RSA Authentication Manager 7.1 Microsoft Active Directory Integration Guide

The Security Division of EMC

Contact Information

Go to the RSA corporate web site for regional Customer Support telephone and fax numbers**:** **www.rsa.com**

Trademarks

RSA and the RSA logo are registered trademarks of RSA Security Inc. in the United States and/or other countries. For the most up-to-date listing of RSA trademarks, go to **www.rsa.com/legal/trademarks_list.pdf**. EMC is a registered trademark of EMC Corporation. All other goods and/or services mentioned are trademarks of their respective companies.

License agreement

This software and the associated documentation are proprietary and confidential to RSA, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by RSA.

Third-party licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed in the **thirdpartylicenses.pdf** file.

Note on encryption technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Limit distribution of this document to trusted personnel.

RSA notice

The RC5™ Block Encryption Algorithm With Data-Dependent Rotations is protected by U.S. Patent #5,724,428 and #5,835,600.

June 2009

Contents

Preface 5
About This Guide 5
Getting Support and Service 5
Before You Call Customer Support 6

Chapter 1: Integrating Active Directory with RSA Authentication Manager 7
Identity Source Overview 7
How RSA Authentication Manager Uses LDAP 8
Mapping User Data 8
Configuring Read-Only and Read/Write Access 9
RSA Authentication Manager and LDAP Configurations 10
Runtime and Administrative Identity Sources 10
Failover LDAP Access 10

Chapter 2: Using Active Directory Global Catalogs and Domain Controllers as Identity Sources 13
Using Global Catalogs 13
Requirements for Using Global Catalogs with Restricted Authentication Agents 15
Using Domain Controllers 15
Using Global Catalogs and Domain Controllers in the Same Deployment 16

Chapter 3: Choosing an LDAP Administration Model for Your Deployment 17
LDAP Integration Models 17
Static LDAP Integration Model 18
Dynamic LDAP Integration Model 19

Chapter 4: Securing Your LDAP Connection with SSL 21
Using SSL with LDAP 21
Adding an SSL Certificate to RSA Authentication Manager 21
Obtaining the Root Signing Certificate 21
Importing the Certificate into RSA Authentication Manager 23

Chapter 5: Managing Users 25
Mapping User Attributes 26
Core Attributes 26
Custom Attributes 28
Moving Users 28
Deleting Users 30
Managing Duplicate Users 30
Managing Password Policies 31

Preface

About This Guide

This guide provides information on how to integrate Active Directory with RSA Authentication Manager 7.1. With this integration, you can use Active Directory as your source of user and user group information.

This guide includes the following topics:

RSA Authentication Manager and Active Directory Integration. Provides an overview of identity sources and how to use them to access user data from your LDAP.

Using Active Directory Global Catalogs and Domain Controllers as Identity Sources. Describes how to use Global Catalogs and domain controllers for processing authentication requests and administering users.

Choosing an LDAP Administration Model for Your Deployment. Describes the different ways in which you can integrate your LDAP with Authentication Manager.

Securing Your LDAP Connection with SSL. Describes how to use SSL with your LDAP and how to obtain the appropriate certificate.

Managing Users. Provides information about mapping user attributes to your LDAP, the various issues that can arise when moving or deleting users, how to manage duplicate users, and how to manage password policies.

For instructions on configuring an Active Directory identity source, see the *RSA Authentication Manager 7.1 Installation and Configuration Guide*.

Getting Support and Service

RSA SecurCare Online	**https://knowledge.rsasecurity.com**
Customer Support Information	**www.rsa.com/support**
RSA Secured Partner Solutions Directory	**www.rsa.com/rsasecured**

RSA SecurCare Online offers a knowledgebase that contains answers to common questions and solutions to known problems. It also offers information on new releases, important technical news, and software downloads.

The RSA Secured Partner Solutions Directory provides information about third-party hardware and software products that have been certified to work with RSA products. The directory includes Implementation Guides with step-by-step instructions and other information about interoperation of RSA products with these third-party products.

Before You Call Customer Support

Make sure you have access to the computer running the RSA Authentication Manager software.

Please have the following information available when you call:

- Your RSA License ID. You can find this number on your license distribution media, or in the RSA Security Console by clicking **Setup** > **Licenses** > **Status > View Installed Licenses**.
- The Authentication Manager software version number. You can find this in the RSA Security Console by clicking **Help > About RSA Security Console > See Software Version Information**.
- The names and versions of the third-party software products that support the Authentication Manager feature on which you are requesting support (operating system, data store, web server, and browser).
- The make and model of the machine on which the problem occurs.

1 Integrating Active Directory with RSA Authentication Manager

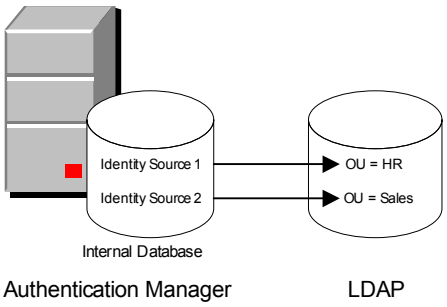
Identity Source Overview

If you use Active Directory as an LDAP directory to store user and user group data, you can integrate Active Directory with RSA Authentication Manager 7.1. After you integrate, you can use Active Directory as your authoritative source for user and user group data.

When you integrate your LDAP directory servers with Authentication Manager, they are called identity sources. To integrate Active Directory with Authentication Manager, you must create one or more identity sources for Active Directory within Authentication Manager. When you create an identity source, you provide Authentication Manager with the location of your user and user group data. The identity source acts as a search filter for your LDAP.

Note: Authentication Manager accesses the data in the LDAP, but by default does not alter the directory or the schema. If you grant Authentication Manager read/write access to your LDAP, Authentication Manager can alter the data but does not alter the schema. For more information, see the following section, "How RSA Authentication Manager Uses LDAP."

For example, assume you have an Active Directory with two OUs, Human Resources and Sales. In Authentication Manager, you can create one identity source for each OU. Each identity source references only the data within the specified OU.



You use the RSA Operations Console to create the identity sources for your LDAP. By default, you can add up to 30 identity sources to Authentication Manager. When you create your identity sources, remember:

- You can create more than one identity source for each LDAP. This enables you to control administrative granularity.

  For more information, see Chapter 3, "Choosing an LDAP Administration Model for Your Deployment."
- You can link each identity source to only one realm.

  For more information on realms, see the *RSA Authentication Manager 7.1 Administrator's Guide*.
- You can link multiple identity sources to the same realm.
- If you link multiple identity sources to the same realm, consider how to handle situations in which users with the same User ID exist in each identity source. If two users with the same User ID attempt to access the same protected resource, an authentication failure can result.

  For more information on duplicate users, see Chapter 5, "Managing Users."

How RSA Authentication Manager Uses LDAP

Authentication Manager queries your LDAP user data and uses it for administration and authentication.

User data that is specific to Authentication Manager, such as token assignments and PINs, is maintained in the Authentication Manager internal database, not in your LDAP. When you perform an operation on an end user, such as assigning a token, Authentication Manager creates a user record in the internal database. This record maps to the corresponding user record in your LDAP. When this happens, the user becomes a "managed user." By mapping the two user records, Authentication Manager can access and use the data stored in your LDAP.

Mapping User Data

When you add an identity source for your LDAP, you map the fields in your LDAP to fields in the Authentication Manager internal database. These fields are the core attributes, and this allows you to use the RSA Security Console to view user and user group data stored in your LDAP.

Note: If you grant Authentication Manager read/write access to your LDAP, you can alter LDAP data using the RSA Security Console. For more information on read/write access, see the following section, "Configuring Read-Only and Read/Write Access."

You can also define custom attributes, called identity attribute definitions, that contain information tailored to your organization. Identity attribute definitions are stored in the Authentication Manager internal database. By default, the attribute value is stored in the internal database. You can also map the identity attribute definition to a field in your LDAP.

For example, you can define an identity attribute definition named “Department” and enter a user’s department name in the internal database, for example, “HR” or “Finance.” You can also define an identity attribute definition called “user mobile phone” and map it to the “mobile” attribute in the LDAP directory.

There are two important things to note about user attributes:

- Core attribute mappings (those defined when adding an identity source) apply to that identity source only. Therefore, you can map each identity source differently.
- Identity attribute definitions are independent of a specific identity source. Therefore, they are available to all identity sources that have a mapping for that attribute.

For more information on mapping user attributes, see Chapter 5, “Managing Users.”

Configuring Read-Only and Read/Write Access

When you integrate Active Directory with Authentication Manager, you must indicate whether you want Authentication Manager to have read-only access or read/write access to the LDAP directory:

Read-only access. Authentication Manager only reads data from your LDAP directory. Your LDAP data can only be altered using an LDAP-specific administrative interface such as the Microsoft Management Console for Active Directory.

Note: Active Directory Global Catalogs are always read-only.

Read/write access. You can use the RSA Security Console to make changes to user and user group data stored in your LDAP. For example, you can change a user’s password in the RSA Security Console and that change is also made in the user’s LDAP record. You can also use the RSA Security Console to add, change, or remove users or user groups from your LDAP.

If your LDAP is read/write, and you use the RSA Security Console to make changes to your LDAP data, the changes are attributed to the administrator who was configured when you created the identity source.

In both cases, Authentication Manager data, such as token, realm, and security domain information, is stored in the internal database, and not in your LDAP.

RSA Authentication Manager and LDAP Configurations

Runtime and Administrative Identity Sources

To account for the architecture of an Active Directory forest, Authentication Manager recognizes two distinct types of identity sources:

Runtime identity source. An identity source configured for runtime operations only, to find and authenticate users, and to resolve group membership within the forest. If you use Active Directory Global Catalogs, you can configure the Global Catalogs to be runtime, but not administrative identity sources.

In this type of identity source, Authentication Manager uses the Global Catalog at runtime as another directory to find and authenticate users, and to resolve group membership within the forest.

Note: Global Catalogs and runtime identity sources are not a requirement for Authentication Manager. If you use a Global Catalog with Active Directory, you do not have to use it with Authentication Manager.

Administrative identity source. An identity source used for administrative operations such as adding users and groups. This identity source maps to a domain controller, and Active Directory replicates any domain changes to the Global Catalog.

Authentication Manager does not use the Global Catalog for administrative operations.

Note: If you create a runtime identity source, you must create at least one administrative identity source, and link it to the runtime identity source.

If you have a multidomain Active Directory forest, you can add a Global Catalog as a runtime identity source, and you can add the domain controllers as administrative and runtime identity sources.

For more information on using Global Catalogs and domain controllers, see Chapter 2, "Using Active Directory Global Catalogs and Domain Controllers as Identity Sources."

Failover LDAP Access

When you create an identity source, you specify the LDAP directory URL. You can also specify a failover directory URL. If you do not specify a failover URL and the primary connection to the LDAP server becomes unavailable, your users will not be able to authenticate. If you specify a failover URL, Authentication Manager establishes connections to the failover machine. Authentication Manager uses these connections until the primary server is available or the failover server becomes unavailable.

Note: Primary and failover LDAP URLs must be for machines in the same domain, containing the same user and user group data.

You can specify primary and failover LDAP URLs for your Authentication Manager primary instance and all replica instances in your deployment.

When specifying primary and failover LDAP URLs, remember:

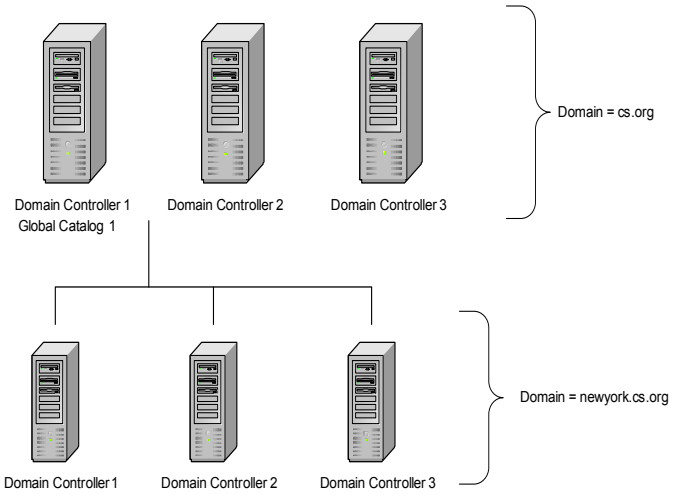
- RSA recommends that you connect your replica instances to separate, replicated LDAP servers, and that you do not connect all replica instances to the same LDAP server.

  For example, you might connect your replica instance to a replicated LDAP server that is geographically closer to your replica location. If you connect all of your replica instances to the same LDAP server and that server goes down, you may lose all your authentication services.
- If you add a replica instance after adding your identity sources, you must configure the LDAP connections information for the new replica instance.

2 Using Active Directory Global Catalogs and Domain Controllers as Identity Sources

An Active Directory deployment can have one or more Global Catalogs and one or more domain controllers.

The following figure shows a domain, cs.org, with three domain controllers, and a sub-domain, newyork.cs.org, with three domain controllers. There is also a Global Catalog associated with the first domain controller in cs.org.



When you integrate your Active Directory with RSA Authentication Manager, you can use your Global Catalog for runtime operations and your domain controllers for administrative operations.

Important: Be careful when you change your domain setup. Some changes may cause you to lose the user, token, and policy associations within Authentication Manager. For more information, see "Managing Users" on page 25.

Using Global Catalogs

When configured to do so, Authentication Manager uses the Global Catalog at runtime as another directory to find and authenticate users, and to resolve group membership within the forest. Authentication Manager does not use the Global Catalog for administrative operations.

Note: Global Catalogs are not a requirement for Authentication Manager.

The main benefit to using a Global Catalog as your runtime identity source is faster authentications. Because Global Catalogs contain data for all of the users in the forest, and because they are read-only, they result in more efficient authentications. However, because Global Catalogs are only partially replicated, you can see only a subset of user attributes.

In addition, Global Catalogs have some group limitations that affect how they behave with restricted authentication agents. For more information, see the following section, "Requirements for Using Global Catalogs with Restricted Authentication Agents."

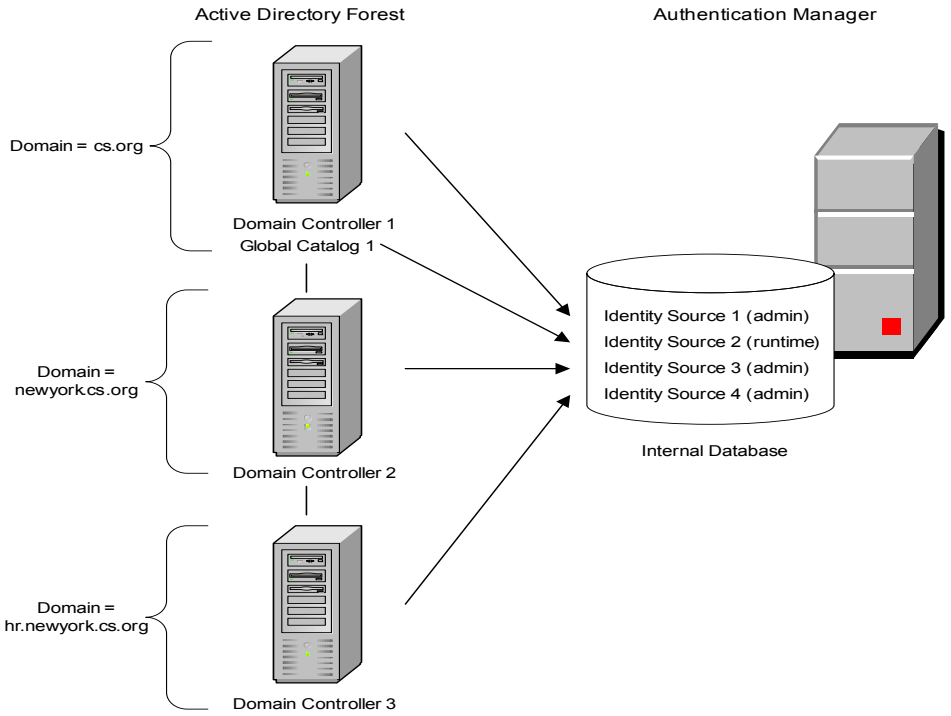
When you use the Active Directory Global Catalog as your runtime identity source, you must integrate the following with Authentication Manager:

The Global Catalog. If your forest has more than one Global Catalog, you can use one for failover. In this case, you do not need to create an identity source record for the additional Global Catalog. Instead, you can specify it as a failover URL when you create the identity source record for the first Global Catalog.

All domain controllers that replicate data to the Global Catalog. Each additional domain must be added as an administrative identity source.

The following figure shows a forest composed of three domains, each consisting of one domain controller, and a single Global Catalog. You must enable at least four identity sources in Authentication Manager:

- 3 administrative identity sources (domain controllers, possibly with failover domain controllers)
- 1 runtime source (Global Catalog, possibly with a failover Global Catalog server)



Requirements for Using Global Catalogs with Restricted Authentication Agents

Global Catalogs have group limitations that affect access to restricted authentication agents. The main issue is the group type used in Active Directory. When you authenticate using a Global Catalog, Authentication Manager only finds Universal group types when checking for groups. Access to restricted agents is dictated by group membership, so this is an issue if you use restricted agents and the group type is not found.

Note: When you use the RSA Security Console to view Active Directory groups, the Security Console displays all groups, regardless of type. If you select a group from this list to activate users on restricted agents, make sure you select a Universal group.

For example, if the restricted agent is looking for an Active Directory group and the group is the Global type (Active Directory groups are Global by default), authentication fails because Authentication Manager cannot find the group. If the group type is Universal, the authentication succeeds.

To use a Global Catalog as a runtime identity source with your restricted authentication agents, make sure all the users are in Universal groups. Remember:

- To use Universal groups, the entire forest must be composed of Windows 2003 domain controllers running in Windows 2003 native mode.
- If your Active Directory is read-only in Authentication Manager, only the Windows administrator can change the group type in Active Directory.
- If the Active Directory is read/write in Authentication Manager, you can use the RSA Security Console to change the group type.

Note: Global group membership data is only visible in its domain. Therefore, if you have a flat domain structure, group types do not need to be Universal because the Global Catalog and domain controllers contain the same user and user group data.

Using Domain Controllers

You can use your domain controllers as administrative or runtime identity sources. At runtime, they are used as another directory to find and authenticate users, and to resolve group membership within the forest. If Authentication Manager has read/write access to the identity source, you can also use your domain controllers for administration and managing user records.

Each domain controller in a domain contains all of the users and data in that domain. Administrators can see all of the data associated with each user, not just a subset as they would with a Global Catalog. However, Global Catalogs enable you to see all of the users within the entire forest, whereas domain controllers only allow you to see users in that domain.

Note: You must map each domain to its own identity source if you want to administer users in that domain.

Using Global Catalogs and Domain Controllers in the Same Deployment

In your Authentication Manager deployment, you may use a Global Catalog and domain controllers so that you have both runtime and administrative identity sources. When you use a Global Catalog with your domain controllers, your domain controllers replicate a subset of their data to the Global Catalog.

For example, suppose GC1 is the Global Catalog that you want to use as your runtime identity source, and DC1, DC2, and DC3 are domain controllers that you want to use as administrative identity sources. Authentication Manager accesses GC1 for authentication requests, and accesses DC1, DC2, and DC3 for all other administrative operations.

If you grant Authentication Manager read/write access to your LDAP, Authentication Manager makes all the administrative changes in DC1, DC2, and DC3, and reflects these changes in GC1.

Using a Global Catalog with your domain controllers offers these advantages:

- Using a Global Catalog as a runtime identity source allows Authentication Manager to access all the users in one identity source. This results in faster authentication requests, and makes it easier to apply permissions across an entire user population.
- Using your domain controllers as administrative identity sources allows you to create your identity sources according to your administrative needs. For example, you can create one identity source for each domain, or you can create more identity sources for greater administrative granularity.

For more information on the different ways you can set up and map identity sources to your LDAP, see Chapter 3, "Choosing an LDAP Administration Model for Your Deployment."

3 Choosing an LDAP Administration Model for Your Deployment

LDAP Integration Models

When you integrate your LDAP with RSA Authentication Manager, you can customize the way Authentication Manager accesses and groups your user data. You can create and define your identity sources to meet your administrative and organizational needs. For example, you can create one identity source and map it to your entire domain, or you can create a different identity source for each OU in your LDAP.

When you create an identity source, you specify the exact location where you want Authentication Manager to look for your user data. You do this by specifying the base DN when you create the identity source. For example, if you set the base DN to OU = Sales, that identity source includes objects only in the Sales OU and below.

Flexible identity source configurations allow you to:

Control administrative scope. Designate which administrators have access to certain user data. Using the example above, you can create an administrator whose scope is limited to the Sales identity source. That administrator can only see data in the Sales OU.

Group users and user groups within Authentication Manager for easier administration and access control. Organize users based on your administrative and business needs. For example, you can apply authentication policies based on how your users are organized.

Control user access. Grant or deny access to restricted agents based on LDAP user groups.

Do not create overlapping identity sources. A user cannot belong to more than one identity source. For example, make sure that two identity sources do not point to the same base DNs for user and group searches. For Active Directory, a runtime identity source has overlapping scope with the corresponding administrative sources, but two runtime identity sources cannot have overlapping scope.

While there are countless ways you can map identity sources to your LDAP, there are two main types of administration models:

Static LDAP Integration Model. This model allows more administrative granularity.

Dynamic LDAP Integration Model. This model allows more flexibility with moving users within your LDAP.

These models are described in the following sections.

Static LDAP Integration Model

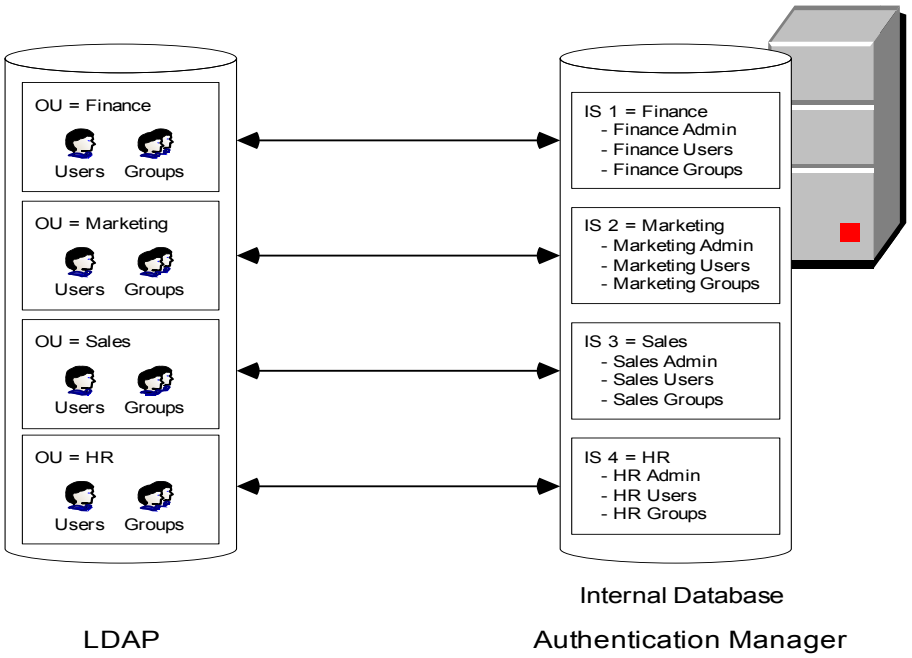
When you create your identity sources, you specify the base Distinguished Name (DN), which determines which users belong to the identity source. Because administrative duties can be assigned based on an identity source, your base DN can also affect how you administer users.

For example, you can specify a base DN at the top of your directory structure to create a broad user base within your identity source, or you can set a base DN to a specific OU for a smaller group of users. If you map your identity source to an OU, your identity source contains objects in that OU and below.

This type of model works well if you:

- Require more administrative scope and granularity.
- Do not plan on moving users within your directory.

For example, assume that you have an OU for each department in your company, and you create and map an identity source to each OU. You can designate a different administrator for each identity source. Each of these administrators has administrative scope over the OU mapped to his or her identity source. This allows you to designate administration more efficiently. The following figure shows this configuration.



When you add new users to an OU in your LDAP, those users are automatically visible in the appropriate identity source in Authentication Manager. For example, in the figure above, if you add a new user to the Finance OU, the Authentication Manager Finance administrator can administer that user.

If you use the static model, and you move users within your LDAP, you can experience problems. For more information on moving users within your LDAP, see "Moving Users" on page 28.

Dynamic LDAP Integration Model

You can also map your identity source to a larger group of users. For example, you can map an identity source to your entire domain. Because administrative duties can be assigned based on an identity source, you can create administrators who can administer users in your entire domain.

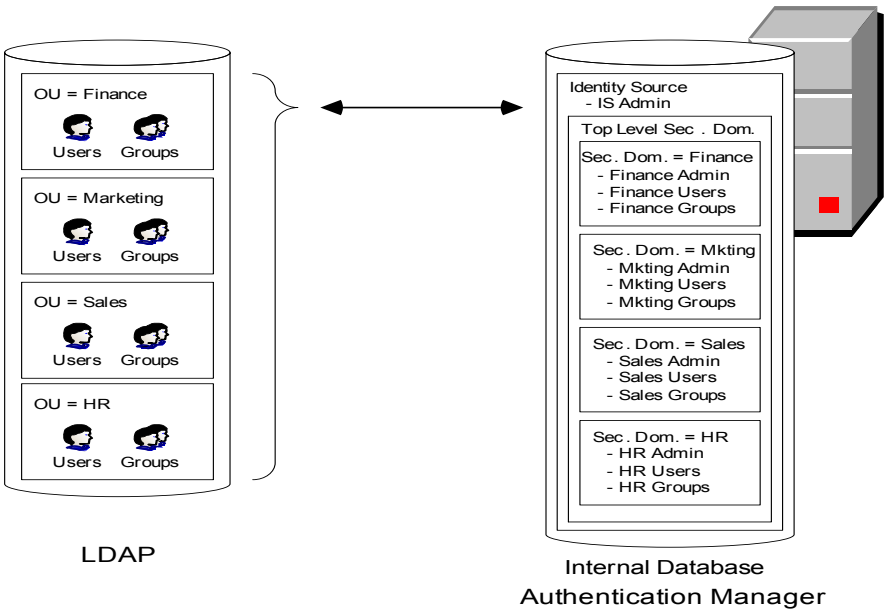
If you have this type of model, and you want to limit administrative scope, you can create security domains within your identity source. You can then create different administrative roles for your security domains.

This type of model works well if you:

- Do not require as much administrative scope and granularity.
- Plan on adding and moving users within your LDAP.

For example, assume that you have an OU for each department in your company, and you create one identity source that includes all of your OUs. An administrator for that identity source can administer the users and groups in all of those OUs.

If you want to limit administrative scope in this model, you can add a security domain for each OU, and then add the users for that OU to their respective security domain. You can designate a different administrator for each security domain, and each of these administrators has administrative scope over his or her security domain and its contents. The following figure shows this configuration.



When you add new users to an OU in your LDAP, those users are added in the default security domain for the identity source. If you create multiple security domains to create administrative flexibility, only administrators with the appropriate permissions can view the newly added user.

For example, in the previous figure, if you add a user to the Sales OU, the user is added to the default security domain in the identity source. The identity source administrator can view and administer this user, but the Sales administrator cannot. In order for the Sales administrator to administer the user, you must move the user to the Sales security domain.

4 Securing Your LDAP Connection with SSL

Using SSL with LDAP

If RSA Authentication Manager has read/write access to Active Directory, you must configure SSL on the connection before adding the identity source. Your LDAP directory server must already be configured for SSL connections and have access to the SSL root signing certificate.

Note: Configuring SSL is optional if Authentication Manager has read-only access to Active Directory.

For SSL-enabled identity sources, Authentication Manager uses an encrypted connection to communicate with the LDAP. Active Directory is configured to severely limit administrative operations performed over non-SSL connections. In addition, non-SSL LDAP potentially allows third parties to examine the logon IDs being used in the system.

Adding an SSL Certificate to RSA Authentication Manager

SSL enables you to establish a secure communication between Authentication Manager and your LDAP. When establishing an SSL connection, the LDAP presents a certificate that asserts the identity of the server (for example, it contains the hostname). To accept the server certificate as valid, Authentication Manager must trust either the certificate itself or its root certificate. For an SSL certificate to be trusted, you must add it to Authentication Manager by doing the following:

1. Obtain the root signing certificate from the domain controller.
2. Import the certificate into Authentication Manager.

Obtaining the Root Signing Certificate

You must perform these steps to obtain the root signing certificate:

1. Verify that SSL is enabled on Active Directory.
2. Export the certificate from the domain controller.

Verify That SSL Is Enabled on Active Directory

Before you begin, make sure you:

- Set up the Active Directory domain.
- Install and configure Authentication Manager on a Windows 2003 system.

- Install the Windows Certificate Authority (CA) Active Directory domain.

  Note: If you have RSA Certificate Manager installed, you can use it to perform these steps instead of the Windows Certificate Authority.

- Ensure that Windows Support Tools is installed on the Active Directory machine. The **suptools.msi** setup program is located in the **\Support\Tools** directory on your Microsoft Windows installation CD.

To verify that SSL is enabled on Active Directory:

1. On your Windows Domain Controller, click **Start > All Programs > Windows > Support Tools > Command Prompt**.
   a. At the command prompt, type:

      ```
      ldp
      ```

   b. Press ENTER.
2. From the LDAP window, click **Connection > Connect**.
   a. Enter the hostname and port number (636).
   b. Enable the SSL checkbox.
   c. Click **OK**.

If the connection is successful, you see a window containing information related to the Active Directory SSL connection.

If the connection is not successful, restart your system, and repeat the procedure above. If the connection is unsuccessful, it may be because the Certificate Authority (or RSA Certificate Manager) is not installed.

To install the Certificate Authority (CA):

1. Click **Start > Control Panel > Add or Remove Programs**.
2. Click **Add/Remove Windows Components**.
3. Select **Certificate Services**.
   Install the Certificate Services CA using the procedure provided. Use the **Enterprise CA** option.

Export the Root Signing Certificate

Once you have verified that SSL is enabled on Active Directory, you can export the root signing certificate from the domain controller.

Note: This procedure assumes you are using the Windows Certificate Authority. If you have the RSA Certificate Manager installed, see the product documentation.

To export the root signing certificate:

1. Log on to the Active Directory domain server as a Domain Administrator.
2. Open the CA Microsoft Management Console (MMC). Click **Start > Programs > Administrative Tools > Certificate Authority**.
   a. Highlight the CA machine.
   b. Right-click, and click **Properties**.
3. In the Properties window, select the **General** tab, and click **View Certificate**.
4. In the Certificates window, select the **Details** tab, and click **Copy to File**.
5. In the Certificate Export Wizard window, click **Next**.
6. Select **Base-64 Encoded X-509 (.CER)** as the export file format, and click **Next**.
7. Save the CA certificate to **C:\temp\win2003-ca.cer**, and click **Next**.
8. Click **Finish**, and then click **OK** to continue.

After exporting the certificate, you must import the certificate into Authentication Manager. For more information, see the following section, "Importing the Certificate into RSA Authentication Manager."

Importing the Certificate into RSA Authentication Manager

You must import the root signing certificate into Authentication Manager to secure the connection with your LDAP.

To import the SSL certificate:

1. Log on to the RSA Operations Console.
2. Click **Deployment Configuration > Certificates > Identity Source Certificates > Add New**.
3. Enter the **Certificate Name**.
4. Browse to the certificate location.

   Note: Certificates must have .cer, .pem, or .der file extensions.

5. Enter any **Notes**.
6. Click **Save**.

5 Managing Users

When you map an RSA Authentication Manager identity source to your LDAP directory, Authentication Manager accesses the user data directly from that directory. Your user data is not stored in the Authentication Manager internal database.

Once you use the RSA Security Console to perform an operation on an LDAP user, such as assigning a token, Authentication Manager creates a user record in the internal database. This user record maps to the user's LDAP record, and contains all of the Authentication Manager data associated with that user (for example, token assignments). Once Authentication Manager creates this internal database record, the user is called a "managed user."

Note: Users who are not yet managed users can exist only in the default security domain. When you move users to another security domain, they become managed users.

When you add an identity source to Authentication Manager, you specify the user attributes that Authentication Manager uses to map managed user records in the internal database to their corresponding LDAP user records. Because these user records are linked, you must be careful when performing the following tasks:

- Moving users in your LDAP
- Deleting users from your LDAP
- Managing duplicate users
- Managing password policies

This chapter provides more information on performing each of these tasks, as well as detailed information on mapping user attributes.

Note: For information on migrating users from RSA Authentication Manager 6.1, see the *RSA Authentication Manager 7.1 Migration Guide*.

Mapping User Attributes

To see the user and user group data in your LDAP, you must map the Authentication Manager fields to corresponding fields in your LDAP. These fields are called attributes. There are two types of user attributes:

Core Attributes. These include basic user attributes such as User ID, first name, and last name. You are required to map these when you create your identity source.

Custom Attributes. You can create your own custom attribute in Authentication Manager, and map it to a field in your LDAP. For example, you can create a custom attribute for a user's department.

Note: You can also include identity source attributes in RADIUS authentication responses. For example, you might include the "memberOf" attribute in RADIUS responses so that the authentication agent can change access rules based on group membership. For information, see the *RSA Authentication Manager 7.1 RADIUS Reference Guide*.

Core Attributes

Mapping the fields in your LDAP to the fields in Authentication Manager allows you to use the RSA Security Console to view user and user group data stored in your LDAP directory. For example, when you create an identity source, you map the Authentication Manager User ID field to the appropriate field within your LDAP.

You map core attributes when creating an identity source in the RSA Operations Console.

If your Active Directory identity source is read-only (the default), make sure that all user fields map to non-null fields. For example, User ID is mapped to samAccountName by default, but it can be mapped to any unique attribute for a user.

If your Active Directory identity source is read/write, make sure that you map all of the fields that you need when you add the identity source. If you do not map a field, the field remains blank when you add users. Active Directory does not provide any values for user's records for unmapped fields. There are some cases where it is necessary to create custom attributes in order to ensure that these fields are populated correctly. For more information, see "Custom Attributes" on page 28.

If you have multiple identity sources, try to map your attributes consistently. For example, if you map User ID to samAccountName in one identity source, do the same for your other identity sources.

Mapping a Unique Identifier

When you create your identity source and map the core attributes, you can map the Unique Identifier field, also known as an EXUID. This field helps Authentication Manager map internal database records to their corresponding LDAP records. The EXUID is an additional parameter that uniquely defines each user in your LDAP, and is very important if you move or rename users in your LDAP.

Important: If you move or rename users and have not mapped the EXUID field, you can lose all of the Authentication Manager data associated with those users. For more information on moving users, see "Moving Users" on page 28.

By default, the Unique Identifier field maps to the ObjectUID field in Active Directory.

When you map the EXUID, you can select the "Use as an additional attribute to uniquely identify users in the identity source directory" checkbox to make sure this attribute is used to identify your users.

Important: Once you have configured the Unique Identifier field mapping, you cannot change it.

Map the Unique Identifier field on the Add New Identity Source page in the RSA Operations Console. For more information, see the Help topic "Add LDAP-Based Identity Sources."

Enabling and Disabling User Access

The Enabled attribute reports the enabled or disabled state of a user's account in Authentication Manager, as controlled in the RSA Security Console. Unlike many other user attributes, you cannot alter the mapping of the Enabled attribute.

When you create an LDAP identity source in the RSA Operations Console, you can control how Authentication Manager determines whether a user is enabled for remote access. You can set the User Account Enabled State to Directory or to Internal Database.

- If you set User Account Enabled State to Directory, Authentication Manager consults only the user's enabled state in the LDAP directory.

  Use the Directory setting if you want LDAP alone to control whether a user is enabled in Authentication Manager. A user cannot be disabled in Authentication Manager without disabling the user in LDAP (that is, disabling the user's Windows Domain account in Active Directory).

  If the LDAP identity source is connected with read/write permissions, disabling the user in the RSA Security Console also disables the user's LDAP account.

- If you set User Account Enabled State to Internal Database, Authentication Manager consults both the user's enabled state in the LDAP directory and a separate enabled state in the Authentication Manager internal database.

  Use the Internal Database setting if you want to be able to disable the user in Authentication Manager, but allow the user to remain enabled in the LDAP. In this case, the user is not permitted to authenticate with Authentication Manager for remote access, but the user can still log on to Windows because the Windows Domain account remains enabled.

  If the LDAP identity source is connected with read/write permissions, disabling the user from the RSA Security Console does not affect the user's Windows Domain account.

Whichever settings you choose for User Account Enabled State, the user's account in LDAP must be enabled for the user to authenticate with Authentication Manager.

Custom Attributes

In addition to the core attributes, you can define custom attributes, called identity attribute definitions, that contain information tailored to your organization. You can map these custom attributes to your LDAP, which allows Authentication Manager to read these attribute values from the directory.

For example, you can create a custom attribute called "Department" in Authentication Manager, and map it to a field in your LDAP directory.

When you define a custom attribute, the attribute definition is stored in the Authentication Manager internal database. You can store the attribute value in the internal database, but it is not required.

There are some cases where it is necessary to create custom attributes in order to ensure that these fields are populated correctly. For example, when adding the identity source, if you mapped User ID to either the samAccountName or the userPrincipalName attribute, you must make sure both fields contain the correct data.

Use the RSA Security Console to create and map custom attributes.

Moving Users

There may be times when you need to move a user within your LDAP. When you move a user in Active Directory, the user's DN changes, but the ObjectUID (unique identifier/EXUID) does not. If you are using the unique identifier field as an additional attribute, Authentication Manager can use the unique identifier (EXUID) to locate the user and update the DN, as long as the move did not change the user's identity source in Authentication Manager.

Because an identity source maps to a location in the LDAP directory, it is possible that moving a user within your LDAP can result in the user changing identity sources within Authentication Manager.

For example, assume that you have configured Authentication Manager so that you have a different identity source for each OU in your directory. Now assume that you have a user "jdoe" in Finance (OU=Finance, DC=abc, DC=com). The user moves to the Marketing department (OU=Marketing, DC=abc, DC=com). In making that move, jdoe moves from the Finance identity source to the Marketing identity source.

If moving a user within you LDAP results in that user belonging to a different identity source in Authentication Manager, the following happens:

- User jdoe is deleted from the first identity source and created in the second identity source. When the user is deleted from the first identity source, all of the associated Authentication Manager data, such as token and policy information, is lost. The token is orphaned and assigned to an "unknown" user.

  To resolve this issue, run the orphaned users report and the identity source cleanup job. This removes the leftover records so that you can manage the user in the new identity source.

  Note: Moving the user back to his or her original identity source does not rebuild the lost data associations.

- Depending on how you have configured your administrators, you might have an administrator who can no longer manage the user.

  In the example above, if you have one administrator whose scope is limited to the Finance identity source, that administrator cannot manage jdoe once he is moved to the Marketing identity source.

- You cannot manage the user in the new identity source until you have used the identity source cleanup job to remove the user from the first identity source.

Important: You cannot use the RSA Security Console to move users between identity sources. Users are bound to their identity source, and you cannot move them.

Some administrative setups are more conducive to moving users. For more information on administrative models, see Chapter 3, "Choosing an LDAP Administration Model for Your Deployment."

Deleting Users

When you delete users and user groups from your LDAP directory, you can experience some issues within Authentication Manager. Here are two potential issues and their solutions:

- When a user or group is deleted from the LDAP, you cannot view the user through the RSA Security Console because the user is considered "orphaned." To remove orphaned users, run the orphaned data report. The report lists all of the users not found in the LDAP. The orphaned data report also shows all of the EXUIDs for users who are no longer associated with their original DNs. After running the orphaned data report, run the cleanup job to remove the orphaned user records from Authentication Manager.
- You cannot reassign tokens belonging to orphaned users because they belong to "unknown" users. To release the token so that it can be reassigned, you can:
  - Run the identity source cleanup.
  - Search for all tokens assigned to "unknown" and unassign them.

Managing Duplicate Users

You can have duplicate users in Authentication Manager if you have one or more of the following scenarios:

- You have multiple domains. For example, users are only unique based on the UPN and GUID in the domain. At your company, there may be a jdoe@abc.com and a jdoe@xyz.com. They are unique users based on data in your directory, but the logon ID in Authentication Manager is the same (jdoe).
- You have the same user in two identity sources. This causes problems in Authentication Manager. This scenario can occur if you set up overlapping identity sources (search scope is not unique). For example, if you set up an identity source for your entire domain, and then create another identity source that just maps to a specific OU, you have users that belong to both.

  For more information on configuring your identity sources for administration, see Chapter 3, "Choosing an LDAP Administration Model for Your Deployment."
- You deleted a user from your LDAP and then added the same user back to your LDAP.

Having duplicate users can result in authentication failures. For example, assume your deployment includes jdoe@abc.com and jdoe@xyz.com. These are two unique users in your LDAP. If you grant both of these users access to the same agents, authenticating failures can occur.

When the same User IDs are present in multiple identity sources, you have the following options:

- Map the User ID to another field where there are no duplicate values. For example, you might be able to map it to the Active Directory UPN field. For more information, see "Mapping User Attributes" on page 26.
- Create an alias within Authentication Manager that allows the user to log on under a different User ID. For more information on creating user aliases, see the *RSA Authentication Manager 7.1 Administrator's Guide.*
- Change one of the User IDs in your identity source so that the User IDs become unique. This option may not be practical if the User ID is used for other applications.
- Assign tokens to only one of the users with the non-unique User ID. This option is not practical if tokens must be assigned to more than one user with the non-unique User ID.

Managing Password Policies

Active Directory has a default password policy that is more strict than the default Authentication Manager password policy. This can lead to errors such as "Will Not Perform" when adding and updating users.

Note: This issue only exists when Authentication Manager has read/write access to Active Directory.

To manage password policies with Active Directory identity sources, do one of the following:

- Make the password requirements in your Authentication Manager password policy more strict. See the chapter "Preparing RSA Authentication Manager for Administration" in the *RSA Authentication Manager 7.1 Administrator's Guide.*
- Relax the complexity requirements in the Windows 2003 Group Policy Editor. For more information, see your Windows documentation.