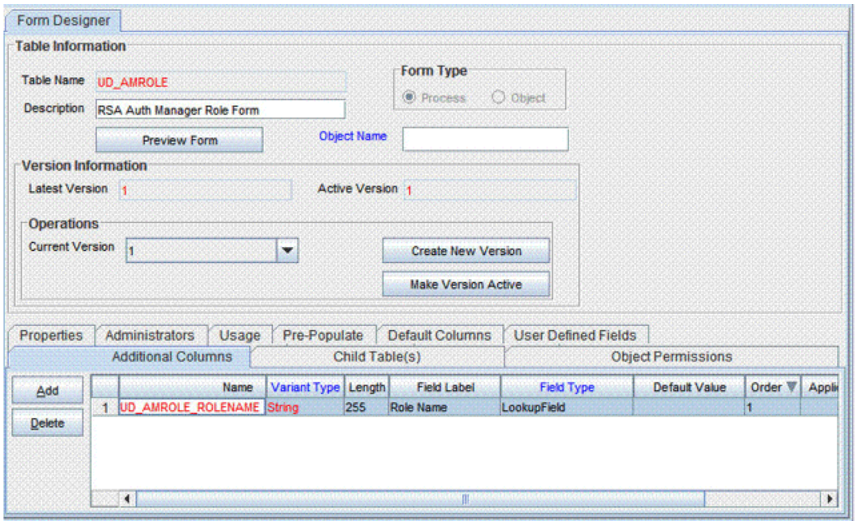


Table Name: UD_AMROLE

Description: RSA Auth Manager Role Form

Form Type: ● Process ○ Object

Object Name:

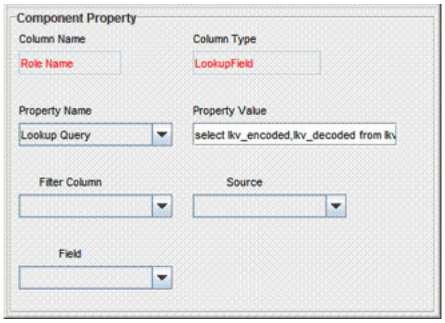
Latest Version: 1

Active Version: 1

Current Version: 1

| | Name | Variant Type | Length | Field Label | Field Type | Default Value | Order | Appli |
|---|---|---|---|---|---|---|---|---|
| 1 | UD_AMROLE_ROLENAME | String | 255 | Role Name | LookupField | | 1 | |

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



Column Name: Role Name

Column Type: LookupField

Property Name: Lookup Query

Property Value: select lkv_encoded,lkv_decoded from lkv

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.

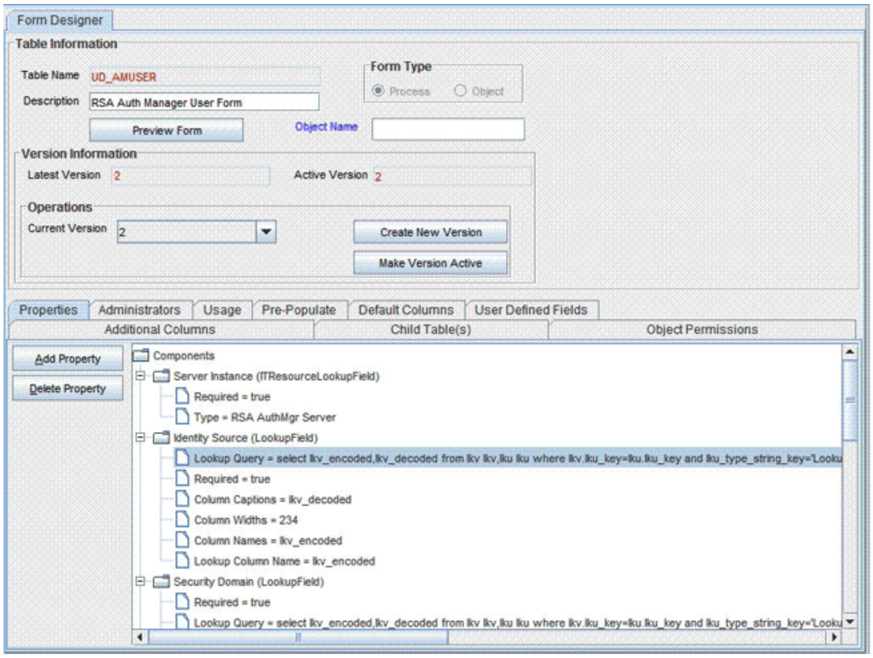


Table Information

Table Name: UD_AMUSER

Description: RSA Auth Manager User Form

Form Type: ● Process ○ Object

Object Name:

Version Information

Latest Version: 2

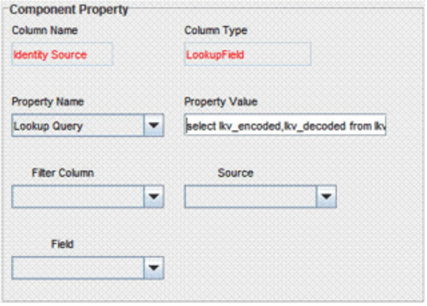
Active Version: 2

Operations

Current Version: 2

```
Components
  Server Instance (ITResourceLookupField)
    Required = true
    Type = RSA AuthMgr Server
  Identity Source (LookupField)
    Lookup Query = select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Looku
    Required = true
    Column Captions = lkv_decoded
    Column Widths = 234
    Column Names = lkv_encoded
    Lookup Column Name = lkv_encoded
  Security Domain (LookupField)
    Required = true
    Lookup Query = select lkv_encoded,lkv_decoded from lkv lkv,lku lku where lkv.lku_key=lku.lku_key and lku_type_string_key='Looku
```

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



Component Property

Column Name: Identity Source

Column Type: LookupField

Property Name: Lookup Query

Property Value: select lkv_encoded,lkv_decoded from lkv

Filter Column:

Source:

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 | 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)>0 |
| 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('$Form data.UD_AMTOKEN_ITRESOURCE$' + '~' ,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.

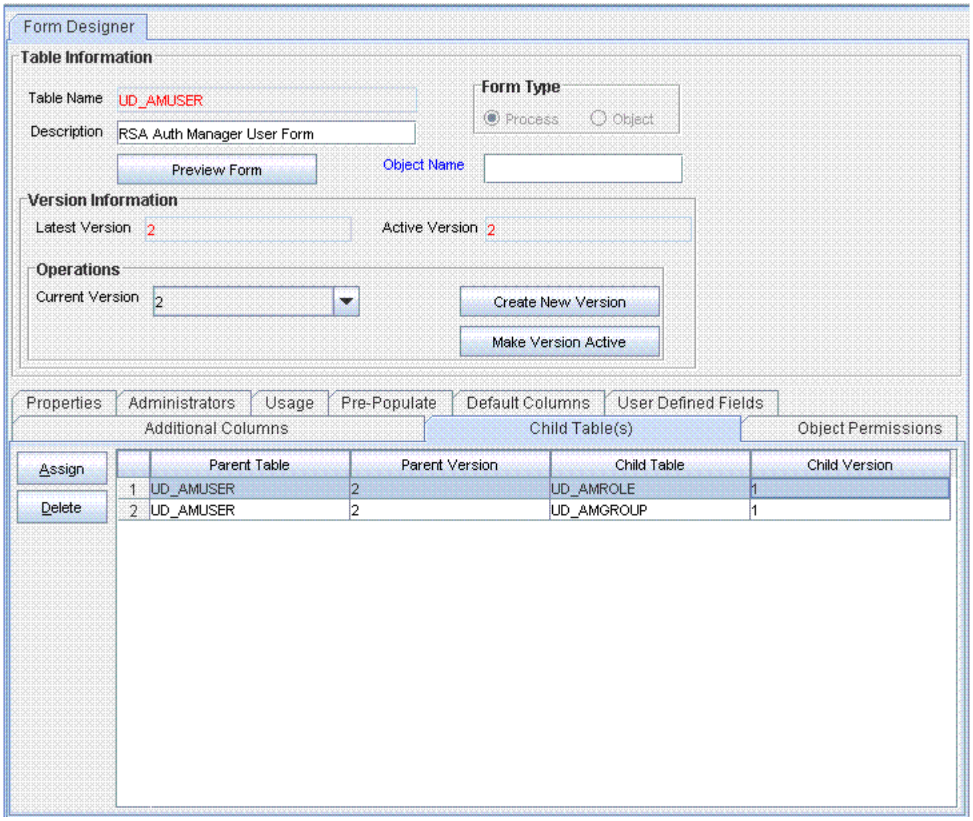


Table Name: UD_AMUSER

Description: RSA Auth Manager User Form

Form Type: ● Process ○ Object

Latest Version: 2

Active Version: 2

Current Version: 2

| | Parent Table | Parent Version | Child Table | Child Version |
|---|---|---|---|---|
| 1 | UD_AMUSER | 2 | UD_AMROLE | 1 |
| 2 | UD_AMUSER | 2 | UD_AMGROUP | 1 |

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.

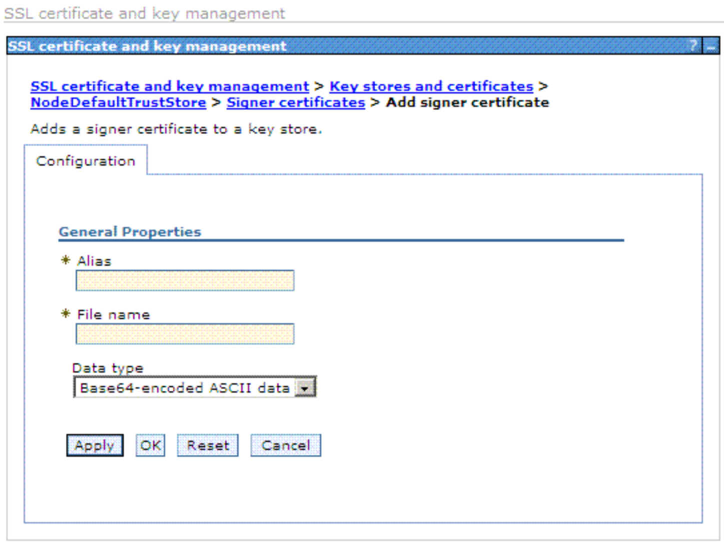
     b. Log in to the IBM WebSphere administrative console.

     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:



SSL certificate and key management

SSL certificate and key management

SSL certificate and key management > Key stores and certificates > NodeDefaultTrustStore > Signer certificates > Add signer certificate

Adds a signer certificate to a key store.

Configuration

General Properties

* Alias

* File name

Data type

Base64-encoded ASCII data

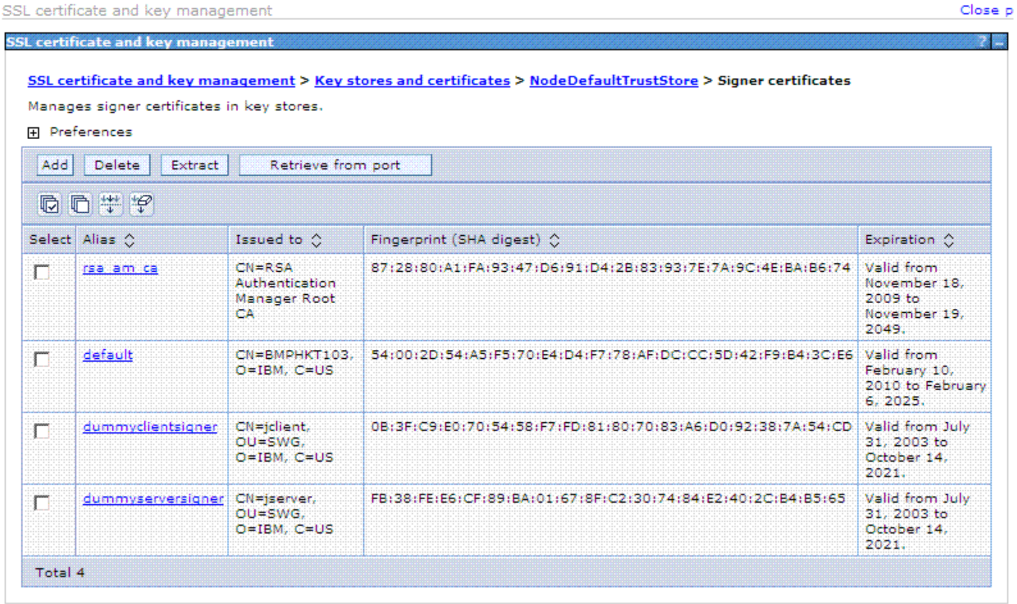
     e. In the **Alias** field, enter `rsa_am_ca`.

     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:



SSL certificate and key management | Close p

SSL certificate and key management

SSL certificate and key management > Key stores and certificates > NodeDefaultTrustStore > Signer certificates

Manages signer certificates in key stores.

⊞ Preferences

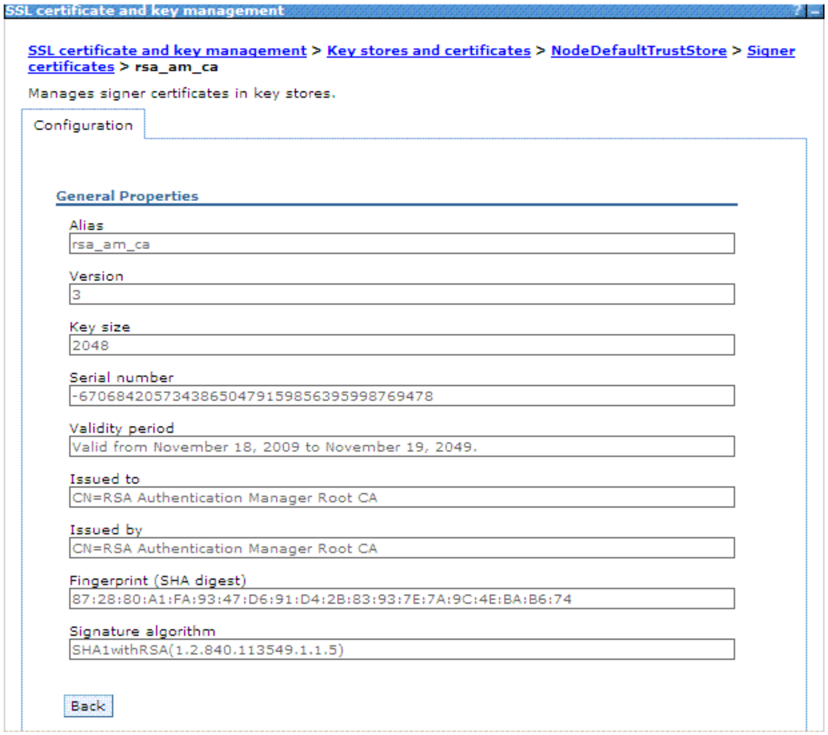
Add | Delete | Extract | Retrieve from port

| Select | Alias | Issued to | Fingerprint (SHA digest) | Expiration |
|---|---|---|---|---|
| □ | rsa_am_ca | CN=RSA Authentication Manager Root CA | 87:28:80:A1:FA:93:47:D6:91:D4:2B:83:93:7E:7A:9C:4E:BA:B6:74 | Valid from November 18, 2009 to November 19, 2049. |
| □ | default | CN=BMPHKT103, O=IBM, C=US | 54:00:2D:54:A5:F5:70:E4:D4:F7:78:AF:DC:CC:5D:42:F9:B4:3C:E6 | Valid from February 10, 2010 to February 6, 2025. |
| □ | dummyclientsigner | CN=jclient, OU=SWG, O=IBM, C=US | 0B:3F:C9:E0:70:54:58:F7:FD:81:80:70:83:A6:D0:92:38:7A:54:CD | Valid from July 31, 2003 to October 14, 2021. |
| □ | dummyserversigner | CN=jserver, OU=SWG, O=IBM, C=US | FB:38:FE:E6:CF:89:BA:01:67:8F:C2:30:74:84:E2:40:2C:B4:B5:65 | Valid from July 31, 2003 to October 14, 2021. |

Total 4

h. Select **rsa_am_ca**.

A page with information similar to the following is displayed:



SSL certificate and key management

SSL certificate and key management > Key stores and certificates > NodeDefaultTrustStore > Signer certificates > rsa_am_ca

Manages signer certificates in key stores.

Configuration

General Properties

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)

Back

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 on Oracle Identity Manager

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.*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
- *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

In addition, the following files are available in the *SDK_HOME*/lib/java directory on the RSA Authentication Manager host computer.

- am-client.jar

- axis-1.3.jar
- commons-beanutils-1.7.0.jar
- commons-discovery-0.2.jar
- commons-lang-2.3.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

**Depending on the application server that you use, copy the specified files 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*/*APPSERVER_HOME*/lib directory.

  In addition, perform the following procedure:

  1. In a text editor, open the *WEBSPHERE_HOME*/profiles/AppSrv02/bin/setupCmdLine.sh (or setupCmdLine.cmd) file.
  2. In this file, search for the WAS_CLASSPATH variable.
  3. 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%\l
     ib\bootstrap.jar;%WAS_HOME%/lib/j2ee.jar;%WAS_HOME%/lib/lmproxy.jar;%WAS_HO
     ME%/lib/urlprotocols.jar;%JAVA_HOME%\lib\tools.jar;%WAS_HOME%/lib/license.b
     ea;%WAS_HOME%/lib/wlcipher.jar;%WAS_HOME%/lib/wlfullclient.jar;%WAS_HOME%/l
     ib/com.bea.core.process_5.3.0.0.jar;%WAS_HOME%/lib/EccpressoAsn1.jar;%WAS_H
     OME%/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_H
     OME%/lib/commons-lang-2.3.jar;%WAS_HOME%/lib/axis-1.3.jar;%WAS_HOME%/lib/co
     mmons-discovery-0.2.jar;%WAS_HOME%/lib/commons-beanutils-1.7.0.jar
     ```

  4. Save and close the file.
  5. 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:

1. 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.
2. Extract the contents of the *ORACLE_HOME*/j2ee/home/oc4j.jar file into a temporary directory.
3. In a text editor, open the boot.xml file. This is one of the files in the oc4j.jar file.
4. 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"/>
   ```

5. Re-create the oc4j.jar file and copy it into the *ORACLE_HOME*/j2ee/home directory.
6. 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:\OC4JOIM\Server\xellerate
   -Dlog4j.configuration=file:D:\OC4JOIM\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.

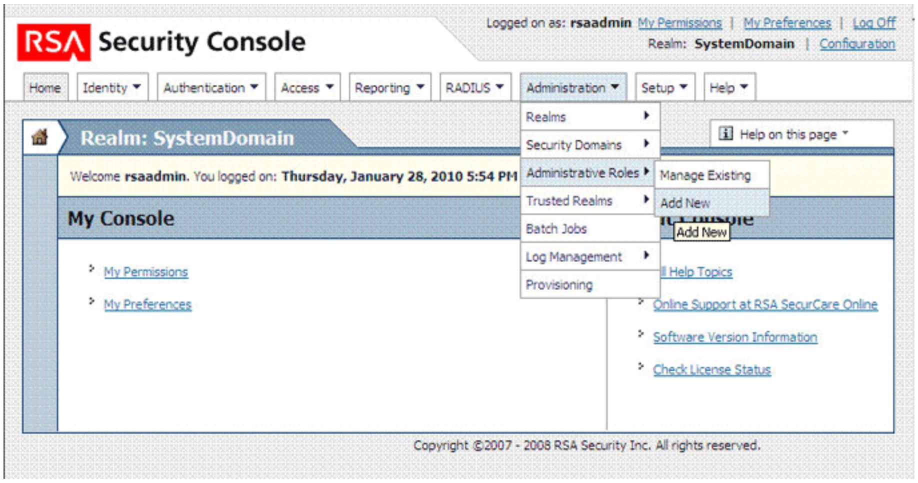
### 2.3.8 Creating a Target System Account for Connector Operations

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.

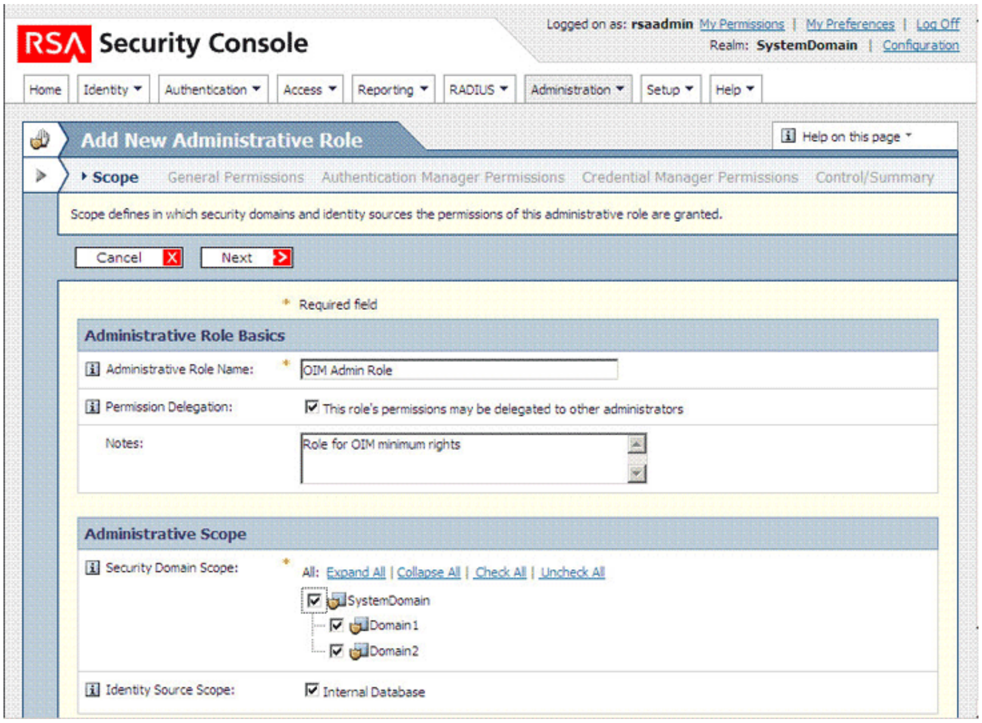
c. Select the **Permission Delegation** check box.

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.


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
Cancel
Next
Required field
Administrative Role Basics
Administrative Scope
All: Expand All | Collapse All | Check All | Uncheck All

Scope defines in which security domains and identity sources the permissions of this administrative role are granted.

Administrative Role Name: OIM Admin Role

Permission Delegation: ☑ This role's permissions may be delegated to other administrators

Notes: Role for OIM minimum rights

Security Domain Scope: ☑ SystemDomain
☑ Domain1
☑ Domain2

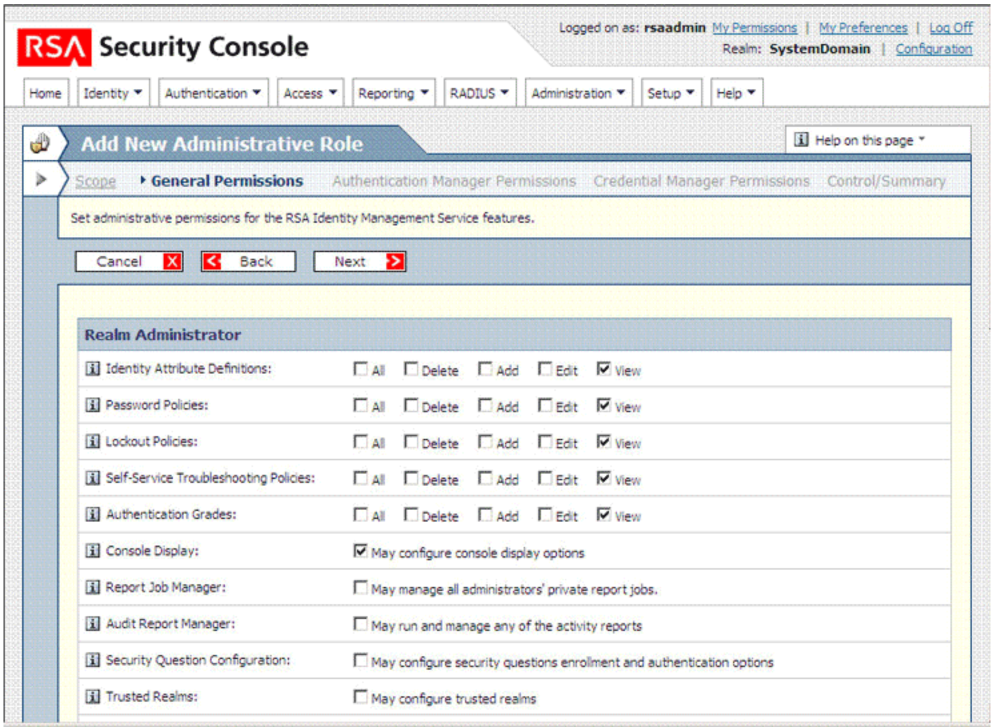
Identity Source Scope: ☑ Internal Database

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:


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
Cancel
Back
Next

Set administrative permissions for the RSA Identity Management Service features.

**Realm Administrator**

| | |
|---|---|
| Identity Attribute Definitions: | □ All □ Delete □ Add □ Edit ☑ View |
| Password Policies: | □ All □ Delete □ Add □ Edit ☑ View |
| Lockout Policies: | □ All □ Delete □ Add □ Edit ☑ View |
| Self-Service Troubleshooting Policies: | □ All □ Delete □ Add □ Edit ☑ View |
| Authentication Grades: | □ All □ Delete □ Add □ Edit ☑ View |
| Console Display: | ☑ May configure console display options |
| Report Job Manager: | □ May manage all administrators' private report jobs. |
| Audit Report Manager: | □ May run and manage any of the activity reports |
| Security Question Configuration: | □ May configure security questions enrollment and authentication options |
| Trusted Realms: | □ May configure trusted realms |

h. In the Manage Delegated Administration region, select the following permissions:

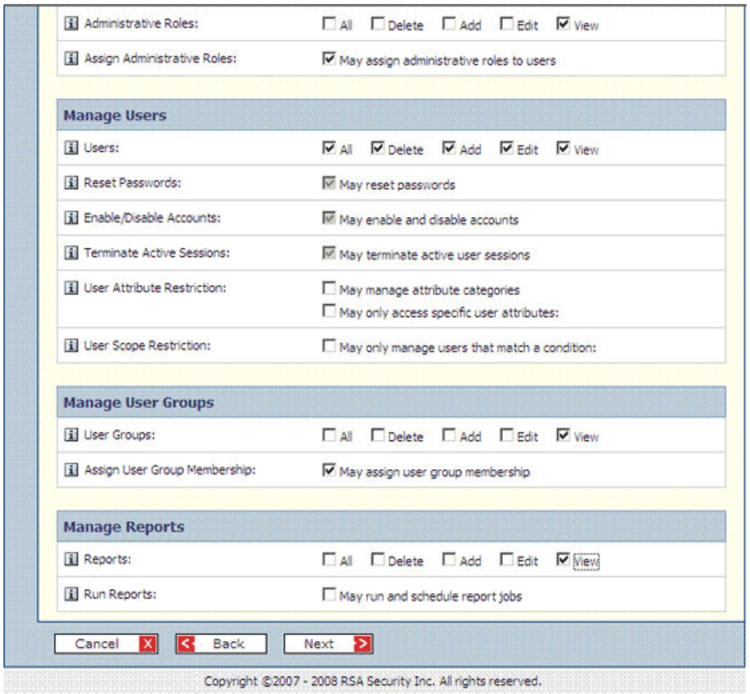
   - View check box for Security Domains
   - View check box for Administrative Roles
   - Assign Administrative Roles

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: | □ All □ Delete □ Add □ Edit ☑ View |
| Assign Administrative Roles: | ☑ May assign administrative roles to users |

**Manage Users**

| | |
|---|---|
| Users: | ☑ All ☑ Delete ☑ Add ☑ Edit ☑ View |
| Reset Passwords: | ☑ May reset passwords |
| Enable/Disable Accounts: | ☑ May enable and disable accounts |
| Terminate Active Sessions: | ☑ May terminate active user sessions |
| User Attribute Restriction: | □ May manage attribute categories<br>□ May only access specific user attributes: |
| User Scope Restriction: | □ May only manage users that match a condition: |

**Manage User Groups**

| | |
|---|---|
| User Groups: | □ All □ Delete □ Add □ Edit ☑ View |
| Assign User Group Membership: | ☑ May assign user group membership |

**Manage Reports**

| | |
|---|---|
| Reports: | □ All □ Delete □ Add □ Edit ☑ View |
| Run Reports: | □ May run and schedule report jobs |

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

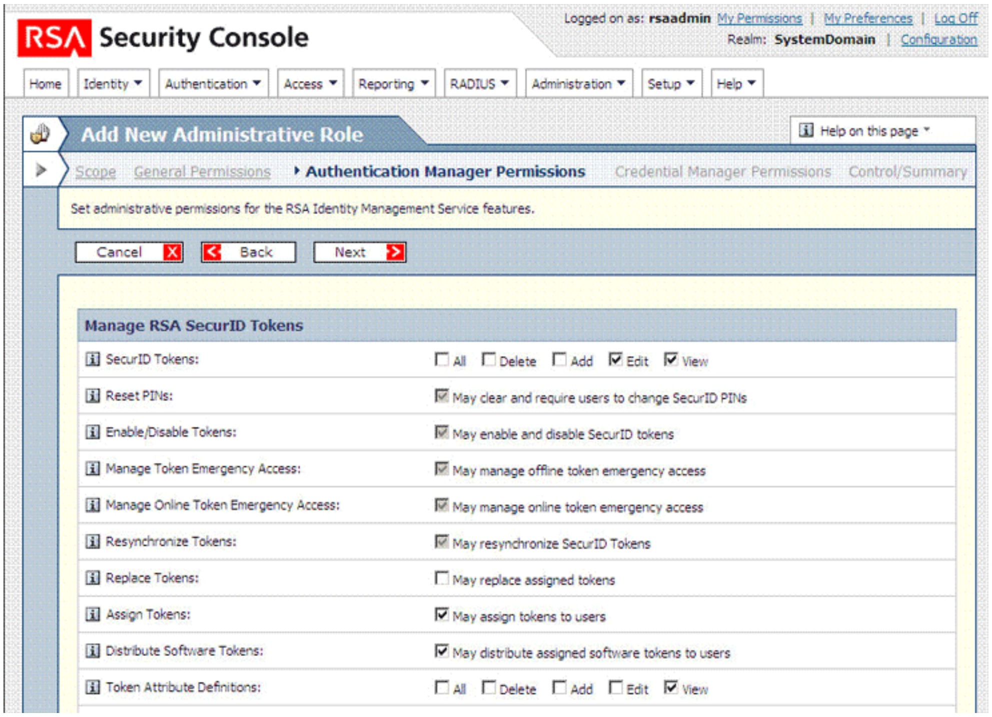
**l.** Click **Next**.

**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
Help on this page
Scope
General Permissions
Authentication Manager Permissions
Credential Manager Permissions
Control/Summary
Cancel
Back
Next

Add New Administrative Role

Set administrative permissions for the RSA Identity Management Service features.

**Manage RSA SecurID Tokens**

| | |
|---|---|
| SecurID Tokens: | □ All □ Delete □ Add ☑ Edit ☑ View |
| Reset PINs: | ☑ May clear and require users to change SecurID PINs |
| Enable/Disable Tokens: | ☑ May enable and disable SecurID tokens |
| Manage Token Emergency Access: | ☑ May manage offline token emergency access |
| Manage Online Token Emergency Access: | ☑ May manage online token emergency access |
| Resynchronize Tokens: | ☑ May resynchronize SecurID Tokens |
| Replace Tokens: | □ May replace assigned tokens |
| Assign Tokens: | ☑ May assign tokens to users |
| Distribute Software Tokens: | ☑ May distribute assigned software tokens to users |
| Token Attribute Definitions: | □ All □ Delete □ Add □ Edit ☑ 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.

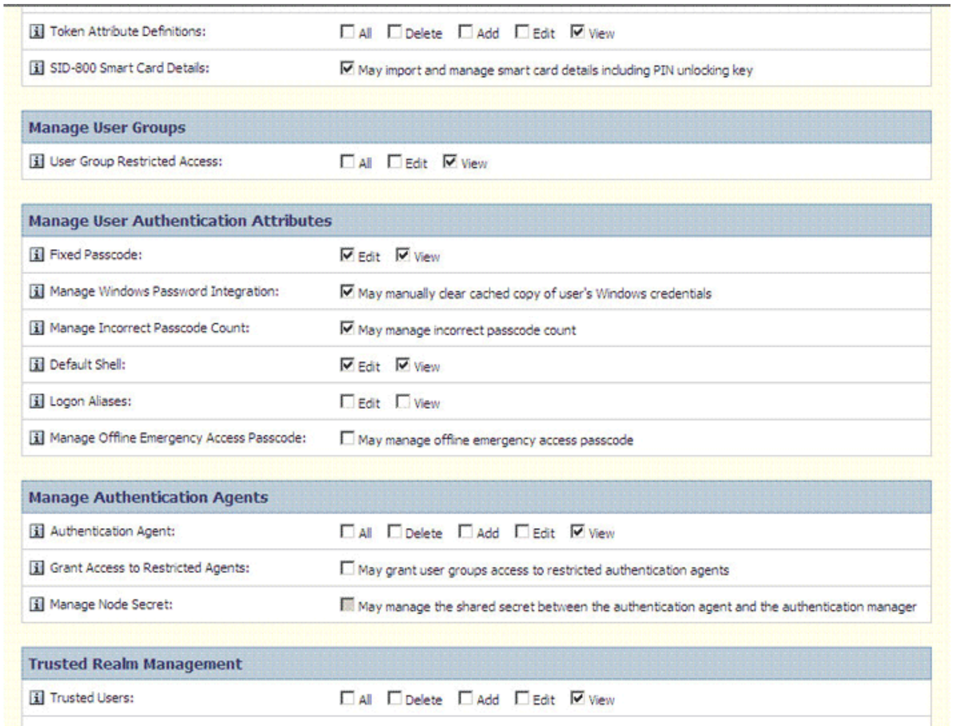
**t.** In the Trusted Realm Management region, select the following check boxes

– **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:

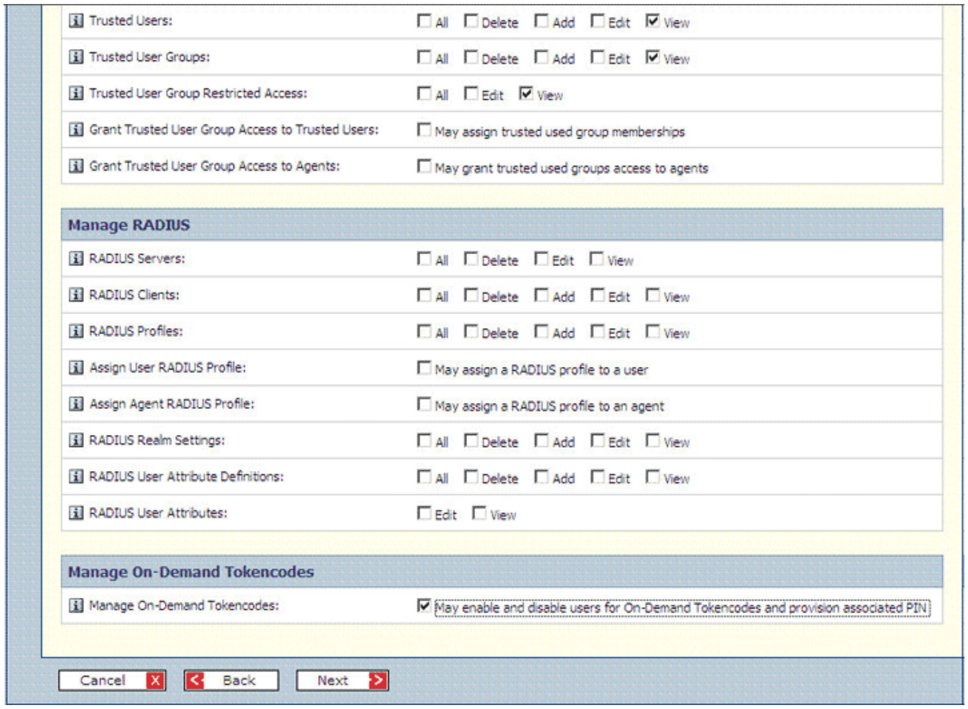


| | |
|---|---|
| Token Attribute Definitions: | □ All □ Delete □ Add □ Edit ☑ View |
| SID-800 Smart Card Details: | ☑ May import and manage smart card details including PIN unlocking key |
| **Manage User Groups** | |
| User Group Restricted Access: | □ All □ Edit ☑ View |
| **Manage User Authentication Attributes** | |
| Fixed Passcode: | ☑ Edit ☑ View |
| Manage Windows Password Integration: | ☑ 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: | □ All □ Delete □ Add □ Edit ☑ View |
| Trusted User Groups: | □ All □ Delete □ Add □ Edit ☑ View |
| Trusted User Group Restricted Access: | □ All □ Edit ☑ View |
| Grant Trusted User Group Access to Trusted Users: | □ May assign trusted used group memberships |
| Grant Trusted User Group Access to Agents: | □ May grant trusted used groups access to agents |

**Manage RADIUS**

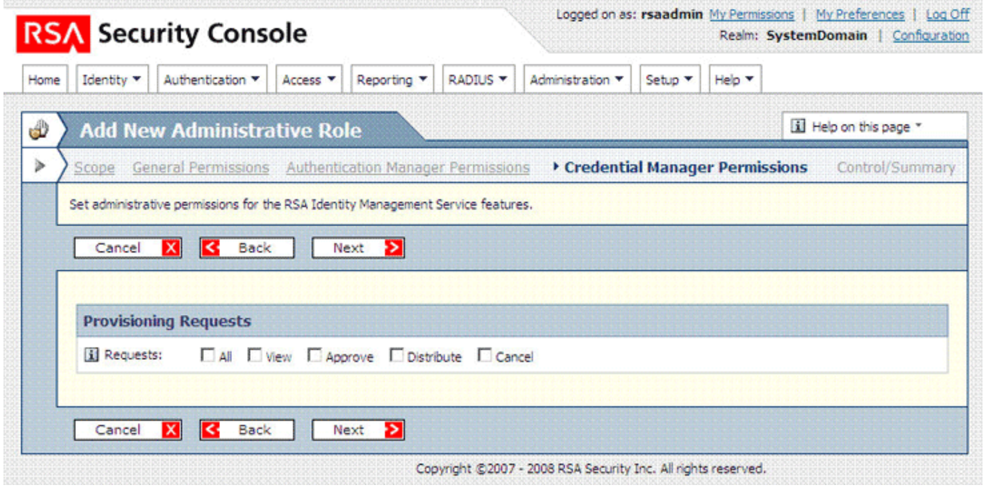
| | |
|---|---|
| RADIUS Servers: | □ All □ Delete □ Edit □ View |
| RADIUS Clients: | □ All □ Delete □ Add □ Edit □ View |
| RADIUS Profiles: | □ All □ Delete □ Add □ Edit □ View |
| Assign User RADIUS Profile: | □ May assign a RADIUS profile to a user |
| Assign Agent RADIUS Profile: | □ May assign a RADIUS profile to an agent |
| RADIUS Realm Settings: | □ All □ Delete □ Add □ Edit □ View |
| RADIUS User Attribute Definitions: | □ All □ Delete □ Add □ Edit □ View |
| RADIUS User Attributes: | □ Edit □ View |

**Manage On-Demand Tokencodes**

| | |
|---|---|
| Manage On-Demand Tokencodes: | ☑ May enable and disable users for On-Demand Tokencodes and provision associated PIN |

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

The following screenshot shows 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
Cancel
Back
Next

Set administrative permissions for the RSA Identity Management Service features.

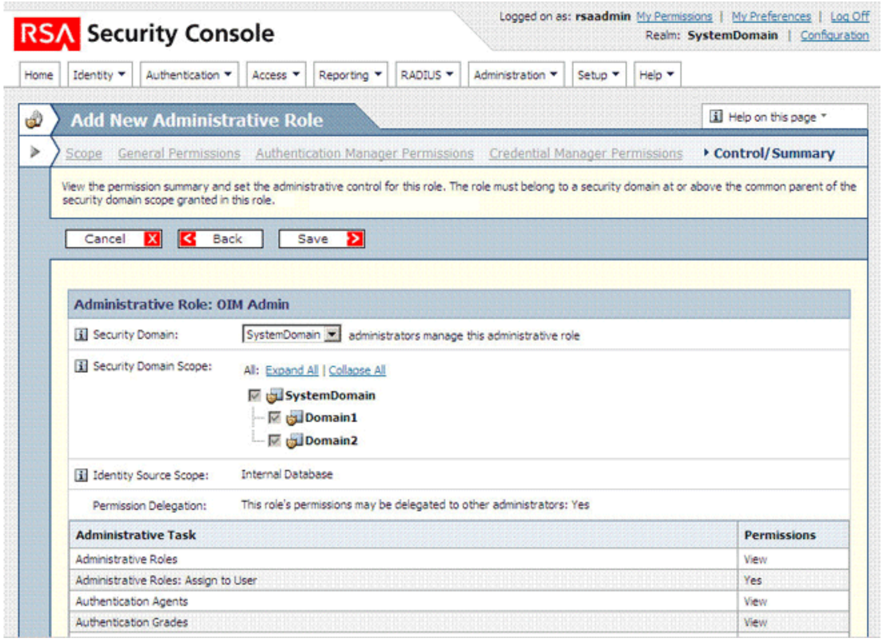
**Provisioning Requests**

| | |
|---|---|
| Requests: | □ All □ View □ Approve □ Distribute □ Cancel |

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:


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
Cancel
Back
Save

View the permission summary and set the administrative control for this role. The role must belong to a security domain at or above the common parent of the security domain scope granted in this role.

**Administrative Role: OIM Admin**

Security Domain: SystemDomain administrators manage this administrative role

Security Domain Scope: All: Expand All | Collapse All

- ☑ SystemDomain
  - ☑ Domain1
  - ☑ Domain2

Identity Source Scope: Internal Database

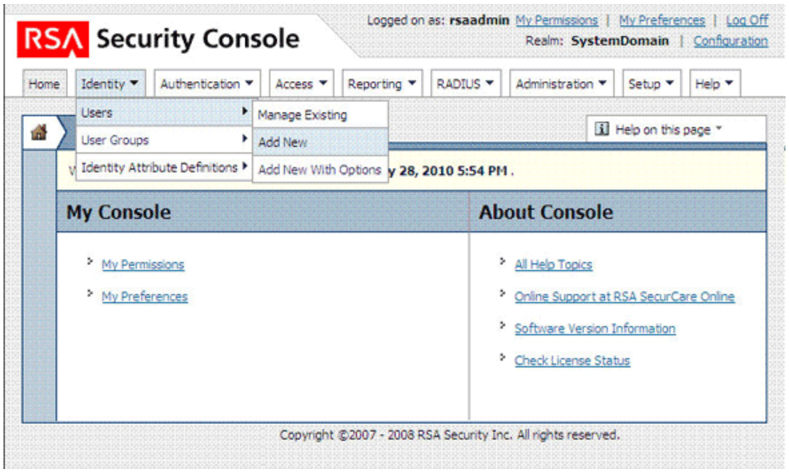
Permission Delegation: This role's permissions may be delegated to other administrators: Yes

| Administrative Task | Permissions |
|---|---|
| Administrative Roles | View |
| Administrative Roles: Assign to User | Yes |
| Authentication Agents | View |
| Authentication Grades | View |

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:



y 28, 2010 5:54 PM .

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

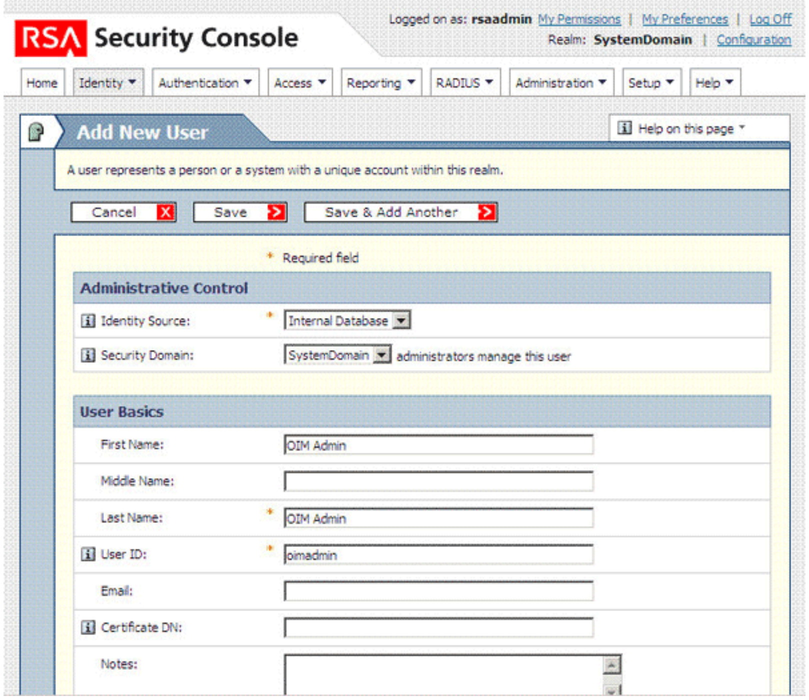
   b. On the Add New User page, enter the required values and then click **Save**.

**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:



Add New User

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

* 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

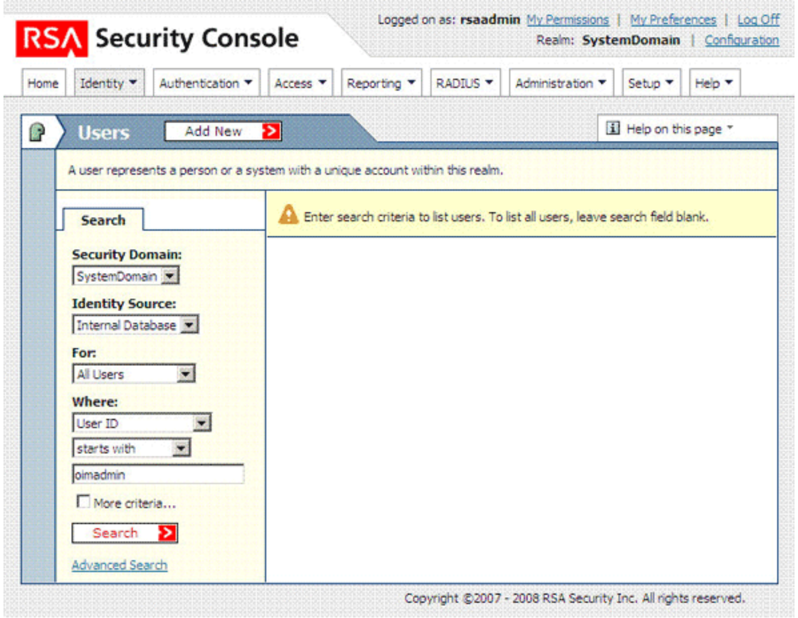
Email:

Certificate DN:

Notes:

c. Use the Search feature to open the details of the newly created user.

The following screenshot shows this page:



Users

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

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

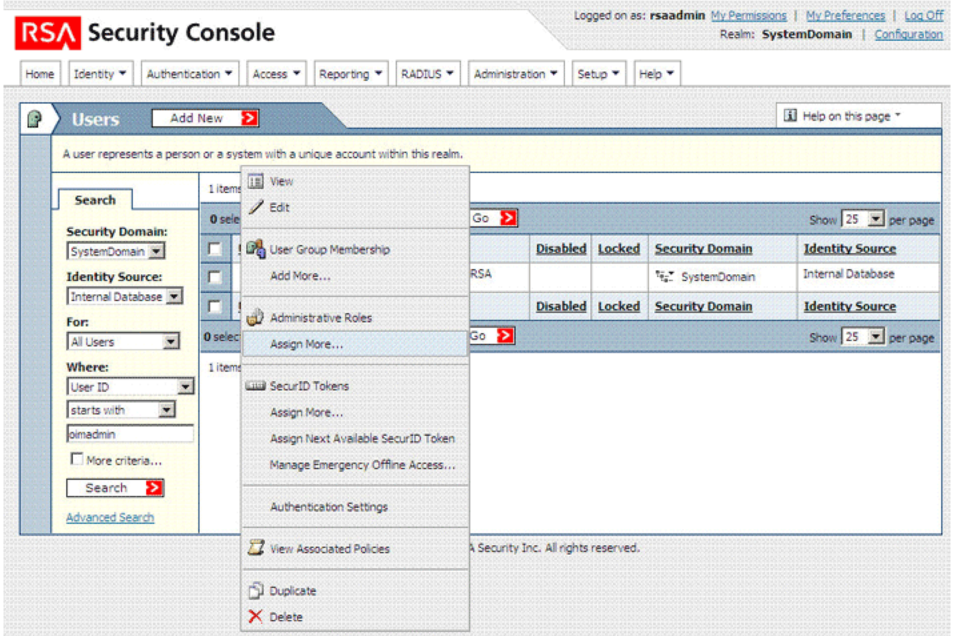
oimadmin

□ More criteria...

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

d. Click the arrow displayed next to the user name and then select **Assign More**.

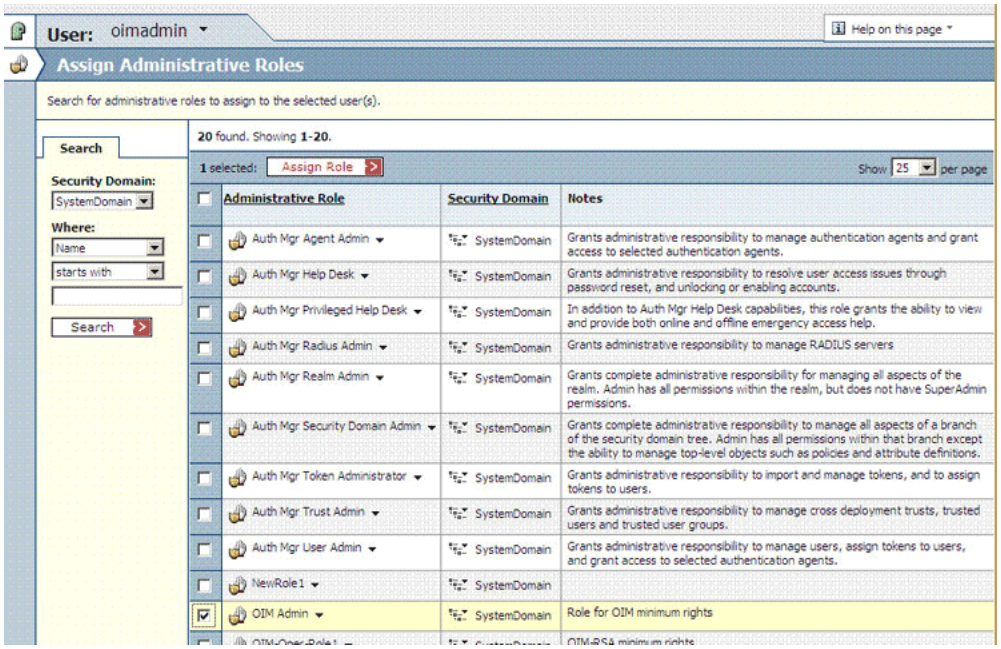
The following screenshot shows this page:



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

**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:



Search for administrative roles to assign to the selected user(s).

20 found. Showing 1-20.

| | Administrative Role | Security Domain | Notes |
|---|---|---|---|
| □ | Auth Mgr Agent Admin | SystemDomain | Grants administrative responsibility to manage authentication agents and grant access to selected authentication agents. |
| □ | Auth Mgr Help Desk | SystemDomain | Grants administrative responsibility to resolve user access issues through password reset, and unlocking or enabling accounts. |
| □ | Auth Mgr Privileged Help Desk | SystemDomain | In addition to Auth Mgr Help Desk capabilities, this role grants the ability to view and provide both online and offline emergency access help. |
| □ | Auth Mgr Radius Admin | SystemDomain | Grants administrative responsibility to manage RADIUS servers |
| □ | Auth Mgr Realm Admin | SystemDomain | Grants complete administrative responsibility for managing all aspects of the realm. Admin has all permissions within the realm, but does not have SuperAdmin permissions. |
| □ | Auth Mgr Security Domain Admin | SystemDomain | Grants complete administrative responsibility to manage all aspects of a branch of the security domain tree. Admin has all permissions within that branch except the ability to manage top-level objects such as policies and attribute definitions. |
| □ | Auth Mgr Token Administrator | SystemDomain | Grants administrative responsibility to import and manage tokens, and to assign tokens to users. |
| □ | Auth Mgr Trust Admin | SystemDomain | Grants administrative responsibility to manage cross deployment trusts, trusted users and trusted user groups. |
| □ | Auth Mgr User Admin | SystemDomain | Grants administrative responsibility to manage users, assign tokens to users, and grant access to selected authentication agents. |
| □ | NewRole1 | SystemDomain | |
| ☑ | OIM Admin | SystemDomain | Role for OIM minimum rights |
| □ | OIM-Oper-Role1 | SystemDomain | OIM-RSA minimum rights |

## 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:

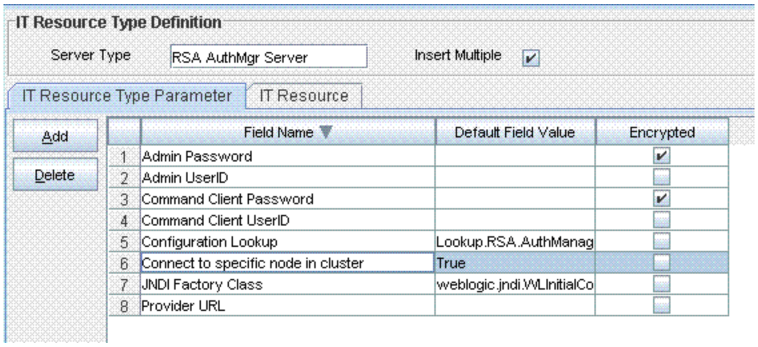
1. Add the connection property as a parameter in the RSA AuthMgr Server IT resource type definition as follows:

   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.



IT Resource Type Definition

Server Type: RSA AuthMgr Server

Insert Multiple ☑

| | Field Name | Default Field Value | Encrypted |
|---|---|---|---|
| 1 | Admin Password | | ☑ |
| 2 | Admin UserID | | □ |
| 3 | Command Client Password | | ☑ |
| 4 | Command Client UserID | | □ |
| 5 | Configuration Lookup | Lookup.RSA.AuthManag | □ |
| 6 | Connect to specific node in cluster | True | □ |
| 7 | JNDI Factory Class | weblogic.jndi.WLInitialCo | □ |
| 8 | Provider URL | | □ |

   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.<br>Default value: `Lookup.RSA.AuthManager.Constants` |
| 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.<br>Default value: `Lookup.RSA.AuthManager.DateMappings` |
| 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.<br>See Section 2.3.11, "Setting Up the Lookup.RSA.AuthManager.ExclusionList Lookup Definition" for more information.<br>Default value: `Lookup.RSA.AuthManager.ExclusionList` |
| Full Recon Filter | This entry holds the name of the lookup definition that contains entries used by the connector during full reconciliation.<br>Default value: `Lookup.RSA.AuthManager.FullReconFilter` |
| IT Resource Mapping | This entry holds the name of the lookup definition that maps some of the IT resource parameters with parameters of the RemoteCommandTargetBean API.<br>Default value: `Lookup.RSA.AuthManager.ITResourceMapping` |
| 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.<br>Default value: `Lookup.RSA.AuthManager.LookupReconMapping` |

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

| Code Key | Description |
|---|---|
| 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.<br>Default value: `yyyy/MM/dd hh:mm:ss z` |
| Target TimeZone | Enter the time zone of the target system. For example, enter `GMT-07:00` if the target system is in Arizona in the United States.<br>Default value: `GMT+05:30` |
| 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.<br>Default value: `UD_AMTOKEN_TOKEN_GUID` |
| 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.<br>Default value: `UD_AMTOKEN_SERIAL_NUMBER` |
| 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.<br>Default value: `UD_AMTOKEN_USERID` |
| 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.<br>Default value: `Token Serial Number` |
| 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.<br>Default value: `User Identity Source` |
| 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.<br>Default value: `Token GUID` |
| 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.<br>Default value: `User ID` |
| 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.<br>Default value: `User Guid` |
| 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.<br>Default value: `Lookup.RSA.AuthManager.TokenAttrMap` |
| 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.<br>Default value: `Lookup.RSA.AuthManager.TokenReconAttrMap` |
| Token SerialNumber MaxLength | Enter the maximum length of the token serial number allowed on your RSA Authentication Manager installation.<br>Default value: `12` |

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

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

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

| Code Key | Description |
|---|---|
| Use Validation For UserProv | Enter `yes` if you want to configure validation of token attributes that are sent to RSA Authentication Manager during provisioning. Otherwise, enter `no`.<br>Default value: `no`<br>See Section 4.4, "Configuring Validation of Data During Reconciliation and Provisioning" for more information. |
| Use Validation For UserRecon | Enter `yes` if you want to configure validation of user attributes that are brought into Oracle Identity Manager during reconciliation. Otherwise, enter `no`.<br>Default value: `no`<br>See Section 4.4, "Configuring Validation of Data During Reconciliation and Provisioning" for more information. |
| User UDF USERGUID | If you create a copy of the user process form, then specify the column name of the UDF for the User GUID attribute.<br>Default value: `USR_UDF_USERGUID` |
| USRFORMCOL ITResource | 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.<br>Default value: `UD_AMUSER_ITRESOURCE` |
| USRFORMCOL UserID | 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.<br>Default value: `UD_AMUSER_USER_ID` |
| USRROField UserGUID | 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.<br>Default value: `User GUID` |
| USRROField Expire Time Hours | 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.<br>Default value: `Expire Time Hours` |
| USRROField Expire Time Mins | 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.<br>Default value: `Expire Time Mins` |
| USRFORMCOL UserGUID | 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.<br>Default value: `UD_AMUSER_RSA_GUID` |
| USRROField IdentitySource | 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.<br>Default value: `User Identity Source` |
| USRROField Security Domain | 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.<br>Default value: `Security Domain` |

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

| Code Key | Description |
|---|---|
| USRROField Start Time Hours | 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.<br>Default value: `Start Time Hours` |
| USRROField Start Time Mins | 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.<br>Default value: `Start Time Mins` |
| USRROField UserID | 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.<br>Default value: `User ID` |
| Validation Lookup For Token Provisioning | This entry holds the name of the lookup definition that maps token process form fields with the Java validation classes that you create.<br>Value: `Lookup.RSA.AuthManager.TokenProvisioningValidation`<br>See Section 4.4, "Configuring Validation of Data During Reconciliation and Provisioning" for more information about this feature. |
| Validation Lookup For Token Recon | This entry holds the name of the lookup definition that maps token resource object fields with the Java validation classes that you create.<br>Value: `Lookup.RSA.AuthManager.TokenReconValidation`<br>See Section 4.4, "Configuring Validation of Data During Reconciliation and Provisioning" for more information about this feature. |
| Validation Lookup For User Prov | This entry holds the name of the lookup definition that maps user process form fields with the Java validation classes that you create.<br>Value: `Lookup.RSA.AuthManager.UserProvisioningValidation`<br>See Section 4.4, "Configuring Validation of Data During Reconciliation and Provisioning" for more information about this feature. |
| Validation Lookup For User Recon | This entry holds the name of the lookup definition that maps user resource object fields with the Java validation classes that you create.<br>Value: `Lookup.RSA.AuthManager.UserReconValidation`<br>See Section 4.4, "Configuring Validation of Data During Reconciliation and Provisioning" for more information about this feature. |

### 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. Log in to the Administrative and User Console.
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. Expand **Resource Management,** and then click **Manage IT Resource.**
   - For Oracle Identity Manager release 11.1.1:
     a. On the Welcome page, click Advanced in the upper-right corner of the page.
     b. On the Welcome to Oracle Identity Manager Advanced Administration page, in the Configuration region, click **Manage IT Resource.**
3. In the IT Resource Name field on the Manage IT Resource page, enter `RSA Server Instance` and then click **Search**.
4. Click the edit icon for the IT resource.
5. From the list at the top of the page, select **Details and Parameters**.
6. 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<br>See Section 2.3.8, "Creating a Target System Account for Connector Operations" for more information. |
| Admin UserID | Enter the user ID of the target system user account that you create for connector operations<br>See Section 2.3.8, "Creating a Target System Account for Connector Operations" for more information. |
| Command Client Password | Enter the command client password.<br>Setting the command client user name and password is one of the tasks in the procedure mentioned in Section 2.3.5, "Addressing Prerequisites for Using the Java API of RSA Authentication Manager." |
| Command Client UserID | Enter the command client user name.<br>Setting the command client user name and password is one of the tasks in the procedure mentioned in Section 2.3.5, "Addressing Prerequisites for Using the Java API of RSA Authentication Manager." |
| Configuration Lookup | This parameter holds the name of the configuration lookup definition.<br>Default value: `Lookup.RSA.AuthManager.Configuration` |
| JNDI Factory Class | This parameter holds the name of the initial context factory class on the target system.<br>Value: `weblogic.jndi.WLInitialContextFactory`<br>You must not change this value. |
| Provider URL | Enter the following value:<br>`https://`*`IP_ADDRESS or HOSTNAME`*`:7002/ims-ws/services/CommandServer`<br>**Note:**<br>If RSA Authentication Manager is installed in a clustered environment, then replace *`IP_ADDRESS or HOSTNAME`* with a comma-separated list of IP addresses or host names of all the nodes of the cluster. For example:<br>`https://`*`IP_ADDRESS1 or HOSTNAME1`*`,`*`IP_ADDRESS2 or HOSTNAME2`*`,...`:7002<br>Sample value: `https://hostNode1,hostNode74,hostNode21:7002` |

7. 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.

- 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:** Perform the procedure described in this section only if you are using Oracle Identity Manager release 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.

# 3
# 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"
- Section 3.9, "Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1"

## 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, 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.

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.<br>Default value: `RSA Server Instance` |
| 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.<br>Value: `RSA Auth Manager Lookup Recon` |

## 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.<br>This is one of the attributes that are used to implement limited reconciliation. Section 3.4.2, "Limited Reconciliation" 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.<br>This is one of the attributes that are used to implement limited reconciliation. Section 3.4.2, "Limited Reconciliation" 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.<br>Default value: `Internal Database` |
| IsDeleteAllowed | Enter `yes` 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 `no` as the value of the IsDeleteAllowed attribute. |
| IsTokenReconAllowed | Enter `yes` if you want to reconcile both users and tokens. Enter `no` if you want to reconcile only users.<br>When you set the value of this attribute to `yes`, 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.<br>Default value: `RSA Server Instance` |

*Table 3–2 (Cont.) Attributes of the RSA Auth Manager User Recon Scheduled Task*

| Attribute | Description |
|---|---|
| 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.<br>You can set the value of this attribute to `0` if you want to perform a full reconciliation run. See Section 3.4.1, "Full Reconciliation" for more information. |
| Scheduled Task Name | This attribute holds the name of the scheduled task.<br>Default value: `RSA Auth Manager User Recon`<br>**Note:** 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`.<br>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.<br>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.<br>If you do not want to implement batched reconciliation, then specify nodata.<br>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.<br>This is one of the attributes that are used to implement limited reconciliation. Section 3.4.2, "Limited Reconciliation" describes this feature.<br>See Section 3.4.1, "Full Reconciliation" 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.<br>See Section 3.4.1, "Full Reconciliation" 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.<br>Default value: `Internal database` |
| IT Resource | Enter the name of the IT resource from which you want to reconcile user data.<br>Default value: `RSA Server Instance` |

*Table 3–3 (Cont.) Attributes of the RSA Auth Manager Token Recon Scheduled Task*

| Attribute | Description |
|---|---|
| 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.<br>See Section 3.4.1, "Full Reconciliation" for information about using this attribute to perform a full reconciliation run. |
| Scheduled Task Name | This attribute holds the name of the scheduled task.<br>Default value: `RSA Auth Manager Token Recon`<br>**Note:** 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`.<br>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. Log in to the Administrative and User Console.
2. Perform one of the following:

   a. If you are using Oracle Identity Manager release 9.1.0.*x*, expand **Resource Management,** and then click **Manage Scheduled Task.**

   b. If you are using Oracle Identity Manager release 11.1.1, then on the Welcome to Oracle Identity Manager Self Service page, click **Advanced** in the upper-right corner of the page.
3. 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, 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.

4. 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, 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.

5. 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, then on the Job Details tab, in the Parameters region, specify values for the attributes of the scheduled task.

6. 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, 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" 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

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 3.9, "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"

### 3.8.1 Direct Provisioning

To provision a resource by using the direct provisioning approach:

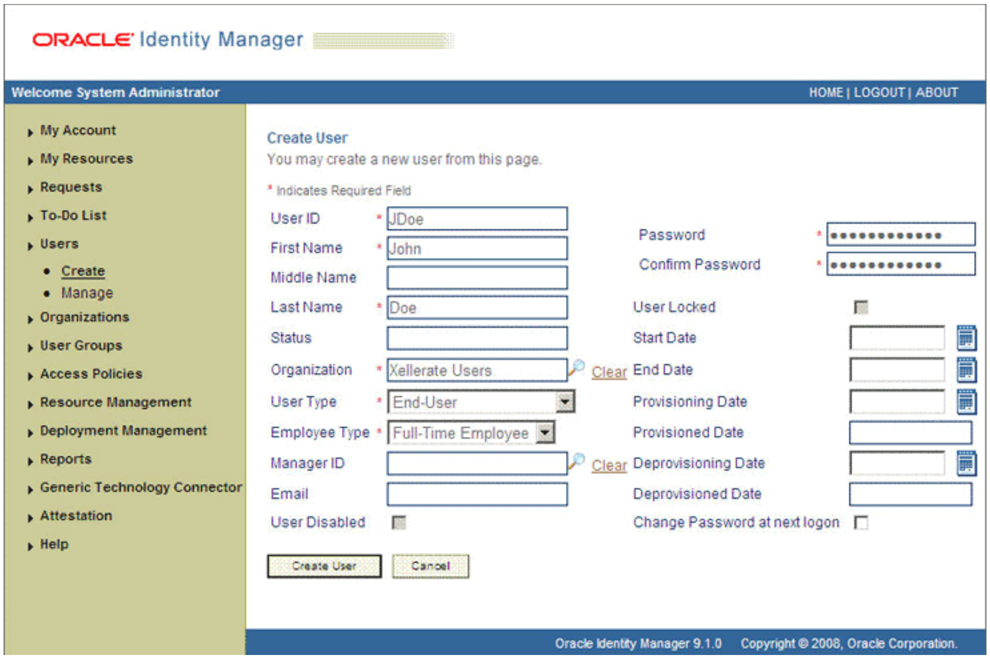
> **Note:** This procedure describes the Create User provisioning operation. The procedure for the Update User provisioning operation is similar to this one.

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*



Create User

You may create a new user from this page.

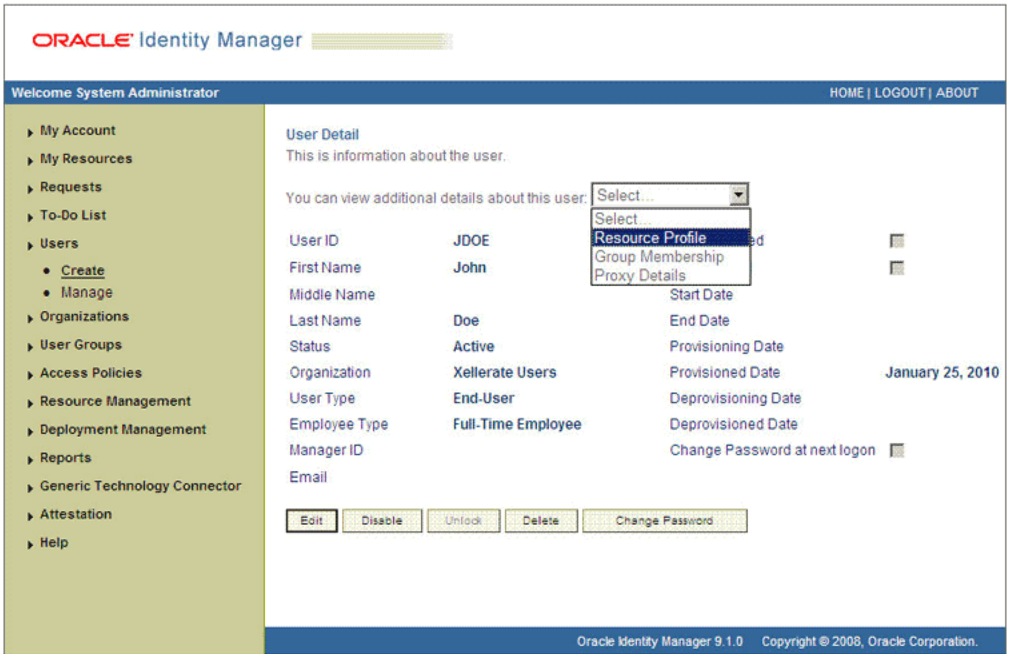
* Indicates Required Field

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

4. 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.

5. 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*



User Detail

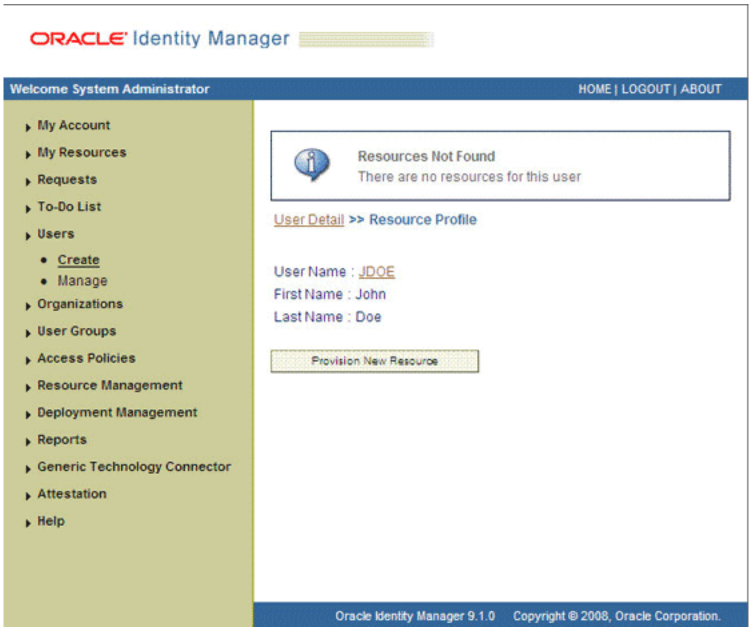
This is information about the user.

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

| | | | |
|---|---|---|---|
| User ID | JDOE | ...ed | □ |
| First Name | John | | □ |
| Middle Name | | Start Date | |
| Last Name | Doe | End Date | |
| Status | Active | Provisioning Date | |
| Organization | Xellerate Users | Provisioned Date | January 25, 2010 |
| User Type | End-User | Deprovisioning Date | |
| Employee Type | Full-Time Employee | Deprovisioned Date | |
| Manager ID | | Change Password at next logon | □ |
| Email | | | |

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

*Figure 3–3 Resource Profile Page*

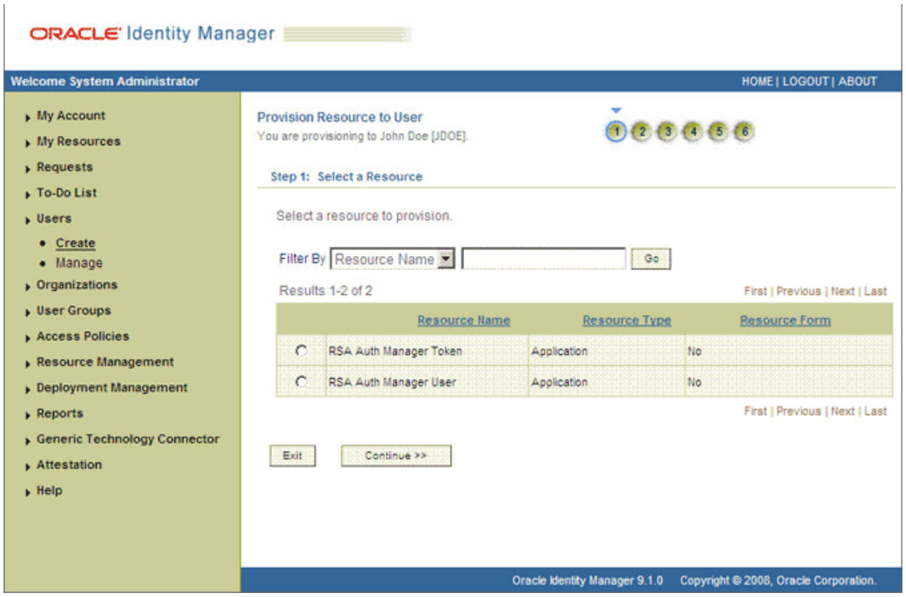


Resources Not Found
There are no resources for this user

User Name : JDOE
First Name : John
Last Name : Doe

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*



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

Step 1: Select a Resource

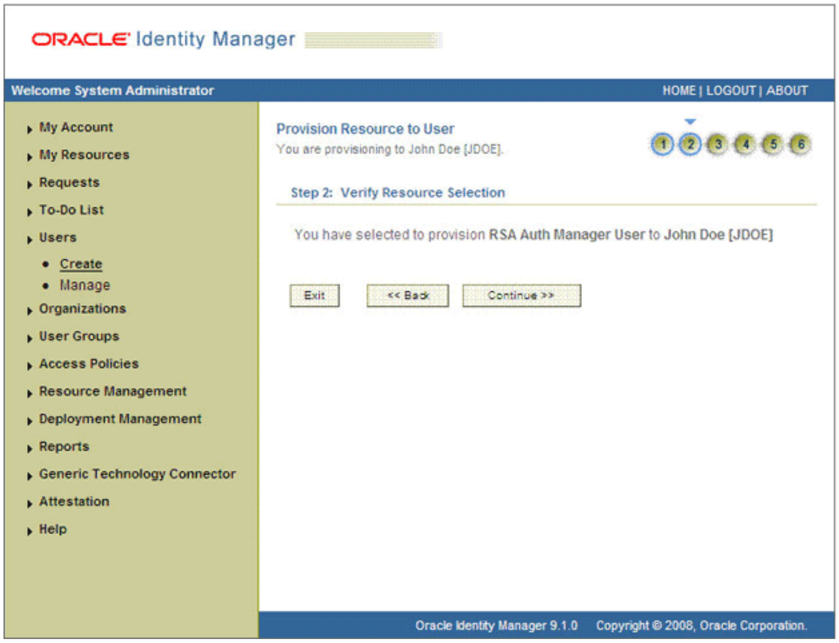
Select a resource to provision.

Results 1-2 of 2

| | Resource Name | Resource Type | Resource Form |
|---|---|---|---|
| ○ | RSA Auth Manager Token | Application | No |
| ○ | RSA Auth Manager User | Application | No |

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*



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]

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***

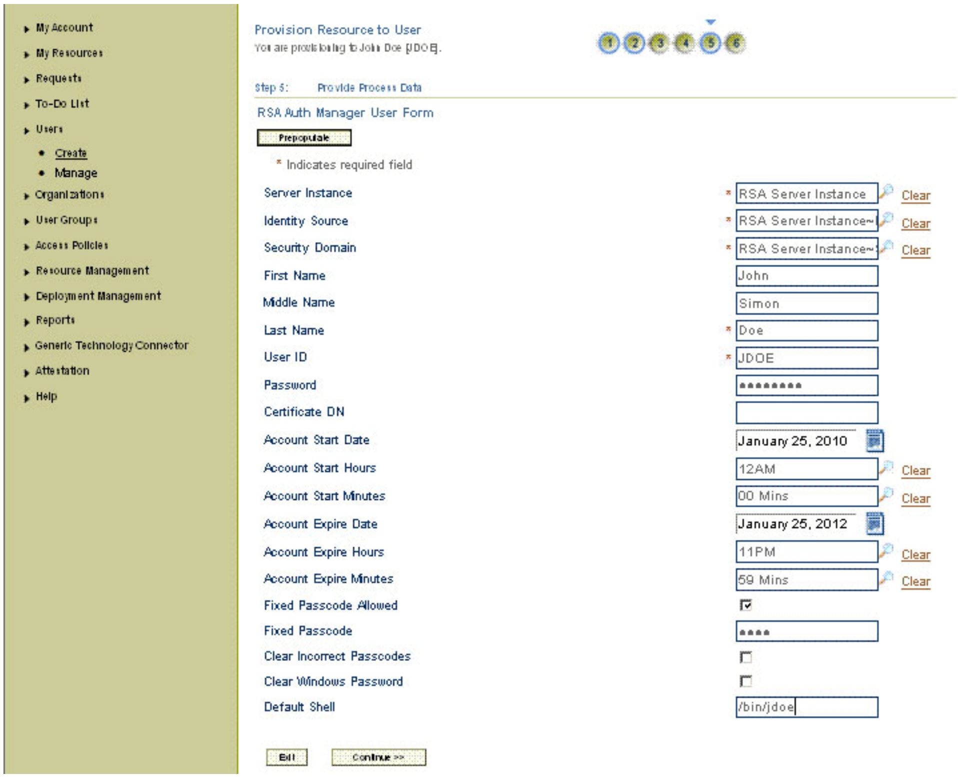
| Field | Description |
|---|---|
| Server Instance | Select the IT resource representing the target system installation on which you want to perform the provisioning operation. |
| Identity Source | Select the identity source in which you want to perform the provisioning operation. |
| Security Domain | 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.<br>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.<br>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.<br>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 | Select the date at which the account must be closed.<br>This field is used in conjunction with the Account Expire Hours and Account Expire Minutes fields. |
| Account Expire Hours | Select the time (in hours) at which the account must be closed.<br>This field is used in conjunction with the Account Expire Date and Account Expire Minutes field. |
| Account Expire Minutes | Select the time (in minutes) at which the account must be closed.<br>This field is used in conjunction with the Account Expire Date and Account Expire Hours field. |
| Fixed Passcode Allowed | Select this check box if you want to allow the user to use a fixed passcode.<br>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. |
| Fixed Passcode | Enter the passcode. The value entered in this field is accepted only if you select the Fixed Passcode Allowed check box. |
| Clear Incorrect Passcode | 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.<br>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. |
| Clear Windows Passcode | 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.<br>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. |
| Default Shell | 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.<br>Sample value: `/bin/jdoe` |

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

* Indicates required field

| | |
|---|---|
| Server Instance | * RSA Server Instance Clear |
| Identity Source | * RSA Server Instance~I Clear |
| Security Domain | * RSA Server Instance~S Clear |
| 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 Clear |
| Account Start Minutes | 00 Mins Clear |
| Account Expire Date | January 25, 2012 |
| 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 |

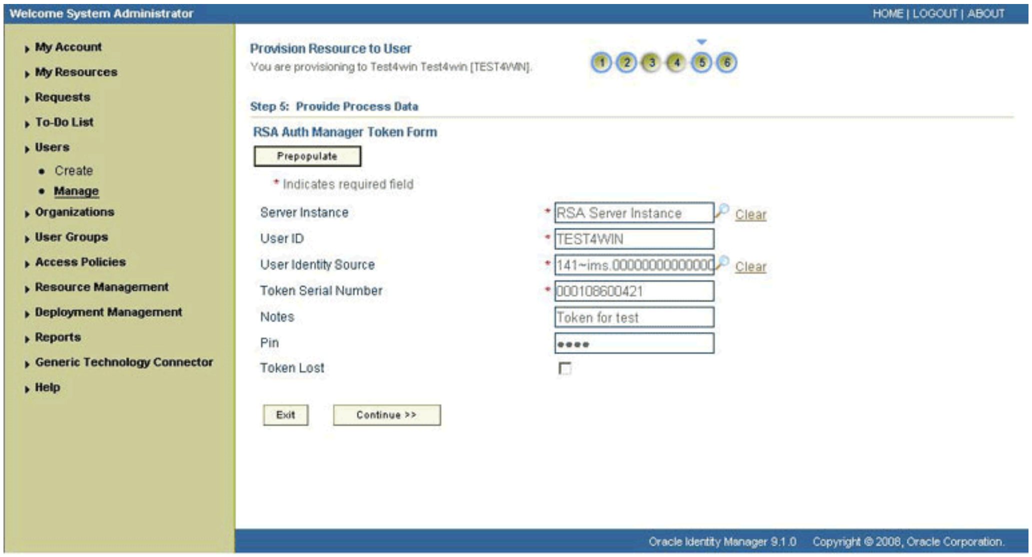
If you are performing a token provisioning operation, then enter values for the fields listed in Table 3–6.

*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***



Provision Resource to User

You are provisioning to Test4win Test4win [TEST4WIN].

Step 5: Provide Process Data

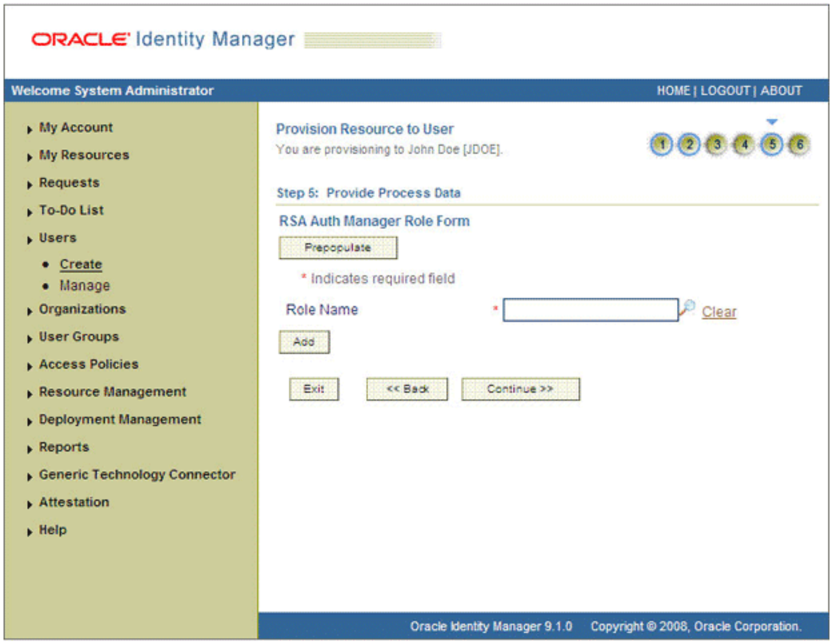
RSA Auth Manager Token Form

* Indicates required field

| | |
|---|---|
| Server Instance | * RSA Server Instance |
| User ID | * TEST4WIN |
| User Identity Source | * 141~ims.000000000000000 |
| Token Serial Number | * 000108600421 |
| Notes | Token for test |
| Pin | •••• |
| Token Lost | □ |

10. 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***



Provision Resource to User

You are provisioning to John Doe [JDOE].

Step 5: Provide Process Data

RSA Auth Manager Role Form

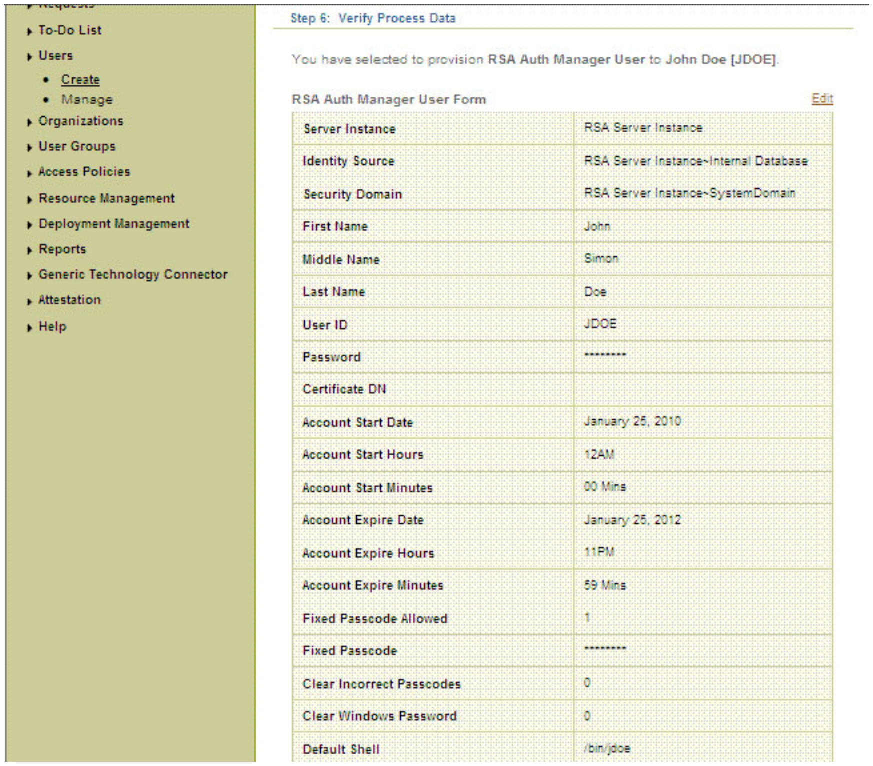
* Indicates required field

Role Name *

11. 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

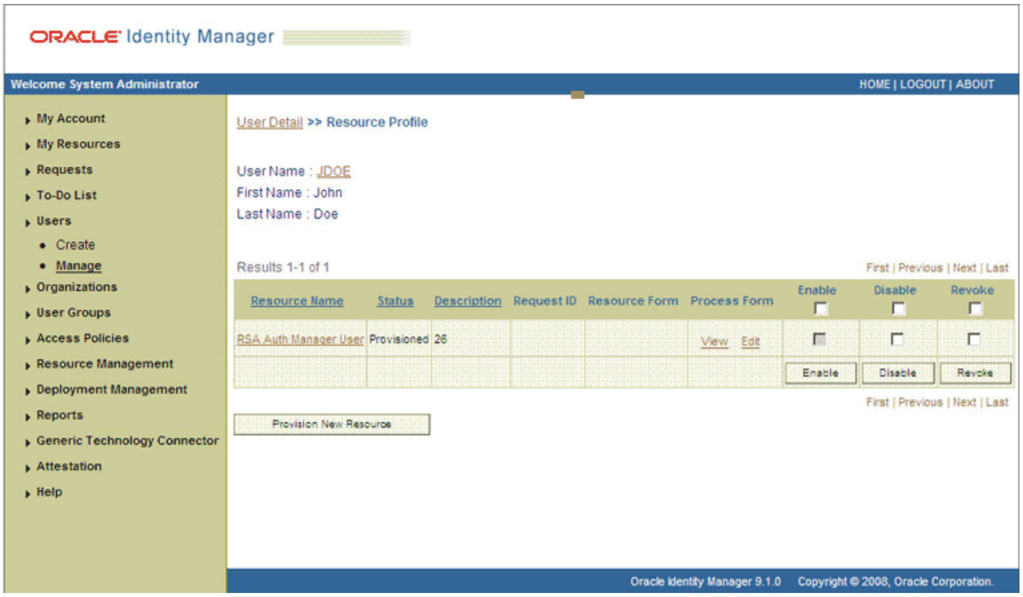
You have selected to provision RSA Auth Manager User to John Doe [JDOE].

RSA Auth Manager User Form

| | |
|---|---|
| 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*



User Detail >> Resource Profile

User Name : JDOE
First Name : John
Last Name : Doe

Results 1-1 of 1 First | Previous | Next | Last

| Resource Name | Status | Description | Request ID | Resource Form | Process Form | Enable □ | Disable □ | Revoke □ |
|---|---|---|---|---|---|---|---|---|
| RSA Auth Manager User | Provisioned | 26 | | | View Edit | □ | □ | □ |
| | | | | | | Enable | Disable | Revoke |

First | Previous | Next | Last

## 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.

## 3.9 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.

# 4 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.

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:

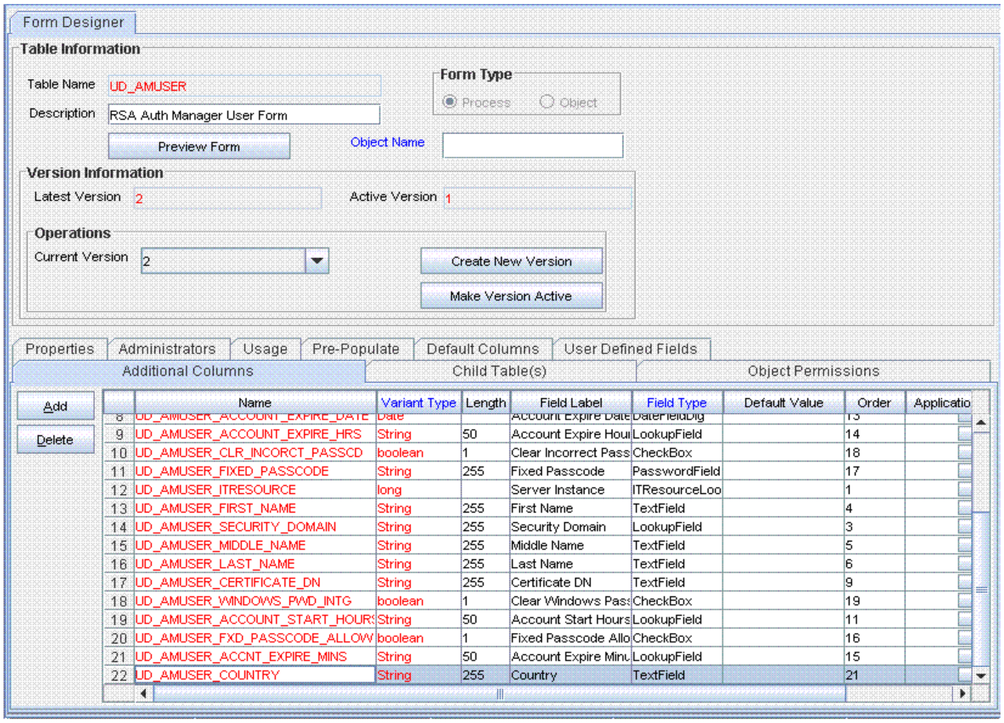


Table Information

Table Name: UD_AMUSER

Description: RSA Auth Manager User Form

Form Type: ● Process ○ Object

Object Name:

Version Information

Latest Version: 2

Active Version: 1

Operations

Current Version: 2

| | Name | Variant Type | Length | Field Label | Field Type | Default Value | Order | Applicatio |
|---|---|---|---|---|---|---|---|---|
| 8 | UD_AMUSER_ACCOUNT_EXPIRE_DATE | Date | | Account Expire Date | DateFieldDlg | | 13 | |
| 9 | UD_AMUSER_ACCOUNT_EXPIRE_HRS | String | 50 | Account Expire Hou | 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_WINDOWS_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 Min | 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.

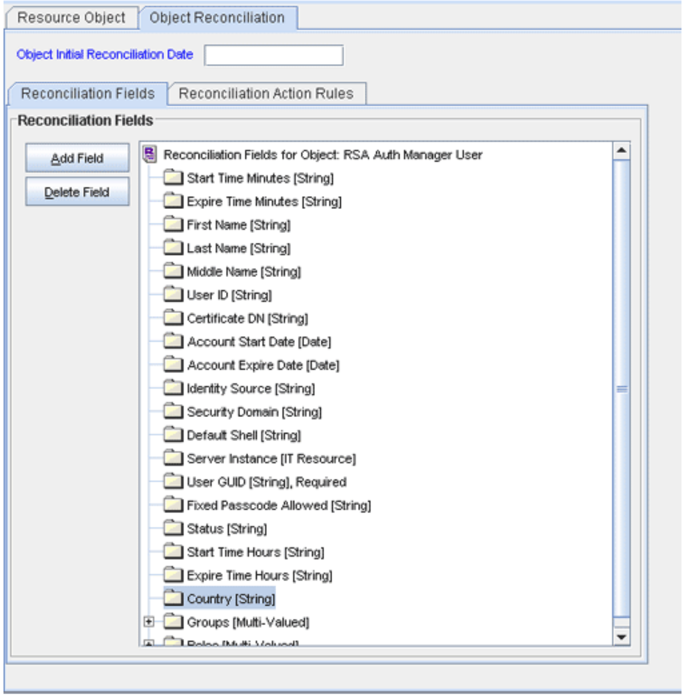
   c. On the Object Reconciliation tab, click **Add Field**.

   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:



Reconciliation Fields for Object: RSA Auth Manager User

- Start Time Minutes [String]
- Expire Time Minutes [String]
- First Name [String]
- Last Name [String]
- Middle Name [String]
- User ID [String]
- Certificate DN [String]
- Account Start Date [Date]
- Account Expire Date [Date]
- Identity Source [String]
- Security Domain [String]
- Default Shell [String]
- Server Instance [IT Resource]
- User GUID [String], Required
- Fixed Passcode Allowed [String]
- Status [String]
- Start Time Hours [String]
- Expire Time Hours [String]
- Country [String]
- Groups [Multi-Valued]
- Roles [Multi-Valued]

f. If you are using Oracle Identity Manager release 11.1.1, 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**.

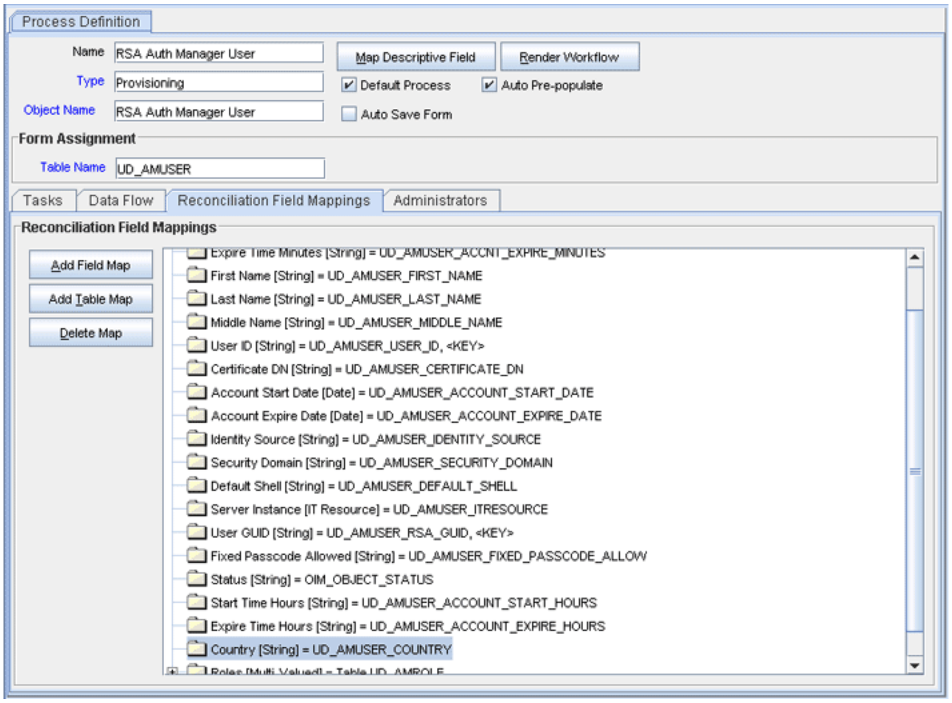
   b. Search for and open either the **RSA Auth Manager User** or the **RSA Auth Manager Token** process definition.

   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:



Name: RSA Auth Manager User

Type: Provisioning

Object Name: RSA Auth Manager User

☑ Default Process ☑ Auto Pre-populate

□ Auto Save Form

Form Assignment

Table Name: UD_AMUSER

Reconciliation Field Mappings

```
Expire Time Minutes [String] = UD_AMUSER_ACCNT_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
Roles [Multi Valued] = Table UD_AMROLE
```

5. Create an entry for the field in the lookup definition for reconciliation as follows:

   a. Expand **Administration**.

   b. Double-click **Lookup Definition.**

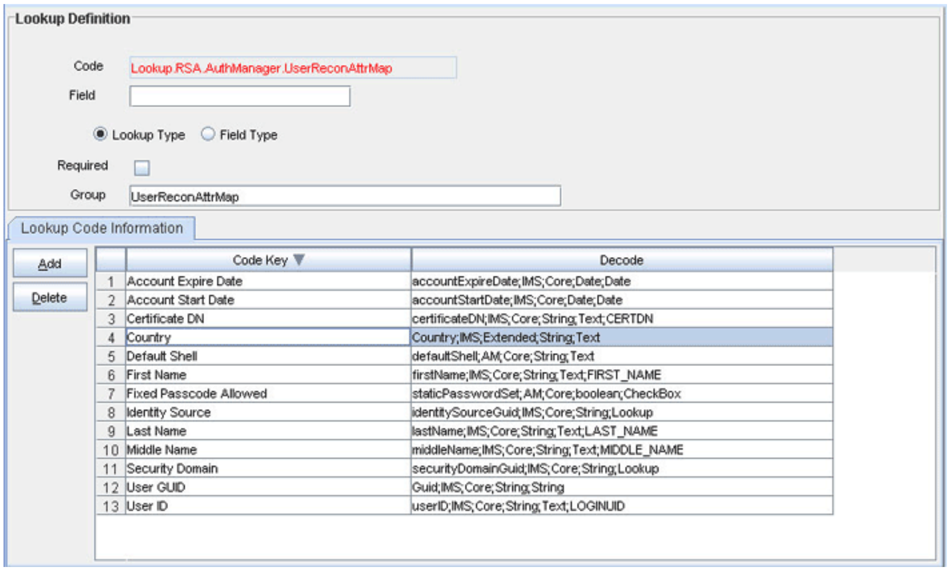
   c. Search for and open either the **Lookup.RSA.AuthManager.UserReconAttrMap** or the **Lookup.RSA.AuthManager.TokenReconAttrMap** lookup definition.

   d. 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.

   e. Click the Save icon. The following screenshot shows the entry added to the lookup definition:



Code: Lookup.RSA.AuthManager.UserReconAttrMap

Field:

● Lookup Type ○ Field Type

Required □

Group: UserReconAttrMap

| | 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.

**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:

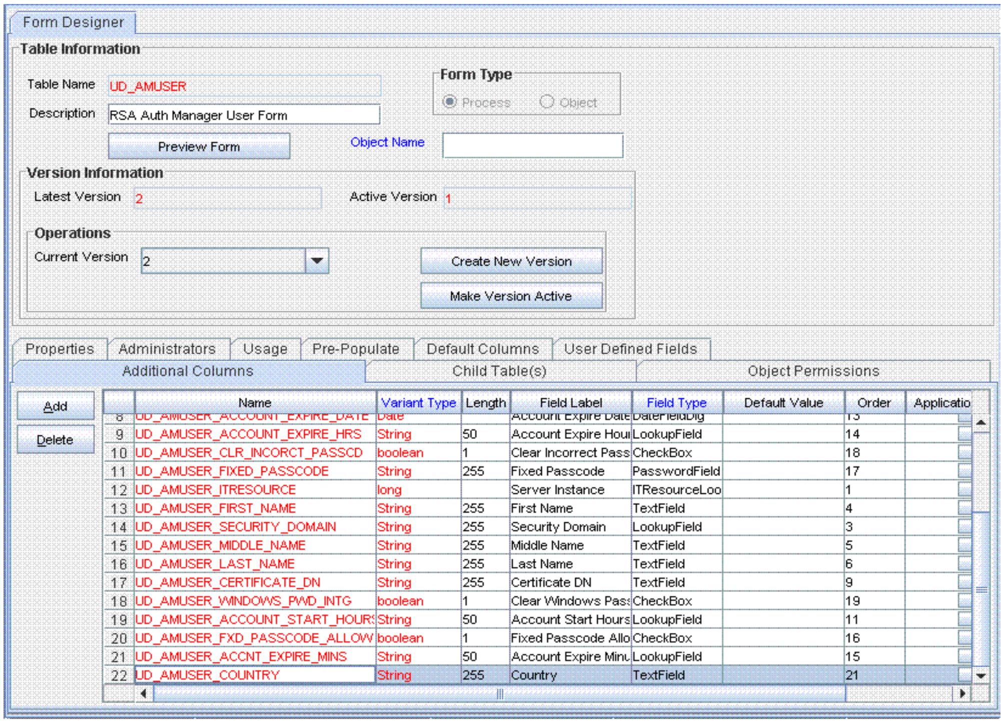


Table Information

Table Name: UD_AMUSER

Description: RSA Auth Manager User Form

Form Type: ● Process ○ Object

Object Name:

Version Information

Latest Version: 2

Active Version: 1

Operations

Current Version: 2

| | Name | Variant Type | Length | Field Label | Field Type | Default Value | Order | Applicatio |
|---|---|---|---|---|---|---|---|---|
| 8 | UD_AMUSER_ACCOUNT_EXPIRE_DATE | Date | | Account Expire Date | DateFieldDlg | | 13 | |
| 9 | UD_AMUSER_ACCOUNT_EXPIRE_HRS | String | 50 | Account Expire Hou | 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_WINDOWS_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 Minu | LookupField | | 15 | |
| 22 | 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.**

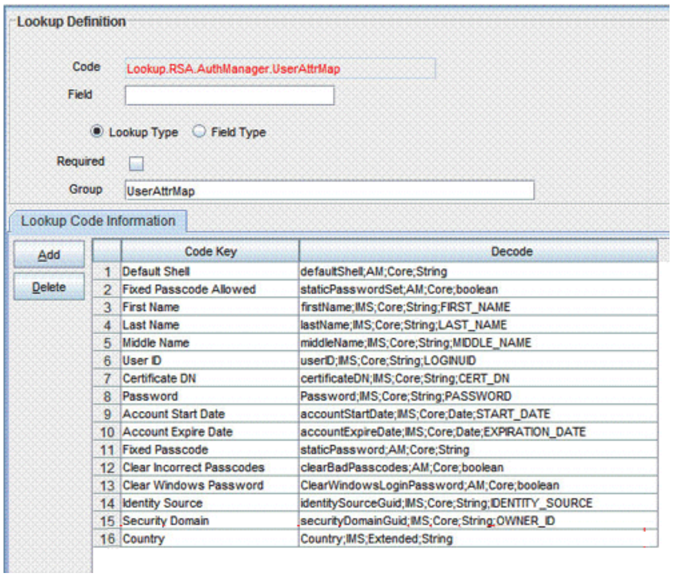
   b. Double-click **Lookup Definition.**

   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 Lookup.RSA.AuthManager.UserAttrMap

Field

● Lookup Type ○ Field Type

Required □

Group UserAttrMap

| | 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:

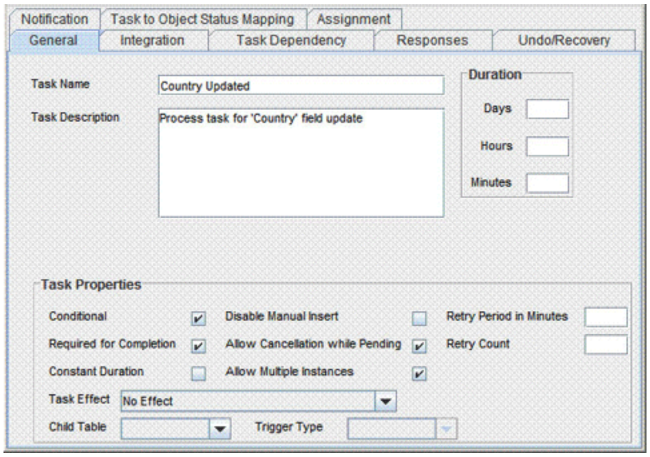
      Conditional

      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:



Task Name: Country Updated

Task Description: Process task for 'Country' field update

Days:

Hours:

Minutes:

| | | | | | |
|---|---|---|---|---|---|
| Conditional | ☑ | Disable Manual Insert | □ | Retry Period in Minutes | |
| Required for Completion | ☑ | Allow Cancellation while Pending | ☑ | Retry Count | |
| Constant Duration | □ | Allow Multiple Instances | ☑ | | |

Task Effect: No Effect

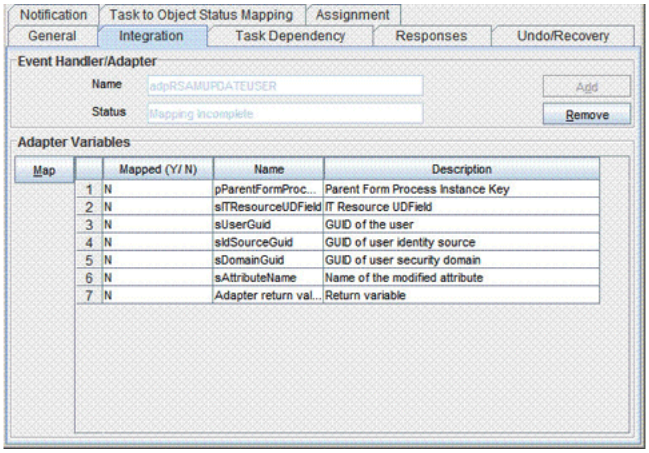
Child Table:

Trigger Type:

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:



Name: adpRSAMUPDATEUSER

Status: Mapping Incomplete

| | 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<br>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<br>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 on 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)<br>RSA Auth Manager User Recon (scheduled task)<br>RSA Auth Manager Token Recon (scheduled task) | Create a copy of the IT resource.<br>See Section 2.3.13, "Configuring Connection Parameters" for more information. |
| Resource objects | RSA Auth Manager User (user resource object)<br>RSA Auth Manager Token (token resource object) | RSA Auth Manager User Recon (scheduled task)<br>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.<br>See Section 3.4.4, "Reconciliation Scheduled Tasks" 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<br>Lookup.RSA.AuthManager.UserChildAttrMap<br>Lookup.RSA.AuthManager.UserReconAttrMap<br>Lookup.RSA.AuthManager.UserReconChildAttrMap<br>Lookup.RSA.AuthManager.TokenAttrMap<br>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.<br>See the following sections for more information:<br>Section 1.6, "Connector Objects Used During Reconciliation"<br>Section 1.7, "Connector Objects Used During Provisioning" |
| 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.<br>See Section 2.3.10, "Setting Up the Configuration Lookup Definition in Oracle Identity Manager" 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.

# 5

# 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, 3-9
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, 2-2, 2-7
communication modes
  SOAP-based, 2-43
connector files and directories, 2-1
connector functionality, extending, 4-1
Connector Installer, 2-5
connector operations, target system account, 2-26
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, 2-9
exclusion list, 1-6, 1-10, 2-36, 2-40
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, 3-3
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, 2-42
IT resources, parameters, 2-42

## J

Java API, 2-18
JAVA_OPTIONS parameters, 2-23

## K

known issues, 5-1

## L

limitations, 5-1
limited reconciliation, 1-5, 3-3
ListTokenDTO API, 1-13, 1-14, 1-15, 1-19, 1-21
logging enabling, 2-9
lookup definitions
  Lookup.RSA.AuthManager.AdminRole, 1-9, 1-10
  Lookup.RSA.AuthManager.Configuration, 1-10, 2-36, 2-43, 4-11, 4-13, 4-14, 4-15
  Lookup.RSA.AuthManager.Constants, 1-10, 2-36
  Lookup.RSA.AuthManager.DateMappings, 1-10, 2-36
  Lookup.RSA.AuthManager.FullReconFilter, 1-10, 2-36
  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, 2-34, 2-35, 2-36
  Lookup.RSA.AuthManager.LookupReconMapping, 1-9, 2-36
  Lookup.RSA.AuthManager.Minutes, 1-10
  Lookup.RSA.AuthManager.SecurityDomain, 1-8, 1-10
  Lookup.RSA.AuthManager.TokenAttrMap, 1-11, 1-20, 2-37, 4-7, 4-15
  Lookup.RSA.AuthManager.TokenProvisioningVali

- dation, 1-12, 2-40, 4-11
- Lookup.RSA.AuthManager.TokenReconAttrMap, 1-11, 1-14, 2-37, 4-5, 4-15
- Lookup.RSA.AuthManager.TokenReconValidation, 2-40, 4-11
- Lookup.RSA.AuthManager.TokenTransformMapping, 2-38
- Lookup.RSA.AuthManager.UserAttrMap, 1-11, 1-19, 2-38, 4-7, 4-15
- Lookup.RSA.AuthManager.UserChildAttrMap, 1-11, 1-20, 2-38, 4-15
- Lookup.RSA.AuthManager.UserProvisioningValidation, 2-40, 4-11
- Lookup.RSA.AuthManager.UserReconAttrMap, 1-11, 1-12, 2-38, 4-5, 4-15
- Lookup.RSA.AuthManager.UserReconChildAttrMap, 1-11, 1-14, 2-38, 4-15
- Lookup.RSA.AuthManager.UserReconValidation, 1-12, 2-40, 4-11
- Lookup.RSA.AuthManager.UserTransformMapping, 2-38, 4-13
- Lookup.SAP.UM.ExclusionList, 1-6, 1-10, 2-36, 2-40

lookup field synchronization, 1-6, 3-2

lookup fields, 1-6, 3-2

Lookup.RSA.AuthManager.AdminRole lookup definition, 1-9, 1-10

Lookup.RSA.AuthManager.Configuration lookup definition, 1-10, 2-36, 2-43, 4-11, 4-13, 4-14, 4-15

Lookup.RSA.AuthManager.Constants lookup definition, 1-10, 2-36

Lookup.RSA.AuthManager.DateMappings lookup definition, 1-10, 2-36

Lookup.RSA.AuthManager.FullReconFilter lookup definition, 1-10, 2-36

Lookup.RSA.AuthManager.Group lookup definition, 1-7, 1-10, 2-16

Lookup.RSA.AuthManager.Hours lookup definition, 1-10

Lookup.RSA.AuthManager.IdentitySource lookup definition, 1-8, 1-10

Lookup.RSA.AuthManager.ITResourceMapping lookup definition, 1-11, 2-34, 2-35, 2-36

Lookup.RSA.AuthManager.LookupReconMapping lookup definition, 1-9, 2-36

Lookup.RSA.AuthManager.Minutes lookup definition, 1-10

Lookup.RSA.AuthManager.SecurityDomain lookup definition, 1-8, 1-10

Lookup.RSA.AuthManager.TokenAttrMap lookup definition, 1-11, 1-20, 2-37, 4-7, 4-15

Lookup.RSA.AuthManager.TokenProvisioningValidation lookup definition, 1-12, 2-40, 4-11

Lookup.RSA.AuthManager.TokenReconAttrMap lookup definition, 1-11, 1-14, 2-37, 4-5, 4-15

Lookup.RSA.AuthManager.TokenReconValidation lookup definition, 2-40, 4-11

Lookup.RSA.AuthManager.TokenTransformMapping lookup definition, 2-38

Lookup.RSA.AuthManager.UserAttrMap lookup definition, 1-11, 1-19, 2-38, 4-7, 4-15

Lookup.RSA.AuthManager.UserChildAttrMap lookup definition, 1-11, 1-20, 2-38, 4-15

Lookup.RSA.AuthManager.UserProvisioningValidation lookup definition, 2-40, 4-11

Lookup.RSA.AuthManager.UserReconAttrMap lookup definition, 1-11, 1-12, 2-38, 4-5, 4-15

Lookup.RSA.AuthManager.UserReconChildAttrMap lookup definition, 1-11, 1-14, 2-38, 4-15

Lookup.RSA.AuthManager.UserReconValidation lookup definition, 1-12, 2-40, 4-11

Lookup.RSA.AuthManager.UserTransformMapping lookup definition, 2-38, 4-13

Lookup.SAP.UM.ExclusionList lookup definition, 1-6, 1-10, 2-36, 2-40

## M

Microsoft SQL Server, 2-14

## P

parameters of IT resources, 2-42

PrincipalDTO API, 1-13, 1-20

provisioning
- direct provisioning, 3-10
- provisioning triggered by policy changes, 3-10
- request-based provisioning, 3-10

provisioning functions, supported, 1-19

PurgeCache utility, 2-6

## R

reconciliation
- adding new attributes, 4-2
- full, 1-5
- incremental, 1-5

reconciliation rule for token data, 1-16

reconciliation rule for user data, 1-15

release number of connector, determining, 2-2

request-based provisioning, 2-42

RSA Auth Manager Lookup Recon scheduled task, 1-7, 1-9, 2-36, 3-2, 3-7, 4-15

RSA Auth Manager Token Recon scheduled task, 1-3, 3-6, 3-7, 4-15, 4-16

RSA Auth Manager User Recon scheduled task, 1-3, 1-6, 3-5, 3-7, 4-15, 4-16

RSA Authentication Manager 7.1, 1-2

RSA Authentication Manager APIs
- AMPrincipalDTO, 1-13, 1-20
- ListTokenDTO, 1-13, 1-14, 1-15, 1-19, 1-21
- PrincipalDTO, 1-13, 1-20
- TokenDTO, 1-13, 1-14, 1-15, 1-19, 1-21

RSA Authentication Manager attributes, 1-13, 1-19, 1-21

RSA Authentication Manager Java API, 2-18

## S

scheduled tasks
- configuring, 3-7

RSA Auth Manager Lookup Recon, 1-7, 1-9, 2-36, 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, 2-43
software tokens, assigning, 3-9
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, 2-26
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, 2-38, 4-12

U

user reconciliation rule, 1-15

V

validation, 1-6, 1-12, 2-38, 2-39, 2-40, 4-10