

RSA Authentication Manager 7.1 Migration Guide



The Security Division of EMC

Contact Information

See 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 the Security Division of EMC 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.html](#) files.

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.]

Contents

Preface	11
About This Guide.....	11
RSA Authentication Manager Documentation	11
Related Documentation.....	12
Getting Support and Service	12
Before You Call Customer Support.....	12
Chapter 1: Important RSA Authentication Manager 7.1 Changes	13
Important Changes to Terms and Concepts	13
License Types and Options.....	16
Physical Architecture.....	17
The Replication Model	18
Logical Architecture	19
Realms	21
Security Domains.....	21
User Groups	23
Trusted Realms	26
Administrative Capabilities.....	30
Browser-Based Administration.....	31
Increased Administrative Scoping	31
Custom Administration Applications	36
Viewing Authentication Manager Activity in Real-Time	36
Reports.....	37
RSA RADIUS.....	38
Chapter 2: Planning For Migration	39
Hardware and Operating System Requirements	39
Linux System Requirements.....	41
Solaris System Requirements	43
Supported Data Stores	44
Internal Database	44
Identity Sources	44
Supported Browsers.....	44
Port Usage.....	45
Synchronizing Clocks	47
Planning Hardware to Handle Your Authentication Requirements.....	48
Configuring Your Browser to Support the RSA Authentication Manager	
Consoles.....	48
Enabling JavaScript	48
Adding the RSA Security Console to Trusted Sites	49
Logging On to the Consoles	49



- Pre-Migration Tasks..... 50
 - Pre-Migration Checklist for Windows..... 51
 - Pre-Migration Checklist for Solaris and Linux..... 52
- Choosing a Migration Path 55
 - Upgrading On the Same Hardware..... 55
 - Migrating to New Hardware 56
 - Understanding the Installation Methods..... 57
- RSA Authentication Manager Components..... 57
- Migrating Administrative Roles..... 58
 - Group Administrators 59
- Supporting Your Authentication Agents..... 59
 - Installed RSA Authentication Agents..... 59
 - Embedded Agents in Third-Party Hardware and Products..... 59
 - Customized Agents Created Using the Authentication API..... 60
- Planning Data Migration Options 60
 - Mapping LDAP Identity Sources 60
 - Planning How the Migration Handles Data Conflicts 61
 - Migrating Only a Subset of Your Data..... 62
 - Migrating Data to a Specific Security Domain..... 62
 - Converting Logon Names from NTLM to UPN..... 62
- Migrating Self-Service and Provisioning Data 63
- Planning a Test Migration..... 63
- Migration Planning Checklist 64
- Chapter 3: Migrating the Primary Server 65**
 - Installing the RSA Authentication Manager 7.1 Software 65
 - Mounting the Media on Linux 66
 - Mounting an ISO Image 66
 - Creating a RADIUS Migration Package File 67
 - Performing an Installation 68
 - Backing Up the Version 7.1 Database 72
 - Prerequisites..... 72
 - Performing the Backup 73
 - Dumping and Transferring Version 6.1 Data..... 73
 - Transferring Files..... 73
 - Dumping the Data 74
 - Exporting the LDAP Directory Certificates 75
 - Migrating Data Using the RSA Operations Console 76
 - Reviewing the Migration Report..... 77
 - Restoring the Database..... 77
 - Securing Backup Files 79
 - Migrating Log Files 80

Chapter 4: Migrating a Replica Server	81
Generating a Replica Package File	82
Transferring the Replica Package File	84
Dumping the Replica Server Database	84
Migrating the Replica Server	85
Performing the Replica Instance Installation.....	86
Attaching the Replica Instance	89
Migrating Delta Records from the Replica Instance	90
Rebalancing Contact Lists	90
Securing Backup Files	91
Chapter 5: Migrating a Standalone RSA RADIUS Server	93
Planning to Migrate a Standalone RSA RADIUS Server	93
Determining the Migration Path for RADIUS.....	93
RSA RADIUS System Requirements.....	94
RSA RADIUS and Firewalls	95
RSA RADIUS Access Planning	95
Specifying the RSA RADIUS Default Profile.....	95
Preparing to Migrate a Standalone RADIUS Primary Server.....	96
Creating an RSA RADIUS Package File.....	96
Copying the RSA RADIUS Package File.....	97
Migrating a Standalone RSA RADIUS Primary Server	97
Preparing to Migrate a Standalone RSA RADIUS Replica Server	100
Copying the RSA RADIUS Package File.....	100
Copying the RSA RADIUS Replica Package File	100
Migrating a Standalone RSA RADIUS Replica Server.....	101
Chapter 6: Planning User Self-Service and Token Provisioning	105
Overview of RSA Credential Manager	105
Licensing Options	105
RSA Self-Service Console	106
RSA Security Console	107
RSA Credential Manager Deployment Decisions	108
Deploying Self-Service.....	108
Deploying Provisioning	108
Implications of Read/Write or Read-Only Access.....	109
Planning the RSA Credential Manager User Experience	111
User Logon	111
User Enrollment.....	111
User Self-Service Troubleshooting	113
Planning Provisioning	115
Workflows	115
Select User Groups	116
Select Tokens	117

Token Distribution	118
E-mail Notifications.....	119
Emergency Access	120
RSA Self-Service Console Security and Disaster Recovery	120
Disaster Recovery for Users	121
Training for RSA Credential Manager Administrators and Users.....	122
RSA Credential Manager Summary	122
Chapter 7: Performing Post-Migration Tasks	125
Backing Up a Standalone Primary Instance.....	125
When To Perform a Backup	125
Backing Up a Standalone Primary Instance on Windows	126
Backing Up a Standalone Primary Instance on Linux and Solaris	127
Securing the Connection Between the Primary Instance and Replica Instances	127
Synchronizing Clocks	128
Starting and Stopping RSA Authentication Manager Services	128
Starting and Stopping RSA Authentication Manager Services	
on Windows	129
Starting and Stopping RSA Authentication Manager Services	
on Solaris and Linux	130
Configuring Your Browser to Support the RSA Authentication Manager	
Consoles.....	131
Enabling JavaScript	131
Adding the RSA Security Console to Trusted Sites	132
Logging On to the Consoles	132
Administering System Security	134
Managing Passwords and Keys	134
Managing Certificates and Keystores for SSL	136
Importing LDAP Certificates.....	136
Legacy Compatibility Keystore	137
Configuring Optional Proxy Servers for Remote Token-Key Generation	137
Adding a Proxy Server to Create Secure URLs.....	137
Configuring a Proxy Server for CT-KIP Failover	138
Configuring an Optional Proxy Server for Remote RSA Self-Service Console	
Access	138
Adding a Proxy Server for Secure RSA Self-Service Console Access	138
Configuring a Proxy Server for RSA Self-Service Console Failover	139
Integrating the RSA RADIUS Server into the Existing Deployment.....	140
Configuring the RADIUS Server on the Primary Instance.....	140
Migrating the RSA RADIUS 6.1 Data Files on the Primary Instance	141
Configuring the RADIUS Server on the Replica Instance	141
Editing the RADIUS Server Configuration Files	142
Using the RSA Security Console to Replicate Changes.....	142
Adding Clients to the RADIUS Server and Editing Clients.....	142

Testing RSA RADIUS Operation	143
Configuring Custom Port Numbers	143
Removing Authentication Manager 6.1	144
Chapter 8: Installing the RSA Authentication Manager	
MMC Extension	145
MMC Extension Overview	145
System Requirements and Prerequisite	145
Installation Process	146
Installing the MMC Extension for Local Access.....	146
Installing the MMC Extension for Remote Access	147
Post-Installation	148
Configuring Internet Explorer Security Settings	148
Starting the Active Directory User and Computer Management Console.....	149
Appendix A: Migration Data Conversion	151
Data Conversion Table.....	151
Migration Report.....	156
Multivalued Extension Data	156
Users in Multiple Groups in Different Sites	156
Groups Containing Users from Multiple Identity Sources	157
Activations on Restricted Agents When LDAP Synchronization Jobs	
Do Not Contain Group Data	157
PIN Options for Emergency Codes	158
Adding SecurID_Native as a Method of Administrator Authentication	158
Appendix B: Migration Scenarios	161
Scenario 1: Small Business, Single Site, Migration on Same Hardware.....	161
B & B Boxing (a single office location with 50 remote users).....	161
Scenario 2: Mid-Sized Business, Single Site, Multiple LDAP Synchronization Jobs ...	165
Middlewiz Media Corporation (2,500 Employees).....	165
Scenario 3: Large Enterprise, Multiple Geographic Sites, Multiple Realms.....	171
Meyecom Inc. (25,000 Employees).....	171
Appendix C: Integrating an LDAP Directory	181
Overview of LDAP Directory Integration	181
Integrating an LDAP Identity Source	181
Failover Directory Servers.....	184
Mapping Identity Attributes for Active Directory	184
Integrating Active Directory Forest Identity Sources	185
Preparing for LDAP Integration	186
Setting Up SSL for LDAP	186
Password Policy Considerations	187
Supporting Groups	187
Active Directory Forest Considerations	188

Adding an Identity Source	188
Linking an Identity Source to a Realm	192
Verifying the LDAP Identity Source	193
Appendix D: Troubleshooting	195
Accessing Installation Files on a Network	195
Unsuccessful Installation or Removal	196
DVD Read Errors	196
Installation Logs	196
Viewing Installation Logs	197
Unsuccessful Installation	197
Unsuccessful Removal	199
Reinstalling RSA Authentication Manager Components	199
Cleanup Script for Reinstallation (Windows Only)	199
Cleanup for Linux Systems	199
Obscured Error Messages	200
Server Does Not Start	200
RADIUS Server Does Not Start After Installation on a Windows Platform	200
RSA Security Console Does Not Start	200
Using the Collect Product Information Utility	200
MMC Extension Does Not Start	201
Message Indicates Node Manager Service Not Started	201
Test Authentication Between RSA RADIUS and RSA Authentication Manager	
Unsuccessful	202
Unsuccessful End-to-End Authentication on RSA RADIUS	202
The RSA Security Console Times Out When Searching for Users	202
Appendix E: Removing RSA Authentication Manager	205
Removing All RSA Authentication Manager Instances	205
Removing a Replica Instance	205
Rebalancing the Contact List	207
Removing the Primary Instance	207
Removing an RSA RADIUS Standalone Server	208
Appendix F: Reverting RSA Authentication Manager 7.1	
to Version 6.1	211
Reverting a Migration on the Same Hardware	211
Reverting a Migration to Different Hardware Using a Different Hostname	
and IP Address	212
Reverting a Migration to Different Hardware Using the Same Hostname	
and IP Address	213
Appendix G: RSA Authentication Manager 6.1 Command Line	
Utilities	215
Dumping the Database Using the Command Line	215
Dumping the Log Using the Command Line	216

Appendix H: Command Line Utilities	217
Overview	217
Collect Product Information Utility	219
Using the Collect Product Information Utility	219
Options for collect-product-info	220
Data Migration Utility	220
Using the Data Migration Utility	220
Options for migrate-amapp	221
Generating a Replica Package File	223
Manage Secrets Utility	224
Using the Manage Secrets Utility	225
Options for manage-secrets	227
Manage SSL Certificate Utility	228
Using the Manage SSL Certificate Utility	228
Options for manage-ssl-certificate	232
Glossary	235
Index	255

Preface

About This Guide

This guide is intended for administrators who are planning and implementing a migration of their RSA Authentication Manager deployment from version 6.1 to version 7.1.

RSA Authentication Manager Documentation

For more information about RSA Authentication Manager, see the following documentation:

Release Notes. Provides information about what is new and changed in this release, as well as workarounds for known issues.

Getting Started. Lists what the kit includes (all media, diskettes, licenses, and documentation), specifies the location of documentation on the DVD or download kit, and lists RSA Customer Support web sites.

Planning Guide. Provides a general understanding of RSA Authentication Manager, its high-level architecture, its features, and deployment information and suggestions.

Installation and Configuration Guide. Describes detailed procedures on how to install and configure RSA Authentication Manager.

Administrator's Guide. Provides information about how to administer users and security policy in RSA Authentication Manager.

Migration Guide. Provides information for users moving from RSA Authentication Manager 6.1 to RSA Authentication Manager 7.1, including changes to terminology and architecture, planning information, and installation procedures.

Developer's Guide. Provides information about developing custom programs using the RSA Authentication Manager application programming interfaces (APIs). Includes an overview of the APIs and Javadoc for Java APIs.

Performance and Scalability Guide. Provides information to help you tune your deployment for optimal performance.

RSA Security Console Help. Describes day-to-day administration tasks performed in the RSA Security Console. To view Help, click the **Help** tab in the Security Console.

RSA Operations Console Help. Describes configuration and setup tasks performed in the RSA Operations Console. To log on to the Operations Console, see "Logging On to the RSA Operations Console" in the *Administrator's Guide*.

RSA Self-Service Console Frequently Asked Questions. Provides answers to frequently asked questions about the RSA Self-Service Console, RSA SecurID two-factor authentication, and RSA SecurID tokens. To view the FAQ, on the **Help** tab in the Self-Service Console, click **Frequently Asked Questions**.

Note: To access the *Developer's Guide* or the *Performance and Scalability Guide*, go to <https://knowledge.rsasecurity.com>. You must have a service agreement to use this site.

Related Documentation

RADIUS Reference Guide. Describes the usage and settings for the initialization files, dictionary files, and configuration files used by RSA RADIUS.

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

Important RSA Authentication Manager 7.1 Changes

This chapter provides an overview of the differences between RSA Authentication Manager 6.1 and version 7.1.

- [Important Changes to Terms and Concepts](#)
- [License Types and Options](#)
- [Physical Architecture](#)
- [Logical Architecture](#)
- [Administrative Capabilities](#)

Important Changes to Terms and Concepts

The physical and logical architecture of the Authentication Manager has changed. The following table lists new terms introduced in version 7.0 or version 7.1 and maps old terminology to the new terminology.

Version 6.1 Term	Version 7.1 Term	Comment
Server	Instance	An instance is one physical installation of Authentication Manager acting as a single cohesive processing unit. In a single deployment, there can be a 1 primary instance and up to 15 replica instances. Each instance has a designated database server and can have multiple server nodes.

Version 6.1 Term	Version 7.1 Term	Comment
Realm	Realm	<p>In version, 7.1, a realm is a hierarchy of organizational units, called security domains, for administrative purposes. A realm includes all the objects that your administrators need to manage in Authentication Manager, including users, user groups, identity sources, tokens, policies, and more.</p> <p>In version 6.1, a realm is the physical installation of the primary Authentication Manager and its replica servers. While all objects exist within the realm, the organizational hierarchy follows a simpler model of realm, sites, and groups. Version 7.1 security domains can contain lower-level security domains and user groups. Version 6.1 sites exist at one level below the realm, and contain only groups or users, but never another site.</p>
Cross-realm	Trusted Realm	<p>In version 7.1, establishing a trusted realm relationship requires the delivery of a specific file called a trust package.</p>
Site	Security Domain	<p>Sites have been replaced with security domains. A security domain is an organizational container that defines an area of administrative management within a realm. Security domains can be organized in terms of business units, for example, departments or partners. They establish ownership and namespaces for objects (for example, users, roles, permissions, other security domains) within the system. Security domains are hierarchical.</p>
Group	User group	<p>User groups are equivalent to groups. The ability to activate a group on an agent host and control access times remains in version 7.1.</p>
User	User	<p>No change.</p>

Version 6.1 Term	Version 7.1 Term	Comment
Agent	Agent	<p>Agents no longer allow user activations, only group activations.</p> <p>You do not need to specify an agent type (such as UNIX agent or single-transaction server) when adding an agent.</p> <p>As part of the migration process, you can specify whether the IP address of a self-registered agent is maintained when the agent is migrated.</p>
Token	Token	<p>Version 7.1 introduces a new type of non-time synchronous, event-based token called an RSA SecurID Display Card. For more information, see the <i>Administrator's Guide</i>.</p>
Administrative roles	Administrative roles	<p>The scope and task lists of the Authentication Manager 6.1 default roles (realm, site, and group) are migrated. In version 7.1, you can create roles by defining a set of permissions. You then assign the role to an administrator. The scope of the role is defined by the security domain in which the role is created.</p>
Scope	Scope	<p>In version 6.1, the scope of an administrative role defines who the administrator can administer. For example, the administrator can be scoped to a realm, site, or group. In version 7.1, the ability to scope administrative roles to security domains greatly expands the flexibility of administration. With permissions and task lists, fine distinctions can be made.</p>

Version 6.1 Term	Version 7.1 Term	Comment
Task lists	Administrative roles	The default task lists (realm, site and group) are migrated to sets of administrative permissions called roles. Version 7.1 roles contain permissions that allow administrators to perform certain tasks. Version 6.1 custom task lists are migrated to roles that approximate the same administrative capabilities. Version 7.1 contains additional predefined roles. For more information, see “Predefined Administrative Roles” on page 35.
N/A	Identity source	The internal database or a specified LDAP directory. User and user group data can reside in either type of identity source. Product-specific data resides in the internal database.
LDAP synchronization job	N/A	Like version 6.1, version 7.1 enables you to use existing user and user group data. In version 7.1 however, the up-to-date LDAP data is accessed at runtime, rather than updated in the internal database by regularly scheduled or manually run LDAP synchronization jobs. As a result, the latest LDAP data is always available and always used to validate authentications.

License Types and Options

Each Authentication Manager installation has one or more software licenses associated with it. The license represents permission to use the Authentication Manager software. Your installation personnel need to understand how the license type impacts the installation of Authentication Manager. Review these license types and options with your installers:

Base Server. Allows up to two instances of Authentication Manager.

Enterprise Server. Allows up to 15 instances of Authentication Manager.

Each license type has a limit on the number of instances of Authentication Manager that can be installed and whether or not multiple realms are allowed. User limits are determined on an individual basis, based on the customer’s usage requirements.

For example, a customer with 10,000 employees may purchase a license for 11,000 users to accommodate current employees and to allow for future hiring.

The following table shows the attributes for each license type.

License Feature	Base Server	Enterprise Server
Number of users	Specified by customer at time of purchase	Specified by customer at time of purchase
Number of instances	2 ¹	15
Allows multiple realms?	No	Yes
Allows clusters?	No	Yes
RSA Credential Manager self-service	Yes	Yes
RSA Credential Manager provisioning	No	Yes
On-demand tokencode service	Optional	Optional
RADIUS	Yes	Yes
Business Continuity	Optional	Optional
Allows offline authentication?	Yes	Yes

¹Licenses with a two instance limit allow a third instance for disaster recovery situations.

Physical Architecture

In version 6.1, the primary server is the administrative server and contains the authoritative data source, the primary database. The primary server is responsible for:

- Administration of the database
- Replication of changes to the replica servers
- Authentication of users, optionally

In version 7.1, the primary instance is still able to perform these functions, but you can improve performance by installing the database on a dedicated machine (a database server). This reduces the burden on the primary instance of handling all runtime or authentication changes made by the server nodes.

The Replication Model

The replication model in version 7.1 remains the same as in version 6.1. The replica instances continue to provide the following benefits:

- Data recovery, and minimizing data loss in the event of a hardware disaster
In the event of a catastrophic failure of the primary instance, the version 6.1 disaster recovery procedures apply in version 7.1. Any disaster recovery plans you may have in place are still valid and only need to be refined to accommodate any new benefits of version 7.1. For more information, see the chapter “Disaster Recovery” in the *Administrator’s Guide*.
- Failover of administration
- Failover of authentication, allowing authentication to continue while the primary instance is offline

Note: You can now install 15 replica instances for each primary instance.

All changes that occur on a replica instance are replicated to the primary instance, which then replicates the changes to all other replica instances in the deployment.

Replication propagates two types of updates to the database:

Administrative Updates. You must perform all administrative changes, such as adding or deleting users, at the primary instance. The primary instance propagates the administrative changes to all replica instances.

Runtime Updates. Runtime changes, such as those resulting from user authentication, can be initiated at any primary or replica instance. If the runtime change occurs at a replica instance, the change is first propagated to the primary instance. The primary instance then propagates the change to all other replica instances.

The following table lists the runtime updates that can occur on a replica instance.

Object	Change That Is Replicated
User	Any change to the user’s fixed passcode or PIN.
Agent	<ul style="list-style-type: none"> • The creation of an agent through agent auto-registration. • Assignment of an agent to a contact list. • Updating a node secret.

Object	Change That Is Replicated
Token	<p>Any changes that occur as a result of the following activities:</p> <ul style="list-style-type: none"> • Authentication. • Token replacement, including disabling, unassigning and deleting an existing token, and assigning and enabling a replacement token. The exact changes that occur depend upon how you configure Authentication Manager to handle token replacement. See “Replacing Tokens” in the <i>Administrator’s Guide</i>. • Emergency passcode processing. • The distribution of offline authentication data to agents. • Seed initialization of a Software Toolbar Token.

Log data on a replica instance is not replicated in the same way as changes resulting from authentication. Log data is sent only to the primary instance, or to a designated centralized log. It is not replicated to all instances in your system.

Important: Any user or user group data that resides in an LDAP directory is not replicated by Authentication Manager. In a replicated LDAP environment, it is your responsibility to properly configure LDAP to replicate LDAP changes.

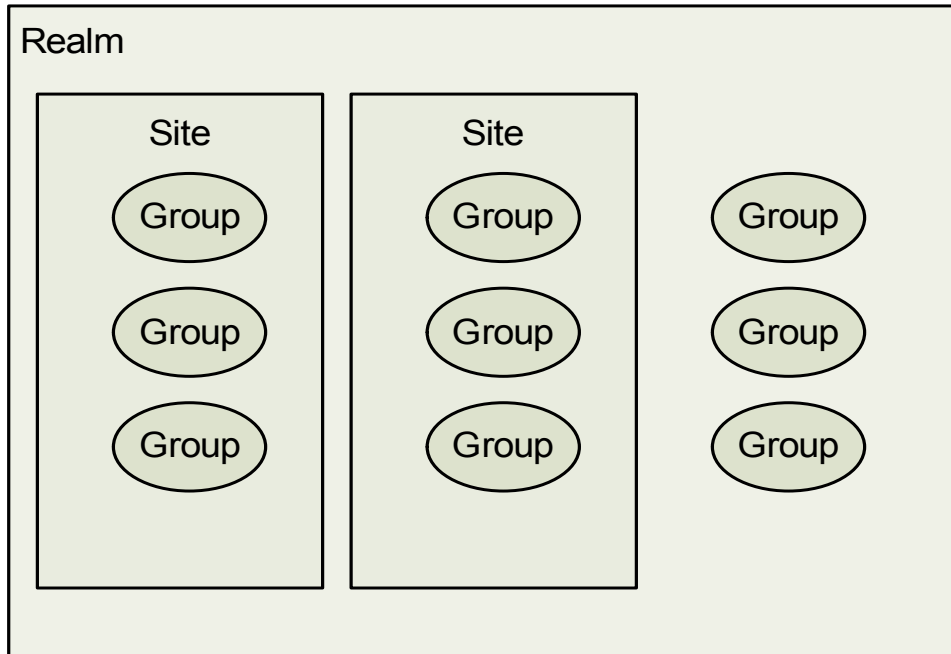
Logical Architecture

The logical architecture of version 6.1 is based on a hierarchy of realms, sites, and groups. A realm contains users, sites, and groups; a site contains users and groups; and a group contains users. Version 7.1 expands this strict hierarchy to allow multiple security domains to exist in a hierarchical chain: a single realm can contain multiple levels of security domains, user groups, and users; a security domain can contain multiple levels of security domains, user groups, and users; and user groups can contain other user groups and users.

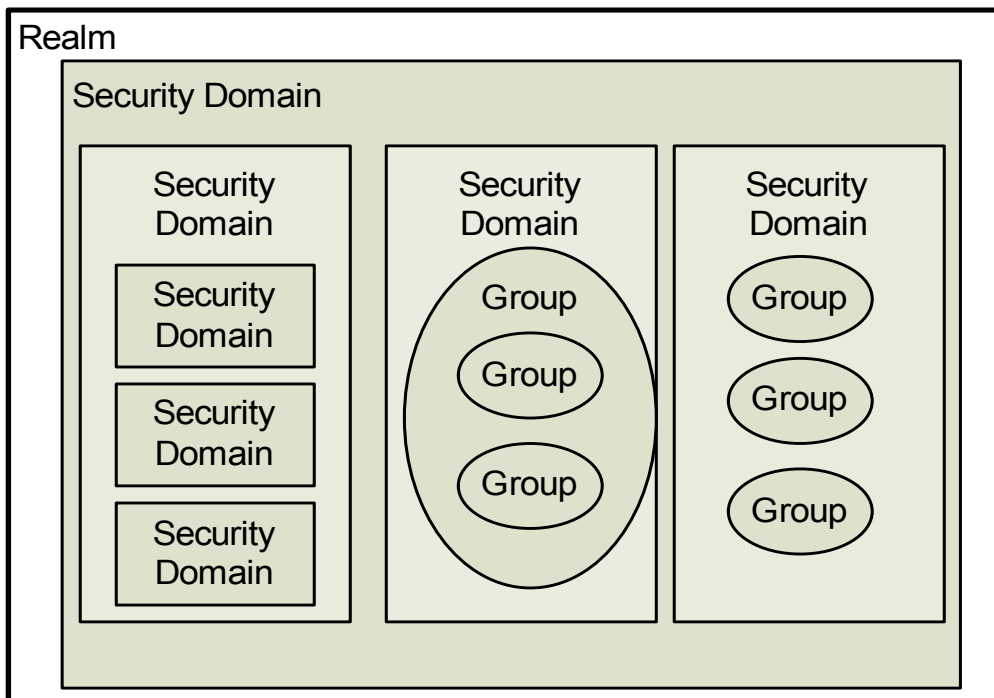
The following table lists the objects in the hierarchy and the names of the objects they may contain in version 6.1 and version 7.1.

Object	Version 6.1	Version 7.1
Realm	Sites Groups Users	Security domains User groups Users
Site (version 6.1) / Security domain (version 7.1)	Groups Users	Security domains User groups Users
Group	Users	User groups Users

The following figure shows the hierarchy of RSA Authentication Manager 6.1.



The following figure shows the hierarchy of RSA Authentication Manager 7.1.



Realms

A realm is an independent organizational unit that contains all objects in your deployment, such as users and user groups, administrative roles, tokens, and policies for passwords, lockout, and tokens.

When you install Authentication Manager, a default realm is automatically created. You can build your entire organizational hierarchy within this one realm, or you can create additional realms, either on the same machine as your original realm, or on separate machines. Realms function much as they did in version 6.1. For example:

- Each realm has its own set of users, user groups, tokens, authentication agents, and so on.
- You cannot transfer objects such as users, user groups, or tokens between realms.
- Users in one realm cannot use an authentication agent in another realm to authenticate unless a trust relationship (known as a cross-realm relationship in version 6.1) is in place.

For more information on trust relationships, see the *Administrator's Guide*.

Each realm may be associated with multiple identity sources, but each identity source may only be associated with a single realm.

Users and user groups managed by a realm are stored in identity sources. Such identity sources are:

- An external LDAP directory
- The Authentication Manager internal database

Administrators can manage only the realm in which their user record is stored. They cannot manage multiple realms. Super Admins are the only exception to this. Super Admins can manage all realms in the deployment.

If your organizational needs require you to move users, user groups, tokens, and other objects between organizational units—departments within your company, for example—create a security domain hierarchy, rather than multiple realms. Multiple security domains allow you more flexibility to reorganize your deployment than multiple realms.

Security Domains

Security domains are equivalent to sites in version 6.1. However, security domains can be nested, one within, or beneath another in the organizational hierarchy of your realm. Additionally, security domains are the only method available to scope administrators to grouped objects. You cannot scope administrators to groups. For more information on groups, see [“User Groups”](#) on page 23.

Security domains represent areas of administrative responsibility, typically business units, departments, partners, and so on. Security domains establish ownership and namespaces for objects (users, roles, permissions, and so on) within the system. All Authentication Manager objects are managed by a security domain. Security domains allow you to:

- Organize and manage your users.
- Enforce system policies.

- Delegate administration.
The extensive delegation capabilities of version 7.1 limit the scope of administrators' control by limiting the security domains to which they have access.

When a new realm is created—either automatically when you install Authentication Manager, or by an administrator—a top-level security domain is automatically created in the realm. The top-level security domain is assigned the same name as the realm.

By default, all users are managed in the top-level security domain. You can transfer users from the top-level security domain to other security domains within the realm.

For example, you can create separate security domains for each department, such as Finance, Research and Development (R&D), and Human Resources (HR), and then move users and user groups from each department into the corresponding security domain.

To manage users in a given security domain, an administrator must have permission to manage that security domain. Know the following about security domains:

- Security domains are organized in a hierarchy within a realm. Create as many security domains as your organization requires.
- Security domains are often created to mirror the departmental structure or the geographic locations of an organization.

Policies and Security Domains

You also use security domains to enforce system policies. Policies control various aspects of a user's interaction with Authentication Manager, such as RSA SecurID PIN lifetime and format, fixed passcode lifetime and format, password length, format, and frequency of change.

The following policies are assigned to security domains:

- Password policies
- Token policies
- Lockout policies
- Offline authentication policies
- Emergency authentication policies

For each security domain, you can use the default policy, or create a custom policy for each policy type. When you create a new security domain, the default policy is automatically assigned. You can optionally assign a custom policy to the new security domain. If you assign the default policy to a security domain, whatever policy designated as the default is automatically assigned to the security domain. When a new policy is designated as the default, the new default is automatically assigned to the security domain.

Note: The policy assigned to a lower-level security domain is not inherited from upper-level security domains. New security domains are assigned the default policy regardless of which policy is assigned to security domains above them in the hierarchy. For example, if the top-level security domain is assigned a custom policy, lower-level security domains are still assigned the default policy.

User Groups

The ability to create hierarchies of security domains has lessened the need for groups or user groups, as they are known in version 7.1. As a result, user groups no longer function as they did in version 6.1.

User groups have the following characteristics:

- They can be made up of one or more user groups.
- They can occur across security domains. This means that users in security domain A and users in security domain B can both be members of the same user group and thus access the same protected resources.

Note: Because any object in the realm (users, user groups, agents, and so on) can exist only in one security domain, you may encounter situations where the privileges of the administrators of the security domain, in which the group resides, do not allow them to see all members of the migrated group.

- A user can be a member of more than one user group.

You can create user groups through the RSA Security Console, or for external data sources such as Active Directory, using the directory user interface.

User Group Administration

In version 7.1, the ability to scope administrators to user groups is no longer available. Administrative control of groups is defined by the security domain in which the group resides, and not by any administrative scoping to the group, as was the case in version 6.1.

For example, if you migrate groups that do not belong to a site, they are migrated to the top-level security domain. The Super Admin has administrative control of this security domain. If your groups belong to a site, they are migrated to the lower-level security domain created for the migrated site. The administrator of the site, which is the administrator of the lower-level security domain, has control of this security domain.

User and User Group Activation on Agents

Version 7.1 maintains the ability to activate groups on restricted authentication agents and restrict access times for the group, but does not support individual user activation on agents. Because it is no longer possible to activate individual users on agents, migration uses group activations to maintain a similar behavior.

The following table describes the effect that migration has on groups activated on agents.

Pre-Migration	Post-Migration
Group activated with access time restrictions on a restricted agent	The group is migrated with access time restrictions and activated on the agent. The agent remains a restricted agent.
Group activated with no access time restrictions on a restricted agent	The group is migrated with no access time restrictions and activated on the agent. The agent remains a restricted agent.
Group activated with access time restrictions on an unrestricted agent	The group is migrated with access time restrictions and activated on the agent. The agent is migrated as a restricted agent. Note: As a result of converting an unrestricted agent to a restricted agent, users who are not activated on the agent (either directly or through membership in a group activated on the agent) will no longer be able to authenticate through the agent.
Group activated with no access time restrictions on an unrestricted agent	The group is migrated with no access time restrictions and activated on the agent. The agent is migrated as a restricted agent. Note: As a result of converting an unrestricted agent to a restricted agent, users who are not activated on the agent (either directly or through membership in a group activated on the agent) will no longer be able to authenticate through the agent.

The following table describes the effect that migration has on users activated on agents.

Pre-Migration	Post-Migration
User activated with access time restrictions on a restricted agent	A group containing a single user is created and activated on the agent. The group has the same access time restrictions that the user had in version 6.1. The agent remains a restricted agent.

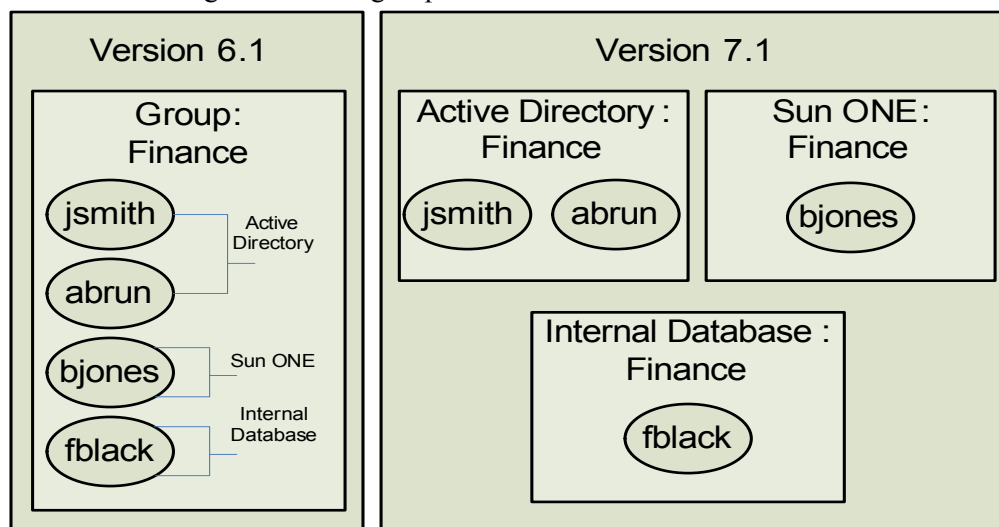
Pre-Migration	Post-Migration
User activated with no access time restrictions on a restricted agent	<p>A group containing a single user is created and activated on the agent.</p> <p>The group has no access time restrictions.</p> <p>The agent remains a restricted agent.</p>
User activated with access time restrictions on an unrestricted agent	<p>A group containing a single user is created and activated on the agent.</p> <p>The group has the same access time restrictions that the user had in version 6.1.</p> <p>The agent is migrated as a restricted agent.</p> <hr/> <p>Note: As a result of converting an unrestricted agent to a restricted agent, users who are not activated on the agent (either directly or through membership in a group activated on the agent) will no longer be able to authenticate through the agent.</p>
User activated with no access time restrictions on an unrestricted agent	<p>A group containing all users with user activations on the agent is created, and the group is activated on the agent.</p> <p>The group has no access time restrictions.</p> <p>The agent is migrated as a restricted agent.</p> <hr/> <p>Note: As a result of converting an unrestricted agent to a restricted agent, users who are not activated on the agent (either directly or through membership in a group activated on the agent) will no longer be able to authenticate through the agent.</p>

Migrated Groups Containing LDAP and Non-LDAP Users

Version 6.1 administration allows groups that contain a mix of LDAP and non-LDAP users, that is, users added to the database through an LDAP synchronization job and users added through the Database Administration application. In version 7.1, all users in a user group must reside in the same identity source. For each version 6.1 group that contains a mix of LDAP and non-LDAP users, the migration process creates a group for each identity source containing the users that reside in the identity source.

Note: If your LDAP directory is read-only and the groups do not yet exist in the directory server, you must add them from your directory servers administration application. If your directory server is read/write, migration creates user groups and assigns membership.

The following figure shows how one group of LDAP and non-LDAP users in version 6.1 is migrated to user groups in version 7.1.



Trusted Realms

Trusted realms function much like cross-realm relationships in version 6.1. They both allow access to a network by a visiting employee. The trusted realm feature allows you to create a trust relationship between multiple realms, so that users from one realm can be authenticated through agents in another realm.

There are three main differences between cross-realm and trusted realms. In trusted realms:

- Establishing trust requires the exchange of generated trust packages.
- Trust can be one-way or two-way.
- There is increased administrative control over remote users.

Additionally, the terminology has changed. The term “home” realm is no longer used, and the “remote” realm in version 6.1 is now known as the “trusted” realm.

Note: For performance reasons, RSA recommends that you have no more than six trusted realms.

Establishing Trusted Realms

When establishing a cross-realm relationship in version 6.1, one of the administrators must provide a set number of passcodes to be input by the administrator of the other realm. Once the realm relationship is established, users from either realm can authenticate in the other realm through any open agent in the realm, as long as cross-realm is enabled.

In trusted realms, an administrator who wants to allow users from his realm to authenticate from another realm (the “trusted” realm) must exchange trusted realm credentials called a trust package. The administrator then delivers the trust package to the “trusted” realm. The administrator of the “trusted” realm must then import the trust package into his realm.

Note: You can choose to migrate all existing realm relationships. It is also possible to establish realm relationships between version 5.2 or version 6.1 and version 7.1 realms. You must do this from the version 5.2 or 6.1 realm, using the Database Administration application. For more information, see the version 5.2 or 6.1 Help topic “Setting Up Cross-Realm Authentication.”

Upgrading Trust

Migration allows version 7.1 realms to continue to authenticate users from version 6.1 realms. However, when you migrate additional realms to version 7.1, the trust between existing version 7.1 realms and the migrated realm is broken. As a result, you must reestablish, or upgrade, the trust between any migrated version 7.1 realms. Trust between a migrated version 7.1 realm and any remaining version 6.1 realms is maintained.

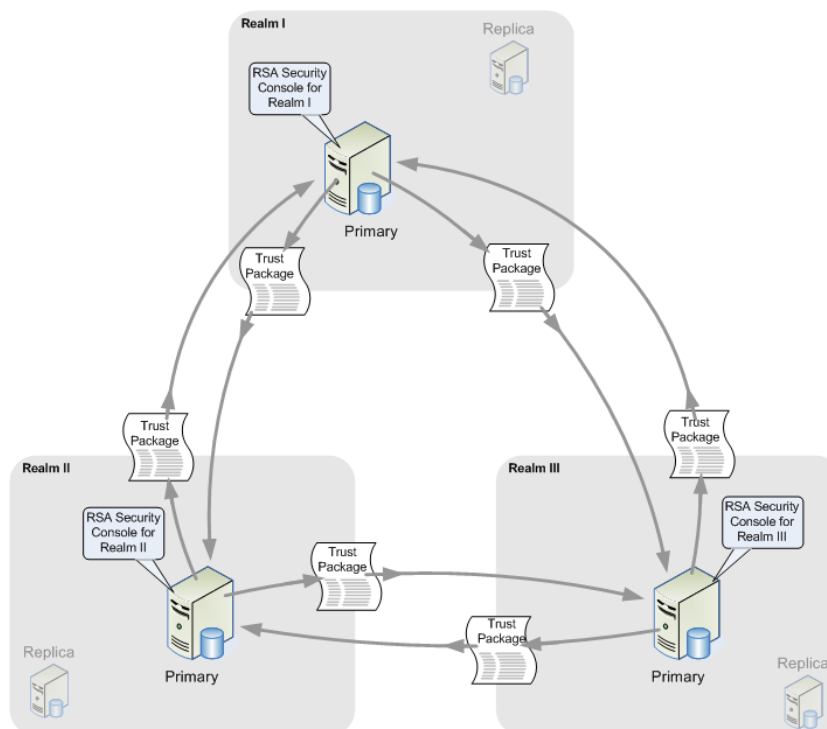
Note: When there are multiple version 7.1 realms on a single machine, the version 6.1 realm cannot establish a cross-realm relationship with more than one of the version 7.1 realms. If you attempt to add an additional realm from the same version 7.1 machine, an IP address conflict occurs, and the version 6.1 Database Administration application will not allow you to add the realm.

For more information on upgrading trusts, see the Security Console Help topic “Realms.”

One-Way Or Two-Way Trusted Realms

While cross-realm relationships in version 6.1 are always two-way, trusted realm relationships in version 7.1 can be either one-way or two-way. In a one-way trusted realm, the relationship is not mutual. For example, users from realm A may authenticate in realm B, but the users from realm B may not authenticate in realm A. In a two-way trusted realm, the users from either realm may authenticate in the other realm. This capability provides additional administrative control over the realm and ensures that establishing a trusted relationship with another realm is a deliberate act, understood and approved by the realm’s administrator.

The following figure shows the two-way trusted realm relationships between three realms.



Administrative Control

Version 7.1 provides more administrative control to the administrator when users from his realm authenticate to a “trusted” realm. You can decide which of your users can access the authentication agents on the trusted realm by creating duplicate authentication agent records in your realm.

Once you create the authentication agent record, you can restrict which users can authenticate by performing the following tasks:

- Make the agent a restricted agent.
- Add the users to a user group.
- Activate the user group on the agent.

The following table describes the three types of trust relationships you can establish with version 7.1.

Trust Type	Description	How Trust is Established
One-way between two version 7.1 realms	<ul style="list-style-type: none"> Your users visiting the trusted realm can gain access by way of authentication from your realm. No visiting users from the trusted realm can gain access to your realm. 	<ol style="list-style-type: none"> The administrator in the other realm adds a trusted realm that points to your realm. The administrator in the other realm imports a trust package from your realm.
Two-way between two version 7.1 realms	<ul style="list-style-type: none"> Your users visiting the trusted realm can gain access by way of authentication from your realm. Users visiting from the trusted realm can gain access to your realm by authenticating to their own realm. 	<ol style="list-style-type: none"> The administrator in the other realm adds a trusted realm that points to your realm. You create a trusted realm that points to the other realm. You and the administrator of the other realm create, exchange, and import trust packages.
Two-way between a version 6.1 realm and a version 7.1 realm	<ul style="list-style-type: none"> Your users visiting the version 6.1 realm can gain access by way of authentication from your realm. Users visiting from the version 6.1 realm can gain access to your realm by authenticating to their own version 6.1 realm. 	<ol style="list-style-type: none"> In the version 6.1 realm, the remote realm administrator must create a realm in the version 6.1 database, and import the realm secret. Your realm requires the automatic creation of a trusted realm that refers to the version 6.1 realm instead of another version 7.1 realm.

Establishing Trust When Using Network Address Translation

Generally, creating a trusted realm relationship when you are using a firewall with network address translation (NAT) requires the following:

- Add the hostname and NATed IP address of the machines inside the firewall to the machines outside the firewall.
- Establish the realm relationship using the NATed IP address of machines inside the firewall.

The following table describes how to establish trusted realms.

	Version 6.1 Outside a Firewall	Version 7.1 Outside a Firewall
Version 6.1 Inside a Firewall	Not applicable.	<ul style="list-style-type: none"> • Add the realm in the version 6.1 Database Administration application using the real IP addresses of both the remote servers (version 7.1 instances) and the local servers (version 6.1 servers). • On the version 7.1 machine, edit the hosts file. Add the hostname and NATed IP address of the version 6.1 machine.
Version 7.1 Inside a Firewall	<ul style="list-style-type: none"> • Add the realm in the version 6.1 Database Administration application using the NATed IP addresses of the remote servers (version 7.1 instances) and the real IP addresses of the local servers (version 6.1 servers). • Do not edit the hosts file. 	<ul style="list-style-type: none"> • On each version 7.1 machine, edit the hosts file. Add the hostname and NATed IP address of the other version 7.1 machine.

Administrative Capabilities

Administration of version 7.1 functions much like version 6.1. You perform administrative tasks through the RSA Security Console just as you did through the Database Administration application in version 6.1. There is no need to install any remote client software on your administration hardware, as the new RSA Security Console is browser-based, which allows you to access it from any supported and correctly configured browser.

Browser-Based Administration

Version 7.1 provides the following GUI-based administration interfaces that enable you to manage and configure your deployment.

RSA Security Console. The browser-based interface for administering the system, including RSA RADIUS.

Operations Console. The browser-based interface for running Authentication Manager utilities, configuring RSA RADIUS, and migrating data.

Self-Service Console. The browser-based interface for users to request tokens (if the provisioning feature is enabled) and perform self-service tasks.

Note: If you are using Microsoft Active Directory as your identity source, you can perform token-related administration tasks through the Microsoft Management Console using the Authentication Manager MMC snap-in. You can assign and unassign tokens to users; enable, disable and edit tokens; and manage PINs and replace tokens. For more information, see Chapter 8, [“Installing the RSA Authentication Manager MMC Extension.”](#)

RSA Security Console

The RSA Security Console provides access to every day administrative tasks. The Security Console interface reflects the administrative permissions and scope of the administrator using it so that only the tasks and objects appropriate to the administrator’s assigned role are visible. Almost all of the tasks that you performed in the version 6.1 Database Administration application are now performed through the Security Console.

RSA Operations Console

The RSA Operations Console handles tasks that you may need to perform only infrequently, such as migrating data from a version 6.1 realm or configuring RADIUS servers.

RSA Self-Service Console

The RSA Self-Service Console provides an interface for users where they can activate tokens, test authentication, request enrollment, tokens, and user group membership, or perform troubleshooting tasks.

The features that appear in the Self-Service Console depend on the license you use when installing Authentication Manager. For more information, see “Licenses” in the chapter “Administering RSA Authentication Manager” in the *Administrator’s Guide*.

Increased Administrative Scoping

The version 7.1 administrative model is built on the concepts of roles, permissions, and scope. Authentication Manager includes a set of predefined administrative roles and it enables you to create custom roles. You can create as many types of administrators, and as many of each type, as your deployment requires. See [“Predefined Administrative Roles”](#) on page 35.

The following table describes the elements that define administrators.

Element	Description
Role	Governs which aspects of the system an administrator can manage. For example, user accounts.
Permission	Governs the actions an administrator can perform. For example, assign tokens to users.
Scope	Governs the boundaries of an administrator's authority. Scope is limited by the security domain.

Administrative Roles

An administrative role has two components:

- A collection of permissions based on a job function profile.
Permissions are equivalent to task lists in version 6.1. For more information, see the following section, "[Permissions.](#)"
- The scope in which the permissions apply.
Scope functions in the same way as it did in version 6.1. However, scoping in version 7.1 is much more flexible. You can refine or expand the scope based on the security domain hierarchy. In version 6.1, you are limited to realm, site, or group scope. For more information, see "[Scope](#)" on page 33.

You can assign administrative roles to any user in your identity source. When you do so, you give the user permission to perform the administrative actions specified by the role within the specified security domain. You may assign more than one administrative role to an administrator.

When assigning roles to administrators, be sure to assign roles that grant only enough permission to accomplish their tasks. Avoid granting administrative roles that are overly broad.

Authentication Manager provides a set of predefined roles that you can assign to users, allowing them to manage specific aspects of your deployment. You can assign these predefined roles in their default form, or you can modify them by editing the permissions assigned to the roles.

Permissions

The permissions you assign to an administrative role govern the actions that may be taken by an administrator assigned the role. Be sure to assign enough permissions to administrative roles so that administrators can manage all the objects, such as users, user groups, and attributes, necessary to accomplish their assigned tasks, but not so many as to let them manage objects not vital to their responsibilities.

For example, an administrator's only task is assigning tokens to users. You assign the following permissions to the role:

- View users
- View tokens

- Assign tokens to users
- Issue assigned software tokens
- Replace assigned tokens
- Import tokens (optional)
- Enable and disable tokens (optional)

The optional permissions in the previous example give the administrative role slightly expanded capabilities that complement the stated task of assigning tokens to users. Notice that this role does not include permission to add and delete users, resynchronize tokens, or manage emergency offline authentication. These permissions are not related to the stated task of assigning tokens to users.

When you assign permissions to a role, keep in mind that an administrator in that role might need to associate two objects in the deployment. The administrator must have the appropriate permissions and scope for both objects at both ends of the association. For example:

- To assign tokens to users, an administrator must be able to view tokens, assign tokens, and view users.
- To move users between security domains, an administrator must be able to view security domains and users.
- To assign administrative roles to users, an administrator must be able to view roles, assign roles, and view users.

Scope

The scope of an administrative role controls where an administrator may perform specified administrative tasks. Scope consists of two parts:

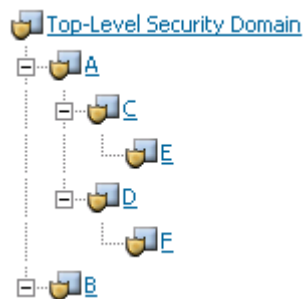
- The portion of the security domain hierarchy that the administrative role can manage
- The identity sources the administrative role can manage

Be sure to assign a scope broad enough so that the administrator can access all security domains and identity sources necessary to perform the responsibilities of the role. However, avoid assigning a scope so broad that you grant access to security domains and identity sources where the administrator has no responsibilities.

For example, a Help Desk Administrator can edit the user record of any other administrator within his scope. This means that a Help Desk Administrator can change the password of a higher-level administrator and gain the administrative privileges of the higher-level administrator. To avoid such situations, assign the higher-level administrator to a security domain that is not within the scope of the Help Desk Administrator.

When you plan the scope of your administrative roles, consider the following:

- The role manages within the security domain where the role definition was saved. This includes all of the lower-level security domains in the same security domain.
- You can limit the scope of an administrative role for those security domains that are at or below the level of the security domain that owns the role. An administrative role can only manage down the security domain hierarchy, never up.
- An administrative role that manages a top-level security domain always manages the lower-level security domains beneath it.



For example, consider the following hierarchy:

- You can scope an administrative role saved in the top-level security domain to manage any one or more security domains in the realm. For example, you can scope it to manage only security domain F, or every security domain in the realm.
- An administrative role saved in security domain A can be defined to manage security domains: A, C, and E, or A, D, and F.
- An administrative role saved in security domain C manages security domains C and E, or E.
- An administrative role saved in security domain E can be defined to manage only security domain E.
- An administrator whose own LDAP record resides in security domain E can manage users in security domain A, C, D, and F if the administrator's role was saved at or above security domain A and includes C, D, and F.

Predefined Administrative Roles

Authentication Manager provides you with a set of predefined roles that you can assign to users, allowing them to manage specific aspects of your deployment. You can assign predefined roles in their default form, or you can edit the permissions assigned to the roles through the RSA Security Console. The following sections describe the default administrative roles.

- **Super Admin**

This role grants complete administrative responsibility for Authentication Manager. The Super Admin role is the only role with full administrative permission in all realms and security domains in your deployment. You can use it to create other administrators and to create your realm and security domain hierarchy.

RSA recommends that you assign the Super Admin role to at least two administrators. This ensures that you still have full administrative control in situations where a Super Admin leaves for vacation or some other extended absence.
- **Realm Administrator**

This role grants complete administrative responsibility for managing all aspects of the realm. This role is limited in scope to the realm in which it is created and it does not include Super Admin permissions. The Realm Administrator can delegate some of the responsibilities of this role.
- **Security Domain Administrator**

This role grants complete administrative responsibility to manage all aspects of a branch of the security domain tree. This administrator has all permissions within that branch except to manage top-level objects such as policies and attribute definitions. By default, this role's scope includes the entire realm. If you want to limit this role's scope to a lower-level security domain in the realm, edit this role, or duplicate this role and then edit the scope of the duplicate role. This role has the same permissions as the Realm Administrators, but is limited to the security domain in which it is created. The Security Domain Administrator can delegate some of the responsibilities of this role.
- **User Administrator**

This role grants administrative responsibility to manage users, assign tokens to users, and access selected authentication agents. This administrator cannot delegate any of the responsibilities of this role.
- **Token Administrator**

This administrative role grants complete administrative responsibility to import and manage tokens, and to assign tokens to users. This administrator cannot delegate any of the responsibilities of this role.
- **Token Distributor**

This role grants administrative responsibility to manage token provisioning requests. Token Distributors also determine how to assign and deliver tokens to users. This administrator can delegate the responsibilities of this role.

- **Request Approver**
This role grants administrative responsibility to approve, update, and reject token provisioning requests including new user accounts, user group membership, token requests, and the on-demand tokencode service. This administrator can delegate the responsibilities of this role.
- **Privileged Help Desk Administrator**
This role grants administrative responsibility to resolve user access issues through password reset, and unlocking or enabling accounts. It also grants permission to view and provide offline emergency access help. This administrator cannot delegate any of the responsibilities of this role.
- **Help Desk Administrator**
This role grants administrative responsibility to resolve user access issues through password reset, and unlocking or enabling accounts. This administrator cannot delegate any of the responsibilities of this role.
- **Agent Administrator**
This role grants administrative responsibility to manage authentication agents and grants access to selected authentication agents. This administrator cannot delegate any of the responsibilities of this role.

For more information, including lists of the default permissions for these roles, see the chapter “Preparing RSA Authentication Manager for Administration,” in the *Administrator’s Guide*.

Custom Administration Applications

You can no longer use any administrative utilities created using the version 6.1 API (application programming interface) because the RSA Authentication Manager 7.1 software has been completely rewritten in Java. The version 6.1 Administrative API includes C and TCL functions that allow you to develop administration applications and TCL scripts. The version 7.1 API includes C# and Java only. You must rewrite custom administrative applications using the new java toolkit available in `RSA_AM_HOME/sdk`.

Viewing Authentication Manager Activity in Real-Time

Activity Monitors allow you to view, in real time, log messages from activities that occur in the Authentication Manager. There are three Activity Monitors, each of which displays a different type of information:

Authentication Activity Monitor. Displays information such as who is authenticating, where the authentication request is coming from, and to what server node they are authenticating.

System Activity Monitor. Displays information such as the time of an activity, a description of the activity, whether the activity was successful, and the server node where the activity took place.

Administration Activity Monitor. Displays information about changes to the Authentication Manager deployment, such as when users are added or deleted, or when tokens are assigned.

The messages that display in the Activity Monitors are configurable. For example, you can use the Administration Activity Monitor to view the activity of a specific administrator, User ID, authentication agent, or security domain.

For more information, see the Security Console Help topic “Troubleshoot Problems Using the Activity Monitors.”

Reports

You can use Authentication Manager to create and run customized reports describing system events and objects (users and tokens, for example). These reports can provide you with more detailed information on the events that occur within the system.

You can create custom reports using the predefined set of report templates provided with Authentication Manager. Each template includes a predefined set of variables, column headings, and other report information. The following templates are available:

- All Users
- All User Groups
- Distributed Token Requests
- Administrators with a Specified Role
- Users with Disabled Accounts
- Administrators of a Security Domain
- Users and User Groups Missing From Identity Source
- Expired User Accounts
- Administrator Activity
- User and User Group Life Cycle Activity
- Object Life Cycle Activity (Non User/User Group)
- System Log Report
- Authentication Activity
- Users with Tokens Set Online Emergency Access Tokencode
- Agents with Unassigned IP Address
- Agent Not Updated By Auto Registration More than Given Number of Days
- Token Expiration Report
- List All Users with Assigned RADIUS Profile for a Given Realm
- List All RSA Agents with Assigned RADIUS Profile for a Given Realm
- List All RSA Agents with Assigned RADIUS Client/RADIUS Server for a Given Realm
- Software Token Deployed on Device Report
- Administrators with Fixed Passcode
- Users with Days Since Last Logon Using Specific Token
- Users with Tokens Using Wildcards

- User Never Logged On with Token
- General On-Demand Tokencode Service
- Event Token Expiration by Event
- Credential Manager Distribution Reports

Important: Any Custom SQL queries or TCL scripts you created in version 6.1 are not migrated to version 7.1. Review the preceding list to match the functionality of your custom queries to the functionality of the predefined report templates.

Version 7.1 provides the ability to view reports within the Security Console, and reports in multiple formats, including comma-separated value, HTML, and XML.

For more information on the reporting functionality, see “Generating Reports” in the chapter “Logging and Reporting” in the *Administrator’s Guide* and the Security Console Help topic “Reports.”

RSA RADIUS

The RSA RADIUS server is now fully integrated into the administrative interface of Authentication Manager. Configuration of the RADIUS server is performed through the Operations Console, which allows you to:

- Start and stop a RADIUS server.
- View the RADIUS server IP address.
- Promote a RADIUS replica server to the RADIUS primary server.
- Edit the RADIUS dictionary and configuration files.

Administration of the RADIUS server is performed through the Security Console. You can use the Security Console to complete most tasks associated with managing RADIUS day-to-day operations related to the RADIUS servers, clients, profiles, and user attributes.

If want to migrate an existing RSA RADIUS server, be aware of the following issues:

- If you want to migrate your existing RADIUS server to the same hardware as your RSA Authentication Manager 7.1, you must migrate them at the same time.
- The RADIUS migration is supported on Solaris 10 and Windows 2003 platforms. If you want to migrate from any other platform, you must migrate to one of these supported platforms. For instructions, see “[Determining the Migration Path for RADIUS](#)” on page 93.

For more information on the administrative consoles, see “[Browser-Based Administration](#)” on page 31.

2

Planning For Migration

- [Hardware and Operating System Requirements](#)
- [Migration Planning Checklist](#)
- [Choosing a Migration Path](#)
- [RSA Authentication Manager Components](#)
- [Migrating Administrative Roles](#)
- [Supporting Your Authentication Agents](#)
- [Planning Data Migration Options](#)
- [Migrating Self-Service and Provisioning Data](#)
- [Planning a Test Migration](#)
- [Migration Planning Checklist](#)

Hardware and Operating System Requirements

Ensure that your system meets these minimum requirements for supported platform and system components. The requirements listed in this section serve only as guidelines. Hardware requirements vary depending on a number of factors, including authentication rates, number of users, frequency of reporting, and log retention. For more information, see the *Performance and Scalability Guide*.

The values listed for RSA RADIUS disk space and memory are in addition to those for Authentication Manager when RADIUS is installed on the same machine with Authentication Manager. When RADIUS is installed on a standalone machine, the values listed for Authentication Manager are sufficient.

Note: You must install all of your Authentication Manager and RADIUS software on the same system types. For example, do not configure Authentication Manager on Solaris and then configure RADIUS on Windows.

RSA recommends that you deploy Authentication Manager on machines to which only authorized users have access. For example, avoid deploying Authentication Manager on machines that host other applications to which non-administrative users have access.

Note: Ensure that your UNIX and Windows servers are designated by fully qualified domain names, for example, *hostname.example.com*.

The server name must observe these conventions:

- Each label, for example, “hostname” or “com,” only contains the letters “A” to “Z” (uppercase) or “a” to “z” (lowercase), the digits “0” through “9”, and the hyphen “-”.
- Each label starts and ends with a letter or digit except for the label after the last dot “.”, which must begin with a letter, for example, .com.

For more information, see the Internet Engineering Task Force documents RFC 1034 and RFC 2609.

Windows System Requirements

Operating System	Microsoft Windows Server 2003 SP2 Standard (32-bit) Microsoft Windows Server 2003 SP2 Standard (64-bit) Microsoft Windows Server 2003 Enterprise R2 SP2 (32-bit) Microsoft Windows Server 2003 Enterprise SP2 (32-bit) Microsoft Windows Server 2003 Enterprise R2 SP2 (64-bit) Microsoft Windows Server 2003 Enterprise SP2 (64-bit) Note: RADIUS is not supported on 64-bit Windows.
Hardware	Intel Xeon 2.8 GHz or equivalent (32-bit) Intel Xeon 2.8 GHz or equivalent (64-bit)
Disk Space	RSA Authentication Manager: 60 GB free space recommended Important: Do not allow all disk space to become consumed. At that point, Authentication Manager may stop operating and be difficult to restore. RSA RADIUS: Add 125 MB of free space
Memory Requirements	RSA Authentication Manager: 2 GB RSA RADIUS: Add 512 MB
Page File	2 GB

Linux System Requirements

Operating System	Red Hat Enterprise Linux 4.7 ES (32-bit) Red Hat Enterprise Linux 4.7 ES (64-bit) Red Hat Enterprise Linux 4.7 AS (32-bit) Red Hat Enterprise Linux 4.7 AS (64-bit) Note: RADIUS is not supported on 64-bit Linux systems.
Hardware	Intel Xeon 2.8 GHz or equivalent (32-bit) Intel EM64T 2.8 GHz or AMD Operon 1.8 GHz, or equivalent (64-bit)
Disk Space	RSA Authentication Manager: 60 GB free space recommended Important: Do not allow all disk space to become consumed. At that point, Authentication Manager may stop operating and be difficult to restore. RSA RADIUS: Add 470 MB of free space
Memory Requirements	RSA Authentication Manager: 2 GB RSA RADIUS: Add 512 MB
Swap Space	4 GB
Kernel Version	2.6.9-22.EL and later
Kernel Parameters	Maximum shared memory must be at least 256 MB

Packages (RPM) 32-bit	The following packages must be installed: binutils-2.15.92.0.2-12 bog1-0.1.18-4 compat-db-4.1.25-9 compat-libstdc++-296.2.9.6-132.7.2 compat-openldap coreutils 5.2.1-31.2 or later control-center-2.8.0-12 cyrus-sasl-gssapi-2.1.19-5 cyrus-sasl-ntlm-2.1.19-5 cyrus-sasl-sql-2.1.19-5 fribidi-0.10.4-6 gcc-3.4.3-22.1 gcc-c++-3.4.3-22.1 gnome-libs-1.4.1.2.90-44.1 glibc-common-2.3.4-2.19 glibc-2.3.2-95.20 gsl-1.5-2 gtkspell-2.0.7-2 kdelibs initscripts 7.93.20 or later libstdc++-3.4.3-22.1 libaio-0.3.105-2.i386 libavc1394-0.4.1-4 libdbi-0.6.5-10 make-3.80-5 libstdc++-devel-3.4.3-22.1 pdksh-5.2.14-30 setarch-1.6-1 sysstat-5.0.5-1 xscreensaver-4.18-5 Note: To check your RPM versions on Linux, use the command, <code>rpm -q package name</code> .
Packages (RPM) 64-bit	Install the following packages: Compatibility Arch Development Support Compatibility Arch Support Note: Make sure that all components in each package are selected.

Solaris System Requirements

Operating System	Solaris 10 (64-bit)
Hardware	<p>UltraSPARC 1.5 GHz, or equivalent</p> <p>For improved performance, use Sun 6 or 8 core UltraSPARC T1 servers.</p> <p>Note: On Sun UltraSPARC systems, Authentication Manager start-up and migration processes can take considerable time. For example, restarting Authentication Manager can take 15 minutes or more. Migration of a large database can take 12 hours or more. In general, Sun UltraSPARC systems with faster processors will yield better start-up and migration performance.</p>
Disk Space	<p>RSA Authentication Manager: 60 GB free space recommended 20 GB free space minimum</p> <p>RSA RADIUS: Add 650 MB of free space</p>
Memory Requirements	<p>RSA Authentication Manager: 4 GB</p> <p>RSA RADIUS: Add 512 MB</p>
Swap Space	4 GB
Packages	<p>SUNWarc</p> <p>SUNWbtool</p> <p>SUNWhea</p> <p>SUNWlibm</p> <p>SUNWlibms</p> <p>SUNWspot</p> <p>SUNWtoo</p> <p>SUNWi1of</p> <p>SUNWi1cs</p> <p>SUNWi15cs</p> <p>SUNWxwft</p>

Supported Data Stores

You can store data in:

- The internal database
- One or more LDAP directories (called an identity source within Authentication Manager)

If you use the Authentication Manager internal database only, it contains all user, user group, policy, and token data. If you integrate Authentication Manager with external identity sources, only user and user group data reside in the external identity source. Policy and token data are stored in the Authentication Manager internal database.

Internal Database

Authentication Manager is installed with an internal database. The internal database contains all application and policy data, and you can choose to store user and user group data in it.

Identity Sources

Authentication Manager supports the use of an external LDAP directory for user and user group data.

Supported LDAP directories are:

- Sun Java System Directory Server 5.2, SP3
- Microsoft Active Directory 2003, SP2

Note: Active Directory Application Mode (ADAM) is not supported.

Sun Java System Directory Server can be located on the same machine as Authentication Manager or on a different machine. When the Sun Java System Directory Server is not on the same machine, a network connection between the two machines is required. Active Directory must be located on a different machine.

Authentication Manager LDAP integration does not modify your existing LDAP schema, but rather creates a map to your data that Authentication Manager uses.

RSA requires SSL for LDAP connections to avoid exposing sensitive data passing over the connection. For example, if bind authentications are performed over a non-SSL connection, the password is sent in the clear. The use of SSL-LDAP requires that the appropriate certificate is accessible by Authentication Manager.

Supported Browsers

This section describes the browsers supported for the RSA Security Console for your platform.

On Windows

- Internet Explorer 6.0 with SP2 for Windows XP
- Internet Explorer 7.0 for Windows XP and Windows Vista
- Firefox 2.0

On Linux

- Firefox 2.0

On Solaris

- Firefox 2.0
- Mozilla 1.07

Note: On all browsers, JavaScript must be enabled. Microsoft Internet Explorer may require configuration depending on its security level setting. See the Microsoft Internet Explorer Help for more information.

Port Usage

The following port numbers must be available to enable authentication, administration, replication, and other services on the network. RSA recommends that you reserve these ports for Authentication Manager, and make sure that no other applications or services are configured to use them.

Port Number	Protocol	Service	Description
1161	UDP	SNMP agent	Used to communicate with a Network Management Server using the Simple Network Management Protocol.
1162	UDP	SNMP agent	Used to communicate with a Network Management Server using the Simple Network Management Protocol.
1645	UDP	RADIUS authentication (legacy port)	Used for authentication requests from RADIUS clients.
1646	UDP	RADIUS accounting (legacy port)	Used for requests for accounting data.
1812	UDP	RADIUS (standard port)	Used for RADIUS authentication.
1812	TCP	RADIUS (standard port)	Used for RADIUS SNMP and CCM/replicating communication.
1813	TCP	RADIUS (standard port)	Used for RADIUS administration.
1813	UDP	RADIUS (SSL port)	Used for RADIUS accounting.

Port Number	Protocol	Service	Description
2334	TCP	RSA Authentication Manager database listener	Used to replicate data between instances.
5500	UDP	Agent authentication	Used for communication with authentication agents. This service receives authentication requests from agents and sends replies.
5550	TCP	Agent auto-registration	Used for communication with authentication agents that are attempting to register with Authentication Manager.
5556	TCP	RSA Authentication Manager node manager	Used to monitor and manage various services.
5580	TCP	Offline authentication service	Used to receive requests for additional offline authentication data, and send the offline data to agents. Also used to update server lists on agents.
7002	TCP	RSA Authentication Manager	Used for SSL-encrypted administration connections.
		RSA Authentication Manager Microsoft Management Console snap-in	Used for SSL-encrypted connections.
7004	TCP	RSA Authentication Manager proxy server	Used for load balancing of administration in an instance with multiple server nodes. This port is used for SSL connections.
		RSA Self-Service Console proxy server/SSL	Used for communication from users to Authentication Manager for requests and maintenance tasks. This port is used for SSL connections.
		RSA Authentication Manager Microsoft Management Console snap-in proxy server	Used for load balancing of administration in an instance with multiple server nodes. This port is used for SSL connections.

Port Number	Protocol	Service	Description
7006	TCP	RSA Authentication Manager administration channel	Internal use only.
7008	TCP	RSA Authentication Manager administration server	Internal use only.
7012	TCP	RSA Authentication Manager administration channel	Internal use only.
7014	TCP	RSA Authentication Manager proxy server administration channel	Internal use only.
7022	TCP	Network access point	Used for mutually authenticated SSL-encrypted trusted realm connections.
7071	TCP	RSA Operations Console	Used for non-SSL connection.
7072	TCP	RSA Operations Console	Used for SSL connections.
7082	TCP	RADIUS configuration SSL	Used for configuration changes to the RADIUS back-end server.

If your current Authentication Manager uses ports other than those listed in the table above, you must reconfigure port numbers through the Security Console. For more information, see the Security Console Help topic “Configure RSA Authentication Manager.”

Synchronizing Clocks

You must ensure that the primary instance clock is accurate because the replica instances automatically synchronize their clocks with the primary instance.

On Windows, type the following command at all replica instances:

```
NET time \\primarycomputername /set
```

On Linux, type the following command at all replica instances:

```
net time set -S primarycomputername
```

Note: RSA strongly recommends that all Authentication Manager instances have their time synchronized to the same NTP server. Authentication Manager will attempt to keep the time of all the Authentication Manager instances synchronized, but due to several technical constraints, time can drift. Having a different time on several Authentication Manager instances can result in authentication failures and problematic replication behavior.

Planning Hardware to Handle Your Authentication Requirements

The strategic placement of Authentication Manager instances and hardware can facilitate authentication of users in deployments composed of multiple geographic sites. Given the roles that replica instances and server nodes play in the Authentication Manager model, you can configure your deployment to best suit your needs.

Server nodes can fulfill authentication rate requirements in a single geographic site. Replica instances deployed strategically across multiple geographic sites can enable those users originating in the sites to authenticate more quickly.

Note: You must install the server nodes of an instance in the same subnet.

Appendix B, “[Migration Scenarios](#)” contains three scenarios that describe sample Authentication Manager deployments.

Configuring Your Browser to Support the RSA Authentication Manager Consoles

The Authentication Manager administrative interfaces (the RSA Security Console, the RSA Operations Console, and the RSA Self-Service Console) are browser-based. Before you can log on and administer Authentication Manager, you must configure your browser to support the consoles as described in the following sections.

Enabling JavaScript

Before you log on, enable JavaScript.

Enabling JavaScript for Internet Explorer

To enable JavaScript:

1. In Internet Explorer, select **Tools > Internet Options > Security**.
2. Select the appropriate web content zone. If you use the default security level, JavaScript is enabled.
3. If you use a custom security setting, click **Custom Level**, and do the following:
 - a. Scroll down to **Miscellaneous > Use Pop-up Blocker**, and select **Disable**.
 - b. Scroll down to **Scripting > Active Scripting**, and select **Enable**.
 - c. Scroll down to **Scripting > Allow paste operations via script**, and select **Enable**.
 - d. Scroll down to **Scripting > Scripting of Java Applets**, and select **Enable**.

Enabling JavaScript for Mozilla Firefox

Generally, you do not need to enable JavaScript for Firefox. If JavaScript is disabled, perform the following procedure:

To enable JavaScript:

1. Open the Firefox browser.
2. Click **Tools > Options > Content**.
3. Select **Enable JavaScript**.
4. Click **OK**.

Adding the RSA Security Console to Trusted Sites

If Internet Explorer is configured for enhanced security levels, you must add the Security Console URL to the list of trusted sites.

To add the RSA Security Console to trusted sites:

1. In Internet Explorer, select **Tools > Internet Options > Security**.
2. Select the Trusted Sites icon, and click **Sites**.
3. Type the URL for the Security Console in the entry next to the Add button.
4. Clear **Require server verification (https:) for all sites**.
5. Click **Add**.

Logging On to the Consoles

You can access any of the three consoles by clicking the link on the desktop, or by opening a supported browser and typing the URLs listed in the following table.

Console	URL
RSA Security Console	https://<fully qualified domain name>:7004/console-ims
RSA Operations Console	https://<fully qualified domain name>:7072/operations-console
RSA Self-Service Console	https://<fully qualified domain name>:7004/console-selfservice

For example, if the fully qualified domain name of your Authentication Manager installation is “host.mycompany.com”, to access the Security Console, you would type the following in your browser:

https://host.mycompany.com:7004/console-ims

Note: On Windows systems, you can also access the Security Console by clicking **Start > Programs > RSA Security > RSA Security Console**.

To log on to the RSA Security Console:

1. Access the Security Console.
2. When prompted, type the User ID of the Super Admin specified during installation.
3. At the password prompt, type the Super Admin password specified during installation.

Note: The Super Admin role includes the ability to create a new Super Admin and other administrators. See the chapter “Preparing RSA Authentication Manager for Administration” in the *Administrator’s Guide*.

Important: When you log on to the Security Console for the first time, you are asked whether you want to trust the self-signed web certificate. To remove the security alert, save the self-signed web root to your browser’s trusted root repository.

To save the self-signed web root certificate:

1. In the security alert window, click **View Certificates**.
2. In the Certificate window, select the **Certification Path** tab.
You will see an untrusted certificate called “RSA Authentication Manager Root CA.”
3. Double-click the RSA certificate to open a new Certificate window.
4. In the Certificate window, click **Install Certificate**.
5. In the Certificate Import Wizard, click **Next**.
6. Click the **Automatically select the certificate store based on the type of certificate** option (this is the default), and click **Next**.
7. Click **Finish** to exit the Wizard.
8. In the security warning window, click **Yes**.
9. Click **OK** to return to the Certificate window.
10. In the Certificate window, click **OK**.
11. In the original Certificate window, click **OK**.
12. In the original security alert window, click **Yes** to open the Security Console.

Pre-Migration Tasks

This section describes important pre-migration tasks required to prepare your system for installation of RSA Authentication Manager 7.1. Carefully review the pre-migration checklist for your platform.

Before migrating Authentication Manager, review the *Release Notes*, which contain important configuration and installation information.

Pre-Migration Checklist for Windows

You must perform these tasks prior to proceeding with the installation of RSA Authentication Manager 7.1.

You must have:

- A machine that meets all the hardware, disk space, memory, and platform requirements described in [“Windows System Requirements”](#) on page 40.
- Local administrator privileges on the machine.
- A static IP address. DHCP is not supported.

Note: If the machine has multiple network interface cards, make sure that the IP address and hostname that you specify during installation belong to the interface you want to use. The default is for the primary network adapter. The Security Console listens only to the IP address that you specify. Failure to verify the IP address and hostname will result in installation or server startup problems.

- A password between 8 and 32 characters including at least six alphabetic characters and one non-alphanumeric character. This case-sensitive password is used in Authentication Manager for the Super Admin password as well as the master password for initial access to protect the vault containing important system passwords. You can change both passwords after installation if desired.
- A temporary directory defined on the host machine. The TEMP variable must be defined, or the installer fails. Installation logs are copied to this directory.
- The following entry in `%WINDIR%\system32\drivers\etc\hosts`:

```
127.0.0.1 localhost.localdomain localhost
```

If this entry does not exist, you must add it before installing Authentication Manager. Type the entire line exactly as shown.

You must:

- If you downloaded the ISO image of Authentication Manager, you must perform a checksum to make sure the sum matches the published checksum on the RSA download site. If the sum does not match, an error may have occurred in transmission. Download the ISO image again.
- Verify that the host does not have an existing installation of Oracle. An existing Oracle database server must be uninstalled before you proceed with the new installation, which includes an internal database.
- Verify that the ports described in [“Port Usage”](#) on page 45 are available.

- ❑ Perform a forward and reverse lookup from each primary and replica instance in the deployment (each machine where you will install Authentication Manager) to every other primary or replica instance. You must perform a forward and reverse lookup as follows:
 - From a fully qualified hostname name (FQHN) to a numeric IP
 - From a short hostname (hostname without domain) to a numeric IP
 - From a numeric IP to a FQHN

Important: If the preceding requirements are not all met, you cannot install a replica instance.

- ❑ If you are using network storage, make sure the disk is mounted at the same location on all server nodes in the cluster.
- ❑ Back up your Windows registry settings.

Pre-Migration Checklist for Solaris and Linux

You must perform these tasks prior to proceeding with the installation of RSA Authentication Manager 7.1.

You must have:

- ❑ A machine that meets all the hardware, disk space, memory, and platform requirements described in “[Linux System Requirements](#)” on page 41 or “[Solaris System Requirements](#)” on page 43.
- ❑ Local administrator privileges on the machine. Run the installer as root user.

Important: RSA recommends that you set up an account specifically for the Authentication Manager installation that can be accessed by any administrator. Do not use a personal account.

- ❑ A static IP address. DHCP is not supported.

Note: If the machine has multiple network interface cards, make sure that the IP address and hostname that you specify during installation belong to the interface you want to use. The default is for the primary network adapter. The Security Console listens only to the IP address that you specify. Failure to verify the IP address and hostname results in installation or server startup problems.

- ❑ A password between 8 and 32 characters including at least six alphabetic characters and one non-alphanumeric character. This case-sensitive password is used in Authentication Manager for the Super Admin password as well as the master password for initial access to protect the vault containing important system passwords. You can change the Super Admin password after installation if desired.

- ❑ The following entry in your `/etc/hosts` file:

```
127.0.0.1 localhost.localdomain localhost
```

If this entry does not exist, you must add it before installing Authentication Manager. Type the entire line exactly as shown.

Note: This entry must not contain the hostname that will be used for the Authentication Manager configuration. Make sure it only contains `localhost` and `localhost.localdomain`.

You must:

- ❑ Create a new user with write permission to the installation location. The default installation location is `/usr/local/RSASecurity/RSAAuthenticationManager`. Run the installer as root user. During installation, you assign ownership of Authentication Manager to the newly created user.
- ❑ Verify that the host does not have an existing installation of Oracle. An existing Oracle database server must be uninstalled before you proceed with the new installation, which includes an internal database.
- ❑ For Red Hat Enterprise Linux 4.0-1 ES (64-bit) and 4.0 AS (64-bit), install the following packages from your Red Hat 4.0 64-bit installation disks:
 - Compatibility Arch Support
 - Compatibility Arch Development Support
- ❑ Verify that the ports described in [“Port Usage”](#) on page 45 are available.
- ❑ On Linux, set or verify the following configuration attributes in your configuration files prior to installation. If any of these parameters are not set properly, the Linux installer dynamically creates a script to correct them and prompts you to run the script as root user before proceeding with the installation.

- In `/etc/sysctl.conf`, add:

```
'kernel.sem' is set to: '250      32000   32      128'
```

Note: These kernel semaphore parameters are minimum values. If you have already set them to a higher value, you do not need to change them.

- In `/etc/security/limits.conf`, add:

```
user soft nproc 2047
user hard nproc 16384
user soft nofile 1024
user hard nofile 65536
```

where *user* is the User ID for the user installing Authentication Manager.

- In `/etc/pam.d/login`, add:

```
session required /lib/security/pam_limits.so
```

- ❑ View the current values specified for resource controls and change them if necessary for the Authentication Manager installation account.

The kernel parameters recommended in the *RSA Authentication Manager 6.1 for UNIX Installation Guide* are not sufficient to run version 7.1. Additionally, in Solaris 10, some kernel parameters are obsolete, or their functionality has been replaced by resource controls. If you are migrating on the same machine, view the current values specified for resource controls, and change them if necessary for the Authentication Manager installation account.

To view and change the values:

Note: You must be logged on as root to change the values.

- a. At a command prompt, type:

```
# id -p username // to verify the project id uid=uid
gid=gid projid=projid
# projmod -n project.max-shm-memory -i project projid
# projmod -n project.max-sem-ids -i project projid
```

where:

- *uid* is the User ID of the Authentication Manager installation account.
- *gid* is the group ID of the Authentication Manager installation account.
- *projid* is the project ID of the Authentication Manager installation account.

- b. If the **max-shm-memory** is less than 6 GB, type:

```
# projmod -n project.max-shm-memory -v 6gb -r -i project
projid
```

- c. If the **max-sem-ids** is less than 256, type:

```
# projmod -n project.max-sem-ids -v 256 -r -i project
projid
```

- ❑ Perform a forward and reverse lookup from each primary and replica instance in the deployment (each machine where you will install Authentication Manager) to every other primary or replica instance. You must perform a forward and reverse lookup as follows:
 - From a fully qualified hostname name (FQHN) to a numeric IP
 - From a short hostname (hostname without domain) to a numeric IP
 - From a numeric IP to a FQHN

Important: If the preceding requirements are not all met, you cannot install a replica instance.

- ❑ If running the GUI-based installer on Linux, you must set the *DISPLAY* environment variable to point to a valid X Windows server, for example:

```
export DISPLAY=hostname:0
```
- ❑ If you are using network storage, make sure the disk is mounted at the same location on all server nodes in the cluster.

Choosing a Migration Path

One of the most important steps in your migration is choosing the correct migration path. Choose one of these methods:

- Upgrade your existing version 6.1 on the hardware on which it is installed.
- Migrate your version 6.1 data to a new installation of version 7.1 on new, supported hardware, using the same hostnames and IP address as your existing version 6.1.
- Migrate your version 6.1 data to a new installation of version 7.1 on new, supported hardware with new hostnames and IP address.

The following sections provide a brief overview of each method and describe considerations for choosing the method you want to use.

Upgrading On the Same Hardware

This is the simplest method of migrating to version 7.1. However, you cannot use this method if your version 6.1 servers do not meet all of the system requirements described in [“Hardware and Operating System Requirements”](#) on page 39.

Note: The system requirements for version 7.1 are significantly greater than the version 6.1 system requirements. For example, the minimum amount of RAM required to run version 6.1 is 256 MB plus 2 MB for every 1,000 users. An installation with a 100,000 user database would require less than half a gigabyte of RAM. For version 7.1, the minimum amount of RAM is 2 GB.

The installation detects the existing version 6.1 server and finds all the necessary license, database dump, and LDAP files required to migrate, and starts the Operations Console, which performs the actual migration of your data. You can still choose to perform a custom migration, which allows you to migrate only specific data from the database. For more information, see [“Planning Data Migration Options”](#) on page 60.

Note: If you run the installer in console mode, you cannot perform an automatic migration of data. You must manually start the Operations Console and specify the locations of your license and database dump file.

Additionally, using the same hardware retains the same IP address for the server. You do not have to update any of the configuration (**sdconf.rec**) files on your authentication agents. You do not have to reestablish any cross-realm relationships.

Migrating to New Hardware

If you choose to migrate to new hardware, you must decide if you want to continue using the same hostname and IP address for each server. There are advantages and disadvantages to either method.

Using the Same Machine Name and IP Address

Using the same hostname and IP address for your new hardware can save you the time and effort of updating your authentication agents, because there is no need to generate and distribute new configuration (**sdconf.rec**) files to each agent.

Additionally, you do not have to reestablish any cross-realm relationships.

However, you will experience some additional downtime of your Authentication Manager servers because you must remove the existing hardware from the network and add the new hardware using the same name and IP address. You can minimize the impact by installing version 7.1 in a test environment. You can then shut down the existing version 6.1 system, and immediately move the version 7.1 system from the test environment to your live network.

If you find it necessary to remove the installed version 7.1 and revert to version 6.1, the process may take slightly longer, given the need to remove the version 7.1 hardware and add the version 6.1 hardware back to your network. Again, installing version 7.1 in a test environment ensures that any issues are discovered and resolved prior to going live.

Additionally, you must delete the **sdstatus.12** file from each RSA Authentication Agent to ensure that the agents are sent a new contact list, which is the list of all the servers in the realm.

Using a New Machine Name and IP Address

Using a new hostname and IP address for your new hardware requires you to generate and distribute new configuration files to each of your authentication agents. The configuration file contains the new hostname and IP address. Until you do this, none of your users can authenticate, because the authentication agents do not know the updated hostname and IP address. Therefore, the agents cannot send authentication requests to the correct Authentication Manager. Consider the number of agents in your deployment and the length of time it will take to update all of them.

You will also need to reestablish each existing cross-realm relationship.

If you find it necessary to revert to version 6.1, the process requires shutting down the version 7.1 instances, and restarting the version 6.1 servers. Additionally, you must delete the **sdstatus.12** file from each RSA Authentication Agent to ensure that the agents are sent a new contact list, which is the list of all the servers in the realm.

Understanding the Installation Methods

RSA provides two methods for installing Authentication Manager: a GUI-based installer and a command line installer.

Use the GUI-based installer if you prefer standard graphical screens to assist you through the process. The command line installer provides the same functionality as the GUI-based installer. On Linux and Solaris platforms, the installer checks to ensure that all required components of the operating system are installed and can create a script that will facilitate updating your system with the necessary components.

RSA Authentication Manager Components

Understand the following Authentication Manager components before you choose an installation type:

Authentication Server. The server that handles runtime authentication operations.

Internal database. The database required for policy data, which can optionally contain all user and group data also.

RSA Security Console. The web application for administering the system.

RSA Operations Console. The web application for running Authentication Manager utilities.

RSA Self-Service Console. The web application that allows users to perform self-service tasks.

(optional) LDAP identity source. Provides access to user and group data residing in LDAP directories.

If it is part of your deployment plan, configure Authentication Manager to use your organization's LDAP directory to access your user data. Authentication Manager modifies certain existing user data fields in the LDAP directory only if you allow it. Those data fields include a user's first and last name, e-mail address, and password.

After installation, you can use the Operations Console and the Security Console to create a data connection between your LDAP directory and Authentication Manager. You must specify a base DN that contains all users in your LDAP directory who you want to be Authentication Manager users or administrators. For instructions on how to run the utility, see Appendix C, [“Integrating an LDAP Directory.”](#)

Migrating Administrative Roles

In version 6.1, roles are composed of a task list (what tasks can be performed by an administrator assigned the role) and a scope (which objects the administrator can administer). There are three predefined roles: realm, site, and group. Each of these roles can be assigned to an administrator and that administrator can be scoped to the realm or to a particular site or group within the realm.

Version 7.1 provides the following predefined administrative roles:

- Super Admin
- Realm Administrator
- Security Domain Administrator
- User Administrator
- Token Administrator
- Privileged Help Desk Administrator
- Help Desk Administrator
- Agent Administrator
- RADIUS Administrator
- Trusted Administrator
- Request Approver
- Token Distributor

Note: For full descriptions of these roles, see [“Predefined Administrative Roles”](#) on page 35.

The most important predefined role is the Super Admin role. This role is the only role with full administrative permission in all realms and security domains in your deployment. Installation of version 7.1 creates the Super Admin role and assigns it to the user you specify as the Super Admin. The following table shows how the version 6.1 roles are migrated.

Version 6.1	Version 7.1
Realm Administrator	Realm Administrator.
Site Administrator	Security Domain Administrator.
Group Administrator	Migrated as a custom administrator role, but not assigned to version 6.1 group administrators. For more information, see the following section, “Group Administrators.”
Custom administrators	Migrated as a custom administrator role.

Group Administrators

In version 7.1, it is no longer possible to scope an administrator to a group. Administrators are scoped to security domains only. To ensure that no administrators are migrated with a higher level scope than they had in version 6.1, the group administrator role is migrated, but not assigned to any version 6.1 group administrators.

For example, group administrators in version 6.1 can only view and change users in their scoped groups. When these administrators are migrated, if they were assigned a group administrator role, their privileges could only be scoped to a security domain, which could contain other users or groups over which the administrator did not previously have any privileges. Rather than expand the privileges and abilities of these administrators, the migration process restricts their privileges.

After migration, former group administrators have no administrative power. You must assign administrative roles to these former group administrators, and scope them to particular security domains.

Supporting Your Authentication Agents

To ensure that users can continue to authenticate through existing agents and RSA Secured hardware, verify that all authentication agents installed on the existing system are supported with Authentication Manager 7.1. Version 5 agents and later are supported. Any custom agent developed using the authentication API prior to version 5 is no longer supported.

Installed RSA Authentication Agents

The supported RSA Authentication Agents are listed on the RSA web site in the Agent Supported Platform Matrix. Go to <http://www.rsa.com/node.aspx?id=2573>. You can download the latest versions of the RSA Authentication Agent software from the same site.

Embedded Agents in Third-Party Hardware and Products

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 inter-operation of RSA products with these third-party products.

If you have any third-party agents on your network, go to <http://www.rsasecured.com>, search for your products, and verify that they are supported by version 7.1.

Customized Agents Created Using the Authentication API

If you are using custom authentication agents that were built with an RSA authentication API, they will continue to work as long as these agents were developed using version 5 of the authentication API.

For custom Windows agents, you can determine the protocol used by viewing the properties of the **aceclnt.dll** file used by your agent. Locate the **aceclnt.dll** file, right-click, select **Properties**, and then click the **Version** tab. The file version must be 5.0 or higher.

Planning Data Migration Options

This section describes the additional data migration capabilities available when you perform a custom migration. It also provides information so that you can decide how, or if, you want to take advantage of these features. During the migration, the RSA Operations Console prompts you to choose the options for these features.

There are three modes of data migration that the Operations Console can perform:

Custom Mode. Allows you to select which objects found in the dump file will be migrated, including the ability to perform a test migration. See the remainder of this section for a description of the options you can select.

Typical Mode. A typical migration performs the migration with the default values of the custom migration selected, including the following:

- Test Migration. Performs the migration, not a test migration.
- Data conflicts. Makes a best effort to migrate data, rather than stop the migration when a data conflict is detected.
- Select objects to migrate. Migrates all found objects.
- User Migration. Migrates all users to the internal database, including any found LDAP users.
- Migrate into Sub-Domain. Migrates all objects into the internal database.

Rolling Upgrade Mode. Migrates only the delta records found in the dump file. Select the rolling upgrade mode when you are migrating a replica server.

The options described in the following sections are only available to you when you choose to perform a custom migration.

Mapping LDAP Identity Sources

Version 7.1 refers to user and user group data in an LDAP directory in real time. In version 6.1, the database is synchronized with the data in the LDAP directory. The major difference is that in version 6.1, the database contains copies of the LDAP data. Version 7.1 contains references to the data in the LDAP directory. Administration of LDAP users and user groups is usually restricted to the LDAP administrator, and not the Authentication Manager administrator, unless you have configured your LDAP directory to allow Authentication Manager read/write-access.

The Operations Console prompts you to specify how to map jobs to identity sources as part of the migration of your version 6.1 data. RSA recommends that you plan how you will merge synchronization jobs into identity sources before you begin to migrate your deployment.

Note: When mapping identity sources, the Operations Console displays only the identity sources linked to the default realm. Identity sources linked to another realm are not displayed.

If you used LDAP synchronization jobs in version 6.1, the migration process can create an identity source for each job. However, you may be able to map multiple synchronization jobs to a single identity source, and minimize the administrative burden of managing identity sources and users.

In version 6.1, configuring LDAP synchronization jobs requires you to specify the following information:

- An LDAP host
- A base DN
For each synchronization job, examine the Base DN of the job to determine if there are any common Base DNs that you can merge into a single identity source.
- A scope
The scope of the job specifies the number of levels below the base DN that the job extends. If the scope of a job is just the base DN or one level below the base DN, you may have other jobs at lower levels of the directory tree that you can combine into one identity source.
- An optional query filter
The query filter allows you to select users that meet certain criteria. If you have filtered users in Authentication Manager to overcome any restrictions in the number of records your directory can update at the same time, you can overcome this restriction by merging the jobs. For example, you may have multiple jobs that filter on the last name of users. One job filters users whose last name begins from A to G, another job filters from H to S, and another filters from T to Z. If these jobs have the same base DN, combine them into one identity source.

Planning How the Migration Handles Data Conflicts

You can configure the installation to handle data conflicts in the dump file in these ways:

- The installation can detect a data conflict, log it, and continue the migration of the remaining data.
- The installation can detect a data conflict, and stop the migration of the data.
Changes made before a conflict is detected are maintained in the database, and in your LDAP directory, if the directory is read/write enabled.

The ability to run a test migration can alleviate any concerns you may have about data conflicts, and allows you to see the results of the migration before making any changes to the database. For more information, see [“Planning a Test Migration”](#) on page 63.

Migrating Only a Subset of Your Data

The version 6.1 database dump utility allows you to select the specific data that you want to dump. Version 7.1 provides you with the ability to filter the data in your dump file, and then you can migrate the specific data you want and ignore the rest. You can filter your dump file based on the following types of data:

- System settings
For example, administrator authentication methods allowed, Windows password integration status, required PIN lengths, and password expiration limits.
- Administrative roles
- Cross-realm relationships
- RSA RADIUS profile names and assignments
- Active LDAP synchronization jobs

For more information, see the Operations Console Help topic “Customize Migration.”

Migrating Data to a Specific Security Domain

When migrating data into the version 7.1 deployment, the administrator migrating the data can choose to migrate the data to a specific security domain. For example, when multiple version 6.1 realms are migrated into a single version 7.1 realm, you may want to maintain some of the existing structure by creating lower-level security domains for each version 6.1 realm, and migrating the data to the lower-level security domain.

The Super Admin can migrate data into any security domain in the realm. If lower-level administrators are migrating the data in the dump file, they can only migrate the data into a security domain over which they have administrative scope. In such a case, only those security domains over which the administrator has scope are visible in the Operations Console interface.

Converting Logon Names from NTLM to UPN

Version 7.1 has the ability to access and store user logon names in the UPN (User Principal Name) format. An example of a UPN-formatted name is **ausер@domain.com**. Version 6.1 stores user logon names in the NTLM (Windows NT Lan Manager) format. An example of an NTLM-formatted name is **DOMAIN\ausер**. As part of migration, you have the option to map NTLM-formatted names to an equivalent UPN-formatted name, so that authenticating requests from existing authentication agents can be processed.

If you choose not to perform any mapping, be aware that existing agents may not be able to authenticate users.

Migrating Self-Service and Provisioning Data

RSA Deployment Manager, the self-service and provisioning solution provided by RSA for previous versions of Authentication Manager, has been discontinued. Token provisioning and user self-service have been integrated into the Security Console. These features are known as RSA Credential Manager.

There is no migration of any Deployment Manager data to Credential Manager. As a result, if you are licensed to use the provisioning features of Deployment Manager, you must make sure that all pending provisioning requests have been processed before you migrate to version 7.1. Once you migrate, any pending requests are lost. You must notify the users who made the requests that they will need to make another request once Credential Manager is properly configured.

Note: The token provisioning feature requires an Enterprise Server license.

Version 7.1 does provide predefined approver and distributor roles that you can assign to administrators responsible for handling account and token requests.

For more information, see Chapter 6, [“Planning User Self-Service and Token Provisioning.”](#)

Planning a Test Migration

A test migration allows you to see the results of a migration without actually migrating any data, or affecting the database in any way. A test migration processes the data in the dump file, but does not commit any changes to the database. At the end of the test migration, a report is generated, which details each change that would be made during an actual migration.

You can configure the test migration to run just as you want the real migration to run. For example, you can configure it to process all or part of the data in the dump file, or to continue even when data conflicts are found. Once the test migration completes, you can read the generated migration report to learn how your data will be processed, determine the severity of the conflicts, and plan methods of correcting the conflicts after the migration of the data completes.

For more information on data conversion and migration reports, see Appendix A, [“Migration Data Conversion.”](#)

Migration Planning Checklist

- Determine your migration path:
 - Migrate on the existing hardware.
 - Migrate to new hardware using the same hostname and IP address as the existing hardware.
 - Migrate to new hardware using a new hostname and IP address.
- Determine where you want to install the database:
 - On the same hardware as Authentication Manager
 - On separate hardware
- Determine the identity sources that you want to use:
 - The internal database
 - Microsoft Active Directory Server
 - Sun ONE Directory Server
- Verify that the administrator responsible for migration has access to, and sufficient administrative privileges on, the version 6.1 servers to perform the following tasks:
 - Dump the database
 - Perform administrative tasks required to clean up the database

For more information on issues that may require cleaning up the database, see [“Migration Report”](#) on page 156.
- Verify that you are using supported and correctly configured browsers to access the RSA consoles.
- Determine if the version 6.1 servers use custom ports for administration, authentication, and other services. If your existing servers use custom ports, you must configure version 7.1 to use the same ports after migration.
- Verify that installed authentication agents are supported, including the following:
 - RSA authentication agents
 - RSA Secured third-party devices with embedded agent software
 - Custom agents created using the version 6.1 authentication
- Determine how LDAP synchronization jobs map to which identity sources.
- Determine the set of data that you want to migrate from version 6.1.
- Determine if you want to migrate any of your data to a specific security domain.

Note: Migrating to a specific security domain can affect the administrative capabilities of some administrators.

- Determine if you need to map user logon names in the NTLM format to the UPN format.
- Resolve all pending RSA Deployment Manager token provisioning requests

3

Migrating the Primary Server

- [Installing the RSA Authentication Manager 7.1 Software](#)
- [Backing Up the Version 7.1 Database](#)
- [Dumping and Transferring Version 6.1 Data](#)
- [Migrating Data Using the RSA Operations Console](#)
- [Reviewing the Migration Report](#)
- [Restoring the Database](#)
- [Securing Backup Files](#)
- [Migrating Log Files](#)

Migrating the primary server requires first installing the RSA Authentication Manager 7.1 software, and then migrating your existing version 6.1 data to the installed version 7.1 instance. Effectively, you are performing a new installation of version 7.1.

The actual migration of data is performed through the RSA Operations Console. To perform the migration, the Operations Console requires a number of existing version 6.1 data files. The Operations Console can find these files itself when version 7.1 is installed on the same hardware as the existing version 6.1 server. The one exception is the log dump file, which you must manually dump and import after the completion of the migration.

RSA recommends that you first install and test version 7.1, while maintaining your existing version 6.1.

Note: If you are migrating on the same hardware as the version 6.1 Authentication Manager, the installer detects the existing version 6.1 server, finds all the necessary license, database dump, and LDAP files required to migrate, and starts the Operations Console, which you use to migrate your data.

Installing the RSA Authentication Manager 7.1 Software

If you are migrating to a new host machine, you must first install RSA Authentication Manager 7.1 on the new host machine, and then load the dump file into the new version 7.1 database.

If you are migrating on the same hardware used by version 6.1, the installation process asks you if you want to migrate. If you answer yes, the installer finds all the necessary files and prompts you to select which data you want to migrate from the dump file.

When you install a primary instance of RSA Authentication Manager 7.1, RSA RADIUS is always installed as well. If you plan to use RADIUS on the primary instance host, you complete the installation of RADIUS by configuring RADIUS using the primary instance RSA Operations Console. You use the Operations Console to migrate the RADIUS 6.1 data after you configure RADIUS.

Note: RADIUS can only be installed on the following platforms:

- 32-bit Windows
- 32-bit Linux
- 64-bit Solaris 10

When you install the 64-bit version of Authentication Manager software on a Windows or Linux 64-bit operating system, RADIUS is not installed. If you want to install RADIUS in this situation, use the Authentication Manager DVD or download kit containing the 32-bit installation program. Install RADIUS only on a separate 32-bit machine running the same operating system as Authentication Manager.

Important: During the installation process, an internal operating system user account for RADIUS is created. This account is used internally and does not require direct interaction. The account name and password must never expire in order for Authentication Manager to function properly. The account name begins with “Radius,” for example, Radius9Ymgx1A. Ensure that this account is not restricted by any network policies that might cause it to expire.

An RSA RADIUS primary server cannot communicate with Authentication Manager through a firewall with network address translation (NAT). You cannot install a standalone RADIUS primary server outside of a firewall with NAT. An RSA RADIUS replica server can be installed outside of a firewall with NAT, but to enable communication through the firewall, you must specify the fully qualified hostname of the RADIUS replica server when you generate the RADIUS replica package.

Mounting the Media on Linux

For a list of commands that may be required to access the installation media, refer to your operating system documentation.

Mounting an ISO Image

If you have received the Authentication Manager software as an ISO image, you must mount the image to make it readable to your system before you can perform the installation.

Important: RSA recommends that you do not create a DVD from the supplied ISO image. Variations in DVD hardware can cause installations to fail.

On Windows

Windows provides no method for mounting or accessing an ISO image. RSA recommends using third-party software to unpack the installation files from the ISO image to the local machine or using third-party software to mount the ISO image and access the installation files within it.

On Linux

You must manually mount the ISO image.

To mount the ISO image:

At a command prompt, type:

```
mount -o loop filename.iso /mountpoint
```

where:

- *filename* is the name of the ISO file.
- *mountpoint* is an existing directory.

On Solaris

You must create a block device for the file, and mount it.

To mount the ISO image:

1. At a command prompt, type:

```
lofiadm -a /directory/filename.iso /dev/lofi/1
```

where:

- *directory* is the location of the ISO file.
- *filename* is the name of the ISO file.

2. Mount the block device. Type:

```
mount -F udfs -o ro /dev/lofi/1 /mountpoint
```

where *mountpoint* is an existing directory.

Creating a RADIUS Migration Package File

In order to export the existing RADIUS 6.1 data, you must create a RADIUS migration package file using the RADIUS Export utility. This utility is provided on the RSA Authentication Manager 7.1 installation media.

Important: You must create the RADIUS migration package before you install RSA Authentication Manager 7.1 because the RADIUS Export utility uses Remote Administration to connect to RSA Authentication Manager 6.1.

After making the RSA Authentication Manager 7.1 installation media available on the Authentication Manager 6.1 primary server host, navigate to *root_directory/client/util*, copy the **am61RADIUSExportUtility.zip** file to the Authentication Manager primary server host, and unpack the file.

To create a RADIUS migration package file:

1. On the Authentication Manager 6.1 primary server host, open a new command shell, and change directories to the directory where you unpacked the **am61RADIUExportUtility.zip** file. Type:

```
patchRemoteAdmin.bat
```

2. Press ENTER.
3. Read the explanatory information, type “y”, and press ENTER.
4. Type the absolute path to base installation directory. For example: C:\Program Files\RSA Security\RSA Authentication Manager.

Note: If you installed Authentication Manager in the default base installation directory, press ENTER.

5. Press ENTER.
6. When prompted, on the Windows desktop do one of the following:
 - For Authentication Manager on the local host machine, click **Start > Programs > RSA Security > RSA Authentication Manager Host Mode** to open the Authentication Manager 6.1 Administration client.
 - For Authentication Manager on a remote host machine, click **Start > Programs > RSA Security > RSA Authentication Manager Remote Mode**. Log on to the remote host machine to open the Authentication Manager 6.1 Administration client.
7. On the Authentication Manager Administration client toolbar, click **RADIUS > Manage RADIUS server**. The RSA AM 6.1 Export utility dialog box opens.
8. In the RSA AM 6.1 Export utility dialog box, click **Export**.
9. When the export is complete, the RSA AM 6.1 Export Utility dialog box displays the location of the RADIUS migration package file, **RSA_AM_HOME/prog/radius/Admin/**.
10. At the **Have you completed the export operation and are ready to restore the client to its original state** prompt, type “y”, and press ENTER.
11. At the **Do you really want to remove this update** prompt, type “y”, and press ENTER.
12. After the export patch is successfully removed, type “exit”, and press ENTER.

Performing an Installation

You can perform an installation using the GUI or the command line interface.

Use the GUI-based installer if you prefer standard graphical screens to assist you through the process. If you prefer a command line interface, you can use the command line installer.

Installation time varies depending on system speed and memory. Make sure you allow at least one hour to perform the installation.

For Linux and Solaris:

- Run the installer as root user.
- When using the GUI installer, define and set the *DISPLAY* environment variable to a display server configured to allow access.

To migrate Authentication Manager:

Note: For Solaris and Linux operating systems, run the installer as root user.

1. Locate and launch the installer for your platform, using the information in the following table.

Platform	Location	Command
Windows 32-bit	auth_mgr\windows-x86	setup.exe
Windows 64-bit	auth_mgr\windows-x86_64	setupwinAMD64.exe
Linux 32-bit	auth_mgr/linux-x86	setupLinux.sh
Linux 64-bit	auth_mgr/linux-x86_64	setupLinux64.sh
Solaris 10-sparc	auth_mgr/solaris-sparc_64	setupSolaris.sh

Note: For the command line interface, you must add the `-console` option to the command. The command line installer displays navigation prompts with instructions on how to proceed or select options.

2. On the **Welcome** screen, click **Next**.
3. If you are installing Authentication Manager on a Solaris or Linux operating system, specify the local user.

Note: This local user cannot be root user. RSA recommends that you set up an account specifically for the Authentication Manager installation that can be accessed by any administrator. Do not use a personal account.

The installer requires access to the user's home directory for this account. If you are installing on Solaris or Linux, use the `-d` and `-m` options with the `useradd` command to ensure that the user's home directory is created along with the account, for example, `useradd -d /home/user_name -m user_name`, where `user_name` is the User ID for this account.

4. If you are migrating on the same machine:
 - Click **Perform software upgrade and data migration** if you want the installer to locate your existing version 6.1 files and begin the migration process automatically. At the end of the installation, your version 6.1 server will be stopped.
 - Click **Perform software upgrade only** if you want to install version 7.1 and then manually locate and migrate your existing version 6.1 data. At the end of the installation, your version 6.1 server will still be running.
5. If the installer detects that an RSA RADIUS 6.1 server is installed on the machine where you are performing the installation, a warning screen prompts you to generate a RADIUS migration package if you have not done so.
6. Respond to the prompts for **Select Region** and **License Agreement**.
7. Select **Primary Instance**.

Important: At this point, the installer informs you if there are unmet or missing requirements and prerequisites for installation and offers you the option to continue anyway. Select **Continue anyway** only if you are directed to do so by RSA Customer Support or if you are certain that you want to accept the risk.

8. Verify the directory name, or click **Browse** to install Authentication Manager in a different directory.
9. When the installer displays the hostname and IP address that will be used for installation, verify the information.

Note: If the machine has multiple network interface cards, make sure that the IP address and hostname that you specify during installation belong to the interface you want to use. The default is for the primary network adapter. The RSA Security Console listens only to the IP address that you specify. Failure to verify the IP address and hostname results in installation or server startup problems.

If the information is correct, click **Next**. If it is not correct, modify the information as necessary, and click **Next**.

10. Click **Browse** to locate the folder that contains your Authentication Manager license file, server key, and certificate files. The license allows you access to certain functionality and limits the number of users that can be registered. The server key and certificate are used to verify (authenticate) the identity of the server. Select the folder, click **Open**, and click **Next**.

Note: When you select the folder, the filenames do not display and the folder appears to be empty.

11. Verify the license information, and click **Next**.

12. When prompted, enter and confirm a User ID and password.

Note: The User ID that you specify is the initial user name for the Security Console and the Operations Console. The Security Console account is given Super Admin permissions, meaning that the account can perform all tasks within Authentication Manager.

The password you enter is used in three ways:

- As the initial password for the Security Console administrator
- As the initial password for the Operations Console administrator
- As the master password for operations, such as installing a replica instance or handling security certificates

The Super Admin password expires according to the password policy. The master password does not expire or change unless it is altered with the Manage Secrets utility.

The password must be between 8 and 32 characters and include at least 6 alphabetic characters and 1 non-alphanumeric character. “@” and “~” are not allowed.

13. Enable or disable **Sign Administration Logs**, **Sign System Logs**, and **Sign Runtime Logs**.

Note: Log signing enables you to verify that your logs have not been tampered with or altered in any way. You cannot enable or disable log signing once Authentication Manager is installed.

For information on log signing or the Verify Archive Log utility, see the *Administrator's Guide*.

14. Review the summary screen, verifying the features you have selected and the disk space required.

15. To begin installing Authentication Manager, click **Install**.

The installer begins and displays a progress indicator.

If you are migrating on the same hardware as the version 6.1

Authentication Manager, the Operations Console automatically starts at the completion of the installation. If you want to start the migration of your version 6.1 data, proceed to [“Migrating Data Using the RSA Operations Console”](#) on page 76.

16. When the installation is complete, the Finish screen is displayed.

- a. To verify that the installation was successful, leave **Start RSA Security Console** selected.

Note: If you choose to open the *Release Notes*, they will open in your default browser after you click Finish.

- b. Click **Finish** to close the installer.

- c. When prompted by your browser, accept the certificate for the Security Console. As part of the normal installation, the installer creates a certificate authority and uses it to sign the Security Console browser certificate.
- d. Log on to the Security Console using the User ID and password that you specified in [step 12](#).

Note: If you are unable to log on to the Security Console, see Appendix D, [“Troubleshooting.”](#)

17. RADIUS is installed by default. If you want to run RADIUS on the same machine as the primary instance, you must configure it using the Operations Console to complete the installation. For more information on post-migration configuration tasks, see [“Integrating the RSA RADIUS Server into the Existing Deployment”](#) on page 140. For testing procedures, see [“Testing RSA RADIUS Operation”](#) on page 143.

Backing Up the Version 7.1 Database

To verify that your data is properly formatted and secure, RSA recommends that you migrate multiple times to a test system. Before you can re-migrate, you must remove all previously migrated version 6.1 data from the version 7.1 database. To do this, you must back up the version 7.1 database immediately after installation, and restore it after you migrate the data and review the migration report. This is required because once data is migrated to the version 7.1 database, present in the database as version 7.1 data, it cannot be migrated again. If the migration process encounters data already present in the version 7.1 database, the data is discarded and the already existing data is preserved.

When there are any issues with the version 6.1 data, the migration report indicates which data has issues. Typical instances of data that requires manual clean up prior to migration are described in [“Migration Report”](#) on page 156.

The backup contains a copy of the database prior to the migration. When the backup is restored, the database contains only the data that was present prior to the migration.

Prerequisites

If you are backing up a database on a Network File System (NFS) partition, you must mount the partition with values in the rsize and wsize fields. These values force connection attempts to retry until the NFS file server responds.

Field	Purpose	Recommended Value for NFS v. 2	Recommended Value for NFS v. 3
rsize	NFS read chunk size	8192	32768
wsize	NFS write chunk size	8192	32768

See your NFS documentation for instructions on configuring these fields.

Performing the Backup

You can back up the database by running the Manage Backups utility on the machine hosting the database.

To back up a database hosted on a separate machine:

1. On the machine hosting the database, from a command prompt, change directories to ***RSA_AM_HOME***.
2. Type:

```
rsautil manage-backups -action export
-f absolute path
```

where *absolute path* is the absolute path and filename of the backup file, including the file extension. For example: `c:\backup\filename.dmp`.

In this example, the system generates two files based on the name you provide, and puts them in the `c:\backup` folder:

filename.dmp The database backup file.

filename.secrets. The user credentials backup file.

Dumping and Transferring Version 6.1 Data

If you install version 7.1 on new hardware, you must manually collect and transfer all of the data files to the new hardware. The required data and files include a dump file of the primary database and the version 6.1 license files. If you are migrating on the same hardware, the installation process collects the required files and data, and starts the Operations Console, which enables you to migrate your data. If you are migrating to new hardware, you must copy the files from your existing Authentication Manager primary server to the new database server hardware.

Important: When transferring the files using ftp, use binary mode to avoid corrupting the files.

Transferring Files

The following table lists the files you need to copy, their locations in the RSA Authentication Manager 6.1 application directory, and a short description of the purpose of the files.

Filename	Location in the Application Directory	Description
<code>sdserv.dmp</code>	<code>data</code>	Contains the data from your existing version 6.1 database. For more information, see “Dumping the Data” on page 74.
<code>sdlog.dmp</code>	<code>data</code>	Contains version 6.1 logs. For more information, see “Migrating Log Files” on page 80.

Filename	Location in the Application Directory	Description
license.rec	data	Your original license file from the version 6.1 primary server. The migration uses the license file to decrypt certain encrypted fields in the version 6.1 database. This file is required to decrypt certain encrypted fields in the version 6.1 dump file.
startup.pf	rdbms32	The startup parameter file specifies the language used by the system running version 6.1. This file is required if you are using any of the following languages: <ul style="list-style-type: none"> • Chinese • Japanese • Korean • Spanish
active.map sunone.map	utils/toolkit	The LDAP synchronization job map files specify the location of the LDAP directories that contain the user information for LDAP users. These files are required if you are migrating user and user group data to LDAP identity sources. If you are using only the internal database to store user and user group data, you do not need to transfer these files.
SSL certificates	data\cert7.db data\key3.db	These certificates are required to establish SSL connections to your LDAP directory servers and are contained in the cert7.db and key3.db files. For more information on exporting the certificates to version 7.1, see “Exporting the LDAP Directory Certificates” on page 75. If you are using only the internal database to store user and user group data, you do not need to export or transfer these files.
sdtacplus.arg sdtacplus.cfg	data	The TACACS+ startup file and configuration file. For more information, see “Migrating Data Using the RSA Operations Console” on page 76. You need these files if you are currently using TACACS+ with your version 6.1 Authentication Manager.

Dumping the Data

Version 6.1 provides a GUI-based utility for dumping the database on Windows and a command line utility for dumping the database on Windows, Linux, or Solaris. For instructions on using the command line version of the dump utility to dump the database, see [“Dumping the Database Using the Command Line”](#) on page 215.

To dump the version 6.1 database using the GUI:

1. On the version 6.1 machine, stop all Authentication Manager processes.

Note: You can dump the database without shutting down the Authentication Manager by selecting **Allow database connection in multi-user mode** after [step 3](#) of this procedure. However, the resulting dump file may not contain the most up-to-date changes.

- a. Click **Start > Programs > RSA Security > RSA Authentication Manager Control Panel**.
 - b. In the Control Panel menu, click **Start & Stop RSA Authentication Manager Services**.
 - c. Under Stop Services, click **Stop All**.
2. Click **Start > Programs > RSA Security > RSA Authentication Manager Database Tools > Dump**.
The Authentication Manager Database Dump dialog box opens.
 3. Under **Select Databases to dump**, select **Dump Server Database** and, if you want to migrate log data, **Dump Log Database**.
 4. Under **Options**, select **Include delta tables in dump file** to ensure that all unreplicated changes are preserved.
 5. Under **Selective Dump**, do not select any of the boxes.
 6. Under **Disk Space Requirements**, verify that the amount of disk space available exceeds the amount of space required.
 7. In the **Output Directory** field, specify the directory path where you want to create the dump files.
 8. Click **OK**.
This displays the status of the dump process.
 9. Do one of the following:
 - If you want to save the status report of the dump process, click **Save As**, specify a filename and a directory, click **Save**, and then click **Close**.
 - Click **Close** when the dump process is done.

Exporting the LDAP Directory Certificates

The LDAP directory certificate enables you to connect to your LDAP identity source using the Secure Sockets Layer (SSL) protocol. SSL ensures that communication between the Authentication Manager and the LDAP directory is encrypted. If you do not have access to the certificate files for each directory server, you can export the certificates from your existing version 6.1 installation using the following procedure. If you can access the certificates, you do not need to perform the procedure. In either case, you will need to import the certificates into your version 7.1 deployment. For more information on importing the certificates, see [“Setting Up SSL for LDAP”](#) on page 186.

To export the LDAP certificates:

1. List the certificates in the files. On the version 6.1 primary server, at the command line prompt, go to the **ACEPROG** directory, and type:

```
certutil -L -d \ACEDATA\cert7.db + key3.db
```

where *ACEDATA* is the version 6.1 data directory containing the files.

2. Export each certificate in the list. Type:

```
certutil -L -d -n certname -r >filename.cer
```

where:

- *certname* is the name of the certificate.
- *filename* is a name you choose for the certificate file.

3. Copy the exported certificate files to the version 7.1 machine, and import them after migration.

Migrating Data Using the RSA Operations Console

The Operations Console is the tool that migrates your data. You can run it in typical mode, which migrates data with minimal interaction from you, or in custom mode, which allows you to filter migrated data, configure how certain data is migrated, and specify how LDAP synchronization jobs map to identity sources.

Important: Before proceeding, read “[Planning Data Migration Options](#)” on page 60, and plan which data you want to migrate, which identity sources you are using, and address any other issues described in that section.

To migrate version 6.1 data:

1. If you are performing a manual migration of data or installed version 7.1 using the `-console` option, start the Operations Console, and log on using the Super Admin User ID and password. Otherwise, go to [step 3](#).
2. Click **Deployment Configuration > Migration > AM 6.1**, and log on using the Super Admin User ID and password.
3. If you are manually migrating data, specify the location of the following files on the Locate Files screen:
 - The **sdserv.dmp** file
 - The version 6.1 **license.rec** file
 - (Optional) The **startup.pf** file

Note: If you performed the migration using the `-console` option, the installation process created the **sdserv.dmp** file in the **RSA_AM_HOME/utils/migration61** directory.

4. Review the Scan Results screen to verify that the data found in the dump file is the data you want to migrate.
5. Select the Migration Mode you want to use, and click **Next**.
The following list provides a brief description of the modes. For more information, see the Operations Console Help topic “Customize Migration.”
Typical Mode. Uses default settings.
Custom Mode. Allows you to customize the behavior of the migration, including which data is migrated, how conflicts are resolved, running a test migration, and where the data is migrated. If you select this mode, when you click **Next**, the Customize Migration screen displays the customizable options.
Rolling Upgrade Mode. Migrates the delta records only. This mode is for migrating your replica servers.
6. Proceed through the remainder of the screens. For more information, see the Operations Console Help topic “Migration Overview.”

Reviewing the Migration Report

When the migration completes, it generates a migration report that lists which data was successfully migrated, which data failed to migrate, and any changes that were made to the data to accommodate the new logical model used in version 7.1.

Click the link to the migration report and review the report to assist you in cleaning up your existing data. There are a number of issues related to the format of your data that you need to resolve to ensure that your migrated Authentication Manager functions correctly and securely. Use the version 6.1 Database Administration application to fix any of the issues that you find in the migration report. For more information, see [“Migration Report”](#) on page 156.

Restoring the Database

You must restore the database to return it to the same state as when it was first installed. The database is effectively empty, except for the Super Admin record and version 7.1 default values, for example, default policies. Once you restore the database, you can repeat the process of creating a dump file of the version 6.1 database and migrating it to version 7.1. Once you have verified that your data is formatted correctly, you can perform the remaining procedures described in this chapter.

No other processes can connect to the database because the Authentication Manager Service is stopped. The following procedures assume that you have no replica instances or additional server nodes installed.

Restoring the Database

The following procedures restore the version 7.1 database to a freshly installed state. Use the first procedure when the database exists on the same machine as the primary instance. Use the second procedure if you installed a standalone database server.

To restore the database:

1. On the primary instance, stop all Authentication Manager Services, except for the internal database and the database listener.

2. From a command prompt, change directories to ***RSA_AM_HOME/utills***.

3. Remove the primary metadata. Type:

```
rsautil setup-replication -a remove-primary
```

4. Import the **filename.dmp** and **filename.secrets** files into the database. Type:

```
rsautil manage-backups -a import -D -f absolute path
```

where *absolute path* is the absolute path and filename of the backup file, including the file extension. For example: **c:\backup\filename.dmp**.

Important: You must include the -D flag in order for the restore operation to work properly.

5. Reset the primary metadata. Type:

```
rsautil setup-replication -a set-primary
```

6. Copy ***RSA_AM_HOME/etc/systemfields.properties*** from the database server to a temporary location on the primary instance.

7. Import **systemfields.properties**. Type:

```
rsautil manage-secrets -a import -f absolute path
```

where *absolute path* is the absolute path and filename to the temporary copy of **systemfields.properties**.

8. When prompted for the import file password, enter the master password.

Important: Restoring the backup overwrites all existing data in the database.

9. Repeat the migration process described in [“Migrating Data Using the RSA Operations Console”](#) on page 76.

To restore a standalone database:

1. On the primary instance, stop all Authentication Manager Services, except for the internal database and the database listener.

2. On the database server, from a command prompt, change directories to ***RSA_AM_HOME/utills***.

3. Remove the primary metadata. Type:

```
rsautil setup-replication -a remove-primary
```

4. Import the **filename.dmp** and **filename.secrets** files into the database. Type:

```
rsautil manage-backups -a import -D -f absolute path
```

where *absolute path* is the absolute path and filename of the backup file, including the file extension. For example: c:\backup\filename.dmp.

Important: You must include the -D flag in order for the restore operation to work properly.

5. Reset the primary metadata. Type:

```
rsautil setup-replication -a set-primary
```

6. Copy **RSA_AM_HOME/etc/systemfields.properties** file from the database server to a temporary location on the primary instance.
7. On the primary instance, import **systemfields.properties**. Change directories to **RSA_AM_HOME\utils**. Type:

```
rsautil manage-secrets -a import -f absolute path
```

where *absolute path* is the absolute path and filename to the temporary copy of **systemfields.properties**.

8. When prompted for the import file password, enter the master password.

Important: Restoring the backup overwrites all existing data in the database.

9. Repeat the migration process described in [“Migrating Data Using the RSA Operations Console”](#) on page 76.

Securing Backup Files

The installer automatically backs up a list of important files to **RSA_AM_HOME/backup**. Immediately after installation, copy the backup directory to a secure location.

Important: For highest security, store **SYSTEM.SRK**, included in your backup folder, on removable media. Retrieve this private key only for disaster recovery. You may want to consider making an additional backup of this data that you store in an alternate, secure location.

RSA recommends storing the **license.rec** file and the database dump file in separate locations, because certain encrypted tables and fields require the license file to be decrypted.

For more information, see the chapter “Disaster Recovery” in the *Administrator’s Guide*.

Migrating Log Files

The Operations Console provides the ability to migrate the logs from your version 6.1 server to the version 7.1 database. Some of the version 6.1 log messages are migrated to equivalent version 7.1 log messages. The other version 6.1 log messages are migrated as generic log messages, with the exact text of the message stored in a notes field of the generic message.

You must manually create the log dump file on your version 6.1 primary server according to the procedure in “[Dumping the Data](#)” on page 74, and transfer the file to the new version 7.1 primary instance. You can import the legacy log messages into version 7.1 by running the Operations Console according to the following procedure.

To import the log messages:

1. On the version 7.1 primary instance, start the Operations Console, and log on using the Super Admin User ID and password.
2. Click **Deployment Configuration > Migration > Log Migration**, and log on using the Super Admin User ID and password.
3. On the Locate Files page, browse to the log dump file.

Note: If you performed the migration on Solaris 10 using the `-console` option, the installation process created the `sdlog.dmp` file in the `RSA_AM_HOME/utils/migration61` directory.

4. Review the Summary - Log Migration page.
5. Click **Start Log Migration**.
The Log Migration Status page displays each migration task as it runs. Click **Refresh** to update the page. You can cancel the log migration at any time by clicking **Cancel Log Migration**.
The Log Migration Results page is displayed when the log migration completes.
6. To view the log migration report in the browser, click **migrate.log**, or click **Done** to exit the page.

Important: If you import the log messages again, duplicate log entries are created.

4

Migrating a Replica Server

- [Generating a Replica Package File](#)
- [Transferring the Replica Package File](#)
- [Dumping the Replica Server Database](#)
- [Migrating the Replica Server](#)
- [Attaching the Replica Instance](#)
- [Rebalancing Contact Lists](#)
- [Securing Backup Files](#)

Once you have migrated your primary server, the replica servers cannot send database changes (delta records) to the primary instance until you migrate the replica servers. The only important data that needs to be migrated from the replica database is the changes, or delta records, that accumulate as a result of any authentications that occur on the replica server while it is not communicating with the primary server.

The contents of the primary database are transferred to the replica instance in the same way they are transferred in version 6.1. This is done by generating and installing a replica package file and, if you are doing a manual data transfer, the primary data .dmp file.

If you are migrating on the same host machine used by version 6.1, the installation process asks you if you want to migrate. If you answer yes, the installer dumps the replica database, finds the required version 6.1 license file, and migrates only the delta records from the dump file.

Depending on how you choose to migrate your replica server, you may need to perform one or more of the following tasks:

- Create a replica package and, if you are doing a manual data transfer, the primary data .dmp file on the primary instance.
- Transfer the replica package and, if you are doing a manual data transfer, the primary data .dmp file to the replica instance host machine.
- If you are migrating to new hardware, dump the version 6.1 replica database.
- Install the version 7.1 software on the replica instance host machine specifying the replica package and, if you are doing a manual data transfer, the primary data .dmp file.
- Attach the replica instance to the primary instance using the RSA Operations Console.
- Migrate the replica database using the Operations Console.
- Configure RADIUS using the Operations Console.
- Migrate the RSA RADIUS 6.1 data using the Operations Console.

Generating a Replica Package File

When you install an Authentication Manager replica instance, you must provide a replica package file and, if you are doing a manual data transfer, the primary data .dmp file.

Replica package file. A.pkg file containing information about the Authentication Manager primary instance that enables replication from the primary to the replica instances.

Primary data file. A.dmp file containing a copy of the data in the primary database. The data from the primary database must be copied to the replica database when a replica instance is first installed.

Use the RSA Operations Console on the Authentication Manager primary instance to generate the replica package file and, if you are doing a manual data transfer, the primary data .dmp file.

Once the Operations Console generates the files, it prompts you to download the replica package file to your local machine, and it might prompt you to download the primary data file to your local machine.

From your local machine, you copy the data to the replica host. When installing the replica instance, you are prompted for the necessary files.

During the process of generating the replica package and, if you are doing a manual data transfer, the primary data .dmp file, you must select one of the following options:

Manual. Two files are created: the replica package file and the primary data file. In the process of attaching the replica to the primary instance, the replica database is created locally using the data in the primary data file. After that, changes in the primary database are synchronized over the network.

Important: The primary data file cannot be used after seven days. The file must never be renamed.

Automatic. Only the replica package file is created. After installation of the replica instance, all of the data from the primary database is copied directly to the replica database over the network, which can take a long time. If you have a large primary database, and a relatively slow network connection, select the manual option.

Each replica package file can be used for only one replica instance to ensure security during the replica installation process. Therefore, you need to generate a new replica package file, and, if you are doing a manual data transfer, the primary data .dmp file for each replica instance that you install.

Important: Do not generate more than one replica package file and primary data .dmp file at a time. If you do not use the most recent primary data .dmp file, the replica attachment fails.

To generate and download the replica files:

Note: You must be a Super Admin to perform this task.

1. On the primary instance, start the Operations Console, and log on using your Operations Console User ID and password.
2. Click **Deployment Configuration > Instances > Generate Replica Package**.
3. If you have not previously entered your Super Admin credentials, you are prompted to enter your Super Admin User ID and password.
4. In the **Replica Hostname** field, enter the fully qualified hostname of the replica server host.
5. In the **Replica IP Address** field, enter the IP address of the replica server host.
6. In the **Master Password** field, enter the master password that you created when you installed the Authentication Manager primary instance.
7. In the **Initial Data Transfer** field, select **Automatic** or **Manual**.
8. Click **Generate File(s)** to create the replica package file and, if you are doing a manual data transfer, the primary data .dmp file.

Note: You will get an error message if another replica attachment is still in progress or if a previous replica attachment has failed. This error message provides directions for resolving these problems.

9. On the Download Files page, do one of the following, depending on your choice in [step 7](#):
 - If you selected **Automatic**, click **Download > Save**. In the SaveAs dialog box, select a location for the replica package file, and click **Save** to save the file to your local machine.
 - If you selected **Manual**, do the following:
 - Click **Download > Save**. In the SaveAs dialog box, select a location for the replica package file, and click **Save** to save the file to your local machine.
 - Click **Download > Save**. In the SaveAs dialog box, select a location for the primary data file, and click **Save** to save the file to your local machine.
10. Click **Done** to return to the Operations Console home page.

Transferring the Replica Package File

Once you have generated the replica package file and, optionally, the primary data file using the Operations Console, copy the files to the appropriate target host.

Note: The encrypted replica package file and the primary data file contain sensitive data. RSA recommends that you transfer the replica package file and, if you are doing a manual data transfer, the primary data .dmp file through a secure network or by removable media.

Note the location on the target host where you copy the files. This information, along with the master password, is required during installation.

When transferring the file using ftp, use binary mode to avoid corrupting the file.

Dumping the Replica Server Database

Version 6.1 provides a GUI-based utility for dumping the database on Windows and a command line utility for dumping the database on Windows, Linux, or Solaris. For instructions on using the command line version of the dump utility to dump the database, see [“Dumping the Database Using the Command Line”](#) on page 215.

To dump the version 6.1 database using the GUI:

1. On the version 6.1 machine, stop all Authentication Manager processes. Click **Start > Programs > RSA Security > RSA Authentication Manager Control Panel**.
2. In the Control Panel menu, click **Start & Stop RSA Authentication Manager Services**.
3. Under Stop Services, click **Stop All**.
4. Click **Start > Programs > RSA Security > RSA Authentication Manager Database Tools > Dump**.
The Authentication Manager Database Dump dialog box opens.
5. Under **Select Databases to dump**, select **Dump Server Database**.
6. Under **Options**, select **Include delta tables in dump file** to dump all associated delta information.
7. Under **Disk Space Requirements**, verify that the amount of disk space available exceeds the amount of space required. In the **Output Directory** box, specify the directory path where you want to create the dump files.

8. Click **OK**.
This displays the status of the dump process.
9. Do one of the following:
 - Click **Close** when the dump process is done.
 - If you want to save the status report of the dump process, click **Save As**, specify a filename and a directory, click **Save**, and then click **Close**.

Migrating the Replica Server

When you migrate a replica instance of RSA Authentication Manager, RSA RADIUS is always installed as well. If you plan to use RADIUS on the replica instance host, you complete the installation of RADIUS by configuring RADIUS using the replica instance RSA Operations Console.

Note: RADIUS can only be installed on the following platforms:

- 32-bit Windows
- 32-bit Linux
- 64-bit Solaris 10

When you install the 64-bit version of Authentication Manager software on a Windows or Linux 64-bit operating system, RADIUS is not installed. If you want to install RADIUS in this situation, use the Authentication Manager DVD or download kit containing the 32-bit installation program. Install RADIUS only on a separate 32-bit machine running the same operating system as Authentication Manager.

Important: During the installation process, an internal operating system user account for RADIUS is created. This account is used internally and does not require direct interaction. The account name and password must never expire in order for Authentication Manager to function properly. The account name begins with “Radius,” for example, Radiuss9Ymgx1A. Ensure that this account is not restricted by any network policies that might cause it to expire.

An RSA RADIUS primary server cannot communicate with Authentication Manager through a firewall with network address translation (NAT). You cannot install a standalone RADIUS primary server outside of a firewall with NAT. An RSA RADIUS replica server can be installed outside of a firewall with NAT, but to enable communication through the firewall, you must specify the fully qualified hostname of the RADIUS replica server when you generate the RADIUS replica package.

Performing the Replica Instance Installation

Important: Before installing an RSA RADIUS replica server, be sure that the clock on the RADIUS replica server is synchronized with the clock on the RADIUS primary server.

After making the RSA Authentication Manager 7.1 installation media available on the replica server host machine, you perform a replica instance installation using the GUI or the command line interface.

Use the GUI-based installer if you prefer standard graphical screens to assist you through the process. If you prefer a command line interface, you can use the command line installer.

Installation time varies depending on system speed and memory. Make sure you allow at least one hour to perform the installation. An installation on Solaris can take more than an hour.

Important: When you install multiple replica instances, you must attach them one at a time. Do not attempt to attach them in parallel. You must generate a new replica package file and, if you are doing a manual data transfer, the primary data .dmp file for each replica that you install. For more information, see [“Generating a Replica Package File”](#) on page 82.

For Linux and Solaris:

- Run the installer as root user.
- When using the GUI installer, define and set the *DISPLAY* environment variable to a display server configured to allow access.

To install a replica instance:

1. Locate and launch the installer for your platform using the information in the following table.

Platform	Location	Command
Windows 32-bit	auth_mgr\windows-x86	setup.exe
Windows 64-bit	auth_mgr\windows-x86_64	setupwinAMD64.exe
Linux 32-bit	auth_mgr/linux-x86	setupLinux.sh
Linux 64-bit	auth_mgr/linux-x86_64	setupLinux64.sh
Solaris 10-sparc	auth_mgr/solaris-sparc_64	setupSolaris.sh

Note: For the command line interface, you must add the *-console* option to the command. The command line installer displays navigation prompts with instructions on how to proceed or select options.

Important: If you plan to implement your deployment with a firewall between the primary instance and replica instances, you must install the replica instance using the `-V FORCE_CONTINUE=true` command option. If you see the “Package Verification Failed” message, click **Yes** to continue installing the replica instance. If you attempt to install the replica without this option, installation verification fails because it cannot resolve the hostname and IP address.

2. On the **Welcome** screen, click **Next**.
3. If you are installing Authentication Manager on a Solaris or Linux operating system, specify the local user.

Note: This local user cannot be root user. RSA recommends that you set up an account specifically for the Authentication Manager installation that can be accessed by any administrator. Do not use a personal account.

The installer requires access to the user’s home directory for this account. If you are installing on Solaris or Linux, use the `-d` and `-m` options with the `useradd` command to ensure that the user’s home directory is created along with the account, for example, `useradd -d /home/user_name -m user_name`, where `user_name` is the User ID for this account.

4. If you are migrating on the same machine:
 - Click **Perform software upgrade and data migration** if you want the installer to locate your existing version 6.1 files, and begin the migration process automatically. At the end of the installation, your version 6.1 server will be stopped.
 - Click **Perform software upgrade only** if you want to install version 7.1 and then manually locate and migrate your existing version 6.1 data. At the end of the installation, your version 6.1 server will still be running.
5. If the installer detects that an RSA RADIUS 6.1 server is installed on the machine where you are performing the installation, a warning screen prompts you to generate a RADIUS migration package if you have not done so.
6. Respond to the prompts for **Select Region** and **License Agreement**.
7. Select **Replica Instance**.

Important: At this point, the installer informs you if there are any unmet or missing requirements and prerequisites for installation. Cancel the installation and ensure that the system meets all requirements.

8. Verify the installation directory name, or click **Browse** to install Authentication Manager in a different directory.
9. When the installer displays the hostname and IP address to use for installation, verify these are correct, and click **Next**. If they are not correct, modify the information as necessary, and click **Next**.

Note: If the machine has multiple network interface cards, make sure the IP address and hostname you specify during installation belong to the interface you want to use. The default is for the primary network adapter. The Security Console listens only to the IP address you specify. Failure to verify the IP address and hostname will result in installation or server startup problems.

10. Click **Browse** to locate the folder that contains your Authentication Manager license file, server key, and certificate files. The license allows you access to certain functionality and limits the number of users that can be registered. The server key and certificate are used to verify (authenticate) the identity of the server. Select the folder, click **Open**, and click **Next**.

Note: When you select the folder, the filenames do not display and the folder appears to be empty.

11. Verify the license information, and click **Next**.
12. Enter the following information:
 - The location of the Authentication Manager replica package file that you created and transferred from the Authentication Manager primary instance. If you have not completed these tasks, see [“Generating a Replica Package File”](#) on page 82.
 - The master password, specified during the primary instance installation. If this password has been changed, use the current master password.
13. If prompted, enter the location of the primary data .dmp file that you created and transferred from the Authentication Manager primary instance.
14. Review the summary screen, verifying the features you have selected and the disk space required.
15. To begin installing Authentication Manager, click **Install**.
The installer begins and displays a progress indicator.
16. After the installer has finished, click **Finish** to close the installer.

Note: If you select **View Release Notes**, they will open in your default browser after you click **Finish**.

If you encounter any problems installing Authentication Manager, see Appendix D, [“Troubleshooting.”](#)

Attaching the Replica Instance

After you have installed the replica instance, you must attach it to the primary instance using the replica instance RSA Operations Console.

To attach the replica instance to the primary instance:

1. On the replica instance, open a web browser, and launch the Operations Console.
2. When prompted by your browser, accept the certificate for the Operations Console.

Note: RSA Authentication Manager acts as a certificate authority to issue and manage product certificates such as the SSL certificate for browsing to the Security Console. By default, these are self-signed, but they can optionally be signed by a verified certificate from an external certificate authority that you provide after the installation completes. For more information, see [“Managing Certificates and Keystores for SSL”](#) on page 136.

3. Log on to the Operations Console using your Operations Console User ID and master password.

Note: If you are unable to log on to the Operations Console, see Chapter 11, [“Troubleshooting.”](#)

4. A page displays that explains the process of adding the new instance as a replica. Do one of the following:
 - Under Reuse Replica Package, select **Yes, use the replica package file stored on this server**, enter the master password, and click **Next**.
 - Under Reuse Replica Package, select **No, I will provide a new replica package file**. Enter the location of the new replica package file. Enter the master password, and click **Next**.
5. If prompted to provide directions for the primary data file, do one of the following:
 - Under Reuse Primary Data File, select **Yes, use the existing primary data file that is stored on this server**, enter the master password, and click **Next**.
 - Under Reuse Primary Data File, select **No, I will provide a new primary data file**. Enter the location of the new primary data file. Enter the master password, and click **Next**.
6. On the Progress Monitor page, the attach process displays. When the attach process is finished, click **Done**.
7. The Manage Instance Replication page displays showing that the instance has been added as a replica.

8. If you want to run RADIUS on the same machine with Authentication Manager, you must configure it using the Operations Console to complete the installation. For more information on post-migration configuration tasks, see [“Integrating the RSA RADIUS Server into the Existing Deployment”](#) on page 140. For testing procedures, see [“Testing RSA RADIUS Operation”](#) on page 143.
9. Continue to [“Securing Backup Files”](#) on page 79 to perform important post-installation tasks.

Migrating Delta Records from the Replica Instance

To migrate delta records:

1. If you are performing a manual migration of data or installed RSA Authentication Manager 7.1 using the -console option, start the Operations Console, and log on using the Super Admin User ID and password. Otherwise, go to [step 4](#).
2. Click **Deployment Configuration > Migration > AM 6.1**, and log on using the Super Admin User ID and password.
3. If you are manually migrating data, specify the location of the following files on the Locate Files screen:
 - The **sdserv.dmp** file
 - The version 6.1 **license.rec** file
 - (Optional) The **startup.pf** file

Note: If you performed the migration on Solaris 10 using the -console option, the installation process created the **sdserv.dmp** file in the **RSA_AM_HOME/utils/migration61** directory.

4. Review the Scan Results screen to verify that the data found in the dump file is the data you want to migrate.
5. Select **Rolling Upgrade Mode**, which migrates the delta records only.
6. Proceed through the remainder of the screens. For instructions, see the Operations Console Help topic “Perform a Typical Mode or Rolling Upgrade Migration.”

Rebalancing Contact Lists

After you add a replica instance and any server nodes to that replica instance, you must rebalance the contact lists in the primary instance Security Console. This updates references to the new replica instances and server nodes.

Note: If the servers are restarted, the references to the new replica instances and server nodes are automatically updated.

To update your contact lists:

1. Click **Access > Authentication Agents > Authentication Manager Contact List > Automatic Rebalance**.
2. Click **Rebalance**.
3. Perform an authentication.

Securing Backup Files

The installer automatically backs up a list of important files to ***RSA_AM_HOME/backup***. Immediately after installation, copy the backup directory to a secure location.

Important: For highest security, store **SYSTEM.SRK**, included in your backup folder, on removable media. Retrieve this private key only for disaster recovery. You may want to consider making an additional backup of this data that you store in an alternate, secure location.

5

Migrating a Standalone RSA RADIUS Server

- [Planning to Migrate a Standalone RSA RADIUS Server](#)
- [Preparing to Migrate a Standalone RADIUS Primary Server](#)
- [Migrating a Standalone RSA RADIUS Primary Server](#)
- [Preparing to Migrate a Standalone RSA RADIUS Replica Server](#)
- [Migrating a Standalone RSA RADIUS Replica Server](#)

Planning to Migrate a Standalone RSA RADIUS Server

A standalone RADIUS server is a RADIUS server that is installed on a machine separate from Authentication Manager. This chapter describes the procedures for migrating a standalone RADIUS primary or replica server. These procedures provide the steps to migrate an RADIUS 6.1 standalone server to an RSA RADIUS 7.1 standalone server either on the same machine or on a new machine.

Note: For information on migrating a RADIUS primary or replica server on the same machine as Authentication Manager, see Chapter 3, “[Migrating the Primary Server](#),” and Chapter 4, “[Migrating a Replica Server](#).”

Determining the Migration Path for RADIUS

Most RSA RADIUS 6.1 servers will have to be migrated to new hardware, because the only common operating systems that support both version 6.1 and version 7.1 are Windows 2003 Server (Standard or Enterprise) and Solaris 10. If you have RSA RADIUS 6.1 installed on Windows 2003 Server (Standard or Enterprise) or Solaris 10, you have the option of migrating RADIUS on the same hardware if the server meets the RSA RADIUS 7.1 system requirements. See the following section “[RSA RADIUS System Requirements](#).”

The following table lists the platforms that support the RSA RADIUS 6.1 server and the supported platforms for RSA RADIUS 7.1 to which you can migrate each RSA RADIUS 6.1 server. In all cases, you must install RADIUS on the same operating system type as Authentication Manager within a given deployment. For example, do not install Authentication Manager on Windows and RADIUS on Solaris.

Supported Platforms for RSA RADIUS 6.1	Supported Platforms for RSA RADIUS 7.1
Red Hat Enterprise Linux 3.0	Red Hat Enterprise Linux 4.0-1 ES or AS (32-bit)
Solaris 9	Solaris 10 (64-bit)

Supported Platforms for RSA RADIUS 6.1	Supported Platforms for RSA RADIUS 7.1
Solaris 10	Solaris 10
SUSE Linux Enterprise Server 9	Red Hat Enterprise Linux 4.0-1 ES or AS (32-bit)
Microsoft Windows 2000 Server or Advanced Server	<ul style="list-style-type: none"> • Microsoft Windows Server 2003 Standard R2 SP2 (32-bit)
Microsoft Windows 2003 Server (Standard or Enterprise)	<ul style="list-style-type: none"> • Microsoft Windows Server 2003 Enterprise R2 SP2 (32-bit) • Microsoft Windows Server 2003 Standard SP2 (32-bit) • Microsoft Windows Server 2003 Enterprise SP2 (32-bit)

Note: RSA recommends migrating to new hardware to minimize the amount of time that the RADIUS server is unavailable during migration.

Once you determine the migration path available to you, proceed through the remainder of this chapter to prepare and perform the RADIUS migration.

RSA RADIUS System Requirements

RSA RADIUS hardware requirements are the same as the Authentication Manager requirements listed in [“Hardware and Operating System Requirements”](#) on page 39. However, only the following operating systems are supported for RADIUS:

- Microsoft Windows Server 2003 Standard R2 SP2 (32-bit)
- Microsoft Windows Server 2003 Enterprise R2 SP2 (32-bit)
- Microsoft Windows Server 2003 Standard SP2 (32-bit)
- Microsoft Windows Server 2003 Enterprise SP2 (32-bit)
- Red Hat Enterprise Linux 4.0-1 ES or AS (32-bit)
- Solaris 10 (64-bit)

Note: RADIUS can only be installed on a 32-bit Windows or Linux platform. When you install the 64-bit version of Authentication Manager software on a supported 64-bit operating system, the installer does not install RADIUS. If you want to install RADIUS in this situation, make sure you use the Authentication Manager DVD or download kit containing the 32-bit installation program. Install RADIUS on a separate 32-bit machine running the same operating system as Authentication Manager.

When migrating RADIUS primary and replica installations on machines that are separate from Authentication Manager, you must perform the migrations of Authentication Manager and RADIUS in the following order:

1. RSA Authentication Manager 6.1 primary server
2. RSA Authentication Manager 6.1 replica server (optional)
3. RSA RADIUS 6.1 primary server
4. RSA RADIUS 6.1 replica server (optional)

Important: In order to export the existing RADIUS 6.1 data, you must create a RADIUS migration package file using the RADIUS Export utility on the Authentication Manager 6.1 primary server. You must create the RADIUS migration package before you migrate the Authentication Manager server. For more information, see [“Creating a RADIUS Migration Package File”](#) on page 67.

RSA RADIUS and Firewalls

To allow RSA RADIUS servers to communicate through a firewall with network address translation, you must configure your DNS server so that each RSA RADIUS server can resolve the fully qualified hostname of any other RSA RADIUS server.

For example, for an RSA RADIUS server outside a firewall to communicate with an RSA RADIUS server inside the firewall, the name of the RSA RADIUS server inside the firewall must resolve to the NATed IP address. When the RSA RADIUS servers are inside a firewall, the names must resolve to the real IP addresses of the machines.

RSA RADIUS Access Planning

It is important to coordinate a migration of the RADIUS servers with the necessary IT personnel to ensure that administrators with the required RADIUS access are available during the migration. You must have:

- An administrator who has physical access to the RADIUS clients.
- An administrator with the RADIUS administrator role in Authentication Manager who can log on to the RSA Security Console or RSA Operations Console and make any required changes related to RADIUS.

Specifying the RSA RADIUS Default Profile

RSA RADIUS supports a default profile. When a RADIUS user authenticates and has no assigned profile, he or she receives the attributes and values that are defined in the default profile, if one is specified.

When you migrate from version 6.1 to version 7.1 of RADIUS, the profile used as the default profile in the version 6.1 installation of RADIUS (if one was configured to be the default) is migrated. However, in version 7.1, that profile is no longer designated as the default profile.

If you want this profile (or any profile) to be designated as the default in the version 7.1 installation, you must specify it as the default after the migration. You can use the Security Console to specify the default profile. Specify the default on the Realm Configuration page. For more information, see the Security Console Help topic “Configure Your Realm.”

Note: Although RSA recommends using the Security Console to specify the default profile, you can also specify a default profile in the **securid.ini** RADIUS configuration file. The default profile specified in Authentication Manager always overrides any default profile specified in the **securid.ini** files.

Preparing to Migrate a Standalone RADIUS Primary Server

This section describes the process of migrating a standalone RADIUS primary server. The process includes the following steps:

1. Create a RADIUS package file on the RSA Authentication Manager 7.1 primary instance host machine using the Generate RADIUS Package utility.
2. Copy the RADIUS package file to the machine where the RSA RADIUS 7.1 primary server will be installed.

Details for each task are provided in the following sections.

Creating an RSA RADIUS Package File

Before you install a standalone RSA RADIUS primary server, create a RADIUS package file (using the Generate RADIUS Package utility) on the Authentication Manager primary instance to gather information needed by both the standalone RADIUS primary and replica servers.

Note: Generating a data file requires up to two times the disk space used by the data.

To create a RADIUS package file:

1. From a command prompt on the Authentication Manager primary instance host, change directories to ***RSA_AM_HOME*/utils**.
2. Type:


```
rsautl gen-radius-pkg
```
3. Press ENTER.
4. When prompted, enter the master password, and press ENTER.
 The master password is the password you specify when you install the Authentication Manager primary instance. (By default, this is the same as the Super Admin password, unless the Super Admin password is changed after installation.)

When the package file creation is complete, the message “Successfully generated *AMprimaryhost-radius.pkg*” is displayed.

For more information on the Generate RADIUS Package utility, see Appendix H, “[Command Line Utilities](#).”

Copying the RSA RADIUS Package File

Once you have created the RSA RADIUS package file, copy it from the ***RSA_AM_HOME/utls*** directory on the Authentication Manager primary instance to the machine where you will install the RSA RADIUS 7.1 primary standalone server. The RADIUS package filename is ***AMprimaryhost-radius.pkg*** and is located in the ***RSA_AM_HOME/utls*** directory. RSA recommends that you copy the RADIUS package file through a secure network or by removable media. Note the directory where you copy the package file. You will supply this location during the standalone RADIUS primary migration.

Migrating a Standalone RSA RADIUS Primary Server

This section provides the procedure for migrating a standalone RSA RADIUS primary server.

Use the GUI-based installer if you prefer standard graphical screens to assist you through the process. If you prefer a command line interface, you can use the command line installer.

Important: During the installation process, an internal operating system user account for RADIUS is created. This account is used internally and does not require direct interaction. The account name and password must never expire in order for Authentication Manager to function properly. The account name begins with “Radius,” for example, *Radiuss9Ymgx1A*. Ensure that this account is not restricted by any network policies that might cause it to expire.

Installation time varies depending on system speed and memory. Ensure you allow at least one hour or more to perform the installation.

For Linux and Solaris:

- Run the installer as root user.
- When using the GUI installer, define and set the *DISPLAY* environment variable to a display server configured to allow access.

To migrate a standalone RADIUS primary:

1. Locate and launch the installer for your platform using the information in the following table.

Platform	Location	Command
Windows 32-bit	auth_mgr\windows-x86	setup.exe
Linux 32-bit	auth_mgr/linux-x86	setupLinux.sh
Solaris 10-sparc	auth_mgr/solaris-sparc_64	setupSolaris.sh

Note: For the command line interface, you must add the `-console` option to the command. The command line installer displays navigation prompts with instructions on how to proceed or select options.

2. On the **Welcome** screen, click **Next**.
3. If you are installing Authentication Manager on a Solaris or Linux operating system, specify the local user.

Note: The local user cannot be root user. RSA recommends that you set up an account specifically for the Authentication Manager installation that can be accessed by any administrator. Do not use a personal account.

The installer requires access to the user's home directory for this account. If you are installing on Solaris or Linux, use the `-d` and `-m` options with the `useradd` command to ensure that the user's home directory is created along with the account, for example, `useradd -d /home/user_name -m user_name`, where `user_name` is the User ID for this account.

4. If you are migrating from RSA RADIUS 6.1 to RSA RADIUS 7.1 on the same machine, the installer displays a message advising you to export the RSA RADIUS 6.1 data. If you have not already done this, see "[Creating a RADIUS Migration Package File](#)" on page 67.
5. Respond to the prompts for **Select Region** and **License Agreement**.
6. Select **Radius Only**.

Important: At this point, the installer informs you if there are any unmet or missing requirements and prerequisites for installation and offers you the option to continue anyway. Select **Continue anyway** only if you are directed to do so by RSA Customer Support or if you are certain that you want to accept the risk.

7. When the installer displays the name and path of the directory where RADIUS will be installed, verify the information, and click **Next**. To select a different location, click **Browse**.

8. When the installer displays the hostname and IP address that will be used for installation, verify the information, and click **Next**. If it is not correct, modify the information as necessary.
 9. Click **Browse** to find and select the directory that contains your Authentication Manager license file, server key, and certificate files. Click **Next**.
 10. Verify the license information, and click **Next**.
 11. Browse to the location of the RADIUS package file containing information about the Authentication Manager primary instance. You must also enter the master password you created during installation of the Authentication Manager primary instance. If this password has been changed, use the current master password. Click **Next**.
 12. Enter the User ID and password, specified during the Authentication Manager primary instance installation. If this User ID and password have been changed, use the current UserID and password. This user has Super Admin privileges, which are required for this task. Click **Next**.
 13. Select the realm with which the RADIUS server will be associated, and click **Next**.
 14. When prompted for the RADIUS server type, click **Next**. The appropriate RADIUS server type is selected by default and cannot be changed.
 15. When the installer displays an automatically generated local system account for the RADIUS administrator, click **Next**. This account is used internally and does not require direct interaction.
 16. Enter and confirm a replication secret. The replication secret secures communication between the RADIUS primary server and a RADIUS replica server. (You can choose any value for the replication secret. There are no rules for the length or character type except that you cannot use spaces.)
 17. Review the summary screen, verifying the features you have selected and the disk space required.
 18. To begin installing RADIUS, click **Install**.
The installer begins and displays a progress indicator.
 19. Click **Finish** to close the installer.
 20. For post-migration RADIUS server and client configuration information, see [“Integrating the RSA RADIUS Server into the Existing Deployment”](#) on page 140.
 21. For testing information, see [“Testing RSA RADIUS Operation”](#) on page 143.
- If you encounter any problems installing RADIUS, see Appendix D, [“Troubleshooting.”](#)

Preparing to Migrate a Standalone RSA RADIUS Replica Server

Important: Before installing a standalone RSA RADIUS replica server, be sure that the clock on the RADIUS replica server host is synchronized with the clock on the RADIUS primary server host.

This section describes the process of migrating an RSA RADIUS replica server on a separate machine. The process includes the following steps:

1. Copy the RADIUS package file that you created on the version 7.1 Authentication Manager primary instance to the machine where the RADIUS replica server will be installed.
2. Copy the RSA RADIUS replica package file, **replica.ccmpkg**, (which is created automatically when the RADIUS primary server is installed) from the RADIUS primary host machine to the RADIUS replica host machine. Alternatively, you can provide the required information during the RADIUS replica installation.

Details on these tasks are provided in the following sections.

Copying the RSA RADIUS Package File

Copy the RSA RADIUS package file, **AMprimaryhost-radius.pkg**, from the **RSA_AM_HOME/utls** directory on the version 7.1 Authentication Manager primary instance to the machine where you will install the RADIUS replica server. RSA recommends that you copy the RADIUS package file through a secure network or by removable media. Note the directory where you copy the package file. You will have to supply this location during the standalone RADIUS replica migration.

Important: When transferring the file using FTP, use binary mode to avoid corrupting the data.

Copying the RSA RADIUS Replica Package File

Before you start the actual installation process, decide whether you want to use the RSA RADIUS replica package file, **replica.ccmpkg**, that was created automatically on the RADIUS primary server during installation. The replica package file contains information about the RADIUS primary server that is needed by the RADIUS replica server.

As an alternative to using the RADIUS replica package file, you can enter the required information manually during the RADIUS replica installation process. If you use the manual process, you enter the following information when prompted: primary server name, primary server IP address or addresses, and the replication secret.

Note: One advantage to using the replica package file is that you do not have to memorize or store the replication secret, which should be a large, random password.

To copy the RSA RADIUS replica package file:

1. On the RADIUS primary server, locate the RSA RADIUS replica package file, **replica.ccmpkg**, in *RSA_AM_HOME*\radius\Service (Windows) or *RSA_AM_HOME*/radius (Linux or Solaris).
2. Copy the **replica.ccmpkg** file to a directory on the RADIUS replica server host. RSA recommends that you copy the package file through a secure network or removable media. Make note of where you copy the package file on the RADIUS replica server as the location will be required during the RADIUS replica installation.

Note: If you transfer the file using FTP, use binary mode to avoid corrupting the data.

3. After the export patch is successfully removed, type “exit”, and press ENTER.

Migrating a Standalone RSA RADIUS Replica Server

This section provides the procedure for migrating a standalone RSA RADIUS replica server.

Note: You must install a RADIUS primary server before you can install a RADIUS replica server.

Important: Before installing an RSA RADIUS replica server, ensure that the clock on the RADIUS replica server is synchronized with the clock on the RADIUS primary server.

You can perform an installation using the GUI or the command line interface. Use the GUI-based installer if you prefer standard graphical screens to assist you through the process. If you prefer a command line interface, you can use the command line installer.

Important: During the installation process, an internal operating system user account for RADIUS is created. This account is used internally and does not require direct interaction. The account name and password must never expire in order for Authentication Manager to function properly. The account name begins with “Radius,” for example, Radius9Ymgx1A. Ensure that this account is not restricted by any network policies that might cause it to expire.

Installation time varies depending on system speed and memory. Make sure you allow at least one hour to perform the installation.

For Linux and Solaris:

- Run the installer as root user.
- When using the GUI installer, define and set the *DISPLAY* environment variable to a display server configured to allow access.

To migrate a standalone RADIUS replica:

1. Locate and launch the installer for your platform using the information in the following table.

Platform	Location	Command
Windows 32-bit	auth_mgr\windows-x86	setup.exe
Linux 32-bit	auth_mgr/linux-x86	setupLinux.sh
Solaris 10-sparc	auth_mgr/solaris-sparc_64	setupSolaris.sh

Note: For the command line interface, you must add the `-console` option to the command. The command line installer displays navigation prompts with instructions on how to proceed or select options.

2. On the **Welcome** screen, click **Next**.
3. If you are installing Authentication Manager on a Solaris or Linux operating system, specify the local user.

Note: The local user cannot be root user. RSA recommends that you set up an account specifically for the Authentication Manager installation that can be accessed by any administrator. Do not use a personal account.

The installer requires access to the user's home directory for this account. If you are installing on Solaris or Linux, use the `-d` and `-m` options with the `useradd` command to ensure that the user's home directory is created along with the account, for example, `useradd -d /home/user_name -m user_name`, where `user_name` is the User ID for this account.

4. If you are migrating from RSA RADIUS 6.1 to RSA RADIUS 7.1 on the same machine, the installer displays a message advising you to export the RSA RADIUS 6.1 data. If you have not already done this, see "[Creating a RADIUS Migration Package File](#)" on page 67.
5. Respond to the prompts for **Select Region** and **License Agreement**.
6. Select **Radius Only**.

Important: At this point, the installer informs you if there are any unmet or missing requirements and prerequisites for installation and offers you the option to continue anyway. Select **Continue anyway** only if you are directed to do so by RSA Customer Support or if you are certain that you want to accept the risk.

7. When the installer displays the name and path of the directory where RADIUS will be installed, verify the information, and click **Next**. To select a different location, click **Browse**.

8. When the installer displays the hostname and IP address that will be used for installation, verify the information, and click **Next**. If it is not correct, modify the information as necessary.
9. Click **Browse** to find and select the directory that contains your Authentication Manager license file, server key, and certificate files. Click **Next**.
10. Verify the license information, and click **Next**.
11. Browse to the location of the RADIUS package file containing information about the Authentication Manager primary instance in your deployment. You must also enter the master password that you created when you installed the Authentication Manager primary instance.
12. Enter the User ID and password, specified during the Authentication Manager primary instance installation. If this User ID and password have been changed, use the current UserID and password. This user has Super Admin privileges, which are required for this task. Click **Next**.
13. Select the realm with which the RADIUS server will be associated, and click **Next**.
14. When prompted for the RADIUS server type, click **Next**. The appropriate RADIUS server type is selected by default and cannot be changed.
15. When the installer displays an automatically generated local system account for the RADIUS administrator, click **Next**. This account is used internally and does not require direct interaction.
16. Do one of the following:
 - If you want to use the **replica.ccmpkg** package file that you copied from the primary RADIUS server to provide the configuration information about the primary RADIUS server, select **Replica package file**, and click **Next**. The installer then prompts you for the location of the **replica.ccmpkg** file. Click **Browse** to provide the location of the replica package file, and click **Next**.
 - If you want to provide the configuration information about the primary RADIUS server manually through an additional installation screen, select **Enter primary RADIUS server hostname, IP address and replication secret manually**, and click **Next**. The installer then prompts you to enter the primary server name, the replication secret specified during the primary replica server installation, and a confirmation of the replication secret. Click **Next**.
17. Review the summary screen, verifying the features you have selected and the disk space required.
18. To begin installing RADIUS, click **Install**.
The installer begins and displays a progress indicator.

19. Click **Finish** to close the installer.
 20. For post-migration RADIUS server and client configuration information, see [“Integrating the RSA RADIUS Server into the Existing Deployment”](#) on page 140.
 21. For testing information, see [“Testing RSA RADIUS Operation”](#) on page 143.
- If you encounter any problems installing RADIUS, see Appendix D, [“Troubleshooting.”](#)

6

Planning User Self-Service and Token Provisioning

- [Overview of RSA Credential Manager](#)
- [RSA Credential Manager Deployment Decisions](#)
- [Implications of Read/Write or Read-Only Access](#)
- [Planning the RSA Credential Manager User Experience](#)
- [Planning Provisioning](#)
- [RSA Self-Service Console Security and Disaster Recovery](#)
- [Training for RSA Credential Manager Administrators and Users](#)
- [RSA Credential Manager Summary](#)

Overview of RSA Credential Manager

RSA Credential Manager is a web-based workflow system that automates the token deployment process and provides user self-service options.

Provisioning streamlines the token deployment process if you are rolling out a large-scale token deployment. It also reduces administrative services and the time typically associated with deploying tokens.

Self-service allows you to reduce the time that the Help Desk spends servicing deployed tokens—when users forget their PINs, misplace their tokens, and require emergency access, or resynchronization. Users perform token maintenance tasks and troubleshoot tokens using the RSA Self-Service Console without involving administrators.

Licensing Options

The Base Server license includes self-service. The Enterprise Server license includes self-service and provisioning.

Note: If you want provisioning, and have a Base Server license, you must upgrade to the Enterprise Server license.

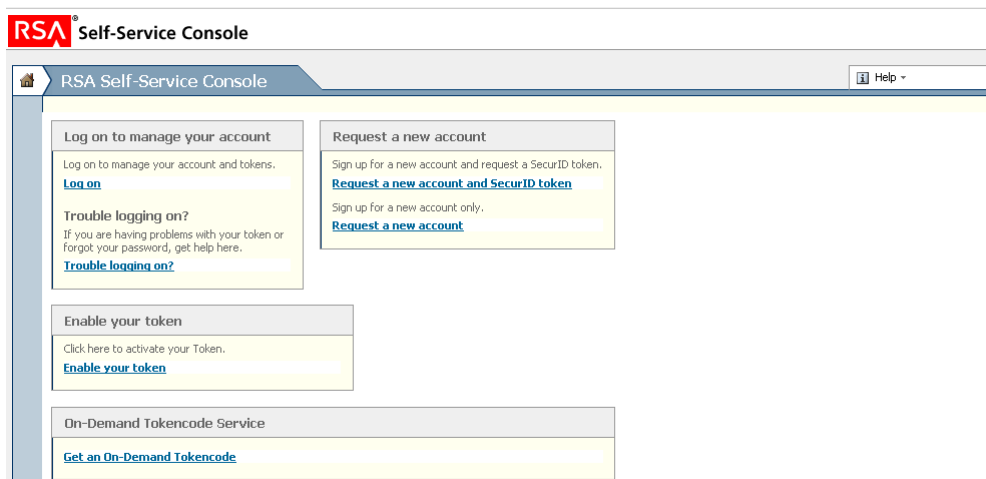
RSA Self-Service Console

The Self-Service Console is a browser-based interface where users can request tokens, troubleshoot tokens, and perform token maintenance tasks. You can customize the header text of the landing page of the Self-Service Console using the RSA Security Console. For more information, see the Security Console Help topic “Customize the RSA Self-Service Console Landing Page.”

You can customize the Self-Service Console Help (RSA Self-Service Console Frequently Asked Questions) to reflect how your company uses self-service and provisioning. For more information, see “Customizing Help for the RSA Self-Service Console” in the *Administrator’s Guide*.

Note: The tasks that users can perform from the Self-Service Console depend on the type of access to identity sources and the license installed.

The following figure shows the landing page of the Self-Service Console.



RSA Security Console

Super Admins use the Security Console to configure Credential Manager. The following figure shows the Credential Manager Configuration - Home page. For more information, see the Security Console Help topic “Configure Credential Manager.”

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

Home | Identity | Authentication | Access | Reporting | RADIUS | Administration | Setup | Help

Credential Manager Configuration - Home | Help on this page

This page is a portal to all of the self-service configuration options for configuring the enrollment and user account maintenance tasks including options for both provisionees and workflow participants (approvers & distributors).

Basic Configuration

- [Set Self-Service Console authentication method](#)
Define authentication settings to determine what credential or combination of credentials are required for an end user to login to manage their account.
- [Select identity sources](#)
Define which of your identity sources are available for your enrolling users to add their profile information to optionally provide user-friendly names for those selected identity sources. For example, if you want users to be able to add themselves to your Employee directory, but not your Partners directory, you do that here.
- [Select security domains](#)
Define which of your security domains are available for your enrolling users to add their accounts to and optionally provide user-friendly names for those selected domains. For example, if you want users to be able to add themselves to your RSA > NA > Headquarters domain, but not your RSA > NA domain, you do that here.
- [Customize user profiles](#)
Customize what fields your users are required, editable, read-only or hidden. Optionally provide helpful text for each entry field and provide friendly label for each entry field.
- [Customize the RSA Self-Service Console Home page](#)
Customize the header text of your RSA Self-service Console Home page.

Token Provisioning

- [Select groups for User Group Membership](#)
Define which of your user groups are available for your enrolling users to join and optionally provide user-friendly names for those selected groups. For example, if you want users to be able to join your VPN Users group, but not your IT Administrators group, you do that here.
- [Set workflow definitions](#)
Define what self-service operations require approval and distribution steps.
- [Define e-mail settings](#)
Define mail server connection settings to allow e-mail notifications for workflow participants and end users. Set whether or not workflow participants receive e-mail, and customize e-mail notifications.
- [Manage tokens](#)
Define how your company prefers to distribute tokens. Define how your company wants users to request tokens. For example, what information they need to provide when requesting tokens, and what types of tokens they can request.
- [Set shipping address](#)
Define the shipping address attributes so that requested token will be send to the user on that address.

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

RSA Credential Manager Deployment Decisions

This section describes the benefits of deploying self-service and provisioning.

The tasks that users can perform are dependent on the license you install and whether you decide to make your identity source read/write or read-only. Self-service is available with all licenses. Provisioning is available with the Enterprise Server license.

Note: If you want provisioning, and have a Base Server license, you must upgrade to the Enterprise Server license.

Deploying Self-Service

When deciding whether to deploy self-service, consider the following:

- Does the Help Desk receive a large number of calls from users for token maintenance, troubleshooting tokens, and emergency access?
- Do you need to reduce the number of calls to the Help Desk?
- Do you need to reduce the cost of maintaining the Help Desk?

With self-service, users can use the Self-Service Console to:

- Enroll. When users enroll in self-service, they become users without administrative privileges.
- Test tokens, resynchronize tokens, change token PINS, and report problems with tokens. This eliminates a call to the Help Desk.
- Update user profiles. User profiles contain user name, user ID, e-mail address, and password.
- Change passwords for the Self-Service Console. They can do this only if the identity source is read/write.
- Troubleshoot tokens and get emergency access for lost, broken, or temporarily unavailable tokens.

Deploying Provisioning

When deciding about whether to deploy provisioning, consider the following:

- Do you have a large number of tokens to deploy or continual token deployment requirements?
- Do you need to reduce token deployment costs?

With provisioning, users can use the Self-Service Console to:

- Request enrollment. Users need approval to enroll in provisioning. When users get approval and enroll, they become users without administrative privileges.
- Request new or additional tokens.
- Enable a token.
- Request the on-demand tokencode service.

- Request on-demand tokencodes.
- Request replacement tokens if tokens are lost, broken, temporarily unavailable, or about to expire.
- Request user group membership for access to protected resources.

Implications of Read/Write or Read-Only Access

If you configure Authentication Manager to have read-only access to identity sources, some Credential Manager tasks are unavailable. If you configure Authentication Manager to have read/write access to identity sources, all Credential Manager tasks are available.

The following table shows the tasks that users can perform with the Base Server and Enterprise Server licenses, and whether these tasks are available if the identity source is set to read/write or read-only access.

Note: If a directory server is read-only, user information must exist in the directory server or in the Authentication Manager internal database for users to perform tasks using the Self-Service Console.

User Task	Identity Source (Base Server License)		Identity Source (Enterprise Server License)	
	Read/Write	Read-Only	Read/Write	Read-Only
Enrollment Tasks				
Request an account	✓	✓	✓	✓
Request an account, a token, or the on-demand tokencode service			✓	✓
Select identity source	✓	✓	✓	✓
Select security domain	✓	✓	✓	✓
Create user profile	✓		✓	
Create password	✓		✓	
Answer security questions	✓	✓	✓	✓
Select user group membership			✓	

User Task	Identity Source (Base Server License)		Identity Source (Enterprise Server License)	
	Read/Write	Read-Only	Read/Write	Read-Only
Troubleshoot problems using the self-service troubleshooting authentication method	✓	✓	✓	✓
Log On to the Self-Service Console				
Log on to the Self-Service Console	✓	✓	✓	✓
Token Management Tasks				
Request a token or the on-demand tokencode service			✓	✓
Enable a token			✓	✓
Change token PIN	✓	✓	✓	✓
Test a token	✓	✓	✓	✓
Report a problem with a token	✓	✓	✓	✓
Request a replacement token			✓	✓
Management Tasks				
Update profile	✓		✓	
Change password	✓		✓	
Request additional user group membership			✓	

Planning the RSA Credential Manager User Experience

To plan the Credential Manager user experience, consider how users will log on to the Self-Service Console, enroll in Credential Manager, and troubleshoot issues.

User Logon

You need to decide how users log on to the Self-Service Console. The following table lists the primary logon methods.

Primary Logon Method	Description
RSA password	The RSA password is the default method for protecting the Self-Service Console. The RSA password is optional for the internal database.
LDAP password	If you use a directory server as your identity source, you may also want to enable LDAP passwords as an authentication method. This allows users whose user records are saved in the identity source to access the Self-Service Console.
SecurID token	For additional security, you can configure Credential Manager to require users to present a credential more secure than a password, such as a passcode, before they access the Self-Service Console. A passcode consists of a PIN and tokencode. For more information, see the “RSA Self-Service Frequently Asked Questions.”

User Enrollment

When users enroll in Credential Manager, they must:

- Enter or review information in a user profile
- Select a security domain
- Select an identity source

Entering Information in the User Profile

Credential Manager uses the information in user profiles to allow users to log on to the Self-Service Console and to send e-mail notifications to users.

Note: Users must enroll in Credential Manager to log on to the Self-Service Console or perform tasks such as requesting tokens.

There are several different enrollment paths for Credential Manager users that affect how users enter information into a user profile. The enrollment paths are:

New users. If a user is not in Authentication Manager and not in a directory server, the user enters all the required information in the user profile.

Users not in Authentication Manager, but in a read/write directory server. The directory server enters information in the user profile from the directory server, and the user can edit the information.

Users not in Authentication Manager, but in a read-only directory server. The directory server enters information in the user profile from the directory server, and the user cannot edit any information.

You can use the default user profile provided for users, or customize the user profile for each identity source that you make available to users. When deciding whether to customize user profiles, consider the following:

- Does your company have different names for some of the fields in the default user profile, for example, “User name” instead of “User ID”?
- Do you need to add descriptive text to instruct users about the information to enter for any of the fields?
- Do you need to add custom attributes, for example, a home address for users?
- Do you need to change fields in the user profile to require read/write, read-only, or hidden depending on the identity source that you use?

Note: If you use an identity source for enrollment, and it is read/write, you can make user profile fields read/write or read-only. If an identity source is read-only, all user profile fields are read-only.

Select Security Domains

Users must select a security domain when enrolling in Credential Manager. You need to plan which security domains to make available to the users. Consider the following when planning which security domains to make available:

- Make security domains available if you want users in those security domains to use self-service and provisioning. For example, if a security domain gets a large number of Help Desk calls from users, or deploys a large number of tokens, make that security domain available.
- Make all security domains available, if users can easily identify the correct ones. For example, if your company has security domains for locations or for departments, users can identify the correct security domain.
- Do not select security domains that are not appropriate for users. For example, if users in a security domain are not intended for self-service or provisioning, do not make that security domain available.

To make sure that users select the correct security domains, you can customize the names and descriptive text of all available security domains that appear on the Self-Service Console. For example, if you configure security domains for each department in your company, you can label each security domain with the department name and add instructions for users to pick their departments.

Select Identity Sources

Users must select an identity source when enrolling in Credential Manager. You need to plan which identity sources to make available to the users. Consider the following when planning which identity sources to make available:

- Make all identity sources available if users can easily identify which ones to select. For example, if your company has an identity source for company employees and another identity source for partners, users can easily identify the correct identity source.
- Do not select identity sources that are not appropriate for users.

To make sure that users select the correct identity sources, you can customize the names and descriptive text of all available identity sources that appear on the Self-Service Console. For example, if identity sources are set up for different locations in your company, you can label the identity sources with the locations and add instructions for users to pick their locations.

User Self-Service Troubleshooting

Self-service troubleshooting policies provide authentication that allows users to troubleshoot problems from the Self-Service Console.

Users can troubleshoot problems with tokens or with the Self-Service Console by clicking **Problems Logging on?** on the Self-Service Console. Users can perform the following troubleshooting tasks after authenticating with a self-service troubleshooting authentication method or after logging on to the Self-Service Console:

- Reset their password
- Reset their PIN
- Resynchronize their token
- Request a new token (if they lost the old one)
- Request an emergency access tokencode

The type of troubleshooting that users can do depends on the type of authentication method that you plan. The following table describes the authentication methods available for self-service troubleshooting and what users can troubleshoot with each method.

Self-Service Troubleshooting Authentication Method	Description	What Users Can Troubleshoot
Security questions	Users must answer security questions when they enroll.	Users can troubleshoot tokens and passwords from the Self-Service Console.
Passwords	Users must enter the password that is associated with their identity source (either directory server or the internal database).	Users can troubleshoot tokens only from the Self-Service Console. If users do not have a password, or forget their passwords, they must call the Help Desk for assistance. Note: Passwords are less secure than two-factor authentication.
None	Use if company policy does not allow users to store personal information (security questions and answers) in the system.	Users cannot perform self-service troubleshooting tasks, and this may result in additional calls to the Help Desk for assistance.

Number of Incorrect Self-Service Troubleshooting Authentication Attempts

You can configure an unlimited number of incorrect self-service troubleshooting authentication attempts, or you can allow a specified number of failed attempts within a specified number of days, hours, or minutes.

Note: The number of attempts applies only to self-service troubleshooting authentication attempts. All other authentication attempts are governed by the lockout policies associated with the security domain that manages the authenticating user.

For more information, see the Security Console Help topic “Self-Service Troubleshooting Policies.”

You can require that administrators must unlock accounts after users have exceeded the limit of incorrect attempts, or you can allow the system to automatically unlock accounts after a specified number of days, hours, or minutes.

For instructions, see the Security Console Help topic “Add Self-Service Troubleshooting Policies.”

Planning Provisioning

For provisioning, consider:

- How user requests are routed through provisioning systems
- What user groups to make available to users
- Which RSA SecurID token types to make available to users
- How to distribute hardware tokens
- What information you want to include in automated e-mail notifications to users
- What kinds of emergency access to make available to users

Workflows

A workflow defines the number of steps or work items for each type of user provisioning request. Provisioning uses workflows to automate token deployment. Users can request enrollment in provisioning, new or additional tokens, the on-demand tokencode service, replacement tokens, or changes in user group membership.

Workflow Definitions

A workflow definition consists of a combination of the following steps or work items for each type of request:

- One or two approval steps
- One distribution step for token requests
- Optionally, add one distribution step for software token requests

You can plan definitions for each type of request using the available steps or work items.

You need to consider the following when you plan definitions:

- How many approvals does each type of request require? For example, do you want a manager and an administrator to approve each request for enrollment for new employees.
- Do hardware token requests require a distribution step?
- Do software token requests require a distribution step?

Provisioning Roles

There are two predefined roles for provisioning:

Request Approver. Views user requests and approves, defers, or rejects user requests.

Token Distributor. Views user requests and determines how to deliver tokens to users. The Token Distributor also records how tokens are delivered to users and closes token requests.

You can use the predefined roles or customize your own roles. For more information, see [“Predefined Administrative Roles”](#) on page 35.

Consider the following when you plan provisioning roles:

- How many approvers do you need for the number of user requests you expect?
- Do you need approvers for each security domain?
- How many distributors do you need?
- Do you need distributors for each location?

Scope for Approvers

Scope for approvers is the same as scope for an Authentication Manager administrator. For example, when approving tokens, approvers can approve requests for tokens only if there are unassigned tokens available in their scope.

The exceptions are:

- Approvers can only approve requests for group membership if the user and the group is in their scope. Be sure to define approvers with scope over both users and user groups so that approvers can approve requests for group membership.
For example, suppose an approver’s only responsibility is to assign users in the identity source “Developers” to groups in the security domain “Boston.” Users can request membership in any group that is in the same identity source to which they belong. If a user requests membership in a group in the security domain “Newton,” which is in their identity source, and the approver does not have scope over the “Newton” security domain, the approver cannot approve the request.
- If you set default groups for Credential Manager enrollment, any approver with scope for a user can approve the user request for enrollment in the default group, regardless of the approver’s scope over the group. For example, if a user requests membership in a default group in the “Newton” security domain, and the approver does not have scope for “Newton,” the approver can approve that request because the request is for a default group.
- If you set up default groups from multiple identity sources and there is more than one identity source, users can only belong to default groups from the identity source in which they are registered.

Select User Groups

User group membership allows provisioning users access to protected resources. See [“User Groups”](#) on page 23.

When you select user groups for Credential Manager, consider the following:

- Users can request membership in any groups that are in the same identity source to which they belong.
- If you set up more than one identity source, and set a default group from multiple identity sources, users can only belong to the default group in the identity source to which they belong.

- Which user groups provide users with the access to resources that they need?
- Are there any user groups that you do not want users to access?
- Is there a user group that you want all users to access?

Select Tokens

You need to decide which type of tokens you want to allow users to request.

The following table lists the available token types.

Tokens	Description
Hardware tokens	Handheld devices, such as a key fob, that display tokencodes that change at regular intervals.
Software tokens	Software-based tokens that reside on a user's computer, PDAs, or mobile devices. Once installed, the software token generates tokencodes that are displayed on the device screen.

On-Demand Tokencode Service

In addition to receiving tokencodes on hardware and software tokens, users can receive on-demand tokencodes delivered to mobile devices or e-mail addresses using the Short Message Service (SMS) or Simple Mail Transfer Protocol (SMTP).

Important: RSA SecurID hardware tokens offer the highest level of security. Other methods of tokencode delivery, such as software tokens and on-demand tokencodes, are easier to use but do not provide the same level of security as a hardware token. RSA recommends using hardware tokens.

You can set up Credential Manager to allow users to request the on-demand tokencode service themselves, instead of having users call the Help Desk for this service. After the on-demand tokencode service is approved, users request on-demand tokencodes from the on-demand tokencode site.

Choosing a Default

Optionally, you can choose a default token type or the on-demand tokencode service for user requests.

Replacement Tokens for Expiring Tokens

If a token is about to expire, users can get replacement tokens through the Self-Service Console. You can decide how many days to allow users to request replacement tokens before the expiration date of a token.

Customizing Token Graphics

Users view token graphics when they request new or additional tokens from the Self-Service Console. You can replace the default token graphics that ship with Credential Manager with your company's custom token graphics. For more information, see "Customizing Token Graphics" in the *Administrator's Guide*.

Token Distribution

You must decide how to distribute tokens to the user. This varies depending on the token type.

On-Demand Tokencode Distribution

Users get on-demand tokencodes from the on-demand tokencode site. On-demand tokencodes are not distributed.

Hardware Token Distribution

For hardware tokens, ease of administration and security are factors in determining the method of hardware token distribution that you use.

Authentication Manager provides report templates you can use to create customized reports for hardware distribution. The distribution report template lists details about requests, tokens, shipping addresses, and information about users who made the requests. Token Distributors can use the information in the distribution report to distribute hardware tokens or send the distribution reports to third-party distribution companies. You can optionally customize distribution reports for token requests.

You also need to plan how to collect shipping addresses for token requests from users. You can collect shipping addresses in one of the following ways:

- If you use a directory server to store user information, you can map an attribute from the directory server for the shipping address, or create a custom attribute for the shipping address in the directory server.
- If you do not use a directory server for user information, users can enter their shipping address every time they request tokens.

Methods for Issuing Software Tokens

You can use Credential Manager to automatically deliver software tokens by e-mail to users when user requests are approved. You do not need to plan a distribution method for this type of token. However, there is a risk that an unauthorized person can intercept the token file and use the software token.

You can require users to supply passwords for token files to protect software tokens. For tokens with PINs, the password for token files is optional. For tokens without PINs, which have one-factor authentication, the password is required.

You can select from the following methods for issuing software tokens:

ZIP file format. Credential Manager packs up the token record into a single .sdtid file, adds the .sdtid file to a .zip archive, and e-mails it to the user.

SDTID file format. The software token record is written to an .sdtid file, and Credential Manager e-mails it to the user.

E-mail Notifications

Credential Manager sends e-mail notifications automatically to users about requests for enrollment, tokens, the on-demand tokencode service, and user group membership. Also, Credential Manager sends e-mail notifications automatically to workflow participants (approvers and distributors.)

Plan for E-mail Servers

You need to know the following information for e-mail servers:

Hostname. Decide which e-mail server to use to send e-mail notifications.

SMTP port. Determine which SMTP port to use. Simple Mail Transfer Protocol (SMTP) is the standard for e-mail transmissions across the Internet.

E-mail address. The address from which Credential Manager sends e-mail notifications.

Logon. Find out if your e-mail server requires a User ID and password.

For more information, see the Security Console Help topic “Configure the SMTP Mail Service.”

Customize E-mail Notifications

You can change the content of e-mail notifications by customizing the Credential Manager e-mail notifications. Consider the following:

- Do you need to send information about requests that is unique to your company?
- Do you have information that is appropriate only for certain situations? You can use conditional statements in your e-mail templates to include information, if certain conditions are met.

For more information, see the appendix “Customizing RSA Credential Manager” in the *Administrator’s Guide*.

Enabling or Disabling E-mail Notifications

The default setting for e-mail notifications is to send e-mail notifications to workflow participants (approvers and distributors). If workflow participants do not want to receive e-mail notifications about requests, you can disable this setting. Workflow participants who decide not to receive e-mail notifications can view all requests by clicking the **Pending Request** tab on the Provisioning Requests page of the Security Console.

Note: Credential Manager sends e-mail notifications automatically to users about their requests for enrollment, tokens, the on-demand tokencode service, and user group membership. You cannot disable e-mail notifications to users.

You can also enable e-mail notifications to Super Admins and workflow participants in the parent security domain. When you nest security domains to create an administrative hierarchy, the top-level security domain is the parent security domain. If you enable e-mail to workflow participants in the parent security domain, all approvers and distributors in security domains above the security domain where a request originates receive e-mail notifications.

Decide who you want e-mail notifications sent to:

- All workflow participants
- Super Admins
- Participants in the parent security domain

Emergency Access

If tokens are temporarily unavailable or permanently lost or broken, users may require emergency access to the resources protected by Authentication Manager. Users can get emergency access using the Self-Service Console.

You need to consider the following when planning emergency access:

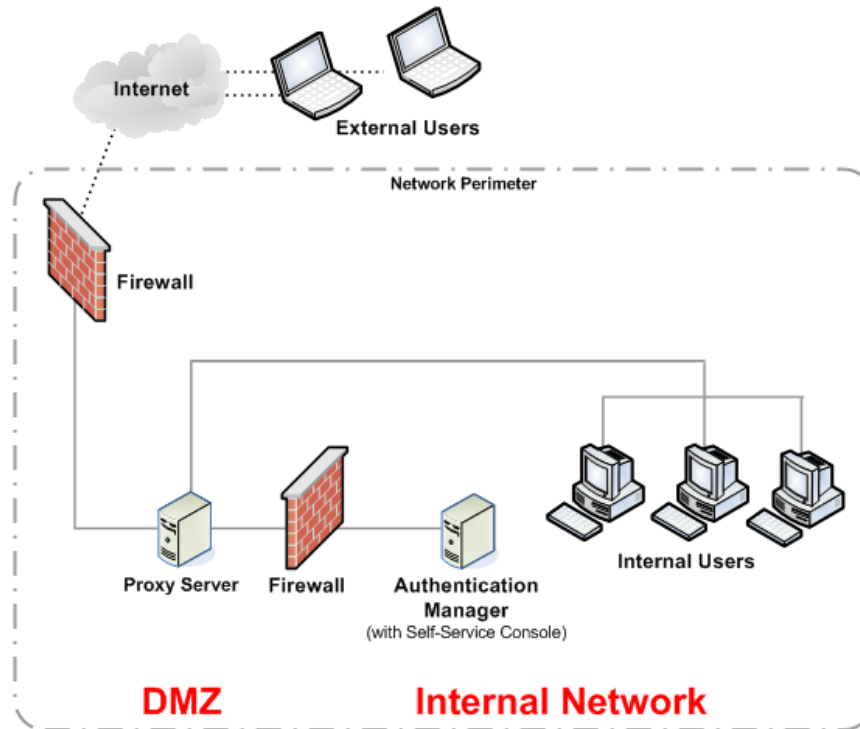
- Whether to allow users to get emergency access.
- The type of emergency access tokencodes available: temporary fixed tokencodes, one-time tokencodes, or on-demand tokencodes.
- The lifetime of emergency access tokencodes.
- The number of one-time tokencodes to issue in a set. One-time tokencodes are issued in sets. The number of tokencodes in the set is determined by your business rules.
- What happens if temporarily unavailable tokens becomes available:
 - Deny authentication with tokens.
 - Allow authentication with tokens and disable emergency access.
 - Allow authentication with tokens after the emergency access lifetime expires, and then disable emergency access.

RSA Self-Service Console Security and Disaster Recovery

Because the RSA Self-Service Console is installed on the same machine as Authentication Manager, RSA recommends that you set up a proxy server in your network DMZ to protect Authentication Manager and accept requests.

Note: If you set up a proxy server in your network DMZ to protect Authentication Manager, you must customize the e-mail notifications to replace the URL for the authentication server with information for the proxy server. For more information, see “Customizing E-mail Notifications for Proxy Servers” in the *Administrator’s Guide*.

The following figure shows a basic network setup with Self-Service Console traffic directed through a proxy server.



Disaster Recovery for Users

In the case of failover, the administrator must immediately change the IP address that is associated with the Self-Service Console alias URL to that of the new primary instance. This allows users to use the same Self-Service Console URL when a primary instance is removed from a deployment and a replica is promoted. If this change is not made, the proxy server continues to try to access the original primary server, causing downtime for users.

If you do not set up an alias for the proxy server, you need to consider how you want to notify users if the primary instance goes down and the replica instance is promoted to the primary instance. The RSA Self-Service Console uses the same port as Authentication Manager. The URL for the Self-Service Console is:
<https://machinename:7004/console-selfservice>.

If the primary instance is down, users cannot create any requests from the RSA Self-Service Console or do any other tasks until the replica has been promoted to the primary. You need to plan how you want to notify users about the new address (URL) for the RSA Self-Service Console when a replica is promoted to the primary because of the machine name change. For more information about disaster recovery, see the chapter “Planning for Failover and Disaster Recovery” in the *Planning Guide*.

Training for RSA Credential Manager Administrators and Users

Develop a plan to train your users and administrators. If you have any tasks that are unique and specific to your business, remember to add them to your list of training topics. For information about training administrators and users, see the *Planning Guide*.

RSA Credential Manager Summary

Know the following when planning self-service and provisioning:

- Whether to deploy self-service or provisioning.
- How to notify users about self-service and provisioning.
- Implications of read/write or read-only identity sources on self-service and provisioning tasks.
- How to plan the user experience.
- Which primary logon method for the Self-Service Console to use.
- Which security domains to make available for user enrollment.
- How to customize user profiles for user enrollment.
- What authentication method to use for self-service troubleshooting.
- How and when to lock a user account for self-service troubleshooting.
- How and when to unlock a user account for self-service troubleshooting.
- How to set up a proxy server to protect Authentication Manager when allowing users access with the Self-Service Console.

In addition, you need to understand the following when planning provisioning:

- Whether to deploy provisioning.
- How to customize workflows for requests.
- Which predefined administrative roles meet your needs.
- Which user groups to make available.
- Which tokens to make available.
- How to distribute hardware tokens.
- How to use distribution reports.
- How to distribute software tokens.
- Which e-mail server port to use.
- Which e-mail address to use to send e-mail notifications.
- Which participants to send e-mail notifications.
- How to customize e-mail templates, if necessary.

- Whether to allow Self-Service Console users to request emergency access.
- What method to make available for emergency access.
- How to set the lifetime for lost or broken tokens or for temporarily unavailable tokens.
- What to do if a missing token is recovered.
- What training approvers and distributors need for requests.

7

Performing Post-Migration Tasks

- [Backing Up a Standalone Primary Instance](#)
- [Securing the Connection Between the Primary Instance and Replica Instances](#)
- [Synchronizing Clocks](#)
- [Starting and Stopping RSA Authentication Manager Services](#)
- [Configuring Your Browser to Support the RSA Authentication Manager Consoles](#)
- [Administering System Security](#)
- [Configuring Optional Proxy Servers for Remote Token-Key Generation](#)
- [Configuring an Optional Proxy Server for Remote RSA Self-Service Console Access](#)
- [Integrating the RSA RADIUS Server into the Existing Deployment](#)
- [Testing RSA RADIUS Operation](#)
- [Configuring Custom Port Numbers](#)
- [Removing Authentication Manager 6.1](#)

Backing Up a Standalone Primary Instance

If your deployment has a standalone primary instance (no replica instances), you must back up the database immediately after installing Authentication Manager. If the machine hosting the primary instance fails, use this backup to restore the database. Perform this backup periodically to ensure that a current version of the database is always available for disaster recovery. Store the backup in a safe location.

When To Perform a Backup

You must back up both the registry and the specified files (listed in the following sections, “[Backing Up a Standalone Primary Instance on Windows](#)” and “[Backing Up a Standalone Primary Instance on Linux and Solaris](#)”) immediately after installation. In addition, you must back up the specified files only (not the registry) after you perform the following operations:

- Add or delete a replica instance or server node.
- Add or delete an identity source.

Note: For instructions on restoring a backup, see the chapter “Disaster Recovery” in the *Administrator’s Guide*.

Backing Up a Standalone Primary Instance on Windows

To back up the primary instance:

1. Make sure that all Authentication Manager services are shut down. See [“Starting and Stopping RSA Authentication Manager Services on Windows”](#) on page 129.
2. Back up all of the files in the following directories (or wherever you chose to install Authentication Manager):
 - **C:\RSA_AM_HOME\RSA Authentication Manager**
 - **C:\Program Files\Common Files\InstallShield\Universal\rsa_am**
3. Back up the following registry keys:
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\OracleJobScheduler**
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\OracleRSATNSListener**
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\OracleService**

Important: Your key names do not match those specified above because the database SID is added to the end of each Oracle key. Make sure that you save all three key names.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RSAAM

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RSAAM_ADM

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RSAAM_NM

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RSAAM_PS

HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE

HKEY_LOCAL_MACHINE\SOFTWARE\RSA Security

4. Start the Authentication Manager database process. From the Windows Control Panel, click **Administrative Tools > Services > RSA Authentication Manager Database Server**.
5. Back up the internal database using the Manage Backups utility. For instructions, see the chapter “Disaster Recovery” in the *Administrator’s Guide*.

Backing Up a Standalone Primary Instance on Linux and Solaris

To back up the primary instance:

1. Make sure that all Authentication Manager services are shut down. See [“Starting and Stopping RSA Authentication Manager Services on Solaris and Linux”](#) on page 130.
2. Back up all of the files in the ***RSA_AM_HOME*** directory, all files in the ***\$HOME/InstallShield/Universal/rsa_am*** directory, and the following two files:

- ***/etc/security/limits.conf***
- ***/etc/services***

Use the following command:

```
gtar -czf am_backup.tar.gz
/$HOME/InstallShield/Universal/rsa_am
/RSA_AM_HOME/RSAsecurity
/etc/security/limits.conf
/etc/services
```

3. Start the RSA Authentication Manager database process. See [“Starting and Stopping RSA Authentication Manager Services on Solaris and Linux”](#) on page 130.
4. Back up the internal database using the Manage Backups utility. For instructions, see the chapter “Disaster Recovery” in the *Administrator’s Guide*.

Securing the Connection Between the Primary Instance and Replica Instances

Authentication Manager encrypts sensitive data in the database. Data that is not considered sensitive is stored in an unencrypted format. As part of Authentication Manager’s high availability and failover, data is sent between replication server nodes in both encrypted and unencrypted formats. RSA recommends that you implement your company’s networking best practices to ensure that network connections between server nodes in a WAN are secure. An example of best practice may include the use of a VPN and IPSec.

Synchronizing Clocks

RSA requires that all Authentication Manager instances and standalone RADIUS servers have their time synchronized to the same NTP server. In the absence of a reliable external time source, Authentication Manager will make a best effort attempt to synchronize the clock on each instance. Even with these controls, time drift may still exceed acceptable levels. Having a different time on several Authentication Manager instances can result in authentication failures and problematic replication behavior.

Note: If you use VMware, you must link the host to an NTP server and the guest OS to the same NTP server.

Configure the NTP server, and confirm that the synchronization is working before installing Authentication Manager.

Important: If the time on your system differs by more than 10 minutes from UTC, call RSA Customer Support before changing the time on a primary or replica instance.

To configure the NTP server, do the following on each instance:

1. Stop all Authentication Manager services.
2. Synchronize the system time with the NTP server time.
3. Start all Authentication Manager services.
4. Perform steps 1 to 3 on all your instances.

Starting and Stopping RSA Authentication Manager Services

If you need to start or stop Authentication Manager services manually for testing, troubleshooting, or other ongoing system administration, follow the instructions provided in this section.

This section describes:

- [“Starting and Stopping RSA Authentication Manager Services on Windows”](#)
- [“Starting and Stopping RSA Authentication Manager Services on Solaris and Linux”](#)

Note: The Node Manager is a watchdog process that starts and stops the Authentication Manager services. Node Manager must be running at all times in order for Authentication Manager services to be running.

Starting and Stopping RSA Authentication Manager Services on Windows

On Windows, Authentication Manager runs as services. The installer creates the following services:

- RSA Authentication Manager
- RSA Authentication Manager Administration Server
- RSA Authentication Manager Database Instance
- RSA Authentication Manager Database Listener
- RSA Authentication Manager Database Server
- RSA Authentication Manager Proxy Server
- RSA Authentication Manager Job Scheduler
- RSA Authentication Manager Node Manager

To start the RSA Authentication Manager services:

1. From the Windows Control Panel, click **Administrative Tools > Services**.
2. In the Services list, right-click **RSA Authentication Manager**, and click **Start** in the pop-up menu.

The corresponding status changes to **Started**. It may take several minutes for the service to actually start. The other Authentication Manager services also start automatically (if they are not already running).

Note: One service is not used: RSA Authentication Manager Job Scheduler (startup type = disabled). Ignore this service.

3. Close the Services dialog box.

To stop the RSA Authentication Manager services:

Note: Stop the primary instance.

1. From the Windows Control Panel, click **Administrative Tools > Services**.
2. In the Services list, right-click the services that you want to stop, and click **Stop** in the pop-up menu.

It may take several minutes for the services to actually stop.

Note: You must stop each service individually.

3. Close the Services dialog box.

Starting and Stopping RSA Authentication Manager Services on Solaris and Linux

On Solaris and Linux, the Authentication Manager services are automatically started if you reboot the system. You can start and stop the servers manually by using the **rsaam** command found in the **RSA_AM_HOME/server** directory. Use the command with the service name to stop, start, restart, and view the status of all servers or each service independently:

```
./rsaam stop|start|status|restart manager
./rsaam stop|start|status|restart proxy
./rsaam stop|start|status|restart admin
./rsaam stop|start|status|restart dblistener
./rsaam stop|start|status|restart db
./rsaam stop|start|status|restart dbconsole
./rsaam stop|start|status|restart all
./rsaam stop|start|status|restart nodemanager
```

Important: Do not start the servers as root user. RSA recommends that you create a Solaris or Linux security administrator for administration of Authentication Manager.

To start the RSA Authentication Manager services:

Change directories to **RSA_AM_HOME/server**, and type:

```
./rsaam start all
```

The following messages appear:

```
RSA Authentication Manager Database Listener: [OK]
RSA Authentication Manager Database Server: [OK]
RSA Authentication Manager Node Manager: [OK]
RSA Authentication Manager Administration Server: [OK]
RSA Authentication Manager Proxy Server: [OK]
RSA Authentication Manager: [OK]
RSA Authentication Manager Operations Console: [OK]
RSA Authentication Manager Radius: [OK]
RSA RADIUS Operations Console: [OK]
```

To stop the RSA Authentication Manager services:

Note: Stop the primary instance.

Change directories to **RSA_AM_HOME/server**, and type:

```
./rsaam stop all
```

The following messages appear:

```
RSA Authentication Manager: [OK]
RSA Authentication Manager Proxy Server: [OK]
RSA Authentication Manager Administration Server: [OK]
RSA Authentication Manager Node Manager: [OK]
RSA Authentication Manager Database Server: [OK]
RSA Authentication Manager Database Listener: [OK]
RSA Authentication Manager Operations Console: [OK]
RSA Authentication Manager Radius: [OK]
RSA RADIUS Operations Console: [OK]
```

Configuring Your Browser to Support the RSA Authentication Manager Consoles

The Authentication Manager administrative interfaces (the RSA Security Console, the RSA Operations Console, and the RSA Self-Service Console) are browser based. Before you can log on and administer Authentication Manager, you must configure your browser to support the Consoles as described in the following sections.

Enabling JavaScript

Before you log on, enable JavaScript.

Enabling JavaScript for Internet Explorer

To enable JavaScript:

1. In Internet Explorer, select **Tools > Internet Options > Security**.
2. Select the appropriate web content zone. If you use the default security level, JavaScript is enabled.
3. If you use a custom security setting, click **Custom Level**, and do the following:
 - a. Scroll down to **Miscellaneous > Use Pop-up Blocker**, and select **Disable**.
 - b. Scroll down to **Scripting > Active Scripting**, and select **Enable**.
 - c. Scroll down to **Scripting > Allow paste operations via script**, and select **Enable**.
 - d. Scroll down to **Scripting > Scripting of Java Applets**, and select **Enable**.

Enabling JavaScript for Mozilla Firefox

Generally, you do not need to enable JavaScript for Firefox. If JavaScript is disabled, perform this procedure.

To enable JavaScript:

1. Open the Firefox browser.
2. Click **Tools > Options > Content**.
3. Select **Enable JavaScript**.
4. Click **OK**.

Adding the RSA Security Console to Trusted Sites

If Internet Explorer is configured for enhanced security levels, you must add the Security Console URL to the list of trusted sites.

To add the RSA Security Console to trusted sites:

1. In Internet Explorer, select **Tools > Internet Options > Security**.
2. Select the Trusted Sites icon, and click **Sites**.
3. Type the URL for the Security Console in the entry next to the Add button.
4. Clear **Require server verification (https:) for all sites**.
5. Click **Add**.

Logging On to the Consoles

You can access any of the three Consoles by clicking the link on the desktop, or by opening a supported browser and typing the URLs listed in the following table.

Console	URL
RSA Security Console	https://<fully qualified domain name>:7004/console-ims
RSA Operations Console	https://<fully qualified domain name>:7072/operations-console
RSA Self-Service Console	https://<fully qualified domain name>:7004/console-selfservice

For example, if the fully qualified domain name of your Authentication Manager installation is “host.mycompany.com”, to access the Security Console, you would type the following in your browser:

https://host.mycompany.com:7004/console-ims

Note: On Windows systems, you can also access the Security Console by clicking **Start > Programs > RSA Security > RSA Security Console**.

To log on to the RSA Security Console:

1. Access the Security Console.
2. When prompted, type the User ID of the Super Admin specified during installation.
3. At the password prompt, type the Super Admin password specified during installation.

Note: The Super Admin role includes the ability to create a new Super Admin and other administrators. See the chapter “Preparing RSA Authentication Manager for Administration” in the *Administrator’s Guide*.

Important: When you log on to the Security Console for the first time, you are asked whether you want to trust the self-signed web certificate. To remove the security alert, save the self-signed web root to your browser’s trusted root repository.

To save the self-signed web root certificate:

1. In the security alert window, click **View Certificates**.
2. In the Certificate window, select the **Certification Path** tab.
You will see an untrusted certificate called “RSA Authentication Manager Root CA.”
3. Double-click the RSA certificate to open a new Certificate window.
4. In the Certificate window, click **Install Certificate**.
5. In the Certificate Import Wizard, click **Next**.
6. Click the **Automatically select the certificate store based on the type of certificate** option (this is the default), and click **Next**.
7. Click **Finish** to exit the Wizard.
8. In the security warning window, click **Yes**.
9. Click **OK** to return to the Certificate window.
10. In the Certificate window, click **OK**.
11. In the original Certificate window, click **OK**.
12. In the original security alert window, click **Yes** to open the Security Console.

Administering System Security

With the exception of system passwords, it is typically not necessary to change the default security settings described in this section.

Managing Passwords and Keys

The Authentication Manager installer generates keys and passwords used to access internal services such as the internal database. These credentials are stored in ***RSA_AM_HOME/utills/etc/systemfields.properties***. These files should also be backed up in ***RSA_AM_HOME/backup*** to assist in disaster recovery.

The Authentication Manager installer also generates a private key used for disaster recovery, **SYSTEM.SRK**. This private key is stored in ***RSA_AM_HOME/utills/etc/***. For highest security, remove the **SYSTEM.SRK** file from the system and store it in a secure location, such as removable media.

Default Administrator Account Password

You create default administrator accounts for the Security Console and the Operations Console during the primary instance installation. The Security Console account is given Super Admin permissions, meaning that the account can perform all tasks within Authentication Manager. The password you give for these accounts during installation is also used as the master password. You can change either or both the master password and the password for the default administrator accounts after installation.

Note: The default administrator account password for the Security Console and the Operations Console will expire according to the password policy of the security domain in which the accounts were created.

You use the Security Console to change the password for the default administrator accounts. For instructions, see the Security Console Help topic “Change a User’s Password.”

Master Password

Choosing a strong but memorable master password is important. The master password protects other sensitive credentials, and is used with many of the Authentication Manager command line utilities. The master password is initially the same as the password you assign to the default administrator account.

Note: The master password will not expire or change unless it is altered with the Manage Secrets utility.

RSA recommends that you develop a policy for maintaining the master password. The master password is needed to perform several critical tasks in the Operations Console.

When you add replica instances, you must use the master password to install them. After installation, the replica instances use this same master password for all internal uses, such as using command line utilities.

If you want to change your master password from the one specified during the installation of the primary instance, it is easiest to change it before adding replica instances. If you change it later, you must run the manual password change procedure on each replica instance.

You change your master password using the Manage Secrets utility.

To change your master password using manage-secrets:

1. From a command prompt, change directories to *RSA_AM_HOME/utills*.
2. Type:

```
rsautil manage-secrets --action change --new-password  
new_password
```
3. When prompted, type your current master password (the one you want to change). The message “Master password changed successfully” appears.
4. To make sure that your new master password is backed up, copy **systemfields.properties** to a secure location.

Important: When you change the master password on any primary instance, you are only changing it for that instance. You must also change the master password on each instance and on each remote RADIUS server. In addition, if you have a local RADIUS server, you must change the master password in the **radiusoc/utills** directory.

Internal System Passwords

The Manage Secrets utility is used to recover or change the passwords used to access various internal services. These services include:

- User name/password for managing the embedded WebLogic server
- User name/password for authenticating to the command server
- User name/password for accessing the database
- User name/password for managing the database schema
- User name/password for managing the database replication policies

To view a list of your system passwords, use the `--action listall` option. This command lists each password name and its value.

To view a list of your system passwords using manage-secrets:

1. From a command prompt, change directories to *RSA_AM_HOME/utills*.
2. Type:

```
rsautil manage-secrets --action listall
```
3. When prompted, type your master password.

Managing Certificates and Keystores for SSL

SSL is enabled by default for all communication ports. During installation, a self-signed root certificate for the deployment is generated and stored in *RSA_AM_HOME/server/security/root.jks*.

Additional server certificates are generated and signed by this root certificate when you add additional server nodes and replica instances.

Internet Explorer 6 Considerations

Because the newly created default self-signed certificate is not in your list of trusted root certificates, you receive a warning when first accessing the Security Console. Importing the root certificate into the browser, as described in the installation procedure, prevents this warning from displaying.

Internet Explorer 7 Considerations

When accessing the Security Console, in Internet Explorer 7, a message appears warning you that there is a problem with the web site's security certificate, and advises you not to continue to the web site. Click **Not Recommended** to get to the Security Console. A "Certificate Error" message appears on the Security Console URL. Adding the self-signed root certificate to the trusted root list prevents this warning from appearing.

Replacing Installed Certificates

If you have an existing certificate authority and prefer to issue your own certificates, you can replace the certificates that the Authentication Manager installer generates with certificates of your own using the approved replacement procedure.

Replacing the installed certificates requires familiarity with Public Key Infrastructure (PKI), and this procedure can take an hour or more to complete. This procedure replaces the certificate used for web browser connections to the RSA Security Console and RSA Self-Service Console as well as connections to the API. This procedure does not replace the certificate used for trusted realms, the RADIUS Operations Console, or web browser connections to the RSA Operations Console.

If you want to perform the approved replacement procedure, contact RSA Customer Support for more information.

Importing LDAP Certificates

If you choose to integrate LDAP directories, it may be necessary to import additional trusted root certificates for Authentication Manager to correctly authenticate the LDAP server. See "[Setting Up SSL for LDAP](#)" on page 186.

Legacy Compatibility Keystore

Certain internal services and protocols use these certificates and keys provided with your license:

sdti.cer. A copy of the **sdti.cer** signing certificate.

server.cer. RSA Authentication Manager server certificate generated by manufacturing for each license and signed by **sdti.cer**.

server.key. Private key representation for **server.cer**.

These certificates and keys are not replaceable.

Configuring Optional Proxy Servers for Remote Token-Key Generation

RSA recommends that you configure the following two proxy servers for use by the Authentication Manager Remote Token-Key Generation service. This service uses the Cryptographic Token-Key Initialization Protocol (CT-KIP).

Adding a Proxy Server to Create Secure URLs

If you install Authentication Manager inside of a secure DMZ, you may decide only to allow traffic to it through a proxy server. If you choose to proxy the traffic going to your Authentication Manager, RSA recommends the following:

- Establish your proxy on the standard http port, which is port 80, or the standard SSL port, which is port 443.
- From the Security Console, click **Setup > Component Configuration > Authentication Manager**. Edit the **Token Key Generation** and **Service Address** fields to reflect the location of the proxy server.
- Configure your proxy server to forward all traffic to Authentication Manager and maintain all path information and URL parameters. A typical URL passed to the proxy server looks as follows:

`https://mydomain.com/...`

The proxy server transforms this URL similar to the following:

`https://am-server.na.ex.net:7004/...`

Note: The ellipse in the above URLs represents a dynamically generated query string. Authentication Manager automatically generates this string, which must be passed along as part of the URL.

Note the following about the above URLs:

- The domain name changes.
- The port changes to 7004.

The remainder of the URL stays the same.

Configuring a Proxy Server for CT-KIP Failover

Occasionally, it may be necessary to remove your primary instance from your deployment and promote a replica instance to replace it. When this happens, token-key generation URLs and service addresses that you have distributed to users, but that users have not yet used, become invalid.

If your proxy server supports failover mode, you can configure it to pass CT-KIP data to the new primary instance. This allows users to use the original token-key generation URLs and service addresses and saves administrators from the task of sending new URLs to users.

Configuring an Optional Proxy Server for Remote RSA Self-Service Console Access

Because the Self-Service Console is installed on the same machine as Authentication Manager, RSA recommends that you set up a proxy server in your network's DMZ to protect Authentication Manager and accept self-service requests.

Adding a Proxy Server for Secure RSA Self-Service Console Access

To restrict users from directly accessing Authentication Manager, configure a proxy server to accept Self-Service Console requests and proxy to the Self-Service Console. Administrators who need to access Authentication Manager through the Internet can use a VPN to gain access to the internal network, and Authentication Manager.

The Self-Service Console uses the same port as the Security Console, port 7004. The URL for the Self-Service Console is:

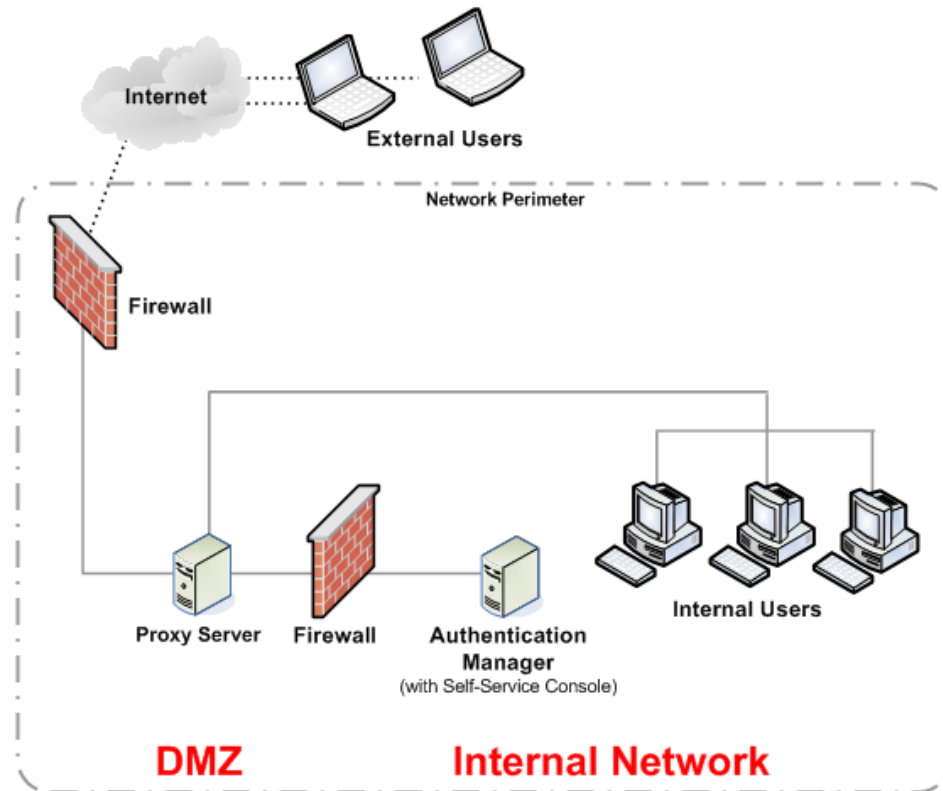
`https://<fully qualified domain name>:7004/console-selfservice`

To hide the domain name from Self-Service Console users, set up an alias URL that routes traffic to the Self-Service Console web server after the user has authenticated. Once you have set up an alias URL, you must manually edit the Self-Service Console e-mail templates to reflect the new URL. For instructions, see “Customizing E-mail Notifications for Proxy Servers” in the *Administrator's Guide*.

An example of an alias URL is:

`https://mydomain.com/self-service`

The following figure shows a basic network setup with Self-Service Console traffic directed through a proxy server.



For more information on setting up a proxy server in your network, go to <http://www.rsa.com/node.aspx?id=2535>.

Configuring a Proxy Server for RSA Self-Service Console Failover

In the case of failover, the administrator should immediately change the IP address that is associated with the Self-Service Console alias URL to that of the new primary instance. This allows users to use the same Self-Service Console URL when a primary instance is removed from a deployment and a replica is promoted. If this change is not made, the proxy server continues to try to access the original primary server, causing downtime for users.

Integrating the RSA RADIUS Server into the Existing Deployment

This section describes the RADIUS server post-installation tasks.

Configuring the RADIUS Server on the Primary Instance

After installing RSA Authentication Manager and RADIUS server on the primary instance host machine, you must configure RADIUS to complete the installation.

To configure the RADIUS server on the primary instance:

1. On the primary instance, launch and log on to the RSA Operations Console.
2. Click **Deployment Configuration > RADIUS > Configure Server**.
3. On the Additional Credentials Required page, enter the current Super Admin User ID and password. Click **OK**.

Important: Configuring the RADIUS server cannot be undone. Ensure that you have correctly supplied the required information before you submit it. If you make a mistake, use the Operations Console to delete the server and then configure the server again. To configure a RADIUS server again, you must start the RADIUS Operations Console service. The RADIUS Operations Console service must be up and running when you configure the RADIUS server again.

4. On the Configure RADIUS Server page, enter the required information:
 - **Replication Secret.** Enter and confirm a replication secret. The replication secret secures communication between the RADIUS primary server and a RADIUS replica server. (You can choose any value for the replication secret. There are no rules for the length or character type except that you cannot use spaces.)
 - **Master Password.** The current master password.

Important: When entering the administrator User ID and password, ensure that you do this correctly. This cannot be undone.

- **Administrator User ID.** The current Super Admin User ID.
 - **Administrator Password.** The current Super Admin password.
5. Click **Configure**.

Migrating the RSA RADIUS 6.1 Data Files on the Primary Instance

After you configure the RADIUS server on the primary instance, use the RSA Operations Console to migrate the RSA RADIUS 6.1 data files.

To migrate the RSA RADIUS 6.1 data files on the primary instance:

1. On the primary instance, launch and log on to the RSA Operations Console.
2. Click **Deployment Configuration > Migration > RADIUS Database**.
3. On the Additional Credentials Required page, enter the current Super Admin User ID and password. Click **OK**.
4. On the RADIUS Server Migration page, browse to the location of the RADIUS migration package file.
You generate the RADIUS migration package file before you install the primary instance. For more information, see [“Creating a RADIUS Migration Package File”](#) on page 67.
5. Click **Start Migration**.
6. Click **Done**.
7. Use the RSA Security Console to force replication to all RADIUS replica servers:
 - a. On the primary instance, launch and log on to the RSA Security Console.
 - b. Click **RADIUS > RADIUS Servers**.
 - c. Click **Force Replication to All**.

Configuring the RADIUS Server on the Replica Instance

After installing RSA Authentication Manager and the RADIUS server on the replica instance machine, you must configure RADIUS to complete the installation.

To configure the RADIUS server on the replica instance:

1. On the replica instance, launch and log on to the RSA Operations Console.
2. Click **Deployment Configuration > RADIUS > Configure Server**.
3. On the Additional Credentials Required page, enter the current Super Admin User ID and password. Click **OK**.

Important: Configuring the RADIUS server cannot be undone. Ensure that you have correctly supplied the required information before you submit it. If you make a mistake, use the Operations Console to delete the server and then configure the server again. To configure a RADIUS server again, you must start the RADIUS Operations Console service. The RADIUS Operations Console service must be up and running when you configure the RADIUS server again.

4. On the Configure RADIUS Server page, enter the required information.
 - **Realm.** If necessary, select the realm for which the RADIUS server is being configured.
 - **Replication Secret.** Enter and confirm the replication secret specified during the configuration of the RADIUS server on the primary instance.
 - **Master Password.** The current master password.
 - **Primary Hostname.** The fully qualified hostname of the primary instance.
 - **Primary IP Address.** The IP address of the primary instance.

Important: When entering the administrator User ID and password, ensure that you do this correctly. This cannot be undone.

- **Administrator User ID.** The current Super Admin User ID.
 - **Administrator Password.** The current Super Admin password.
5. Click **Configure**.

Editing the RADIUS Server Configuration Files

Usually, the default settings in the RADIUS server configuration and dictionary files (such as *.ini or *.dct) are satisfactory. If you need to make any changes to the default settings, use the Operations Console. For instructions, see the Operations Console Help topic “List and Edit RADIUS Configuration Files.”

Using the RSA Security Console to Replicate Changes

Changes made in the RADIUS primary database are not automatically propagated to all of the RADIUS replica servers. You must use the Security Console to force the replication of database changes each time they occur. For information on how to replicate primary database changes, see the Security Console Help topics “Force Replication to a Single RADIUS Replica Server” and “Force Replication to All RADIUS Replica Servers.”

Adding Clients to the RADIUS Server and Editing Clients

After installing a RADIUS server, you must add RADIUS clients to the new RADIUS server. For instructions, see the Security Console Help topic “Adding RADIUS Clients.” However, you do not have to add any RADIUS clients that already existed in the RADIUS server prior to a migration from RSA RADIUS 6.1.

If you added a new IP address or changed the IP address of the RADIUS server as part of the installation, you must use the Security Console to edit the RADIUS clients so that they know about new or modified server IP addresses. For instructions on updating RADIUS clients, see the Security Console Help topic “Edit RADIUS Clients.”

Testing RSA RADIUS Operation

There are two ways to test RSA RADIUS operation:

- Test to see that RSA SecurID authentication works between the RSA RADIUS server and Authentication Manager. You can use one of the many third-party RADIUS test authentication tools to facilitate your testing. (You can find many of these tools on the Internet.)
- Test end-to-end authentication to ensure that a RADIUS client can successfully authenticate using RSA RADIUS and Authentication Manager.

Testing End-to-End Authentication

Use the following test to ensure that a user can successfully authenticate using RSA RADIUS and Authentication Manager.

To test end-to-end authentication:

1. Configure a RADIUS client to communicate with the RSA RADIUS server. For more information, see the Security Console Help topic “Add RADIUS Clients.”
2. Provide a test user with an RSA SecurID token and any required software.
3. If you want to test one particular RADIUS server, shut down other RADIUS servers to force testing of the active server.
4. Have the user attempt to access a protected resource using the SecurID token.

If the user can successfully authenticate, RADIUS is properly configured.

If the user cannot successfully authenticate, see “[Unsuccessful End-to-End Authentication on RSA RADIUS](#)” on page 202 for troubleshooting tips.

Configuring Custom Port Numbers

If your version 6.1 servers used custom ports, rather than the default ports, for the following services, you can edit the port numbers through the Security Console.

- agent authentication
- agent auto-registration
- offline authentication download

For more information, see the Security Console Help topic “Configure RSA Authentication Manager.”

Removing Authentication Manager 6.1

The version 7.1 installation process disables version 6.1, but does not uninstall it. The version 6.1 installation is maintained in case you want to revert to it. As a result, you must manually uninstall version 6.1 when you no longer need it.

Note: In Windows, the Start menu items for version 6.1 remain available until you remove RSA Authentication Manager 6.1 from the system.

On Windows

Use the Add/Remove Software Control Panel to uninstall RSA Authentication Manager.

1. Click **Start > Settings > Control Panel > Add or Remove Software**.
2. Select **RSA Authentication Manager**, click **Remove**, and then click **Yes**.
Version 6.1 is removed.

On Linux and Solaris

Delete the directory in which version 6.1 was originally installed.

For more information on reverting, see Appendix F, "[Reverting RSA Authentication Manager 7.1 to Version 6.1](#)."

8

Installing the RSA Authentication Manager MMC Extension

- [MMC Extension Overview](#)
- [System Requirements and Prerequisite](#)
- [Installation Process](#)
- [Post-Installation](#)

MMC Extension Overview

The RSA Authentication Manager 7.1 MMC Extension extends the Microsoft Active Directory Users and Computers Management (ADUC) snap-in. It extends the context menus, property pages, control bars, and toolbars to provide a convenient way for Windows Active Directory users to perform RSA SecurID token management. For more information on the administrative actions enabled by this extension, see the *Administrator's Guide*.

System Requirements and Prerequisite

Install the RSA Authentication Manager 7.1 MMC Extension only on the following platforms:

- Windows XP Professional SP1 or later, with Windows Server 2003 Administration Tools Pack and Internet Explorer 6.0 or later installed
- Windows Server 2003 SP1 or later (if Active Directory is not available, install Windows Server 2003 Administration Tools Pack), with Internet Explorer 6.0 or later installed

The following prerequisite must be met for installation of the MMC Extension.

The administrator running the installation for the MMC Extension setup program must have the appropriate administrative permissions to perform an installation. The appropriate level of permissions (for example, domain level) depends on your Windows network configuration. At a minimum, the installer must be a domain administrator and a local machine administrator.

Installation Process

Choose one of these installation processes depending on whether you want to administer locally on the Active Directory host or remotely from a Windows station:

- [“Installing the MMC Extension for Local Access”](#)
- [“Installing the MMC Extension for Remote Access”](#)

Installing the MMC Extension for Local Access

Use this installation process if you want to perform Authentication Manager administration through the MMC Extension directly on the host where Active Directory is installed.

To install the MMC Extension on the Active Directory host:

1. Locate and launch the installer at `client\mmc\rsammc.exe`.
2. Respond to the prompts for **Welcome**, **Select Region**, and **License Agreement**.
3. When prompted for **Destination Location**, either accept the default location or enter an alternative location.
4. For Authentication Manager server settings, enter your values for:
 - Authentication Manager server hostname
 - Authentication Manager server port number
 - RSA Security Console URL

Note: Replace the Security Console fully qualified name and port number with your actual values, but do not change console-am.

5. Review the Pre-installation screen, and click **Next** to continue.
6. Click **Finish**.

Installing the MMC Extension for Remote Access

To use the MMC Extension remotely from Windows XP or a Windows Server 2003 without Active Directory installed, make sure that you meet these additional requirements before installing on the remote host:

- Windows Server 2003, with Active Directory installed, can be accessed from the Windows XP machine, and the Windows XP machine is part of the domain defined by the Windows Server 2003 machine.
- The administrator uses a domain user account to log on to the Windows XP machine.
- The administrator using the Windows Server 2003 administration pack to remotely administer the Active Directory is granted appropriate administrative permissions. The appropriate level of permissions (for example, domain level) depends on your Windows network configuration.

Note: Remote administration mode is not available on Windows x64. You must install MMC in local admin mode on 64-bit computers and use remote Desktop or the Windows Management Instrumentation Command-line (WMIC).

Windows Server 2003 Administration Tools Pack

The Windows Server 2003 Administration Tools Pack installs a set of server administration tools onto a Windows XP Professional or Windows Server 2003 machine. This allows administrators to remotely manage Windows 2000 as well as Windows Server 2003.

The tools contained in the file are officially part of the Windows Server 2003 product, and the Administration Tools Pack installs them onto your Windows XP Professional or Windows Server 2003 machine. Download the Administration Tools Pack for your specific operating system and service pack from the Microsoft web site.

To install the MMC Extension on the Active Directory host:

1. Install the Administration Tools Pack, and restart the machine if necessary.
2. Locate and launch the installer at **client\mmc\rsammc.exe**.
3. Respond to the prompts for **Welcome**, **Select Region**, and **License Agreement**.
4. When prompted for **Destination Location**, either accept the default location or enter an alternative location.

5. For Authentication Manager server settings, enter your values for:
 - Authentication Manager server hostname
 - Authentication Manager server port number
 - Security Console URL

Note: Replace the Security Console fully qualified name and port number with your actual values, but do not change console-am.

6. Review the Pre-installation screen, and click **Next** to continue.
7. Click **Finish**.

Post-Installation

After a successful installation, configure your Internet Explorer security settings and start the ADUC before administering Authentication Manager through the MMC Extension.

Also, make sure that:

- Authentication Manager is installed and running.
- Active Directory is configured and registered as an identity source. See Appendix C, [“Integrating an LDAP Directory.”](#)
- The Windows user for the MMC Extension is a valid Active Directory administrator and a valid Authentication Manager administrative user. For more information on administrator and administrative permissions, see the *Administrator’s Guide*.

Configuring Internet Explorer Security Settings

Add the Security Console to your list of trusted sites, and make sure that your security settings comply with the following requirements.

To add the Security Console deployment to your Internet Explorer list of trusted sites:

1. Open Internet Explorer on the machine hosting the MMC Extension.
2. Click **Control Panel > Internet Options > Security > Local Intranet > Sites > Advanced**, and enter the URL for your Security Console. For example: `https://mypc.mydomain.com:7004/console-am`
3. Click **OK** or **Apply** to save the changes.

To configure Internet Explorer security settings:

1. In Internet Explorer, select **Tools > Internet Options > Security**.
2. Click **Custom Level**.

3. At the bottom of the Security Settings window, in **Reset custom settings**, select **Medium** from the drop-down menu, and click **Reset**.
4. In the Settings window, select **enable** for these two settings:
 - **Download signed ActiveX controls**
 - **Launching programs and files in an IFRAME**
5. Click **OK > OK**.
6. Close the browser, and open a new browser window for the Security Console.

Starting the Active Directory User and Computer Management Console

To use the MMC Extension for Authentication Manager administration, you must start the Active Directory User and Computer Management Console. Do one of the following:

- Click **Control Panel > Administrative Tools > Active Directory Users and Computers**.
- From a command prompt, run **dsa.msc**.

A

Migration Data Conversion

- [Data Conversion Table](#)
- [Migration Report](#)

Data Conversion Table

The following table describes how different types of data are migrated.

Data	Migration Result
LDAP synchronization jobs	Records with direct LDAP associations, like users and groups, are verified to ensure they exist in the identity source. Records with no LDAP associations are created in the internal database. When a group contains both LDAP and non-LDAP users, multiple groups are created: one for the non-LDAP users and one for each LDAP source associated with the LDAP users in the group.
User data	User data is migrated, including the following: <ul style="list-style-type: none"> • The name of the RADIUS profile, if any assigned. • Cross-realm association, if any. • Logons with domain name. The name may be converted from NTLM to UPN.
PIN data	PINs are migrated. Expiration dates for PINs are not migrated. If you want to set expiration dates for migrated PINs, see the Security Console Help topic “Edit RSA SecurID PIN Lifetime and Format Requirements.”
Site data	Sites are migrated to security domains.
Group data	Groups are migrated to user groups. In version 6.1, groups may contain LDAP and non-LDAP users. Migration creates parallel groups for LDAP and non-LDAP users. Group access restrictions are also migrated. Group administration associations are not migrated.
User to group membership data	Group memberships are migrated to user group memberships. Other group membership data, such as the group alias and shell data is also migrated.

Data	Migration Result
Agent to group activation data	<p>Group activations on authentication agents are migrated. Any agent with a group association is migrated as a restricted agent, due to the implementation of group activations in version 7.1.</p>
User agent activation data	<p>User activations on authentication agents are migrated only when the agent is a restricted agent. If an agent is open to all users (unrestricted), existing user-agent associations for that agent are not migrated. These cases are noted in the migration report.</p> <p>If an agent is restricted, migration maintains user activations (and their access time restrictions) by manufacturing a new group, adding the user to the group, and activating the group on the agent, with the access time restrictions of the user. In cases where there are multiple users activated on the same restricted agent, the groups are created based on the access time restrictions.</p> <p>For example, if there are three users activated on an agent, and their access times are between 8 a.m. and 5 p.m., and the other user's access time is between 3 p.m. and 11 p.m., two groups are created: one with access times between 8 p.m. and 5 p.m., and one with access times between 3 p.m. and 11 p.m. The appropriate users are then added to the groups, and the groups are activated on the agent. In each case, the agent is migrated as a restricted agent.</p>
Agent data	<p>Agent data is migrated, including agent name, IP address, group activations, and secondary nodes. Individual user activations on agents are migrated to new activated groups.</p> <p>Agent auto-registration settings are migrated. For RSA SecurID for Windows Authentication Agent 6.1.2, this includes the ability to allow auto-registration to change the primary IP address of an agent. For RSA SecurID for Windows Authentication Agents prior to version 6.1.2, you can choose to protect the IP addresses of auto-registered agents during the migration process as part of the advanced configuration options.</p> <p>RADIUS connection parameters stored in the agent record are not migrated.</p>
Token data	<p>Token records and their user assignments are migrated.</p>
Secondary node data	<p>Secondary nodes for authentication agents are migrated.</p>
One-time password data	<p>One-time password data is migrated, both lost token fixed passwords and one-time tokencode sets.</p>

Data	Migration Result
Client type data	<p>Agent types are not migrated. Version 7.1 recognizes only two types of agents: standard agent and web agent. The version 6.1 agent types currently have no impact on runtime behavior related to Next Tokencode mode. Additionally, version 7.1 does not support single transaction agents.</p>
System settings data	<p>You can choose to migrate all system settings, except for the PIN generation setting.</p> <p>The ability to allow users to choose between a system-generated PIN, and a user-created PIN is no longer available. You must set the PIN policy to be either system-generated or user-created.</p>
Administrator data	<ul style="list-style-type: none"> • Realm and site administrators are migrated. However, administrators assigned to groups are not migrated as administrators because in version 7.1 administrators cannot be scoped to groups, only to security domains. • Any administrator whose assigned task list contains only the ability to edit system parameters is not migrated as an administrator. Since system parameters are not migrated, administrators with only the ability to edit System Parameters have no equivalent version 7.1 task available to them. • Any administrator whose assigned task list includes the ability to list realms does not have the ability to view trusted realms (the version 7.1 equivalent of version 6.1 cross-realm relationships). For example, an administrator assigned the version 6.1 Group Task List or Site Task List cannot view trusted realms. In version 7.1, the ability to view trusted realms requires permission to configure trusted realms.
Administrative role data	<p>Realm and site administrative roles are migrated. The group role is migrated, but not assigned to any administrator. Customized roles are migrated to equivalent custom roles.</p> <p>RSA recommends that you verify the scope and permissions of each migrated administrative role to ensure that assigned administrators retain sufficient privileges.</p>

Data	Migration Result
Task lists data	<p>Task list data is migrated to version 7.1 permissions, except when there is no equivalent permission. For example, the task allowing administrators to edit System Parameters, any tasks related to LDAP Sync Jobs, or any tasks related to group administration.</p> <p>The following tasks related to the configuration of logging are not migrated, as there are no equivalent permissions in version 7.1:</p> <ul style="list-style-type: none"> • Automate Log Maintenance • Configure Logged Events • Delete Log Entries • Edit System Log Parameters • Enable/Disable System Logging • Restore Filter Configuration • Save Filter Configuration • Log Statistics <p>The following tasks related to policies require the Super Admin role. Version 6.1 administrators whose task lists include these tasks can no longer perform these tasks unless they are assigned the Super Admin role.</p> <ul style="list-style-type: none"> • Add/Edit/Delete Offline Auth Configuration • Add/Edit/Delete RADIUS Policy • Add/Edit/Delete EAP Protected OTP Policies • Add/Edit/Delete Token Policies <hr/> <p>Note: Any administrator whose task list contains only the ability to edit system parameters is not migrated as an administrator. Since system parameters are not migrated, administrators with only the ability to edit System Parameters have no equivalent version 7.1 task available to them.</p> <hr/>
User extension data	User extension data is migrated, and is exported to a comma-separated value (.csv) file in the migration output directory.
Token extension data	Token extension data is migrated to the notes field of the token, and is exported to a comma-separated value (.csv) file in the migration output directory.
Group extension data	Group extension data is migrated to the notes field of the group, and is exported to a comma-separated value (.csv) file in the migration output directory.

Data	Migration Result
Agent extension data	Agent extension data is migrated to the notes field of the agent, and is exported to a comma-separated value (.csv) file in the migration output directory.
Site extension data	Site extension data is migrated to the notes field of the migrated security domain, and is exported to a comma-separated value (.csv) file in the migration output directory.
RADIUS profile data	The RADIUS profile names and profile assignments to users are migrated. The profile attributes and values are stored in the RSA RADIUS server database and migrated separately from Authentication Manager data. Note: If a RADIUS profile was designated as the default profile in version 6.1, the profile is migrated to version 7.1 but it is no longer designated as the default profile. To specify this profile, or any profile, as the default after migration, use the RSA Security Console. For more information, see the Security Console Help topic “Configure Your Realm.”
Replica data	Data about replica servers is not migrated. However, the replica servers themselves can be migrated. The migrated primary instance does not attempt to communicate with legacy replica servers.
Cross-realm data	Cross-realm relationships are migrated. Version 7.1 implements a new trusted realm model that is different than the legacy cross-realm. For more information see “Trusted Realms” on page 26.
Agent delta data	Changes to authentication agents made on replica servers are migrated and processed.
User delta data	Changes to users made on replica servers are migrated and processed.
Token delta data	Changes to tokens made on replica servers are migrated and processed. This includes the deletion of tokens and the processing of replacement tokens.
One-time password delta data	Changes to one-time passwords made on replica servers are migrated. This includes the deletion of a one-time password that has been used to authenticate.
Log records	Log records must be manually migrated. For more information, see “Migrating Log Files” on page 80.

Migration Report

The migration report lists how your data is processed during the migration, including if data was migrated with no changes, with some changes, or not migrated at all. The report includes the following information:

- Parameters and options you selected for the migration.
- A summary of the dump file analysis results, including which type of data was found in the dump file.
- A list of the objects migrated, including users, user groups, tokens, agents, policies, administrative roles, and extension data.

The following sections outline some situations that you may encounter while migrating and is designed to let you perform some cleanup tasks on your data.

Multivalued Extension Data

In version 6.1, extension data can be defined for individual objects (such as individual users, groups, agents and tokens) only, and cannot be defined on a system-wide basis (so you cannot define one set of extension data for all users, all groups, all agents or all tokens). As a result, it is possible that your database may contain multiple extension fields that contain the same type of data (for example, a phone number for users), but it may be inconsistently named, and the format of the value may be inconsistent as well. Each of these extension fields is migrated as a separate field and added to each related object in the database.

For example, there may be an extension field for the phone number of users, but the name of the extension field may be different for each user (Phone Num., Phone Number, Ph. Num.). After migration, every migrated user has multiple extension attributes for phone number. In the example, every user has extension attributes named Phone Num., Phone Number, and Ph. Num. Two of the three attributes are empty. Only the attribute that was specified as an extension field for the user contains the data for the phone number.

If the migration report shows inconsistent use of extension data, review the report, and determine which field name you want to use. Edit the extension data of the non-compliant users to match the preferred extension field name.

Users in Multiple Groups in Different Sites

In version 6.1, it is possible for a user to have multiple group memberships, with the groups belonging to different sites. In version 7.1, a user or user group can exist in only one identity source. Therefore, a user from one identity source cannot be a member of a user group from a different identity source.

When sites are migrated to security domains, it is no longer possible for a user to belong to groups that were in different sites, because, after migration, these user groups belong to different security domains, and a user cannot belong to more than one security domain. The migration process has to determine which security domain owns the user, and make the user a member of the user group that belongs to the same security domain.

Groups Containing Users from Multiple Identity Sources

In version 6.1, it is possible for a group to contain users from multiple identity sources (for example, the internal database and a directory server). A group can belong to a single identity source (either the internal database or a directory server). In version 7.1, a user or user group can exist in only one identity source. Therefore, a user from one identity source cannot be a member of a user group from a different identity source.

The process of determining where to migrate group members can be complicated when there is a mixture of users from multiple identity sources in the group. A user created from an LDAP synchronization job belongs to an LDAP identity source, while a user created through the version 6.1 Database Administration application belongs to the internal database. For a group that contains a mixture of users from LDAP directories and the internal database, the migration process creates multiple groups: one for the internal database, and additional user groups for each of the LDAP directories specified in the LDAP synchronization jobs.

Important: The directory server must be read/write enabled to allow the migration process to create the required groups in the directory servers.

In such cases, the migration report states that new groups are created for the users belonging to the LDAP identity sources. After migration, your deployment contains one group for each identity source. The non-LDAP users are added to a group in the internal database. The LDAP users reside in groups created, if necessary, in the directory server.

Activations on Restricted Agents When LDAP Synchronization Jobs Do Not Contain Group Data

LDAP users cannot authenticate through certain agents after migration, if the following conditions exist prior to migration:

- The LDAP synchronization job that synchronizes the user is not configured to synchronize the LDAP group to which the user belongs.
- The directory server accessed by the LDAP synchronization job is read-only.
- The user belongs to a group that exists only in the version 6.1 database.
For example, the administrator adds an LDAP user to a group created using the version 6.1 Database Administration application.
- The version 6.1 group is activated on one or more restricted authentication agents.
If the user is activated on an authentication agent, migration attempts to create a user group with the user as a member, and activate the user group on the agent.

In version 6.1, it is possible to synchronize LDAP users without synchronizing their LDAP groups. Users synchronized by such a job may have a group specified, but the group resides only in the internal database, meaning that the group relationship is known only to Authentication Manager. Any group membership specified in the directory server is unknown to Authentication Manager.

Migration processes these users with no group membership. If the group specified in version 6.1 was activated on a restricted agent, migration cannot create an equivalent group. This causes users assigned to groups activated on restricted agents to fail in their authentication attempts.

To resolve this problem, contact the administrator responsible for the directory server, and request the group data so that you can add it to the LDAP synchronization job.

Important: The directory server must be read/write enabled to allow the migration process to migrate the required groups in the directory servers.

PIN Options for Emergency Codes

After migration, the PIN options for offline emergency tokencodes are also applied to the authentication methods available to users who have lost their tokens. In version 7.1, these methods are known as online emergency codes. In version 6.1, there are two methods available: fixed password or one-time password sets. The PIN options for the fixed password or one-time password sets are selected by the administrator when the password or sets are generated. There is no system-wide parameter for the PIN options

However, after migration, the values configured for the generation of offline emergency codes are applied to these online emergency codes as well. Existing fixed passwords and one-time password sets are migrated, and continue to function in the migrated version 7.1 deployment, but any newly generated fixed passwords (known as fixed passcodes in version 7.1) and one-time password sets (known as emergency codes in version 7.1) adhere to the PIN options configured for the version 6.1 offline emergency codes. To view the existing version 6.1 settings, in the Authentication Manager 6.1 Database Administration application, from the System menu, click **System Configuration > Edit Offline Auth Config**, and look under **Codes Contain**.

Adding SecurID_Native as a Method of Administrator Authentication

If you see the following message in the migration report, you must configure the Security Console to use the SecurID_Native method of authentication:

```
SecurId_Native authentication is allowed in the dump file.  
As system settings were not migrated, an admin may not be  
able to log into admin console using SecurID as an  
authentication method.
```

The above message is displayed in migration reports under the following conditions:

- Your version 6.1 Authentication Manager System Parameters include SecurID cards, fobs, or USB as an Administrator Authentication Method.
- You did not migrate the System Parameters.

As a result, any Authentication Manager administrators who use SecurID cards, fobs or USB tokens as their exclusive method of authenticating to the version 6.1 Database Administration application will not be able to log on to the Security Console. You can resolve this issue by migrating the System Parameters, or by enabling **SecurID_native** as a method of Console Authentication.

To add SecurID_Native as a method of Console Authentication:

1. In the Security Console, click **Setup > Authentication Methods**.
2. In the Console Administration field, add **SecurID_Native** as an authentication method.
3. Click **Save**.

B

Migration Scenarios

- [Scenario 1: Small Business, Single Site, Migration on Same Hardware](#)
- [Scenario 2: Mid-Sized Business, Single Site, Multiple LDAP Synchronization Jobs](#)
- [Scenario 3: Large Enterprise, Multiple Geographic Sites, Multiple Realms](#)

Scenario 1: Small Business, Single Site, Migration on Same Hardware

B & B Boxing (a single office location with 50 remote users)

B & B Boxing is a small private company with 1,000 employees, 50 of whom require remote access to their network. As a private company, they have no specific Sarbanes-Oxley requirements. However, there is the possibility of other legal or customary compliance issues.

The company has a small, Windows-based network with Windows-based client PCs and laptops managed by four full-time IT administrators. The network includes a domain controller inside the corporate firewall, which contains a variety of file and print servers, and a client database. In the demilitarized zone (DMZ), the network includes a VPN server and a proxy server. They use password authentication for all network access inside the corporate firewall, and RSA SecurID authentication for remote access through a VPN.

Business Needs

B & B Boxing uses RSA SecurID authentication to satisfy the business goal of secure remote access.

How Migration Affects the Existing Deployment

Physical Deployment

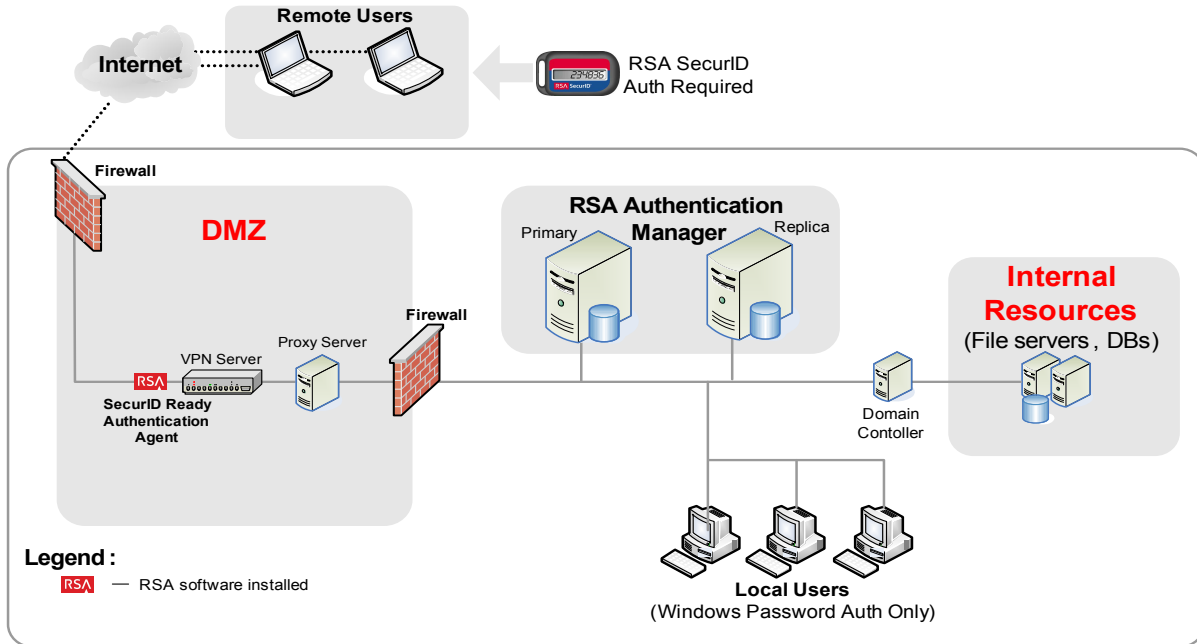
B & B Boxing has a Base Server license and has no need to upgrade to an Enterprise Server license. They have one Authentication Manager primary instance and one replica instance (for authentication and failover) at the same geographic site. The company uses the Authentication Manager internal database as the sole identity source. There are no changes to the network or to the physical machines on which the Authentication Manager is installed. Administrators manually assigned and distributed RSA SecurID tokens to the 50 employees who are required to use them.

The following table lists the hardware affected by the Authentication Manager migration, the impact upon the hardware, and any tasks that the administrator needs to perform as a result of migration.

Hardware	Impact/Task
Server	<p>Perform a rolling upgrade to version 7.1 on the same hardware as the existing versions 6.1.</p> <p>There are no changes to the hardware configuration. Delta records that accumulated on the replica while the primary was being migrated are merged into the migrated replica and replicated to the migrated primary. There is no data loss.</p>
Agent	<p>Verify that third-party agents and RSA Secured products are supported.</p> <p>No change to the sdconf.rec file is required. During the rolling upgrade, agents authenticate to the replica while the primary is being migrated. Once the primary is migrated and brought online, the replica is shut down, and agents authenticate to the primary. The primary sends the latest server list (which contains only the primary until the replica is migrated and brought online) to the agents.</p>
Replicas	<p>There are no changes to the hardware configuration.</p>
Server nodes	<p>The deployment does not use multiple server nodes in the migrated environment.</p>

System Diagram Before and After Migration:

B & B Boxing



Logical Deployment

The small size of B & B Boxing simplified their logical deployment and allowed them to accept many of Authentication Manager’s default settings. The company was already using a single realm, with no sites or groups, so continued to use only a single realm. In the migrated version 7.1 environment, a single, top-level security domain contains all users, administrative roles, authentication agents, tokens and reports. The company’s small user population and small number of administrators does not require a security domain hierarchy, as there is no need to limit administrative scope.

The company also decided to use the default system policies (password, lockout, token, offline authentication, and emergency authentication). All users have the same usage requirements, so it was not necessary to maintain more than one of each type of security policy.

Four administrators perform all the Authentication Manager administrative chores. Two are assigned the Super Admin role.

The following table lists the Authentication Manager data affected by the migration, the impact upon the data and any tasks that the administrator needs to perform as a result of migration.

Data	Impact/Task
Realm	The version 6.1 realm becomes a version 7.1 realm with one top-level security domain.
Administrators	Realm Administrators become Super Admins.

Data	Impact/Task
Sites	The deployment has no version 6.1 sites
Groups	Groups from the version 6.1 realm are migrated to groups in the version 7.1 realm.
Agents	During migration of the primary, agents authenticate to the replica exclusively. After migration, agents that authenticate to the primary receive the server list, which contains only the primary. After receiving the server lists, agents authenticate to the primary only, until the replica is migrated and brought online, at which time the server list is updated (to include the replica) and sent again to the agent.
Tokens	Tokens are migrated to the top-level security domain.
Users	Users are all migrated to the top-level security domain, and user data resides in the internal database).
Administrative Roles	Group administration privileges are not migrated. In version 7.1, administrators are scoped to security domains, not to groups.
RADIUS	The scenario has no RADIUS server.

Benefits of Migration

Secure Web-Based Administration

The addition of the browser-based interface enables administration through supported browsers, allowing administrators to deal with authentication issues off-site and in off-hours, with no need to install any remote administration client software.

Self-Service Features

To lighten the administrative workload, B & B Boxing uses RSA Credential Manager (a component of Authentication Manager) to allow users to troubleshoot problems with their assigned tokens. The following self-service features are available:

- Change token PINs.
- Create new token PINs.
- Get an emergency access code.
- Test tokens.

The migration from RSA Deployment Manager 1.2 to RSA Credential Manager requires all users to provide answers to security questions, as their previous answers are not migrated.

Scenario 2: Mid-Sized Business, Single Site, Multiple LDAP Synchronization Jobs

Middlewizr Media Corporation (2,500 Employees)

Middlewizr Media Corporation is a publicly traded, medium-sized company with 2,500 employees in one location. Because the company is publicly traded, it must meet all Sarbanes-Oxley requirements and maintain detailed records of all business and network transactions.

Middlewizr Media Corporation maintains a Linux-based network with Windows-based client PCs and laptops. They employ an IT staff of 28, including eight system administrators who oversee general administrative tasks, and 20 lower-level administrators who operate the Help Desk. All employee data is maintained in a Sun ONE Directory Server. Employees have local and remote access to the network.

Business Needs

Middlewizr Media Corporation has the following business needs:

Secure remote access. Enable secure remote, wireless, and dial-in access to e-mail, applications, and confidential proprietary files, intellectual property, and research materials for management, researchers, and certain other employees.

Secure access from inside the corporate firewall. Enable secure on-site access to sensitive confidential proprietary files, intellectual property, and research materials for management, developers, and certain other employees.

More efficient administration of user data. Prior to migration, available LDAP data was referenced in the Authentication Manager database. After migration the data is always directly accessible from the linked LDAP directory and up to date.

How Migration Affects the Existing Deployment

Physical Deployment

The network includes a Linux Network Information Service (NIS) server inside the corporate firewall, which contains a variety of file and print servers, and a client database.

In the DMZ, the network includes a VPN server, a proxy server, a web server, a PAM-protected server, TACACS+ protected servers, an OWA front end, a wireless router connected to a RADIUS server, and a VPN server. The VPN is certified by RSA SecurID and includes a built-in version 5 custom agent. Users directly connected to the internal network use RSA SecurID for Windows local authentication client. RSA SecurID authentication is required for all network access inside the corporate firewall, and for remote access through the VPN and RADIUS.

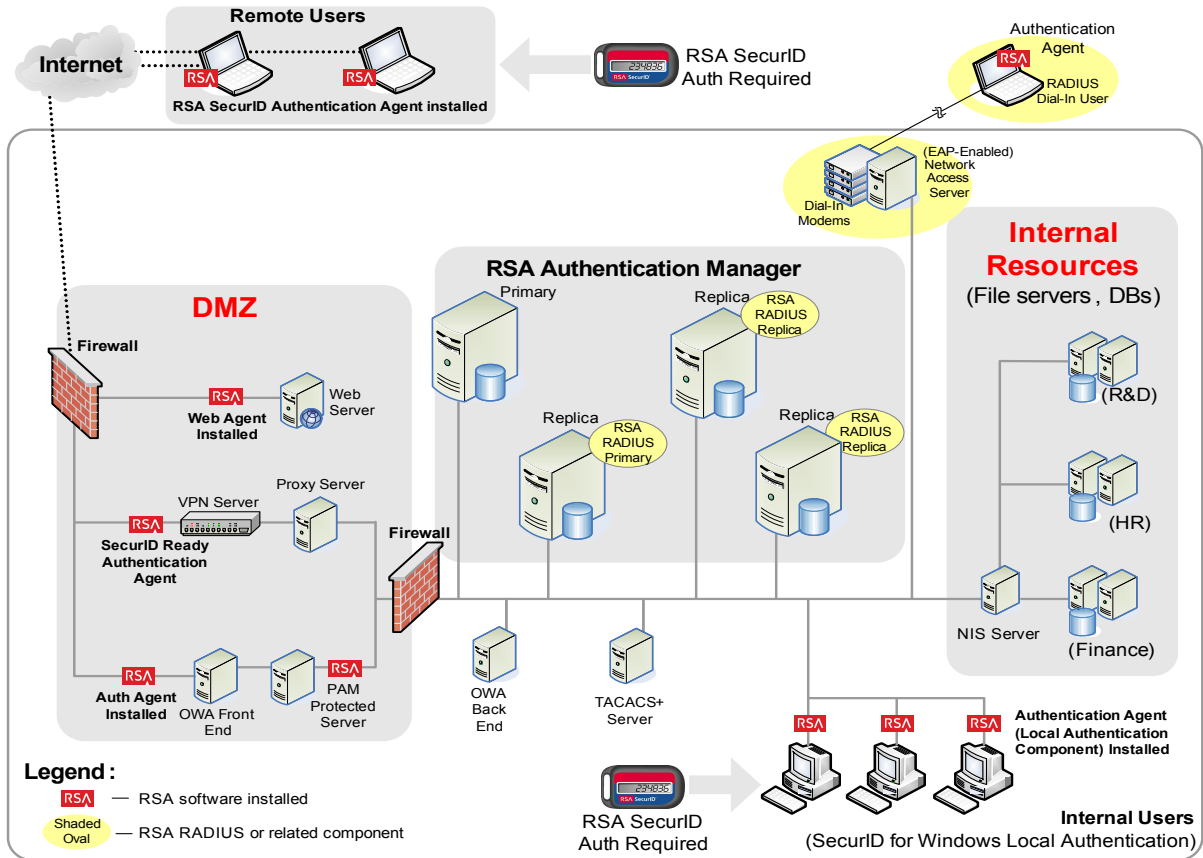
Middlewizr Media Corporation has an Enterprise Server license. Prior to migration, there is one Authentication Manager Primary Server and three Replica Servers (for authentication load and failover). After migration to version 7.1, there is one three-node primary instance, and one three-node replica instance. The company has a Sun ONE Directory Server deployed, and uses an upgraded Sun Java System Directory Server as the authoritative identity source.

The following tables lists the hardware affected by the Authentication Manager migration, the impact upon the hardware, and any tasks that the administrator needs to perform as a result of migration.

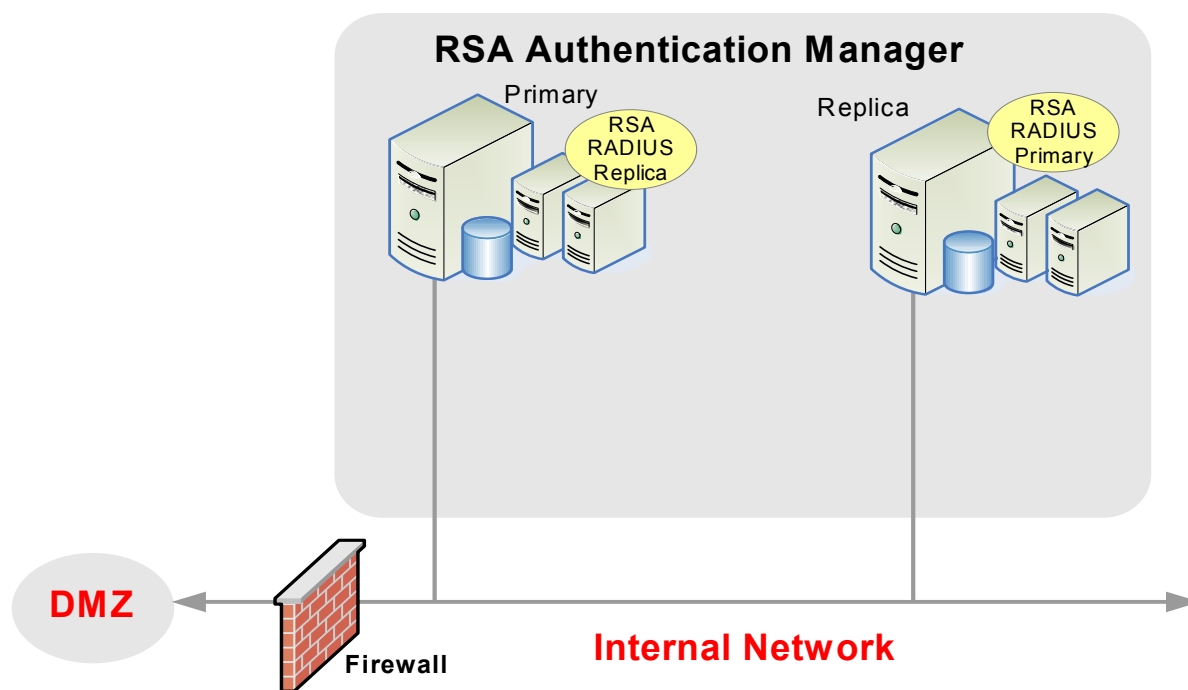
Hardware	Affected Item/Task
Server	The administrator installs version 7.1 on new hardware (with a new hostname and IP address). The administrator must perform a dump of the version 6.1 database and license files, and copy them to a location accessible from the new hardware prior to the installation of version 7.1.
Agent	The administrator must update the sdconf.rec files on each Agent Host to point to the new hardware, and verify that third-party agents and other RSA Secured products are supported.
Replicas	In the migrated environment, the number of replicas has been reduced, but server nodes are added to enhance performance. Replicas ensure the ability to recover data and administration capabilities in the event of an emergency. For business continuity, in each geographic site, the primary and replica are housed in separate locations.
Server nodes	In the migrated version 7.1 realm, multiple server nodes enhance performance.
Custom administration and agent applications	Custom administration applications built using the version 6.1 administration API are no longer supported. The administrator must verify that any custom authentication applications were built with a supported version of the authentication APIs. For more information, see “Customized Agents Created Using the Authentication API” on page 60.

System Diagram Before Migration:


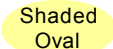
Middlewiz Media Corporation



System Diagram After Migration (Showing changes only):



Legend:

-  — RSA software installed
-  — RSA RADIUS or related component

Logical Deployment

Middlewiz Media Corporation uses a single realm with an Enterprise Server license. Prior to migration, there were separate Authentication Manager sites for Finance, HR, and R&D. During the migration process, lower-level security domains were automatically created for these sites. Users who are members of these departments are contained in the lower-level security domains. Multiple security domains allow administrators' scope to be limited by, in this case, department.

Sun ONE Directory Server is currently deployed with ten synchronization jobs in the version 6.1 database. In the migrated environment, these ten synchronization jobs become three identity sources. Although it is not required to support version 7.1, the company is upgrading to Sun Java System Directory Server after migration.

The Finance department uses a combination of default and custom security policies. Because of the sensitive nature of the department's work, the password policies are stricter and require more frequent password changes. The lockout and token policies are also more strict than the default policy used by other departments. Likewise, the company uses a custom restricted access time policy that limits when users can access the network. Default policies (password, lockout, token, offline authentication, and emergency authentication) are used in the top-level, HR and R&D security domains.

The following table lists the Authentication Manager data affected by the migration, the impact upon the data, and any tasks that the administrator needs to perform as a result of migration.

Data	Affected Item/Task
Realm	The version 6.1 realm becomes a version 7.1 realm with one top-level security domain, and three lower-level security domains (Finance, HR and R&D).
Administrators	Eight Realm Administrators become two Super Admins and six administrators scoped to one of the three security domains (2 in each). 20 Help Desk Administrators remain 20 Help Desk Administrators able to perform common tasks on all users.
Sites	The three sites (Finance, HR and R&D) in the version 6.1 realm become lower-level security domains in the migrated environment.
Groups	Groups from the version 6.1 realm are migrated to groups in the version 7.1 realm. However, administrative scoping is not migrated. A single group is migrated as multiple groups when the original group contains users from multiple identity sources (for example, a group containing non-LDAP users and LDAP users, or a group containing LDAP users created from different LDAP synchronization jobs).
Agents	In the migrated environment, administrators must update existing agents with new sdconf.rec files. Any agent that has a group association becomes a restricted agent, regardless of its state prior to migration, and is migrated to the same security domain as the group. User activations on an agent are migrated only when the agent is a restricted agent. For more information, see “Users” in this table.
Tokens	Tokens can be migrated to a domain specified by the migrating administrator (if he or she has privileges that allow access to that security domain), or to the security domain of the administrator.

Data	Affected Item/Task
Users	<p>Any users specified in an LDAP synchronization job are mapped to the appropriate LDAP identity source. The administrator may need to manually map each job to an identity source. Any users not specified in an LDAP synchronization job are migrated to the internal database.</p> <p>The user's group association changes when the original version 6.1 group membership includes both LDAP and non-LDAP users, or LDAP users from multiple LDAP directories. Group membership data defined for the user is also migrated. For more information, see "Groups" in this table.</p> <p>User activations on a restricted agent are migrated to a group activation on the same agent. The group is created during migration, and any users activated on the agent are added to the group. Any activation data (such as an alternative user logon or shell) is migrated.</p>
Administrative roles	<p>Administrative roles are managed in the top-level security domain. Site administrators retain privileges in the migrated lower-level security domain. Their privileges are restricted to that security domain only.</p> <p>Group administration privileges are not migrated. In version 7.1, administrators are scoped to security domains, not to groups.</p>
RADIUS	<p>RADIUS data and configuration files must be manually exported from the existing RSA RADIUS server and imported during installation of the updated RSA RADIUS 7.1 server, just like the Authentication Manager database and license files. The migration upgrades the RSA RADIUS server from SBR v5 to SBR v6.</p>
Reports	<p>Custom 4GL reports created in version 6.1 are not migrated to the new version 7.1 environment. Migrating users may use the canned reports provided with version 7.1. Reports specific to a department are contained in the lower-level security domains. Reports of a more general nature are contained in the top-level security domain.</p>

Benefits of Migration

More Administrative Control

In the migrated environment, administrative control is enhanced by the ability to restrict administrative responsibilities. Prior to migration, three version 6.1 sites are defined in the database for Finance, HR, and R&D. After migration to version 7.1, three lower-level security domains exist for these departments. Users who are members of these departments are contained in the lower-level security domains. Multiple security domains allow administrators' scope to be limited by, in this case, department.

Secure Web-Based Administration

The addition of the browser-based interface enables administration through supported browsers, allowing administrators to deal with authentication issues off-site and in off-hours, with no need to install any remote administration client software.

More Flexible Policies

Because of the sensitive nature of the Finance department's work, the company wants the department's password policies to be stricter, and require more frequent password changes. In the migrated environment, the administrators can assign custom password, lockout, and token policies to the department. The lockout and token policies can be more restrictive than the default policy used by other departments. Default policies (password, lockout, token, offline authentication, and emergency authentication) are used in the top-level, HR, and R&D security domains.

Better Utilization of External Authoritative Identity Sources

After migration, all user and group data in the identity source is accessible in real-time. In this deployment, the LDAP directories are configured to be read/write. Therefore, the Authentication Manager can update user or group data in the LDAP directories.

Improved Performance and Scalability Through the Implementation of Nodes

Multiple server nodes per instance of Authentication Manager improve authentication performance to enable multiple authenticating machines to function as a single Authentication Manager.

Self-Service and Provisioning Features

To lighten the administrative workload, Middlewurz Media Corporation uses RSA Credential Manager (a component of Authentication Manager) to allow users to troubleshoot problems with their assigned tokens and to request new tokens. All self-service and provisioning features are available because the company has granted Authentication Manager read/write access to the Active Directory identity source.

Scenario 3: Large Enterprise, Multiple Geographic Sites, Multiple Realms

Meyecom Inc. (25,000 Employees)

Meyecom Inc. is a publicly traded, large-sized company with 25,000 employees in three locations. Because the company is publicly traded, it must meet all Sarbanes-Oxley requirements and maintain detailed records of all business and network transactions.

Meyecom Inc. is a multi-platform shop, maintaining a Linux-based environment in Tokyo, and two Windows-based environments (Boston and London). The company uses Sun Java System Directory Servers and Active Directory as identity sources, and has enabled read only access to them. The Authentication Manager administrators assigned and distributed RSA SecurID tokens to 15,000 employees.

The company employs an IT staff of over 90, including sixteen system administrators, who oversee general administrative tasks, and 75 other administrators who operate the Help Desk. Employee data is maintained in Sun ONE Directory Server (pre-migration) and multiple Active Directory Servers. As Meyecom Inc. is often a government contractor, they have extremely strong security requirements and have configured their LDAP directories for read-only access. Employees have local and remote access to the network.

Business Needs

Meyecom Inc. has the following business needs:

Secure remote access. Enable secure remote, wireless, and dial-in access to e-mail, applications, and confidential proprietary files, intellectual property, and research materials for management, researchers, and certain other employees.

Secure access from inside the corporate firewall. Enable secure on-site access to sensitive confidential proprietary files, intellectual property, and research materials for management, developers, and certain other employees.

More efficient administration of user data. Prior to migration, available LDAP data was referenced in the Authentication Manager database. After migration the data is always directly accessible from the linked LDAP directory and up to date.

Secure access across geographic sites. In the migrated environment, users traveling to the different geographic sites will need to authenticate securely.

How Migration Affects the Existing Deployment

Physical Deployment

Meyecom Inc. has an Enterprise Server license. Prior to migration, there are three Authentication Manager Primary Servers and three Replica Servers, one in each of the geographic locations, for a total of three realms. The Replicas provide failover administration and additional authentication performance in the pre-migrated environments. In the migrated environment, the Windows-based realms are merged into one realm, and the Solaris realm continues running version 6.1. This realm is upgraded at a later date.

The Boston and London sites have multiple domain controllers inside the corporate firewall, which contains a variety of file and print servers. They use Active Directory servers.

The Tokyo site includes a Network Information Service (NIS) server inside the corporate firewall, which contains a variety of file and print servers. The site has a Sun ONE Directory Server deployed, and will use an upgraded Sun Java System Directory Server after migration as the authoritative identity source.

In the DMZ, the network includes a VPN server and a proxy server. The VPN is certified by RSA SecurID and includes a built-in version 5 custom agent. Users directly connected to the internal network use RSA SecurID for Windows local authentication client. RSA SecurID authentication is required for all network access inside the corporate firewall and for remote access through the VPN and RADIUS.

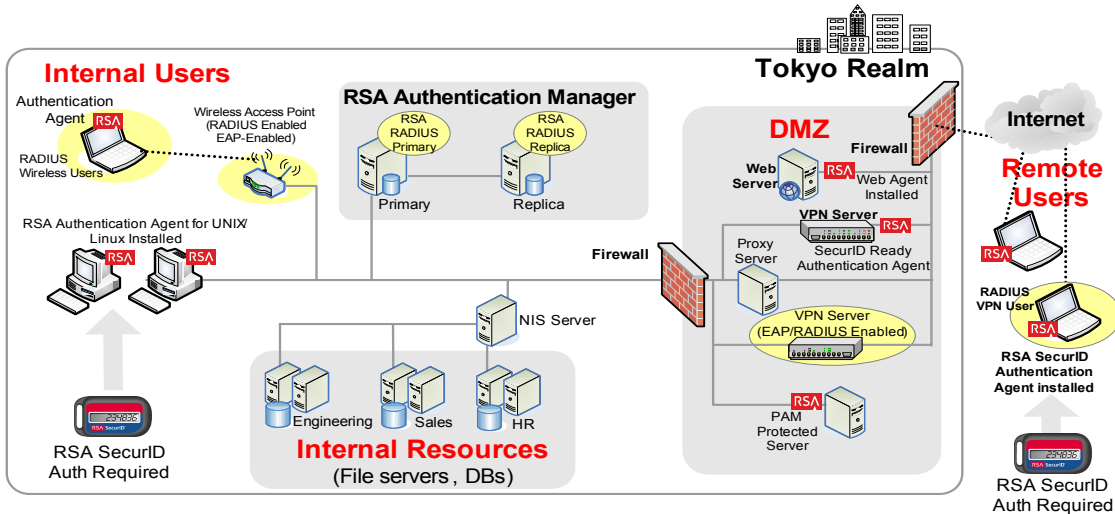
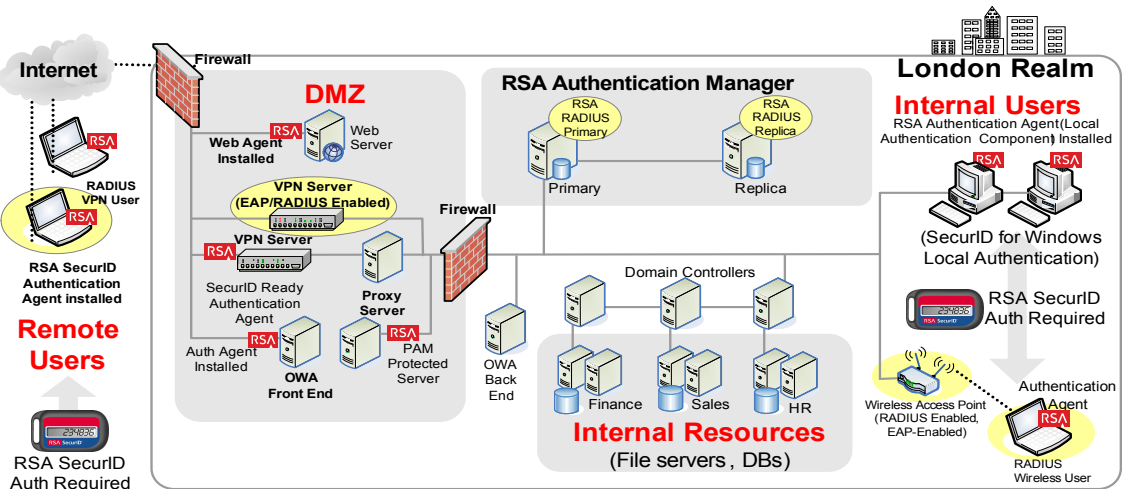
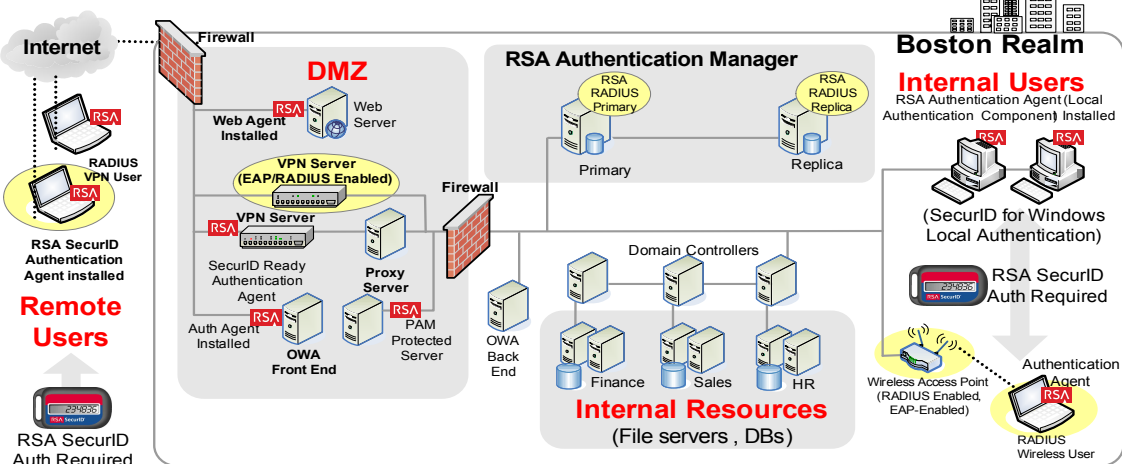
Additionally, there is a RADIUS and EAP-enabled VPN server that can handle other authentication methods that adhere to the EAP standard. Users directly connected to the internal network use RSA SecurID for Windows local authentication client. Some protected resources (web server, PAM-protected servers, TACACS+ servers) are deployed in the DMZ.

The deployment includes a Network Management System to take advantage of SNMP trapping tools in Authentication Manager.

The following table lists the hardware affected by the Authentication Manager migration, the impact upon the hardware, and any tasks that the administrator needs to perform as a result of migration.

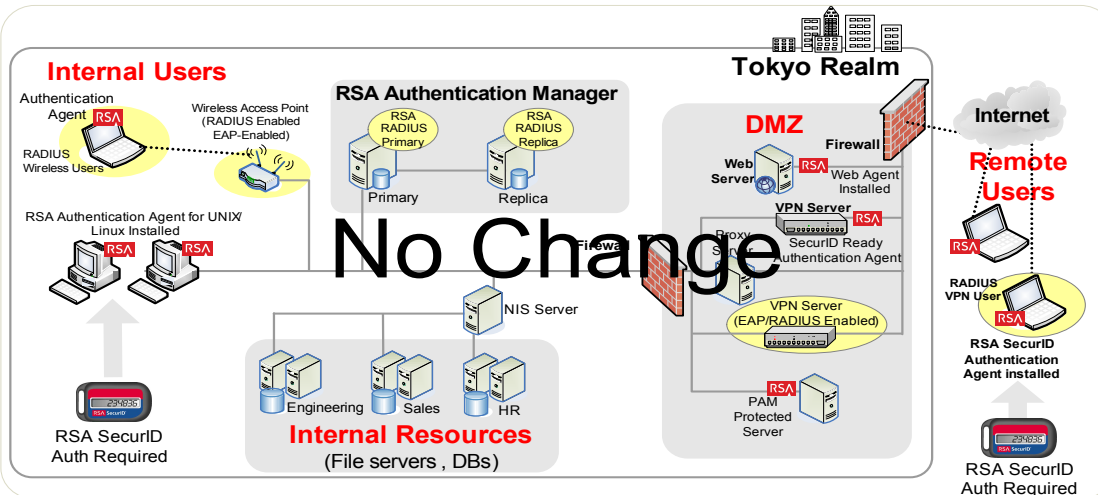
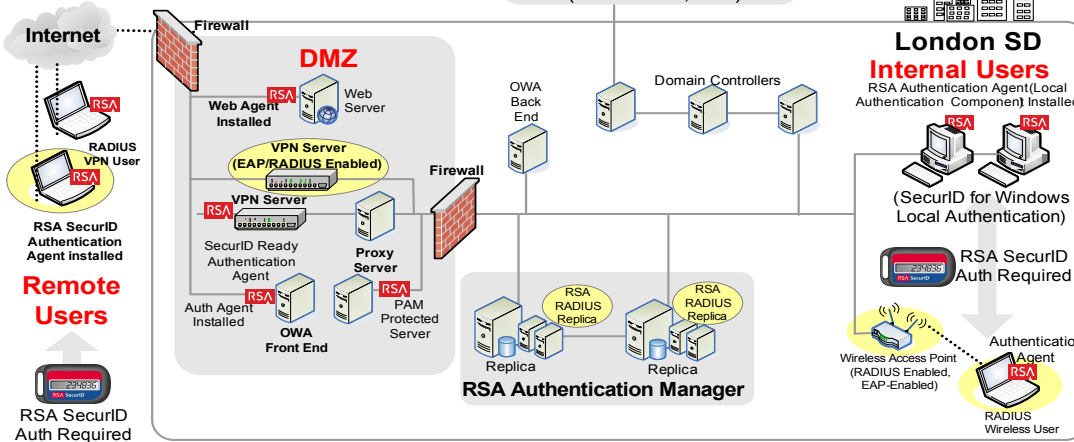
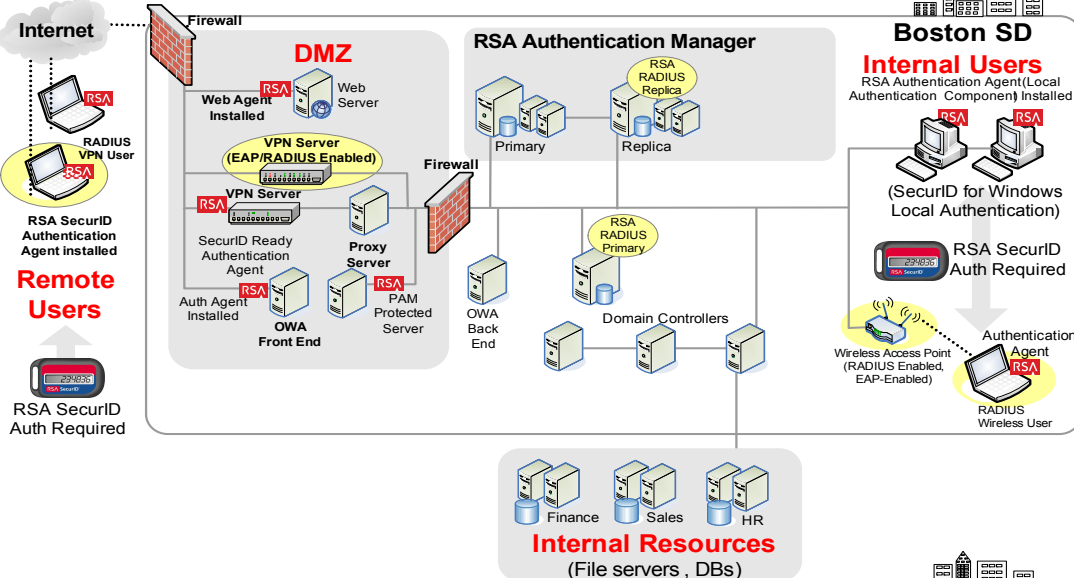
Hardware	Impact/Task
Server	The administrator installs version 7.1 on new hardware (using the same hostname and IP address as the existing version 6.1 hardware). The administrator must perform a dump of the version 6.1 database and license files, and make them available to the new hardware prior to the installation of version 7.1.
Agent	The administrator must verify that third-party agents and RSA Secured products are supported.
Replicas	In the migrated version 7.1 realm, the number of replica instances is reduced to three (one in Boston, two in London). Both the primary instance and the replica instances use three server nodes to enhance performance. Replica instances ensure the ability to recover data and administration capabilities in the event of an emergency. For business continuity, in each geographic site, the primary and replica instances are housed in separate locations.
Server nodes	In the migrated version 7.1 realm, each instance (the primary and the three replicas) uses a cluster with three server nodes to enhance performance.
Custom administration and agent applications	Custom administration applications built using the version 6.1 administration API are no longer supported. The administrator must verify that any custom authentication applications were built with a supported version of the authentication APIs. For more information, see “Customized Agents Created Using the Authentication API” on page 60.

Meyecom Inc. (Before Migration)



Legend:
 — RSA software installed
 — RSA RADIUS or related component

Meyecom Inc. (After Migration)



No Change

- Legend:**
- RSA software installed
 - RSA RADIUS or related component

Logical Deployment

Prior to migration, the company has three realms (Boston and London on Windows and Tokyo on Solaris) with multiple Enterprise Server licenses. The use of multiple realms by the company is a result of corporate mergers. In the migrated environment, two of the realms (Windows platform) are merged into a single migrated realm, while the third realm (Solaris platform) is not migrated and remains a version 6.1 realm.

An Active Directory forest is already deployed with a domain for the Boston and London sites. In the migrated environment, the Active Directory forest (through an Active Directory Global Catalog) is just one of the identity sources for Authentication Manager user and user group data. Sun Java System Directory Server is deployed as the identity source for the Tokyo site, which is a recently acquired company. The Sun Java System Directory Server was already deployed and was quickly integrated with Authentication Manager.

Sixteen administrators are available to perform Authentication Manager administrative chores. Four are Super Admins. Twelve are assigned the System Administrator role and have all administrative permissions, except those for Super Admins only.

An additional IT staff of 75 spend 10% of their time on general administrative tasks and staff a 9 a.m. to 8 p.m. Help Desk. There are 35 Privileged Help Desk administrators at the Boston site, 20 at London site, and 20 at the Tokyo site. Multiple security domains allow the scope of the Privileged Help Desk administrators to be limited by, in this case, location. Users are managed in the security domains associated with those sites. Administrative roles are managed in the top-level security domain.

After migration, default policies (password, lockout, token, offline authentication, and emergency authentication) are used for the top-level security domain, and the Boston and London security domains. The Tokyo security domain uses custom password, lockout, and token policies. The administrators of the Tokyo location use stricter password policies that require more frequent password changes, as well as lockout and token policies that are stricter than the default policy used by other locations.

The following table lists the Authentication Manager data affected by the migration, the impact upon the data, and any tasks that the administrator needs to perform as a result of migration.

Data	Impact/Task
Realm	The company has decided to merge two of the version 6.1 realms into one version 7.1 realm with one top-level security domain and two lower-level security domains (London and Boston). One realm (Tokyo) remains a version 6.1 realm, requiring the administrator of the version 6.1 realm to establish a trusted relationship with the new version 7.1 realm.

Data	Impact/Task
Administrators	<p>16 Realm Administrators become 2 Super Admins and 10 administrators scoped between the two security domains. 4 Realm Administrators remain in the Tokyo realm.</p> <p>75 Help Desk Administrators remain as 75 Help Desk Administrators able to perform common tasks on all users in their realms. They are divided between the new merged realm and the remaining version 6.1 realm.</p>
Sites	<p>Any sites in the Boston and London version 6.1 realms become lower-level security domains within the security domains of Boston or London.</p> <p>The three sites (Finance, Sales and HR) in the version 6.1 realm become lower-level security domains in the migrated environment.</p>
Groups	<p>Groups from the version 6.1 realm are migrated to groups in the version 7.1 realm. However, administrative scoping is not migrated.</p> <p>A single group is migrated as multiple groups when the original group contains users from multiple identity sources (for example, a group containing non-LDAP users and LDAP users, or a group containing LDAP users created from different LDAP synchronization jobs).</p>
Agents	<p>In the migrated environment, administrators must update existing agents with new sdconf.rec files.</p> <p>Any agent that has a group association becomes a restricted agent, regardless of its state prior to migration, and is migrated to the same security domain as the group.</p> <p>User activations on an agent are migrated only when the agent is a restricted agent. For more information, see “Users” in this table.</p>
Tokens	<p>Tokens can be migrated to a domain specified by the migrating administrator (if he or she has privileges that allow access to that security domain), or to the security domain of the administrator.</p>

Data	Impact/Task
Users	<p>Any users specified in an LDAP synchronization job are mapped to the appropriate LDAP identity source. The administrator may need to manually map each job to an identity source. Any users not specified in an LDAP synchronization job are migrated to the internal database.</p> <p>The user's group association changes when the original version 6.1 group membership includes both LDAP and non-LDAP users, or LDAP users from multiple LDAP directories. Group membership data defined for the user is also migrated. For more information, see "Groups" in this table.</p> <p>User activations on a restricted agent are migrated to a group activation on the same agent. The group is created during migration, and any users activated on the agent are added to the group. Any activation data (such as an alternative user login or shell) is migrated.</p>
Administrative roles	<p>Administrative roles are managed in the top-level security domain. Site administrators retain privileges in the migrated lower-level security domain. Their privileges are restricted to that security domain only.</p> <p>Group administration privileges are not migrated. In version 7.1, administrators are scoped to security domains, not to groups.</p>
RADIUS	<p>RADIUS data and configuration files must be manually exported from the existing RSA RADIUS server and imported during installation of the updated RSA RADIUS 7.1 server, just like the Authentication Manager database and license files. The migration upgrades the RSA RADIUS server from SBR v5 to SBR v6.</p>
Reports	<p>Custom 4GL reports created in version 6.1 are not migrated to the new version 7.1 environment. Migrating users may use the canned reports provided with version 7.1. Reports specific to a department are contained in the lower-level security domains. Reports of a more general nature are contained in the top-level security domain.</p>

Benefits of Migration

More Administrative Control

In the migrated environment, administrative control is enhanced by the ability to restrict administrative responsibilities. Prior to migration, three version 6.1 sites are defined in the database for Finance, Sales and HR. After migration to version 7.1, three lower-level security domains exist for these departments. Users who are members of these departments are contained in the lower-level security domains. Multiple security domains allow administrators' scope to be limited by, in this case, department.

Secure Web-Based Administration

The addition of the browser-based interface enables administration through supported browsers, allowing administrators to deal with authentication issues off-site and in off-hours, with no need to install any remote administration client software.

More Flexible Policies

Because of the sensitive nature of the Finance department's work, the company wants the department's password policies to be stricter, and require more frequent password changes. In the migrated environment, the administrators can assign custom password, lockout, and token policies to the department. The lockout and token policies can be more restrictive than the default policy used by other departments. Default policies (password, lockout, token, offline authentication, and emergency authentication) are used in the top-level, HR and R&D security domains.

Better Utilization of External Authoritative Identity Sources

After migration, all user and group data in the identity source is accessible in real-time. In this deployment, the LDAP directories are configured to be read-only. Therefore, the Authentication Manager cannot update user or group data in the LDAP directories.

Improved Performance and Scalability Through The Implementation Of Nodes.

Multiple server nodes per instance of Authentication Manager improve authentication performance to enable multiple authenticating machines to function as a single Authentication Manager.

Self-Service and Provisioning Features

To lighten the administrative workload, Meyecom Inc. uses RSA Credential Manager (a component of Authentication Manager) to allow users to troubleshoot problems with their assigned tokens and to request new tokens. A limited set of self-service features is available because the company has granted Authentication Manager read-only access to the LDAP identity sources.

C

Integrating an LDAP Directory

- [Overview of LDAP Directory Integration](#)
- [Preparing for LDAP Integration](#)
- [Adding an Identity Source](#)
- [Linking an Identity Source to a Realm](#)
- [Verifying the LDAP Identity Source](#)

Overview of LDAP Directory Integration

You can integrate LDAP directories with RSA Authentication Manager 7.1 to access user and group data without modifying the LDAP schema. Depending on your needs, you can configure Authentication Manager to only read data from the LDAP directory, or to perform both read and write operations.

To integrate an LDAP directory, you perform certain tasks using the RSA Operations Console and other tasks using the RSA Security Console.

Microsoft Active Directory single forest environments require additional configuration steps, as described in [“Integrating Active Directory Forest Identity Sources”](#) on page 185.

Important: Many of the tasks in the following sections require detailed knowledge of LDAP and your directory server deployment. RSA recommends that these tasks be performed by someone with LDAP experience and familiarity with the directory servers to be integrated.

Important: RSA recommends that you configure all identity sources as read-only.

Integrating an LDAP Identity Source

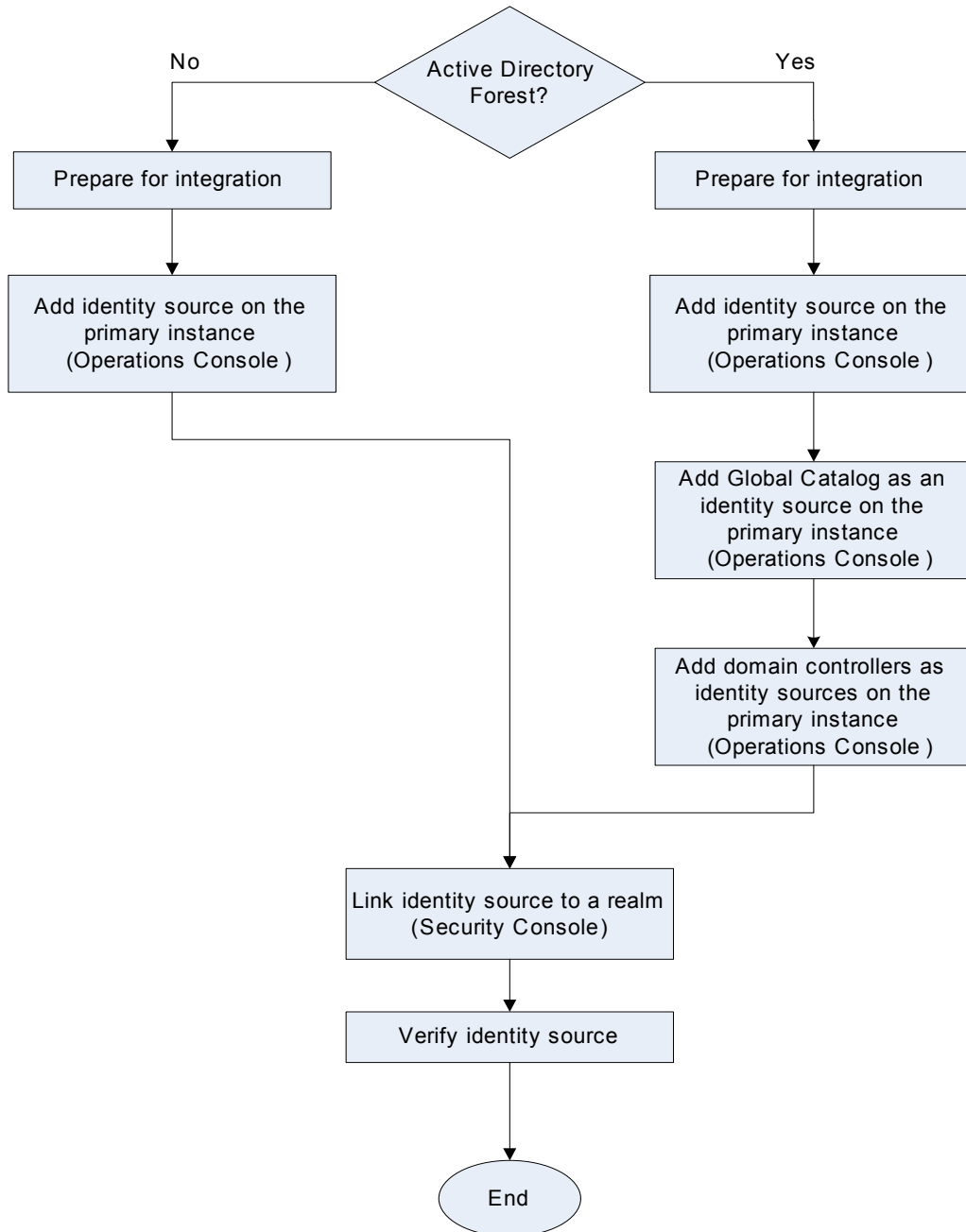
Task	See
1. Prepare your directory for integration:	
Set up SSL connections between your LDAP directory server and Authentication Manager.	“Setting Up SSL for LDAP” on page 186.
Consider the password policy (Active Directory only).	“Password Policy Considerations” on page 187.
Verify your domain functional level (Active Directory only).	“Supporting Groups” on page 187.



Task	See
Verify that the Active Directory server name is a valid DNS name (Active Directory Forest only).	“Active Directory Forest Considerations” on page 188.
2. Add the identity source.	“Adding an Identity Source” on page 188.
3. Link the identity source to a realm.	“Linking an Identity Source to a Realm” on page 192.
4. Verify the LDAP integration.	“Verifying the LDAP Identity Source” on page 193.

The following figure shows the process flow for integrating an LDAP directory as an identity source.

LDAP Integration Tasks



Failover Directory Servers

If you have failover directory servers, you can specify them when adding an identity source. Provide the failover URL in the **LDAP Failover URL** field as described in [“Adding an Identity Source”](#) on page 188. If you have a failure in your primary directory server, the system automatically connects to the failover server you specified.

Important: The directory server for failover must be a replica, or mirror image, of the primary directory server.

Mapping Identity Attributes for Active Directory

You must follow specific guidelines when you use the Security Console to map identity attributes to physical attribute names in an Active Directory identity source schema. You use the Add Identity Source page to map attributes.

If your Active Directory identity source is read-only (default), make sure that all user fields map to non-null fields. The User ID is mapped to the 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 you need when you add the identity source. If you do not map a field, the field will remain blank when you add users. Active Directory does not provide any values for user’s records for unmapped fields, except in one case: when you create a user without supplying the saMAccountName. In this case, Active Directory generates a random string for the saMAccountName value. You can handle this issue using identity attribute definitions.

If your environment requires specific attributes, you must explicitly map the identity source to those attributes using the Identity Source Mapping page in the Security Console. By default, when you add a new user, the user is mapped to the fields that are configured for the identity source. For example, the User ID is mapped to the saMAccountName by default, but the **User Principal Name (UPN)** field is left blank. Use the Security Console to create an identity attribute definition that you can map to the UPN field in your Active Directory. Then, use the Security Console to map the new attribute.

If you map the User ID to an attribute other than saMAccountName, for example to UPN, Active Directory generates a random value for saMAccountName. To avoid this scenario, follow the instructions described previously and define an identity attribute definition for saMAccountName. Make sure that you provide a proper value for this attribute every time you add a new user to Active Directory using the Security Console.

Integrating Active Directory Forest Identity Sources

Configuring Authentication Manager to access user and group data from an Active Directory forest entails some additional considerations and procedures.

Runtime and Administrative Identity Sources

To account for the architecture of an Active Directory forest, this section refers to 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. This identity source maps to your Active Directory Global Catalog.

Administrative identity source. An identity source used for administrative operations such as adding users and groups. This identity source maps to a domain controller.

In a multidomain Active Directory forest setup, the Global Catalog is added as an identity source and the domain controller servers are added as administrative identity sources. The Global Catalog is used at runtime as another directory to find and authenticate users, and to resolve group membership within the forest.

The Global Catalog is used only for runtime operations, such as authentication. Authentication Manager does not use the Global Catalog for administrative operations. Administrative actions (for example, adding users) are performed against the administrative identity sources (domain) only. Changes to the domain are replicated by Active Directory to the Global Catalog.

Note: Active Directory supports multiple types of groups, such as Universal, Domain Local, and Global. The default is Universal groups. When you view the Active Directory groups from the Security Console, the Security Console displays all groups, regardless of type.

Integration Process for Active Directory Forests

The extent of the integration process depends on the scale of your Active Directory forest. Each Global Catalog must be added as a separate runtime identity source.

Note: If a forest has more than one Global Catalog, you can use one for failover. In this case, you do not need to deploy the Global Catalog, but you must specify it as a failover URL when you deploy the first Global Catalog.

Likewise, each additional domain controller must be added as an administrative identity source.

Using an Active Directory Global Catalog as an Identity Source

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

- The Global Catalog
- All Active Directories that replicate data to the Global Catalog

For instructions, see [“Adding an Identity Source”](#) on page 188.

For example, suppose GC1 is the Global Catalog that you want to use as your identity source, and AD1, AD2, and AD3 replicate a subset of their data to GC1. You must perform the procedure on each of the identity sources.

After you perform the integration, Authentication Manager accesses GC1 for authentication requests only. Authentication Manager accesses AD1, AD2, and AD3 for all other administrative operations. If you grant Authentication Manager read/write access to your identity sources, Authentication Manager makes all administrative changes in AD1, AD2, and AD3, which replicate the changes to GC1.

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

Preparing for LDAP Integration

Perform these tasks prior to adding an identity source. SSL setup is required for an Active Directory read/write connection and optional for Sun Java System Directory Server. For Active Directory, there are additional important considerations for password policies and group membership support.

Setting Up SSL for LDAP

To set up SSL connections between your LDAP directory server and Authentication Manager, perform the following tasks. In addition to importing a certificate, you must specify an LDAP URL when adding an identity source.

Note: A read-only connection to Active Directory does not require SSL. By default, all identity sources are read-only, but you can configure them to read/write.

Importing the SSL Certificate

To establish a secure connection between your deployment and your identity sources, you must add an SSL (ca root) certificate on all server nodes in the primary and replica instances, including the database servers and attached server node machines.

Note: Your directory server must already be configured for SSL connections and you need ready access to the directory server’s certificate. If your system does not meet these requirements, see your directory server documentation for instructions on setting up SSL.

To add a new SSL certificate:

1. On the RSA Operations Console, click **Deployment Configuration > Certificates > Identity Source Certificates > Add New**.
2. Enter a name for the new SSL certificate.
3. Navigate to the directory where the SSL certificate is located.
4. Click **Save**.

Specifying SSL-LDAP for Your Identity Source

When you perform the steps described in “[Adding an Identity Source](#)” on page 188, make sure that you specify a secure URL in the **LDAP URL** field. If you are using the standard SSL-LDAP port 636, specify the value as “ldaps://hostname?”. For any other port, you must also specify the port number, for example “ldaps://hostname:port?”.

Password Policy Considerations

If your Active Directory identity source is read/write, you must consider the following.

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.

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

- Make your Authentication Manager password policy password requirements more strict. See the chapter “Preparing RSA Authentication Manager for Administration” in the *Administrator’s Guide*.
- Relax the complexity requirements in the Windows 2003 Group Policy Editor. See your Windows documentation.

Supporting Groups**Setting the Domain Level for Group-to-Group Membership**

To support group-to-group membership in Active Directory, you must set the domain functional level to Windows 2003. For more information about how to raise the domain functional level, go to

<http://technet2.microsoft.com/windowsserver/en/library/5084a49d-20bd-43f0-815d-88052c9e2d461033.mspx?mfr=true>.

Specifying a Group Container in the RSA Security Console

The default organizational unit “Groups” does not exist in the default Active Directory installation. Make sure that a valid container is specified for the Group Base DN when adding the identity source.

Active Directory Forest Considerations

The Active Directory server name must be a valid DNS name. Make sure that the name is resolvable for both forward and reverse lookups, and that the Active Directory server can be reached from the Authentication Manager server.

Adding an Identity Source

For this part of the LDAP integration process, you use the Operations Console to provide information about your LDAP directory in order to map Authentication Manager operations to the actual named location of user and group data in your schema. Authentication Manager reads and writes data to and from these locations if you have configured the system for read/write operations. However, Authentication Manager never modifies the schema or adds to it in any way.

Important: You may be prompted to enter your Security Console User ID and password. You must be a Super Admin to perform this task.

This process requires you to enter values in fields on the Operations Console. Each completed value saves integration information to Authentication Manager.

In particular, note these important parameters:

Identity Source Name. Defines the name for the identity source that is displayed to the administrator in the Security Console. Once an identity source is added to the system, you cannot change the name of the identity source.

Type. Defines the type of identity source that you are adding. For example, Microsoft Active Directory or Sun Java System Directory Server. Once an identity source is added to the system, you cannot change the identity source type.

Read-Only. Determines whether Authentication Manager is permitted to write to the LDAP directory. Select this checkbox for read-only operations, or clear it for read/write operations.

To add an identity source in the Operations Console:

1. Click **Deployment Configuration > Identity Sources > Add New**.
2. In the Identity Source Basics section, do the following:
 - a. In the **Identity Source Name** field, enter the name of the identity source.
 - b. In the **Type** field, select the type of identity source that you want to add.
 - c. In the **Notes** field, enter any important information about the identity source.
3. In the Directory Connection section, do the following:
 - a. In the **Directory URL** field, enter the URL of the new identity source.

Note: If you are using the standard SSL-LDAP port 636, specify the value as “ldaps://hostname”. For any other port, you must also specify the port number, for example “ldaps://hostname:port”. If you are using a non-SSL connection, specify the value as “ldap://hostname:port”.

For Active Directory identity sources, RSA recommends that you use an SSL connection because it is required for password management.

- b. Optional. In the **Directory Failover URL** field, enter the URL of a failover identity source.
The system connects to the failover LDAP if the connection with the primary LDAP directory fails.
- c. In the **Directory User ID** field, enter the directory administrator user ID.
- d. In the **Directory Password** field, enter the directory administrator password.

Note: Do not let this password expire. If this password expires, the connection will fail.

- e. Click **Test Connection** to make sure that the system can successfully connect to the LDAP directory.
4. Repeat [step 3](#) for each replica instance in your deployment.

Note: You must configure a connection for the primary instance and each replica instance in your deployment.

5. Click **Next**.
6. In the Directory Settings section, do the following:
 - a. In the **User Base DN** field, enter the base DN for directory user definitions.
 - b. In the **User Group Base DN** field, enter the base DN for directory user group definitions.
 - c. Optional. Select **Read-only** to prevent administrators from using the Security Console to edit the users and groups in the identity source.
 - d. In the **Search Results Time-out** field, limit the amount of time a search is allowed to continue. If searches for users or groups are timing out on the directory server, either extend this time, or narrow individual search results. For example, instead of Last Name = *, try Last Name = G*.
 - e. Optional. In the **User Account Enabled State** drop-down menu, specify whether the system checks an external directory or the internal database to determine whether a user is enabled.
 - f. Optional. Select **Validate Map Against Schema** if you want the mapping of identity attribute definitions to the LDAP schema to be validated when identity attribute definitions are created or modified.
7. If the identity source is an Active Directory, in the Active Directory Options section, do one of the following:
 - If the identity source you are adding is a Global Catalog, select **Global Catalog**.
 - If the identity source is not a Global Catalog, select whether to authenticate users to this identity source, or select a Global Catalog to which you want users to authenticate.

- In the **Default Group Type**, select a default user group type for the identity source. All user groups created in the new Active Directory identity source are assigned the default user group type. You can edit the user group type if necessary.
8. If the identity source is an Active Directory Forest, specify a Global Catalog as the identity source for authentication for each administrative domain controller added. In the Active Directory Options section, do the following:
 - a. Select **Authenticate Users to a global catalog**.
 - b. From the drop-down list, select the appropriate Global Catalog for the domain controller.

Note: If your Active Directory identity source is read-only, you do not need any administrative domain controllers.

9. In the Directory Configuration - Users section, do the following:
 - a. Enter the directory attributes that you want to map to user attributes. For example, First Name might map to givenname, and Last Name might map to sn.
 - b. Select **Unique Identifier**. This field helps the Security Console find users whose DNs have changed. This checkbox is selected by default. The default unique identifier for Active Directory is ObjectGUID. For Sun Java Directory Server, it is nsUniqueI. You can edit these identifiers to point to other fields.

Important: RSA recommends that you select the **Unique Identifier** checkbox. You must select this checkbox before you move or rename LDAP users who are viewed or managed through the Security Console. Otherwise, the system creates a duplicate record for the users that you moved, and disassociates them from data the system has stored for them.

- c. In the **Search Filter** field, enter the filter that specifies how user entries are distinguished in your LDAP directory, such as a filter on the user object class. Any valid LDAP filter for user entries is allowed. For example, (objectclass=inetOrgPerson).
- d. From the **Search Scope** drop-down list, select the scope of user searches in the LDAP tree. By default, this is set to search all sub-levels in an LDAP tree. You can also search only a single level.
- e. In the **RDN Attribute** field, enter the user attribute used for the Relative Distinguished Name. For example, in Active Directory, cn, in Sun Java System Directory Server, uid.
- f. In the **Object Classes** field, enter the object class of users that are created or updated using the Security Console. For example, inetOrgPerson,organizationalPerson,person.

- g. For Active Directory only, use the **Required Attribute** fields if you want to populate two Active Directory user attributes with the value of a single RSA user identity attribute. For example, if you want to map the identity attribute User ID to the Active Directory attributes CN and samaccountname, map User ID to CN and then use the **Required Attribute** field to assign the value of User ID to samaccountname.
- h. For read/write setups only, in the **Fixed Attribute** fields, enter the name and fixed value of an attribute for all users. For example, you could create an attribute named “location,” with the value “headquarters” for all users.

Note: “Location” must be a defined attribute for the user object class.

10. In the Directory Configuration - User Groups section, do the following:

- a. In the **User Group Name** field, enter the directory attribute that maps to the user group name attribute. For example, User Group Name might map to cn.
- b. In the **Search Filter** field, enter an LDAP filter that returns only group entries, such as a filter on the group object class. For example, (objectclass=groupOfUniqueNames).
- c. From the **Search Scope** drop-down list, select the scope of user group searches in the LDAP tree. By default, this is set to search all sub-levels in an LDAP tree. You can also search only a single level.
- d. In the **RDN Attribute** field, enter the user group attribute used for the Relative Distinguished Name. For example, in Active Directory, cn, in Sun Java System Directory Server, uid.
- e. In the **Object Classes** field, enter the object class of users that are created or updated using the Security Console. For example, inetOrgPerson,organizationalPerson,person.
- f. For Active Directory only, use the **Required Attribute** fields if you want to populate two Active Directory user group attributes with the value of a single RSA user group attribute. For example, if you want to map the RSA attribute User ID to the Active Directory attributes CN and samaccountname, you could map User ID to CN and then use the **Required Attribute** field to assign the value of User ID to samaccountname.
- g. For read/write setups only, in the **Fixed Attribute** fields, enter the name and fixed value of an attribute for all users. For example, you could create an attribute named “location,” with the value “headquarters” for all users.

Note: “Location” must be a defined attribute for the user object class.

- h. In the **Membership Attribute** field, enter the attribute that contains the DNs of all the users and user groups that are members of a user group.

- i. Select **User MemberOf Attribute** to enable the system to use the MemberOf Attribute for resolving membership queries.
 - j. In the **MemberOf Attribute** field, enter the user and user group attribute that contains the DNs of the user groups to which they belong.
11. Click **Save**.

Linking an Identity Source to a Realm

To enable administration of an identity source, you must link it to a realm. Use the Security Console to link identity sources and realms. You can link multiple identity sources with a realm but you cannot link an identity source with more than one realm. When you link an identity source with a realm, all of the users in the identity source can be read and managed with the Security Console. Users in an identity source are visible in the top-level security domain by default, but can be moved to other security domains as necessary.

Note: Do not configure multiple identity sources with overlapping scope in the same realm or across realms. 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 can have overlapping scope with the corresponding administrative source, but two runtime identity sources cannot have overlapping scope.

Important: Only the Super Admin can manage realms and identity sources, and the linkage between them.

Linking an Active Directory Global Catalog with a Realm

If you are linking an Active Directory Global Catalog, you must also link each identity source that replicates user data to that Global Catalog.

For example, if identity sources IS1 and IS2 replicate information to Global Catalog GC1, and you link GC1 to a realm as your identity source, you must also link IS1 and IS2 to the realm.

To link the new identity source to a realm:

1. Log on to the Security Console as Super Admin.
2. Click **Administration > Realms > Manage Existing**.
3. Use the search fields to find the appropriate realm.
4. Select the realm.
5. From the Context menu, click **Edit**.

6. From the list of available identity sources, select the identity sources that you want to link with the realm, and click the right arrow.
If you link the realm to an Active Directory that is a Global Catalog, you must also link the identity sources that replicate to the Global Catalog.
7. Click **Save**.

Verifying the LDAP Identity Source

To verify that you have successfully added an identity source, you can view the particular users and groups from the LDAP identity source through the Security Console.

To verify the LDAP identity source:

1. Click **Identity > Users > Manage Existing**.
2. Use the search fields to find the appropriate realm and identity source, and click **Search**.
3. View the list of users from your LDAP identity source.

D

Troubleshooting

- [Accessing Installation Files on a Network](#)
- [Unsuccessful Installation or Removal](#)
- [Server Does Not Start](#)
- [RSA Security Console Does Not Start](#)
- [MMC Extension Does Not Start](#)
- [Message Indicates Node Manager Service Not Started](#)
- [Test Authentication Between RSA RADIUS and RSA Authentication Manager Unsuccessful](#)
- [Unsuccessful End-to-End Authentication on RSA RADIUS](#)
- [The RSA Security Console Times Out When Searching for Users](#)

Accessing Installation Files on a Network

RSA recommends installing RSA Authentication Manager on a machine that has a local DVD drive, or, if installing from an ISO, mounting the ISO image on the installation machine.

As an alternative, you can install Authentication Manager from a network drive, or copy the installation files from the network drive to the host machine. If you attempt to install from a network drive, or to copy the contents of the DVD or the ISO image from a UNIX machine to a Windows machine, you may encounter errors that cause the installation to fail, including the following:

Error 3001. This error occurs when you attempt to install from a network drive using a UNC path.

Error 2001. This error occurs when you attempt to install Authentication Manager using files you have copied from the DVD or ISO image to a network drive.

To avoid these errors, perform the following procedure:

1. Copy the contents of the DVD, or the ISO image, to the UNIX machine.
2. Navigate to the Windows subdirectory, and change the permissions of the **ora10g2** directory using the following command. Type:

```
chmod -R a+rx ora10g2
```
3. Copy the DVD or ISO installation files to the local machine and perform the installation.

Unsuccessful Installation or Removal

Perform these checks and tasks if the installer fails to run to completion.

DVD Read Errors

Occasionally, the Authentication Manager installer fails at 54% on the progress bar. This happens because of a read error caused by a DVD drive that lacks a high tolerance for physical inconsistencies in the media or by an error introduced when you create your own DVD from an RSA ISO image.

You can confirm that the problem is caused by a read error by navigating the DVD to see if opening any file causes a CRC error. You can also examine the **installActions_RSA.log** file stored in **RSA_AM_HOME\db\oraInventory\logs** to see if the Oracle installer was unable to extract any files.

This is typically an intermittent problem that can be resolved by restarting the installation process. If restarting the installation process does not resolve the problem, you may need to upgrade the DVD drive or re-create a new DVD from the RSA ISO image using a higher quality media.

Installation Logs

The Authentication Manager installer uses the **Temp** directory of the user performing the installation as a file staging area. If this directory has read-only permissions, the installer will not proceed with the installation.

The Authentication Manager installer also generates .log files, **rsa_am_install.log** or **install_err.log**, that are stored in this **Temp** directory. For example,

```
C:\Documents and Settings\User_ID\Local
Settings\Temp\1\rsa_am_20150406142928\installation_log_name
```

where:

- *User_ID* is the User_ID of the user performing the installation, for example, adminuser.
- *installation_log_name* is the name of the .log file, for example, rsa_am_install.log.

The Authentication Manager installation logs are stored in a directory that includes a time stamp using this format: YYYYMMDDHHmmSS. For example, rsa_am_20150406142928.

The Authentication Manager installer does not log specific installation details for third-party software. If a problem installing third-party software causes an unsuccessful Authentication Manager installation, examine the third-party log directory to find the source of the problem.

For example, if there is a permissions issue with an Oracle source file that prevents the installation of the internal database, the Oracle installer may report a high-level failure in the **rsa_am_install.log** file and may also log messages to the **RSA_AM_HOME\db\oraInventory\logs** directory. To determine the cause of the problem, navigate to **RSA_AM_HOME\db\oraInventory\logs**, and examine the **installActions_RSA.log** file for specific installation details.

In the case of an installation failure that causes a rollback of the installation, the **installActions_RSA.log** file (as well as other .log files from `\oraInventory\logs`) is copied to the **Temp** directory of the user performing the installation where it can be examined. The location for these .log files is **Temp/rsa_am_YYYYMMDDHHmmSS/oracleLogs/logs**.

Viewing Installation Logs

Authentication Manager records a log of all installations. You can find the following logs at these locations:

- Successful installation log (installation details):
Temp/rsa_am_YYYYMMDDHHmmSS/rsa_am_install.log
- Unsuccessful installation log (installation failures):
Temp/rsa_am_YYYYMMDDHHmmSS/install_err.log
- Successful installation log (configuration details):
RSA_AM_HOME/install/logs/config/config_trace.log
- Unsuccessful installation log (installation configuration errors):
RSA_AM_HOME/install/logs/config/config_err.log

An unsuccessful removal operation also creates a time-stamped uninstall log directory at **Temp/rsa_am_YYYYMMDDHHmmSS/rsa_am_uninstall.log**.

Unsuccessful Installation

Remove InstallShield Vital Product Data

If a LoggedSoftwareObject error occurs, do the following:

1. Remove InstallShield Vital Product Data (VPD) from your machine. Do one of the following:
 - On Windows, delete the contents of the InstallShield directory, **C:\Program Files\Common Files\IntallShield**.
 - On Solaris or Linux, delete the contents of the directory, **/root_home/InstallShield**.
2. Run the cleanup script. Do one of the following:
 - On Windows, type:
`RSA_AM_HOME\uninstall\clean.cmd`
 - On Solaris or Linux, type:
`RSA_AM_HOME/uninstall/cleanup.sh`

Failed to Configure Authentication Manager on Linux 32-bit

If the installation is unsuccessful because the oom-killer stops a process, temporarily alter the lower zone memory protection threshold and disable the out-of-memory process terminator until after the installation is complete.

Note: To check if the oom-killer stopped the process, check the messages file in `/var/log/` for the text “out of memory: killed process”.

Important: This procedure involves changing critical operating system files. RSA recommends that you make a backup copy of the original files before beginning these changes. Root user access is required.

To configure the system:

1. Change the lower zone memory protection threshold on the running system. Type:


```
echo "250" > /proc/sys/vm/lower_zone_protection
```
2. Disable the out-of-memory process terminator (oom-killer) on the running system. Type:


```
echo "0" > /proc/sys/vm/oom-kill
```

Note: Make sure that you remove the lower zone protection and re-enable oom-killer after the Authentication Manager installation (`echo "1" > /proc/sys/vm/oom-kill`).

Authentication Manager Services Cannot Be Started

If the error message “<BEA-149205> <Failed to initialize the application ‘am-app’ due to error weblogic.management.DeploymentException: Exception occurred while downloading files” appears in the `RSA_AM_HOME/server/logs/hostname_server.log` file, restart the Authentication Manager Service until it starts properly. This error is a transient network access issue and may take up to four tries to start the server properly.

After the Authentication Manager Service is started, restart the Operations Console service. If you have RADIUS selected, it must be manually configured.

To manually configure RADIUS:

1. Open a new command shell, and change directories to `RSA_AM_HOME/config`.
2. Type one of the following:
 - On Windows:


```
configUtil configure radius
```
 - On Solaris or Linux:


```
./configUtil.sh configure radius
```

Multihome System Installation Failures

If you are performing an installation on a multihome system and both IP addresses resolve to the same fully qualified hostname, you must reverse the order of the IP addresses in the hosts file. Type the secondary IP address first, followed by the primary IP address.

For example, if you have IP address “A” on a primary NIC, and IP address “B” on a secondary NIC, modify the hosts file and type IP address “B” before IP address “A”.

Unsuccessful Removal

Installer Fails to Remove RSA Authentication Manager

If the installer fails to remove Authentication Manager, do one of the following:

- On Windows, delete the contents of the directory, **C:\Program Files\Common Files\IntallShield\Universal**.
- On Solaris or Linux, delete the contents of the directory, **/root_home/InstallShield/Universal/rsa_am/Gen1**.

Uninstall Stops Responding

If the uninstall process stops responding, do the following:

1. Terminate the uninstall process.
2. Make sure that all of the servers are stopped.
3. Run the cleanup script. Do one of the following:
 - On Windows, type:

```
RSA_AM_HOME\uninstall\clean.cmd
```
 - On Solaris or Linux, type:

```
RSA_AM_HOME/uninstall/cleanup.sh
```

Reinstalling RSA Authentication Manager Components

If you have an Authentication Manager component installed on a machine, the Authentication Manager installer will not allow the installer to run on that machine again without first uninstalling the original component.

Cleanup Script for Reinstallation (Windows Only)

If you intend to perform an installation following a canceled or failed installation on a Windows system, first run the installer as described in [“Removing All RSA Authentication Manager Instances”](#) on page 205.

If the removal fails on a Windows system, make sure that all servers are stopped, and run the cleanup script at **RSA_AM_HOME\uninstall\clean.cmd**.

After you run this script on the target host, you can perform another installation of Authentication Manager.

Cleanup for Linux Systems

If you intend to perform an installation following a canceled or failed installation that did not revert or was abruptly terminated on a Linux system, you need to go to the home directory of the user who performed the failed installation, and do the following:

1. Delete the **~/InstallShield** directory.
2. Remove everything in the **RSA_AM_HOME** directory.
3. Remove the RSA RADIUS package file.
4. Make sure that you have stopped all Authentication Manager services.

Obscured Error Messages

The installer and removal programs may obscure error messages in a way that gives the appearance of an unresponsive installer. If the installer or removal programs appear to freeze, use ALT-TAB to determine if an error message window is open.

For example, in the case of a failed installation, there may be residual files left on your system. When you run the installer again, it may detect these files and prompt you whether to overwrite them. However, the error message may be obscured or minimized. If this situation occurs, click through all open windows or error messages, and select the option to allow the system to overwrite files.

Server Does Not Start

If one or all of the Authentication Manager services fail to start, examine the logs for information that may help you in troubleshooting the problem.

The logs are located in *RSA_AM_HOME/server/servers/service/logs* where *service* is the service that did not start, such as AdminServer or proxy_server.

RADIUS Server Does Not Start After Installation on a Windows Platform

If an error message appears indicating that Windows could not start the RSA RADIUS server, one possible cause is that the Windows Routing and Remote Access Service, the Windows Internet Authentication Service (IAS), or both are running on the server host. These two Windows services, when running, use ports that RSA RADIUS needs to run, and you must disable the Windows services.

To see if this is the problem, check the RADIUS log for the date of your installation. The log is located in *RSA_AM_HOME/radius/Service/yyyymmdd.log*.

Search the log for an entry similar to the following:

```
03/24/2008 18:23:45 Unable to bind UDP socket for Radius
requests 03/24/2008 18:23:45 Failed in attempt to bind to
0.0.0.0 and well-known port 1813.
```

Entries like this indicate that RSA RADIUS cannot listen on the ports it needs because the ports are already in use. You must disable the Windows services that are using the ports. Consult your Microsoft documentation for instructions on disabling the Windows services.

RSA Security Console Does Not Start

The Security Console may take considerable time to start on its initial startup. This may extend to ten minutes in some cases.

Using the Collect Product Information Utility

If your Security Console fails to start, use the Collect Product Information utility, collect-product-info, to gather information that may help you in troubleshooting the problem.

You can use the import command option flag to view the information. If required, you can send the data package to RSA Customer Support for analysis.

See [“Collect Product Information Utility”](#) on page 219.

MMC Extension Does Not Start

Perform these tasks if the MMC Extension fails to start:

1. Try to start the Security Console in a web browser to see if you can log on and perform a standard operation, such as listing a user-assigned token.
2. Try to use the Windows user account to log on to the Security Console. If this fails, the appropriate administrative role is not assigned to the Windows user.
3. Verify that the current Windows user account used to launch the MMC is Domain and Local administrator. If not, assign the appropriate privilege to the Windows user, and restart the MMC.
4. Open the Windows registry to see whether you have read/modify permission to the registry key:
HKEY_LOCAL_MACHINE\SOFTWARE\RSASecurity\AuthenticationManager\MMC.
5. (Remote access users only.) Verify that the client machine is part of the Active Directory domain.
6. (Remote access users only.) Verify that the Microsoft Toolkit is installed.

Message Indicates Node Manager Service Not Started

You might see the following message:

```
Could not start the RSA Authentication Node Manager service on
Local Computer.
Error 1053: The service did not respond to the start or control
request in a timely fashion
```

Although the message gives the impression that the service cannot start, in fact, the service may simply be taking a very long time to start. To resolve, clear the error message and continue to check for the service to start.

Test Authentication Between RSA RADIUS and RSA Authentication Manager Unsuccessful

If the test authentication between RSA RADIUS and Authentication Manager is not successful, complete the following steps:

- Verify that Authentication Manager and RSA RADIUS are running.
- Check to see if the RADIUS server is registered with Authentication Manager by using the Security Console to list the RADIUS servers. For instructions, see the Security Console Help topic “View RADIUS Servers.” If the RADIUS server is not registered, it will not show up in the list. Contact RSA Customer Support for assistance.

Unsuccessful End-to-End Authentication on RSA RADIUS

If the user is unable to use a RADIUS client to access a protected resource, complete the following steps:

- Use a third-party RADIUS test authentication tool to see if the RSA SecurID test authentication can succeed from the RSA RADIUS server to Authentication Manager. If it cannot, the problem is likely between the RADIUS server and the Authentication Manager server. See the preceding section, “[Test Authentication Between RSA RADIUS and RSA Authentication Manager Unsuccessful](#).”
- Check to see if there is a RADIUS client entry for the RADIUS server and the machine from which the RADIUS test authentication is occurring.
- Using the client’s administrative interface, check to see if the RADIUS secret is established on the client.
- Check the IP address of the client.

The RSA Security Console Times Out When Searching for Users

If the server exception error `PRINCIPAL_SEARCH_TIME_EXCEEDED` appears, you must re-index your Sun Java System Directory Server, and increase the cache size to 100 MB.

To re-index the directory:

1. In the Sun Java System Directory Server console, select the Directory Server, and click **Open**.
2. In the Sun Java System Directory Server, click the **Configuration** tab.
3. Expand the Data node and select the suffix that you want to re-index.
4. Select the **Indexes** tab.
5. Under Additional Indexes, select all of the checkboxes for **uid**, including **Approximate**, **Equality**, **Presence** and **Substring**.

6. Click **Save**.
7. Click **Reindex Suffix**.
8. Click **Check All**.
9. Click **OK** to begin re-indexing.
10. Click **Yes** to confirm.
11. When re-indexing completes, click **Close**.

To increase the cache size:

1. In the Sun Java System Directory Server console, click the **Configuration** tab.
2. Click the **Performance** node.
3. Select the **Caching** tab.
4. Change the Database cache size to 100 MB.
5. Click **Save**.
6. Click **OK**.
7. On the **Tasks** tab, click **Restart Directory Server**.

E

Removing RSA Authentication Manager

- [Removing All RSA Authentication Manager Instances](#)
- [Removing a Replica Instance](#)
- [Rebalancing the Contact List](#)
- [Removing the Primary Instance](#)
- [Removing an RSA RADIUS Standalone Server](#)

Removing All RSA Authentication Manager Instances

Remove all of the Authentication Manager instances from your deployment in this order:

1. Replica instances
2. Primary instance

After removing a replica instance, perform the tasks described in [“Rebalancing the Contact List”](#) on page 207.

Removing a Replica Instance

Perform the following procedure for each replica instance that you want to remove from your deployment.

Note: If you have RSA RADIUS installed on the Authentication Manager replica host machine, it is automatically removed when you remove the Authentication Manager replica instance.

To remove a replica instance on Windows:

1. On the primary instance host, open and log on to the RSA Operations Console.
2. Click **Deployment Configuration > Instances > Manage Existing**.
3. On the Manage Instance Replication page under **Manage Replication**, click **Delete Replica(s)**.
4. Select the replica instance that you are removing.
5. Click **Delete**.
6. Select the **Yes, delete the replica(s)** checkbox.
7. Click **Delete**.
8. Click **Done**.

9. On the replica instance host, click **Start > Settings > Control Panel**.
10. On the Control Panel page, double-click **Add or Remove Programs**.
11. Under **Currently installed programs**, select **RSA Authentication Manager**, and click **Remove**.
The RSA Authentication Manager installer screen is displayed.
12. Click **Next > Uninstall**.
13. Click **Finish**.
14. Perform the tasks described in [“Rebalancing the Contact List”](#) on page 207.

Note: When using the GUI-based uninstaller on Solaris and Linux operating systems, the DISPLAY environment variable must be defined and set to a display server configured to allow access.

For the command line interface, you must add the -console option to the uninstall.sh command in [step 11](#) of the following procedure. The command line uninstaller displays navigation prompts with instructions on how to proceed or select options.

Run the following procedure as root user.

To remove a replica instance on Solaris or Linux:

1. On the primary instance host, open and log on to the RSA Operations Console.
2. Click **Deployment Configuration > Instances > Manage Existing**.
3. On the Manage Instance Replication page under **Manage Replica**, click **Delete Replica(s)**.
4. Select the replica instance that you are removing.
5. Click **Delete**.
6. Select the **Yes, delete the replica** checkbox.
7. Click **Delete**.
8. On the replica instance host, open a command prompt.
9. Type:
`cd /`
10. Press ENTER.
11. Type:
`RSA_AM_HOME/uninstall/uninstall.sh`
where *RSA_AM_HOME* is the base installation directory.
12. Press ENTER.
13. When prompted to confirm the command, enter the appropriate response.
14. Perform the tasks described in [“Rebalancing the Contact List”](#) on page 207.

Rebalancing the Contact List

Each time that you remove a replica instance, rebalance the contact list using the primary instance RSA Security Console. The contact list directs agents to available servers. Deleting references to the removed replica instance prevents an agent from trying to authenticate using a server that no longer exists.

To rebalance the contact list:

1. On the primary instance, launch and log on to the RSA Security Console.
2. Click **Access > Authentication Agents > Authentication Manager Contact List > Automatic Rebalance**.
3. Click **Rebalance**.

Removing the Primary Instance

Ensure that Authentication Manager is running before you begin removal. It must be running during the removal process.

Note: If you have RSA RADIUS installed on the primary server, it is automatically removed when you remove the primary instance.

To remove the primary instance on Windows:

1. On the primary instance host, click **Start > Settings > Control Panel**.
2. On the Control Panel page, double-click **Add or Remove Programs**.
3. Under **Currently installed programs**, select **RSA Authentication Manager**, and click **Remove**.
The GUI uninstaller program is displayed on your screen.
4. Click **Next > Uninstall**.
5. Click **Finish**.

Note: When using the GUI-based uninstaller on Solaris and Linux operating systems, the DISPLAY environment variable must be defined and set to a display server configured to allow access.

For the command line interface, you must add the `-console` option to the `uninstall.sh` command in [step 4](#) of the following procedure. The command line uninstaller displays navigation prompts with instructions on how to proceed or select options.

Run the following procedure as root user.

To remove the primary instance on Solaris or Linux:

1. On the primary instance host, open a command prompt.
2. Type:


```
cd /
```
3. Press ENTER.
4. Type:


```
RSA_AM_HOME/uninstall/uninstall.sh
```

 where *RSA_AM_HOME* is the base installation directory.
5. Press ENTER.
6. When prompted to confirm the command, enter the appropriate response.

Removing an RSA RADIUS Standalone Server

The method of removing an RSA RADIUS standalone server (a RADIUS primary or replica server installed on a separate host machine) is the same as removing a primary or replica instance.

To remove an RSA RADIUS standalone server on Windows:

1. On the RADIUS standalone server host, click **Start > Settings > Control Panel**.
2. On the Control Panel page, double-click **Add or Remove Programs**.
3. Under **Currently installed programs**, select **RSA Authentication Manager**, and click **Remove**.
The RSA Authentication Manager installer screen is displayed.
4. Click **Next > Uninstall**.
5. Click **Finish**.

Note: When using the GUI-based uninstaller on Solaris and Linux operating systems, the DISPLAY environment variable must be defined and set to a display server configured to allow access.

For the command line interface, you must add the `-console` option to the `uninstall.sh` command in [step 4](#) of the following procedure. The command line uninstaller displays navigation prompts with instructions on how to proceed or select options.

Run the following procedure as root user.

To remove an RSA RADIUS standalone server on Solaris or Linux:

1. On the RADIUS standalone server host, open a command prompt.
2. Type:


```
cd /
```
3. Press ENTER.

4. Type:

```
RSA_AM_HOME/uninstall/uninstall.sh
```

where *RSA_AM_HOME* is the base installation directory.
5. Press ENTER.
6. When prompted to confirm the command, enter the appropriate response.

F

Reverting RSA Authentication Manager 7.1 to Version 6.1

- [Reverting a Migration on the Same Hardware](#)
- [Reverting a Migration to Different Hardware Using a Different Hostname and IP Address](#)
- [Reverting a Migration to Different Hardware Using the Same Hostname and IP Address](#)

After migration to version 7.1, all of the required version 6.1 data and application files still exist on the original Authentication Manager hardware. However, reverting to version 6.1 is not just simply stopping version 7.1 and restarting version 6.1. There are four important issues to consider when reverting:

- **Data loss**
All data concerning any version 7.1 administration or authentication activity is lost and cannot be recovered for use in version 6.1. Your version 6.1 servers will be in the same state they were in at the time of migration.
- **Authentication downtime and updating authentication agents**
The amount of time that administration capabilities are unavailable is minimal, since in all cases, reverting involves stopping version 7.1 and restarting version 6.1. However, the ability to authenticate is affected by the time it takes to update all the authentication agents.
- **Authentication agents**
To enable authentication agents to communicate with the reverted version 6.1 servers, you must either generate new configuration files for all agents, or delete the **sdstatus.12** file from all authentication agents, depending on the type of migration.
- **Replication traffic**
The reverted version 6.1 replica databases still contain delta records that will be replicated to the primary server when the replica server is started. Therefore, you may see a lot of activity occurring between the primary server and any replica servers on your network

Reverting a Migration on the Same Hardware

This section describes the steps to revert a migration performed on the same hardware as the original version 6.1 installation.

To revert a migration on the same hardware:

1. On the version 7.1 primary instance, stop all Authentication Manager services.
2. At the command line, type the appropriate command.
On Windows:

```
RSA_AM_HOME\server\rsaam stop all
```


On Linux and Solaris:

```
RSA_AM_HOME/server/rsaam stop all
```
3. Start the version 6.1 primary server.
On Windows:
 - a. On the version 6.1 primary server, click **Start > Programs > RSA Security > RSA Authentication Manager Control Panel**.
 - b. In the left-hand menu, click **Start & Stop RSA Authentication Manager Services**.
 On Linux and Solaris:
On the version 6.1 primary server, at the command line, type:

```
ACEPROG/sdconnect start  
ACEPROG/aceserver start
```
4. For each RSA Authentication Agent, delete the **sdstatus.12** file.
Deleting this file forces each agent to read the **sdconf.rec** file, which contains the names of the primary server and a replica server. When the agent contacts one of these servers, a new version 6.1 server list is sent from the server to the agent. Until the agent receives the new server list, it can communicate with the servers listed in the **sdeconf.rec** file only.
5. Repeat steps 1 and 2 for each replica instance.

Reverting a Migration to Different Hardware Using a Different Hostname and IP Address

If you migrated to new hardware with a new hostname or IP address, the process of reverting to version 6.1 requires that you generate new version 6.1 configuration files for any agent that authenticated to an version 7.1 instance.

To revert a migration to different hardware using a different hostname and IP address:

1. On the version 7.1 primary instance, stop all Authentication Manager services.
2. At the command line, type the appropriate command:
On Windows:

```
RSA_AM_HOME\server\rsaam stop all
```


On Linux and Solaris:

```
RSA_AM_HOME/server/rsaam stop all
```

3. Start the version 6.1 primary server.
On Windows:
 - a. On the version 6.1 primary server, click **Start > Programs > RSA Security > RSA Authentication Manager Control Panel**.
 - b. In the left-hand menu, click **Start & Stop RSA Authentication Manager Services**.
 - c. Under Start Services, click **Start All**.On Linux and Solaris:
On the version 6.1 primary server, at the command line, type:

```
ACEPROG/sdconnect start
ACEPROG/aceserver start
```
4. In the Database Administration application, generate new configuration files for all authentication agents.
 - a. Click **Agent Host > Generate Configuration Files**.
 - b. Click **All Agent Hosts**.
 - c. Click **OK**.The **sdconf.rec** file is created in a directory in the **ACEDATA/config_files** directory. The directory is named for the assigned Acting Master (or Acting Master/Slave pair) and the IP addresses of the assigned Acting Servers.
5. On each version 7.1 replica instance, stop all Authentication Manager services.
6. Restart any version 6.1 replica servers.
7. Distribute the new **sdconf.rec** files to any agents that authenticated to the version 7.1 instances.

Reverting a Migration to Different Hardware Using the Same Hostname and IP Address

To revert a migration to different hardware using the same hostname and IP address:

1. On the version 7.1 primary instance, stop all Authentication Manager services.
2. At the command line, type the appropriate command.
On Windows:

```
RSA_AM_HOME\server\rsaam stop all
```

On Linux and Solaris:

```
RSA_AM_HOME/server/rsaam stop all
```
3. Remove the version 7.1 primary instance from the network.
4. Add the version 6.1 primary server to the network using the same hostname and IP address as the version 7.1 primary instance.



5. Start the version 6.1 primary server.
On Windows:
 - a. On the version 6.1 primary server, click **Start > Programs > RSA Security > RSA Authentication Manager Control Panel**.
 - b. In the left-hand menu, click **Start & Stop RSA Authentication Manager Services**.On Linux and Solaris:
On the version 6.1 primary server, at the command line, type:

```
ACEPROG/sdconnect start
ACEPROG/aceserver start
```
6. Stop all version 7.1 replica instances.
7. For each RSA Authentication Agent, delete the **sdstatus12** file.
Deleting this file forces each agent to read the **sdconf.rec** file, which contains the names of the primary server and a replica server. When the agent contacts one of these servers, a new version 6.1 server list is sent from the server to the agent. Until the agent receives the new server list, it can communicate with the servers listed in the **sdeconf.rec** file only.
8. Remove all version 7.1 replica instances from the network.
9. Add the version 6.1 replica servers to the network using the same hostname and IP address as the version 7.1 replica instances.



RSA Authentication Manager 6.1 Command Line Utilities

- [Dumping the Database Using the Command Line](#)
- [Dumping the Log Using the Command Line](#)

This appendix contains procedures for using the version 6.1 command line utilities required to dump your existing server and log databases.

Dumping the Database Using the Command Line

The Database Dump utility, `sddumpsrv`, allows you to create a dump file from the database using the command line. There is additional functionality in this command line version that is not available using the GUI version of the dump utility. This additional functionality includes the ability to selectively dump tables from the Server database.

The following table describes the options and arguments for this utility.

Option	Argument	Description
-d	<i>database name</i>	Specifies database filename.
-f	<i>filename</i>	Specifies dump filename.
-t	<i>table list</i>	Specifies a list of tables containing associated data for each record to be read from the dump file.
-p	None	Dumps required parent tables.
-r	None	Dumps replica (delta) records.
-m	None	Allows you to dump the database in multiuser mode (while the database brokers are running).
-g	None	Dumps group, group members, users, and their tokens.
-u	<i>login</i>	Dumps a user record and tokens by associated default login.
-l	<i>login</i>	Same as -u .
-a	<i>serial number</i>	Dumps a single token, specified by the serial number.
-v	None	Provides detailed output information.

The **-p** option is only valid if selective dump mode (**-t**) is used. Options **-t**, **-g**, **-u**, and **-a** are mutually exclusive.

Dumping the Log Using the Command Line

The dump log utility, `sddumplog`, allows you to dump a log database using the command line.

The following table describes the options and arguments for this utility.

Option	Argument	Description
-d	<i>dbname</i>	Specifies a database filename.
-f	<i>filename</i>	Specifies a load filename.
-m	None	Allows you to dump the database in multiuser mode while the database brokers are running.

H

Command Line Utilities

- [Collect Product Information Utility](#)
- [Data Migration Utility](#)
- [Generating a Replica Package File](#)
- [Manage Secrets Utility](#)
- [Manage SSL Certificate Utility](#)

Overview

The following information is helpful to know before running a command line utility (CLU).

Using rsautil

The rsautil script provides the execution environment configuration necessary to run the RSA Authentication Manager CLUs that RSA provides. The rsautil script also runs custom Java or Jython applications using the RSA application programming interface (API) and software development kit (SDK). The rsautil script is located in the *RSA_AM_HOME/utills* directory.

Terminating Batch Jobs in Windows

If you are using a Windows environment, you can terminate a command line utility by pressing CTRL-C. When you press CTRL-C, Windows asks you if you would like to terminate the batch job, and allows you to select “Y” or “N.” The command line utility that you are running terminates regardless of whether you choose “Y” or “N.”

The CLU terminates because pressing CTRL-C interrupts the CLU, and Windows is unable to keep the CLU from terminating, even if you choose “N.”

Note: This same behavior occurs when you run WebLogic inside a command window.

Credentials Required to Run Command Line Utilities

The following table lists the credentials that are required to run the command line utilities described in the Authentication Manager documentation set. Each command line utility requires one (or more) of the following:

Master password. The utility requires the password specified at installation. This password is required for most of the utilities.

Super Admin. The utility must be run by an administrator with Super Admin credentials.

Administrator password. The utility must be run by an administrator who has the appropriate permissions for running the utility. Administrators with the appropriate permissions can enter their own passwords on the command line.

Utility	Required Credentials
Archive Requests	master password & Super Admin
Collect Product Information	master password
Data Migration	master password
Generate Database Package	master password
Generate RADIUS Package	master password
Import PIN Unlocking Key	administrator password ¹
Manage Backups	master password
Manage Batchjob	Super Admin
Manage Database	master password
Manage Nodes	master password
Manage RSA Operations Console Administrators	Super Admin
Manage Replication	master password
Manage Secrets	master password
Manage SSL Certificate	master password
Restore Super Admin	master password
Set Trace	Super Admin
Setup Replication	master password
Store	master password
Update Instance Nodes	master password
User Groups and Token Bulk Requests	master password & Super Admin
Verify Archive Log	master password

¹The administrator must be assigned a role that has PIN Unlock Key management (import and view) permissions.

Collect Product Information Utility

Use the Collect Product Information utility, `collect-product-info`, to collect system information, such as system log files and version information. This information is used to diagnose problems.

This utility collects the information, packages it into a file named **product_info.jar**, and encrypts the file. The encrypted file is transferred to a recipient who analyzes its contents. The recipient uses the Collect Product Information utility to decrypt the file.

Important: An improper DNS configuration can cause errors when this utility collects patch information from nodes in a cluster. If the patch information for a server node is not in the support package file, ensure that the DNS is configured correctly, and restart any of the servers in the cluster.

Important: The user who runs this utility to decrypt the **product_info.jar** file must know the package password you specify when you run this utility to create the **product_info.jar** file.

Using the Collect Product Information Utility

To use `collect-product-info`:

1. Open a new command shell, and change directories to *RSA_AM_HOME/utils*.
2. Type:

```
rsautil collect-product-info options
```

For relevant options, see the following section, [“Options for `collect-product-info`.”](#)

To collect system information and export it to an encrypted file, you use the following options:

```
rsautil collect-product-info --export  
--archive-time "2006-07-17 22:32:10.000"  
--package-password package_password
```

where:

- “2006-07-17 22:32:10.000” is the archive time.
- *package_password* is the password to encrypt the **product_info.jar** file.

Important: Although it is possible to enter the master password on the command line along with the other options, this creates a potential security vulnerability. RSA recommends that you enter the master password only when the utility presents a prompt.

Important: The support package file can contain sensitive data. RSA recommends that you move this file to a directory with appropriate access control after it is generated.

Options for collect-product-info

The following table describes the options for this utility.

Flag	Alternate Flag	Description
-t	--archive-time	This is the archive time. The log files are retrieved from the data store after this local time stamp and until the current time. The format is “yyyy-mm-dd hh:mm:ss.SSS”.
		Note: You must have double quotation marks around the archive time, and specify it in local 24-hour military time. If the archive time is not provided, log records from the previous hour are exported.
	--export	Collects system information and exports it to the encrypted product_info.jar file.
-h	--help	Displays help for this utility.
	--import	Decrypts the product_info.jar file.
		Note: The file must be located in the current working directory.
-m	--master-password	Master password of the encrypted properties file.
-p	--package-password	Password to encrypt or decrypt the product_info.jar file.
-v	--version	Displays version and copyright information.

Data Migration Utility

Use the Data Migration utility, `migrate-amapp`, to move user data from RSA Authentication Manager 7.0 to RSA Authentication Manager 7.1. The Data Migration utility is used during the process of upgrading the primary instance and its replica instances. This utility can also be used to revert an upgrade to the previous version.

Using the Data Migration Utility

To use migration:

1. Open a new command shell, and change directories to ***RSA_AM_HOME/utils***.
2. Type:

```
rsutil migrate-amapp options
```

For relevant options, see the following section, [“Options for migrate-amapp.”](#)

For example, to migrate primary instance data, specify these options:

```
rsautil migrate-amapp -a migratePrimary
--fileName primary_instance.dat
--scriptDir migration_scripts_directory
```

where:

- *primary_instance.dat* is the name of the destination file for backup or the source file for import.
- *migration_scripts_directory* is the SQL script directory.

Important: Although it is possible to enter the master password on the command line along with the other options, this creates a potential security vulnerability. RSA recommends that you enter the master password only when the utility presents a prompt.

Options for migrate-amapp

The following table describes the options for this utility.

Flag	Alternate Flag	Description
-a	--action	<p>Specifies an action to perform. Select one of the following:</p> <p>initMigration. Initialize RSA_MIGRATION_ADMIN and related migration packages.</p> <p>enableAudit. Enable data capture on all replica instances.</p> <p>backupPrimary. Back up primary instance data.</p> <p>importPrimary. Import primary instance data.</p> <p>migratePrimary. Migrate primary instance data.</p> <p>initMigrationOnReplica. Initialize additional migration configuration data on the replica instance.</p> <p>backupAudit. Back up captured runtime data on the replica instance.</p> <p>backupReplica. Back up replica instance data.</p> <p>importReplica. Import replica instance data.</p>

Flag	Alternate Flag	Description
-a	--action	<p>migrateReplica. Migrate replica instance data.</p> <p>importAudit. Import captured runtime data to the replica instance.</p> <p>enableReplication. Enable replication after reverting to the previous version.</p> <p>rollbackAudit. Import captured runtime data to the replica instance after reverting to the previous version.</p> <p>reportPrimary. Generate primary instance migration report.</p> <p>validatePrimary. Validate primary instance.</p> <p>reportReplica. Generate replica instance migration report.</p> <p>validateReplica. Validate replica instance.</p>
-d	--scriptDir	The SQL script directory.
-DMIGRATION_PROPERTIES		The system properties filename to initialize migration.
-f	--fileName	Destination file for backup or source file for import.
-h	--help	Displays help for this utility.
-I	--interactive	Runs utility in interactive mode.
-m	--master-password	Master password for the encrypted properties file.
-o	--oldHostName	The name of the machine where the data is migrating from. This is required if the data is migrating to a different machine, and it is used with the migratePrimary command.
-t	--hostName	The name of the machine where the data is migrating to. This is required if the data is migrating to a different machine, and it is used with the migratePrimary command.
-v	--version	Displays the version and copyright information.
-V	--verbose	Enable verbose reporting.

Generating a Replica Package File

When you install an Authentication Manager replica instance, you must provide a replica package file and, if you are doing a manual data transfer, the primary data .dmp file.

Replica package file. A.pkg file containing information about the Authentication Manager primary instance that enables replication from the primary to the replica instances.

Primary data file. A.dmp file containing a copy of the data in the primary database. The data from the primary database must be copied to the replica database when a replica instance is first installed.

Use the RSA Operations Console on the Authentication Manager primary instance to generate the replica package file and, if you are doing a manual data transfer, the primary data .dmp file.

Once the Operations Console generates the files, it prompts you to download the replica package file to your local machine, and it might prompt you to download the primary data file to your local machine.

From your local machine, you copy the data to the replica host. When installing the replica instance, you are prompted for the necessary files.

During the process of generating the replica package and, if you are doing a manual data transfer, the primary data .dmp file, you must select one of the following options:

Manual. Two files are created: the replica package file and the primary data file. In the process of attaching the replica to the primary instance, the replica database is created locally using the data in the primary data file. After that, changes in the primary database are synchronized over the network.

Important: The primary data file cannot be used after seven days. The file must never be renamed.

Automatic. Only the replica package file is created. After installation of the replica instance, all of the data from the primary database is copied directly to the replica database over the network, which can take a long time. If you have a large primary database, and a relatively slow network connection, select the manual option.

Each replica package file can be used for only one replica instance to ensure security during the replica installation process. Therefore, you need to generate a new replica package file, and, if you are doing a manual data transfer, the primary data .dmp file for each replica instance that you install.

Important: Do not generate more than one replica package file and primary data .dmp file at a time. If you do not use the most recent primary data .dmp file, the replica attachment fails.

To generate and download the replica files:

Note: You must be a Super Admin to perform this task.

1. On the primary instance, start the Operations Console, and log on using your Operations Console User ID and password.
2. Click **Deployment Configuration > Instances > Generate Replica Package**.
3. If you have not previously entered your Super Admin credentials, you are prompted to enter your Super Admin User ID and password.
4. In the **Replica Hostname** field, enter the fully qualified hostname of the replica server host.
5. In the **Replica IP Address** field, enter the IP address of the replica server host.
6. In the **Master Password** field, enter the master password that you created when you installed the Authentication Manager primary instance.
7. In the **Initial Data Transfer** field, select **Automatic** or **Manual**.
8. Click **Generate File(s)** to create the replica package file and, if you are doing a manual data transfer, the primary data .dmp file.

Note: An error message is displayed if another replica attachment is still in progress or if a previous replica attachment has failed. This error message provides directions for resolving these problems.

9. On the Download Files page, do one of the following, depending on your choice in [step 7](#):
 - If you selected **Automatic**, click **Download > Save**. In the SaveAs dialog box, select a location for the replica package file, and click **Save** to save the file to your local machine.
 - If you selected **Manual**, do the following:
 - Click **Download > Save**. In the SaveAs dialog box, select a location for the replica package file, and click **Save** to save the file to your local machine.
 - Click **Download > Save**. In the SaveAs dialog box, select a location for the primary data file, and click **Save** to save the file to your local machine.
10. Click **Done** to return to the Operations Console home page.

Manage Secrets Utility

The Manage Secrets utility, manage-secrets, exports or imports the encrypted **properties** file that contains the system fingerprint to or from a password-protected file. The exporting feature backs up a secured copy of the **properties** file encrypted by a password provided by the administrator. Using the importing feature, the administrator can unlock the **properties** file for disaster recovery.

Note: The Manage Secrets utility is a password storage tool. This utility does not change the passwords for the services, it simply stores the passwords. It is the responsibility of the user to make sure that the passwords and user names in the **properties** file are kept in synchronization with the passwords set through the services. The encrypted passwords are stored in ***RSA_AM_HOME/etc/systemfields.properties***.

Using the Manage Secrets Utility

To use manage-secrets:

1. Open a new command shell, and change directories to ***RSA_AM_HOME/utils***.
2. Type:

```
rsautil manage-secrets options
```

For relevant options, see the following section, [“Options for manage-secrets.”](#)

Important: Although it is possible to enter the master password on the command line along with the other options, this creates a potential security vulnerability. RSA recommends that you enter the master password only when the utility presents a prompt.

Use the indicated options to perform the following tasks:

- To export a system fingerprint-encrypted file into a password-protected file, type:

```
rsautil manage-secrets --action export  
--file myfile.exp --file-password file_password
```

where:

- *myfile.exp* is the name of the system fingerprint-encrypted file being exported.
- *file_password* is the password to unlock the file.

- To import a password-protected file that was created by the export command on either the same system or a different system, type:

```
rsautil manage-secrets --action import  
--file myfile.exp --file-password file_password
```

where:

- *myfile.exp* is the name of the password-protected file being imported.
- *file_password* is the password to unlock the file.

- To change a system fingerprint-encrypted file master password to a new value, type:

Important: When you change the master password on any primary instance, you are only changing it for that instance. You must also change the master password on each instance and on each remote RADIUS server.

```
rsautil manage-secrets --action change
--new-password new-master-password
```

- To recover the system fingerprint-encrypted file after the host machine is reconfigured, type:
- To load a number of keys (in bulk) from a plain text file into an encrypted file, type:

```
rsautil manage-secrets --action recover
```

```
rsautil manage-secrets --action load
--file mysecrets.properties
```

where *mysecrets.properties* is the name of the plain text file.

- To display a subset of the stored secrets in the file, type:

```
rsautil manage-secrets --action list
```

By default, this displays only the Command API Client User ID and Password.

- To display a subset of the raw key names (not localized names) to use when setting the values, type:

```
rsautil manage-secrets --action listkeys
```

By default, this displays only the raw key names or the Command API Client User ID and Password.

Note: You can use this option to find the raw key name before changing a value using the set or get commands. The set and get commands accept the raw key name, not the localized name.

- To set a previously stored secret to a specified value, type:

```
rsautil manage-secrets --action set com.rsa.appserver.
admin.password administrator_password
```

where *administrator_password* is the name of the password being set for *com.rsa.appserver.admin.password*.

- To list the current value of a single stored secret by name, type:

```
rsautil manage-secrets
--action get secret.raw.key.name
```

Options for manage-secrets

The following table describes the options for this utility.

Flag	Alternate Flag	Description
-a	--action	<p>Specifies an action to perform. Select one of the following:</p> <p>import. Imports a password-protected file to be system fingerprint encrypted. A file can be imported to the same system or a different system.</p> <p>export. Exports a system fingerprint-encrypted file to a password-protected file. This is used for backup purposes or to transport the managed secrets to a new server node that is being bootstrapped.</p> <p>change. Changes a system fingerprint-encrypted file master password. This option only changes the password that is used by the command line utilities to open the fingerprint-encrypted file. It does not affect the machine fingerprint.</p> <p>recover. Recovers a system fingerprint-encrypted file using the master password. This may be necessary if the host machine is reconfigured with more memory, new IP addresses, or new disks.</p> <p>load. Loads a plain text properties file into an encrypted file.</p> <p>list. Displays a subset of the secrets in the file. By default, this action only displays the CmdClient user name and password.</p> <p>listkeys. Displays a subset of the key names used for setting values. By default, this action only displays the CmdClient user name and password key names.</p> <p>set. Sets a property to a specified value. You must specify the name and value of the property to set. This can also be used to add a new secret in the secure storage.</p> <p>get. Lists the current value for a specified property. You must specify the name of the property to get. This option can be useful for scripting applications.</p>
-f	--file	Name of the password-protected file to import, export, or load.
-h	--help	Displays help for this utility.
-k	--file-password	Password to lock or unlock the file.
-m	--master-password	Master password for the encrypted properties file.
-n	--new-password	New master password for the change action.
-v	--version	Displays the version and copyright information.

Flag	Alternate Flag	Description
-X	--debug	Displays debug messages.

Manage SSL Certificate Utility

Use the Manage SSL Certificate utility, `manage-ssl-certificate`, to manage certificates signed by a trusted certificate authority (CA).

This utility simplifies managing SSL keystores and certificates. You must perform the tasks in this order:

1. Generate public and private key pairs in a keystore.
2. Create certificate signing requests (CSR) that the user submits to a certificate authority.
3. Import the root certificate of the CA to the keystore.
4. Import the server certificate signed by the CA to the keystore.
5. Update the application server configuration including the private key alias and password for the new certificate.

Using the Manage SSL Certificate Utility

To use `manage-ssl-certificate`:

1. Open a new command shell, and change directories to `RSA_AM_HOME/utlils`.
2. Type:

```
rsautl manage-ssl-certificate options
```

For relevant options, see the following section, "[Options for `manage-ssl-certificate`](#)."

Important: Although it is possible to enter the master password on the command line along with the other options, this creates a potential security vulnerability. RSA recommends that you enter the master password only when the utility presents a prompt.

Use the indicated options to perform the following tasks:

- To generate public and private key pairs in the keystore, type:

```
rsautil manage-ssl-certificate --genkey  
--alias private_key_alias --dname "certificate_DN"  
--keystore keystore_path
```

where:

- *private_key_alias* is the alias you enter here for the private key, for example, myPrivateKeyAlias.
 - "*certificate_DN*" is the distinguished name of the certificate, which is surrounded by quotes. For example, "CN=myserverhostname.mycompany.com,OU=AM,L=mycity,C=US". The commonName (CN) value must be the fully qualified domain name (FQDN) of the server host.
 - *keystore_path* is the absolute path of the keystore file (*server_hostname.jks*), for example, "C:\Program Files\RSA Security\RSA Authentication Manager\server\security\myServerHostname.jks".
- To create a certificate signing request (CSR), type:

```
rsautil manage-ssl-certificate --certreq  
--alias private_key_alias --keystore keystore_path  
--csr-file CSR_path
```

where:

- *private_key_alias* is the alias you enter here for the private key, for example, myPrivateKeyAlias.
- *keystore_path* is the absolute path of the keystore file, for example, "C:\Program Files\RSA Security\RSA Authentication Manager\server\security\myServerHostname.jks".
- *CSR_path* is the absolute path and name of the certificate signing request (CSR) output .pem file, for example, C:\certificates\myCertReq.pem. You must specify an existing path, for example, C:\certificates\ (the utility does not automatically generate a folder for this file). You must also specify a name for this file, for example, myCertReq.pem.

- To place a CA root certificate into the root keystore, type:


```
rsautil manage-ssl-certificate --import --trustcacerts
--alias ca_cert_alias
--cert-file ca_certificate_file_path
--keystore root_keystore_path
```

where:

 - *ca_cert_alias* is the alias you enter here for the CA root certificate, for example, myCACertAlias.
 - *ca_certificate_file_path* is the absolute path of the CA root certificate file from the certificate authority, for example, C:\certificates\myCACertificate.cer.
 - *root_keystore_path* is the absolute path of the root keystore file (**root.jks**), for example, *RSA_AM_HOME*\server\security\root.jks.
- To place the CA root certificate into the server keystore, type:


```
rsautil manage-ssl-certificate --import --trustcacerts
--alias ca_cert_alias
--cert-file ca_certificate_file_path
--keystore keystore_path
```

where:

 - *ca_cert_alias* is the alias for the CA root certificate, for example, myCACertAlias.
 - *ca_certificate_file_path* is the absolute path of the CA root certificate file from the certificate authority, for example, C:\certificates\myCACertificate.cer.
 - *keystore_path* is the absolute path of the server keystore file (**server_hostname.jks**), for example, *RSA_AM_HOME*\server\security\myServerHostname.jks.
- To place the signed server certificate from the certificate authority into the server keystore, type:


```
rsautil manage-ssl-certificate --import
--alias private_key_alias
--cert-file signed_certificate_file_path
--keystore keystore_path
```

where:

 - *private_key_alias* is the alias you specified, for example, myPrivateKeyAlias.
 - *signed_certificate_file_path* is the absolute path of the signed certificate file from the certificate authority, for example, C:\certificates\myServerCertificate.cer.
 - *keystore_path* is the absolute path of the server keystore file, for example, *RSA_AM_HOME*\server\security\myServerHostname.jks.

- To place the root certificate that you received from the certificate authority into the JDK CA certificate keystore, type:

```
rsautl manage-ssl-certificate --import --trustcacerts
--alias ca_cert_alias
--cert-file ca_certificate_file_path
--keystore JDK_keystore_path
```

where:

- *ca_cert_alias* is the alias you specified, for example, myCACertAlias.
 - *ca_certificate_file_path* is the absolute path of the CA root certificate file from the certificate authority, for example, C:\certificates\myCACertificate.cer.
 - *JDK_keystore_path* is the absolute path of the JDK CA keystore file (**cacerts**), for example, *RSA_AM_HOME*\appserver\jdk\jre\lib\security\cacerts.
- To configure the RSA Authentication Manager Administration Server to use the new private key alias and password, type:

```
rsautl manage-ssl-certificate --config-server
--alias private_key_alias --keystore keystore_path
--server-name AdminServer
```

where:

- *private_key_alias* is the alias you specified, for example, myPrivateKeyAlias.
 - *keystore_path* is the absolute path of the server keystore file, for example, *RSA_AM_HOME*\server\security\myServerHostname.jks.
- To configure the RSA Authentication Manager Proxy Server to use the new private key alias and password, type:

```
rsautl manage-ssl-certificate --config-server
--alias private_key_alias --keystore keystore_path
--server-name proxy_server
```

where:

- *private_key_alias* is the alias you specified, for example, myPrivateKeyAlias.
- *keystore_path* is the absolute path of the server keystore file, for example, *RSA_AM_HOME*\server\security\myServerHostname.jks.

- To configure the RSA Authentication Manager to use the new private key alias and password, type:

```
rsautil manage-ssl-certificate --config-server
--alias private_key_alias --keystore keystore_path
--server-name myServerHostname_server
```

where:

- *private_key_alias* is the alias you specified, for example, myPrivateKeyAlias.
- *keystore_path* is the absolute path of the server keystore file, for example, *RSA_AM_HOME*\server\security\myServerHostname.jks.
- *myServerHostname* is the hostname of the server.

Options for manage-ssl-certificate

The following table describes the options for this utility.

Flag	Alternate Flag	Description
	--alias	Alias for the key entry.
	--ca-alias	Alias for the CA certificate.
	--ca-cert-file	Absolute path of the CA certificate file.
	--cert-file	Absolute path of the signed (encoded) certificate file from CA.
	--certreq	Creates certification signing request (CSR).
	--config-server	Configures the server node to use the new private key.
	--csr-file	Optional. Absolute path of the CSR output file.
-x	--debug	Displays debugging messages.
	--dname	Specifies the distinguished name of the certificate. This is usually the name of the server host.
-g	--generate-cert-request	Generates key and CSR at the same time.
	--genkey	Generates public and private key pairs.
-h	--help	Displays help for this utility.
	--import	Imports CA and server certificates to the keystore.
	--keypass	Password for the key entry or alias.
	--keystore	Absolute path of the keystore file.
	--list	Lists one or more entries in the keystore.

Flag	Alternate Flag	Description
-m	--master-password	Master password of the encrypted properties file.
	--printcert	Displays the certificate file information.
	--server-name	Application server node name.
	--trustcacerts	CA certificate flag (used only if importing a CA certificate).
-u	--update-server-certs	Imports the CA, the server certificates, and the updates to the application server configurations at the same time.
-v	--version	Displays the version and copyright information.

Glossary

Term	Definition
Active Directory	The directory service that is included with Microsoft Windows 2000 Server, Microsoft Windows Server 2003, and Microsoft Windows Server 2008.
Active Directory forest	A federation of identity servers for Windows Server environments. All identity servers share a common schema, configuration, and Global Catalog.
AD	See Active Directory.
adjudicator	A component that defends Authentication Manager against replay attacks in which an intruder attempts to reuse an old passcode or acquires the current passcode for a token and sets the system clock back to use the captured passcode.
administrative command	A command other than a system-generated command.
administrative role	A collection of permissions and the scope within which those permissions apply.
administrator	Any user with one or more administrative roles that grants administrative permission to manage administrative resources.
Advanced Encryption Standard (AES)	The current cryptographic standard, adopted by the National Institute of Standards and Technology (NIST) in November, 2001. AES replaces Data Encryption Standard (DES) because it is considered to be more secure.
AES	See Advanced Encryption Standard.
agent	A software application installed on a device, such as a domain server, web server, or desktop computer, that enables authentication communication with Authentication Manager on the network server.
agent auto-registration utility	A utility included in the RSA Authentication Agent software that enables you to automatically register new authentication agents in the internal database, and updates the IP addresses for existing agents.
agent host	The machine on which an agent is installed.

Term	Definition
Agent Protocol Server	The Authentication Manager component that manages the ACE protocol packet traffic to and from agents. The inbound request packets are routed to the appropriate message handler. The response packets are sent to the originating agent.
approver	A Request Approver or an administrator with approver permissions.
attribute	A characteristic that defines the state, appearance, value, or setting of something. In Authentication Manager, attributes are values associated with users and user groups. For example, each user group has three standard attributes called Name, Identity Source, and Security Domain.
attribute mapping	The process of relating a user or user group attribute, such as User ID or Last Name, to one or more identity sources linked to a given realm. No attribute mapping is required in a deployment where the internal database is the primary identity source.
audit information	Data found in the audit log representing a history of system events or activity including changes to policy or configuration, authentications, authorizations, and so on.
audit log	A system-generated file that is a record of system events or activity. The system includes four such files, called the Trace, Administrative, Runtime Audit, and System logs.
authentication	The process of reliably determining the identity of a user or process.
authentication authority	The central entry point for authentication services.
authentication broker	A component that handles the authentication process and issuance of authentication tickets.
authentication method	The type of procedure required for obtaining authentication, such as a one-step procedure, a multiple-option procedure (user name and password), or a chained procedure.
authentication policy	A collection of rules that specify the authentication requirements. An authentication policy may be associated with one or more resources.
authentication protocol	The convention used to transfer credentials of a user during authentication. For example, HTTP-BASIC/DIGEST, NTLM, Kerberos, and SPNEGO.

Term	Definition
Authentication Server	An Authentication Manager component made up of services that handle authentication requests, database operations, and connections to the RSA Security Console.
authenticator	A device used to verify a user's identity to Authentication Manager. This can be a hardware token (for example, a key fob) or a software token.
authorization	The process of determining if a user is allowed to perform an operation on a resource.
authorization data	Information defined by the provisioning server, which is necessary to complete the provisioning of a CT-KIP-enabled token. Authorization data includes the appropriate serial number and places the new token credentials in the Authentication Manager internal database.
auto-registration	A setting which, if enabled, permits unregistered users to become registered upon a successful authentication to a system-managed resource. If auto-registration is disabled, only an administrative action can register users. Also see registered user and unregistered user.
Base Server license	Authentication Manager license that allows one primary instance and one replica instance. (Multiple replica instances are not allowed.) Includes RSA Credential Manager self-service. Credential Manager provisioning can be added.
Business Continuity option	Authentication Manager option that allows you to temporarily increase the number of users allowed into your system and the number of users allowed to use on-demand authentication.
certificate	An asymmetric public key that corresponds with a private key. It is either self-signed or signed with the private key of another certificate.
certificate DN	The distinguished name of the certificate issued to the user for authentication.
chained authentication	The process of creating a strong form of authentication by combining two weaker forms. For example, the user is required to use a PIN and a tokencode.
client time-out	The amount of time (in seconds) that the user's desktop can be inactive before reauthentication is required.
CLU	See command line utility.

Term	Definition
command line utility (CLU)	A utility that provides a command line user interface.
connection pool	A named group of identical connections to a data store.
contact list	A list of instances provided by the Authentication Manager to the agent, to which the agent can direct authentication requests.
context-based authentication	An authentication sequence in which the system presents the user with only the authentication options that are appropriate for the User ID entered. The options are based on policy requirements and the authenticators that the user owns.
core attributes	The fixed set of attributes commonly used by all RSA products to create a user. These attributes are always part of the primary user record, whether the deployment is in an LDAP or RDBMS environment. You cannot exclude core attributes from a view, but they are available for delegation.
Credential Manager Provisioning	An option that automates the token deployment process and provides user self-service options.
cryptographic algorithm	A mathematical function that uses plain text as the input and produces cipher text as the output and vice-versa. It is used for encryption and decryption.
CT-KIP	Cryptographic Token-Key Initialization Protocol.
CT-KIP-capable token	A token that is capable of storing the authorization data and seed generated as a result of CT-KIP operations between a CT-KIP 1.0 client and an Authentication Manager CT-KIP server.
CT-KIP client	A program that implements the CT-KIP client-side protocol and interacts with a CT-KIP server for the secure initialization of CT-KIP-capable tokens.
CT-KIP server	A software component of Authentication Manager that implements the CT-KIP server-side protocol and interacts with a CT-KIP client application for the secure initialization of CT-KIP-capable tokens.
CT-KIP toolkit	An implementation of the CT-KIP client-server protocol. It provides the API for creating CT-KIP server or client applications.
customer name	The name of the enterprise to which the license is issued.

Term	Definition
data encryption standard (DES)	The cryptographic standard prior to November 2001, when the National Institute of Standards and Technology (NIST) adopted the Advanced Encryption Standard (AES).
data store	A data source such as a relational database (Oracle or DB2) or directory server (Sun Java System Directory Server or Microsoft Active Directory). Each type of data source manages and accesses data differently.
data transfer object	Simple object used to pass data between tiers. It does not contain business logic.
delegated administration	A scheme for defining the scope and responsibilities of a set of administrators. It permits administrators to delegate a portion of their responsibilities to another administrator.
denial of service	The process of making a system or application unavailable. For example, the result of barraging a server with requests that consume all the available system resources, or of passing malformed input data that can cause the system to stop responding.
delivery address	The e-mail address or the cell phone number where the on-demand token codes will be delivered.
deployment	The arrangement of Authentication Manager instances into appropriate locations in a network to perform authentication.
DES	See data encryption standard.
distribution file	A shared secret between a hardware or software authenticator and an authentication server. The authenticator, sometimes called a token, and the server work together in a time synchronous, or time dependent mode to provide a one-time passcode that the token holder enters at logon.
distribution file password	A password used to protect the distribution file when the distribution file is sent by e-mail to the user.
distributor	A Token Distributor or an administrator with distributor permissions.
DTO	See data transfer object.
dump	An RSA ACE/Server format used to back up, restore, and merge database information. A dump file is a binary data file that contains all database tables and columns in table-dependency order.

Term	Definition
EAP	See extensible authentication protocol.
EAP-POTP	An RSA-proposed IETF (Internet Engineering Task Force) standard that defines the method for one-time password (RSA SecurID) authentication. It provides capabilities, such as end-to-end protection of one-time passwords and support for token exception cases (New PIN, Next Tokencode, and others).
EAP-POTP client	Client that supports the EAP-POTP method.
e-mail notifications	Contain status information about requests for user enrollment, tokens, and user group membership are sent to users who initiated the request. For token requests, e-mail notifications also contain information about how to download and activate tokens. Request Approvers and Token Distributors receive e-mail notifications about requests that require their action. See e-mail templates.
e-mail templates	Templates that administrators can use to customize e-mail notifications about user requests for user enrollment, tokens, user group membership, or the on-demand tokencode service. See e-mail notifications.
emergency access	The process for enabling a token for a user whose token is not available or is not functioning. Used in connection with offline authentication access.
emergency access passcode	A complete authentication code that, if enabled, can be used by a user to perform an offline authentication without an authenticator or PIN.
emergency access tokencode	A partial authentication code that, if enabled, can be used by a user to perform an offline authentication without an authenticator. The user is required to provide his or her PIN.
Enterprise Server license	Authentication Manager license that allows a primary instance and multiple replica instances.
Evaluation license	Authorizes an evaluation copy of the product at a customer site.
event-based token	A hardware token that displays a tokencode whenever the user presses the button on the token.

Term	Definition
excluded words dictionary	A dictionary containing a record of words that users cannot use as passwords. It includes several thousand commonly used words that are likely to be included as part of any dictionary attacks on the system, for example, “password.” The excluded words dictionary prevents users from using common, and therefore, easily guessed words as passwords.
extensible authentication protocol (EAP)	An authentication framework that supports multiple authentication methods.
failover mode	The state in which the connection pool management service has to use the secondary connection pools for serving the connection requests, because the primary connection pools are not available due to the failed primary data servers.
four-pass CT-KIP	The exchange of two protocol data units (PDUs) between the client and server.
Global Catalog	A read-only, replicated repository of a subset of the attributes of all entries in an Active Directory forest.
graded authentication	A mechanism for noting the relative strengths of authentication methods (either individually or as combinations). For example, an RSA SecurID token is stronger than a user name and password. Equivalently ranked methods may be used interchangeably.
group membership	See user group.
hardware token	A physical device, such as an RSA SecurID standard card, key fob, or PINPad that displays a tokencode.
high-water mark	The highest numbered interval used by a user to authenticate.
identity attribute definition	Customer-defined attributes that are mapped to an existing customer-defined schema element. They are always stored in the same physical repository as the user’s or user group’s core attribute data. You can search, query, and report on these attributes. Each identity attribute definition must map to an existing attribute in the LDAP or RDBMS.
Identity Management Services	The set of shared components, toolkits, and services used to build RSA products, for example, Authentication Manager.
identity source	A data store containing user and user group data. The data store can be the internal database or an external directory server, such as Sun Java System Directory Server or Microsoft Active Directory.

Term	Definition
IMS	See Identity Management Services.
initial time-out	The wait time, in seconds, before the initial remote access prompt appears. (The term is used in relation to remote RSA SecurID authentication.)
instance	An installation of RSA Authentication Manager and the internal database. An instance can also include a local RADIUS server. You can install one primary instance and multiple replica instances.
instance ID	This ID identifies a single logical installation of a product or component.
instance name	The hostname of the instance.
interval	A value used to represent a specific time-based PRN code being generated by an authenticator.
internal database	The Authentication Manager proprietary data source.
J2EE	See Java 2 Enterprise Edition.
Java 2 Enterprise Edition	A framework for building enterprise applications using Java technology.
Java Cryptographic Architecture (JCA)	The set of APIs provided by the Java 2 platform that establishes the architecture and encapsulates limited cryptographic functionality from various cryptographic providers.
Java Cryptographic Extensions (JCE)	The set of APIs provided by the Java 2 platform that encapsulates additional cryptographic functionality from various cryptographic providers.
Java keystore (JKS)	The Java 2 platform implementation of a keystore provided by Sun Microsystems.
Java Management Extensions (JMX)	The set of APIs provided by the Java 2 platform that enables building distributed, web-based, dynamic, and modular solutions for managing and monitoring devices, applications, and service-driven networks.
Java Messaging Service (JMS)	A standard Java interface for interacting with message queues and topics.
Java Server Pages (JSP)	A commonly used technology for dynamic web content.
JCA	See Java Cryptographic Architecture.

Term	Definition
JCE	See Java Cryptographic Extensions.
JKS	See Java keystore.
JMS	See Java Messaging Service.
JMX	See Java Management Extensions.
JSP	See Java Server Pages.
keystore	The Java 2 platform facility for storing keys and certificates.
Key Management services	The management of the generation, use, storage, security, exchange, and replacement of cryptographic keys.
Key Management encryption key	The key used for encryption or decryption operations of keys managed by Key Management services.
license	A verifiable piece of information that represents permission from RSA to use Authentication Manager, its features, or both. A license is a component of the License Management Service.
license category	A way of grouping different types of licenses. The license categories for Authentication Manager are Base Server, Enterprise Server, and Evaluation.
license creation date	The date when the license file is created.
license deployment	Specifies either a server or floating license.
license file	An XML file containing license data that is common across all IMS-based products. The categories of data are: client, product, and feature. A license file is a component of LMS.
license file version	The version of the license schema to which the generated license conforms.
license ID	An internal identifier associated with the license. RSA Manufacturing assigns the license ID.
License Management Service (LMS)	A service responsible for managing and validating product licenses.
license.rec	A license record file containing the database key needed to extract critical information from the dump file.
LMS	See License Management Service.

Term	Definition
local authentication client component	An RSA Authentication Agent component that requires users to enter valid RSA SecurID passcodes to access their Microsoft Windows desktops.
locked license	A license limited to a specific server instance. See server license.
lockout policy	A set of conditions specifying when an account will be locked and whether the account must be unlocked by an administrator or will unlock on its own after a designated amount of time. Lockout policies are applied to security domains. Each realm has a default lockout policy.
log archival	Creates a backup copy of the log for noncurrent, permanent storage.
logging service	A component responsible for recording system, audit, and trace events.
lower-level security domain	In a security domain hierarchy, a security domain that is nested within another security domain.
Management Information Base (MIB)	A type of virtual database used to manage the devices (switches and routers, for example) in a communication network. For example, SNMP uses MIB to specify the data in a device subsystem.
MD5	An algorithm that produces a 128-bit message digest.
member user	A user who is a member of a member user group.
member user group	A user group that is a member of another user group. For example, an organization might define a Sales Managers user group within a North America user group. All member user groups must belong to the same identity source as the parent group, with one exception: any user group from any identity source can be assigned to a parent group that is stored in the internal database.
MIB	See Management Information Base.
Microsoft Management Console (MMC)	A user interface through which system administrators can configure and monitor the system.
MMC	See Microsoft Management Console.
namespace	A set of names. A namespace defines a scope for a collection of names.

Term	Definition
Network Management System (NMS)	Software used to manage and administer a network. The NMS uses SNMP to monitor networked devices and is responsible for polling and receiving SNMP traps from agents in the network.
NMS	See Network Management System.
NMS administrator	The person monitoring the network (through the NMS) for significant events. Also known as a network administrator.
node secret	<p>A long-lived symmetric key that the agent uses to encrypt the data in the authentication request.</p> <p>Authentication Manager generates the authentication request when a user makes a successful authentication attempt. The node secret is known only to the Authentication Manager and the agent.</p>
offline emergency tokencode	Provides emergency access for RSA SecurID for Windows users who require emergency access while authenticating offline. Use this option if the user has a temporarily misplaced, lost, or stolen token. The Offline Emergency Access Tokencode is used with the user's PIN.
offline emergency passcode	Provides emergency access for RSA SecurID for Windows users who require emergency access while authenticating offline. Use this option if the user has forgotten his or her PIN. The Offline Emergency Passcode is used in place of the user's PIN and tokencode.
object	Describes the following: security domains, identity sources, attributes, users, user groups, administrative roles, and policies.
offset	A value used to represent the amount of time an authenticator's internal clock has drifted over time.
on-demand tokencode	<p>Tokencodes delivered by SMS or SMTP. They require the user to enter a PIN to achieve two-factor authentication. On-demand tokencodes are user-initiated, as Authentication Manager only sends a tokencode to the user when it receives a user request.</p> <p>An on-demand tokencode can only be used once, and you configure the lifetime of an on-demand tokencode. See on-demand tokencode service.</p>

Term	Definition
on-demand tokencode service	A service that allows users to request on-demand tokencodes delivered by text message or e-mail, instead of tokens. You configure the on-demand tokencode service for requests using the Security Console. Users must be enabled to receive on-demand tokencodes before they can request them.
one-time tokencode set	Used for online emergency access. A set of tokencodes, each of which can be used only once, and is used with the user's PIN to create a passcode. The administrator can specify how many tokencodes are in the set.
PAM	See Pluggable Authentication Modules.
passcode	A code entered by a user to authenticate. The passcode is a combination of a PIN and a tokencode.
password-based encryption	The process of obscuring information so that it is unreadable without knowledge of the password.
password policy	A set of specifications that define what constitutes a valid password and the conditions under which the password expires. Password policies are applied to security domains.
PDU	See Protocol Data Unit.
permissions	Specifies which tasks an administrator is allowed to perform.
Pluggable Authentication Modules (PAM)	Mechanisms that allow the integration of new authentication methods into an API, independent of the existing API authentication scheme.
primary connection pool	Refers to the connection pools containing the connections to the primary instance database server.
primary instance	The machine with the installation of Authentication Manager at which authentication and all administrative actions occur.
private key	In asymmetric key cryptography, the cryptographic key that corresponds to the public key. The private key is usually protected by some external mechanism (for example, smart card, password encrypted, and so on).
PRN	See pseudorandom number.
Protocol Data Unit	A packet of data exchanged between two application programs across a network.
provisioning	See token provisioning.

Term	Definition
provisioning data	The provisioning server-defined data. This is a container of information necessary to complete the provisioning of a token device. Its format is not specified by CT-KIP because it is outside the realm of CT-KIP, but it is necessary for provisioning.
pseudorandom number (PRN)	A random number or sequence of numbers derived from a single seed value.
public key	In asymmetric key cryptography, the cryptographic key that corresponds with the private key. The public key is usually encapsulated within a certificate.
RADIUS	See Remote Authentication Dial-In User Service.
realm	An entire security domain hierarchy consisting of a top-level security domain and all of its lower-level security domains. A realm includes all of the objects managed within the security domain hierarchy (users, tokens, and password policies, for example). Each realm manages users and user groups in one or more identity sources.
regular time-out	The number of seconds before remote access prompts time out. The term is used in relation to remote RSA SecurID authentication.
Remote Authentication Dial-In User Service (RADIUS)	A UDP-based protocol for administering and securing remote access to a network.
remote EAP (extensible authentication protocol)	A remote authentication feature that requires users to submit RSA SecurID passcodes in order to open remote connections to the network. EAP has a graphical user interface and enhanced security and is supported in both Point-to-Point Protocol (PPP) authentication environments and non-PPP authentication environments, including Point-to-Point Tunneling Protocol (PPTP) VPN connections, 802.1x wired, and 802.11 wireless connections, and other specialized network media.
remote post-dial	Refers to the dial-in Point-to-Point Protocol (PPP) authentication support. With a post-dial terminal-based connection, when remote users dial in, a terminal-like character interface presents a simple user name and passcode prompt. If the right passcode is entered, the PPP connection is established. If the wrong passcode is entered, the dial-up connection is severed.

Term	Definition
replica instance	The machine with the installation of Authentication Manager at which authentication occurs and at which an administrator can view the administrative data. No administrative actions are performed on the replica instance. All administrative actions are performed on the primary instance.
requests	Allows users to enroll, as well as request tokens, the on-demand tokencode service, and user group membership.
Request Approver	A predefined administrative role that grants permission to approve requests from users for user enrollment, tokens, or user group membership.
RSA Credential Manager	A component of Authentication Manager that allows users to request, maintain, and troubleshoot tokens.
RSA EAP	The RSA Security implementation of the EAP 15 authentication protocol that facilitates RSA SecurID authentication to networks in PPP, PPTP (VPN), and 802.1x (wireless or port access) environments.
RSA Operations Console	An administrative user interface through which the user configures and sets up Authentication Manager, for example, adding and managing identity sources, adding and managing instances, and disaster recovery.
RSA Protected OTP	The RSA implementation of the EAP 32 authentication protocol that facilitates RSA SecurID authentication to networks in PPP, PPTP (VPN), and 802.1x (wireless or port access) environments.
RSA Security Console	An administrative user interface through which the user performs most of the day-to-day administrative activities.
RSA Self-Service Console	A user interface through which the user requests, maintains, and troubleshoots tokens.
runtime	Describes automated processing behavior—behavior that occurs without direct administrator interaction.
runtime command	A logon or logoff command.
runtime identity source	The runtime representation of the identity source. Runtime identity sources are used during runtime operations, such as authentication and group membership resolution instead of the corresponding administrative source, which is used for all other operations. This is an integral part of Active Directory forest support, which uses the Global Catalog during runtime operations.

Term	Definition
scope	In a realm, the security domain or domains within which a role's permissions apply.
secondary connection pool	The connection pools containing the connections to the secondary data stores.
Secure Sockets Layer (SSL)	A protocol that uses cryptography to enable secure communication over the Internet. SSL is widely supported by leading web browsers and web servers.
security domain	A container that defines an area of administrative management responsibility, typically in terms of business units, departments, partners, and so on. Security domains establish ownership and namespaces for objects (users, roles, permissions, and so on) within the system. They are hierarchical.
security questions	A way of allowing users to authenticate without using their standard method. To use this service, a user must answer a number of security questions. To authenticate using this service, the user must correctly answer all or a subset of the original questions. The answers to security questions are case sensitive.
self-service	Allows users to perform maintenance tasks and troubleshoot tokens themselves, instead of calling the Help Desk. See also Token Provisioning.
Self-Service Console	See RSA Self-Service Console.
self-service requests	See requests.
self-service troubleshooting policy	Provides an emergency form of authentication that allows users to log on to the RSA Self-Service Console to perform troubleshooting tasks.
session	An encounter between a user and a software application that contains data pertaining to the user's interaction with the application. A session begins when the user logs on to the software application and ends when the user logs off of the software application.
session policy	A set of specifications designating the restrictions on overall session lifetime and multiple session handling. Session policies are applied to an instance.
SHA1	A secure hash algorithm function that produces a 160-bit hash result.

Term	Definition
shipping address	An address used by distributors to distribute hardware tokens.
Short Message Service (SMS)	A mechanism of delivery of short messages over mobile networks. It is often called text messaging. In Authentication Manager, it is a means of sending tokencodes to a cell phone. Tokencodes delivered by SMS are called on-demand tokencodes.
Simple Mail Transfer Protocol (SMTP)	A TCP/IP protocol used in sending and receiving e-mail. In Authentication Manager, it is a means of sending tokencodes to e-mail accounts. Tokencodes delivered by SMTP are called on-demand tokencodes.
Simple Network Management Protocol (SNMP)	A protocol for exchanging information about networked devices and processes. SNMP uses MIBs to specify the management data, and then uses the User Datagram Protocol (UDP) to pass the data between SNMP management stations and the SNMP agents.
single sign-on (SSO)	The process of requiring only a single user authentication event in order to access multiple applications and resources.
SMS	See Short Message Service.
SMTP	See Simple Mail Transfer Protocol.
snap-in	A software program designed to function as a modular component of another software application. For example, the MMC has a variety of snap-ins that offer different functionality (for example, Device Manager).
SNMP	See Simple Network Management Protocol.
SNMP agent	Software module that performs the network management functions requested by network management stations.
SNMP trap	An asynchronous event that is generated by the agent to tell the NMS that a significant event has occurred. SNMP traps are designed to capture errors and reveal their locations.
SSL	See Secure Sockets Layer.
SSO	See single sign-on.

Term	Definition
Super Admin	<p>An administrator who has all permissions within the system. A Super Admin:</p> <ul style="list-style-type: none"> • Can create and delete realms • Can link identity sources to realms • Has full permissions within any realm • Can assign administrative roles within any realm
symmetric key	A key that allows the same key value for the encryption and decryption of data.
system event	System-generated information related to nonfunctional system events such as server startup and shutdown, failover events, replication events, and so on.
system log	Persistable store for recording system events.
TACACS+	See Terminal Access Controller Access Control System+.
temporary fixed tokencode	Used for online emergency access. This temporary tokencode is used in conjunction with the user's PIN to create a passcode. The user can use this tokencode more than once. The administrator can configure the expiration date and other Temporary Fixed Tokencode attributes.
Terminal Access Controller Access Control System+ (TACACS+)	A remote authentication protocol that is used to communicate with an authentication server. Allows a remote access server to communicate with an authentication server to determine if a user has access to the network.
time-based token	A hardware token that always displays a tokencode and the tokencode changes automatically every 60 seconds.
token	A hardware device or software program that generates a pseudorandom number that is used in authentication procedures to verify a user's identity.
Token Distributor	A predefined administrative role that grants permission to act upon requests from users for tokens. Distributors record how they plan to deliver tokens to users and close requests.
token provisioning	The automation of all the steps required to provide enrollment, user group membership, RSA SecurID tokens, and the on-demand tokencode service to users. See also self-service.
tokencode	The random number displayed on the front of a user's RSA SecurID token. Tokencodes change at a specified time interval, typically every 60 seconds.

Term	Definition
top-level security domain	The top-level security domain is the first security domain in the security domain hierarchy (realm). The top-level security domain is unique in that it links to the identity source or sources and manages password, locking, and authentication policy for the entire realm.
trace log	Persistable store for trace information.
trusted realm	A trusted realm is a realm that meets these criteria: <ul style="list-style-type: none"> • It is located in a different deployment than your realm. • It has exchanged configuration settings with your realm. The settings are in an XML file called a trust package.
trust package	An XML file that contains configuration information about the realm.
two-factor authentication	An authentication protocol requiring two different ways of establishing and proving identity, for example, something you have (such as an authenticator) and something you know (such as a PIN).
two-pass CT-KIP	The exchange of one protocol data unit (PDU) between the client and server.
UDP	See User Datagram Protocol.
user	An account managed by the system that is usually a person, but may be a computer or a web service.
User Datagram Protocol (UDP)	A protocol that allows programs on networked computers to communicate with one another by sending short messages called datagrams.
user group	A collection of users, other user groups, or both. Members of the user group must belong to the same identity source. User group membership determines access permission in some applications.
User ID	A character string that the system uses to identify a user attempting to authenticate. Typically a User ID is the user's first initial followed by the last name. For example, Jane Doe's User ID might be <i>jdoe</i> .
workflow	The movement of information or tasks through a work or business process. A workflow can consist of one or two approval steps and a distribution step for different requests from users.

Term	Definition
workflow participant	Either approvers or distributors. Approvers review, approve, or defer user requests. Distributors determine the distribution method for token requests and record the method for each request. See also workflow.

Index

A

- Active Directory, 44
 - definition, 235
 - forest, 185
 - Global Catalog, 185
 - group membership, 187
 - MMC Extension, 145
 - password policy, 187
 - starting console, 149
- Active Directory forest
 - definition, 235
- Active Directory Global Catalog, 186
- AD. *See* Active Directory
- adjudicator
 - definition, 235
- administrative command
 - definition, 235
- administrative identity source, 185
- administrative role
 - assigning, 32
 - custom, 31
 - definition, 235
 - predefined, 31, 35
- administrator
 - about, 31
 - assigning roles, 32
 - definition, 235
 - permissions, 32
 - predefined roles, 35
 - scope, 33
- Advanced Encryption Standard
 - definition, 235
- AES. *See* Advanced Encryption Standard
- agent
 - contact lists, 207
 - definition, 235
- agent auto-registration utility
 - definition, 235
- agent host
 - definition, 235
- Agent Protocol Server
 - definition, 236
- approval steps, 115
- approver
 - definition, 236
- attribute
 - definition, 236
- attribute mapping
 - definition, 236
- audit information
 - definition, 236
- audit log
 - definition, 236
- authentication
 - definition, 236
 - self-service troubleshooting, 114
- authentication authority
 - definition, 236
- authentication broker
 - definition, 236
- Authentication Manager
 - certificate and key, 70, 88
 - pre-migration checklist, 51
 - security backup files, 79, 91
 - server fails to start, 200
 - starting services
 - on Solaris and Linux, 130
 - on Windows, 129
 - stopping services
 - on Solaris and Linux, 130
 - on Windows, 129
 - system architecture, 57
 - user for Linux installation, 51, 52
- authentication method, 114
 - definition, 236
- authentication policy
 - definition, 236
- authentication protocol
 - definition, 236
- Authentication Server, 57
 - definition, 237
- authenticator
 - definition, 237
- authorization
 - definition, 237
- authorization data
 - definition, 237
- auto-registration
 - definition, 237

B

- backup
 - post-installation, 79, 91
 - standalone primary instance, 125

- Base Server license, 17
 - definition, 237
 - self-service, 105
- browser
 - security, 44
 - support, 44
- Business Continuity option
 - definition, 237

- C**
- certificate
 - definition, 237
 - LDAP, 136
 - SSL requirements, 136
 - SSL-LDAP, 44
- certificate DN
 - definition, 237
- certificate. *See* SSL
- chained authentication
 - definition, 237
- checklist
 - Credential Manager, 122
- checklists
 - pre-migration, 51
- client time-out
 - definition, 237
- clocks, synchronizing, 47, 128
- CLU
 - Collect Product Information, 219
 - Data Migration, 220
 - Dumping the Database, 215
 - Manage Secrets, 224, 225
 - Manage SSL Certificate, 228
- CLU command
 - collect-product-info, 220
 - manage-secrets, 227
 - manage-ssl-certificate, 232
 - migrate-amapp, 220
 - sddumpsrv, 215
- CLU. *See* command line utility
- Collect Product Information utility, 200, 219
- collect-product-info command, 220
- command line utility
 - definition, 238
- communication
 - port usage, 45
- components, 57
- connection pool
 - definition, 238
- contact list
 - definition, 238
 - rebalancing, 90, 207
- context-based authentication
 - definition, 238
- core attributes
 - definition, 238
- Credential Manager Configuration - Home page, 107
- Credential Manager Provisioning
 - definition, 238
 - license, 17
- Cryptographic Token-Key Initialization Protocol
 - client, 238
 - enabled token, 238
 - server, 238
 - toolkit, 238
- CT-KIP
 - post-installation configuration, 137
- CT-KIP. *See* Cryptographic Token-Key Initialization Protocol
- customer name
 - definition, 238
- customizing
 - e-mail notifications, 119
 - RSA Self-Service Console Help, 106
 - RSA Self-Service landing page, 106
 - token graphics, 118
 - user profiles, 112

- D**
- data encryption standard
 - definition, 239
- Data Migration utility, 220
- data store
 - definition, 239
 - supported, 44
- data transfer object
 - definition, 239
- data, user and group, 44
- database, 44, 51, 57
 - encryption, 127
- default token types, 117
- delegated administration
 - definition, 239
- delivery address
 - definition, 239
- denial of service
 - definition, 239

- deploying
 - self-service, 108
- deployment
 - definition, 239
- DES. *See* data encryption standard
- DHCP, 51
- directory server
 - secure connections, 44
 - supported directories, 44
- disabling
 - e-mail notifications, 119
- disk space, 40
- distributing tokens
 - with Credential Manager, 118
- distribution file
 - definition, 239
- distribution file password
 - definition, 239
- distribution step, 115
- distributor
 - definition, 239
- DN
 - configuring, 57
- download
 - software, 51
- DTO. *See* Data Transfer Object
- dump file
 - definition, 239
- Dumping the database, 74
- E**
- EAP
 - definition, 240
- EAP-POTP
 - client, 240
 - definition, 240
- e-mail address, 117
 - Credential Manager, 119
- e-mail notification
 - customizing for proxy servers, 120
 - definition, 240
 - enabling, 119
 - enabling and disabling, 119
 - planning, 119
- e-mail servers, 119
- e-mail template
 - customizing, 119
 - definition, 240
- emergency access
 - allowing, 120
 - definition, 240
- emergency access passcode
 - definition, 240
- emergency access tokencode
 - definition, 240
- enabling
 - e-mail notifications, 119
- enrolling in Credential Manager, 111
- enrollment paths, 112
- Enterprise Server license, 17
 - definition, 240
 - provisioning, 105
- Evaluation license
 - definition, 240
- event-based token
 - definition, 240
- excluded words dictionary
 - definition, 241
- extensible authentication protocol
 - definition, 241
- F**
- failover mode
 - definition, 241
- Firefox, 44
- firewall
 - and RADIUS, 66
 - establishing trust, 30
 - replica instance installation, 87
 - required open ports, 45
- four-pass CT-KIP
 - definition, 241
- G**
- generate
 - replica package file, 82, 223
- Global Catalog, 186
 - definition, 241
 - mapping to identity source, 185
- graded authentication
 - definition, 241
- group data, 44
- group membership
 - definition, 241
- GUI-based install, 68, 86, 97, 101
- H**
- hardware requirements, 40
- hardware token
 - definition, 241
- high-water mark
 - definition, 241

I

- identity attribute
 - definition, 241
- Identity Management Services
 - definition, 241
- identity source, 57
 - adding, 188
 - administrative, 185
 - definition, 241
 - implications for Credential Manager, 109
 - linking to realm, 192
 - runtime, 185
 - selecting Credential Manager, 113
 - supported, 44
 - user profiles, 113
- IMS. *See* Identity Management Services
- initial time-out
 - definition, 242
- installation
 - fails to complete, 196
 - logs, 197
 - migrating RADIUS with an Authentication Manager primary instance, 66
 - reinstallation cleanup script, 199
 - securing backup files, 79, 91
- instance
 - definition, 242
- instance ID
 - definition, 242
- instance name
 - definition, 242
- internal database, 44, 51, 57
 - definition, 242
- Internet Explorer, 44
- interval
 - definition, 242
- ISO, 66
- issuing
 - software tokens, 118

J

- J2EE. *See* Java 2 Enterprise Edition
- Java 2 Enterprise Edition
 - definition, 242
- Java Cryptographic Architecture
 - definition, 242
- Java Cryptographic Extensions
 - definition, 242

- Java keystore
 - definition, 242
- Java Management Extensions
 - definition, 242
- Java Messaging Service
 - definition, 242
- Java Server Pages
 - definition, 242
- JavaScript, 44
 - enabling, 48, 131
- JCA. *See* Java Cryptographic Architecture
- JCE. *See* Java Cryptographic Extensions
- JKS. *See* Java keystore
- JMS. *See* Java Messaging Service
- JMX. *See* Java Management Extensions
- JSP. *See* Java Server Pages

K

- Key Management encryption key
 - definition, 243
- Key Management services
 - definition, 243
- keystore
 - definition, 243
 - legacy compatibility, 137
 - SSL requirements, 136

L

- landing page. *See* Welcome, what would you like to do? page
- LDAP
 - Active Directory, 185
 - Active Directory forest, 185
 - and replication, 19
 - base DN, 57
 - failover, 184
 - identity source, 57
 - integration, 57
 - SSL setup, 186
 - trusted root certificate, 136
- LDAP directories
 - Active Directory Global Catalog, 186
- license
 - Base Server, 17, 237
 - Business Continuity option, 17
 - definition, 243
 - Enterprise Server, 17, 240
 - Evaluation, 240
 - RSA Credential Manager provisioning option, 17

- license category
 - definition, 243
 - license creation date
 - definition, 243
 - license deployment
 - definition, 243
 - license file
 - definition, 243
 - license file version
 - definition, 243
 - license ID
 - definition, 243
 - determining, 12
 - License Management Service
 - definition, 243
 - license.rec
 - definition, 243
 - link identity source to realm, 192
 - Linux
 - DISPLAY* environment variable, 53
 - kernel semaphore parameters, 53
 - requirements, 41
 - security parameters, 53
 - LMS. *See* License Management Service
 - Local Authentication Client
 - definition, 244
 - locked license
 - definition, 244
 - lockout policy
 - definition, 244
 - log archival
 - definition, 244
 - logging on
 - e-mail server, 119
 - logging service
 - definition, 244
 - installation logs, 197
 - system logs, 200
 - logon methods, 111
 - lower-level security domain
 - definition, 244
- M**
- Manage Secrets utility, 225
 - Manage SSL Certificate utility, 228
 - Management Information Base
 - definition, 244
 - manage-secrets command, 227
 - manage-ssl-certificate command, 232
 - master password, 51, 52
 - member user
 - definition, 244
 - member user group
 - definition, 244
 - memory requirements, 40
 - MIB. *See* Management Information Base
 - Microsoft Management Console
 - definition, 244
 - migrate-amapp command, 220
 - MMC
 - installing, 146
 - post-installation configuration, 148
 - purpose, 145
 - MMC Extension, 201
 - MMC. *See* Microsoft Management Console
 - mobile devices, 117
- N**
- namespace
 - definition, 244
 - network address translation
 - and RADIUS, 66, 85, 95
 - establishing trust, 30
 - Network Management System
 - definition, 245
 - NMS administrator
 - definition, 245
 - NMS. *See* Network Management System
 - node
 - manager, 128
 - node manager
 - troubleshooting, 201
 - node secret
 - definition, 245
- O**
- object
 - definition, 245
 - offset
 - definition, 245
 - on-demand tokencode
 - definition, 245
 - on-demand tokencode service
 - definition, 246
 - delivery methods, 117
 - requesting, 117
 - one-time tokencode
 - definition, 246
 - Operations Console
 - definition, 248

- options
 - Business Continuity, 17, 237
 - provisioning, 17
 - Short Message Service, 17
- Oracle, 51
- P**
- PAM. *See* Pluggable Authentication Module
- parent security domain, 119
- passcode
 - definition, 246
- password
 - Active Directory policy, 187
 - encrypted properties file, 225
 - internal system, 135
 - master, 51, 52, 134
 - self-service troubleshooting, 113
 - Super Admin, 51, 52, 134
- password policy
 - definition, 246
 - planning, 51, 52
- password-based encryption
 - definition, 246
- permissions
 - assigning, 32
 - definition, 246
- PINs, 113
 - troubleshooting, 113
- Pluggable Authentication Module
 - definition, 246
- policy data, 44
- port usage
 - planning, 119
- ports, 45
- ports reserved for Authentication Manager, 51, 53
- post-installation tasks
 - changing passwords, 134
 - SSL, 136
 - starting services, 128
 - stopping services, 128
- predefined roles, 115
- pre-migration checklist, 51
- primary connection pool
 - definition, 246
- primary database server
 - removing, 207, 208
- primary instance
 - backing up standalone, 125
 - definition, 246
 - removing, 205
 - securing data over the network, 127
- private key
 - definition, 246
- PRN. *See* pseudorandom number
- properties file, 224
- Protocol Data Unit
 - definition, 246
- provisioning
 - customizing token graphics, 118
 - definition, 105, 246
 - enrollment, 111
 - license, 17
 - roles, 115
- provisioning data
 - definition, 247
- proxy servers, 120, 137
- pseudorandom number
 - definition, 247
- public key
 - definition, 247
- R**
- RADIUS. *See* Remote Authentication Dial-In User Service
- read/write
 - identity sources, 109
 - user profiles, 112
- read-only
 - identity sources, 109
 - user profiles, 112
- read-only or read/write access, 109
- realm
 - creating, 21
 - definition, 247
 - identity source, 192
- Red Hat Package Manager
 - versions required, 42
- regular time-out
 - definition, 247
- reinstallation cleanup script, 199

- Remote Authentication Dial-In User Service
 - adding clients, 142
 - administrative access, 95
 - and firewalls, 95
 - and network address translation, 66, 85, 95
 - copying a RADIUS package file, 97
 - copying a RADIUS replica package file, 100
 - creating a RADIUS package file, 96
 - definition, 247
 - integration of RADIUS into version 7.1 Authentication Manager, 38
 - migrating profile names and profile assignments, 155
 - migrating RADIUS primary server on a separate machine, 96
 - migrating RADIUS with an Authentication Manager primary instance, 66
 - migrating RADIUS with an Authentication Manager replica instance, 85
 - migrating the default profile, 95, 155
 - platform requirements, 39
 - post-installation configuration, 140
 - RADIUS operating system requirements, 94
 - replication of database changes, 142
 - testing operation, 143
 - uninstall server, 208
- remote EAP
 - definition, 247
- remote post-dial
 - definition, 247
- Remote Token Key Generation Service, 137
- replacement tokens, 117
- replica instance
 - definition, 248
 - rebalancing contact lists, 90
 - synchronizing clocks, 47, 128
- replica package file
 - generate, 82, 223
 - transfer, 84
- replication
 - and LDAP, 19
- Request Approver, 115
 - definition, 248
- requests, 117
 - definition, 248
 - on-demand tokencode service, 115
- requirements
 - system, 39
- roles. *See* administrative role
- RPM. *See* Red Hat Package Manager
- RSA ACE/Server, 51
- RSA Credential Manager
 - configuring, 108
 - Credential Manager Configuration - Home page, 107
 - customizing token graphics, 118
 - definition, 248
 - described, 105
 - e-mail address, 119
 - planning, 113, 117
 - self-service troubleshooting, 113
 - Welcome, what would you like to do? page, 106
- RSA EAP
 - definition, 248
- RSA Operations Console
 - definition, 248
- RSA Protected OTP
 - definition, 248
- RSA Security Console
 - adding to trusted sites, 49, 132
 - definition, 248
 - description, 31, 57
 - fails to start, 200
 - identity source, 57
 - MMC Extension configuration, 148
 - starting service, 129
 - stopping service, 129
 - supported browsers, 44
- RSA Self-Service Console, 106
 - customizing Help, 106
 - definition, 248
 - impact of read-only or read/write access, 109
 - logon methods, 111
 - replacement tokens, 117
 - tasks, 109
 - troubleshooting, 113
- runtime
 - definition, 248
- runtime changes, 18
- runtime command
 - definition, 248
- runtime identity source, 185
 - definition, 248

- S**
- scope
 - assigning, 33
 - definition, 249
 - definition and concept, 33
 - exceptions for Credential Manager, 116
 - sddumpsrv utility, 215
 - SDTID file format, 118
 - secondary connection pool
 - definition, 249
 - Secure Sockets Layer
 - definition, 249
 - Secure Sockets Layer. *See* SSL
 - Security Console, 57
 - adding to trusted sites, 49, 132
 - definition, 248
 - description, 31, 57
 - fails to start, 200
 - identity source, 31, 57
 - MMC Extension configuration, 148
 - starting service, 129
 - stopping service, 129
 - supported browsers, 44
 - security domain
 - definition, 249
 - for Credential Manager, 112
 - security domains, 21, 22
 - security questions, 114
 - definition, 249
 - selecting
 - default token types, 117
 - identity sources, 113
 - on-demand tokencode service, 117
 - tokens for Credential Manager, 117
 - user groups for Credential Manager, 116
 - self-service
 - definition, 105, 249
 - tasks, 108
 - troubleshooting, 114
 - Self-Service Console
 - definition, 248
 - Self-Service Console. *See* RSA Self-Service Console
 - self-service requests
 - definition, 249
 - self-service troubleshooting, 114
 - self-service troubleshooting policy
 - definition, 249
 - server certificate and key, 70, 88
 - services
 - defined, 45
 - protocols used, 45
 - services, fail to start, 200
 - session
 - definition, 249
 - session policy
 - definition, 249
 - shipping address
 - definition, 250
 - Short Message Service
 - definition, 250
 - Short Message Service (SMS). *See* on-demand tokencode service
 - Simple Mail Transfer Protocol
 - definition, 250
 - Simple Mail Transfer Protocol (SMTP), 117, 119
 - Simple Network Management Protocol
 - definition, 250
 - single sign-on
 - definition, 250
 - SMS
 - definition, 250
 - license, 17
 - SMTP
 - definition, 250
 - SMTP. *See* Simple Mail Transfer Protocol
 - snap-in
 - definition, 250
 - SNMP agent
 - definition, 250
 - SNMP trap
 - definition, 250
 - SNMP. *See* Simple Network Management Protocol
 - software tokens
 - issuing, 118
 - Solaris
 - requirements, 43
 - SSL
 - LDAP, 186
 - manage certificate, 228
 - post-installation tasks, 136
 - SSL LDAP, 44
 - SSL. *See* Secure Sockets Layer
 - SSO. *See* single sign-on
 - starting RSA Authentication Manager services, 128

- starting services
 - on Solaris and Linux, 130
 - on Windows, 129
 - stopping RSA Authentication Manager services, 128
 - stopping services
 - on Solaris and Linux, 130
 - on Windows, 129
 - Sun Java System Directory Server, 44
 - Super Admin
 - definition, 251
 - planning password, 51, 52
 - supported browsers, 44
 - symmetric key
 - definition, 251
 - system
 - architecture, 57
 - components, 57
 - fingerprint, 224
 - logs, 200
 - required packages, 42
 - system event
 - definition, 251
 - system log
 - definition, 251
 - system requirements
 - Linux, 41
 - Microsoft Windows, 40
 - Solaris, 43
 - systemfields.properties, 51, 52, 225
- T**
- TACACS+. *See* Terminal Access Controller Access Control System+
 - TCP ports, 51, 53
 - temporary directory for installation logs, 51
 - temporary fixed tokencode
 - definition, 251
 - time-based token
 - definition, 251
 - Token Distributor, 115
 - definition, 251
 - token graphics, 118
 - token provisioning
 - definition, 251
 - tokencode
 - definition, 251
- tokens
 - default, 117
 - definition, 251
 - distributing, 118
 - lost or broken, 120
 - replacement, 117
 - temporarily unavailable, 120
 - top-level security domain
 - definition, 252
 - trace log, 200
 - definition, 252
 - transfer
 - replica package file, 84
 - troubleshooting, 113, 114
 - accessing installation files on a network, 195
 - Collect Product Information utility, 219
 - message indicating Node Manager Service is not started, 201
 - MMC Extension does not start, 201
 - RSA Security Console fails to start, 200
 - Security Console times out when searching for users, 202
 - server fails to start, 200
 - starting node manager, 201
 - unsuccessful authentication between RADIUS and Authentication Manager, 202
 - unsuccessful end-to-end authentication on RADIUS, 202
 - unsuccessful installation, 197
 - unsuccessful installation or removal, 196
 - trust package
 - definition, 252
 - trusted realm
 - definition, 252
 - trusted realms
 - using network address translation, 30
 - two-factor authentication
 - definition, 252
 - two-pass CT-KIP
 - definition, 252
- U**
- UDP ports, 51, 53
 - UDP. *See* User Datagram Protocol
 - uninstall
 - primary database server, 207, 208
 - RADIUS server, 208
 - user and group data, 44

- User Datagram Protocol
 - definition, 252
 - user groups
 - definition, 252
 - membership, 116
 - User ID
 - definition, 252
 - user profiles, 113
 - user requests
 - types of, 115
 - users
 - definition, 252
 - users and groups
 - accessing from LDAP directory, 57
 - utilities
 - sddumpsrv, 215
 - utility
 - Collect Product Information, 219
 - Data Migration, 220
 - Dumping the Database, 215
 - Manage Secrets, 225
 - Manage SSL Certificate, 228
- V**
- version number, determining, 12
- W**
- Welcome, what would you like to do?
 - page, 106
 - Windows registry settings, 51, 53
 - Windows requirements, 40
 - workflow
 - definition, 252
 - workflow definitions, 115
 - workflow participant
 - definition, 253
 - workflows, 115
- Z**
- ZIP file format, 118