Oracle® Identity Manager

Connector Guide for RSA Authentication Manager

Release 11.1.1

E52545-12

Oracle Identity Manager Connector Guide for RSA Authentication Manager, Release 11.1.1

E52545-12

Primary Author: Maya Chakrapani

Contents

Preface

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

1 About the RSA Authentication Manager Connector

2 Deploying the RSA Authentication Manager Connector

3 Using the RSA Authentication Manager Connector

List of Figures

List of Tables

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 that have purchased support 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, visit the following Oracle Help Center page:

http://docs.oracle.com/cd/E52734_01/index.html

For information about Oracle Identity Manager Connectors documentation, visit the following Oracle Help Center page:

http://docs.oracle.com/cd/E22999_01/index.htm

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://download.oracle.com/docs/cd/E22999_01/index.htm`

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 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 11.1.1.5.0.

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

- Software Updates

  This section describes updates made to the connector software. This section also points out the sections of this guide that have been changed in response to each software update.

- Documentation-Specific Updates

  These include major changes made to this guide. For example, the relocation of a section from the second chapter to the third chapter is a documentation-specific update. These changes are not related to software updates.

Software Updates

The following section discusses software updates:

Software Updates in Release 11.1.1.5.0

This is the first release of the Oracle Identity Manager connector for RSA Authentication Manager based on ICF architecture. Therefore, there are no software updates for this release of the connector.

Documentation-Specific Updates

The Chapter Known Issues and Workarounds has been removed.

Documentation Updates in Release 11.1.1.5.0

The following is a documentation-specific update in revision "10" of release 11.1.1.5.0:

Few editorial changes and minor updates to the document structure have been made for better readability.

The following is a documentation-specific update in revision "9" of release 11.1.1.5.0:

The "Oracle Identity Governance or Oracle Identity Manager" row of Table 1-1 has been updated to include support for Oracle Identity Governance release 12*c* PS4 (12.2.1.4.0).

The following is a documentation-specific update in revision "8" of release 11.1.1.5.0:

A "Note" regarding the **Incorrect Passcodes** check box has been added to User Fields for Provisioning.

The following are documentation-specific updates in revision "7" of release 11.1.1.5.0:

- Additional certification details for Oracle Identity Governance 12c (12.2.1.3.0) has been added to Table 1-1.
- The "Target Systems" row in Table 1-1 has been modified to include the supported version RSA Authentication Manager 8.3 and 8.4.

The following are documentation-specific updates in revision "6" of release 11.1.1.5.0:

- The "Target Systems" row in Table 1-1 has been modified to include the supported version RSA Authentication Manager 8.2.
- The "JDK" row has been added to Table 1-1.

The following is a documentation-specific update in revision "5" of release 11.1.1.5.0:

The "Oracle Identity Manager" row of Table 1-1 has been updated.

The following are documentation-specific updates in revision "4" of release 11.1.1.5.0:

- A "Note" regarding lookup queries has been added at the beginning of Extending the Functionality of the RSA Authentication Manager Connector .
- A "Note" regarding lookup queries has been removed from Lookup Definitions Used During Reconciliation and Provisioning.

The following are documentation-specific updates in revision "3" of release 11.1.1.5.0:

- The following are documentation-specific updates in revision "4" of release 11.1.1.5.0:
- A "Note" regarding lookup queries has been added to Lookup Definitions Used During Reconciliation and Provisioning.
- The "Target System" row of Table 1-1 has been updated.

The following is a documentation-specific update in revision "2" of release 11.1.1.5.0:

Configuring Self-Request Provisioning has been added.

1

About the RSA Authentication Manager Connector

This chapter introduces the RSA Authentication Manager connector.

This chapter discusses the following topics:

- Introduction to RSA Authentication Manager Connector
- Certified Components
- Usage Recommendation
- Certified Languages
- Connector Architecture
- Features of the Connector
- Lookup Definitions Used During Reconciliation and Provisioning
- Connector Objects Used During Reconciliation
- Connector Objects Used During Provisioning
- Roadmap for Deploying and Using the Connector

1.1 Introduction to RSA Authentication Manager 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.

1.2 Certified Components

Table 1-1 lists the certified components for the target system.

Table 1-1 Certified Components

Item	Requirement
Oracle Identity Governance or Oracle Identity Manager	You can use one of the following releases of Oracle Identity Manager: • Oracle Identity Governance 12*c* (12.2.1.4.0) • Oracle Identity Governance 12*c* (12.2.1.3.0) • Oracle Identity Manager 11*g* Release 2 PS3 (11.1.2.3.0) • Oracle Identity Manager 11*g* Release 2 PS2 (11.1.2.2.0) and any later BP in this release track • Oracle Identity Manager 11*g* Release 2 PS1 (11.1.2.1.0) and any later BP in this release track • Oracle Identity Manager 11*g* Release 2 (11.1.2.0.0) and any later BP in this release track
Target System	You can use one of the following supported versions of the target system: • RSA Authentication Manager 8.0 or later
Connector Server	11.1.2.1.0
Connector Server JDK	JDK 1.6 or later

1.3 Usage Recommendation

Depending on the Oracle Identity Manager version that you are using, you must deploy and use one of the following connectors:

- If you are using an Oracle Identity Manager release that is earlier than Oracle Identity Manager 11*g* Release 2 (11.1.2.0.0), then you must use the 9.1.0.*x* version of this connector. However, if you are using RSA Authentication Manager 6.0, or 6.1, or 6.1.2, then you must use the 9.0.4.*x* version of this connector.
- If you are using Oracle Identity Manager 11*g* Release 2 or later, then you must use the 11.1.1.*x* version of this connector. However, if you are using RSA Authentication Manager 7.1 with SP3 or later, then use the 9.1.0.*x* version of this connector.

1.4 Certified Languages

The connector supports the following languages:

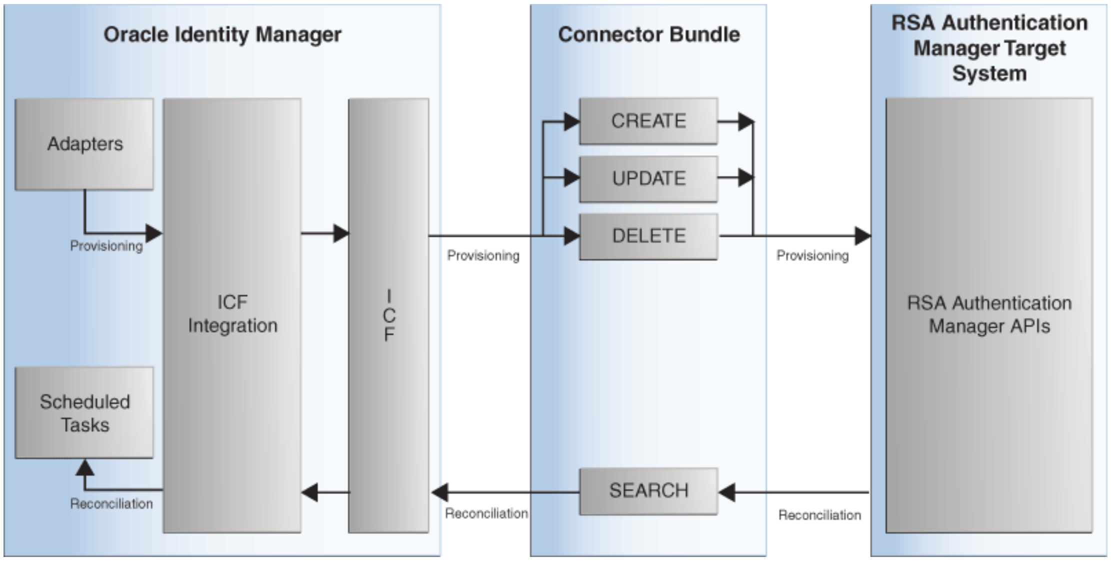
- Arabic
- Chinese (Simplified)
- Chinese (Traditional)
- Czech
- Danish
- Dutch
- English (UK)
- English (US)
- Finnish

- French
- German
- Greek
- Hebrew
- Hungarian
- Italian
- Japanese
- Korean
- Norwegian
- Polish
- Portuguese
- Portuguese (Brazilian)
- Romanian
- Russian
- Slovak
- Spanish
- Swedish
- Thai
- Turkish

1.5 Connector Architecture

Figure 1-1 shows the architecture of the connector.

Figure 1-1 Connector Architecture



The RSA Authentication Manager connector is implemented by using the Identity Connector Framework (ICF). The ICF is a component that provides basic reconciliation and provisioning operations that are common to all Oracle Identity Manager connectors. In addition, ICF provides common features that developers would otherwise need to implement on their own, such as connection pooling, buffering, time outs, and filtering. The ICF is shipped along with Oracle Identity Manager. Therefore, you need not configure or modify the ICF.

This connector is used to manage users and tokens on RSA Authentication Manager through Oracle Identity Manager. This connector integrates Oracle Identity Manager with the target system with the help of a Java API.

The target system can be configured to run in the Account Management mode. Account management is also known as target resource management. In this mode, the target system is used as a target resource and the connector enables the following operations:

- Provisioning:

  Provisioning involves creating, updating, or deleting users and tokens on the target system through Oracle Identity Manager. The connector makes use of the Java API to connect to the RSA AM Server, and in turn provision accounts and tokens.

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

  During user provisioning, data received in the create/update operation will be passed to the target system APIs. RSA APIs accept provisioning data, carry out the required operation on the target system, and then return the response from the target system back to the connector. The connector will return the response to Oracle Identity Manager.

- Target source reconciliation:

  During reconciliation, the connector fetches data (using scheduled jobs) about users created or modified directly on the target system into Oracle Identity Manager. This data is used to add or modify resources allocated to OIM Users.

  Similarly, during reconciliation, the RSA APIs will accept the search criteria, including filters, and return the records to the connector. The connector supports searching for users, tokens, roles, groups, identity sources, security domains and RADIUS profiles on the target.

1.7 Lookup Definitions Used During Reconciliation and Provisioning

Lookup definitions used during reconciliation and provisioning can either be synchronized with the target system or preconfigured. The following sections contain detailed information:

- About Lookup Field Synchronization
- Lookup Definitions Synchronized with the Target System
- Preconfigured Lookup Definitions

1.7.1 About Lookup Field Synchronization

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.

1.7.2 Lookup Definitions Synchronized with the Target System

The following lookup definitions are populated with values fetched from the target system by the scheduled jobs for lookup field synchronization:

- Lookup.RSAAM.UserGroup
- Lookup.RSAAM.IdentitySource
- Lookup.RSAAM.SecurityDomain
- Lookup.RSAAM.AdminRole
- Lookup.RSAAM.TokenSerial
- Lookup.RSAAM.RadiusProfile

> **Note:**
>
> See Scheduled Job for Lookup Field Synchronization.

1.7.2.1 Lookup.RSAAM.UserGroup

The Lookup.RSAAM.UserGroup lookup definition holds details of user groups defined on RSA Authentication Manager. You populate this lookup definition through lookup field synchronization performed using the RSAAM UserGroup Lookup Reconciliation scheduled job.

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~IDENTITY_SOURCE_NAME~SECURITY_DOMAIN_NAME~GROUP_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.

  - *SECURITY_DOMAIN_NAME* is the name of the security domain on the target system.
  - *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
41~ims.898afd743afcb10a1b20d2688a0b14be	RSA Server Instance~Internal Database~SecDom1a~Group1
41~ims.2820d78e3afcb10a1bc9883fa4aedc51	RSA Server Instance~Internal Database~SystemDomain~Group3
41~ims.3139e7eb3afcb10a1bc8f2e9afd7a77e	RSA Server Instance~Internal Database~SystemDomain~Group2

1.7.2.2 Lookup.RSAAM.IdentitySource

In RSA Authentication Manager, an identity source can be the default internal database, an LDAP-based solution, or a database. The Lookup.RSAAM.IdentitySource lookup definition holds details of the identity sources configured for your target system installation. You populate this lookup definition through lookup field synchronization performed using the RSAAM IdentitySource Lookup Reconciliation scheduled job.

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

1.7.2.3 Lookup.RSAAM.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. You populate this lookup definition through lookup field synchronization performed using the RSAAM SecurityDomain Lookup Reconciliation scheduled job.

The Lookup.RSAAM.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.00000000000000000000001000e0011000	RSA Server Instance~SystemDomain
1~ims.6de7d3c19e3714ac017cfd3c69eec20e	RSA Server Instance~Domain1
1~ims.6e3dc8939e3714ac02019a05130a8285	RSA Server Instance~Domain2

1.7.2.4 Lookup.RSAAM.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. You populate this lookup definition through lookup field synchronization performed using the RSAAM AdminRole Lookup Reconciliation scheduled job.

The Lookup.RSAAM.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~SECURITY_DOMAIN_NAME~ROLE_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.
  - *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
41~ims.000000000000000000002000f0035001	RSA Server Instance~SystemDomain~Auth Mgr Root Domain Admin
41~ims.000000000000000000001000e0031001	RSA Server Instance~SystemDomain~TrustedRealmAdminRole

1.7.2.5 Lookup.RSAAM.TokenSerial

On RSA Authentication Manager, a token serial is a unique identification number provided for every token. You populate this lookup definition through lookup field synchronization performed using the RSAAM TokenSerial Lookup Reconciliation scheduled job.

The Lookup.RSAAM.TokenSerial lookup definition stores details of token serials. The following is the format of entries in this lookup definition:

- Code Key: *IT_RESOURCE_KEY~TOKEN_SERIAL_NUMBER*

  In this format:

  - *IT_RESOURCE_KEY* is the key assigned to the IT resource on Oracle Identity Manager.
  - *TOKEN_SERIAL_NUMBER* is the number assigned to the token on the target system.
- Decode: *IT_RESOURCE_NAME~SECURITY_DOMAIN_NAME~TOKEN_SERIAL_NUMBER*

  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.
  - *TOKEN_SERIAL_NUMBER* is the number assigned to the token on the target system.

The following table shows sample entries in this lookup definition:

Code Key	Decode
41~000221996071	RSA Server Instance~SecDom2a~000221996071
41~000221996081	RSA Server Instance~SystemDomain~000221996081

1.7.2.6 Lookup.RSAAM.RadiusProfile

On RSA Authentication Manager, a radius profile is a collection of attributes that specify session requirements for a users authentication using RADIUS. These attributes are contained in a checklist or a return list. You populate this lookup definition through lookup field synchronization performed using the RSAAM RadiusProfile Lookup Reconciliation scheduled job.

The Lookup.RSAAM.RadiusProfile lookup definition stores details of radius profiles. The following is the format of entries in this lookup definition:

- Code Key: *IT_RESOURCE_KEY~RADIUS_PROFILE_GUID*

  In this format:

  - *IT_RESOURCE_KEY* is the key assigned to the IT resource on Oracle Identity Manager.
  - *RADIUS_PROFILE_GUID* is the GUID of the radius profile on the target system.
- Decode: *IT_RESOURCE_NAME~SECURITY_DOMAIN_NAME~RADIUS_PROFILE_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.
  - *RADIUS_PROFILE_NAME* is the name of the profile on the target system.

The following table shows sample entries in this lookup definition:

Code Key	Decode
41~ims.a0f646313afcb10a1ba80b1af3204720	RSA Server Instance~SystemDomain~RAD_PROF2
41~ims.6b630bf63afcb10a1bc062fe04d92672	RSA Server Instance~SystemDomain~RAD_PROF1

1.7.3 Preconfigured Lookup Definitions

This section discusses 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. The other lookup definitions are as follows:

- Lookup.RSAAM.Configuration
- Lookup.RSAAM.UM.Configuration
- Lookup.RSAAM.UM.ProvAttrMap
- Lookup.RSAAM.UM.ReconAttrMap
- Lookup.RSAAM.Token.Configuration
- Lookup.RSAAM.Token.ProvAttrMap
- Lookup.RSAAM.Token.ReconAttrMap
- Lookup.RSAAM.Hours
- Lookup.RSAAM.Minutes

1.7.3.1 Lookup.RSAAM.Configuration

The Lookup.RSAAM.Configuration lookup definition holds connector configuration entries that are used during target resource reconciliation and provisioning operations.

Table 1-2 lists the default entries in this lookup definition.

Table 1-2   Entries in the Lookup.RSAAM.Configuration Lookup Definition

Code Key	Decode	Description
Bundle Name	org.identityconnectors.rsaam	This entry holds the name of the connector bundle package. Do *not* modify this entry.
Bundle Version	1.0.1115	This entry holds the version of the connector bundle class. Do *not* modify this entry.
Connector Name	org.identityconnectors.rsaam.RSAAMConnector	This entry holds the name of the connector class. Do *not* modify this entry.
User Configuration Lookup	Lookup.RSAAM.UM.Configuration	This entry holds the name of the lookup definition that contains user-specific configuration properties. Do *not* modify this entry.
defaultBatchSize	1000	This entry holds the number of records that must be included in each batch during batched reconciliation. This entry is used only when the Batch Size attribute of the user reconciliation scheduled jobs is either empty or set to 0. See Batched Reconciliation for more information about the Batch Size attribute.
Token Configuration Lookup	Lookup.RSAAM.Token.Configuration	This entry holds the name of the lookup definition that contains token-specific configuration properties. Do *not* modify this entry.

If the computer hosting Oracle Identity Manager and RSA Authentication Manger are in different time zones, you can configure it by following the procedure mentioned in Setting up the Lookup Definition for Different Time Zones.

1.7.3.2 Lookup.RSAAM.UM.Configuration

The Lookup.RSAAM.UM.Configuration lookup definition holds configuration entries that are specific to the user object type. This lookup definition is used during user management operations when your target system is configured as a target resource.

Table 1-3 lists the default entries in this lookup definition.

Table 1-3   Entries in the Lookup.RSAAM.UM.Configuration Lookup Definition

Code Key	Decode	Description
Provisioning Attribute Map	Lookup.RSAAM.UM.ProvAttrMap	This entry holds the name of the lookup definition that maps process form fields and target system attributes. See Lookup.RSAAM.UM.ProvAttrMap for more information about this lookup definition.
Recon Attribute Map	Lookup.RSAAM.UM.ReconAttrMap	This entry holds the name of the lookup definition that maps resource object fields and target system attributes. See Lookup.RSAAM.UM.ReconAttrMap for more information about this lookup definition.

1.7.3.3 Lookup.RSAAM.UM.ProvAttrMap

The Lookup.RSAAM.UM.ProvAttrMap lookup definition holds mappings between process form fields and target system attributes. This lookup definitions is used during provisioning. This lookup definition is preconfigured. Table 1-10 lists the default entries.

You can add entries in this lookup definitions if you want to map new target system attributes for provisioning. See Adding New User or Token Attributes for Provisioning.

1.7.3.4 Lookup.RSAAM.UM.ReconAttrMap

The Lookup.RSAAM.UM.ReconAttrMap lookup definition holds mappings between resource object fields and target system attributes. This lookup definition is used during reconciliation. This lookup definition is preconfigured. Table 1-5 lists the default entries.

You can add entries in this lookup definitions if you want to map new target system attributes for reconciliation. See Adding New User or Token Attributes for Reconciliation.

1.7.3.5 Lookup.RSAAM.Token.Configuration

The Lookup.RSAAM.Token.Configuration lookup definition holds configuration entries that are specific to the token object type. This lookup definition is used during token management operations when your target system is configured as a target resource.

Table 1-4 lists the default entries in this lookup definition.

Table 1-4   Entries in the Lookup.RSAAM.Token.Configuration Lookup Definition

Code Key	Decode	Description
Provisioning Attribute Map	Lookup.RSAAM.Token.ProvAttrMap	This entry holds the name of the lookup definition that maps process form fields and target system attributes. See Lookup.RSAAM.Token.ProvAttrMap for more information about this lookup.
Recon Attribute Map	Lookup.RSAAM.Token.ReconAttrMap	This entry holds the name of the lookup definition that maps resource object fields and target system attributes. See Lookup.RSAAM.Token.ReconAttrMap for more information about this lookup.

1.7.3.6 Lookup.RSAAM.Token.ProvAttrMap

The Lookup.RSAAM.Token.ProvAttrMap lookup definition holds mappings between process form fields and target system attributes. This lookup definitions is used during provisioning. This lookup definition is preconfigured. Table 1-11 lists the default entries.

You can add entries in this lookup definitions if you want to map new target system attributes for provisioning. See Adding New User or Token Attributes for Provisioning.

1.7.3.7 Lookup.RSAAM.Token.ReconAttrMap

The Lookup.RSAAM.Token.ReconAttrMap lookup definition holds mappings between resource object fields and target system attributes. This lookup definition is used during reconciliation. This lookup definition is preconfigured. Table 1-7 lists the default entries.

You can add entries in this lookup definitions if you want to map new target system attributes for reconciliation. See Adding New User or Token Attributes for Reconciliation.

1.7.3.8 Lookup.RSAAM.Hours

The Lookup.RSAAM.Hours lookup definition holds the list of configured hours. This is a static lookup definition. You cannot modify or add entries in this lookup definition.

1.7.3.9 Lookup.RSAAM.Minutes

The Lookup.RSAAM.Minutes lookup definition holds the list of configured minutes. This is a static lookup definition. You cannot modify or add entries in this lookup definition.

1.8 Connector Objects Used During Reconciliation

Target resource reconciliation involves fetching data about newly created or modified accounts on the target system and using this data to add or modify resources assigned to OIM Users.

The RSAAM User Target Reconciliation and RSAAM Token Target Reconciliation scheduled jobs are used to initiate a target resource reconciliation run. These scheduled jobs are discussed in Scheduled Jobs for Reconciliation of Token and User Records.

This section discusses the following topics:

- User Fields for Target Resource Reconciliation
- Reconciliation Rule for User Target Resource Reconciliation
- Viewing Reconciliation Rule for User Target Resource Reconciliation
- Reconciliation Action Rules for User Target Resource Reconciliation
- Viewing Reconciliation Action Rules for User Target Resource Reconciliation
- Token Fields for Target Resource Reconciliation
- Reconciliation Rule for Token Target Resource Reconciliation
- Viewing Reconciliation Rule for Token Target Resource Reconciliation
- Reconciliation Action Rules for Token Target Resource Reconciliation
- Viewing Reconciliation Action Rule for Token Target Resource Reconciliation

1.8.1 User Fields for Target Resource Reconciliation

The Lookup.RSAAM.UM.ReconAttrMap lookup definition maps resource object fields and target system attributes. This lookup definition is used for performing target resource user reconciliation runs.

In this lookup definition, entries are in the following format:

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

  METHOD_NAME;PRINCIPAL_TYPE;ATTRIBUTE_TYPE;METHOD_RETURN_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 classes:
  - com.rsa.admin.data.PrincipalDTO
  - com.rsa.authmgr.admin.principalmgt.data.AMPrincipalDTO

  The `get` or `is` 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_RETURN_TYPE* is the data type of the value returned by 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 class.

Table 1-5 provides information about user attribute mappings for target resource reconciliation.

Table 1-5 Entries in the Lookup.RSAAM.UM.ReconAttrMap lookup definition

Code	Decode
Account Expire Date[Date]	accountExpireDate;IMS;Core;Date;EXPIRATION_DATE
Account Expire Hours	AccountExpireHours
Account Expire Minutes	AccountExpireMinutes
Account Start Date[Date]	accountStartDate;IMS;Core;Date;START_DATE
Account Start Hours	AccountStartHours
Account Start Minutes	AccountStartMinutes
Certificate DN	certificateDN;IMS;Core;String;CERT_DN
Clear Incorrect Passcodes	clearBadPasscodes;AM;Core;boolean
Clear Windows Password	clearWindowsLoginPassword;AM;Core;boolean
Default Shell	defaultShell;AM;Core;String
First Name	firstName;IMS;Core;String;FIRST_NAME
Fixed Passcode Allowed	staticPasswordSet;AM;Core;boolean
Groups~Group Name[LOOKUP]	UserGroup
Identity Source[LOOKUP]	identitySourceGuid;IMS;Core;String;IDENTITY_SRC_ID
Last Name	lastName;IMS;Core;String;LAST_NAME

Table 1-5 (Cont.) Entries in the Lookup.RSAAM.UM.ReconAttrMap lookup definition

Code	Decode
Middle Name	middleName;IMS;Core;String;MIDDLE_NAME
Security Domain[LOOKUP]	securityDomainGuid;IMS;Core;String;OWNER_ID
Roles~Role Name[LOOKUP]	AdminRole
Radius Profile[LOOKUP]	radiusProfileGuid;AM;Core;String
Status	_ENABLE_
User GUID	_UID_
User ID	_NAME_

1.8.2 Reconciliation Rule for User Target Resource Reconciliation

> **See Also:**
>
> Reconciliation Engine in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager* for generic information about reconciliation matching and action rules.

The following is the process-matching rule:

Rule name: RSA AuthManager UserRecon

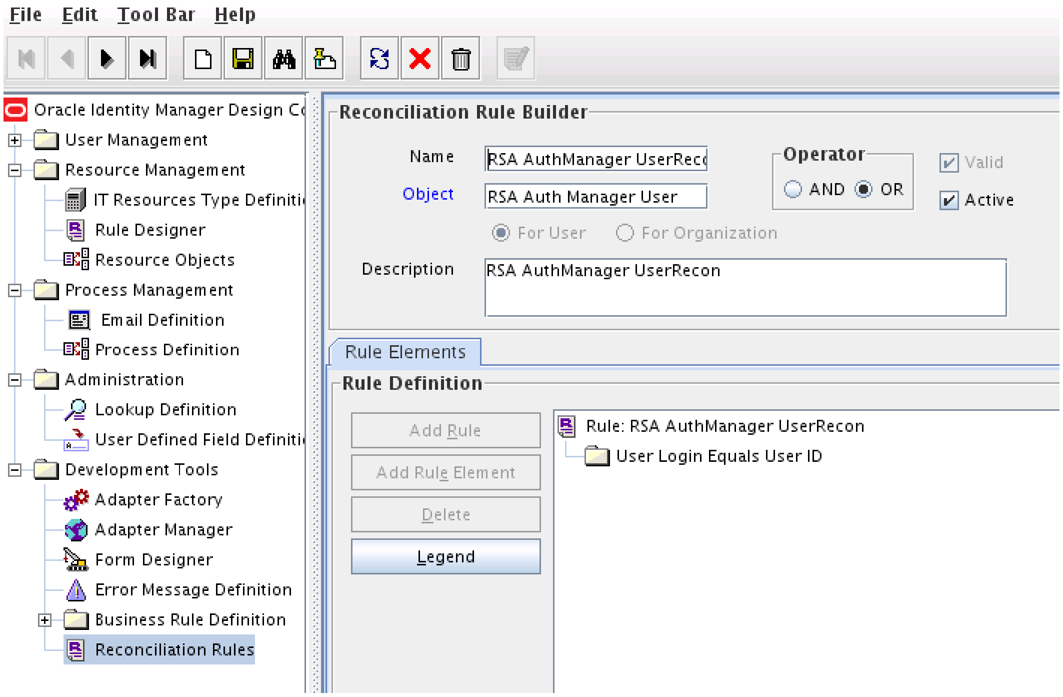
Rule element: User Login Equals User ID where the User Login is the User ID field on the OIM User form and the User ID is the user ID (_NAME_) field of RSA Authentication Manager.

1.8.3 Viewing Reconciliation Rule for User Target Resource Reconciliation

After you have deployed 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 UserRecon**. Figure 1-2 shows the reconciliation rule for target resource reconciliation.

Figure 1-2   Reconciliation Rule for Target Resource Reconciliation



Reconciliation Rule Builder

Name: RSA AuthManager UserRecc

Object: RSA Auth Manager User

Operator: ○ AND ● OR

☑ Valid

☑ Active

● For User ○ For Organization

Description: RSA AuthManager UserRecon

Rule Definition

Rule: RSA AuthManager UserRecon
User Login Equals User ID

1.8.4 Reconciliation Action Rules for User Target Resource Reconciliation

The action rules for target resource reconciliation are listed in Table 1-6.

Table 1-6   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

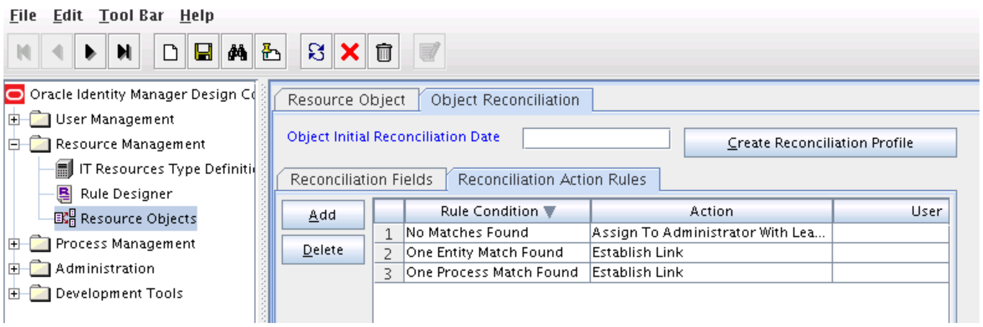
> **Note:**
>
> No action is performed for rule conditions that are not predefined for this connector. You can define your own action rule for such rule conditions. See the following topics in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*:
>
> - Setting a Reconciliation Action Rule (Developing Identity Connectors using Java)
> - Setting a Reconciliation Action Rule (Developing Identity Connectors using .net)

1.8.5 Viewing Reconciliation Action Rules for User Target Resource Reconciliation

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 1-3 shows the reconciliation action rule for target resource reconciliation.

Figure 1-3 Reconciliation Action Rules for Target Resource Reconciliation



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

1.8.6 Token Fields for Target Resource Reconciliation

The Lookup.RSAAM.Token.ReconAttrMap lookup definition maps resource object fields and target system attributes. This lookup definition is used for performing target resource user reconciliation runs.

In this lookup definition, entries are in the following format:

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

  METHOD_NAME;API_NAME;ATTRIBUTE_TYPE;METHOD_RETURN_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 classes:
  - com.rsa.admin.data.ListTokenDTO
  - com.rsa.authmgr.admin.principalmgt.data.TokenDTO

> **Note:**
>
> If the field is present in both ListTokenDTO and TokenDTO, use the field from ListTokenDTO for better performance.

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.
- *`DTO_ATTRIBUTE_NAME`* is the name of the attribute in the ListTokenDTO or TokenDTO class.

Table 1-7 provides information about user attribute mappings for target resource reconciliation.

Table 1-7   Entries in the Lookup.RSAAM.Token.ReconAttrMap lookup definition

Code	Decode
Notes	notes;ListTokenDTO;Core;String
Status	_ENABLE_
Token GUID	_UID_
Token Lost	tokenLost;ListTokenDTO;Core;boolean;tokenLost
Token Serial Number[LOOKUP]	_NAME_
User GUID	principalId;TokenDTO;Core;String
User ID	assignedUser;ListTokenDTO;Core;String;principalID

1.8.7 Reconciliation Rule for Token Target Resource Reconciliation

> **See Also:**
>
> Reconciliation Engine in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager* for generic information about reconciliation matching and action rules

The following is the process-matching rule:

Rule name: RSA AuthManager TokenRecon

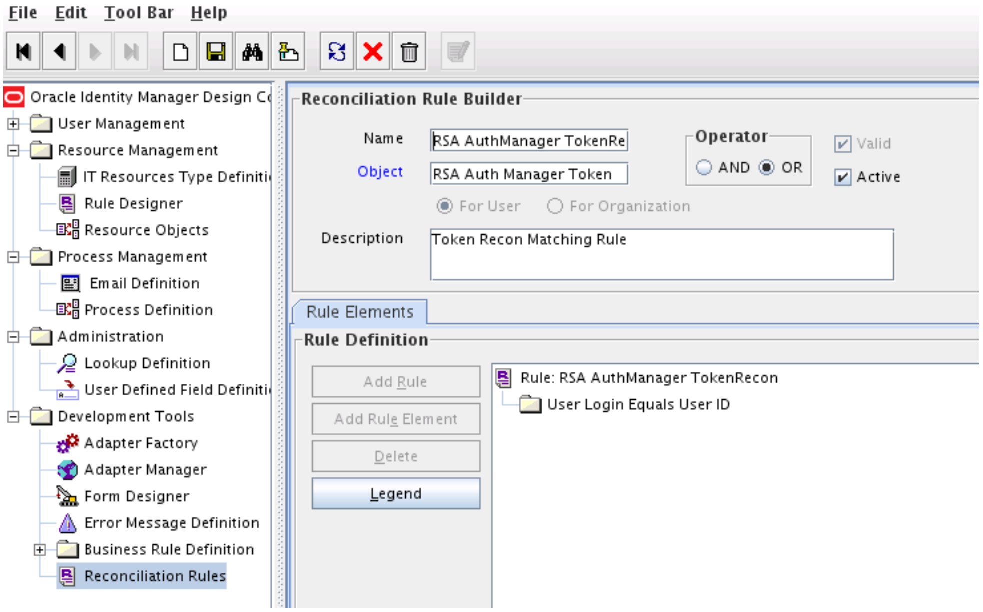
Rule element: User Login Equals User ID where the User Login is the User ID field on the OIM User form and the User ID is the user ID (_NAME_) field of RSA Authentication Manager.

1.8.8 Viewing Reconciliation Rule for Token Target Resource Reconciliation

After you have deployed 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 1-2 shows the reconciliation rule for target resource reconciliation.

Figure 1-4 Reconciliation Rule for Target Resource Reconciliation



Reconciliation Rule Builder

Name: RSA AuthManager TokenRe

Object: RSA Auth Manager Token

Operator: ○ AND ● OR

☑ Valid

☑ Active

● For User ○ For Organization

Description: Token Recon Matching Rule

Rule Definition

Rule: RSA AuthManager TokenRecon
User Login Equals User ID

1.8.9 Reconciliation Action Rules for Token Target Resource Reconciliation

Table 1-8 lists the action rules for target resource reconciliation.

Table 1-8 Action Rules for Target Resource Reconciliation

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

Table 1-8 (Cont.) Action Rules for Target Resource Reconciliation

Rule Condition	Action
One Process Match Found	Establish Link

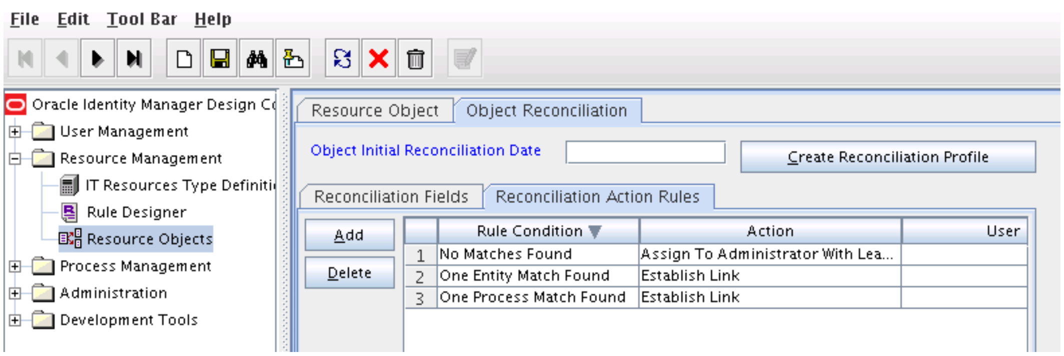
> **Note:**
>
> No action is performed for rule conditions that are not predefined for this connector. You can define your own action rule for such rule conditions. See the following topics in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*:
>
> - Setting a Reconciliation Action Rule (Developing Identity Connectors using Java)
> - Setting a Reconciliation Action Rule (Developing Identity Connectors using .net)

1.8.10 Viewing Reconciliation Action Rules for Token Target Resource Reconciliation

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 Token** 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 1-5 shows the reconciliation action rule for target resource reconciliation.

Figure 1-5 Reconciliation Action Rules for Target Resource Reconciliation



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

1.9 Connector Objects Used During Provisioning

Provisioning involves creating or modifying user data on the target system through Oracle Identity Manager.

> **See Also:**
>
> Managing Provisioning Tasks in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager* for conceptual information about provisioning

This section discusses the following topics:

- Provisioning Functions
- User Fields for Provisioning
- Token Fields for Provisioning

1.9.1 Provisioning Functions

The provisioning functions that are supported by the connector are listed in Table 1-9. The Adapter column gives the name of the adapter that is used when the function is performed.

Table 1-9 Provisioning Functions

Function	Adapter
Create User	adpRSAAMCREATEUSER
Update User	adpRSAAMUPDATEUSER
Delete User	adpRSAAMDELETEUSER
Enable User	adpRSAAMENABLEUSER
Disable User	adpRSAAMDISABLEUSER
Assign Token	adpRSAAMASSIGNTOKEN
Update Token	adpRSAAMUPDATETOKEN
Enable Token	adpRSAAMENABLETOKEN
Disable Token	adpRSAAMDISABLETOKEN
Unassign Token	adpRSAAMUNASSIGNTOKEN
Add Role	adpRSAAMADDROLE
Update Role	adpRSAAMUPDATEROLE
Remove Role	adpRSAAMREMOVEROLE
Add Group	adpRSAAMADDGROUP
Update Group	adpRSAAMUPDATEGROUP
Remove Group	adpRSAAMREMOVEGROUP

Table 1-9 (Cont.) Provisioning Functions

Function	Adapter
Prepopulate Adapter	adpRSAAMPREPOPULATEADAPTER
Multi Update	adpRSAAMMULTIUPDATE
Return Input Value	adpRSAAMRETURNINPUTVALUE

1.9.2 User Fields for Provisioning

The Lookup.RSAAM.UM.ProvAttrMap lookup definition maps process form fields with target system attributes. This lookup definition is used for performing user provisioning operations.

In this lookup definition, entries are in the following format:

- **Code Key:** Name of the process form field
- **Decode:** The value is in the following format:

  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 sets the values for this attribute. This method belongs to one of the following classes:
  - com.rsa.admin.data.PrincipalDTO
  - com.rsa.authmgr.admin.principalmgt.data.AMPrincipalDTO

  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 input type is specified in the Javadocs for the API.
- *DTO_ATTRIBUTE_NAME* is the name of the attribute in the PrincipalDTO or AMPrincipalDTO class.

Table 1-10 lists the user identity fields of the target system for which you can specify or modify values during provisioning operations.

Table 1-10 Entries in the Lookup.RSAAM.UM.ProvAttrMap lookup definition

Code	Decode
Account Expire Date[Date]	accountExpireDate;IMS;Core;Date;EXPIRATION_DATE
Account Expire Hours	AccountExpireHours
Account Expire Minutes	AccountExpireMinutes
Account Start Hours	AccountStartHours
Account Start Minutes	AccountStartMinutes
Account Start Date[Date]	accountStartDate;IMS;Core;Date;START_DATE
Certificate DN	certificateDN;IMS;Core;String;CERT_DN
Clear Incorrect Passcodes	clearBadPasscodes;AM;Core;boolean
Clear Windows Password	clearWindowsLoginPassword;AM;Core;boolean
Default Shell	defaultShell;AM;Core;String
First Name	firstName;IMS;Core;String;FIRST_NAME
Fixed Passcode	staticPassword;AM;Core;String
Fixed Passcode Allowed	staticPasswordSet;AM;Core;boolean
Identity Source[LOOKUP]	identitySourceGuid;IMS;Core;String;IDENTITY_SRC_ID
Last Name	lastName;IMS;Core;String;LAST_NAME
Middle Name	middleName;IMS;Core;String;MIDDLE_NAME
Password	_PASSWORD_
Radius Profile[LOOKUP]	radiusProfileGuid;AM;Core;String
Security Domain[LOOKUP]	securityDomainGuid;IMS;Core;String;OWNER_ID
UD_AMGROUP~GroupName[LOOKUP]	UserGroup
UD_AMROLE~RoleName[LOOKUP]	AdminRole
User GUID	_UID_
User ID	_NAME_

> **Note:**
>
> Incorrect Passcodes and Clear Windows passwords are one-time trigger actions used to clear passcodes and Windows password respectively. However, as a part of provisioning, these changed values will not reflect on the target system side prohibiting it from being reconciled to the Oracle Identity Manager server also.

1.9.3 Token Fields for Provisioning

The Lookup.RSAAM.Token.ProvAttrMap lookup definition maps process form fields with target system attributes. This lookup definition is used for performing token provisioning operations.

In this lookup definition, entries are in the following format:

- **Code Key:** Name of the process form field
- **Decode:** The value is in the following format:

  METHOD_NAME;API_NAME;ATTRIBUTE_TYPE;METHOD_INPUT_TYPE;*DTO_ATTRIBUTE_NAME*

In this format:

- *METHOD_NAME* is the name of the method on the target system that sets values for this attribute. This method belongs to the com.rsa.authmgr.admin.principalmgt.data.TokenDTO class.

  The `set` prefix of the method name is not included in the Decode value.
- *API_NAME* is `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_INPUT_TYPE* is the data type of the value returned 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 TokenDTO class.

Table 1-11 lists the token fields of the target system for which you can specify or modify values during provisioning operations.

Table 1-11 Entries in the Lookup.RSAAM.Token.ProvAttrMap lookup definition

Code	Decode
Notes	notes;TokenDTO;Core;String
Pin	_PASSWORD_
Token GUID	_UID_
Token Lost	tokenLost;TokenDTO;Core;Boloean
Token Serial Number[LOOKUP]	_NAME_
User GUID	principalId;TokenDTO;Core;String
User ID	assignedUser;ListTokenDTO;Core;String;principalId

1.10 Roadmap for Deploying and Using the Connector

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

- Deploying the RSA Authentication Manager Connector describes procedures that you must perform on Oracle Identity Manager and the target system during each stage of connector deployment.
- Using the RSA Authentication Manager Connector describes guidelines on using the connector and the procedure to configure reconciliation runs and perform provisioning operations.
- Extending the Functionality of the RSA Authentication Manager Connector describes procedures that you can perform if you want to extend the functionality of the connector.

1.6 Features of the Connector

The following are features of the connector:

- Support for Reconciliation and Provisioning of RSA Authentication Manager User Accounts and Tokens
- Full and Incremental Reconciliation
- Batched Reconciliation
- Limited (Filtered) Reconciliation
- Enable and Disable User Accounts and Tokens
- Reconciliation of Deleted User Accounts and Unassigned Tokens
- EJB-Based Communication with the Target System
- Standard and Custom Attribute Mapping for Reconciliation and Provisioning.
- Transformation and Validation of Account Data
- Support for Setting a PIN and the Token Lost Attribute
- Connection Pooling

1.6.1 Support for Reconciliation and Provisioning of RSA Authentication Manager User Accounts and Tokens

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

1.6.2 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 Full Reconciliation.

1.6.3 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 Batched Reconciliation.

1.6.4 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 Limited Reconciliation.

1.6.5 Enable and Disable User Accounts and Tokens

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.

Alternatively, you can search for and open the Accounts page on Oracle Identity Manager. Click **Enable/Disable** to enable or disable user accounts or tokens.

> **Note:**
>
> The Enabled or Disabled state of a user account or a token is not related to the Locked or Unlocked state of the account.

1.6.6 Reconciliation of Deleted User Accounts and Unassigned Tokens

You can configure the connector for reconciliation of deleted user accounts and unassigned tokens. In target resource mode, if a user record is deleted or a token is unassigned on the target system, then the corresponding RSA resource is revoked from the OIM User.

See Scheduled Jobs for Reconciliation of Deleted Token and User Records.

1.6.7 EJB-Based Communication with the Target System

The connector supports EJB-based communication between Oracle Identity Manager and the target system. This is a secure connection. By using the connectionType parameter of the IT Resource, you can specify the type of communication (EJB) to be established with the target system.

1.6.8 Standard and Custom Attribute Mapping 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 Extending the Functionality of the RSA Authentication Manager Connector.

1.6.9 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:

- Configuring Transformation of Data During Reconciliation
- Configuring Validation of Data During Reconciliation and Provisioning

1.6.10 Support for Setting a PIN and the Token Lost Attribute

You can use the connector to set the following:

- A PIN for the token that is assigned to a user.

  > **Note:**
  >
  > You are compulsorily required to assign a value for the PIN attribute of each token in order to ensure that provisioning takes place as expected.

- The Token Lost attribute when the token device is lost.

1.6.11 Connection Pooling

A connection pool is a cache of objects that represent physical connections to the target. Oracle Identity Manager connectors can use these connections to communicate with target systems. At run time, the application requests a connection from the pool. If a connection is available, then the connector uses it and then returns it to the pool. A connection returned to the pool can again be requested for and used by the connector for another operation. By enabling the reuse of connections, the connection pool helps reduce connection creation overheads like network latency, memory allocation, and authentication.

One connection pool is created for each IT resource. For example, if you have three IT resources for three installations of the target system, then three connection pools will be created, one for each target system installation.

See Setting up the Lookup Definition for Connection Pooling.

2

Deploying the RSA Authentication Manager Connector

The procedure to deploy the connector can be divided into the following stages:

- Preinstallation
- Installation
- Postinstallation
- About Upgrading the RSA Authentication Manager Connector
- Postcloning the RSA Authentication Manager Connector

2.1 Preinstallation

Before installing the connector, you must copy the external code files and create a target system account to perform all reconciliation and provisioning operations. This information is divided across the following sections:

- Copying the External Code Files
- Creating a Target System Account for Connector Operations

2.1.1 Copying the External Code Files

You must perform the following procedure to copy the external code files:

1. Create a directory named RSAAM-***RELEASE_NUMBER*** under the following directory:

   OIM_HOME/server/ConnectorDefaultDirectory/targetsystems-lib/

   For example, if you are using release 11.1.1.5.0 of this connector, then create a directory named RSAAM-11.1.1.5.0 in the *OIM_HOME*/server/ConnectorDefaultDirectory/targetsystems-lib/ directory.
2. Copy the third party libraries mentioned in the "Java API Library JAR Files" section of the *RSA Authentication Manager Developer's Guide* to the *OIM_HOME*/server/ConnectorDefaultDirectory/targetsystems-lib/RSAAM-***RELEASE_NUMBER*** directory.

2.1.2 Creating a Target System Account for Connector Operations

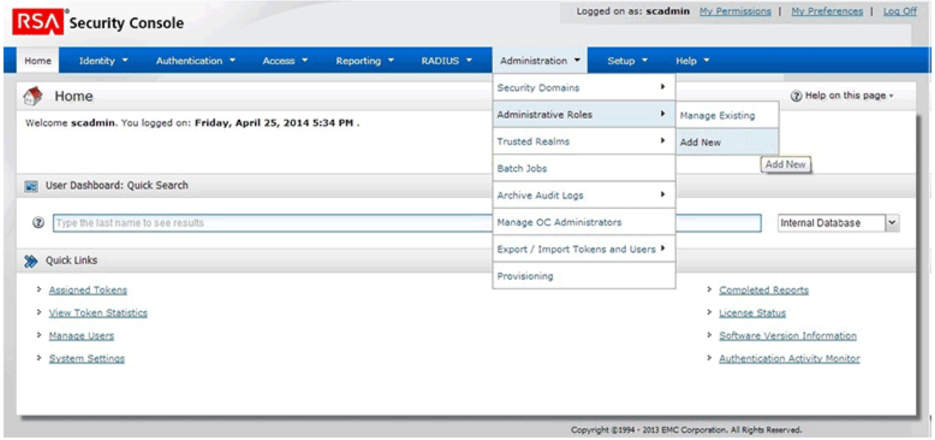
As a part of preinstallation, the connector uses a target system account to perform reconciliation and provisioning operations on the target system. To create this account, you must perform the following procedure:

1. Log in to the RSA Security Console.
2. If you want to assign administrative roles to end-users, then use the SuperAdminRole which is present by default in the target system, since only SuperAdminRole (and no custom role) can have permissions over all the administrative roles. If not, to create a role

having the minimum permissions required for connector operations, perform the following procedure:

a. Expand the **Administration** list, select **Administrative Roles**, and then select **Add New**.

   The following screenshot shows this page:



Welcome scadmin. You logged on: Friday, April 25, 2014 5:34 PM .

b. In the **Administrative Role Name** field, enter a name for the role.

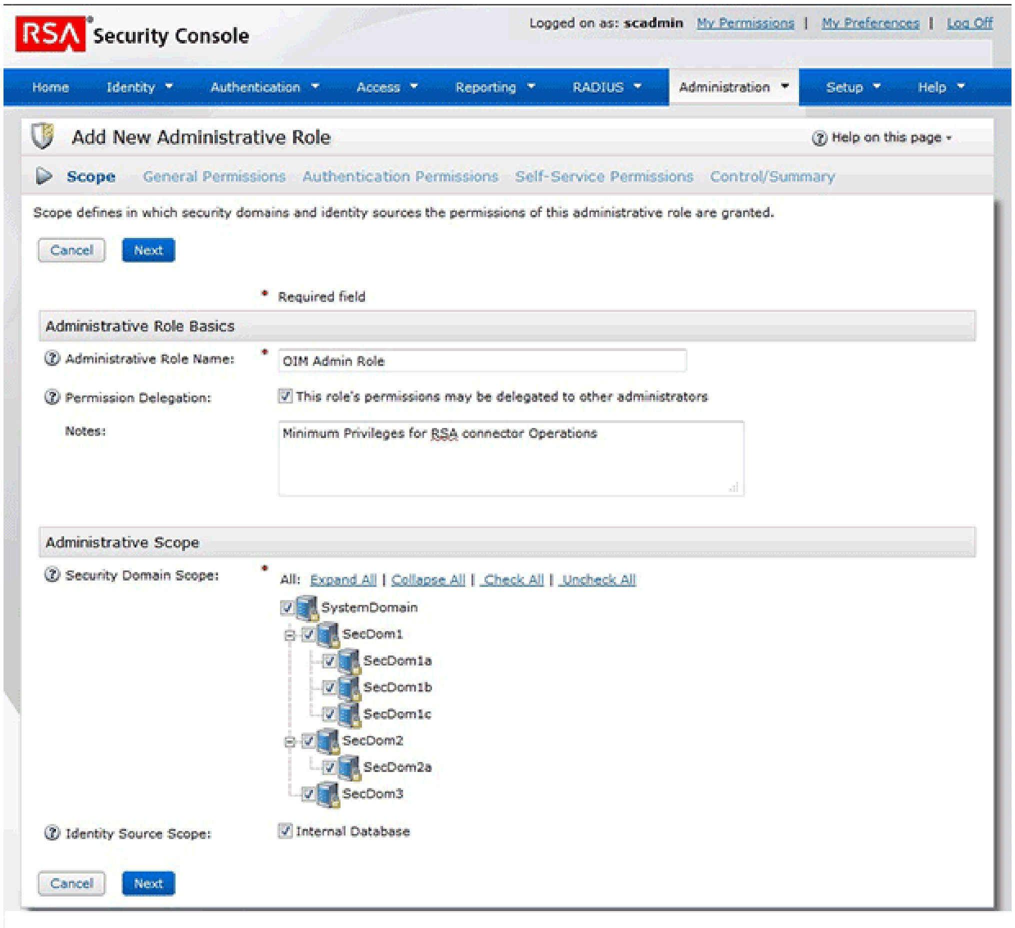
c. Select the **Permission Delegation** check box.

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.



Add New Administrative Role

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

* Required field

Administrative Role Basics

Administrative Role Name: * OIM Admin Role

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

Notes: Minimum Privileges for RSA connector Operations

Administrative Scope

Security Domain Scope: *

- ☑ SystemDomain
  - ☑ SecDom1
    - ☑ SecDom1a
    - ☑ SecDom1b
    - ☑ SecDom1c
  - ☑ SecDom2
    - ☑ SecDom2a
  - ☑ SecDom3

Identity Source Scope: ☑ Internal Database

f. Click **Next**.

g. In the Manager Policies region of the General Permissions page, select the **View** check box for the following permissions:

- Password Policies

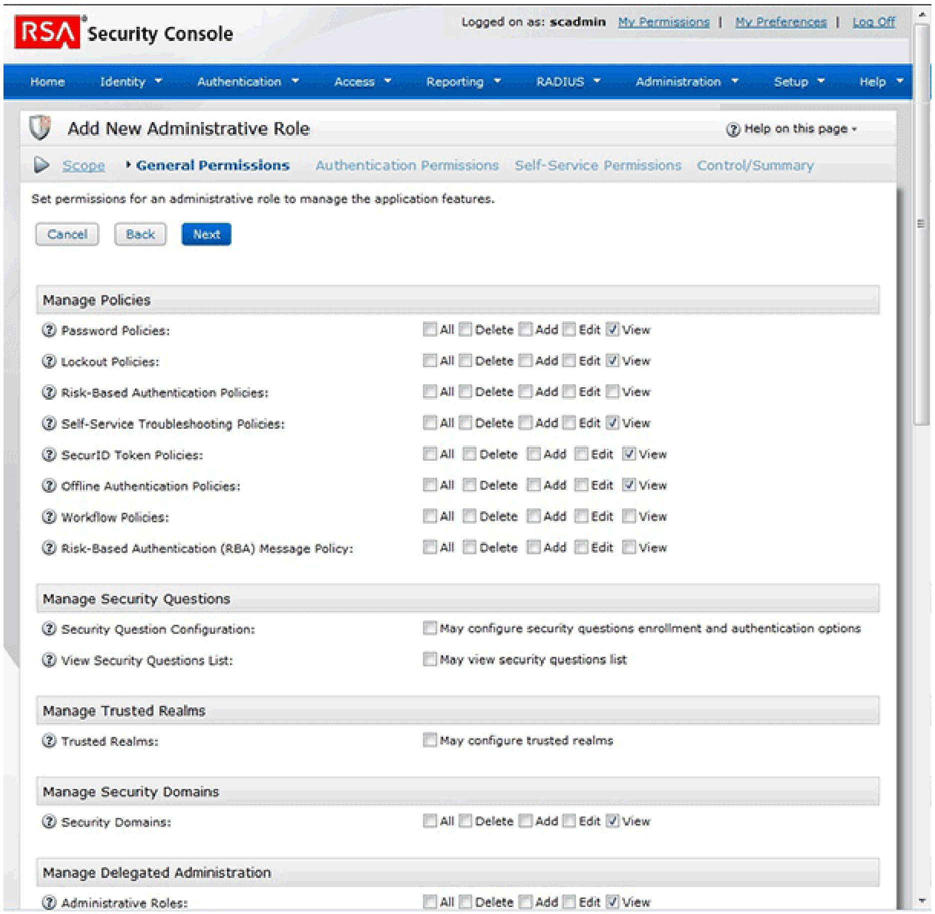
- Lockout Policies

- Self-Service Troubleshooting Policies

- SecurID Token Policies

- Offline Authentication Policies

h. In the Manage Security Domains region, select the **View** check box.



Add New Administrative Role

Set permissions for an administrative role to manage the application features.

Manage Policies

Password Policies: □ All □ Delete □ Add □ Edit ☑ View

Lockout Policies: □ All □ Delete □ Add □ Edit ☑ View

Risk-Based Authentication Policies: □ All □ Delete □ Add □ Edit □ View

Self-Service Troubleshooting Policies: □ All □ Delete □ Add □ Edit ☑ View

SecurID Token Policies: □ All □ Delete □ Add □ Edit ☑ View

Offline Authentication Policies: □ All □ Delete □ Add □ Edit ☑ View

Workflow Policies: □ All □ Delete □ Add □ Edit □ View

Risk-Based Authentication (RBA) Message Policy: □ All □ Delete □ Add □ Edit □ View

Manage Security Questions

Security Question Configuration: □ May configure security questions enrollment and authentication options

View Security Questions List: □ May view security questions list

Manage Trusted Realms

Trusted Realms: □ May configure trusted realms

Manage Security Domains

Security Domains: □ All □ Delete □ Add □ Edit ☑ View

Manage Delegated Administration

Administrative Roles: □ All □ Delete □ Add □ Edit ☑ View

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

- **View** check box for Administrative Roles

- Assign Administrative Roles check box

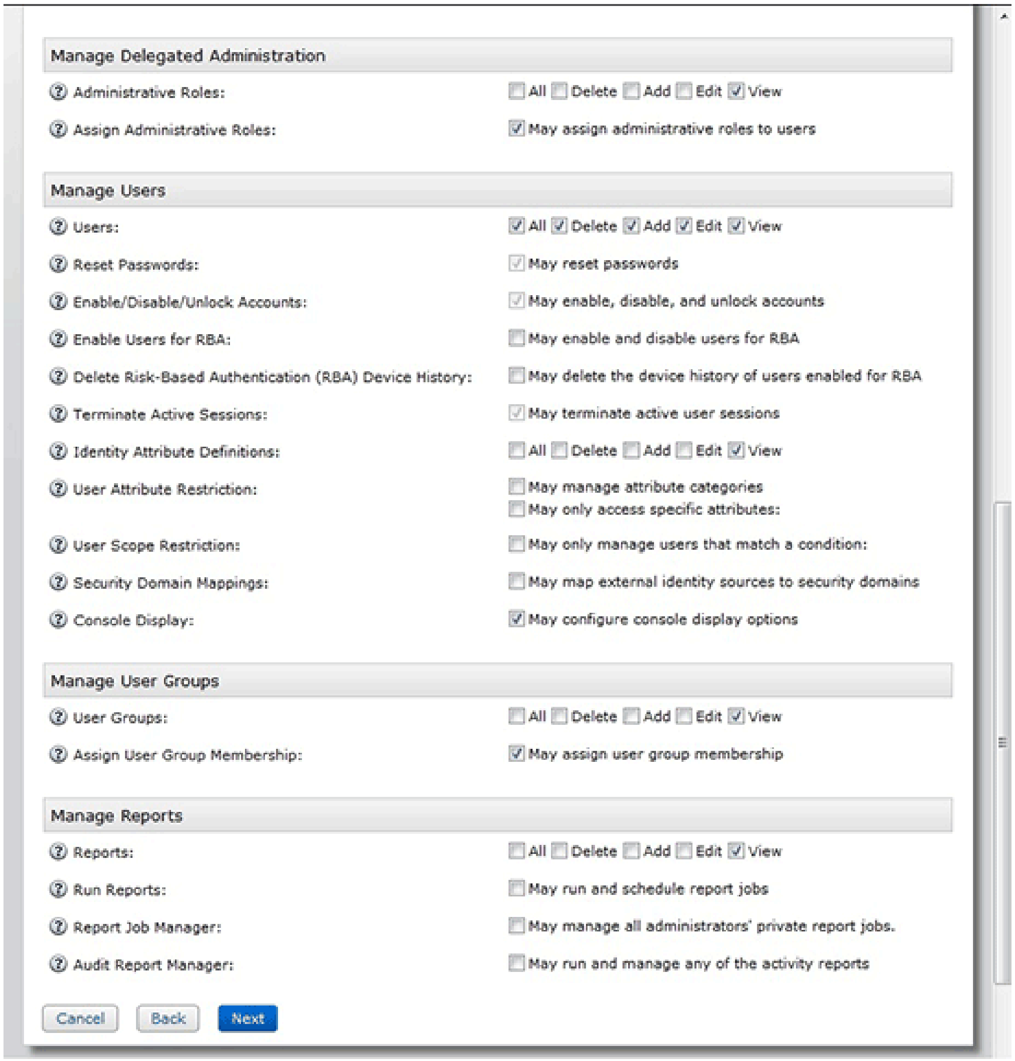
j. In the Manage Users region, select the following permissions:

- **All**, **Delete**, **Add**, **Edit**, and **View** check boxes for Users

- Console Display check box

k. In the Manage User Groups region, select the **View** and **Assign User Group Membership** check boxes.

l. In the Manage Reports region, select the **View** check box for the Reports permission.



Manage Delegated Administration

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/Unlock Accounts:	☑ May enable, disable, and unlock accounts
Enable Users for RBA:	□ May enable and disable users for RBA
Delete Risk-Based Authentication (RBA) Device History:	□ May delete the device history of users enabled for RBA
Terminate Active Sessions:	☑ May terminate active user sessions
Identity Attribute Definitions:	□ All □ Delete □ Add □ Edit ☑ View
User Attribute Restriction:	□ May manage attribute categories □ May only access specific attributes:
User Scope Restriction:	□ May only manage users that match a condition:
Security Domain Mappings:	□ May map external identity sources to security domains
Console Display:	☑ May configure console display options

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
Report Job Manager:	□ May manage all administrators' private report jobs.
Audit Report Manager:	□ May run and manage any of the activity reports

m. Click **Next**.

n. In the Manage RSA SecurID Tokens region of the Authentication Permissions page, select the following permissions:

   - **Edit** and **View** check boxes for SecurID Tokens

   - Assign Tokens

   - Distribute Software Tokens

   - **View** check box for Token Attribute Definitions

   - SecurID 800 Smart Card Details

o. In the Manage User Groups region, select the **View** check box for the User Group Restricted Access permission.

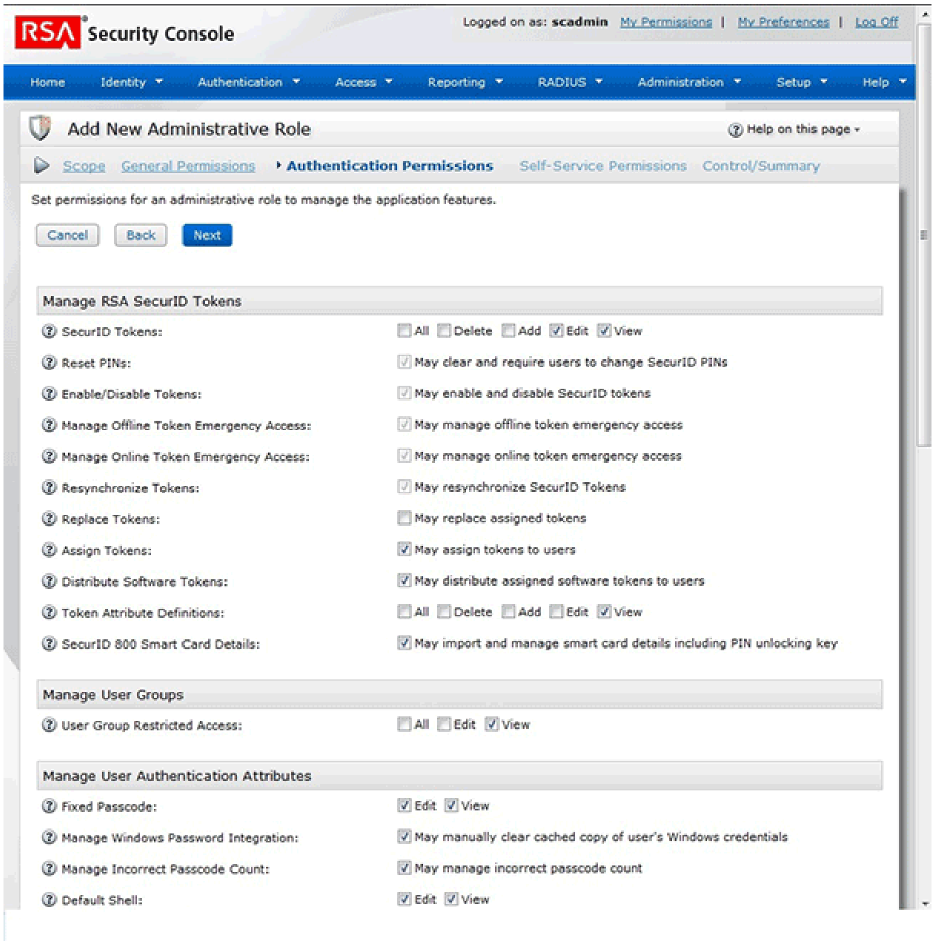
p. In the Manage User Authentication Attributes region, select the following permissions:

   - **Edit** and **View** check boxes for the Fixed Passcode

   - **Manage Windows Password Integration**

- **Manage Incorrect Password Count**

- Edit and **View** check boxes for the Default Shell permission



Add New Administrative Role

Set permissions for an administrative role to manage the application 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 Offline 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
SecurID 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

q. In the Manage Authentication Agents region, select the **View** check box for the Authentication Agent permission.

r. 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

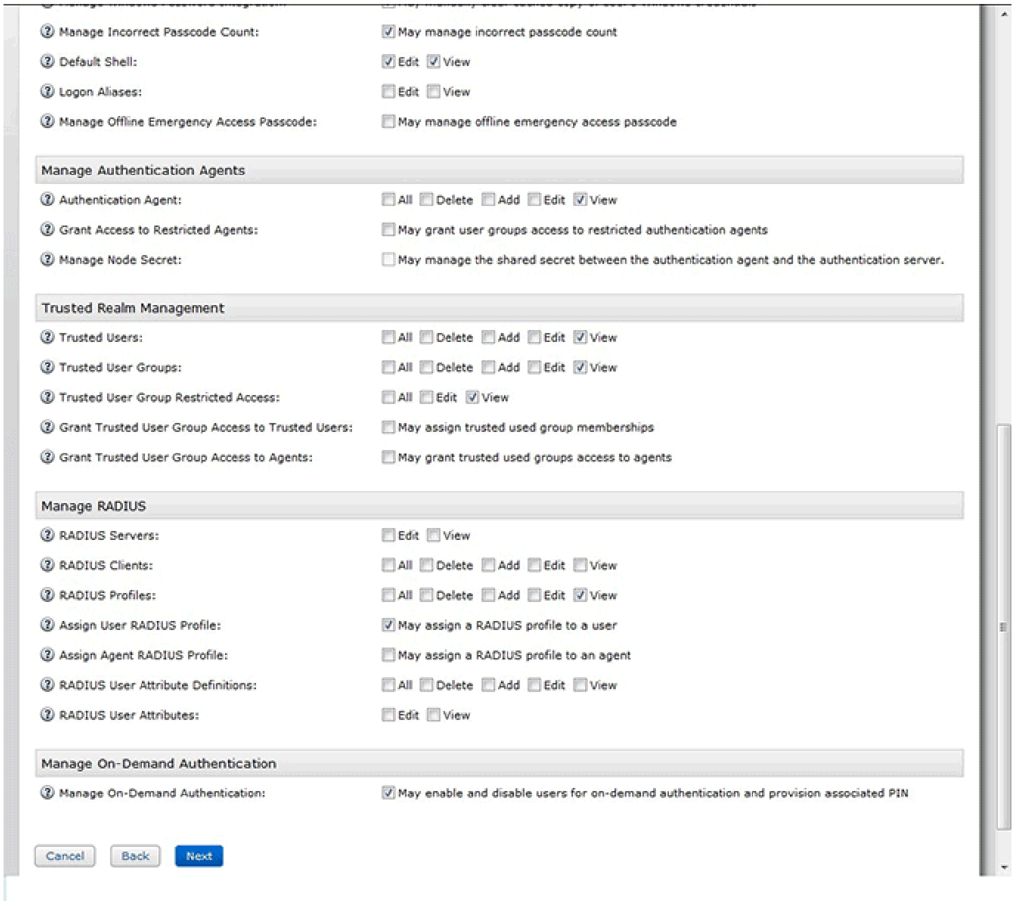
s. In the Manage RADIUS region, select following permissions:

- **View** check box for RADIUS Profiles

- Assign User RADIUS Profile check box

t. In the Manage On-Demand Authentication region, select the **Manage On-Demand Authentication** permission

u. Click **Next**.



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 server.

Trusted Realm Management

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: □ 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

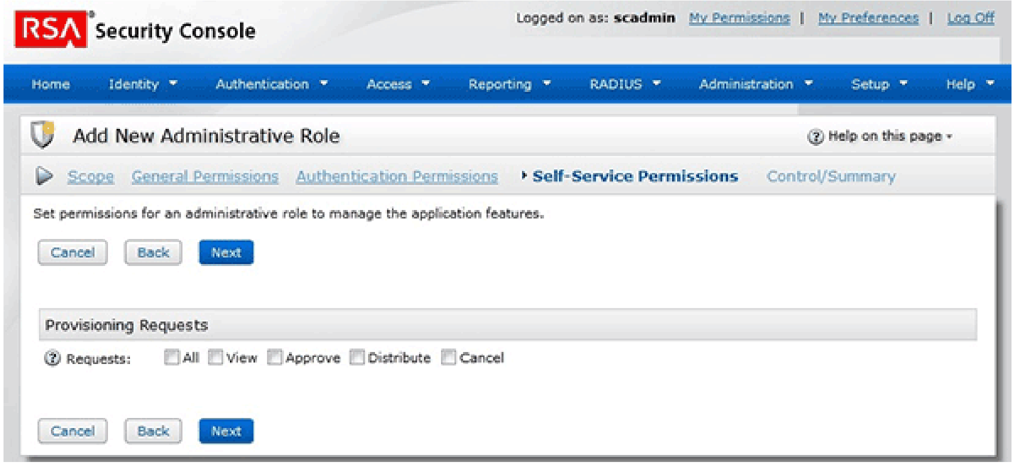
RADIUS User Attribute Definitions: □ All □ Delete □ Add □ Edit □ View

RADIUS User Attributes: □ Edit □ View

Manage On-Demand Authentication

Manage On-Demand Authentication: ☑ May enable and disable users for on-demand authentication and provision associated PIN

v. On the Self-Service Permissions page, in the Provisioning Requests region, click **Next**.



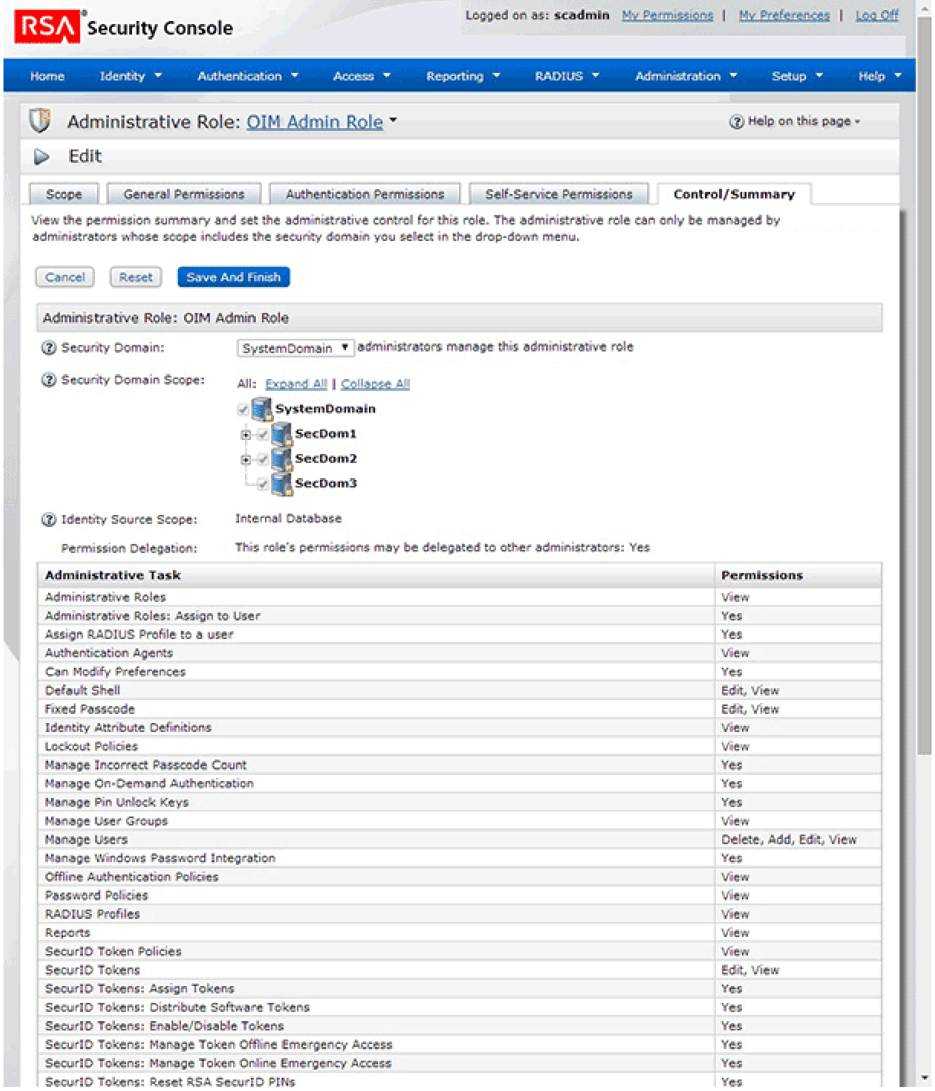
Add New Administrative Role

Set permissions for an administrative role to manage the application features.

Provisioning Requests

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

w. On the Control/Summary page, review the summary of permissions and then click **Save And Finish.**


RSA Security Console
Logged on as: scadmin My Permissions | My Preferences | Log Off
Home Identity Authentication Access Reporting RADIUS Administration Setup Help
Administrative Role: OIM Admin Role
Help on this page
Edit
Scope General Permissions Authentication Permissions Self-Service Permissions Control/Summary
Cancel Reset Save And Finish

View the permission summary and set the administrative control for this role. The administrative role can only be managed by administrators whose scope includes the security domain you select in the drop-down menu.

Administrative Role: OIM Admin Role

Security Domain: SystemDomain administrators manage this administrative role

Security Domain Scope: All: Expand All | Collapse All
- SystemDomain
  - SecDom1
  - SecDom2
  - SecDom3

Identity Source Scope: Internal Database

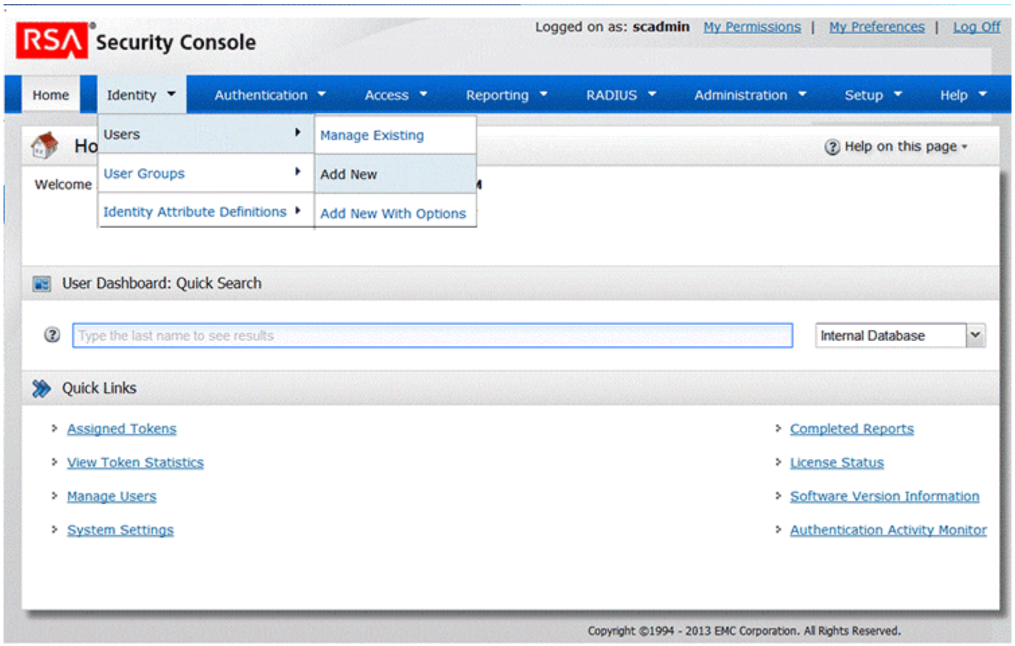
Permission Delegation: This role's permissions may be delegated to other administrators: Yes

Administrative Task	Permissions
Administrative Roles	View
Administrative Roles: Assign to User	Yes
Assign RADIUS Profile to a user	Yes
Authentication Agents	View
Can Modify Preferences	Yes
Default Shell	Edit, View
Fixed Passcode	Edit, View
Identity Attribute Definitions	View
Lockout Policies	View
Manage Incorrect Passcode Count	Yes
Manage On-Demand Authentication	Yes
Manage Pin Unlock Keys	Yes
Manage User Groups	View
Manage Users	Delete, Add, Edit, View
Manage Windows Password Integration	Yes
Offline Authentication Policies	View
Password Policies	View
RADIUS Profiles	View
Reports	View
SecurID Token Policies	View
SecurID Tokens	Edit, View
SecurID Tokens: Assign Tokens	Yes
SecurID Tokens: Distribute Software Tokens	Yes
SecurID Tokens: Enable/Disable Tokens	Yes
SecurID Tokens: Manage Token Offline Emergency Access	Yes
SecurID Tokens: Manage Token Online Emergency Access	Yes
SecurID Tokens: Reset RSA SecurID PINs	Yes

3. Create a user and assign the role to the user as follows:

   a. Expand the Identity list, select **Users**, and then select **Add New**.

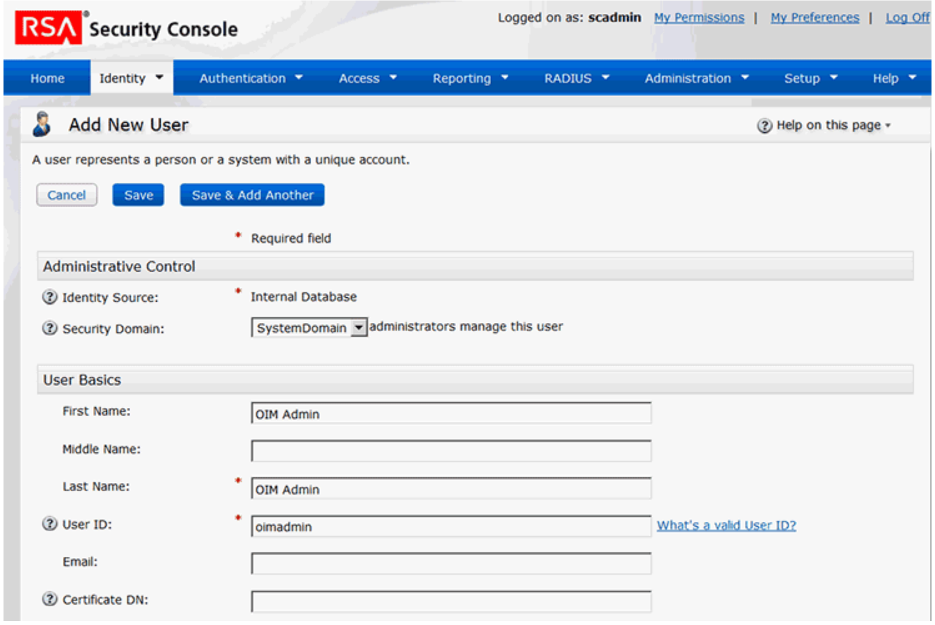
      The following screenshot shows this page:



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

> **Note:**
>
> The user ID and password that you enter on this page must be provided as the values of the Admin UserID and Admin Password IT resource parameters.
>
> 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.

* 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

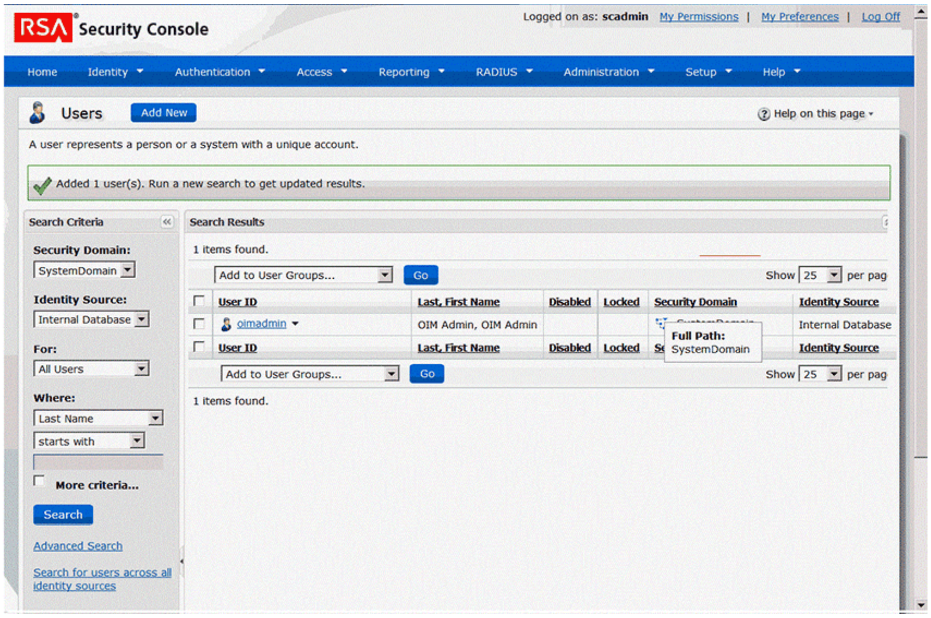
User ID: * oimadmin

Email:

Certificate DN:

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.

Added 1 user(s). Run a new search to get updated results.

Search Criteria

Security Domain: SystemDomain

Identity Source: Internal Database

For: All Users

Where: Last Name starts with

□ More criteria...

Search Results

1 items found.

Add to User Groups...

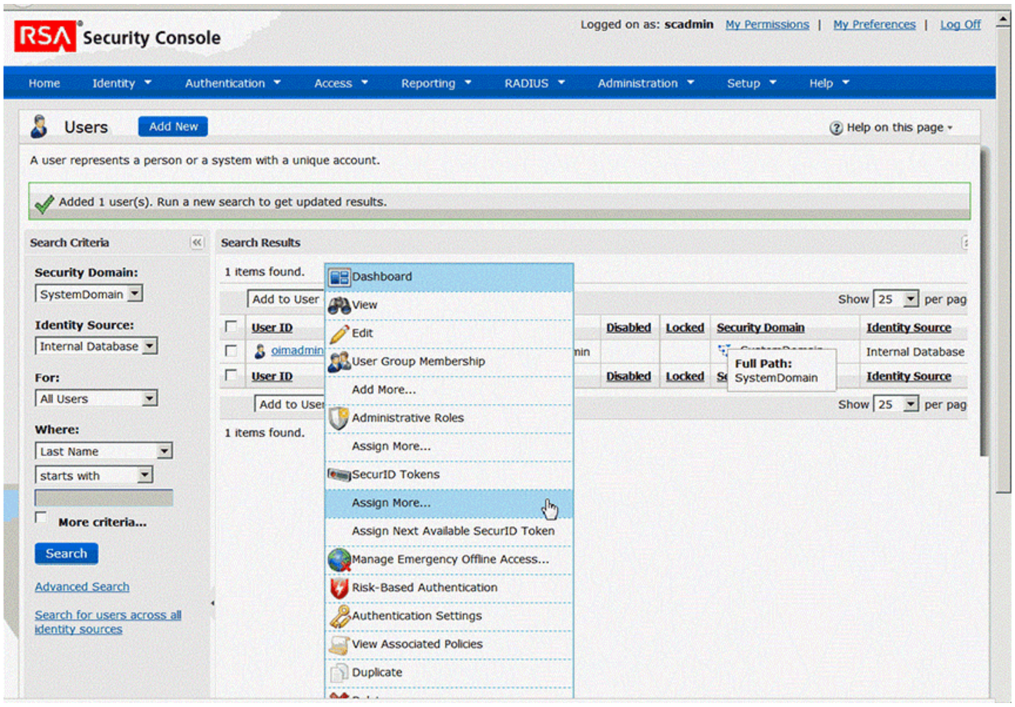
□	User ID	Last, First Name	Disabled	Locked	Security Domain	Identity Source
□	oimadmin	OIM Admin, OIM Admin			SystemDomain	Internal Database

Full Path: SystemDomain

1 items found.

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.

Added 1 user(s). Run a new search to get updated results.

Security Domain: SystemDomain

Identity Source: Internal Database

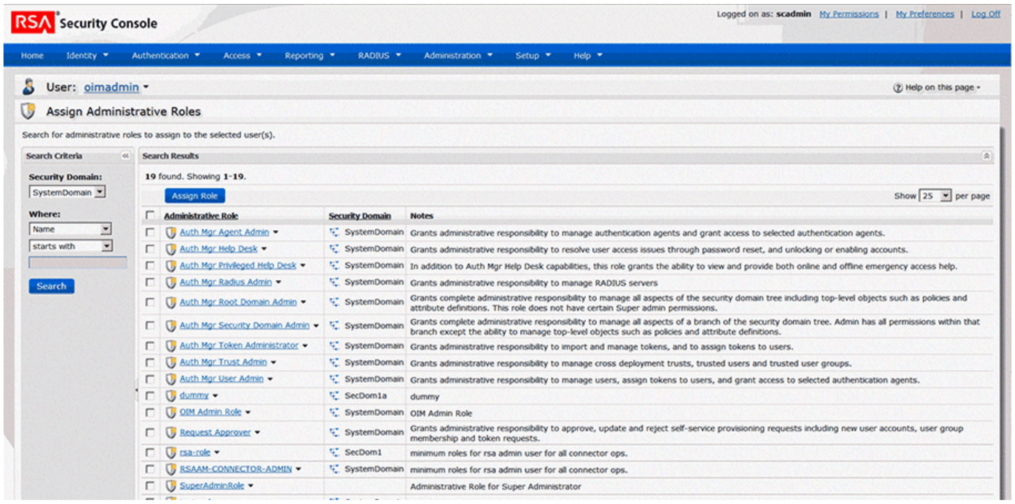
For: All Users

Where: Last Name, starts with

1 items found.

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:



User: oimadmin

Assign Administrative Roles

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

Security Domain: SystemDomain

Where: Name, starts with

19 found. Showing 1-19.

	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 Root Domain Admin	SystemDomain	Grants complete administrative responsibility to manage all aspects of the security domain tree including top-level objects such as policies and attribute definitions. This role does not have certain Super admin 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.
□	dummy	SecDom1a	dummy
□	OIM Admin Role	SystemDomain	OIM Admin Role
□	Request Approver	SystemDomain	Grants administrative responsibility to approve, update and reject self-service provisioning requests including new user accounts, user group membership and token requests.
□	rsa-role	SecDom1	minimum roles for rsa admin user for all connector ops.
□	RSAAM-CONNECTOR-ADMIN	SystemDomain	minimum roles for rsa admin user for all connector ops.
□	SuperAdminRole		Administrative Role for Super Administrator

2.2 Installation

You must install the RSA Authentication Manager connector in Oracle Identity Manager and in the Connector Server, as described in the following sections:

- Understanding Installation
- Installing the Connector in Oracle Identity Manager
- Deploying the Connector in a Connector Server

2.2.1 Understanding Installation

Depending on where you want to run the generated connector, the connector provides the following installation options:

- If you are using Oracle Identity Manager 11*g* Release 2 (11.1.2.0.0) and any later BP in this release track, then you must run the connector code remotely in a Connector Server. To do so, perform the procedures described in Installing the Connector in Oracle Identity Manager and Deploying the Connector in a Connector Server.
- If you are using Oracle Identity Manager 11*g* Release 2 PS1 (11.1.2.1.0) and any later BP in this release track, Oracle Identity Manager 11*g* Release 2 PS2 (11.1.2.2.0) and any later BP in this release track, or Oracle Identity Manager 11*g* Release 2 PS3 (11.1.2.3.0), depending on where you want to run the connector code (bundle), the connector provides the following installation options:
  - To run the connector code locally in Oracle Identity Manager, perform the procedure described in Installing the Connector in Oracle Identity Manager.
  - To run the connector code remotely in a Connector Server, perform the procedures described in Installing the Connector in Oracle Identity Manager and Deploying the Connector in a Connector Server.

2.2.2 Installing the Connector in Oracle Identity Manager

To install the connector on Oracle Identity Manager, you must run the installer and configure the IT Resource parameters as described in the following sections:

- Running the Connector Installer
- Configuring the IT Resource for the Target System

2.2.2.1 Running the Connector Installer

> **Note:**
>
> In this guide, the term **Connector Installer** has been used to refer to the Connector Installer feature of the Administrative and User Console.

To run the Connector Installer:

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

   OIM_HOME/server/ConnectorDefaultDirectory
2. Log in to Oracle Identity System Administration.
3. In the left pane, under System Management, click **Manage Connector.**
4. In the Manage Connector page, click **Install.**

5. From the Connector List list, select **RSAAM Connector *RELEASE_NUMBER.*** This list displays the names and release numbers of connectors whose installation files you copy into the default connector installation directory in Step 1.

   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 **RSAAM Connector *RELEASE_NUMBER.***

6. Click **Load**.

7. To start the installation process, click **Continue.**

   The following tasks are performed, in sequence:

   a. Configuration of connector libraries

   b. Import of the connector XML files (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 is displayed. Depending on the reason for the 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.

8. If all three tasks of the connector installation process are successful, then a message indicating successful installation is displayed. In addition, a list of steps that you must perform after the installation is displayed. These steps are as follows:

   a. Ensuring that the prerequisites for using the connector are addressed

   > **Note:**
   >
   > At this stage, run the Oracle Identity Manager PurgeCache utility to load the server cache with content from the connector resource bundle in order to view the list of prerequisites. SeeClearing 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

   The procedure to configure the IT resource is described later in this guide.

   c. Configuring the scheduled jobs

   The procedure to configure these scheduled jobs 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 Configuring the IT Resource for the Target System.

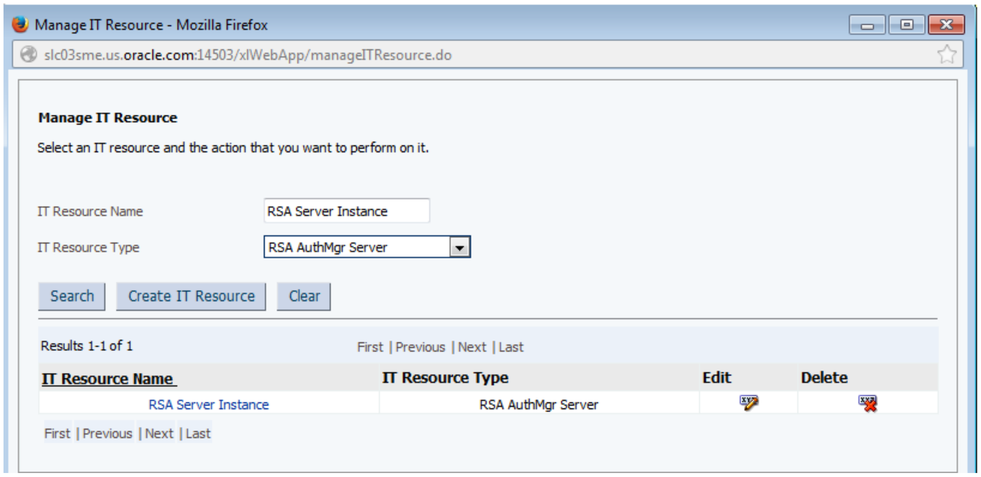
2.2.2.2 Configuring the IT Resource for the Target System

The IT resource for the target system is created during connector installation. This IT resource contains connection information about the target system. Oracle Identity Manager uses this information during reconciliation and provisioning.

You must specify values for the parameters of the RSA Server Instance IT resource as follows:

1. Log in to Oracle Identity System Administration.
2. In the left pane, under Configuration, click **IT Resource.**
3. In the IT Resource Name field on the Manage IT Resource page, enter `RSA Server Instance` and then click **Search**. Figure 2-1 shows the Manage IT Resource page.

Figure 2-1 Manage IT Resource Page


Manage IT Resource - Mozilla Firefox
slc03sme.us.oracle.com:14503/xlWebApp/manageITResource.do
Search
Create IT Resource
Clear
First | Previous | Next | Last

Manage IT Resource

Select an IT resource and the action that you want to perform on it.

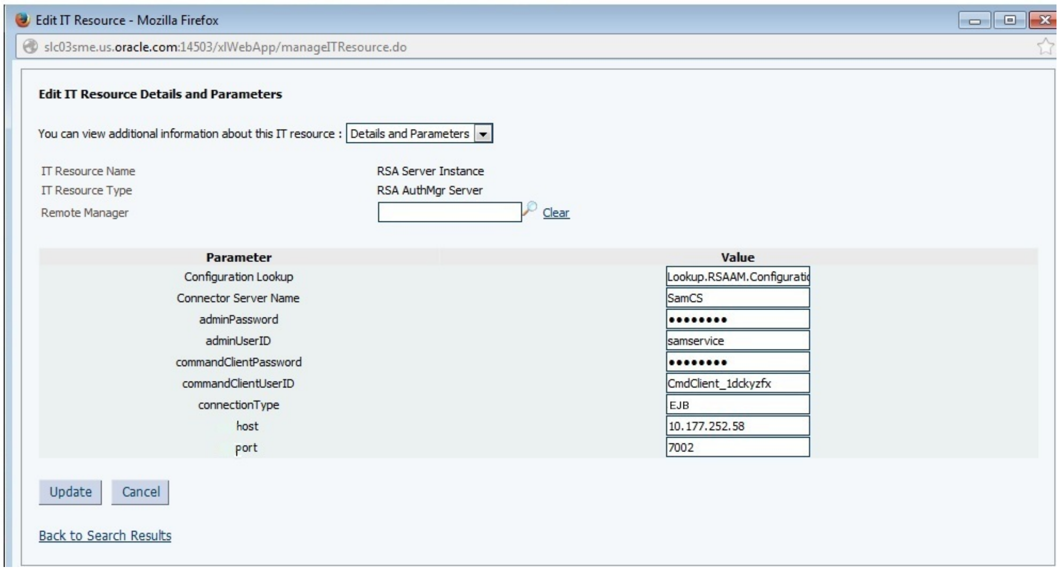
IT Resource Name	RSA Server Instance
IT Resource Type	RSA AuthMgr Server

Results 1-1 of 1

IT Resource Name	IT Resource Type	Edit	Delete
RSA Server Instance	RSA AuthMgr Server	✎	✗

4. Click the edit icon corresponding to the RSA Server Instance IT resource.
5. From the list at the top of the page, select **Details and Parameters**.
6. Specify values for the parameters of the RSA Server Instance IT resource. Figure 2-2 shows the Edit IT Resource Details and Parameters page.

Figure 2-2 Edit IT Resource Details and Parameters Page for the RSA Server Instance IT Resource


Edit IT Resource - Mozilla Firefox
slc03sme.us.oracle.com:14503/xlWebApp/manageITResource.do
Clear
Update
Cancel
Back to Search Results

Edit IT Resource Details and Parameters

You can view additional information about this IT resource : Details and Parameters

IT Resource Name	RSA Server Instance
IT Resource Type	RSA AuthMgr Server
Remote Manager	

Parameter	Value
Configuration Lookup	Lookup.RSAAM.Configurati
Connector Server Name	SamCS
adminPassword	••••••••
adminUserID	samservice
commandClientPassword	••••••••
commandClientUserID	CmdClient_1dckyzfx
connectionType	EJB
host	10.177.252.58
port	7002

The following list describes each parameter of the RSA Authentication Manager IT resource:

- adminPassword

  Enter the password of the target system user account that you create for connector operations.

- adminUserID

  Enter the user ID of the target system user account that you create for connector operations.

  See Creating a Target System Account for Connector Operations.

  commandClient Password

  Enter the command client password.

  Setting the command client user name and password is one of the tasks in the procedure mentioned in Addressing the Prerequisites for Using the Java API of RSA Authentication Manager.

- commandClient UserID

  Enter the command client user name.

  Setting the command client user name and password is one of the tasks in the procedure mentioned in Addressing the Prerequisites for Using the Java API of RSA Authentication Manager.

- Configuration Lookup

  This parameter holds the name of the configuration lookup definition.

  Default value: `Lookup.RSAAM.Configuration`

- Connector Server Name

This parameter holds the hostname of the machine where the connector server resides.

- host

  This parameter holds the hostname of the RSA target.

- port

  This parameter holds the port of the RSA target.

  Default value: `7002`

- connectionType

  This parameter specifies the type of connection to be used to connect to the target system.

  Default value: `EJB`

  Do not change this value.

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

2.2.3 Deploying the Connector in a Connector Server

You can deploy the RSA Authentication Manager connector either locally in Oracle Identity Manager or remotely in the Connector Server. A **connector server** is an application that enables remote execution of an Identity Connector, such as the RSA Authentication Manager connector.

This section discusses the following topics:

- About the Connector Server
- Installing and Configuring the Connector Server
- Installing the Connector on the Connector Server

2.2.3.1 About the Connector Server

You can deploy the RSA Authentication Manager connector either locally in Oracle Identity Manager or remotely in the Connector Server. A **connector server** is an application that enables remote execution of an Identity Connector, such as the RSA Authentication Manager connector.

> **Note:**
>
> To deploy the connector bundle remotely in a Connector Server, you must first deploy the connector in Oracle Identity Manager, as described in Installing the Connector in Oracle Identity Manager.

You can deploy the RSA Authentication Manager connector remotely in the Connector Server. A connector server is a Microsoft Windows application that enables remote execution of an Identity Connector. Connector servers are available in the following two implementations:

- As a .Net implementation that is used by Identity Connectors implemented in .Net

- As a Java Connector Server implementation that is used by Java-based Identity Connectors

The RSA Authentication Manager connector is implemented in Java, so you can deploy this connector to a Java Connector Server.

2.2.3.2 Installing and Configuring the Connector Server

Use the following steps to install and configure the Java Connector Server:

> **Note:**
>
> Before you deploy the Java Connector Server, ensure that you install the JDK or JRE on the same computer where you are installing the Java Connector Server and that your *JAVA_HOME* or *JRE_HOME* environment variable points to this installation.

1. Create a new directory on the computer where you want to install the Java Connector Server.

   > **Note:**
   >
   > In this guide, *CONNECTOR_SERVER_HOME* represents this directory.

2. Unzip the Java Connector Server package in the new directory created in Step 1. You can download the Java Connector Server package from the Oracle Technology Network.
3. Open the ConnectorServer.properties file located in the `conf` directory. In the ConnectorServer.properties file, set the following properties, as required by your deployment.

Property	Description
connectorserver.port	Port on which the Java Connector Server listens for requests. Default is `8763`.
connectorserver.bundleDir	Directory where the connector bundles are deployed. Default is `bundles`.
connectorserver.libDir	Directory in which to place dependent libraries. Default is `lib`.
connectorserver.usessl	If set to **`true`**, the Java Connector Server uses SSL for secure communication. Default is `false`. If you specify **`true`**, use the following options on the command line when you start the Java Connector Server: • `-Djavax.net.ssl.keyStore` • `-Djavax.net.ssl.keyStoreType` (*optional*) • `-Djavax.net.ssl.keyStorePassword`
connectorserver.ifaddress	Bind address. To set this property, uncomment it in the file (if necessary). The bind address can be useful if there are more NICs installed on the computer.

Property	Description
connectorserver.key	Java Connector Server key.

4. Set the properties in the ConnectorServer.properties file, as follows:
   - To set the connectorserver.key, run the Java Connector Server with the `/setKey` option.

     > **Note:**
     >
     > See Running the Connector Server.

   - For all other properties, edit the ConnectorServer.properties file manually.
5. The conf directory also contains the logging.properties file, which you can edit if required by your deployment.

> **Note:**
>
> Oracle Identity Manager has no built-in support for connector servers, so you cannot test your configuration.

2.2.3.3 Running the Connector Server

To run the Java Connector Server, use the ConnectorServer.bat script for Windows and use the ConnectorServer.sh script for UNIX as follows:

1. Make sure that you have set the properties required by your deployment in the ConnectorServer.properties file, as described in Running the Connector Server.
2. Make sure that you have set the JAVA_HOME and the PATH to the java used by Oracle Identity Manager.
3. Change to the *CONNECTOR_SERVER_HOME*\bin directory and find the ConnectorServer.bat script.

   The ConnectorServer.bat supports the following options:

Option	Description
/install [*serviceName*] ["-J *java-option*"]	Installs the Java Connector Server as a Windows service. Optionally, you can specify a service name and Java options. If you do not specify a service name, the default name is `ConnectorServerJava`.
/run ["-J *java-option*"]	Runs the Java Connector Server from the console. Optionally, you can specify Java options. For example, to run the Java Connector Server with SSL: ConnectorServer.bat /run "-J-Djavax.net.ssl.keyStore=mykeystore.jks" "-J-Djavax.net.ssl.keyStorePassword=***password***"

Option	Description
`/setKey [key]`	Sets the Java Connector Server key. The `ConnectorServer.bat` script stores the hashed value of the key in the `connectorserver.key` property in the `ConnectorServer.properties` file.
`/uninstall [serviceName]`	Uninstalls the Java Connector Server. If you do not specify a service name, the script uninstalls the `ConnectorServerJava` service.

4. If you need to stop the Java Connector Server, stop the respective Windows service.

2.2.3.4 Installing the Connector on the Connector Server

See Also:

Using an Identity Connector Server in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for information about installing and configuring connector server and running the connector server

If you need to deploy the RSA Authentication Manager into the Java Connector Server, then follow these steps:

1. Stop the Java Connector Server.

   Note:

   - You can download the necessary Java Connector Server from the Oracle Technology Network web page.
   - Ensure that you are using latest framework JARs of Oracle Identity Manager to keep the Connector Server consistent with your Oracle Identity Manager instance. To do so:

     Copy the framework JAR files, connector-framework.jar and connector-framework-internal.jar, from the *OIM_HOME*/server/ext/internal directory to the *CONNECTOR_SERVER_HOME*/lib/framework directory.

2. Copy the connector bundle JAR file (org.identityconnectors.rsaam-1.0.1115.jar) from the installation media into the Java Connector Server *CONNECTOR_SERVER_HOME*/ bundles directory.
3. Copy the files listed in Table A-1 into the *CONNECTOR_SERVER_HOME*/lib directory:
4. Start the Java Connector Server.

Note:

Use the following command line to start the Connector Server for EJB request:

```
-J-Dweblogic.security.SSL.trustedCAKeyStore=//scratch/OIM/
wlserver_10.3/server/lib/cacerts
```

2.3 Postinstallation

After successfully installing the connector, you must configure Oracle Identity Manager and create an IT Resource for the connector server. The following sections contain detailed information:

- Postinstallation on Oracle Identity Manager
- Creating the IT Resource for the Connector Server

2.3.1 Postinstallation on Oracle Identity Manager

Configuring the Oracle Identity Manager involves performing multiple operations. These operations are discussed in detail in the following procedures:

- Configuring Self-Request Provisioning
- Configuring Oracle Identity Manager
- Clearing Content Related to Connector Resource Bundles from the Server Cache
- Managing Logging for RSA Authentication Manager Connector
- Setting up the Lookup Definition for Connection Pooling
- Setting up the Lookup Definition for Different Time Zones
- Localizing Field Labels in UI Forms
- Addressing Prerequisites for Using the Java API of RSA Authentication Manager

2.3.1.1 Configuring Self-Request Provisioning

To configure self-request provisioning, perform the following procedure:

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 form.
4. Double-click the **Create User** process task.
5. Open the Responses tab and select **SUCCESS.**

   The Copy the UID task is displayed at the bottom of the same page.
6. Delete the **Copy the UID** task under the Task To Generate entry by selecting the delete option.
7. Click **Save.**

2.3.1.2 Configuring Oracle Identity Manager

You must create additional metadata such as a UI form and an application instance, and must run entitlement and catalog synchronization jobs. In addition, you must tag some of the fields in the OIM User process form. These procedures are described in the following sections:

> **Note:**
>
> The procedure mentioned in the following sections have to performed for RSA Auth Manager User resource object and RSA Auth Manager Token resource object.

- Creating and Activating a Sandbox
- Creating a New UI Form
- Creating an Application Instance
- Upgrading User Form in Oracle Identity Manager
- Publishing a Sandbox
- Harvesting Entitlements and Sync Catalog
- Updating an Existing Application Instance with a New Form

2.3.1.2.1 Creating and Activating a Sandbox

You must create and activate a sandbox to begin using the customization and form management features. You can then publish the sandbox to make the customizations available to other users.

See Creating a Sandbox and Activating and Deactivating a Sandbox in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager.*

2.3.1.2.2 Creating a New UI Form

Create a new UI form as follows:

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

2.3.1.2.3 Creating an Application Instance

Create an application instance as follows:

1. In the System Administration page, under Configuration in the left pane, click **Application Instances**.
2. Under Search Results, click **Create.**
3. Enter appropriate values for the fields displayed on the Attributes form and click **Save.**

4. In the Form drop-down list, select the newly created form and click **Apply.**
5. Publish the application instance to an organization to make the application instance available for requesting and subsequent provisioning to users. See Publishing an Application Instance to Organizations in *Oracle Fusion Middleware Administering Oracle Identity Manager*.

2.3.1.2.4 Upgrading User Form in Oracle Identity Manager

This connector creates a new OIM user attribute (UDF) RSAAM User GUID. Although this user attribute (UDF) is added to a new User Form version, the User Form from the old version is only used for all operations. To use the latest form version which contains the GUID field, you must customize the associated pages on the interface to upgrade to the latest User Form and add the custom form fields. To do so, perform the following procedure:

1. Log in to Oracle Identity System Administration.
2. From the Upgrade region, click **Upgrade User Form.** The RSAAM User GUID UDF is listed.
3. Click **Upgrade.**

> **See Also:**
>
> Configuring Custom Attributes in *Oracle Fusion Middleware Administering Oracle Identity Manager*

2.3.1.2.5 Publishing a Sandbox

To publish the sandbox that you created in Creating and Activating a Sandbox:

1. Close all the open tabs and pages.
2. From the table showing the available sandboxes in the Manage Sandboxes page, select the sandbox that you created in Creating and Activating a Sandbox.
3. On the toolbar, click **Publish Sandbox.** A message is displayed asking for confirmation.
4. Click **Yes** to confirm. The sandbox is published and the customizations it contained are merged with the main line.

2.3.1.2.6 Harvesting Entitlements and Sync Catalog

To harvest entitlements and sync catalog:

1. Run the scheduled jobs for lookup field synchronization listed in Scheduled Job for Lookup Field Synchronization.
2. Run the Entitlement List scheduled job to populate Entitlement Assignment schema from child process form table.
3. Run the Catalog Synchronization Job scheduled job.

> **See Also:**
>
> Predefined Scheduled Tasks in *Oracle Fusion Middleware Administering Oracle Identity Manager*

2.3.1.2.7 Updating an Existing Application Instance with a New Form

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

1. Create a sandbox and activate it. See Creating a Sandbox and Activating and Deactivating a Sandbox in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.
2. Create a new UI form for the resource. See Creating Forms By Using the Form Designer in *Oracle Fusion Middleware Administering Oracle Identity Manager*.
3. Open the existing application instance.
4. In the **Form** field, select the new UI form that you created.
5. Save the application instance.
6. Publish the sandbox. See Publishing a Sandbox in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.

2.3.1.3 Clearing Content Related to Connector Resource Bundles from the Server Cache

When you deploy the connector, the resource bundles are copied from the resources directory on the installation media into the Oracle Identity Manager database. 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, 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:
   >
   > ```
   > 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
> ```

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.

2.3.1.4 Managing Logging for RSA Authentication Manager Connector

You can set a log level based on Oracle Java Diagnostic Logging and enable logging in the Oracle WebLogic Server. The following sections contain detailed information:

- Understanding Log Levels
- Enabling Logging

2.3.1.4.1 Understanding Log Levels

Oracle Identity Manager uses Oracle Java Diagnostic Logging (OJDL) for logging. OJDL is based on java.util.logger. To specify the type of event for which you want logging to take place, you can set the logs to one of the following available levels:

- 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 2-1.

Table 2-1 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.

2.3.1.4.2 Enabling Logging

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='rsaam-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="ORG.IDENTITYCONNECTORS.RSAAM" level="[LOG_LEVEL]"
useParentHandlers="false">
     <handler name="rsaam-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 2-1 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 specific to connector operations to be recorded.

   The following blocks show sample values for **`[LOG_LEVEL]`** and **`[FILE_NAME]`** :

```
<log_handler name='rsaam-handler' level='NOTIFICATION:1'
class='oracle.core.ojdl.logging.ODLHandlerFactory'>
<property name='logreader:' value='off'/>
     <property name='path' value=/scratch/RSA/Logs/RSA.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="ORG.IDENTITYCONNECTORS.RSAAM" level="NOTIFICATION:1"
useParentHandlers="false">
     <handler name="rsaam-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.

2.3.1.5 Setting up the Lookup Definition for Connection Pooling

Connection pooling allows reuse of physical connections and reduced overhead for your application. This procedure of setting up the lookup definition for connector pooling can be divided into the following sections:

- Understanding Connection Pooling Properties
- Adding Connection Pooling Properties

2.3.1.5.1 Understanding Connection Pooling Properties

By default, this connector uses the ICF connection pooling. Connection Pooling Properties lists the connection pooling properties, their description, and default values set in ICF:

Table 2-2 Connection Pooling Properties

Property	Description
Pool Max Idle	Maximum number of idle objects in a pool. Default value: `10`
Pool Max Size	Maximum number of connections that the pool can create. Default value: `10`
Pool Max Wait	Maximum time, in milliseconds, the pool must wait for a free object to make itself available to be consumed for an operation. Default value: `150000`
Pool Min Evict Idle Time	Minimum time, in milliseconds, the connector must wait before evicting an idle object. Default value: `120000`
Pool Min Idle	Minimum number of idle objects in a pool. Default value: `1`

2.3.1.5.2 Adding Connection Pooling Properties

If you want to add the connection pooling properties to use values that suit requirements in your environment, then:

1. Log in to the Design Console.
2. Expand **Administration,** and then double-click **Lookup Definition.**
3. Search for and open the Lookup.RSAAM.Configuration lookup definition.
4. On the Lookup Code Information tab, click **Add.**

   A new row is added.
5. In the **Code Key** column of the new row, enter `Pool Max Idle`.
6. In the **Decode** column of the new row, enter a value corresponding to the Pool Max Idle property.
7. Repeat Steps 4 through 6 for adding each of the connection pooling properties listed in Table 2-2.
8. Click the Save icon.

2.3.1.6 Setting up the Lookup Definition for Different Time Zones

Based on your requirement, the time zone property can be configured to define the time zone in which connector operations are performed. This information can be divided into the following sections:

- Time Zone Properties

- Setting up the Time Zone Properties

> **Note:**
>
> Perform the following procedure only if Oracle Identity Manager and RSA Authentication Manger are in different time zones.

2.3.1.6.1 Time Zone Properties

Table 2-3 lists the time zone properties, their code and decode values along with respective descriptions:

Table 2-3 Time Zone Properties

Code Key	Decode	Description
sourceTimeZone	For the decode value, refer the format of the timeZone present in the following URL: `http://docs.oracle.com/javase/1.5.0/docs/api/java/util/TimeZone.html`	This entry is not present by default, and has to be added only if Oracle Identity Manager and RSA Authentication Manger are in different time zones. If this entry is not defined, then the connector retrieves the default time zone from the location where the connector is running (can be either from the Oracle Identity Manager server or the connector server).
targetTimeZone	For the decode value, refer the format of the timeZone present in the following URL: `http://docs.oracle.com/javase/1.5.0/docs/api/java/util/TimeZone.html`	This entry is not present by default, and has to be added only if Oracle Identity Manager and RSA Authentication Manger are in different time zones. If this entry is not defined, then the connector retrieves the default time zone from the location where the connector is running (can be either from the Oracle Identity Manager server or the connector server).

2.3.1.6.2 Setting up the Time Zone Properties

Perform the following procedure only if Oracle Identity Manager and RSA Authentication Manger are in different time zones. To specify the time zone properties:

1. Log in to the Design Console.
2. Expand **Administration,** and then double-click **Lookup Definition.**
3. Search for and open the Lookup.RSAAM.Configuration lookup definition.
4. On the Lookup Code Information tab, click **Add.**

   A new row is added.
5. In the **Code Key** column of the new row, enter `sourceTimeZone`.
6. In the **Decode** column of the new row, enter the value from the URL mentioned in Table 2-3.

7. Repeat Steps 4 through 6 for adding the `targetTimeZone` property.
8. Click the Save icon.

2.3.1.7 Localizing Field Labels in UI Forms

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

1. Log in to Oracle Enterprise Manager.
2. In the left pane, expand **Application Deployments** and then select **oracle.iam.console.identity.sysadmin.ear.**
3. In the right pane, from the Application Deployment list, select **MDS Configuration.**
4. On the MDS Configuration page, click **Export** and save the archive to the local computer.
5. Extract the contents of the archive, and open one of the following files in a text editor:
   - For Oracle Identity Manager 11*g* Release 2 PS2 (11.1.2.2.0) and later:

     SAVED_LOCATION\xliffBundles\oracle\iam\ui\runtime\BizEditorBundle_en.xlf
   - For releases prior to Oracle Identity Manager 11*g* Release 2 PS2 (11.1.2.2.0):

     SAVED_LOCATION\xliffBundles\oracle\iam\ui\runtime\BizEditorBundle.xlf
6. Edit the BizEditorBundle.xlf file in the following manner:
   a. Search for the following text:

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

   b. Replace with the following text:

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

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

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

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

      ```
      <trans-unit id="$
      {adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBundle']
      ['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO.UD_AMU
      SER_FIRST_NAME__c_description']}">
      <source>First Name</source>
      <target/>
      </trans-unit>
      <trans-unit
      id="sessiondef.oracle.iam.ui.runtime.form.model.RSAForm.entity.RSAFormEO.UD_AMU
      SER_FIRST_NAME__c_LABEL">
      <source>First Name</source>
      <target/>
      </trans-unit>
      ```

d. Open the resource file from the connector package, for example RSA-AuthManager_ja.properties, and get the value of the attribute from the file, for example, global.udf.UD_AMUSER_FIRST_NAME=\u540D.

e. Replace the original code shown in Step 6.c with the following:

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

f. Repeat Steps 6.a through 6.d for all attributes of the process form.

g. Save the file as BizEditorBundle_*LANG_CODE*.xlf. In this file name, replace *LANG_CODE* with the code of the language to which you are localizing.

Sample file name: BizEditorBundle_ja.xlf.

7. Repackage the ZIP file and import it into MDS.

> **See Also:**
>
> Deploying and Undeploying Customizations in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for more information about exporting and importing metadata files

8. Log out of and log in to Oracle Identity Manager.

2.3.1.8 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:

- Required Java System Properties
- Exporting and Importing the Server Root Certificate
- Setting the Command Client User Name and Password

2.3.1.8.1 Required Java System Properties

Perform the procedure described in the "Required Java System Properties" section of the *RSA Authentication Manager Developer's Guide.*

2.3.1.8.2 Exporting and Importing the Server Root Certificate

To export and then import the server root certificate:

1. To export the certificate from RSA Authentication Manager, perform the procedure described in the "Making the RSA Root Certificate Available for API Clients (Java)" section of the *RSA Authentication Manager Developer's Guide.*
2. To import the certificate exported in Step 1 into your Application Server (IBM Websphere, JBoss or Oracle Weblogic), follow the procedure described in the "Import the Server Root Certificate" section of the *RSA Authentication Manager Developer's Guide.* Import the certificate into the same keystore defined by the Java property in the previous section depending upon the type of connection with the target system.

2.3.1.8.3 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 Developer's Guide.*

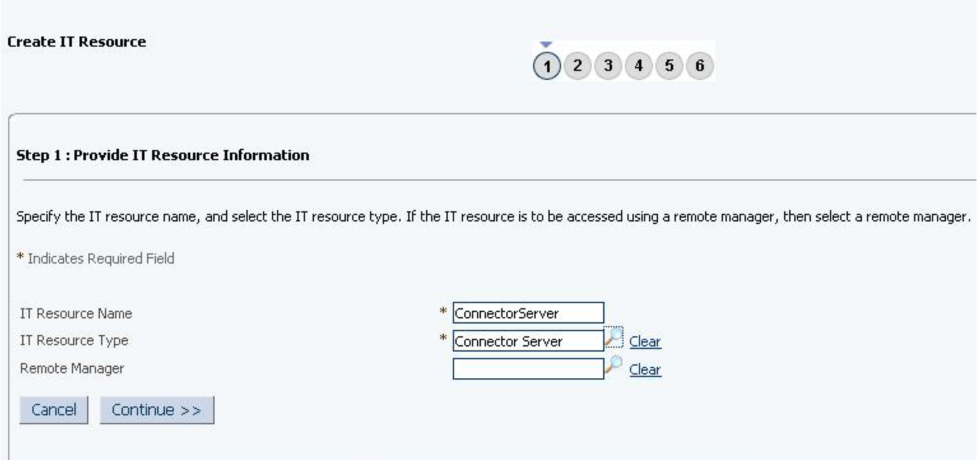
2.3.2 Creating the IT Resource for the Connector Server

> **Note:**
>
> Perform the procedure described in this section *only* if you have deployed the connector bundle remotely in a Connector Server.

To create the IT resource for the Connector Server:

1. Log in to Oracle Identity System Administration.
2. In the left pane, under Configuration, click **IT Resource.**
3. In the Manage IT Resource page, click **Create IT Resource.**
4. On the Step 1: Provide IT Resource Information page, perform the following steps:
   - **IT Resource Name**: Enter a name for the IT resource.
   - **IT Resource Type**: Select **Connector Server** from the IT Resource Type list.
   - **Remote Manager**: Do not enter a value in this field.
5. Click **Continue**. Figure 2-3 shows the IT resource values added on the Create IT Resource page.

Figure 2-3 Step 1: Provide IT Resource Information



Create IT Resource

Step 1 : Provide IT Resource Information

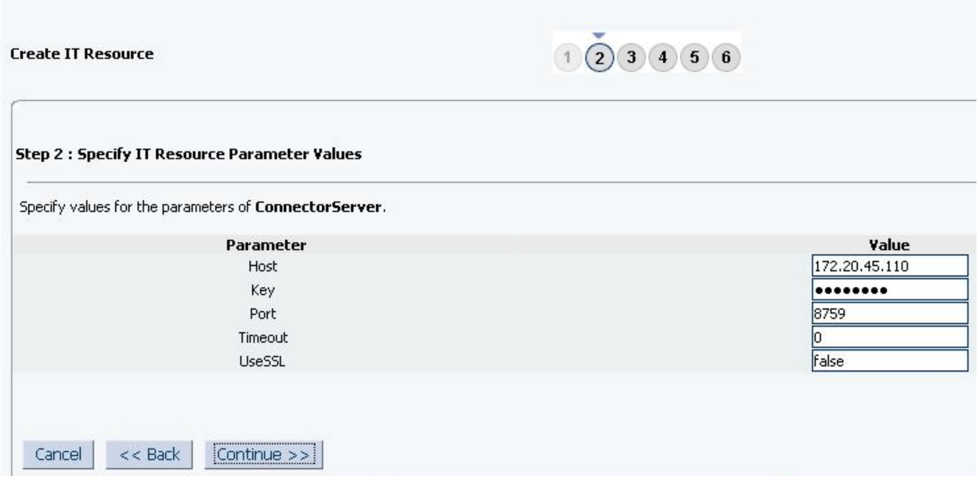
Specify the IT resource name, and select the IT resource type. If the IT resource is to be accessed using a remote manager, then select a remote manager.

* Indicates Required Field

IT Resource Name	* ConnectorServer
IT Resource Type	* Connector Server
Remote Manager	

6. On the Step 2: Specify IT Resource Parameter Values page, specify values for the parameters of the IT resource and then click **Continue**. Figure 2-4 shows the Step 2: Specify IT Resource Parameter Values page.

Figure 2-4 Step 2: Specify IT Resource Parameter Values



Create IT Resource

Step 2 : Specify IT Resource Parameter Values

Specify values for the parameters of **ConnectorServer**.

Parameter	Value
Host	172.20.45.110
Key	••••••••
Port	8759
Timeout	0
UseSSL	false

Table 2-4 provides information about the parameters of the IT resource.

Table 2-4 Parameters of the IT Resource for the Connector Server

Parameter	Description
Host	Enter the host name or IP address of the computer hosting the connector server. Sample value: `RManager`
Key	Enter the key for the Java connector server.
Port	Enter the number of the port at which the connector server is listening. Default value: `8759`

Table 2-4 (Cont.) Parameters of the IT Resource for the Connector Server

Parameter	Description
Timeout	Enter an integer value which specifies the number of milliseconds after which the connection between the connector server and Oracle Identity Manager times out. Sample value: `300`
UseSSL	Enter `true` to specify that you will configure SSL between Oracle Identity Manager and the Connector Server. Otherwise, enter `false`. Default value: `false` **Note:** It is recommended that you configure SSL to secure communication with the connector server. To configure SSL, run the connector server by using the /setKey [*key*] option. The value of this key must be specified as the value of the Key IT resource parameter of the connector server. To use SSL, you must set the value of connectorserver.usessl property to `true`, and then set the value of connectorserver.certifacatestorename to the certificate store name.

7. On the Step 3: Set Access Permission to IT Resource page, the `SYSTEM ADMINISTRATORS` group is displayed by default in the list of groups that have Read, Write, and Delete permissions on the IT resource that you are creating.

   Note:

   This step is optional.

   If you want to assign groups to the IT resource and set access permissions for the groups, then:

   a. Click **Assign Group**.

   b. For the groups that you want to assign to the IT resource, select **Assign** and the access permissions that you want to set. For example, if you want to assign the `ALL USERS` group and set the Read and Write permissions to this group, then you must select the respective check boxes in the row, as well as the Assign check box, for this group.

   c. Click **Assign**.

8. On the Step 3: Set Access Permission to IT Resource page, if you want to modify the access permissions of groups assigned to the IT resource, then:

   Note:

   - This step is optional.
   - You cannot modify the access permissions of the `SYSTEM ADMINISTRATORS` group. You can modify the access permissions of only other groups that you assign to the IT resource.

   a. Click **Update Permissions**.

   b. Depending on whether you want to set or remove specific access permissions for groups displayed on this page, select or deselect the corresponding check boxes.

   c. Click **Update**.

9. On the Step 3: Set Access Permission to IT Resource page, if you want to unassign a group from the IT resource, then:

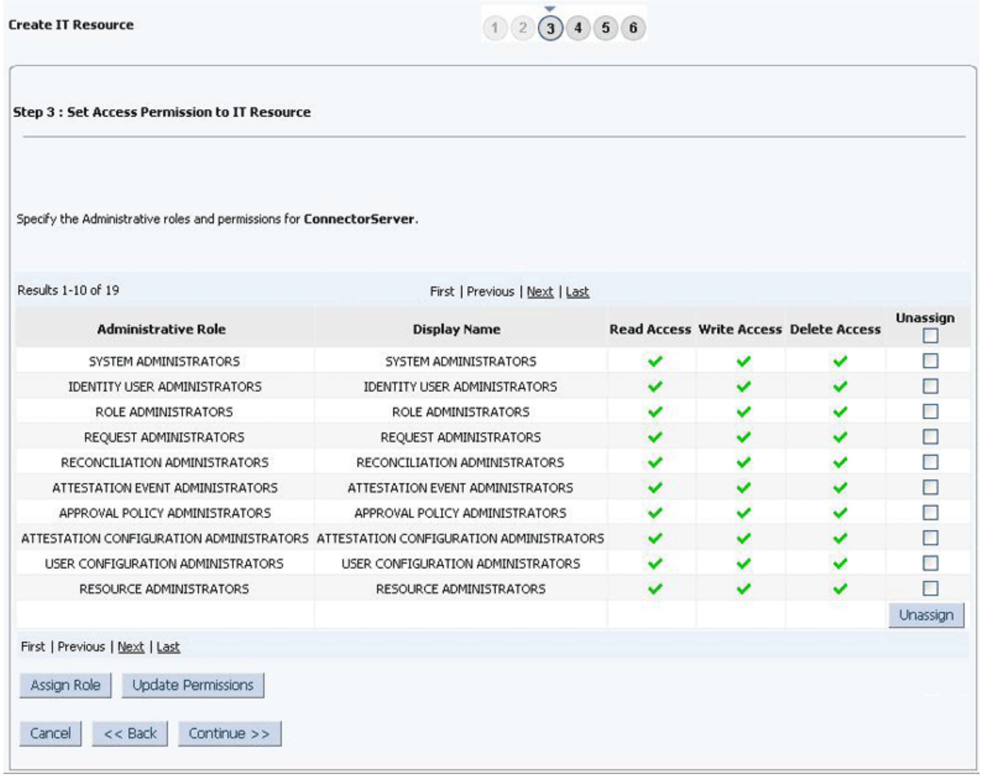
   > **Note:**
   >
   > - This step is optional.
   > - You cannot unassign the `SYSTEM ADMINISTRATORS` group. You can unassign only other groups that you assign to the IT resource.

   a. Select the **Unassign** check box for the group that you want to unassign.

   b. Click **Unassign**.

10. Click **Continue**. Figure 2-5 shows the Step 3: Set Access Permission to IT Resource page.

Figure 2-5 Step 3: Set Access Permission to IT Resource



Create IT Resource

Step 3 : Set Access Permission to IT Resource

Specify the Administrative roles and permissions for **ConnectorServer**.

Results 1-10 of 19

First | Previous | Next | Last

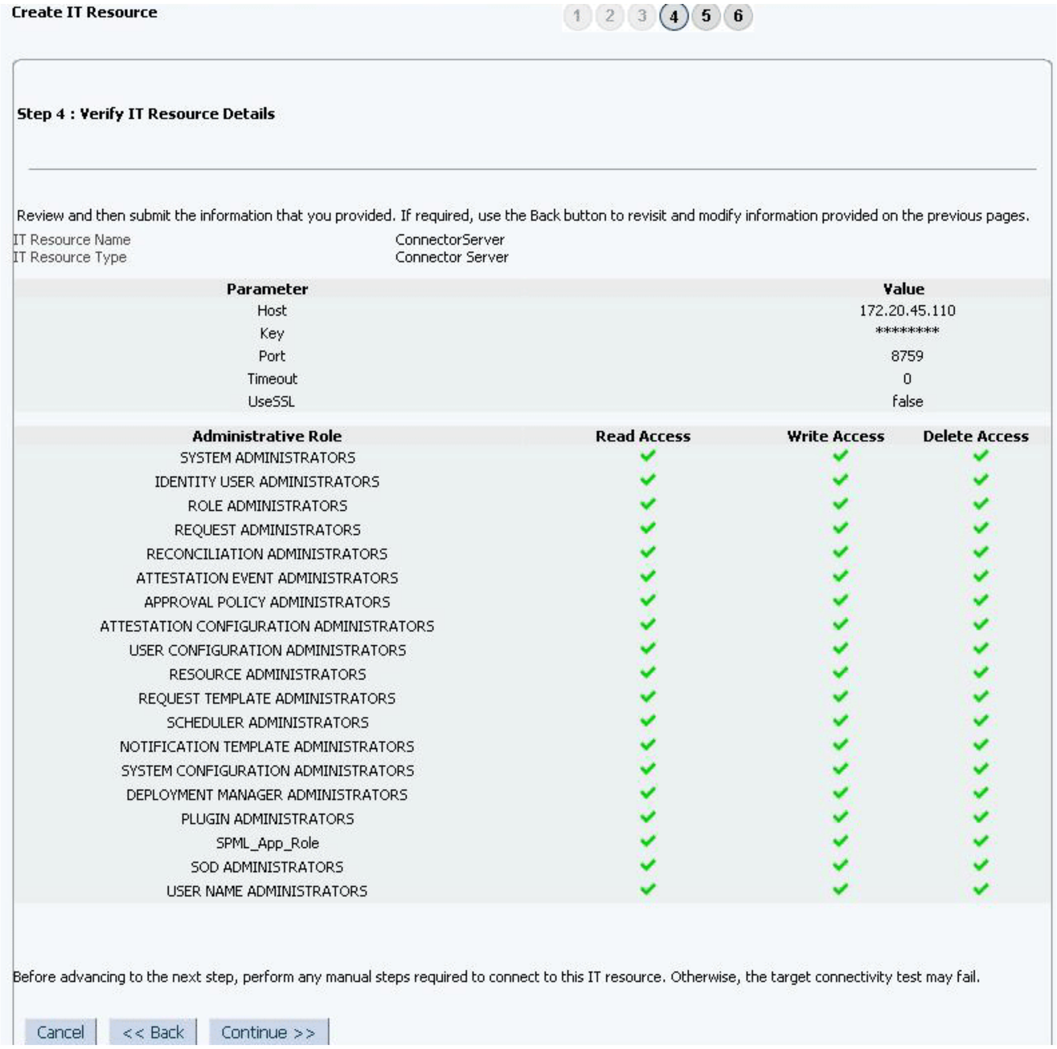
Administrative Role	Display Name	Read Access	Write Access	Delete Access	Unassign □
SYSTEM ADMINISTRATORS	SYSTEM ADMINISTRATORS	✓	✓	✓	□
IDENTITY USER ADMINISTRATORS	IDENTITY USER ADMINISTRATORS	✓	✓	✓	□
ROLE ADMINISTRATORS	ROLE ADMINISTRATORS	✓	✓	✓	□
REQUEST ADMINISTRATORS	REQUEST ADMINISTRATORS	✓	✓	✓	□
RECONCILIATION ADMINISTRATORS	RECONCILIATION ADMINISTRATORS	✓	✓	✓	□
ATTESTATION EVENT ADMINISTRATORS	ATTESTATION EVENT ADMINISTRATORS	✓	✓	✓	□
APPROVAL POLICY ADMINISTRATORS	APPROVAL POLICY ADMINISTRATORS	✓	✓	✓	□
ATTESTATION CONFIGURATION ADMINISTRATORS	ATTESTATION CONFIGURATION ADMINISTRATORS	✓	✓	✓	□
USER CONFIGURATION ADMINISTRATORS	USER CONFIGURATION ADMINISTRATORS	✓	✓	✓	□
RESOURCE ADMINISTRATORS	RESOURCE ADMINISTRATORS	✓	✓	✓	□
					Unassign

First | Previous | Next | Last

11. On the Step 4: Verify IT Resource Details page, review the information that you provided on the first, second, and third pages. If you want to make changes in the data entered on any page, click **Back** to revisit the page and then make the required changes.

12. To proceed with the creation of the IT resource, click **Continue**. Figure 2-6 shows Step 4: Verify IT Resource Details page.

Figure 2-6   Step 4: Verify IT Resource Details



Create IT Resource

Step 4 : Verify IT Resource Details

Review and then submit the information that you provided. If required, use the Back button to revisit and modify information provided on the previous pages.

IT Resource Name	ConnectorServer
IT Resource Type	Connector Server

Parameter	Value
Host	172.20.45.110
Key	********
Port	8759
Timeout	0
UseSSL	false

Administrative Role	Read Access	Write Access	Delete Access
SYSTEM ADMINISTRATORS	✓	✓	✓
IDENTITY USER ADMINISTRATORS	✓	✓	✓
ROLE ADMINISTRATORS	✓	✓	✓
REQUEST ADMINISTRATORS	✓	✓	✓
RECONCILIATION ADMINISTRATORS	✓	✓	✓
ATTESTATION EVENT ADMINISTRATORS	✓	✓	✓
APPROVAL POLICY ADMINISTRATORS	✓	✓	✓
ATTESTATION CONFIGURATION ADMINISTRATORS	✓	✓	✓
USER CONFIGURATION ADMINISTRATORS	✓	✓	✓
RESOURCE ADMINISTRATORS	✓	✓	✓
REQUEST TEMPLATE ADMINISTRATORS	✓	✓	✓
SCHEDULER ADMINISTRATORS	✓	✓	✓
NOTIFICATION TEMPLATE ADMINISTRATORS	✓	✓	✓
SYSTEM CONFIGURATION ADMINISTRATORS	✓	✓	✓
DEPLOYMENT MANAGER ADMINISTRATORS	✓	✓	✓
PLUGIN ADMINISTRATORS	✓	✓	✓
SPML_App_Role	✓	✓	✓
SOD ADMINISTRATORS	✓	✓	✓
USER NAME ADMINISTRATORS	✓	✓	✓

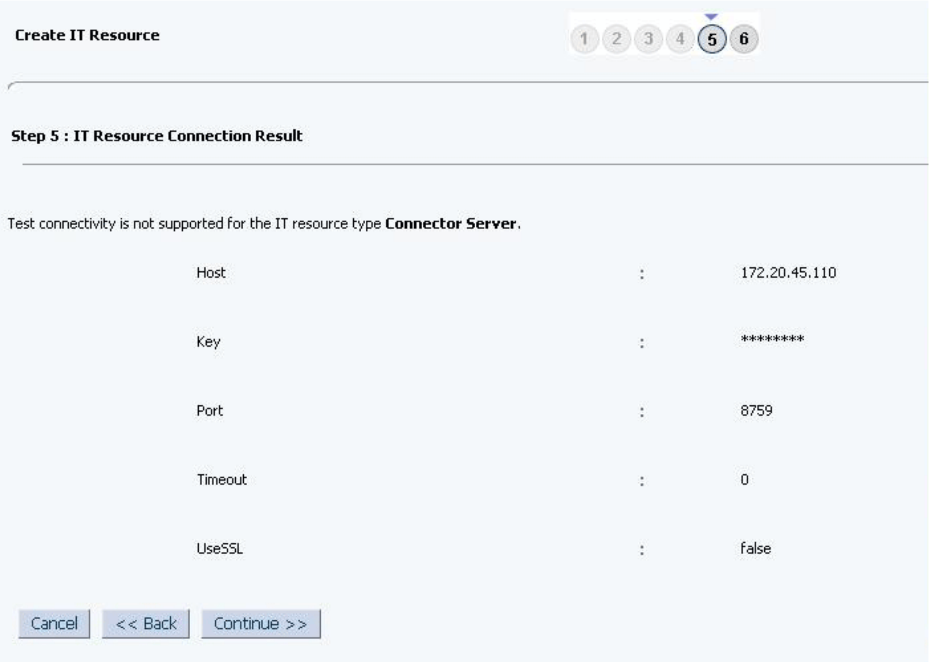
Before advancing to the next step, perform any manual steps required to connect to this IT resource. Otherwise, the target connectivity test may fail.

13. The Step 5: IT Resource Connection Result page displays the results of a connectivity test that is run using the IT resource information. If the test is successful, then click **Continue**. If the test fails, then you can perform one of the following steps:

- Click **Back** to revisit the previous pages and then make corrections in the IT resource creation information.
- Click **Cancel** to stop the procedure, and then begin from the first step onward.

  Figure 2-7 shows the Step 5: IT Resource Connection Result page.

Figure 2-7 Step 5: IT Resource Connection Result



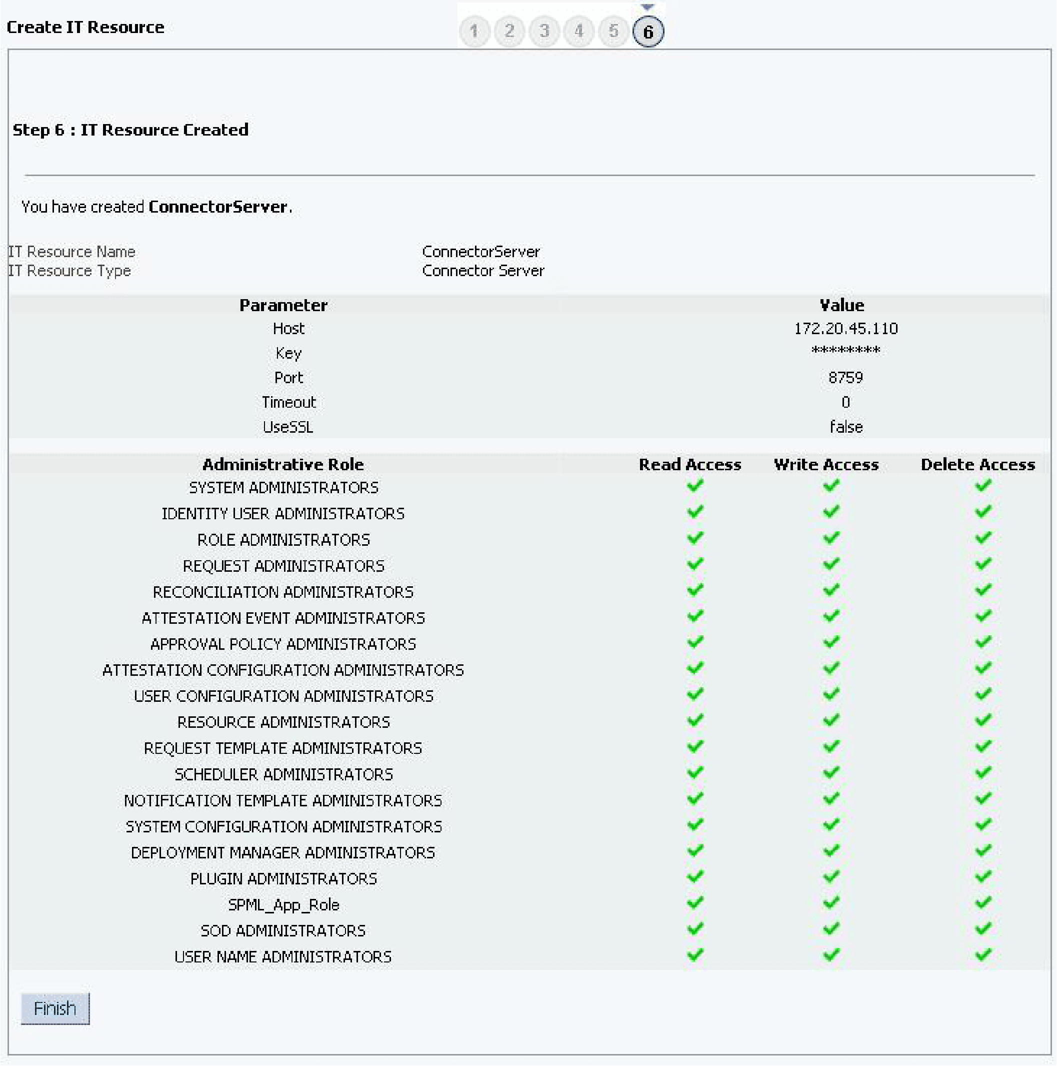
Step 5 : IT Resource Connection Result

Test connectivity is not supported for the IT resource type **Connector Server**.

Host	:	172.20.45.110
Key	:	********
Port	:	8759
Timeout	:	0
UseSSL	:	false

14. Click **Finish**. Figure 2-8 shows the IT Resource Created page.

Figure 2-8   Step 6: IT Resource Created



Step 6 : IT Resource Created

You have created **ConnectorServer**.

IT Resource Name	ConnectorServer
IT Resource Type	Connector Server

Parameter	Value
Host	172.20.45.110
Key	********
Port	8759
Timeout	0
UseSSL	false

Administrative Role	Read Access	Write Access	Delete Access
SYSTEM ADMINISTRATORS	✓	✓	✓
IDENTITY USER ADMINISTRATORS	✓	✓	✓
ROLE ADMINISTRATORS	✓	✓	✓
REQUEST ADMINISTRATORS	✓	✓	✓
RECONCILIATION ADMINISTRATORS	✓	✓	✓
ATTESTATION EVENT ADMINISTRATORS	✓	✓	✓
APPROVAL POLICY ADMINISTRATORS	✓	✓	✓
ATTESTATION CONFIGURATION ADMINISTRATORS	✓	✓	✓
USER CONFIGURATION ADMINISTRATORS	✓	✓	✓
RESOURCE ADMINISTRATORS	✓	✓	✓
REQUEST TEMPLATE ADMINISTRATORS	✓	✓	✓
SCHEDULER ADMINISTRATORS	✓	✓	✓
NOTIFICATION TEMPLATE ADMINISTRATORS	✓	✓	✓
SYSTEM CONFIGURATION ADMINISTRATORS	✓	✓	✓
DEPLOYMENT MANAGER ADMINISTRATORS	✓	✓	✓
PLUGIN ADMINISTRATORS	✓	✓	✓
SPML_App_Role	✓	✓	✓
SOD ADMINISTRATORS	✓	✓	✓
USER NAME ADMINISTRATORS	✓	✓	✓

2.4 About Upgrading the RSA Authentication Manager Connector

Upgrading to this release of the connector from earlier releases is not supported.

2.5 Postcloning the RSA Authentication Manager

If you clone the connector, a copy of the connector is created. Once this is completed, some of the connector objects that might contain the details of the old connector must be modified as a part of postcloning. The following sections contain detailed information:

- About Postcloning
- Updating Child Table Mappings

2.5.1 About Postcloning

You can clone the RSA Authentication Manager connector by setting new names for some of the objects that comprise the connector. The outcome of the process is a new connector XML file. Most of the connector objects, such as Resource Object, Process Definition, Process Form, IT Resource Type Definition, IT Resource Instances, Lookup Definitions, Adapters, Reconciliation Rules and so on in the new connector XML file have new names.

After a copy of the connector is created by setting new names for connector objects, some objects might contain the details of the old connector objects. Therefore, you must modify the following Oracle Identity Manager objects to replace the base connector artifacts or attribute references with the corresponding cloned artifacts or attributes:

- Localization Properties

  You must update the resource bundle of a user locale with new names of the process form attributes for proper translations after cloning the connector. You can modify the properties file of your locale in the resources directory of the connector bundle.

- Lookup Definition

  In the cloned lookup definition for provisioning attribute map, if the code key entries specific to groups and roles contain the old process form details, then you must modify them to reflect the cloned form name.

  For example, consider Lookup.RSAAM.UM.ProvAttr1 and UD_AMROLE1 to be the cloned versions of the Lookup.RSAAM.UM.ProvAttrMap lookup definition and UD_AMROLE child form, respectively.

  After cloning, the Lookup.RSAAM.UM.ProvAttrMap1 lookup definition contains Code Key entries that correspond to the fields of the old child form UD_AMROLE. To ensure that the Code Key entries point to the fields of the cloned child form (UD_AMROLE1), specify UD_AMROLE1~Role Name[LOOKUP] in the corresponding Code Key column. Similarly, you can specify UD_AMGROUP1~Group Name[LOOKUP] in the Code Key column for groups.

- Child Table

  As a result of a change in the name of the child table, you must modify the corresponding mappings for the child table operations to work successfully.

  See Updating Child Table Mappings.

2.5.2 Updating Child Table Mappings

To update the corresponding mappings, perform the following procedure:

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 User1** process form.
4. Double-click the **Add User to Group** process task.

   The Editing Task window is displayed.

5. On the Integration tab, select the row corresponding to the name of the child table, and then click **Map.**
6. The Data Mapping for Variable window is displayed.
7. Change the value in the Literal Value field to the cloned table name. For example, `UD_AMGROUP1`.
8. Click **Save** and close the window.
9. To change the mappings for the Remove User from Group task, perform Steps 1 through 8 of this procedure with the following difference:

   While performing Step 4 of this procedure, instead of double-clicking the Add User to Group task, double-click the **Remove User from Group** task.
10. To change the mappings for the Update User for Group task, perform Steps 1 through 8 with the following difference:

    While performing Step 4 of this procedure, instead of double-clicking the Add User to Group task, double-click the **Update User for Group** task.
11. To change the mappings for the Add User to Role task, perform Steps 1 through 8 with the following difference:

    While performing Step 4 of this procedure, instead of double-clicking the Add User to Group task, double-click the **Add User to Role** task.
12. To change the mappings for the Remove User from Role task, perform Steps 1 through 8 with the following difference:

    While performing Step 4 of this procedure, instead of double-clicking the Add User to Group task, double-click the **Remove User from Role** task.
13. To change the mappings for the Update User for Role task, perform Steps 1 through 8 with the following difference:

    While performing Step 4 of this procedure, instead of double-clicking the Add User to Group task, double-click the **Update User for Role** task.

3 Using the RSA Authentication Manager Connector

This chapter is divided into the following sections:

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:

1. Perform lookup field synchronization by running the scheduled jobs provided for this operation.
2. Perform user and token reconciliation by running the scheduled jobs for user and token reconciliation.

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

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

3.2 Scheduled Job for Lookup Field Synchronization

The following scheduled jobs are used for lookup fields synchronization:

- RSAAM TokenSerial Lookup Reconciliation
- RSAAM SecurityDomain Lookup Reconciliation
- RSAAM RadiusProfile Lookup Reconciliation
- RSAAM IdentitySource Lookup Reconciliation
- RSAAM UserGroup Lookup Reconciliation

- RSAAM AdminRole Lookup Reconciliation

You must specify values for the attributes of these scheduled jobs. Table 3-1 describes the attributes of these scheduled jobs. Scheduled Jobs describes the procedure to configure scheduled jobs.

Table 3-1 Attributes of the Scheduled Jobs for Lookup Field Synchronization

Attribute	Description
Code Key Attribute	Name of the connector or target system attribute that is used to populate the Code Key column of the lookup definition (specified as the value of the Lookup Name attribute). Default value: `__UID__` **Note:** Do *not* change the value of this attribute.
Decode Attribute	Name of the connector or target system attribute that is used to populate the Decode column of the lookup definition (specified as the value of the Lookup Name attribute). Default value: `__NAME__` **Note:** Do *not* change the value of this attribute.
IT Resource Name	Enter the name of the IT resource for the target system installation from which you want to reconcile user records. Default value: `RSA Server Instance`
Lookup Name	Enter the name of the lookup definition in Oracle Identity Manager that must be populated with values fetched from the target system. Depending on the scheduled job that you are using, the default values are as follows: • For TokenSerial Lookup Reconciliation: `Lookup.RSAAM.TokenSerial` • For SecurityDomain Lookup Reconciliation: `Lookup.RSAAM.SecurityDomain` • For RadiusProfile Lookup Reconciliation: `Lookup.RSAAM.RadiusProfile` • For IdentitySource Lookup Reconciliation: `Lookup.RSAAM.IdentitySource` • For UserGroup Lookup Reconciliation: `Lookup.RSAAM.UserGroup` • For AdminRole Lookup Reconciliation: `Lookup.RSAAM.AdminRole`
Object Type	Enter the type of object you want to reconcile. Depending on the scheduled job that you are running, the default value is one of the following: • For TokenSerial Lookup Reconciliation: `TokenSerial` • For SecurityDomain Lookup Reconciliation: `SecurityDomain` • For RadiusProfile Lookup Reconciliation: `RadiusProfile` • For IdentitySource Lookup Reconciliation: `IdentitySource` • For UserGroup Lookup Reconciliation: `UserGroup` • For AdminRole Lookup Reconciliation: `AdminRole`
Resource Object Name	Name of the resource object that is used for reconciliation. Default value: `RSA Auth Manager User`

3.3 Configuring Reconciliation

Reconciliation involves duplicating in Oracle Identity Manager the creation of and modifications to user accounts on the target system. This section discusses the following topics related to configuring reconciliation:

- Full Reconciliation

- Limited Reconciliation
- Batched Reconciliation
- Reconciliation Scheduled Jobs

3.3.1 Full Reconciliation

Full reconciliation involves reconciling all existing user records from the target system into Oracle Identity Manager. After you deploy the connector, you must first perform full reconciliation. In addition, you can switch from incremental reconciliation to full reconciliation whenever you want to ensure that all target system records are reconciled in Oracle Identity Manager.

For performing a full reconciliation run, values for the Latest Token and Filter attributes of the scheduled jobs for reconciling user records must not be present.

At the end of the reconciliation run, the Latest Token attribute of the scheduled job for user record reconciliation is automatically set to the time stamp at which the run ended. From the next reconciliation run onward, only records created or modified after this time stamp are considered for reconciliation. This is incremental reconciliation.

> **Note:**
>
> Incremental reconciliation reflects changes or modifications made in the target system when a change or modification is made in the incremental reconciliation attribute. For example, during user reconciliation, changes like updates to all the fields on the Authentication Settings page (including radius profiles) and group updates will not be reconciled as a part of incremental reconciliation, and a full reconciliation has to be performed in order to reconcile these changes into Oracle Identity Manager.

3.3.2 Limited Reconciliation

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

The connector provides a Filter attribute that allows you to use any of the RSA Authentication Manager resource attributes to filter the target system records.

You can perform limited reconciliation by creating filters for the reconciliation module. This connector provides a Filter attribute (a scheduled job attribute) that allows you to use any of the RSA Authentication Manager resource attributes to filter the target system records.

The following RSA Authentication Manager attributes are supported for filtering:

- For User Reconciliation:
  - CERT_DN
  - EMAIL
  - FIRST_NAME
  - LAST_NAME

  - LOGINUID
  - MIDDLE_NAME
  - PASSWORD
  - ADMINISTRATOR_FLAG
  - PROXIED_AUTHENTICATORS
  - CHANGE_PASSWORD_DATE
  - CHANGE_PASSWORD_FLAG
  - DESCRIPTION
  - ENABLE_FLAG
  - EXPIRATION_DATE
  - EXPIRE_LOCKOUT_DATE
  - EXPIRE_EMERGENCY_LOCKOUT_DATE
  - FAIL_EMERGENCY_COUNT
  - FAIL_EMERGENCY_DATE
  - FAIL_PASSWORD_COUNT
  - FAIL_PASSWORD_DATE
  - IDENTITY_SRC_ID
  - IMPERSONATABLE_FLAG
  - IMPERSONATOR_FLAG
  - LAST_UPDATED_BY
  - LAST_UPDATED_ON
  - LOCKOUT_FLAG
  - EMERGENCY_LOCKOUT_FLAG
  - LOGIN_FAILURE_COUNT
  - OWNER_ID
  - SECURITY_QUES_ANSWERS
  - SECURITY_QUES_REQUIRED_AUTHN
  - SECURITY_QUES_REQUIRED_REG
  - SECURITY_QUES_LANGUAGE
  - SECURITY_QUES_COUNTRY
  - SECURITY_QUES_VARIANT
  - START_DATE

  In addition, all extended attributes that are added in the target system through customization are supported for filtering.

- For Token Reconciliation:
  - assignedBy
  - tokenAssignedDate

- assignedToken
- enabled
- tokenShutdownDate
- importedBy
- importedOn
- lastExportedBy
- lastExportedOn
- tokenRuntime.lastLoginDate
- lastUpdatedBy
- lastUpdatedOn
- tokenLost
- replacedByToken
- pinType
- serialNumber
- softidDeployed
- tokenType

> **Note:**
>
> While entering filters in the scheduled job for user and token reconciliation, the attribute name should be in the same syntax as the decode value in the reconciliation attribute map.
>
> See User Fields for Target Resource Reconciliation and Token Fields for Target Resource Reconciliation for decode values that need to be specified for user and token reconciliation.
>
> In addition, during token reconciliation, use the token attributes from ListTokenDTO and not from TokenDTO target class.

Following are a few examples:

- To reconcile all users whose login id is like 'jo*', use filter `startsWith('__NAME__','jo')`
- To reconcile all users whose email is like '*@company.com', use filter `endsWith('email;IMS;Core;String;EMAIL','@company.com')`
- To reconcile all tokens whose serialnumber is like '0002219*', use filter `startsWith('__NAME__','0002219')`
- To reconcile all tokens which are marked as lost, use filter `equalTo('tokenLost;ListTokenDTO;Core;boolean;tokenLost', true)`

3.3.3 Batched Reconciliation

This section discusses the Batch Size, Batch Start, and Number of Batches attributes of the scheduled jobs for target resource reconciliation.

By default, all target system records that are added or modified after the last reconciliation run are reconciled during the current reconciliation run. 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.

The following are the attributes used to configure batched reconciliation:

- Batch Size: Use this attribute to specify the number of records that must be included in each batch.

  If you set the value of this attribute to 0, then the defaultbatchsize entry of the main configuration lookup (Lookup.RSAAM.Configuration) is considered as the batch size for batched reconciliation. Any numeric value other than 0 takes precedence over the defaultbatchsize entry.
- Batch Start: Use this attribute to specify the record number from which batched reconciliation must begin.

  Set the value of this attribute to `0` to begin reconciliation from the first record in the target system. Similarly, set the value of this attribute to `1` to begin reconciliation from the second record in the target system and so on.
- Number of Batches: Use this attribute to specify the total number of batches that must be reconciled. The default value of this attribute is `0.` This implies that the connector fetches records in the maximum possible number of batches from the target system. In other words, all records starting from the record specified in the Batch Start attribute to the last record available in the target system is fetched. Any other valid number limits the number of batches to that specified value.

To configure batched reconciliation for tokens, specify values for all the above attributes of the RSAAM Token Target Recociliation scheduled job.

To configure batched reconciliation for users, specify a value for the Batch Size attribute of the RSAAM User Target Recociliation scheduled job.

> **See Also:**
>
> Scheduled Jobs for Reconciliation of Token and User Records for more information about the RSAAM Token Target Reconciliation and RSAAM User Target Reconciliation scheduled jobs

3.3.4 Reconciliation Scheduled Jobs

When you run the Connector Installer, the scheduled tasks corresponding to the following scheduled jobs are automatically created in Oracle Identity Manager:

- Scheduled Jobs for Reconciliation of Token and User Records
- Scheduled Jobs for Reconciliation of Deleted Token and User Records

3.3.4.1 Scheduled Jobs for Reconciliation of Token and User Records

Depending on whether you want to implement target resource reconciliation for tokens or users, you must specify values for the attributes of one of the following user reconciliation scheduled jobs:

- RSAAM Token Target Reconciliation

  This scheduled job is used to reconcile token data for assigned tokens.

  Table 3-2 describes the attributes of the scheduled job for reconciliation of token records

Table 3-2 Attributes of the Scheduled Jobs for Reconciliation of Token Records

<table>
<tr><th>Attributes</th><th>Description</th></tr>
<tr><td>Batch Size</td><td>Enter the number of records that must be included in each batch fetched from the target system.
Default value: 0
This attribute is used in conjunction with the Batch Start and Number of Batches attributes. All these attributes are discussed in Batched Reconciliation.</td></tr>
<tr><td>Batch Start</td><td>Enter the number of the target system record from which a batched reconciliation run must begin.
Default value: 0
This attribute is used in conjunction with the Batch Start and Number of Batches attributes. All these attributes are discussed in Batched Reconciliation.</td></tr>
<tr><td>Filter</td><td>Expression for filtering records. Use the following syntax:
syntax = expression (operator expression)*
operator = 'and' | 'or'
expression = ('not')? filter
filter = ('equalTo' | 'contains' | 'containsAllValues'
| 'startsWith' | 'endsWith' | 'greaterThan' |
'greaterThanOrEqualTo'
| 'lessThan' | 'lessThanOrEqualTo') '(' 'attributeName' ','
 attributeValue')'
attributeValue = singleValue | multipleValues
singleValue = 'value'
multipleValues = '[' 'value_1' (',' 'value_n')* ']'
Default value: None</td></tr>
<tr><td>Incremental Recon Attribute</td><td>Attribute that holds the date on which the token record was modified.
Default value: lastUpdatedOn;TokenDTO;Core;Date;lastUpdatedOn
<b>Note:</b> Do <i>not</i> change the value of this attribute</td></tr>
<tr><td>IT Resource Name</td><td>Name of the IT resource instance that the connector must use to reconcile data.
Sample value: RSA Server Instance</td></tr>
</table>

Table 3-2 (Cont.) Attributes of the Scheduled Jobs for Reconciliation of Token Records

Attributes	Description
Latest Token	This attribute holds the value of the attribute that is specified as the value of the Incremental Recon Attribute attribute. The Latest Token attribute is used for internal purposes. By default, this value is empty. **Note:** Do *not* enter a value for this attribute. The reconciliation engine automatically enters a value in this attribute. Sample value: `1354753427000`
Number of Batches	Enter the number of batches that must be reconciled. Default value: `0` This attribute is used in conjunction with the Batch Start and Number of Batches attributes. All these attributes are discussed in Batched Reconciliation.
Object Type	This attribute holds the type of object you want to reconcile. Default value: `Token`
Resource Object Name	Enter the name of the resource object against which reconciliation runs must be performed. Default value: `RSA Auth Manager Token.`
Scheduled Task Name	Name of the scheduled task used for reconciliation.Default value: `RSAAM Token Target Reconciliation.`

- RSAAM User Target Reconciliation

  This scheduled job is used to reconcile user data in the target resource (account management) mode of the connector.

  Table 3-3 describes the attributes of the scheduled job for reconciliation of user records.

Table 3-3 Attributes of the Scheduled Jobs for Reconciliation of User Records

Attribute	Description
Batch Size	Enter the number of records that must be included in each batch fetched from the target system. Default value: `0`

Filter	Expression for filtering records. Use the following syntax:
	`syntax = expression ( operator expression )*`
	`operator = 'and' | 'or'`
	`expression = ( 'not' )? filter`
	`filter = ('equalTo' | 'contains' | 'containsAllValues'`
	`| 'startsWith' | 'endsWith'  | 'greaterThan' | 'greaterThanOrEqualTo'`
	`| 'lessThan' | 'lessThanOrEqualTo' )  '(' 'attributeName' ','`
	` attributeValue')'`
	`attributeValue = singleValue  |  multipleValues`
	`singleValue = 'value'`
	`multipleValues = '[' 'value_1' (',' 'value_n')* ']'`
	Default value: None

IT Resource Name	Name of the IT resource instance that the connector must use to reconcile data. Sample value: `RSA Server Instance`

Table 3-3 (Cont.) Attributes of the Scheduled Jobs for Reconciliation of User Records

Attribute	Description
Object Type	This attribute holds the type of object you want to reconcile. Default value: `User`
Resource Object Name	Enter the name of the resource object against which reconciliation runs must be performed. Default value: `RSA Auth Manager User.`
Incremental Recon Attribute	Attribute that holds the date on which the user record was modified. Default value: `lastModifiedOn;IMS;Core;Date;LAST_UPDATED_ON` **Note:** Do *not* change the value of this attribute
Latest Token	This attribute holds the value of the attribute that is specified as the value of the Incremental Recon Attribute attribute. The Latest Token attribute is used for internal purposes. By default, this value is empty. **Note:** Do *not* enter a value for this attribute. The reconciliation engine automatically enters a value in this attribute. Sample value: `1354753427000`
Scheduled Task Name	Name of the scheduled task used for reconciliation. Default value: `RSAAM User Target Reconciliation.`

3.3.4.2 Scheduled Jobs for Reconciliation of Deleted Token and User Records

Depending on whether you want to implement target resource delete reconciliation for tokens or users, you must specify values for the attributes of one of the following scheduled jobs:

- RSAAM Token Target Delete Reconciliation

  This scheduled job is used to reconcile unassigned token data in the target source (identity management) mode of the connector. After the completion of this scheduled job, all the unassigned tokens are revoked in Oracle Identity Manager.

  Table 3-4 describes the attributes of the scheduled job for reconciliation of deleted token records.

  Table 3-4 Attributes of the Scheduled Jobs for Delete Token Reconciliation

Attributes	Description
IT Resource Name	Name of the IT resource instance that the connector must use to reconcile data. Sample value: `RSA Server Instance`
Object Type	This attribute holds the type of object you want to reconcile. Default value: `Token`
Resource Object Name	Enter the name of the resource object against which reconciliation runs must be performed. Default value: `RSA Auth Manager Token.`

- RSAAM User Target Delete Reconciliation

  This scheduled job is used to reconcile deleted user data in the target source (identity management) mode of the connector.

Table 3-5 describes the attributes of the scheduled job for reconciliation of deleted user records.

Table 3-5 Attributes of the Scheduled Jobs for Delete User Reconciliation

Attributes	Description
IT Resource Name	Name of the IT resource instance that the connector must use to reconcile data. Sample value: `RSA Server Instance`
Object Type	This attribute holds the type of object you want to reconcile. Default value: `User`
Resource Object Name	Enter the name of the resource object against which reconciliation runs must be performed. Default value: `RSA Auth Manager User.`

3.4 Scheduled Jobs

The following sections provide detailed information about scheduled jobs that must be configured along with the procedure to configure them for lookup field synchronization and reconciliation:

- Scheduled Jobs for Lookup Field Synchronization and Reconciliation
- Configuring Scheduled Jobs

3.4.1 Scheduled Jobs for Lookup Field Synchronization and Reconciliation

All scheduled jobs that must be configured are listed in Table 3-6.

Table 3-6 Scheduled Jobs for Lookup Field Synchronization and Reconciliation

Scheduled Task	Description
RSAAM Token Serial Lookup Reconciliation	This scheduled job is used to synchronize values of the token serial lookup fields between Oracle Identity Manager and the target system. See Scheduled Job for Lookup Field Synchronization for information about this scheduled job.
RSAAM Security Domain Lookup Reconciliation	This scheduled job is used to synchronize values of the security domain lookup fields between Oracle Identity Manager and the target system. See Scheduled Job for Lookup Field Synchronization for information about this scheduled job.
RSAAM Radius Profile Lookup Reconciliation	This scheduled job is used to synchronize values of the radius profile lookup fields between Oracle Identity Manager and the target system. See Scheduled Job for Lookup Field Synchronization for information about this scheduled job.
RSAAM Identity Source Lookup Reconciliation	This scheduled job is used to synchronize values of the identity source lookup fields between Oracle Identity Manager and the target system. See Scheduled Job for Lookup Field Synchronization for information about this scheduled job.
RSAAM User Group Lookup Reconciliation	This scheduled job is used to synchronize values of the user group lookup fields between Oracle Identity Manager and the target system. See Scheduled Job for Lookup Field Synchronization for information about this scheduled job.

Table 3-6 (Cont.) Scheduled Jobs for Lookup Field Synchronization and Reconciliation

Scheduled Task	Description
RSAAM Admin Role Lookup Reconciliation	This scheduled job is used to synchronize values of the admin role lookup fields between Oracle Identity Manager and the target system. See Scheduled Job for Lookup Field Synchronization for information about this scheduled job.
RSAAM User Target Reconciliation	This scheduled job is used to fetch user data during target resource reconciliation. See Reconciliation Scheduled Jobs for information about this scheduled job.
RSAAM Token Target Reconciliation	This scheduled job is used to fetch token data during target resource reconciliation. See Reconciliation Scheduled Jobs for information about this scheduled job.
RSAAM User Target Delete Reconciliation	This scheduled job is used to fetch data about deleted users during target resource reconciliation. During a reconciliation run, for each deleted user record on the target system, the RSA Authentication Manager user resource for the corresponding OIM User is revoked. See Reconciliation Scheduled Jobs for information about this scheduled job.
RSAAM Token Target Delete Reconciliation	This scheduled job is used to fetch data about deleted tokens during target resource reconciliation. During a reconciliation run, for each deleted token record on the target system, the token for the corresponding OIM User is revoked. See Reconciliation Scheduled Jobs for information about this scheduled job.

3.4.2 Configuring Scheduled Jobs

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

1. Log in to Oracle Identity System Administration.
2. In the left pane, under System Management, click **Scheduler.**
3. Search for and open the scheduled job as follows:
    a. 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.
    b. In the search results table on the left pane, click the scheduled job in the Job Name column.
4. 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 Creating Jobs in *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information about schedule types.

    In addition to modifying the job details, you can enable or disable a job.
5. On the Job Details tab, in the Parameters region, specify values for the attributes of the scheduled job.

> **Note:**
>
> - Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.
> - Values (either default or user-defined) must be assigned to all the attributes. If even a single attribute value is left empty, then reconciliation is not performed.

6. 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.

3.5 Guidelines On Performing Provisioning Operations

The following is a guideline that you must apply while performing a provisioning operation:

During a provisioning operation, if you do not specify values or clear all the existing values for the Account Expire Date, Account Expire Hours, and Account Expire Minutes fields, then the corresponding account in the target system is set to `Does Not Expire`.

3.6 Performing Provisioning Operations

To perform provisioning operations in Oracle Identity Manager:

1. Log in to Oracle Identity Administrative and User console.
2. Create a user. See Creating a User in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager*.
3. On the Account tab, click **Request Accounts.**
4. In the Catalog page, search for and add to cart the application instance created for the RSA Server Instance IT resource (in Creating an Application Instance), and then click **Checkout.**
5. Specify value for fields in the application form.

> **Note:**
>
> Ensure to select proper values for lookup type fields as there are a few dependent fields. Selecting a wrong value for such fields may result in provisioning failure.

6. Click **Ready to Submit.**
7. Click **Submit.**
8. If you want to provision entitlements, then:
   a. On the Entitlements tab, click **Request Entitlements.**
   b. In the Catalog page, search for and add to cart the entitlement, and then click **Checkout.**
   c. Click **Submit.**

3.7 Uninstalling the Connector

If you want to uninstall the connector for any reason, see Uninstalling Connectors in *Oracle Fusion Middleware Administering Oracle Identity Manager.*

After you uninstall the connector, perform the postuninstall procedure. See Postuninstall in *Oracle Fusion Middleware Administering Oracle Identity Manager*.

4

Extending the Functionality of the RSA Authentication Manager Connector

This chapter describes procedures that you can perform to extend the functionality of the connector for addressing your specific business requirements. This chapter discusses the following sections:

> **Note:**
>
> From Oracle Identity Manager Release 11.1.2 onward, lookup queries are not supported. For information on managing lookups by using the Form Designer in Identity System Administration, see Managing Lookups in *Oracle Fusion Middleware Administering Oracle Identity Manager* .

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 Settings** to display the list of Authentication Manager attributes.

4.2 Adding New User or Token Attributes for Reconciliation

You can add new user or token attributes for reconciliation. By default, the attributes listed in Table 1-5 and Table 1-7 are mapped for reconciliation between Oracle Identity Manager and the target system. If required, you can add new attributes (standard or custom) for reconciliation.

> **Note:**
>
> - This connector supports configuration of the preconfigured and custom attributes of RSA Authentication Manager for reconciliation.
> - Only single-valued attributes can be mapped for reconciliation.

This information is divided across the following sections:

- Adding New Attributes
- Adding Attributes to Reconciliation Fields
- Creating Reconciliation Field Mapping
- Creating Entries in Lookup Definitions
- Performing Changes in a New UI Form

4.2.1 Adding New Attributes

To add a new attribute on the process form, perform the following procedure:

> **Note:**
>
> If you have already added an attribute for provisioning, then you need not repeat steps performed here.

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 EMAIL field, enter `UD_AMUSER_EMAIL` 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:

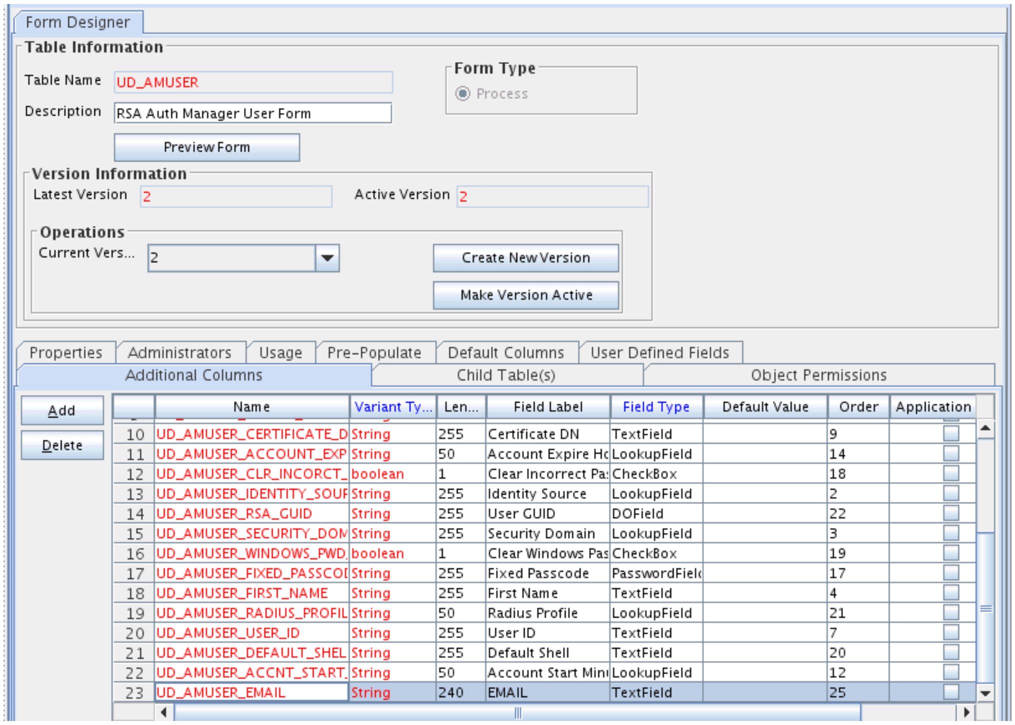


Table Information

Table Name: UD_AMUSER

Description: RSA Auth Manager User Form

Form Type: ● Process

Version Information

Latest Version: 2

Active Version: 2

Operations

Current Vers...: 2

	Name	Variant Ty...	Len...	Field Label	Field Type	Default Value	Order	Application
10	UD_AMUSER_CERTIFICATE_D	String	255	Certificate DN	TextField		9	□
11	UD_AMUSER_ACCOUNT_EXP	String	50	Account Expire Hc	LookupField		14	□
12	UD_AMUSER_CLR_INCORCT_	boolean	1	Clear Incorrect Pa:	CheckBox		18	□
13	UD_AMUSER_IDENTITY_SOUF	String	255	Identity Source	LookupField		2	□
14	UD_AMUSER_RSA_GUID	String	255	User GUID	DOField		22	□
15	UD_AMUSER_SECURITY_DOM	String	255	Security Domain	LookupField		3	□
16	UD_AMUSER_WINDOWS_PWD_	boolean	1	Clear Windows Pas	CheckBox		19	□
17	UD_AMUSER_FIXED_PASSCOI	String	255	Fixed Passcode	PasswordFielc		17	□
18	UD_AMUSER_FIRST_NAME	String	255	First Name	TextField		4	□
19	UD_AMUSER_RADIUS_PROFIL	String	50	Radius Profile	LookupField		21	□
20	UD_AMUSER_USER_ID	String	255	User ID	TextField		7	□
21	UD_AMUSER_DEFAULT_SHEL	String	255	Default Shell	TextField		20	□
22	UD_AMUSER_ACCNT_START_	String	50	Account Start Mini	LookupField		12	□
23	UD_AMUSER_EMAIL	String	240	EMAIL	TextField		25	□

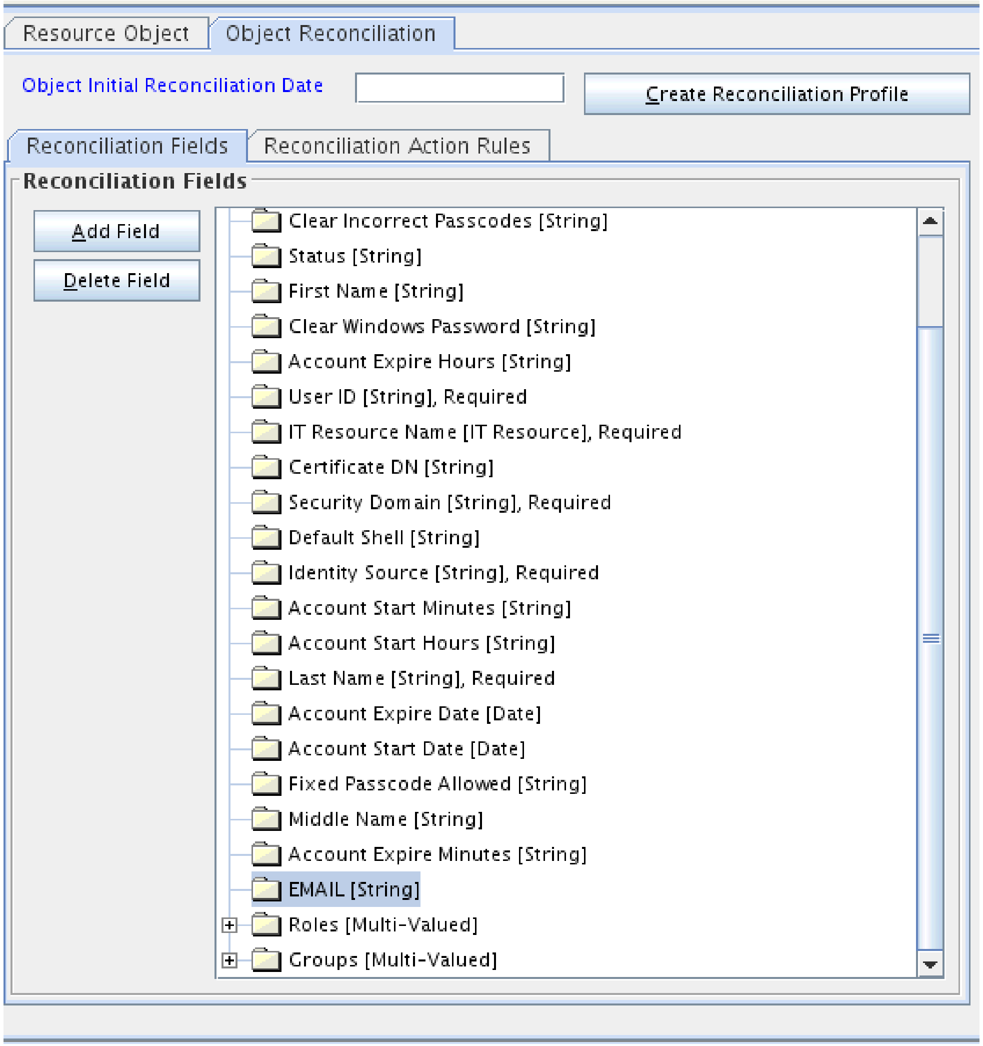
4.2.2 Adding Attributes to Reconciliation Fields

To add the new attribute to the list of reconciliation fields in the resource object, perform the following procedure:

1. Expand **Resource Management**, and double-click **Resource Objects**.
2. Search for and open either the **RSA Auth Manager User** or the **RSA Auth Manager Token** resource object.
3. On the Object Reconciliation tab, click **Add Field**.
4. Enter the details of the field.

   For example, enter `EMAIL` 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.
5. Click the Save icon. The following screenshot shows the new reconciliation field added to the resource object:



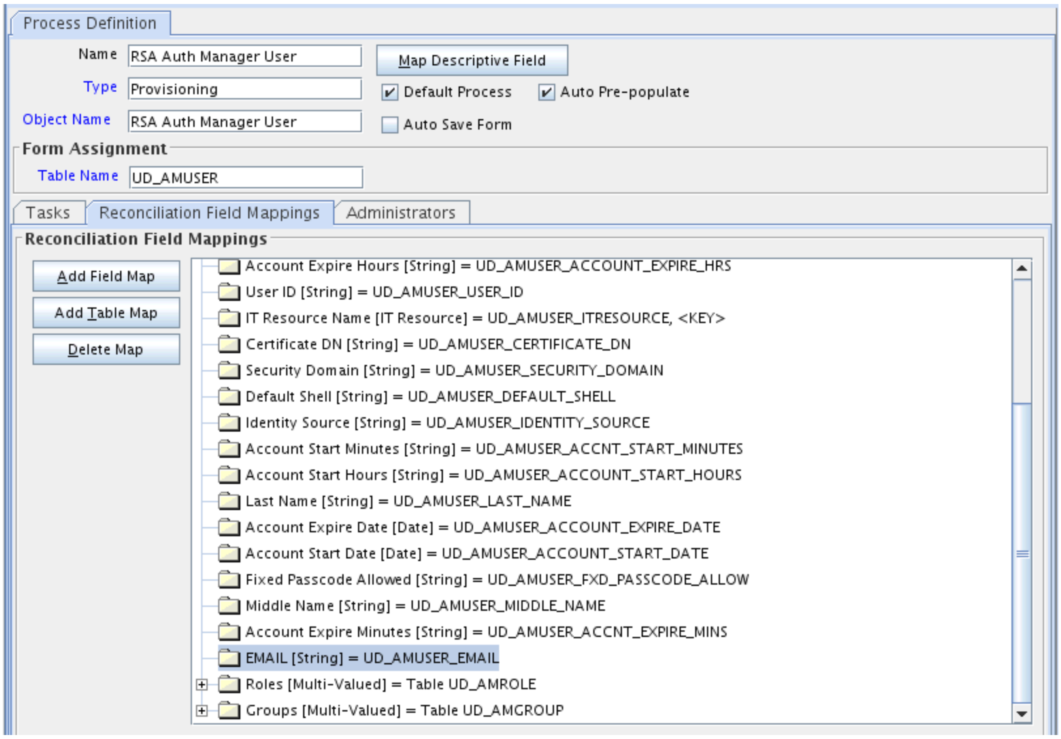
Clear Incorrect Passcodes [String]
Status [String]
First Name [String]
Clear Windows Password [String]
Account Expire Hours [String]
User ID [String], Required
IT Resource Name [IT Resource], Required
Certificate DN [String]
Security Domain [String], Required
Default Shell [String]
Identity Source [String], Required
Account Start Minutes [String]
Account Start Hours [String]
Last Name [String], Required
Account Expire Date [Date]
Account Start Date [Date]
Fixed Passcode Allowed [String]
Middle Name [String]
Account Expire Minutes [String]
EMAIL [String]
Roles [Multi-Valued]
Groups [Multi-Valued]

6. Click **Create Reconciliation Profile**. This copies changes made to the resource object into the MDS.

4.2.3 Creating Reconciliation Field Mapping

To create a reconciliation field mapping for the new attribute in the process definition, perform the following procedure:

1. Expand **Process Management**, and double-click **Process Definition**.
2. Search for and open either the **RSA Auth Manager User** or the **RSA Auth Manager Token** process definition.
3. On the **Reconciliation Field Mappings** tab of the **RSA Auth Manager User** process definition, click **Add Field Map**.
4. From the **Field Name** list, select the field that you want to map.
5. Double-click the **Process Data Field** field, and then select the column for the attribute. For example, select **UD_AMUSER_EMAIL**.
6. 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

- Account Expire Hours [String] = UD_AMUSER_ACCOUNT_EXPIRE_HRS
- User ID [String] = UD_AMUSER_USER_ID
- IT Resource Name [IT Resource] = UD_AMUSER_ITRESOURCE, <KEY>
- Certificate DN [String] = UD_AMUSER_CERTIFICATE_DN
- Security Domain [String] = UD_AMUSER_SECURITY_DOMAIN
- Default Shell [String] = UD_AMUSER_DEFAULT_SHELL
- Identity Source [String] = UD_AMUSER_IDENTITY_SOURCE
- Account Start Minutes [String] = UD_AMUSER_ACCNT_START_MINUTES
- Account Start Hours [String] = UD_AMUSER_ACCOUNT_START_HOURS
- Last Name [String] = UD_AMUSER_LAST_NAME
- Account Expire Date [Date] = UD_AMUSER_ACCOUNT_EXPIRE_DATE
- Account Start Date [Date] = UD_AMUSER_ACCOUNT_START_DATE
- Fixed Passcode Allowed [String] = UD_AMUSER_FXD_PASSCODE_ALLOW
- Middle Name [String] = UD_AMUSER_MIDDLE_NAME
- Account Expire Minutes [String] = UD_AMUSER_ACCNT_EXPIRE_MINS
- EMAIL [String] = UD_AMUSER_EMAIL
- Roles [Multi-Valued] = Table UD_AMROLE
- Groups [Multi-Valued] = Table UD_AMGROUP

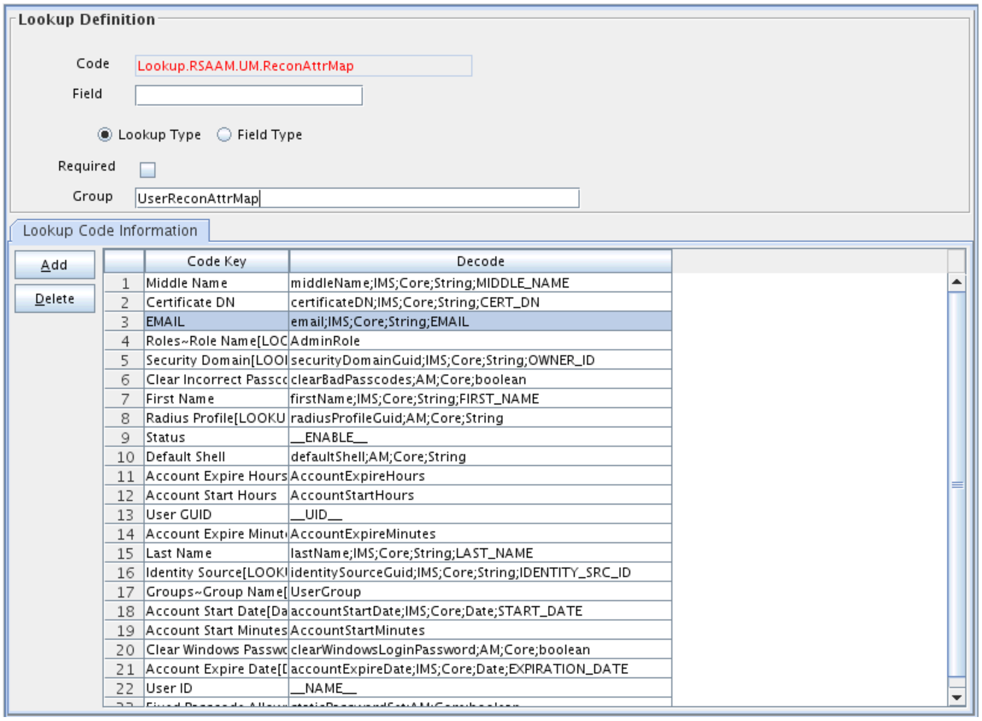
4.2.4 Creating Entries in Lookup Definitions

To create an entry for the field in the lookup definition that holds attribute mappings for reconciliation, perform the following procedure:

1. Expand **Administration**.
2. Double-click **Lookup Definition.**
3. Search for and open one of the following lookup definitions:
   - For Users: **Lookup.RSAAM.UM.ReconAttrMap**
   - For Tokens: **Lookup.RSAAM.Token.ReconAttrMap**
4. 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.

   See User Fields for Target Resource Reconciliation for information about the Decode format for users.

   See Token Fields for Target Resource Reconciliation for information about the Decode format for tokens.
5. Click the Save icon. The following screenshot shows the entry added to the lookup definition:



Lookup Definition

Code: Lookup.RSAAM.UM.ReconAttrMap

Field:

● Lookup Type ○ Field Type

Required □

Group: UserReconAttrMap

Lookup Code Information

	Code Key	Decode
1	Middle Name	middleName;IMS;Core;String;MIDDLE_NAME
2	Certificate DN	certificateDN;IMS;Core;String;CERT_DN
3	EMAIL	email;IMS;Core;String;EMAIL
4	Roles~Role Name[LOC	AdminRole
5	Security Domain[LOOI	securityDomainGuid;IMS;Core;String;OWNER_ID
6	Clear Incorrect Passcc	clearBadPasscodes;AM;Core;boolean
7	First Name	firstName;IMS;Core;String;FIRST_NAME
8	Radius Profile[LOOKU	radiusProfileGuid;AM;Core;String
9	Status	__ENABLE__
10	Default Shell	defaultShell;AM;Core;String
11	Account Expire Hours	AccountExpireHours
12	Account Start Hours	AccountStartHours
13	User GUID	__UID__
14	Account Expire Minut	AccountExpireMinutes
15	Last Name	lastName;IMS;Core;String;LAST_NAME
16	Identity Source[LOOKI	identitySourceGuid;IMS;Core;String;IDENTITY_SRC_ID
17	Groups~Group Name[	UserGroup
18	Account Start Date[Da	accountStartDate;IMS;Core;Date;START_DATE
19	Account Start Minutes	AccountStartMinutes
20	Clear Windows Passwc	clearWindowsLoginPassword;AM;Core;boolean
21	Account Expire Date[D	accountExpireDate;IMS;Core;Date;EXPIRATION_DATE
22	User ID	__NAME__
23	Fixed Passcode Allow	staticPasswordSet;AM;Core;boolean

4.2.5 Performing Changes in a New UI Form

You must replicate all changes made to the Form Designer of the Design Console in a new UI form.

1. Log in to Oracle Identity System Administration.
2. Create and activate a sandbox. See Creating a Sandbox and Activating and Deactivating a Sandbox in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager.*
3. Create a new UI form to view the newly added field along with the rest of the fields. See Creating Forms By Using the Form Designer in *Oracle Fusion Middleware Administering Oracle Identity Manager.*
4. Associate the newly created UI form with the application instance of your target system. To do so, open the existing application instance for your resource, from the Form field, select the form, and then save the application instance.
5. Publish the sandbox. See Publishing a Sandbox in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager.*

4.3 Adding New User or Token Attributes for Provisioning

You can add new user or token attributes for reconciliation. By default, the attributes listed in Table 1-10 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.

This information is divided across the following sections:

- Adding New Attributes
- Creating Entries in Lookup Definitions
- Creating a Task to Enable Update
- Performing Changes in a New UI Form

4.3.1 Adding New Attributes

To add a new attribute on the process form, perform the following procedure:

> **Note:**
>
> If you have already added an attribute for reconciliation, then you need not repeat steps performed here.

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 EMAIL field, enter `UD_AMUSER_EMAIL` 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:

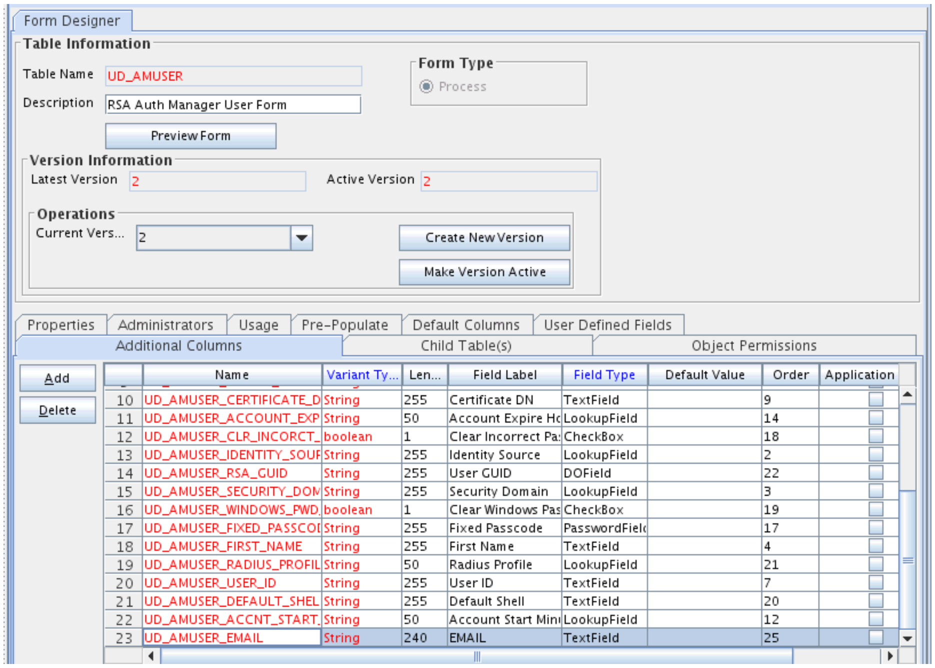


Table Information

Table Name: UD_AMUSER

Description: RSA Auth Manager User Form

Form Type: ● Process

Version Information

Latest Version: 2

Active Version: 2

Operations

Current Vers...: 2

	Name	Variant Ty...	Len...	Field Label	Field Type	Default Value	Order	Application
10	UD_AMUSER_CERTIFICATE_D	String	255	Certificate DN	TextField		9	□
11	UD_AMUSER_ACCOUNT_EXP	String	50	Account Expire Hc	LookupField		14	□
12	UD_AMUSER_CLR_INCORCT_	boolean	1	Clear Incorrect Pa:	CheckBox		18	□
13	UD_AMUSER_IDENTITY_SOUF	String	255	Identity Source	LookupField		2	□
14	UD_AMUSER_RSA_GUID	String	255	User GUID	DOField		22	□
15	UD_AMUSER_SECURITY_DOM	String	255	Security Domain	LookupField		3	□
16	UD_AMUSER_WINDOWS_PWD.	boolean	1	Clear Windows Pas	CheckBox		19	□
17	UD_AMUSER_FIXED_PASSCOI	String	255	Fixed Passcode	PasswordFielc		17	□
18	UD_AMUSER_FIRST_NAME	String	255	First Name	TextField		4	□
19	UD_AMUSER_RADIUS_PROFIL	String	50	Radius Profile	LookupField		21	□
20	UD_AMUSER_USER_ID	String	255	User ID	TextField		7	□
21	UD_AMUSER_DEFAULT_SHEL	String	255	Default Shell	TextField		20	□
22	UD_AMUSER_ACCNT_START_	String	50	Account Start Mini	LookupField		12	□
23	UD_AMUSER_EMAIL	String	240	EMAIL	TextField		25	□

4.3.2 Creating Entries in Lookup Definitions

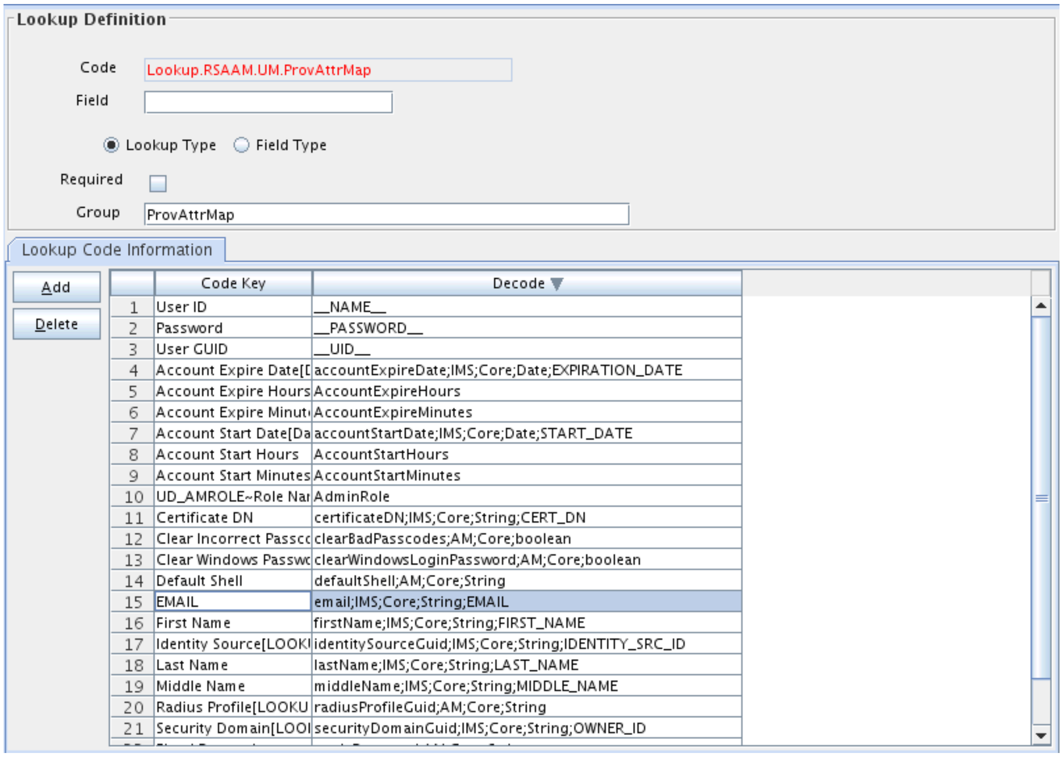
To create an entry for the attribute in the lookup definition that holds attribute mappings for provisioning, perform the following procedure:

1. Expand **Administration.**
2. Double-click **Lookup Definition.**
3. Search for and open one of the following lookup definitions:
   - For Users: **Lookup.RSAAM.UM.ProvAttrMap**
   - For Tokens: **Lookup.RSAAM.Token.ProvAttrMap**
4. Click **Add** and then enter the Code Key and Decode values for the attribute. Enter the Decode value in one of the following format:

   See User Fields for Provisioning for more information about the Decode format for users.

   See Token Fields for Provisioning for more information about the Decode format for tokens.

   For example, enter `EMAIL` in the **Code Key** column and then enter `email;IMS;Core;String;EMAIL` in the **Decode** column. The following screenshot shows the entry added to the lookup definition:



Lookup Definition

Code	Lookup.RSAAM.UM.ProvAttrMap
Field	
	● Lookup Type ○ Field Type
Required	□
Group	ProvAttrMap

Lookup Code Information

	Code Key	Decode
1	User ID	__NAME__
2	Password	__PASSWORD__
3	User GUID	__UID__
4	Account Expire Date[I	accountExpireDate;IMS;Core;Date;EXPIRATION_DATE
5	Account Expire Hours	AccountExpireHours
6	Account Expire Minut	AccountExpireMinutes
7	Account Start Date[Da	accountStartDate;IMS;Core;Date;START_DATE
8	Account Start Hours	AccountStartHours
9	Account Start Minutes	AccountStartMinutes
10	UD_AMROLE~Role Nar	AdminRole
11	Certificate DN	certificateDN;IMS;Core;String;CERT_DN
12	Clear Incorrect Passcc	clearBadPasscodes;AM;Core;boolean
13	Clear Windows Passwc	clearWindowsLoginPassword;AM;Core;boolean
14	Default Shell	defaultShell;AM;Core;String
15	EMAIL	email;IMS;Core;String;EMAIL
16	First Name	firstName;IMS;Core;String;FIRST_NAME
17	Identity Source[LOOKI	identitySourceGuid;IMS;Core;String;IDENTITY_SRC_ID
18	Last Name	lastName;IMS;Core;String;LAST_NAME
19	Middle Name	middleName;IMS;Core;String;MIDDLE_NAME
20	Radius Profile[LOOKU	radiusProfileGuid;AM;Core;String
21	Security Domain[LOOI	securityDomainGuid;IMS;Core;String;OWNER_ID

4.3.3 Creating a Task to Enable Update

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:

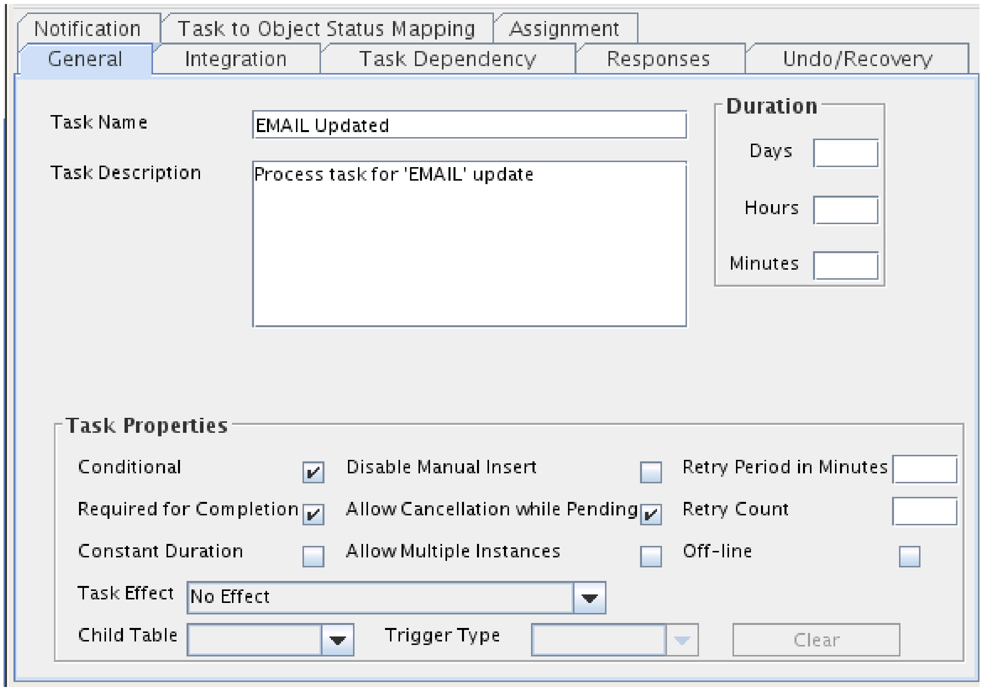
1. Expand **Process Management**, and double-click **Process Definition**.
2. Search for and open either the **RSA Auth Manager User** or the **RSA Auth Manager Token** process definition.
3. Click **Add**.
4. On the General tab of the Creating New Task dialog box, enter a name and description for the task and then select the following:

   Conditional

   Required for Completion

   Allow Cancellation while Pending

   Allow Multiple Instances
5. Click the Save icon. The following screenshot shows the new task added to the process definition:



Task Name: EMAIL Updated

Task Description: Process task for 'EMAIL' update

Duration

Days:

Hours:

Minutes:

Task Properties

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

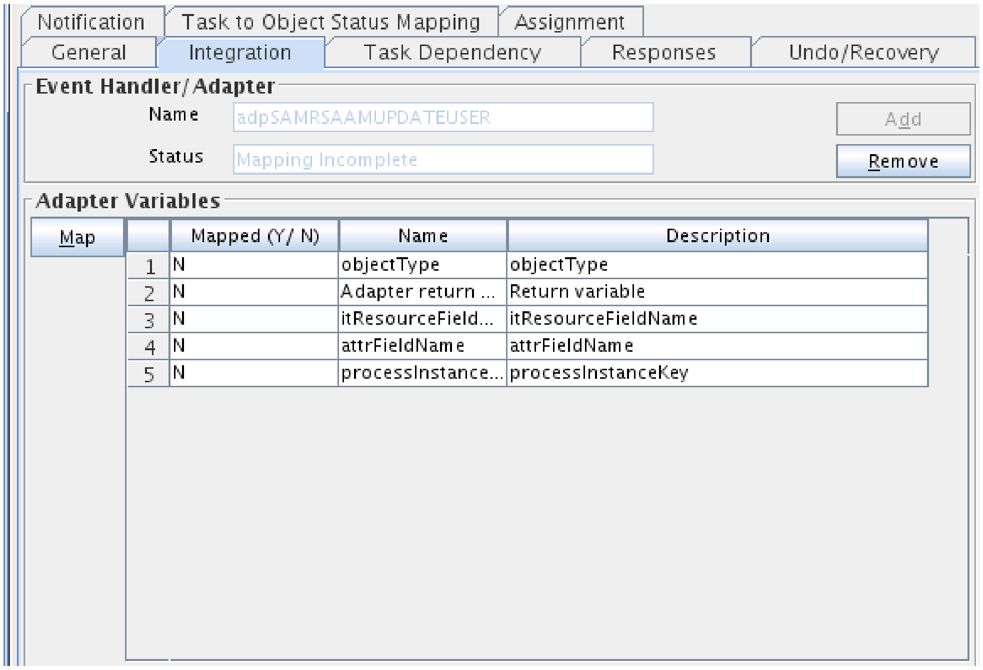
Task Effect: No Effect

Child Table:

Trigger Type:

6. On the Integration tab of the Creating New Task dialog box, click **Add**.
7. 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:



Event Handler/Adapter

Name: adpSAMRSAAMUPDATEUSER

Status: Mapping Incomplete

Adapter Variables

	Mapped (Y/N)	Name	Description
1	N	objectType	objectType
2	N	Adapter return ...	Return variable
3	N	itResourceField...	itResourceFieldName
4	N	attrFieldName	attrFieldName
5	N	processInstance...	processInstanceKey

8. 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: ParentFormProcessInstanceKey

Map To: Process Data

Qualifier: Process Instance

Click the Save icon.

9. To create mappings for the remaining adapter variables, use the data given in the following table:

Variable Name	Data Type	Map To	Qualifier	Literal Value
Adapter return value	Object	Response Code	NA	NA
attributeFieldName	String	Literal	String	EMAIL
itResourceFieldName	String	Literal	String	UD_AMUSER_ITRESOURCE
objectType	String	Literal	String	User
processInstanceKey	Long	Process Data	Process Instance	NA

10. Click the Save icon in the Editing Task dialog box, and then close the dialog box.
11. Click the Save icon to save changes to the process definition.

4.3.4 Performing Changes in a New UI Form

To perform all changes made to the Form Designer of the Design Console in a new UI form, perform the following procedure:

1. Log in to Oracle Identity System Administration.
2. Create and activate a sandbox. See Creating and Activating a Sandbox for more information.
3. Create a new UI form to view the newly added field along with the rest of the fields. See Creating a New UI Form for more information about creating a UI form.
4. Associate the newly created UI form with the application instance of your target system. To do so, open the existing application instance for your resource, from the Form field, select the form (created in Step 5.c), and then save the application instance.
5. Publish the sandbox. See Publishing a Sandbox for more information.

4.4 Configuring Validation of Data During Reconciliation and Provisioning

You can configure validation of reconciled and provisioned single-valued 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 number sign (#). In addition, you can validate data entered in the First Name field on the process form so that the number sign (#) is not sent to the target system during provisioning operations.

To configure validation of data:

1. Write code that implements the required validation logic in a Java class.

   The following sample validation class checks if the value in the First Name attribute contains the number sign (#):

```
package org.identityconnectors.rsaam.extension;
import java.util.*;
public class RSAAMValidator {

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;
        }
      } /* End */
```

2. Create a JAR file to hold the Java class.

3. Run the Oracle Identity Manager Upload JARs utility to post the JAR file created in Step 2 to the Oracle Identity Manager database. This utility is copied into the following location when you install Oracle Identity Manager:

   > **Note:**
   >
   > Before you use 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:**
>
> Upload JAR Utility in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*

4. If you created the Java class for validating a process form field for reconciliation, then:
   a. Log in to the Design Console.
   b. Create a lookup definition named **Lookup.RSAAM.UM.ReconValidation.**
   c. In the Code Key column, enter the resource object field name that you want to validate. For example, `Firstname`. In the Decode column, enter the class name. For example, `org.identityconnectors.rsaam.extension.RSAAMValidator`.
   d. Save the changes to the lookup definition.
   e. Search for and open the **Lookup.RSAAM.UM.Configuration** lookup definition.
   f. In the Code Key column, enter `Recon Validation Lookup`. In the Decode column, enter `Lookup.RSAAM.UM.ReconValidation`.
   g. Save the changes to the lookup definition.
5. If you created the Java class for validating a process form field for provisioning, then:
   a. Log in to the Design Console.
   b. Create a lookup definition by the name **Lookup.RSAAM.UM.ProvValidation.**
   c. In the Code Key column, enter the process form field label. For example, `Firstname`. In the Decode column, enter the class name. For example, `org.identityconnectors.rsaam.extension.RSAAMValidator`.
   d. Save the changes to the lookup definition.
   e. Search for and open the **Lookup.RSAAM.UM.Configuration** lookup definition.
   f. In the Code Key column, enter `Provisioning Validation Lookup`. In the Decode column, enter `Lookup.RSAAM.UM.ProvValidation`.
   g. Save the changes to the lookup definition.
6. Purge the cache to get the changes reflected in Oracle Identity Manager. See Purging Cache in *Oracle Fusion Middleware Administering Oracle Identity Manager*.

4.5 Configuring Transformation of Data During Reconciliation

> **Note:**
>
> This section describes an optional procedure. Perform this procedure only if you want to configure transformation of data during reconciliation.

You can configure the transformation of reconciled single-valued data according to your requirements. For example, you can append the domain name with the User ID.

To configure the transformation of data:

1. Write code that implements the required transformation logic in a Java class.

   This transformation class must implement the transform method. The following sample transformation class modifies the User ID attribute by using values fetched from the __NAME__ attribute of the target system:

   ```
   pacakge oracle.iam.connectors.rsaam;
   import java.util.HashMap;
   public class RSAAMTransformation {
   public Object transform(HashMap hmUserDetails, HashMap
   hmEntitlementDetails, String sField) throws ConnectorException {
         /*
         * 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 sUserName = (String) hmUserDetails.get("__NAME__");
           return sUserName + "@example.com";
           }
   }
   ```

2. Create a JAR file to hold the Java class.

3. Run the Oracle Identity Manager Upload JARs utility to post the JAR file created in Step 2 to the Oracle Identity Manager database. This utility is copied into the following location when you install Oracle Identity Manager:

   > **Note:**
   >
   > Before you use 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:**
   >
   > Upload JAR Utility in *Oracle Fusion Middleware Developing and Customizing Applications with Oracle Identity Manager*

4. Create a new lookup definition by the name **Lookup.RSAAM.UM.ReconTransformations** and then add the following entry:

   a. Log in to the Design Console.

b. Expand **Administration,** and then double-click **Lookup Definition.**

c. In the Code field, enter `Lookup.RSAAM.UM.ReconTransformations` as the name of the lookup definition.

d. Select the **Lookup Type** option.

e. On the Lookup Code Information tab, click **Add.**

f. In the **Code Key** column, enter the resource object field name on which you want to apply the transformation. For example: `User ID`.

g. In the **Decode** column, enter the name of the class file. For example: `oracle.iam.connectors.rsaam.RSAAMTransformation`.

h. Save the lookup definition.

5. Purge the cache to get the changes reflected in Oracle Identity Manager. See Purging Cache in *Oracle Fusion Middleware Administering Oracle Identity Manager*.

5

Troubleshooting the RSA Authentication Manager Connector

This chapter provides solutions to problems you might encounter after you deploy or while using the RSA Authentication Manager connector.

Table 5-1 provides solutions to problems you might encounter with the RSA Authentication Manager connector.

Table 5-1 Troubleshooting for the RSA Authentication Manager Connector

Problem	Solution
The following error message is encountered: `com.rsa.common.SystemException: Failed to construct CommandTarget`	Ensure that you are using the right port in the IT resource parameter. Generally, the port used to access the RSA UI and the port used in the IT resource are different.
The following error message is encountered: `com.rsa.command.exception.InvalidArgumentException: Static password does not meet policy requirements`	Ensure that you are entering the passcode as per the policy defined in RSA Authentication Manager. Generally, the passcode should be between 4 to 8 characters, and should not contain any special characters.
The following error message is encountered: `com.rsa.command.exception.InvalidArgumentException: Password policy not satisfied`	Ensure that you enter the accurate password as per the policies specified in RSA Authentication Manager. The following are the predefined policies to set a password in the connector: • Require at least alphabetic characters • Require at least uppercase characters • Require at least lowercase characters • Require at least numeric characters • Require at least special characters
The following error message is encountered: `javax.naming.CommunicationException [Root exception is java.net.ConnectException: t3s://rsa.idc.oracle.com:7002: Destination unreachable; nested exception is: javax.net.ssl.SSLHandshakeException: General SSLEngine problem; No available router to destination]`	This exception is encountered because the RSA certificate is incorrectly imported, or imported to the incorrect keystore. It is observed that this problem occurs if you have imported the certificate into the wrong keystore. You can fix this issue by checking the Oracle Identity Manager server logs for the correct keystore, and reimporting the same into it.

Table 5-1 (Cont.) Troubleshooting for the RSA Authentication Manager Connector

Problem	Solution

The following error message is encountered:
`com.rsa.command.AuditedLocalizableSystemException:`
`COMMAND_EXECUTION_UNEXPECTED_ERROR`
	This exception is encountered because the <attributename> in the exception is not supported for filtering, but is being used as a filter. For supported attributes for filters, see .Limited Reconciliation

A

Files and Directories On the Installation Media

The contents of the connector installation media directory are described in Table A-1.

Table A-1 Files and Directories On the Installation Media

File in the Installation Media Directory	Description
bundle/org.identityconnectors.rsaam-1.0.1115.jar	This JAR file contains the connector bundle.
configuration/RSAAM-CI.xml	This XML file contains configuration information that is used during the connector installation process.
Files in the resources directory	Each of these resource bundles contains language-specific information that is used by the connector. During connector installation, these resource bundles are copied to the Oracle Identity Manager database. **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/RSAAM-ConnectorConfig.xml	This XML file contains definitions for the following connector components: • Resource objects • IT resource types • IT resource instance • Process forms • Process tasks and adapters • Process definition • Prepopulate rules • Lookup definitions • Reconciliation rules • Scheduled jobs