RSA Authentication Manager 7.1 Installation and Configuration Guide

The Security Division of EMC

Contact Information

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

Trademarks

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

License agreement

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

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

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

Third-party licenses

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

© 2007-2008 RSA Security Inc. All rights reserved.
First printing: April 2008

Contents

Preface 9
- About This Guide 9
- RSA Authentication Manager Documentation 9
- Related Documentation 10
- Getting Support and Service 10
  - Before You Call Customer Support 11

Chapter 1: Preparing for Installation 13
- Hardware and Operating System Requirements 13
  - Windows System Requirements 14
  - Linux System Requirements 15
  - Solaris System Requirements 17
- Supported Data Stores 18
  - Internal Database 18
  - Identity Sources 18
- Supported Browsers 19
- Port Usage 19
- Supported RSA Authentication Agents 22
- Licensing 22
- Maintaining Accurate System Time Settings 22
- RSA Authentication Manager Components 23
- Installation Types 24
  - Primary Instance 25
  - Replica Instance 26
  - Server Node 27
  - Database Only 29
  - Documentation Only 29
  - RADIUS Only 29
- Pre-Installation Tasks 30
  - Pre-Installation Checklist for Windows 30
  - Pre-Installation Checklist for Solaris 31
  - Pre-Installation Checklist for Linux 33

Chapter 2: Identifying the Installation Process for Your Deployment Model 35
- Planning Your Deployment 35
- Deployment Process 35
- Deployment Examples 37
  - Small, Single-Site Deployment 37
  - Medium, Single-Site Deployment 38
  - Large, Multisite Single-Realm Deployment 40
  - Large, Multisite Trusted Realm Deployment 41

Chapter 3: Installing an RSA Authentication Manager Primary Instance 43
Preparing to Install a Primary Instance 43
Synchronizing Clocks 44
Mounting the Media on Linux 44
Mounting an ISO Image 44
Performing an Installation 45
Securing Backup Files 49

Chapter 4: Installing a Replica Instance 51
Preparing to Install a Replica Instance 51
Generating a Replica Package File 54
Transferring the Replica Package File 55
Copying the RSA RADIUS Replica Package File 56
Performing an Installation 56
Rebalancing Contact Lists 60
Securing Backup Files 60

Chapter 5: Installing a Server Node 61
Preparing to Install a Server Node 61
Creating a Node Package File 62
Transferring the Node Package File 62
Performing an Installation 63
Rebalancing Contact Lists 65
Securing Backup Files 65
Verifying Server Node Function 66

Chapter 6: Installing the RSA Authentication Manager Database on a Separate Machine 67
Preparing to Install the Database on a Separate Machine 68
Performing a Standalone Database Installation 69
Generating a Database Package File 71
Transferring the Database Package File 72
Verifying That the Database Installed Successfully 72

Chapter 7: Installing RSA RADIUS on a Separate Machine 73
Preparing to Install RSA RADIUS on a Separate Machine 73
RSA RADIUS and Firewalls 74
RSA RADIUS Access Planning 74
Pre-Installation Tasks 74
Creating an RSA RADIUS Package File 74
Copying the RSA RADIUS Package File 75
Installing RSA RADIUS 76
Installing an RSA RADIUS Primary Server 76
Installing an RSA RADIUS Replica Server 78

Chapter 8: Upgrading from RSA Authentication Manager 7.0 83
Upgrading a Primary Instance........ 84
Preparing to Upgrade a Primary Instance 84
Performing an Upgrade on a Primary Instance........ 90
Migrating User Data on a Primary Instance 90
Upgrading a Replica Instance 95
Preparing to Upgrade a Replica Instance........ 96
Performing an Upgrade on a Replica Instance 100
Migrating User Data on a Replica Instance 101
Upgrading a Server Node........ 102
Verifying the Upgrade 103

Chapter 9: Performing Post-Installation Tasks........ 105
Backing Up a Standalone Primary Instance........ 105
When To Perform a Backup 105
Backing Up a Standalone Primary Instance on Windows 106
Backing Up a Standalone Primary Instance on Linux and Solaris 107
Securing the Connection Between the Primary Instance and Replica Instances 107
Synchronizing Clocks 107
Starting and Stopping RSA Authentication Manager Services 108
Starting and Stopping RSA Authentication Manager Services on Windows 108
Starting and Stopping RSA Authentication Manager Services on Solaris and Linux 109
Configuring Your Browser to Support the RSA Authentication Manager Consoles 110
Enabling JavaScript 110
Adding the RSA Security Console to Trusted Sites 111
Logging On to the Consoles 111
Administering System Security 112
Managing Passwords and Keys 112
Managing Certificates and Keystores for SSL 115
Importing LDAP Certificates........118
Legacy Compatibility Keystore 118
Configuring Optional Proxy Servers for Remote Token-Key Generation 119
Adding a Proxy Server to Create Secure URLs........119
Configuring a Proxy Server for CT-KIP Failover 119
Configuring an Optional Proxy Server for Remote RSA Self-Service Console Access 120
Adding a Proxy Server for Secure RSA Self-Service Console Access 120
Configuring a Proxy Server for RSA Self-Service Console Failover 121
Integrating the RSA RADIUS Server into the Existing Deployment........ 122
Modifying the RADIUS Configuration Files 122
Using the RSA Security Console to Replicate Changes........ 122
Adding Clients to the RADIUS Server and Editing Clients........ 122
Testing RSA RADIUS Operation 123

Chapter 10: Integrating an LDAP Directory 125
- Overview of LDAP Directory Integration 125
  - Integrating an LDAP Identity Source 126
  - Failover Directory Servers 128
  - Mapping Identity Attributes for Active Directory 128
  - Integrating Active Directory Forest Identity Sources 129
- Preparing for LDAP Integration 130
  - Setting Up SSL for LDAP 130
  - Password Policy Considerations 131
  - Supporting Groups 131
  - Active Directory Forest Considerations 131
- Adding an Identity Source 132
- Linking an Identity Source to a Realm 136
- Verifying the LDAP Identity Source 137

Chapter 11: Installing the RSA Authentication Manager MMC Extension 139
- MMC Extension Overview 139
- System Requirements and Prerequisite 139
- Installation Process 140
  - Installing the MMC Extension for Local Access 140
  - Installing the MMC Extension for Remote Access 140
- Post-Installation 142
  - Configuring Internet Explorer Security Settings 142
  - Starting the Active Directory User and Computer Management Console 143

Chapter 12: Removing RSA Authentication Manager 145
- Removing RSA Authentication Manager Servers 145
- Removing a Server Node 145
- Removing a Replica Database Server 147
  - Manual Cleanup for Unsuccessful Removal 148
- Rebalancing Contact Lists 148
- Removing a Primary Database Server 148
- Removing an RSA RADIUS Server 149
- Removing a Standalone Database Server 149

Chapter 13: Troubleshooting 151
- Accessing Installation Files On a Network 151
- Unsuccessful Installation or Removal 152
  - Viewing Installation Logs 152
  - Unsuccessful Installation 152
  - Unsuccessful Removal 154
  - Reinstalling RSA Authentication Manager Components 154
  - Cleanup Script for Reinstallation (Windows Only) 155
  - Cleanup for Linux Systems 155
  - Obscured Error Messages 155

Server Does Not Start 155
RADIUS Server Does Not Start After Installation on a Windows Platform 156
RSA Security Console Does Not Start 156
Using the Collect Product Information Utility 156
MMC Extension Does Not Start 157
Multicast Network Communication Fails 157
Message Indicates Node Manager Service Not Started 157
Test Authentication Between RSA RADIUS and RSA Authentication Manager Unsuccessful 158
Unsuccessful End-to-End Authentication on RSA RADIUS 158
The RSA Security Console Times Out When Searching for Users 158
Unable to Receive Multicast Packets Sent to Self 159

Appendix A: Deployment Checklist 161
Pre-Installation 161
Installation 162
Identity Source Configuration 163
Administrative Configuration 164
Administrative Configuration for Self-Service and Provisioning 166
Post-Installation 170

Appendix B: Command Line Utilities 171
Overview 171
Collect Product Information Utility 173
Using the Collect Product Information Utility 174
Options for collect-product-info 174
Data Migration Utility 175
Using the Data Migration Utility 175
Options for migrate-amapp 176
Generate RADIUS Package Utility 178
Using the Generate RADIUS Package Utility 178
Options for gen-radius-pkg 178
Manage Nodes Utility 179
Using the Manage Nodes Utility 179
Options for manage-nodes 179
Manage Secrets Utility 180
Using the Manage Secrets Utility 180
Options for manage-secrets 182
Manage SSL Certificate Utility 183
Using the Manage SSL Certificate Utility 183
Options for manage-ssl-certificate 186

Multicast Network Test Utility 187
    Utility Messages 187
    Examples.. 188
    Using the Multicast Network Test Utility.. 188
    Options for test-multicast.. 189
Setup Replication Utility.. 190
    Using the Setup Replication Utility 190
    Options for setup-replication 190

Glossary 193

Index 213

Preface

About This Guide

Make sure that you have a basic understanding of your server platform, operating system version, and system peripherals. This guide is intended for network and security administrators who are responsible for installing and managing the RSA Authentication Manager software.

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** > **Manage Existing**, and then clicking **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

Preparing for Installation

- Hardware and Operating System Requirements
- RSA Authentication Manager Components
- Installation Types
- Pre-Installation Tasks

Hardware and Operating System Requirements

Make sure 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.

For CPU speed, memory, and disk speed, RSA recommends that the database server be significantly more powerful than every other machine in your Authentication Manager deployment.

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.

Important: Be sure that your UNIX and Windows servers are known by their fully qualified domain names. If you are installing the Authentication Manager database on a separate machine, configure your DNS server to resolve by both fully qualified name and short name.

Windows System Requirements

Operating System	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 and Linux systems.
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 4.0-1 ES (32-bit) Red Hat Enterprise Linux 4.0-1 ES (64-bit) Red Hat Enterprise Linux 4.0-1 AS (32-bit) Red Hat Enterprise Linux 4.0-1 AS (64-bit) **Note:** RADIUS is not supported on 64-bit Windows and 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	2 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-open1dap 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, rpm -q *package name*.
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	UltraSPARC 1.5 GHz, or equivalent For improved performance, use Sun 6 or 8 core UltraSPARC T1 servers. **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.
Disk Space	**RSA Authentication Manager**: 60 GB free space recommended 20 GB free space minimum **RSA RADIUS:** Add 650 MB of free space
Memory Requirements	**RSA Authentication Manager:** 4 GB **RSA RADIUS:** Add 512 MB
Swap Space	4 GB
Packages	SUNWarc SUNWbtool SUNWhea SUNWlibm SUNWlibms SUNWsprot SUNWtoo SUNWi1of SUNWi1cs SUNWi15cs SUNWxwfnt

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 may 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, SP 3
- Microsoft Active Directory 2003, SP 2

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 Active Directory 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 over the wire 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.

For instructions on enabling JavaScript, see "Logging On to the Consoles" on page 111.

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.

Port Number	Protocol	Service	Description
1645	UDP	RADIUS authentication (legacy port)	Used for authentication requests from RADIUS clients.
1812	UDP	RADIUS authentication (standard port)	Used for RADIUS authentication and accounting.
1646	UDP	RADIUS accounting (legacy port)	Used for requests for accounting data.
1813	TCP	RADIUS (standard port)	Used for RADIUS administration and replication.
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.

Port Number	Protocol	Service	Description
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.
7006	TCP	RSA Authentication Manager cluster administration channel	Internal use only.
7008	TCP	RSA Authentication Manager cluster 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.

Supported RSA Authentication Agents

You install RSA Authentication Agents on the resources that you want to protect, such as local computers, terminal servers, and web servers.

Authentication agents receive authentication requests and forward them to Authentication Manager through a secure channel. Based on the response from Authentication Manager, agents either allow the user to log on or deny the user access.

To download compatible Authentication Agents from the Authentication Agent software page, go to **https://www.rsa.com/node.asp?id=1174**.

Licensing

Before you install Authentication Manager, make sure that you have a valid Authentication Manager license close at hand. RSA provides the license files separately from your RSA Authentication Manager 7.1 DVD or download kit.

The license allows you access to certain functionality and limits the number of users that can be registered. The license file is accompanied by a server key and certificate that are used to verify (authenticate) the identity of the server.

Maintaining Accurate System Time Settings

Authentication Manager relies on standard time settings known as Coordinated Universal Time (UTC). The time, date, and time zone settings on computers running Authentication Manager must always be correct in relation to UTC.

Make sure that the time on the computer on which you are installing Authentication Manager is set to the local time and corresponds to the UTC. For example, if UTC is 11:43 a.m. and Authentication Manager is installed on a computer in the Eastern Standard Time Zone in the United States, make sure that the computer clock is set to 6:43 a.m. This differs during Daylight Saving Time.

To get the correct UTC, go to **www.time.gov**.

Note: If you employ an NTP service, enable it on the primary instance database server only. This database server typically maintains the replica instance time synchronization automatically.

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 for setting up provisioning.

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

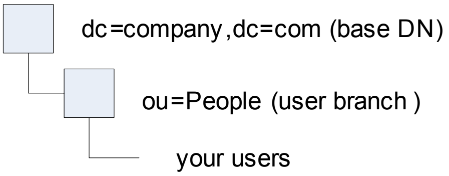
If it is part of your deployment plan, configure Authentication Manager to use your organization's LDAP directory to access your user data. Authentication Manager modifies certain existing user data fields in the LDAP directory only if you allow it. Those data fields include a user's first and last name, 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 Chapter 10, "Integrating an LDAP Directory."

The following examples describe how to specify the base DN and user branch to include all users for two different LDAP configurations.

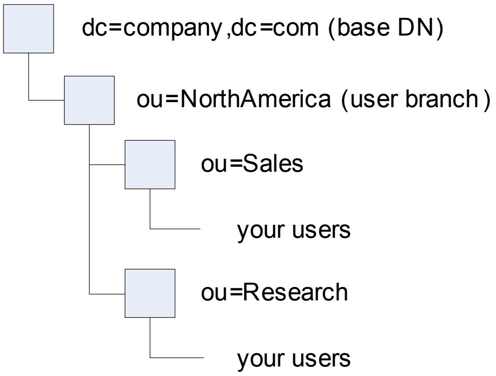
Example 1:

All users reside in one container in the LDAP directory. Specify **dc=company,dc=com** as the base DN. Specify the container **ou=People** as the user branch.



Example 2:

Users reside in multiple containers within a common container. Specify **dc=company,dc=com** as the base DN. Specify the container **ou=NorthAmerica** as the user branch.



This set of Authentication Manager components alone is not sufficient for authentication operations. Your system must include authentication agents and other front-end components that are typically configured following the installation of Authentication Manager. See agent documentation at **https://knowledge.rsasecurity.com**.

Installation Types

At installation time, you must select an installation type. The installer creates differently configured combinations of Authentication Manager components on your system depending on which type of installation you choose: primary instance, replica instance, server node, database only, or RADIUS only. The installer also provides an option to install Authentication Manager documentation only.

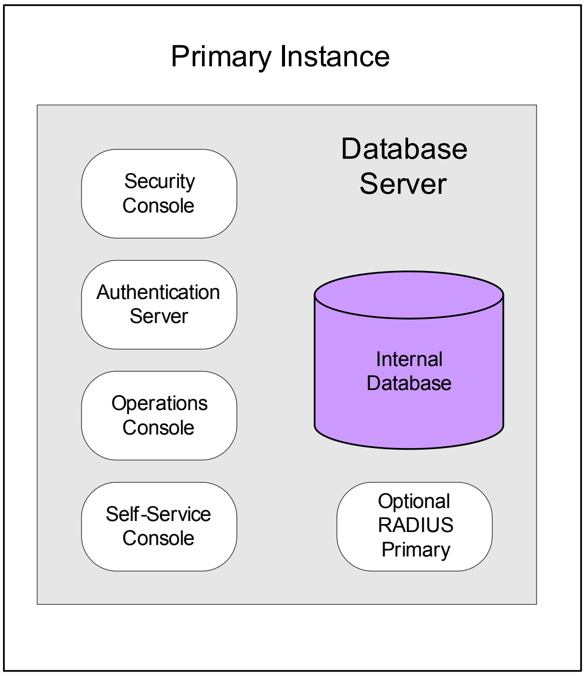
An instance is a single database server, or a database server and one or more server nodes, acting as a single cohesive processing unit.

Primary Instance

The primary instance serves as the central point for administration and data storage in the system. You can add additional server nodes to a primary instance to improve performance. Also, you can connect your primary instance with replica instances that provide redundancy, failover, and improved performance. (You can install the primary instance with or without RSA RADIUS on the same machine. For more information, see "RADIUS Only" on page 29.)

Note: You must have an Enterprise Server license to install server nodes. Server nodes are not available with a Base Server license.

The following figure shows a primary instance with no additional server nodes. The components installed on your database server machine by the installation type "Authentication Manager Primary Instance" are shown on the gray background.

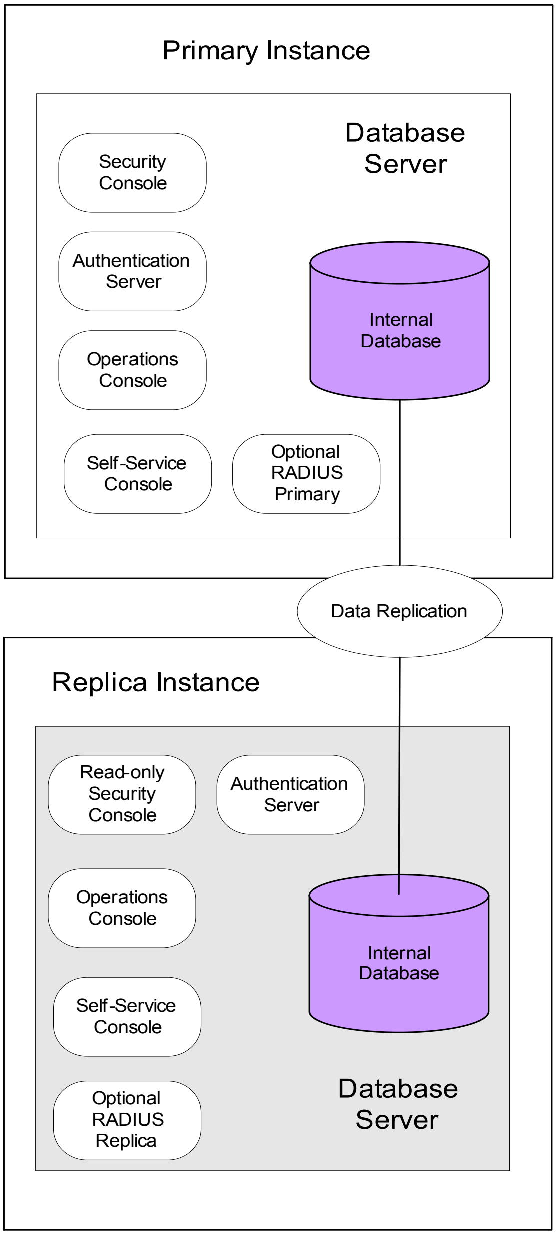

Primary Instance
Database Server
Security Console
Authentication Server
Operations Console
Self-Service Console
Internal Database
Optional RADIUS Primary

The installation procedure for this primary instance is described in Chapter 3, "Installing an RSA Authentication Manager Primary Instance."

Replica Instance

A replica instance provides redundancy for geographical distribution, failover, and improved performance. A replica instance is dependent on a primary instance and cannot perform administrative functions independently. It can, however, connect independently to its own server nodes to provide runtime authentication. (You can install the replica instance with or without RSA RADIUS on the same machine. For more information, see "RADIUS Only" on page 29.)

The following figure shows a replica instance together with the primary instance on which it depends. The components installed on your database server machine by the installation type "Authentication Manager Replica Instance" are shown on the gray background.


Primary Instance
Database Server
Security Console
Authentication Server
Operations Console
Self-Service Console
Internal Database
Optional RADIUS Primary
Data Replication
Replica Instance
Read-only Security Console
Authentication Server
Operations Console
Self-Service Console
Optional RADIUS Replica
Internal Database
Database Server

The replica instance installation creates the same components on the database server as the primary instance installation, but it configures them differently:

- The replica database server is configured to listen for administrative data replication from the primary database server. It logs its runtime operations to the primary database server.
- The Security Console installed with the replica instance is limited to read-only operations.

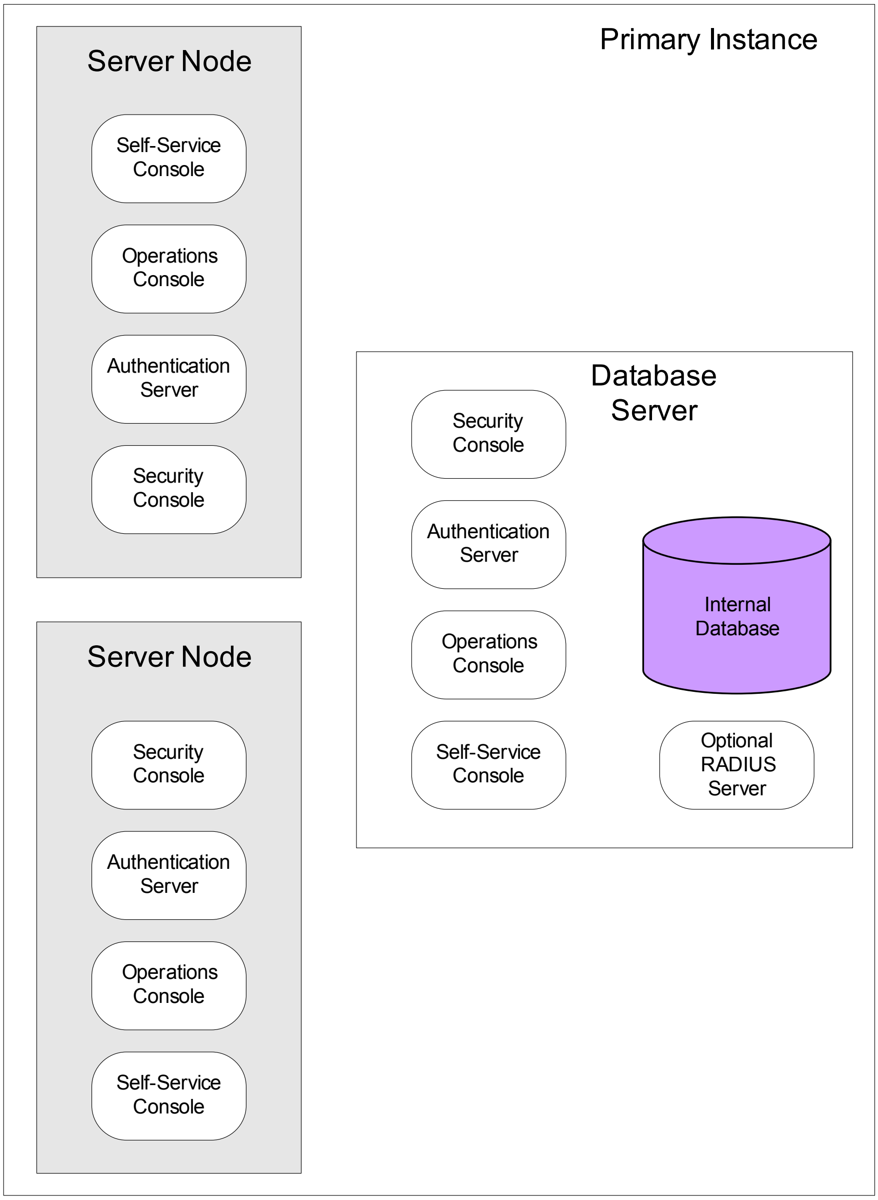
To link a replica instance to a primary instance, you must first install the primary instance and then gather data from it for use in the replica instance installation. This process and all other replica instance installation details are described in Chapter 4, "Installing a Replica Instance."

Server Node

A server node is a host that depends on a primary or replica database server. It handles operations in the same LAN subnet as the database server and provides improved agent authentication performance and failover.

Note: You must have an Enterprise Server license to install server nodes. Server nodes are not available with a Base Server license.

The following figure shows a primary instance with two additional server nodes. You can add server nodes to a replica instance in the same way. The components installed on your server node machines by the installation type “Authentication Manager Server Node” are shown on the gray background.


Server Node
Self-Service Console
Operations Console
Authentication Server
Security Console
Primary Instance
Database Server
Security Console
Authentication Server
Operations Console
Self-Service Console
Internal Database
Optional RADIUS Server
Server Node
Security Console
Authentication Server
Operations Console
Self-Service Console

The Security Consoles shown on the server nodes receive requests distributed by the proxy service on the primary database server. In a typical configuration, browser access to the Security Console is directed to this proxy service at port 7004 on the primary instance database server.

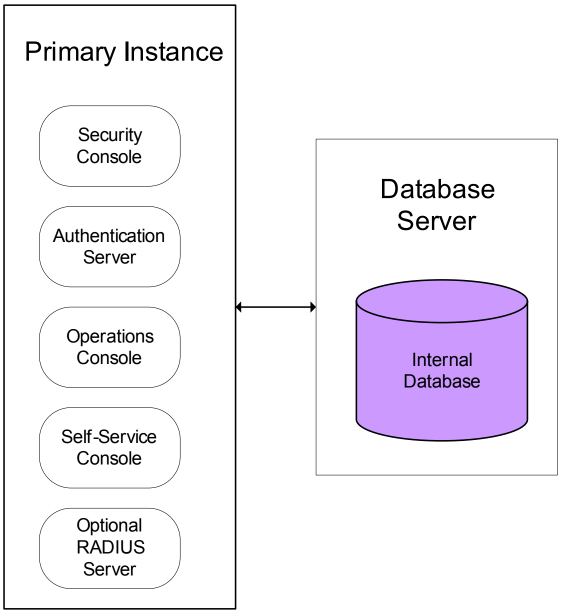
To link a server node to a primary or replica database server, you must first install the primary or replica instance and then gather data from it for use in the server node installation. This process and all other server node installation details are described in Chapter 5, “Installing a Server Node.”

Database Only

It is possible to install the RSA Authentication Manager 7.1 database on a separate machine dedicated to handling all of the database requests.

The process of installing a separate database requires that you install the database first, then install the associated primary or replica instance.

The following figure shows a primary instance with a standalone database. The RSA Authentication Manager 7.1 database is installed on a separate machine that functions as the database server.



Documentation Only

The installer provides an option to install only Authentication Manager documentation and *Release Notes*.

RADIUS Only

RSA RADIUS is an optional feature that is available as part of RSA Authentication Manager 7.1. RADIUS can be installed either along with Authentication Manager on the same machine or separately on a standalone machine. To install RADIUS on a standalone machine, select the **RADIUS Only** installation type.

RADIUS provides both primary and replica server types. You must install a RADIUS primary in your deployment before you can install a RADIUS replica. If you do not want to use RADIUS, simply do not select it as an optional feature during the Authentication Manager installation process.

Because RSA RADIUS is integrated with RSA Authentication Manager 7.1, you can administer RADIUS using the Security Console and the Operations Console without the need for a separate user interface. Use the Security Console to perform many of the RADIUS routine administrative tasks that are done on a regular basis. Use the Operations Console to carry out less frequently performed RADIUS tasks, such as modifying the RADIUS initialization (INI) and dictionary (DCT) files.

Pre-Installation Tasks

This section describes important pre-installation tasks required to prepare your system for installation. Carefully review the pre-installation checklist for your platform.

- "Pre-Installation Checklist for Windows" on page 30
- "Pre-Installation Checklist for Solaris" on page 31
- "Pre-Installation Checklist for Linux" on page 33

Before installing Authentication Manager, review the *Release Notes*, which contain important configuration and installation information. You must perform these pre-installation tasks prior to proceeding with the installation.

Pre-Installation Checklist for Windows

You must have:

☐ A machine that meets all of the hardware, disk space, memory, and platform requirements described in "Windows System Requirements" on page 14.

☐ 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 6 alphabetic characters and 1 non-alphanumeric character. "@" and "~" are excluded. This case-sensitive default administrator account 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. See "Managing Passwords and Keys" on page 112.

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 RADIUS or Oracle. An existing RADIUS server or 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 19 are available.

☐ Configure your system to allow multicast.

Multicast is used by version 7.1 for certain communications between server nodes, and within a single server node. If you have a firewall running on the machine on which you are installing, you must allow the IGMP protocol to communicate through your firewall, and open ports 7000 to 8000. Perform these tasks only on the firewall running on the installation machine. You do not need to open these ports on any firewall that protects your network external threats.

☐ Perform a forward and reverse lookup on the fully qualified hostname and the short hostname (hostname without domain) where you will install Authentication Manager. Make sure that the machine maps to one hostname. If it maps to more than one hostname, you must modify your DNS server configuration settings to have it map to just one.

☐ Back up your Windows registry settings.

Pre-Installation Checklist for Solaris

You must have:

☐ A machine that meets all of the hardware, disk space, memory, and platform requirements described in "Solaris System Requirements" on page 17.

☐ Local administrator privileges on the machine. Run the installer as the 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 will result in installation or server startup problems.

☐ A password between 8 and 32 characters including at least 6 alphabetic characters and 1 non-alphanumeric character. "@" and "~" are excluded. This case-sensitive default administrator account 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. See "Managing Passwords and Keys" on page 112.

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 RADIUS or Oracle. An existing RADIUS server or 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 19 are available.

☐ Configure your system to allow multicast.

Multicast is used by version 7.1 for certain communications between server nodes, and within a single server node. If you have a firewall running on the machine on which you are installing, you must allow the IGMP protocol to communicate through your firewall, and open ports 7000 to 8000. Perform these tasks only on the firewall running on the installation machine. You do not need to open these ports on any firewall that protects your network from external threats.

☐ Perform a forward and reverse lookup on the fully qualified hostname and the short hostname (hostname without domain) where you will install Authentication Manager. Make sure that the machine maps to one hostname. If it maps to more than one hostname, you must modify your DNS server configuration settings to have it map to just one.

☐ 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.

1. At a command prompt, type:

```
# id -p username // to verify the project id uid=uid
gid=gid projid=projid

# prctl -n project.max-shm-memory -i project projid

# prctl -n project.max-sem-ids -i project projid
```

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

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

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

```
# prctl -n project.max-sem-ids -v 256 -r -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.

Pre-Installation Checklist for Linux

You must have:

☐ A machine that meets all of the hardware, disk space, memory, and platform requirements described in "Linux System Requirements" on page 15.

☐ Local administrator privileges on the machine. Run the installer as the 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 will result in installation or server startup problems.

☐ A password between 8 and 32 characters including at least 6 alphabetic characters and 1 non-alphanumeric character. "@" and "~" are excluded. This case-sensitive default administrator account 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. See "Managing Passwords and Keys" on page 112.

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 RADIUS or Oracle. An existing RADIUS server or 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 19 are available.

☐ Configure your system to allow multicast.

Multicast is used by version 7.1 for certain communications between server nodes, and within a single server node. If you have a firewall running on the machine on which you are installing, you must allow the IGMP protocol to communicate through your firewall, and open ports 7000 to 8000. Perform these tasks only on the firewall running on the installation machine. You do not need to open these ports on any firewall that protects your network from external threats.

☐ Perform a forward and reverse lookup on the fully qualified hostname and the short hostname (hostname without domain) where you will install Authentication Manager. Make sure that the machine maps to one hostname. If it maps to more than one hostname, you must modify your DNS server configuration settings to have it map to just one.

☐ 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

2

Identifying the Installation Process for Your Deployment Model

- Planning Your Deployment
- Deployment Process
- Deployment Examples

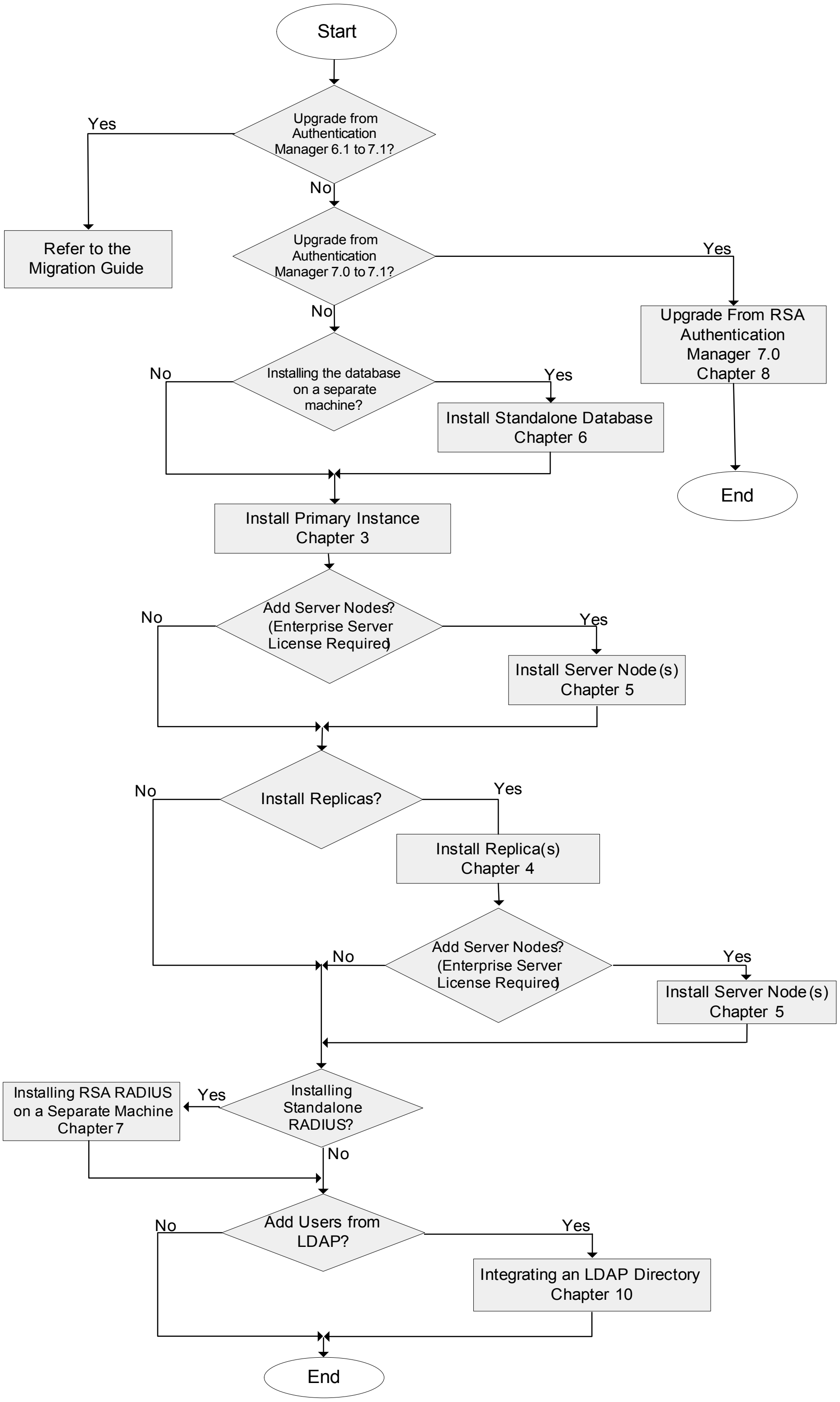
Planning Your Deployment

Before installing any Authentication Manager component, make sure that you know the details of your overall deployment. RSA strongly recommends that you read the *Planning Guide* and complete the installation checklist before beginning your installation. For a copy of the installation checklist, see Appendix A, "Deployment Checklist."

Deployment Process

Make sure that you understand the decision points and tasks required by the Authentication Manager deployment process. Depending on your needs, your deployment may require multiple replica instance or server node installation tasks. The following figure is only a general guide.

Note: You must have an Enterprise Server license if you need to install more than one replica instance.


Start
Upgrade from Authentication Manager 6.1 to 7.1?
Yes
Refer to the Migration Guide
No
Upgrade from Authentication Manager 7.0 to 7.1?
Yes
Upgrade From RSA Authentication Manager 7.0 Chapter 8
End
No
Installing the database on a separate machine?
No
Yes
Install Standalone Database Chapter 6
Install Primary Instance Chapter 3
Add Server Nodes? (Enterprise Server License Required)
No
Yes
Install Server Node (s) Chapter 5
Install Replicas?
No
Yes
Install Replica(s) Chapter 4
Add Server Nodes? (Enterprise Server License Required)
No
Yes
Install Server Node (s) Chapter 5
Installing Standalone RADIUS?
Yes
Installing RSA RADIUS on a Separate Machine Chapter 7
No
Add Users from LDAP?
No
Yes
Integrating an LDAP Directory Chapter 10
End

Deployment Examples

Review the following deployment examples, choose the deployment that best fits your company's requirements, and refer to the related sections.

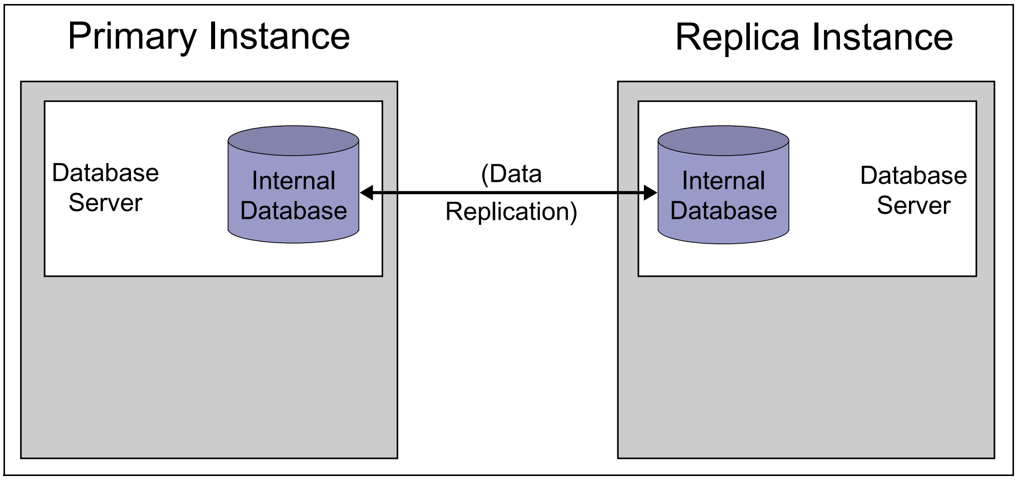
The examples in the following sections provide a high-level view of the steps required to install different types of deployments. Your specific deployment may combine aspects of more than one example.

- Small, Single-Site Deployment
- Medium, Single-Site Deployment
- Large, Multisite Single-Realm Deployment
- Large, Multisite Trusted Realm Deployment

Note: These examples are based on the detailed planning scenarios described in the *Planning Guide*.

Small, Single-Site Deployment

This deployment example illustrates the installation of a primary instance with a replica instance for failover.

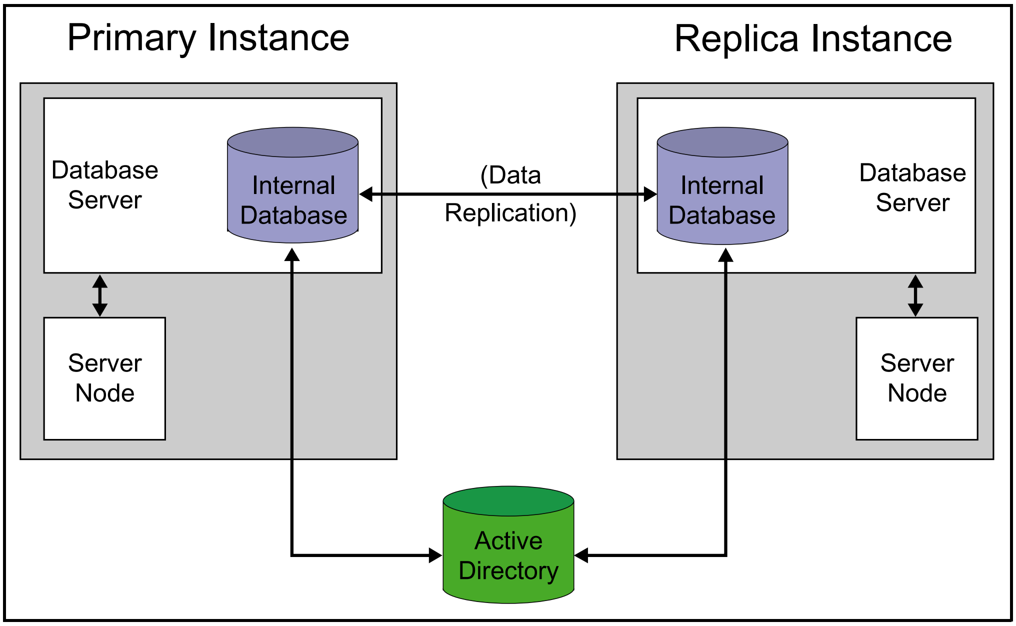


Task	See
1. Verify that all Authentication Manager machines meet the system requirements.	Chapter 1, "Preparing for Installation"
2. Install the primary instance. Be sure to secure backup files, and verify that the installation was successful by performing a test authentication after completing the installation.	Chapter 3, "Installing an RSA Authentication Manager Primary Instance"

Task	See
3. Install the replica instance. Be sure to secure backup files, and verify that the installation was successful by performing a test authentication after completing the installation.	Chapter 4, "Installing a Replica Instance"
4. Perform post-installation tasks to prepare the RSA Security Console for administration.	Chapter 9, "Performing Post-Installation Tasks"

Medium, Single-Site Deployment

This deployment example illustrates installing a primary instance with an additional server node and LDAP integration, and then a replica instance with an additional server node for failover.

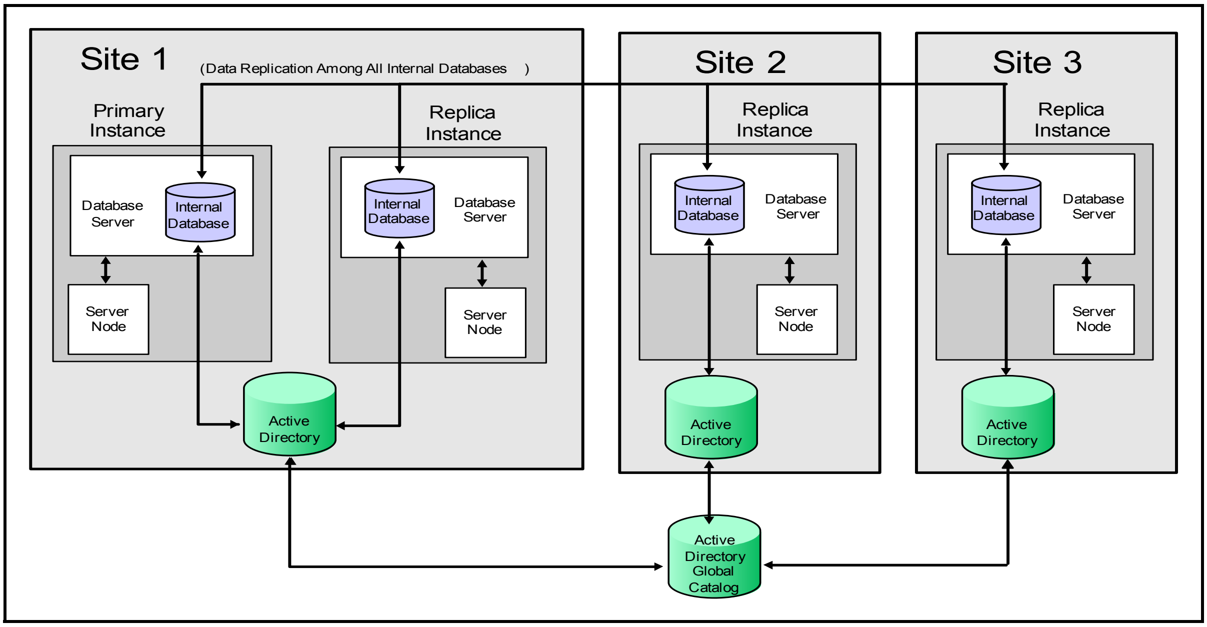

Primary Instance
Replica Instance
Database Server
Internal Database
(Data Replication)
Internal Database
Database Server
Server Node
Server Node
Active Directory

Task	See
1. Verify that all Authentication Manager machines meet the system requirements.	Chapter 1, "Preparing for Installation"
2. Install the primary instance. Be sure to secure backup files, and verify that the installation was successful by performing a test authentication after completing the installation.	Chapter 3, "Installing an RSA Authentication Manager Primary Instance"

Task	See
3. Install a server node. Be sure to secure backup files, and verify that the installation was successful by performing a test authentication after completing the installation. **Note:** Repeat this process for each server node that you want to install.	Chapter 5, "Installing a Server Node"
4. Install the replica instance. Be sure to secure backup files, and verify that the installation was successful by performing a test authentication after completing the installation.	Chapter 4, "Installing a Replica Instance"
5. Install a server node on the replica instance. Be sure to secure backup files, and verify that the installation was successful by performing a test authentication after completing the installation. **Note:** Repeat this process for each server node that you want to install.	Chapter 5, "Installing a Server Node"
6. Perform post-installation tasks to prepare the Security Console for administration.	Chapter 9, "Performing Post-Installation Tasks"
7. Integrate your existing LDAP directory as the authoritative user and group identity source.	Chapter 10, "Integrating an LDAP Directory"

Large, Multisite Single-Realm Deployment

This deployment example extends the medium single-site deployment by adding replica instances at additional sites as well as a heterogeneous LDAP environment that includes Microsoft Active Directory.

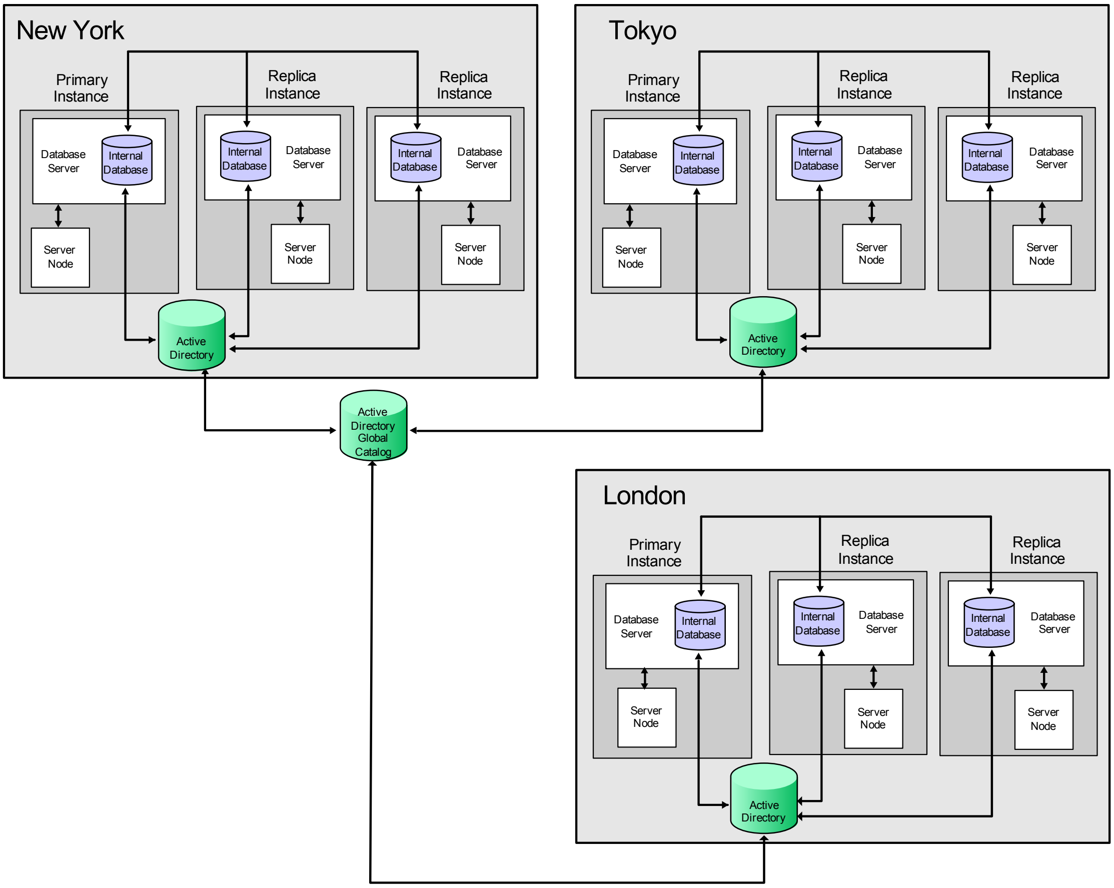

Site 1
(Data Replication Among All Internal Databases)
Primary Instance
Database Server
Internal Database
Server Node
Replica Instance
Internal Database
Database Server
Server Node
Active Directory
Site 2
Replica Instance
Internal Database
Database Server
Server Node
Active Directory
Site 3
Replica Instance
Internal Database
Database Server
Server Node
Active Directory
Active Directory Global Catalog

Task	See
1. Verify that all Authentication Manager machines meet the system requirements.	Chapter 1, "Preparing for Installation"
2. Install the primary instance. Be sure to secure backup files, and verify that the installation was successful by performing a test authentication after completing the installation.	Chapter 3, "Installing an RSA Authentication Manager Primary Instance"
3. Install a server node. Be sure to secure backup files, and verify that the installation was successful by performing a test authentication after completing the installation. **Note:** Repeat this process for each server node that you want to install.	Chapter 5, "Installing a Server Node"
4. Install the replica instance. Be sure to secure backup files, and verify that the installation was successful by performing a test authentication after completing the installation.	Chapter 4, "Installing a Replica Instance"

Task	See
5. Install a server node on the replica instance. Be sure to secure backup files and verify that the installation was successful by performing a test authentication after completing the installation. **Note:** Repeat this process for each server node that you want to install.	Chapter 5, "Installing a Server Node"
6. Perform post-installation tasks to prepare the Security Console for administration.	Chapter 9, "Performing Post-Installation Tasks"
7. Integrate your existing LDAP directory as the authoritative user and group identity source.	Chapter 10, "Integrating an LDAP Directory"

Large, Multisite Trusted Realm Deployment

This deployment example extends the multisite single-realm deployment by adding trusted realm authentication.


New York
Primary Instance
Replica Instance
Replica Instance
Database Server
Internal Database
Server Node
Active Directory
Tokyo
London
Active Directory Global Catalog

Task	See
1. Verify that all Authentication Manager machines meet the system requirements.	Chapter 1, "Preparing for Installation"
2. Install the primary instance. Be sure to secure backup files, and verify that the installation was successful by performing a test authentication after completing the installation.	Chapter 3, "Installing an RSA Authentication Manager Primary Instance"
3. Install a server node. Be sure to secure backup files, and verify that the installation was successful by performing a test authentication after completing the installation. **Note:** Repeat this process for each server node that you want to install.	Chapter 5, "Installing a Server Node"
4. Install the replica instance. Be sure to secure backup files, and verify that the installation was successful by performing a test authentication after completing the installation.	Chapter 4, "Installing a Replica Instance"
5. Install a server node on the replica instance. Be sure to secure backup files and verify that the installation was successful by performing a test authentication after completing the installation. **Note:** Repeat this process for each server node that you want to install.	Chapter 5, "Installing a Server Node"
6. Perform post-installation tasks to prepare the Security Console for administration.	Chapter 9, "Performing Post-Installation Tasks"
7. Integrate your existing LDAP directory as the authoritative user and group identity source.	Chapter 10, "Integrating an LDAP Directory"
8. Create your trusted realm relationships.	The *Administrator's Guide*

3

Installing an RSA Authentication Manager Primary Instance

- Preparing to Install a Primary Instance
- Performing an Installation
- Securing Backup Files

Preparing to Install a Primary Instance

The RSA Authentication Manager database can be installed on the same machine as the primary (local), or on a separate machine (remote) to better handle the load instead of overloading the primary instance. If you are going to use a standalone database, the Authentication Manager database must be installed on a machine before installing a primary or a replica instance on another machine. For instructions on installing a standalone database, see "Installing the RSA Authentication Manager Database on a Separate Machine" on page 43.

You can install a primary instance of RSA Authentication Manager 7.1 with or without RSA RADIUS. You are prompted during the installation as to whether you want to select RADIUS as an additional feature.

Important: If you plan to use RADIUS on this machine, RSA recommends that you select the RADIUS server option (the default selection) during Authentication Manager installation. If you decide to install RADIUS after Authentication Manager is already installed, you can install it on its own host machine. Alternatively, you would have to uninstall Authentication Manager from its host machine and reinstall it with the RADIUS option selected.

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 present the RADIUS option. If you want to install RADIUS in this situation, make sure that 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.

Synchronizing Clocks

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

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

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

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

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

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, rather than a DVD, you must mount the image to make it readable to your system before you can perform the installation.

On Windows

Windows provides no method for mounting or accessing an ISO image. RSA recommends using third-party software to burn the ISO image to DVD or one of the third-party tools that allows you to mount the ISO image and access the installation files within it.

Note: Microsoft provides a command line utility (**dvdburn.exe**) for burning ISO images to DVD in the Windows 2003 Resource Kit Tools, which you can download from the Microsoft web site.

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.

Performing an Installation

You can perform an installation using the Graphical User Interface (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: In most cases, once you have installed Authentication Manager, you cannot change the installation type or add RADIUS to the same machine, unless you uninstall Authentication Manager and reinstall it using the appropriate installation type. (You can, however, promote a replica to a primary, for both Authentication Manager and RADIUS, without reinstalling.) Before you uninstall and reinstall, be sure to back up the Authentication Manager database, the RADIUS database, or both, and restore the databases after reinstalling. If you prefer, you can add RADIUS to your deployment on a separate machine, rather than uninstalling and reinstalling Authentication Manager.

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

Note: When using the GUI-based installer on Solaris and Linux operating systems, the Display environment variable must be defined and set to a display server configured to allow access.

To install Authentication Manager:

Note: For Solaris and Linux operating systems, the installer must be run 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\win32-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 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.

4. Respond to the prompts for **Select Region** and **License Agreement**.
5. 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.

6. On the additional features screen, do one of the following:
   - If you want to install RADIUS on the current machine with Authentication Manager, make sure that **RSA RADIUS** is selected and click **Next**.
   - If you do not want to install RADIUS, or you want to install it on a separate machine, clear the RSA RADIUS checkbox and click **Next**.
7. Verify the directory name, or click **Browse** to install Authentication Manager to a different directory.

8. Select one of the following database types:
   - **Local** - if you want to install the database with the Authentication Manager software on the current machine.
   - **Remote** - if you already installed the database on a separate machine. This selection requires the database package that was generated during the database installation.
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 will result 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, 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. If you chose a local database in step 8, the installer prompts you to enter and confirm a user ID and password.

    Note: The user ID and password that you specify is the initial user name and password 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 will be used as the initial password for both administrator accounts and as the master password for operations such as installing a replica instance or handling security certificates. The Super Admin password will expire according to the password policy. The master password will 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 excluded.

13. If you chose to install RADIUS in step 6, complete the following steps that only apply to a RADIUS installation. If you did not choose to install RADIUS, skip to step 14.

    a. When prompted for the RADIUS server type, click **Next**. **Primary RADIUS server** is selected by default and cannot be changed.

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

    b. When the installer displays an automatically generated local system account for the RADIUS administrator, click **Next**. The account is required for certain RADIUS functions, but you do not need to use it.

    c. Enter and confirm a value for the RADIUS replication secret.

    The replication secret is shared between the RADIUS primary server and the RADIUS replica servers. (You can choose any value for the replication secret; there are no rules for the length or character type. However, you cannot use spaces.)

    d. When prompted to import a version 6.1 RADIUS database, make sure that **No** is selected and click **Next**.

14. If you chose a remote database type, enter the following information:

    - The location of the database package. See "Generating a Database Package File" on page 71.
    - The master password, specified at Database Only installation time.

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

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

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

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

17. To begin copying Authentication Manager files, click **Install**.

    The installer begins copying files and displays a progress indicator.

18. To verify that the installation was successful, leave the checkbox for **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.

    Click **Finish** to close the installer.

19. 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.
20. Log on to the Security Console using the Super Admin user name and password.

Note: If you are unable to log on to the Security Console, see Chapter 13, "Troubleshooting."

21. Continue to the following section, "Securing Backup Files" to perform important post-installation tasks.
22. If you installed RADIUS, see "Integrating the RSA RADIUS Server into the Existing Deployment" on page 122 for post-installation configuration tasks. See "Testing RSA RADIUS Operation" on page 123 for testing information.

If you encounter any problems installing Authentication Manager, see Chapter 13, "Troubleshooting."

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.

4

Installing a Replica Instance

- Preparing to Install a Replica Instance
- Performing an Installation
- Rebalancing Contact Lists
- Securing Backup Files

Preparing to Install a Replica Instance

Replica instances of RSA Authentication Manager are used as a means of minimizing data loss in the event of a hardware disaster. Replica instances are also used for geographically dispersed offices, as well as improving performance.

The Authentication Manager database can be installed on the same machine as the replica instance (local), or on a separate machine (remote) to better handle the load instead of overloading the replica instance. If you are going to use a standalone database, the Authentication Manager database must be installed on a machine before installing a primary or a replica instance on another machine. For a high-level overview of the tasks required for installing a replica instance with a standalone database, see "Installing a Replica Instance with a Standalone Database" on page 53.

You can install a replica instance of RSA Authentication Manager 7.1 with or without RSA RADIUS. You are prompted during the installation as to whether you want to select RADIUS as an additional feature.

Important: If you plan to use RADIUS on this machine, RSA recommends that you select the RADIUS server option (the default selection) during Authentication Manager installation. If you decide to install RADIUS after Authentication Manager is already installed, you can install it on its own host machine. Alternatively, you would have to uninstall Authentication Manager from its host machine and reinstall it with the RADIUS option selected.

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 present the RADIUS option. If you want to install RADIUS in this situation, make sure that 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.

Gather information from the primary instance database server, and make it available to the replica instance database server host. Perform these steps:

1. Make sure that the clock on the Authentication Manager primary instance database server is accurate. After installation, the Authentication Manager replica instance database servers automatically synchronize their clocks with the Authentication Manager primary instance database server.

   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.

2. Copy the license files to the replica so that the license files are available locally.
3. Create a replica package file from the primary server using the Operations Console. You may also need to create a primary data file if you want to copy the primary database to the replica manually. For instructions, see the following section, "Generating a Replica Package File."
4. Copy the replica package file, and optionally the primary data file, to the target host. Each package file is unique, functioning properly only on the host specified during its creation. For instructions, see "Transferring the Replica Package File" on page 55.
5. If you are installing RADIUS on the replica instance, either copy the RADIUS replica package file, **replica.ccmpkg**, from the RADIUS primary to the target host (the package file is created automatically during the RADIUS primary installation process) or provide the information about the primary instance manually during the replica installation process.

Note: There must be network connectivity between the primary and replica servers. A replica server cannot be installed if a network connection cannot be established between the systems.

Installing a Replica Instance with a Standalone Database

The following table provides a high-level overview of the tasks you must perform to install a replica instance with a standalone database.

Task	See
1. Install a primary instance.	Chapter 3, "Installing an RSA Authentication Manager Primary Instance"
2. Generate a replica package file for the replica instance. You must provide the fully qualified hostname of the machine where you will install the replica.	The following section, "Generating a Replica Package File"
3. Transfer the replica package file to the replica and the standalone database.	"Transferring the Replica Package File" on page 55
4. Install the standalone database for the replica using the replica package file that you copied in the previous step.	Chapter 6, "Installing the RSA Authentication Manager Database on a Separate Machine"
5. Generate a database package file on the standalone database machine. You must provide the fully qualified hostname of the machine where you will install the replica.	"Generating a Database Package File" on page 71
6. Transfer the database package file to the replica instance.	"Transferring the Database Package File" on page 72
7. Install a replica instance using the database package file and the replica package file that you transferred to the replica machine.	"Performing an Installation" on page 56

Generating a Replica Package File

When you install an Authentication Manager replica instance or replica standalone database, you must provide one or both of the following:

- Replica package file — contains information about the Authentication Manager primary instance that enables replication from the primary to the replica instances.
- Primary data file — contains a copy of the contents of 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, optionally, the primary data file. The details of the procedure differ somewhat, depending on whether:

- The primary instance has a local or remote database
- The replica instance has a local or remote database
- You want to copy the data from the primary to the replica automatically (over the network without using a primary data file) or manually (by copying the primary data 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, depending on whether your primary instance has a local or remote database. If the primary instance has a remote database, the primary data file is saved on the remote machine and you need to retrieve it from the remote machine to copy it to the replica.

From your local machine, or from the primary remote database machine, you copy the files to either the replica server machine or the replica standalone database machine, depending on your configuration. You are prompted for the necessary files when installing the replica instance or the replica standalone database.

During the process of generating the replica package and primary data files, you must select one of the following options for performing the initial copy of the primary data from the primary database to the replica database:

- Manual — two files are created: the replica package file and the primary data file.
- Automatic — only the replica package file is created. After installation of the replica instance or replica standalone database, 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.

Note: Each replica package file can be used for only one replica instance to ensure security during the replica instance installation process. Therefore, you need to generate a new replica package file, and optionally a new primary data file, for each replica instance that you install. Do not attempt to install replica instances in parallel. Install replica instances one at a time.

To generate and download the replica files:

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

---

1. Start the Operations Console and log on to the Console using your Operations Console user name and password.
2. Click **Deployment Configuration > Instances > Generate Replica Package**.
3. In the **Replica Hostname** field, enter the fully qualified hostname of the replica server host.
4. In the **Replica IP Address** field, enter the IP address of the replica server host.
5. In the **Master Password** field, enter the master password that you created when you installed the Authentication Manager primary instance.
6. In the **Initial Data Transfer** field, select **Automatic** or **Manual**.
7. Click **Generate File(s)** to create the replica package file and, optionally, the primary data file.
8. Do one of the following, depending on your choice in the **Initial Data Transfer** field:
    - If you chose Automatic, click **Download** to save the replica package file to your local machine.
    - If you chose Manual and have a local primary database, click **Download** to save the replica package file to your local machine, and click **Download** to save the primary data file to your local machine.
    - If you chose Manual and have a remote primary database, click **Download** to save the replica package file to your local machine. Retrieve the primary data file from the remote database location displayed on the page and save it to your local machine.
9. 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 contains sensitive data. RSA recommends that you transfer the package 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.

Copying the RSA RADIUS Replica Package File

If you are installing RADIUS as an additional feature on the replica server, decide whether you want to use the RADIUS replica package file, **replica.ccmpkg,** that was created automatically during installation of the RADIUS primary server. The RADIUS replica package file contains information about the primary server that is needed by the replica server.

As an alternative to using the replica package file, you can enter the required information manually during the replica installation process. You have to enter the following information when prompted: primary server name, primary server IP address(es), and the replication secret.

To copy the RSA RADIUS replica package file:

1. On the RADIUS primary server, locate the 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 replica server host. RSA recommends that you transfer the package file through a secure network or by removable media. Make note of where you copy the package file on the replica server as the location will be required during the RADIUS replica installation.

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.

Important: In most cases, once you have installed Authentication Manager, you cannot change the installation type or add RADIUS to the same machine, unless you uninstall Authentication Manager and reinstall it using the appropriate installation type. (You can, however, promote a replica to a primary, for both Authentication Manager and RADIUS, without reinstalling.) Before you uninstall and reinstall, be sure to back up the Authentication Manager database, the RADIUS database, or both, and restore the databases after reinstalling. If you prefer, you can add RADIUS to your deployment on a separate machine, rather than uninstalling and reinstalling Authentication Manager.

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

Important: When you install multiple replica instances, you must install them one at a time. Do not attempt to install them in parallel. You must generate a new replica package file and, optionally, a new primary data file for each replica that you install. For more information, see "Generating a Replica Package File" on page 54.

To install Authentication Manager:

Note: For Solaris and Linux operating systems, the installer must be run 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\win32-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 the Package Verification Failed message appears, 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 operation system, specify the local user.

Note: This 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.

4. Respond to the prompts for **Select Region** and **License Agreement**.
5. Select **Replica 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.

6. On the additional features screen, do one of the following:
   - If you want to install RADIUS on the current machine with Authentication Manager, make sure that the **RSA RADIUS** checkbox is selected and click **Next**.
   - If you do not want to install RADIUS, or you want to install it on a separate machine, clear the RSA RADIUS checkbox and click **Next**.
7. Verify the installation directory name, or click **Browse** to install Authentication Manager to a different directory.
8. Select one of the following database types:
   - **Local** - if you want to install the database with the RSA Authentication Manager software on the current machine.
   - **Remote** - if you already installed the database on a separate machine. This selection requires the database package that was generated during the database installation.
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 will result 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, 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 and, optionally, the primary data file that you created and transferred from the Authentication Manager primary instance. If you have not finished these tasks, see "Preparing to Install a Replica Instance" on page 51.
    - The master password, specified at primary installation time.
13. Enter and confirm the Super Admin user name and password.

14. If you chose to install RADIUS in step 6, complete the following steps that only apply to a RADIUS installation. If you did not choose to install RADIUS, go to step 16.
    a. Select the realm with which the RADIUS server will be associated and then click **Next**.
    b. When prompted for the RADIUS server type, click **Next**. The appropriate RADIUS server type is selected by default and cannot be changed.
    c. When the installer displays an automatically generated local system account for the RADIUS administrator, click **Next**. This account is required for certain RADIUS functions, but you do not need to use it.
    d. 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, as many as four primary server IP addresses separated by commas, the replication secret, and a confirmation of the replication secret. Click **Next**.
    e. When prompted to import a version 6.1 RADIUS database, make sure that **No** is selected and click **Next**.
15. If you chose a remote database type in step 8, enter the following information:
    - The location of the database package. See "Generating a Database Package File" on page 71.
    - The master password, specified at Database Only installation time.
16. Review the summary screen, verifying the features that you have selected and the disk space required.
17. To begin copying Authentication Manager files, click **Install**.

    The installer begins copying files and displays a progress indicator.
18. To verify that the installation was successful, leave the checkbox for **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**.

    Click **Finish** to close the installer.
19. 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.

20. Log on to the Security Console using the Super Admin user name and password.

    Note: If you are unable to log on to the Security Console, see Chapter 13, "Troubleshooting."

21. If you installed RADIUS, see "Integrating the RSA RADIUS Server into the Existing Deployment" on page 122 for post-installation configuration tasks. See "Testing RSA RADIUS Operation" on page 123 for testing information.

If you encounter any problems installing Authentication Manager, see Chapter 13, "Troubleshooting."

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

Installing a Server Node

- Preparing to Install a Server Node
- Performing an Installation
- Rebalancing Contact Lists
- Securing Backup Files
- Verifying Server Node Function

Preparing to Install a Server Node

Server nodes allow both authentication and administrative operations to be distributed between a collection of systems (server nodes). For example, if a primary installation is experiencing heavy system resource utilization due to reports or other administrative functions, adding a server node reduces the load on the primary instance (which may also be handling data replication for other instances).

Note: You must have an Enterprise Server license to install server nodes. Server nodes are not available with a Base Server license.

Gather information from the primary or replica database server and make it available to the server node host by performing these steps:

1. Create a node package file from the database server using the Manage Nodes utility. See the following section, "Creating a Node Package File."
2. Transfer the node package file to the target host. Each package file is unique, functioning properly only on the host specified during its creation. See "Transferring the Node Package File" on page 62.

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

Important: The server node must be installed on the same platform as the primary or replica instance. Also, the host for the server node must be in the same subnet as its primary or replica database server. Server node installation fails if these requirements are not met.

Creating a Node Package File

To create a node package file with the Manage Nodes utility as described in this section, you need to provide the following information:

- Server node hostname
- Super Admin password
- Master password

Note: For complete details on the manage-nodes command, type **rsautil manage-nodes --help** at a command prompt in ***RSA_AM_HOME*/utils**.

To create a node package file using the Manage Nodes utility:

Note: The primary instance must be running for the manage-nodes command to function properly.

---

1. On the host of the primary server, open a new command shell and change directories to ***RSA_AM_HOME*/utils**.
2. Type:

   ```
   rsautil manage-nodes --node-host hostname -u admin-id -a
   add-node
   ```

   where:

   - *hostname* is the fully qualified hostname of the server node host.
   - *admin-id* is the User ID of the administrator.
3. When prompted, enter your Super Admin password.
4. When prompted, enter your master password.

   The message "Adding node to cluster" appears.
5. Verify that the directory contains a file named ***hostname*-node.pkg**, where *hostname* reflects the hostname value that you specified for the --node_host argument.

Transferring the Node Package File

Once you have created a node package file, you must transfer it to the target host. RSA recommends that you transfer the package through a secure network or by removable media.

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

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 that you allow at least one hour to perform the installation.

Important: Make sure that the primary or replica instance where you created the node package is running before you begin the installation.

To install Authentication Manager:

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

Platform	Location	Command
Windows 32-bit	auth_mgr\win32-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 operation system, specify the local user.

Note: This 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.

4. Respond to the prompts for **Select Region** and **License Agreement**.

5. Select **Server Node**.

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.

Important: In most cases, once you have installed Authentication Manager, you cannot change the installation type later on, unless you uninstall Authentication Manager and reinstall it using the appropriate installation type. Before you uninstall and reinstall, be sure to back up the Authentication Manager database, and restore the databases after reinstalling.

---

6. Verify the directory name, or click **Browse** to install Authentication Manager in a different directory.

Note: This location must be the same directory as the one where you installed the primary or replica instance.

7. The installer displays the hostname and IP address that will be used for installation. Verify that this information is correct, and click **Next**.

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.

8. 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, and click **Next**.

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

9. Verify the license information, and click **Next**.
10. When prompted, enter the following information:
    - The location of the node package file that you created and transferred from the primary or replica instance. If you have not finished these tasks, see "Preparing to Install a Server Node" on page 61.
    - The master password for the primary instance, specified at primary installation time.

11. Review the summary screen, verifying the features you have selected and the disk space required.
12. To begin copying Authentication Manager files, click **Install**.

    The installer begins copying files and displays a progress indicator.
13. Click **Finish** to close the installer.

If you encounter any problems installing Authentication Manager, see Chapter 13, "Troubleshooting."

Rebalancing Contact Lists

After you add a server node, you must rebalance the contact lists in the primary instance Security Console. This updates references to the new server nodes.

Note: If the servers are restarted, the references to the new 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.

Verifying Server Node Function

After the installation, do the following:

- On the Authentication Manager primary instance, restart the Operations Console so that the primary instance recognizes the new server node.
- Use the Multicast Network Test utility to make sure that the server node can communicate with other hosts. See "Multicast Network Test Utility" on page 187.
- Verify that the Authentication Manager service is in the Started state in the Windows Services Manager.

6

Installing the RSA Authentication Manager Database on a Separate Machine

- Preparing to Install the Database on a Separate Machine
- Performing a Standalone Database Installation
- Generating a Database Package File
- Transferring the Database Package File
- Verifying That the Database Installed Successfully

It is possible to install the RSA Authentication Manager 7.1 database on a separate machine dedicated to handling all of the database connection requests. This machine functions as the database server. Installing a separate database enhances the scalability of Authentication Manager, helping to maintain performance with large numbers of administrators or self-service users.

The process of installing a separate database requires that you install the database first on a separate machine, then install your first server node, and then install any additional server nodes. The first server node that you install handles replication of data, but distributes administration requests to any of the other server nodes through a proxy server.

This chapter describes the steps to install a standalone database either through the GUI-based installer or the command line installer. This chapter also describes how to generate the database package file, transfer it securely to the server node, and verify that the database installed successfully.

Preparing to Install the Database on a Separate Machine

The system requirements for the separate database machine are the same as the requirements for installing a primary or replica instance. Verify that the machine on which you want to install the database meets all of the system requirements listed in "Hardware and Operating System Requirements" on page 13.

These are the additional requirements for the standalone hardware:

- It cannot have an Oracle database installed on it already.
- It must be on the same local subnet as the other server nodes in the instance.
- Firewalls on the database server and server nodes must be configured to allow communication on port number 2334.
- There can be no network address translation (for example, a firewall with NAT) between the database server and the server nodes.
- Your DNS server must be configured to resolve by both fully qualified name and short name.

  The primary instance must be able to resolve the fully qualified hostname of the standalone database machine, and the standalone database machine must be able to resolve the fully qualified hostname of the primary instance.

Note: If you are installing a standalone database for a replica, you must first create a replica package file on the primary instance using the Operations Console. You may also need to create a primary data file if you want to copy the primary database to the replica instance manually. For instructions, see the Operations Console Help topic "Generate and Download Replica Files."

Important: In most cases, once you have installed Authentication Manager, you cannot change the installation type later on, unless you uninstall Authentication Manager and reinstall it using the appropriate installation type. Before you uninstall and reinstall, back up the Authentication Manager database, restore the database after reinstalling, and generate a new database package before installing the primary or replica instance. Installation types are described in "Installation Types" on page 24.

Performing a Standalone Database Installation

You can perform an installation using the GUI or the command line interface. Installation time varies depending on system speed and memory. Make sure that you allow at least one hour to perform the installation.

Note: Be sure you have copied the RSA Authentication Manager license files to the standalone database machine.

To install the Authentication Manager database:

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\win32-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 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.

4. Respond to the prompts for **Select Region** and **License Agreement**.

5. Select **Database only**, and click **Next**.

   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.

6. Select the directory location, and click **Next**.
7. Select one of the following types of database-only installations, and click **Next**:
   - **Primary.** If you want to use the database with your primary instance.
   - **Replica.** If you want to use the database with a replica instance.
8. When the installer displays the hostname and IP address to use for installation, verify that these are correct, and click **Next**.

   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 sends requests only to the IP address that you specify. Failure to verify the IP address and hostname results in installation or server startup problems.

9. 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, and click **Next**.

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

10. Verify the license information, and click **Next**.
11. When prompted, enter and confirm a Super Admin and master password.

    The value you enter is used for both the initial Super Admin password and the master password for operations such as installing a replica instance or handling security certificates.

    The password must be between 8 and 32 characters and include at least 6 alphabetic characters and 1 non-alphanumeric character. "@" and "~" are excluded.
12. If you are installing a standalone database for a replica, enter the location of the replica package file that you copied from the primary instance. If you also copied the primary data file from the primary instance, enter the location of the primary data file when prompted.
13. Review the summary screen, verifying the features that you have selected and the disk space required.

14. To begin copying Authentication Manager files, click **Install**.

    The installer begins copying files and displays a progress indicator.

15. Click **Finish** to close the installer.

If you encounter any problems installing Authentication Manager, see Chapter 13, "Troubleshooting."

Generating a Database Package File

The database package file contains information that the other server nodes in your instance need to connect to the database.

To create a database package file using the Generate Database Package utility:

1. From a command prompt on the host of the database server, change directories to ***RSA_AM_HOME*/utils**.

   Note: On a Solaris or Linux operating system, you must run the Generate Database Package utility as the install user, that is, the local user you created when installing the standalone database. Do not run the utility as root user.

2. Type:

   ```
   rsautil gen-db-pkg --host hostname --IP ipaddress
   --master-password password --admin-uid userid
   ```

   where:

   - *hostname* is the fully qualified hostname of the remote primary or replica instance that you will install.
   - *ipaddress* is the IP address of the remote primary or replica instance that you will install.
   - *password* is the master password specified during installation of the database.
   - *userid* is the User ID of the Super Admin specified during the installation of the database.

3. Verify that the directory contains a file named ***hostname*-DB.pkg**, where *hostname* reflects the hostname value that you specified for the --host argument.

Transferring the Database Package File

You must copy this database package file to the primary instance or to a replica instance, depending on which type of instance you selected when you installed the database. When you install the RSA Authentication Manager 7.1 software on the primary or replica instance, the installer prompts you to specify the location of this database package file.

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

Verifying That the Database Installed Successfully

On Windows, in the Windows Services Manager, verify that the following services are started:

- RSA Authentication Manager Database Listener
- RSA Authentication Manager Database Server

On Linux or Solaris:

1. From the command line, type:

```
RSA_AM_HOME/server/rsaam status all
```

2. Verify that the following services are running:
    - RSA Authentication Manager Database Listener
    - RSA Authentication Manager Database Server

7

Installing RSA RADIUS on a Separate Machine

- Preparing to Install RSA RADIUS on a Separate Machine
- Installing RSA RADIUS

Preparing to Install RSA RADIUS on a Separate Machine

Note: RADIUS can only be installed on a 32-bit Windows or Linux platform. When you install the 64-bit version of RSA Authentication Manager software on a supported 64-bit operating system, the installer does not present the RADIUS option. If you want to install RADIUS in this situation, make sure that 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.

Before you can install RSA RADIUS on a machine separate from Authentication Manager, you must complete the following tasks in your Authentication Manager deployment. This list of tasks provides a high-level overview. The details for the RADIUS-specific procedures listed below are provided later in this chapter.

- Install the primary Authentication Manager instance.
- Create a RADIUS package file (using the Generate RADIUS Package utility) on the Authentication Manager primary instance to gather information needed by the RADIUS primary and replica servers.
- Copy the RADIUS package file to the machine where the RADIUS server will be installed so that it is accessible during the installation process.
- If you are installing a RADIUS replica, install the RADIUS primary in your deployment first.
- If you are installing a RADIUS replica, copy the **replica.ccmpkg** file, (which is created automatically on the RADIUS primary when the RADIUS primary is installed), to the RADIUS replica host machine so that it is available during the RADIUS replica installation process. (Alternatively, you can supply information about the RADIUS primary manually through one of the installation screens rather than using the **replica.ccmpkg** file.)

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 of a firewall to communicate with an RSA RADIUS server inside of 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 an installation of the RADIUS server with the necessary IT personnel to ensure that administrators with the required RADIUS access are available during the installation. You must have the following types of administrators:

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

Pre-Installation Tasks

This section describes the pre-installation tasks required to prepare your system for a standalone RADIUS installation.

Creating an RSA RADIUS Package File

Before you install RSA RADIUS on a machine separate from Authentication Manager, create a RADIUS package file (using the Generate RADIUS Package utility) on the Authentication Manager primary instance to gather information needed by both the 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 host of the Authentication Manager primary server, change directories to ***RSA_AM_HOME*/utils**.
2. Type:

   ```
   rsautil gen-radius-pkg -m master-password
   ```

   where *master-password* is the master password for the encrypted properties file, which you set when installing the Authentication Manager primary instance. (By default, this is the same as the Super Admin password, unless the Super Admin password was changed after installation.)

When the package file creation is complete, the message "Successfully generated *AMprimaryhost*-radius.pkg" appears and the package file is output to the ***RSA_AM_HOME*/utils** directory as ***AMprimaryhost*-radius.pkg**.

For more information on the Generate RADIUS Package utility, see Appendix B, "Command Line Utilities."

For complete details on the gen-radius-pkg command flags, run **rsautil gen-radius-pkg --help** from a command prompt in ***RSA_AM_HOME*/utils**.

Copying the RSA RADIUS Package File

Before you install an RSA RADIUS primary server on a separate machine, copy the RADIUS package file that you created on the Authentication Manager primary instance to the machine where you will install the RADIUS primary server. The RADIUS package filename is ***AMprimaryhost*-radius.pkg** and is in the directory ***RSA_AM_HOME*/utils**. You can copy the package file to the RADIUS primary server host in several ways, including copying it over a secure network or using removable media.

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

Note the directory where you copy the package file as you will have to supply this location during the RADIUS installation.

Installing RSA RADIUS

This section provides the procedures for installing RSA RADIUS primary and replica servers on machines separate from Authentication Manager.

Installing an RSA 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: In most cases, once you have installed Authentication Manager, you cannot change the installation type or add RADIUS to the same machine, unless you uninstall Authentication Manager and reinstall it using the appropriate installation type. (You can, however, promote a replica to a primary, for both Authentication Manager and RADIUS, without reinstalling.) Before you uninstall and reinstall, be sure to back up the Authentication Manager database, the RADIUS database, or both, and restore the databases after reinstalling. If you prefer, you can add RADIUS to your deployment on a separate machine, rather than uninstalling and reinstalling Authentication Manager.

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

Note: When using the GUI-based installer on Solaris and Linux operating systems, the Display environment variable must be defined and set to a display server configured to allow access.

To install a standalone RADIUS primary server:

Note: For Solaris and Linux operating systems, the installer must be run 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\win32-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: This 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.

4. Respond to the prompts for **Select Region** and **License Agreement**.
5. Select **Radius Only**.

   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.

6. 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**.
7. 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.
8. Click **Browse** to find and select the directory that contains your Authentication Manager license file, server key, and certificate files. Click **Next.**
9. Verify the license information, and click **Next**.
10. Browse to the location of the RADIUS package file containing information about the Authentication Manager primary instance. You must also enter the master password that you created during the Authentication Manager primary instance installation.
11. Enter the user name and password of an administrator with the Super Admin role.
12. Select the realm with which the RADIUS server will be associated, and click **Next**.
13. When prompted for the RADIUS server type, click **Next**. The appropriate RADIUS server type is selected by default and cannot be changed.
14. When the installer displays an automatically generated local system account for the RADIUS administrator, click **Next**. This account is required for certain RADIUS functions, but you do not need to use it.
15. Enter and confirm a value for the RADIUS replication secret.

    The replication secret is shared between the RADIUS primary server and the RADIUS replica servers. (You can choose any value for the replication secret; there are no rules for the length or character type. However, you cannot use spaces.)

16. When prompted to import a version 6.1 RADIUS database, make sure that **No** is selected and click **Next**.
17. Review the summary screen, verifying the features that you have selected and the disk space required.
18. To begin copying RADIUS files, click **Install**.

    The installer begins copying files and displays a progress indicator.
19. Click **Finish** to close the installer.

For post-installation RADIUS server and client configuration information, see "Integrating the RSA RADIUS Server into the Existing Deployment" on page 122.

For testing information, see "Testing RSA RADIUS Operation" on page 123.

If you encounter any problems installing RADIUS, see Chapter 13, "Troubleshooting."

Installing an RSA RADIUS Replica Server

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.

Before installing an RSA RADIUS replica server on a machine separate from Authentication Manager, you must complete the following steps:

1. Install the Authentication Manager primary instance.
2. Install the RADIUS primary instance.
3. Copy the RADIUS package file that you created on the Authentication Manager primary instance to the machine where the RADIUS replica instance will be installed. (The RADIUS package file is named *AMprimaryhost*-radius.pkg and is in the directory ***RSA_AM_HOME*/utils** on the Authentication Manager primary instance.)
4. Copy the RADIUS replica package file, **replica.ccmpkg**, (which is created automatically when the RADIUS primary server is installed) to the RADIUS replica host machine. Alternatively, you could provide the information in the replica package file when prompted during the RADIUS replica 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.

Important: In most cases, once you have installed Authentication Manager, you cannot change the installation type or add RADIUS to the same machine, unless you uninstall Authentication Manager and reinstall it using the appropriate installation type. (You can, however, promote a replica to a primary, for both Authentication Manager and RADIUS, without reinstalling.) Before you uninstall and reinstall, be sure to back up the Authentication Manager database, the RADIUS database, or both, and restore the databases after reinstalling. If you prefer, you can add RADIUS to your deployment on a separate machine, rather than uninstalling and reinstalling Authentication Manager.

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

Note: When using the GUI-based installer on Solaris and Linux operating systems, the Display environment variable must be defined and set to a display server configured to allow access.

Copying the RSA RADIUS Replica Package File

Before you start the actual installation process, decide whether you want to use the replica package file **replica.ccmpkg** that was created automatically on the RADIUS primary server during installation. The RADIUS 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 could enter the required information manually during the RADIUS replica installation process. You would have to enter the following information when prompted: primary server name, primary server IP address(es), 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 RADIUS replica package file:

1. On the RADIUS primary server, locate the 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 machine. RSA recommends that you transfer the package file through a secure network or by removable media. Make note of where you copy the package file on the RADIUS replica machine as the location will be required during the RADIUS replica installation.

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

To install 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\win32-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: This 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.

4. Respond to the prompts for **Select Region** and **License Agreement**.
5. Select **Radius Only.**

Important: At this point, the installer informs you of 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.

6. 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**.
7. 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.
8. Click **Browse** to find and select the directory that contains your Authentication Manager license file, server key, and certificate files. Click **Next.**
9. Verify the license information, and click **Next**.
10. Browse to the location of the RADIUS package file containing information about the Authentication Manager primary instance. You must also enter the master password that you created when you installed the Authentication Manager primary instance.

11. Enter the user name and password of an administrator with the Super Admin role.
12. Select the realm with which the RADIUS server will be associated, and click **Next**.
13. When prompted for the RADIUS server type, click **Next**. The appropriate RADIUS server type is selected by default and cannot be changed.
14. When the installer displays an automatically generated local system account for the RADIUS administrator, click **Next**. This account is required for certain RADIUS functions, but you do not need to use it.
15. 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, as many as four primary server IP addresses separated by commas, the replication secret, and a confirmation of the replication secret. Click **Next**.
16. When prompted to import a version 6.1 RADIUS database, make sure that **No** is selected and click **Next**.
17. Review the summary screen, verifying the features you have selected and the disk space required.
18. To begin copying RADIUS files, click **Install**.

    The installer begins copying files and displays a progress indicator.
19. Click **Finish** to close the installer.

For post-installation RADIUS server and client configuration information, see "Integrating the RSA RADIUS Server into the Existing Deployment" on page 122.

For testing information, see "Testing RSA RADIUS Operation" on page 123.

If you encounter any problems installing RADIUS, see Chapter 13, "Troubleshooting."

8

Upgrading from RSA Authentication Manager 7.0

- Upgrading a Primary Instance
- Upgrading a Replica Instance
- Upgrading a Server Node
- Verifying the Upgrade

Note: This chapter provides the instructions for upgrading from RSA Authentication Manager 7.0 to 7.1. If you are upgrading from RSA Authentication Manager 6.1 to 7.1, see the *Migration Guide*.

Patch 7.0.4 is required to upgrade RSA Authentication Manager 7.0 to RSA Authentication Manager 7.1. If you do not already have patch 7.0.4 installed, download the patch.

To check if patch 7.0.4 is already installed:

1. Open the **jndi.properties** file located in **C:/Program Files/RSA Security/RSA Authentication Manager/utils/etc/**.
2. Search for the patch value of the com.rsa.patchlevel parameter. If the value is not patch 7.0.4, download patch 7.0.4.

   Note: If there is no com.rs.patchlevel parameter, you must download patch 7.0.4.

To download the patch:

1. Go to **https://knowledge.rsasecurity.com**.
2. Enter your RSA SecurCare Online credentials.
3. Click **Downloads** > **All downloads** > **Fixes by product** > **RSA SecurID** > **Authentication Manager**.
4. Click the Patch 7.0.4 for your specific operating system.

Note: Read the *Readme* file that is included with the patch.

Upgrading a Primary Instance

When you upgrade Authentication Manager from version 7.0 to 7.1, you must prepare for the upgrade before you install RSA Authentication Manager 7.1 and migrate the user data. You can migrate the user data on a primary instance using the Data Migration utility.

Preparing to Upgrade a Primary Instance

Important: Before you upgrade and migrate user data, you must back up the entire hard drive image where the RSA Authentication Manager 7.0 primary instance is installed.

To prepare for migration on the primary instance:

1. Add **Patch 7.0.4** to the RSA Authentication Manager 7.0 directory on the primary instance. This installs updated replication command line utilities to the RSA Authentication Manager 7.0 **utils** directory. The patch can be downloaded from RSA SecurCare Online.
2. Create a **utils-7.1** directory within the RSA Authentication Manager 7.0 directory on the primary instance in the same directory as the existing **utils** directory, and copy all of the files from ***DVD_Drive*****/auth_mgr/*****platform*****/ims/ ims-kit/utils** to this directory.
3. Copy the **wlclient.jar** file from ***RSA_AM_HOME*****/appcore/server/lib** to the **utils-7.1/jars/thirdparty** directory.
4. In the **utils-7.1** directory, modify the **rsaenv.cmd** file. Do the following:
    a. Verify that the following line exists in the file:

    ```
    set JAVA_OPTIONS=%JAVA_OPTIONS%
    -DMIGRATION_VERBOSE_MODE=true
    ```

    b. Edit the following values:

    ```
    set BEA_HOME=@BEA_HOME

    set WL_HOME=@WL_HOME

    set JAVA_OPTIONS=%JAVA_OPTIONS%
    -Dweblogic.security.TrustKeyStore=@TRUST_KEY_STORE

    set JAVA_OPTIONS=%JAVA_OPTIONS%
    -Dweblogic.security.CustomTrustKeyStoreFileName=@CUSTO
    M_TRUST_KEY_STORE

    set JAVA_OPTIONS=%JAVA_OPTIONS%
    -Dweblogic.security.SSL.trustedCAKeyStore=@CUSTOM_TRUS
    T_KEY_STORE

    set CLU_USER=@CLU_USER

    set RSA_IMS_HOME=@RSA_IMS_HOME

    set RSA_JAVA_HOME=@RSA_JAVA_HOME

    set PLATFORM_LIBS=@PLATFORM_LIBS
    ```

For example:

```
set BEA_HOME=C:\Program Files\RSA Security\RSA
Authentication Manager\

set WL_HOME=C:\Program Files\RSA Security\RSA
Authentication Manager\appcore

set WLS_HOME=%WL_HOME%\server

set JAVA_OPTIONS=%JAVA_OPTIONS%
-Dweblogic.security.TrustKeyStore=CustomTrust

set
JAVA_OPTIONS=%JAVA_OPTIONS%-Dweblogic.security.CustomT
rustKeyStoreFileName=C:\Program Files\RSA Security\RSA
Authentication Manager\jdk\jre\lib\security\cacerts

set JAVA_OPTIONS=%JAVA_OPTIONS%
-Dweblogic.security.SSL.trustedCAKeyStore=C:\Program
Files\RSA Security\RSA Authentication
Manager\jdk\jre\lib\security\cacerts

set CLU_USER=qeuser

set RSA_IMS_HOME=C:\Program Files\RSA Security\RSA
Authentication Manager\

set RSA_JAVA_HOME=C:\Program Files\RSA Security\RSA
Authentication Manager\jdk

set PLATFORM_LIBS=win32-x86
```

5. Generate the **classpath.jar** file:
   a. Change directories to ***RSA_AM_HOME*/utils-7.1**.
   b. Type:

      ```
      rsautil generate-classpath
      ```

6. Export the managed secrets from RSA Authentication Manager 7.0 to a file named **secrets.prop**:
   a. On the primary instance, change directories to ***RSA_AM_HOME*/utils**.
   b. Type:

      ```
      rsautil manage-secrets --action export --file
      etc\secrets.prop --file-password file_password
      ```

      where:

      - **secrets.prop** is the name of the managed secrets file.
      - *file_password* is the password for opening the managed secrets file.

7. Copy the **secrets.prop** file from the **utils/etc** directory to the **utils-7.1/etc** directory.

8. In the **utils-7.1/etc** directory, modify the **jndi.properties** file. Set the following:

```
java.naming.provider.url=t3://localhost:7001
# IMS Instance name
com.rsa.instanceName=DefaultInstance
# Weblogic admin protocol
com.rsa.appserver.protocol=t3
# Weblogic admin server hostname (FQN)
com.rsa.appserver.hostname=
# Weblogic admin port
com.rsa.appserver.port=7001
# Database server hostname
com.rsa.db.hostname=
# Port database server is listening on
com.rsa.db.port=
# Database instance name
com.rsa.db.instance=
# Database domain
com.rsa.db.domain=
# Oracle Home location
# For Windows, use double slashes \\, not single slashes
com.rsa.db.oracle.home=
# site name
com.rsa.siteName=PRIMARY INSTANCE
# Application installation directory
com.rsa.appdir=
# Application installation directory
com.rsa.appname=
# Alias of the Root CA
com.rsa.ssl.ca.alias=certgenca
# Path to the keystore that contains the Root CA
com.rsa.ssl.ca.store.path=
```

For example:

```
java.naming.provider.url=t3s://10.100.220.23:7002

com.rsa.instanceName=qe-860-23.qe.na.rsa.net

com.rsa.appserver.protocol=t3s

com.rsa.appserver.hostname=qe-860-23.qe.na.rsa.net

com.rsa.appserver.port=7006

com.rsa.db.hostname=qe-860-23.qe.na.rsa.net

com.rsa.db.port=2334

com.rsa.db.instance=woqjkxnt

com.rsa.db.domain=ims.rsa

com.rsa.db.oracle.home=C:\Program Files\RSA Security\RSA
Authentication Manager\db

com.rsa.siteName=qe-860-23.qe.na.rsa.net

com.rsa.appdir=C:\Program Files\RSA Security\RSA
Authentication Manager\server\servers\upload\am-app

com.rsa.appname=am-app

com.rsa.ssl.ca.alias=certgenca

com.rsa.ssl.ca.store.path=C:\Program Files\RSA
Security\RSA Authentication Manager\server\security\
root.jks
```

9. Import the managed secrets from the **secrets.prop** file that you created in step 6. Do the following:

   a. On the primary instance, change directories to ***RSA_AM_HOME*/utils-7.1**.

   b. Type:

   ```
     rsautil manage-secrets --action import
   --file etc\secrets.prop --file-password file_password
   ```

   where:

   - **secrets.prop** is the name of the managed secrets file that you created in step 6.
   - *file_password* is the password that you made for opening the managed secrets file.

10. Create a directory to contain all of the migration script files, such as C:\migration_scripts.

11. Copy all of the script files and directories to the migration script directory that you just created. Do the following:
    a. Copy everything from ***DVDDrive*:/auth_mgr/*platform*/dbscripts/config/ims/db/scripts/schema/oracle/migration** to C:\migration_scripts.
    b. Copy everything from ***DVDDrive*:/auth_mgr/*platform*/dbscripts/config/am/db/scripts/schema/migration** to C:\migration_scripts.

       Note: If prompted that this will overwrite the files, click **Yes** to overwrite the files.

    c. Copy all sql scripts (*.sql) from ***DVDDrive*:/auth_mgr/*platform*/ucm** to C:\migration_scripts/am70_71.

       where:
       - *DVDDrive* is the location of the RSA Authentication Manager 7.1 DVD.
       - *platform* is the platform, such as windows-x86.
12. Make all of the files in the migration script directory writable.
13. Stop all of the RSA Authentication Manager 7.0 primary servers, but keep the database running. If you have any server nodes, stop those as well.
14. Run the updateScripts command:
    a. On the primary instance, change directories to ***RSA_AM_HOME*/utils-7.1**.
    b. Type:

       ```
       rsautil migrate-amapp --action updateScripts
       --scriptDir migration_script_directory -V
       ```

       where *migration_script_directory* is the directory that you created in step 10.
15. Initialize migration on the primary instance:
    a. Change directories to ***RSA_AM_HOME*/utils-7.1**.
    b. Type:

       ```
       rsautil migrate-amapp --action initMigration
       --scriptDir migration_script_directory -V
       ```
16. Enable runtime data capture on each primary instance:
    a. Change directories to ***RSA_AM_HOME*/utils-7.1**.
    b. Type:

       ```
       rsautil migrate-amapp --action enableAudit
       --scriptDir migration_script_directory -V
       ```

17. If you have replica instances in your deployment, remove each replica instance:
    a. Change directories to ***RSA_AM_HOME*/utils**.
    b. Type:

```
rsautil setup-replication --action remove-replica
--name replica_instance_name -i
```

Important: You must remove all replica instances before removing the primary instance or the action will fail.

---

18. Remove the primary instance:
    a. On the primary instance, change directories to ***RSA_AM_HOME*/utils**.
    b. Type:

```
rsautil setup-replication --action remove-primary -i
```

19. Remove the RSA_MIGRATION_ADMIN user from the RSA Authentication Manager 7.0 database:
    a. Change directories to your migration script directory. For example, C:\migration_scripts.
    b. Type:

```
sqlplus sys/password@db_instance as sysdba
@rsaIMSOracleDropMigrationUser.sql
```

Important: Make sure that there is a space between sysdba and @rsaIMSOracleDropMigrationUser.sql.

---

where:

- *password* is the database password. You can get this using the Manage Secrets utility.
- *db_instance* is the name of the RSA Authentication Manager 7.0 database. You can get this from the **jndi.properties** file.

20. Back up the primary instance internal database to a file named **backup.bak**:
    a. On the primary instance, change directories to ***RSA_AM_HOME*/utils-7.1**.
    b. Type:

```
rsautil migrate-amapp --action backupPrimary
--fileName backup.bak --scriptDir
migration_script_directory -V
```

    c. Navigate to ***RSA_AM_HOME*/utils-7.1** and make sure that no errors are recorded in the backup log file. If errors are present, make any necessary changes and run the backupPrimary action again.

21. Copy the managed secrets file, **systemfields.properties**, from ***RSA_AM_HOME*/utils/etc**, to the location where the primary instance data backup file resides. Change the filename to **backup.secrets**.

Performing an Upgrade on a Primary Instance

RSA recommends that you upgrade Authentication Manager on a new machine so that you retain your existing Authentication Manager 7.0 in the event you make a mistake during the upgrade process.

To install RSA Authentication Manager 7.1 on the primary instance:

1. If you are upgrading Authentication Manager on the same machine, do the following:

   Note: This step is not necessary if you are installing RSA Authentication Manager 7.1 on a new machine.

   a. Copy **backup.secrets**, **backup.bak**, and the backup log file to a safe location outside of the installation.

   b. Uninstall Patch 7.0.4.

   c. Uninstall RSA Authentication Manager 7.0.

      For instructions on uninstalling Authentication Manager, see Chapter 12, "Removing RSA Authentication Manager."

2. Install RSA Authentication Manager 7.1 on the primary instance.

   Note: Use the same master password that you used for RSA Authentication Manager 7.0.

   For instructions on installing a primary instance, see Chapter 3, "Installing an RSA Authentication Manager Primary Instance."

3. Stop the RSA Authentication Manager 7.1 primary servers, but keep the database running. If you have a RADIUS server installed, keep the RADIUS server running as well.

Migrating User Data on a Primary Instance

To migrate the user data on the primary instance:

Important: If you are installing the database server on a separate machine, the following steps must be performed on the database server. Otherwise, perform the following steps on the RSA Authentication Manager 7.1 primary server.

1. Remove the old primary instance:

   a. In RSA Authentication Manager 7.1, change directories to ***RSA_AM_HOME*/utils**.

   b. Type:

      ```
      rsautil setup-replication --action remove-primary
      ```

2. Copy the **backup.bak** and **backup.secrets** files to a directory. For example, C:\temp.

3. Back up the new RSA Authentication Manager 7.1 secrets.
   a. Change directories to ***RSA_AM_HOME*/utils**.
   b. Type:

   ```
   rsautil manage-secrets --action export -f
   etc\secrets71.prop -k master_password
   ```

4. Create a directory to contain all of the migration script files, such as C:\migration_scripts.
5. Copy all of the script files and directories to the migration script directory that you just created. Do the following:
   a. Copy everything from ***DVDDrive*:/auth_mgr/*platform*/dbscripts/config/ims/db/scripts/schema/oracle/migration** to C:\migration_scripts.
   b. Copy everything from ***DVDDrive*:/auth_mgr/*platform*/dbscripts/config/am/db/scripts/schema/migration** to C:\migration_scripts.

   Note: If prompted that this will overwrite the files, click **Yes** to overwrite the files.

   c. Copy all sql scripts (*.sql) from ***DVDDrive*:/auth_mgr/*platform*/ucm** to C:\migration_scripts/am70_71.

   where:

   - *DVDDrive* is the location of the RSA Authentication Manager 7.1 DVD.
   - *platform* is the platform, such as windows-x86.

6. Make all of the files in the migration script directory writable.
7. Import the primary instance data from **backup.bak**:
   a. In RSA Authentication Manager 7.1, change directories to ***RSA_AM_HOME*/utils**.
   b. Type:

   ```
   rsautil migrate-amapp --action importPrimary
   --fileName C:\temp\backup.bak --scriptDir
   migration_script_directory -V
   ```

   where *C:\temp\* is the directory that you created in step 2.

8. Update the migration scripts:
   a. In RSA Authentication Manager 7.1, change directories to ***RSA_AM_HOME*/utils**.
   b. Type:

   ```
   rsautil migrate-amapp --action updateScripts -d
   migration_scripts_directory -V
   ```

9. Initialize the migration scripts:
   a. In RSA Authentication Manager 7.1, change directories to ***RSA_AM_HOME*/utils**.
   b. Type:

      ```
      rsautil migrate-amapp --action initMigration -d
      migration_scripts_directory -V
      ```

10. Import the primary instance data:
    a. In RSA Authentication Manager 7.1, change directories to ***RSA_AM_HOME*/utils**.
    b. Type:

       ```
       rsautil migrate-amapp --action importPrimaryComponent
       -f backup.bak -d migration_scripts_directory -V
       ```

11. Migrate the primary instance data:
    a. In RSA Authentication Manager 7.1, change directories to ***RSA_AM_HOME*/utils**.
    b. If you are migrating on the same machine, type:

       ```
       rsautil migrate-amapp -a migratePrimary -d
       migration_scripts_directory -V
       ```

       If you are migrating to a different machine, type:

       ```
       rsautil migrate-amapp -a migratePrimary -t
       new_host_name -o old_host_name -d
       migration_scripts_directory -V
       ```

12. Install the license file:
    a. In RSA Authentication Manager 7.1, change directories to ***RSA_AM_HOME*/utils**.
    b. Type:

       ```
       rsautil migrate-amapp -a installLicense -f
       license_file_name -d migration_scripts_directory -V
       ```

13. Verify the primary instance:
    a. In RSA Authentication Manager 7.1, change directories to ***RSA_AM_HOME*/utils**.
    b. Type:

       ```
       rsautil migrate-amapp -a validatePrimary -d
       migration_scripts_directory -V
       ```

14. Generate a primary instance migration report:
    a. In RSA Authentication Manager 7.1, change directories to ***RSA_AM_HOME*/utils**.
    b. Type:

       ```
       rsautil migrate-amapp -a reportPrimary -d
       migration_scripts_directory -V
       ```

15. Set up the primary instance:
    a. In RSA Authentication Manager 7.1, change directories to ***RSA_AM_HOME*/utils**.
    b. Type:

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

16. If you are installing the database server on a separate machine, export the secrets from the the database server machine and import them to the primary server. Do the following:
    a. On the database server machine, change directories to ***RSA_AM_HOME*/utils**, and type:

    ```
    rsautil manage-secrets -a export -f
    etc\secrets71migrated.secrets --file-password
    file_password
    ```

    b. Transfer the **secrets71migrated.secrets** file to the primary server using FTP.

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

    ---

    c. On the primary server, type:

    ```
    rsautil manage-secrets -a import -f
    /Location/secrets71migrated.secrets --file-password
    file_password
    ```

    where *Location* is the path of where the **secrets71migrated.secrets** file is stored.

17. Start all the servers on the primary instance, and start the Operations Console.
18. Modify the existing identity sources. Do the following:
    a. Start the Operations Console and log on to the Console using your Operations Console user name and password.
    b. Click **Deployment Configuration** > **Identity Sources** > **Manage Existing**.
    c. When prompted, enter your Super Admin user name and password.
    d. Click the identity source that you want to edit.
    e. From the Context menu, click **Edit**.
    f. Add the Directory URL, Directory User ID, and Directory Password.
    g. Click **Save**.

    Repeat this procedure for for each existing identity source.

19. Rebalance the contact lists on the primary instance. Do the following:
    a. Log on to the RSA Security Console.
    b. Click **Access** > **Authentication Agents** > **Authentication Manager Contact List** > **Automatic Rebalance**.
    c. Click **Rebalance.**

20. If you selected to install RADIUS when you installed RSA Authentication Manager 7.1 on the primary instance, make sure that your RADIUS servers are running. To set up the RADIUS server, change directories to ***RSA_AM_HOME*/config**, and type:

    ```
    configUtil.cmd configure radius register
    ```

    If you installed RADIUS on the same machine as Authentication Manager, enter the command on the primary instance. If you installed RADIUS on a separate machine, enter the command on the RADIUS server host machine. On Linux, the command must be run as root user.

21. On the primary instance, revoke RSA_REP tables grants from RSA_MIGRATION_ADMIN:

    a. Change directories to your migration script directory. For example, C:\migration_scripts.

    b. Type:

       ```
       sqlplus sys/password@db_instance as sysdba
       @rsaIMSOracleRevokeRSARepGrantsFromMigrationUser.sql
       ```

       where:

       - *password* is the database password.
       - *db_instance* is the name of the Authentication Manager database.

22. If you have replica instances in your deployment, create a replica package file. Do the following:

    a. Start the Operations Console and log on to the Console using your Operations Console user name and password.

    b. Click **Deployment Configuration** > **Instances** > **Generate Replica Package**.

    c. When prompted, enter your Super Admin user name and password.

    d. In the **Replica Hostname** field, enter the fully qualified hostname of the replica host server.

    e. In the **Replica IP Address** field, enter the IP address of the replica host server.

    f. In the **Master Password** field, enter the master password that you created when you installed the Authentication Manager primary instance.

    g. In the **Database Synchronization** field, select **Automatic** or **Manual**.

h. Click **Generate Package File** to create the package.

i. Click **Download** to save the package file to the local machine.

j. Click **Save to Disk**.

> **Note:** The replica package is output to the desktop as ***hostname*-replica.pkg**.

k. Click **Done**.

For more information on creating a replica package file, see "Generating a Replica Package File" on page 54.

23. Transfer the replica package file to the replica machine.

> **Note:** This encrypted replica package file contains sensitive data. RSA recommends that you transfer the package through a secure network or by removable media.

Upgrading a Replica Instance

When you upgrade Authentication Manager from version 7.0 to 7.1, you must prepare for the upgrade before you install RSA Authentication Manager 7.1 and migrate the user data. You can migrate the user data on a replica instance using the Data Migration utility.

> **Important:** If there is no authentication activity during the migration process, you do not need to complete the steps in the sections, "Preparing to Upgrade a Replica Instance" or "Performing an Upgrade on a Replica Instance." All you need to do is uninstall RSA Authentication Manager 7.0, and install RSA Authentication Manager 7.1 using the replica package file that you created.

Preparing to Upgrade a Replica Instance

Important: Before you upgrade and migrate user data, you must back up the entire hard drive image where the RSA Authentication Manager 7.0 replica instance is installed.

To prepare for migration on the replica instance:

1. Add **Patch 7.0.4** to the RSA Authentication Manager 7.0 directory on the replica instance. This installs updated replication command line utilities to the RSA Authentication Manager 7.0 **utils** directory. The patch can be downloaded from RSA SecurCare Online.
2. Create a **utils-7.1** directory within the RSA Authentication Manager 7.0 directory on the primary instance in the same directory as the existing **utils** directory, and copy all of the files from ***DVD_Drive*/auth_mgr/*platform*/ims/ ims-kit/utils** to this directory.
3. Copy the **wlclient.jar** file from ***RSA_AM_HOME*/appcore/server/lib** to the **utils-7.1/jars/thirdparty** directory.
4. In the **utils-7.1** directory, modify the **rsaenv.cmd** file. Do the following:
   a. Verify that the following line exists in the file:

   ```
   set JAVA_OPTIONS=%JAVA_OPTIONS%
   -DMIGRATION_VERBOSE_MODE=true
   ```

   b. Edit the following values:

   ```
   set BEA_HOME=@BEA_HOME

   set WL_HOME=@WL_HOME

   set JAVA_OPTIONS=%JAVA_OPTIONS%
   -Dweblogic.security.TrustKeyStore=@TRUST_KEY_STORE

   set JAVA_OPTIONS=%JAVA_OPTIONS%
   -Dweblogic.security.CustomTrustKeyStoreFileName=@CUSTO
   M_TRUST_KEY_STORE

   set JAVA_OPTIONS=%JAVA_OPTIONS%
   -Dweblogic.security.SSL.trustedCAKeyStore=@CUSTOM_TRUS
   T_KEY_STORE

   set CLU_USER=@CLU_USER

   set RSA_IMS_HOME=@RSA_IMS_HOME

   set RSA_JAVA_HOME=@RSA_JAVA_HOME

   set PLATFORM_LIBS=@PLATFORM_LIBS
   ```

For example:

```
set BEA_HOME=C:\Program Files\RSA Security\RSA
Authentication Manager\

set WL_HOME=C:\Program Files\RSA Security\RSA
Authentication Manager\appcore

set WLS_HOME=%WL_HOME%\server

set JAVA_OPTIONS=%JAVA_OPTIONS%
-Dweblogic.security.TrustKeyStore=CustomTrust

set
JAVA_OPTIONS=%JAVA_OPTIONS%-Dweblogic.security.CustomT
rustKeyStoreFileName=C:\Program Files\RSA Security\RSA
Authentication Manager\jdk\jre\lib\security\cacerts

set JAVA_OPTIONS=%JAVA_OPTIONS%
-Dweblogic.security.SSL.trustedCAKeyStore=C:\Program
Files\RSA Security\RSA Authentication
Manager\jdk\jre\lib\security\cacerts

set CLU_USER=qeuser

set RSA_IMS_HOME=C:\Program Files\RSA Security\RSA
Authentication Manager\

set RSA_JAVA_HOME=C:\Program Files\RSA Security\RSA
Authentication Manager\jdk

set PLATFORM_LIBS=win32-x86
```

5. Generate the **classpath.jar** file.
   a. Change directories to ***RSA_AM_HOME*****/utils-7.1**.
   b. Type:

      ```
      rsautil generate-classpath
      ```

6. Export the managed secrets from RSA Authentication Manager 7.0 to a file named **secrets.prop**:
   a. On the primary instance, change directories to ***RSA_AM_HOME*****/utils**.
   b. Type:

      ```
      rsautil manage-secrets --action export --file
      etc\secrets.prop --file-password file_password
      ```

      where:

      - **secrets.prop** is the name of the managed secrets file.
      - *file_password* is the password for opening the managed secrets file.

7. Copy the **secrets.prop** file from the **utils/etc** directory to the **utils-7.1/etc** directory.
8. In the **utils-7.1/etc** directory, modify the **jndi.properties** file. Set the following:
   a. The Authentication Manager server hostname (FQN):

      com.rsa.appserver.hostname=*Auth_Mgr_server_fully_qualified_hostname*

   b. The database server hostname:

      com.rsa.db.hostname=*database_server_hostname*

c. The database server name:
com.rsa.db.instance=*database_server_name*

d. The database domain:
com.rsa.db.domain=*database_domain* (for example, ims.rsa)

e. The Oracle home location (Oracle only):
com.rsa.db.oracle.home=*Oracle_installation_directory* (for example, *RSA_AM_HOME*/db)

Note: On Windows, use double slashes (\\) and if there are spaces in the directory, use the short name notation.

9. Import the managed secrets from the **secrets.prop** file that you created in step 6 to **utils-7.1**:

   a. On the primary instance, change directories to ***RSA_AM_HOME*/utils-7.1**.

   b. Type:

```
   rsautil manage-secrets --action import
 --file etc\secrets.prop --file-password file_password
```

   where:

   - **secrets.prop** is the name of the managed secrets file that you created in step 6.
   - *file_password* is the password that you made for opening the managed secrets file.

10. Create a directory to contain all of the migration script files, such as C:\migration_scripts.

11. Copy all of the script files and directories to the migration script directory that you just created. Do the following:

   a. Copy everything from ***DVDDrive*:/auth_mgr/*platform*/dbscripts/config/ims/db/scripts/schema/oracle/migration** to C:\migration_scripts.

   b. Copy everything from ***DVDDrive*:/auth_mgr/*platform*/dbscripts/config/am/db/scripts/schema/migration** to C:\migration_scripts.

   Note: If prompted that this will overwrite the files, click **Yes** to overwrite the files.

   c. Copy all sql scripts (*.sql) from ***DVDDrive*:/auth_mgr/*platform*/ucm** to C:\migration_scripts/am70_71.
   where:

   - *DVDDrive* is the location of the RSA Authentication Manager 7.1 DVD.
   - *platform* is the platform, such as windows-x86.

12. Make all of the files in the migration script directory writable.

13. Stop the RSA Authentication Manager 7.0 server including all primary instances, replica instances, and server nodes, but keep the database running.

14. Update the migration scripts:
    a. In RSA Authentication Manager 7.1, change directories to ***RSA_AM_HOME*/utils**.
    b. Type:

```
rsautil migrate-amapp --action updateScripts -d
migration_scripts_directory -V
```

15. Initialize migration on the replica instance:
    a. On the replica instance, change directories to ***RSA_AM_HOME*/utils-7.1**.
    b. Type:

```
rsautil migrate-amapp -a initMigrationOnReplica
-d migration_scripts_directory -V
```

16. Enable runtime data capture on each replica instance:
    a. On the replica instance, change directories to ***RSA_AM_HOME*/utils-7.1**.
    b. Type:

```
rsautil migrate-amapp -a backupAudit
-d migration_scripts_directory -V
```

17. Back up the replica instance internal database to a file named **replica_backup.bak**:
    a. On the replica instance, change directories to ***RSA_AM_HOME*/utils-7.1**.
    b. Type:

```
rsautil migrate-amapp -a backupReplica
-f replica_backup.bak -d migration_scripts_directory
-V
```

    c. Navigate to ***RSA_AM_HOME*/utils-7.1** and make sure that no errors are recorded in the backup log file. If errors are present, make any necessary changes and run the backupPrimary action again.

Performing an Upgrade on a Replica Instance

To install RSA Authentication Manager 7.1 on the replica instance:

1. If you are upgrading Authentication Manager on the same machine, do the following:

   Note: This step is not necessary if you are installing RSA Authentication Manager 7.1 on a new machine.

   a. Copy **backup.secrets**, **backup.bak**, and the backup log file to a safe location outside of the installation.

   b. Uninstall Patch 7.0.4.

   c. Uninstall RSA Authentication Manager 7.0.

      For instructions on uninstalling Authentication Manager, see Chapter 12, "Removing RSA Authentication Manager."

2. Install RSA Authentication Manager 7.1 on the replica instance.

   Note: Use the replica package file generated by the RSA Authentication Manager 7.1 primary and use the same master password that you used for RSA Authentication Manager 7.0.

   For instructions on installing a replica instance, see Chapter 4, "Installing a Replica Instance."

3. Stop the RSA Authentication Manager 7.1 servers including all primary instances, replica instances, and server nodes. Keep the database running.

Migrating User Data on a Replica Instance

Important: If you are installing the database server on a separate machine, the following steps must be performed on the database server. Otherwise, perform the following steps on the RSA Authentication Manager 7.1 primary server.

To migrate the user data on the replica instance, import captured runtime data on the replica instance:

1. Copy the **replica_backup.bak** file to a directory. For example, C:\temp.
2. Create a directory to contain all of the migration script files, such as C:\migration_scripts.
3. Copy all of the script files and directories to the migration script directory that you just created. Do the following:
    a. Copy everything from ***DVDDrive*****:/auth_mgr/*****platform*****/dbscripts/config/ims/db/scripts/schema/oracle/migration** to C:\migration_scripts.
    b. Copy everything from ***DVDDrive*****:/auth_mgr/*****platform*****/dbscripts/config/am/db/scripts/schema/migration** to C:\migration_scripts.

    Note: If prompted that this will overwrite the files, click **Yes** to overwrite the files.

    ---

    c. Copy all sql scripts (*.sql) from ***DVDDrive*****:/auth_mgr/*****platform*****/ucm** to C:\migration_scripts/am70_71.
    where:
    - *DVDDrive* is the location of the RSA Authentication Manager 7.1 DVD.
    - *platform* is the platform, such as windows-x86.
4. Make all of the files in the migration script directory writable.
5. Update the migration scripts:
    a. In RSA Authentication Manager 7.1, change directories to ***RSA_AM_HOME*****/utils**.
    b. Type:

    ```
    rsautil migrate-amapp -a updateScripts -d
    migration_scripts_directory -V
    ```
6. Import the replica database:
    a. In RSA Authentication Manager 7.1, change directories to ***RSA_AM_HOME*****/utils**.
    b. Type:

    ```
    rsautil migrate-amapp -a importReplica
    -f C:\temp\replica_backup.bak -d
    migration_scripts_directory -V
    ```

    where *C:\temp\* is the directory that you created in step 1.

7. Import the captured audit data to the replica database:
    a. In RSA Authentication Manager 7.1, change directories to ***RSA_AM_HOME*/utils**.
    b. Type:

```
rsautil migrate-amapp -a importAudit
-f replica_backup.bak -d migration_scripts_directory
-V
```

8. Run the migrateAudit command:
    a. In RSA Authentication Manager 7.1, change directories to ***RSA_AM_HOME*/utils**.
    b. Type:

```
rsautil migrate-amapp -a migrateAudit -d
migration_scripts_directory -V
```

9. Generate a replica instance migration report:
    a. In RSA Authentication Manager 7.1, change directories to ***RSA_AM_HOME*/utils**.
    b. Type:

```
rsautil migrate-amapp -a reportReplica -d
migration_scripts_directory -V
```

10. Start all of the servers on the primary and replica instances.

Upgrading a Server Node

When you upgrade Authentication Manager from version 7.0 to 7.1 on a server node, you must uninstall RSA Authentication Manager 7.0, generate a server node package, and install RSA Authentication Manager 7.1.

To upgrade a server node:

1. Uninstall RSA Authentication Manager 7.0.

    For instructions on uninstalling Authentication Manager, see Chapter 12, "Removing RSA Authentication Manager."

2. Generate a node package file on the Authentication Manager 7.1 primary or replica instance. Do the following:
    a. On the primary or replica instance, change directories to ***RSA_AM_HOME*/utils**.
    b. Type:

```
rsautil manage-nodes -n hostname -u admin-id -a
add-node
```

    where *hostname* is the fully qualified hostname of the server node host.

    c. When prompted, enter your Super Admin password.

   d. When prompted, enter your master password.
   e. The message “Adding node to cluster” appears.
   f. Verify that the directory contains a file named ***hostname*-node.pkg**, where *hostname* reflects the hostname value you specified for the --node_host argument.

3. Transfer the node package file to the target host. Note the location on the target host where you copy the package file. This information, along with the master password, is required during installation.

   Note: RSA recommends that you transfer the package through a secure network or by removable media.

4. Install RSA Authentication Manager 7.1 on the server node.

   Note: Use the node package file generated by the RSA Authentication Manager 7.1 primary and use the same master password that you used to install RSA Authentication Manager 7.1 primary instance.

   For instructions on installing a server node, see Chapter 5, “Installing a Server Node.”

Verifying the Upgrade

To verify that the upgrade was successful:

1. Access the Security Console web application from supported browsers by entering the Security Console URL as shown:

   `https://<fully qualified domain name>:7004/console-ims/`

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

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

2. Log on to the Security Console using the Super Admin user name and password.

9

Performing Post-Installation 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

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 108.
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 four 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 109.
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 109.
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

You must ensure that the clocks for the primary instance and replica instance are synchronized.

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

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

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

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

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 Cluster Administration Server
- 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. If you have server nodes, stop the server nodes before stopping 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 Cluster Administration Server:[OK  ]
RSA Authentication Manager Proxy Server: [  OK  ]
RSA Authentication Manager: [  OK  ]
RSA Authentication Manager Node Manager: [  OK  ]
```

To stop the RSA Authentication Manager services:

Note: Stop the primary instance. If you have server nodes, stop the server nodes before stopping 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 Cluster Administration Server:[OK  ]
RSA Authentication Manager Node Manager: [OK]
RSA Authentication Manager Database Server: [  OK  ]
RSA Authentication Manager Database Listener: [  OK  ]
RSA Authentication Manager Node Manager: [  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 these steps:

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 name of the Super Admin specified during installation.
3. At the password prompt, type the Super Admin password specified during installation.

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*.

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*/utils/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*/utils/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 around maintaining the master password.

The master password is needed to access the Operations Console.

When you add replica instances and additional server nodes to your system, you must use the master password to install them. After installation, the new server nodes or replica database servers 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 chosen during installation of the primary instance, it is easiest to change it before adding replica instances and server nodes. If you change it later, you must run the manual password change procedure on each replica instance database server and server node.

You can 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/*****utils**.
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 Authentication Manager server node, you are only changing it for that one server node. If you want the new master password to be common among all server nodes in an instance, you must manually change it on each server node.

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*/utils**.
2. Type:

   ```
   rsautil manage-secrets --action listall
   ```
3. When prompted, type your master password.
   The system displays the list of your internal system passwords.

To change the system passwords, you need to specify the actual property name or key, for the password and its value. Use the --action listkeys command to find the key for the system password you want to change.

To change system passwords using manage-secrets:

1. From a command prompt, change directories to ***RSA_AM_HOME*/utils**.
2. Type:

   ```
   rsautil manage-secrets --action set property_name
   property_value
   ```

   where:

   - *property_name* is the password you want to change.
   - *property_value* is the new password.

   For example:

   rsautil manage-secrets --action set *com.rsa.appserver.admin.password administrator_password*
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 installer-generated certificates with your own. Use the Manage SSL Certificates utility together with your certificate authority to replace the default certificates.

The variables referenced in this section are listed in "Options for manage-ssl-certificate" on page 117.

To replace the default certificates:

Note: Use this same procedure on any replica instances or server nodes that you have in your deployment.

1. From a command prompt, change directories to ***RSA_AM_HOME*****/utils**.
2. Type the command to generate public and private keypairs in a keystore using the --genkey option, entering your master password when prompted:

```
rsautil manage-ssl-certificate --genkey --alias
key-entry-alias --keypass key-entry-password --dname
certificate-distinguished-name --keystore
keystore-file-path
```

For example:

```
rsautil manage-ssl-certificate --genkey --alias myalias --keypass mykeypass
--dname CN=myserver.mycompany.com,OU=AM,L=mycity,C=US
--keystore "C:/Program Files/RSA Security/RSA Authentication
Manager/server/security/myServerName.jks"
```

Note: The *certificate-distinguished-name* is usually the name of the Authentication Manager server machine.

---

3. Type the command to create a certificate signing request to submit to a certificate authority using the public or private key, entering your master password when prompted:

   ```
   rsautil manage-ssl-certificate --certreq --alias
   key-entry-alias --keypass key-entry-password --keystore
   keystore-file-path --csr-file CSR-output-file-path
   ```

   For example:

   ```
   rsautil manage-ssl-certificate --certreq --alias myalias --keystore "C:/Program
   Files/RSA Security/RSA Authentication
   Manager/server/security/myServerName.jks" --csr-file
   C:/certificates/mycertreq.pem
   ```

4. Submit the request to your certificate authority, and create a signed server certificate. See your certificate authority documentation for more information.
5. Physically transfer the signed server certificate to the Authentication Manager database server (primary or replica).
6. Use the Manage SSL Certificate utility to import the signed server certificate into both the root keystore and server keystore, entering your master password when prompted. At ***RSA_AM_HOME*****/utils**, type:

   ```
   rsautil manage-ssl-certificate --import --trustcerts
   --ca-alias myCAAlias --ca-cert-file
   C:/certificates/myCACertificate.cer --ca-keystore
   RSA_AM_HOME/server/security/root.jks
   ```

   and

   ```
   rsautil manage-ssl-certificate --import --alias
   key-entry-alias --cert-file
   C:/certificates/myServerCertificate.cer --keypass
   mykeypass --keystore
   RSA_AM_HOME/server/security/hostname.jks
   ```

Note: If your path includes spaces, use quotes around it in this command.

---

7. Configure the application server for the new key alias and password, entering your master password when prompted. Type:

```
rsautil manage-ssl-certificate --config-server
--alias key_entry_alias --keypass key_entry_password
--server-name server_node_name_server
```

where:

- *key_entry_alias* is the alias for the key entry, for example, myalias.
- *key_entry_password* is the password for the key entry, for example, mykeypass.
- *server_node_name*_server is the name of the server node to use the new private key, for example, *abc*_server.

Note: For the primary instance, you need to configure the proxy server and application server.

8. Restart the server for the config-server changes to take effect.

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.
--debug	-x	Displays debugging messages.
--dname		Specifies the distinguished name of the certificate. This is usually the name of the server host.
--generate-cert-request	-g	Generates key and CSR at the same time.
--genkey		Generates public and private key pairs.
--help	-h	Displays help for this utility.

Flag	Alternate Flag	Description
--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.
--master-password	-m	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).
--update-server-certs	-u	Imports the CA and the server certificates, and the updates to the application server configurations at the same time.
--version	-v	Displays the version and copyright 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 130.

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:

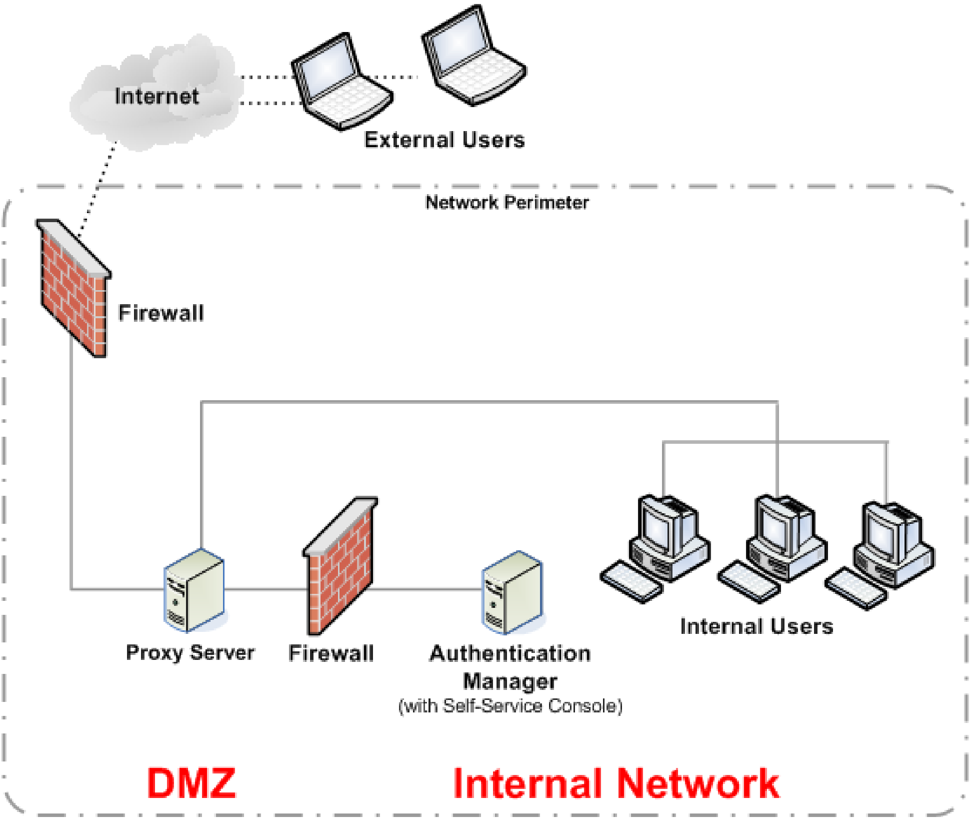
https://<*fully qualified domain name*>:7004/console-selfservice

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 illustrates a basic network setup with Self-Service Console traffic directed through a proxy server.


Internet
External Users
Network Perimeter
Firewall
Proxy Server
Firewall
Authentication Manager
(with Self-Service Console)
Internal Users
DMZ
Internal Network

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 post-installation tasks that you might need to perform to complete the RADIUS configuration.

Modifying the RADIUS 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 version 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 158 for troubleshooting tips.

10 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 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 129.

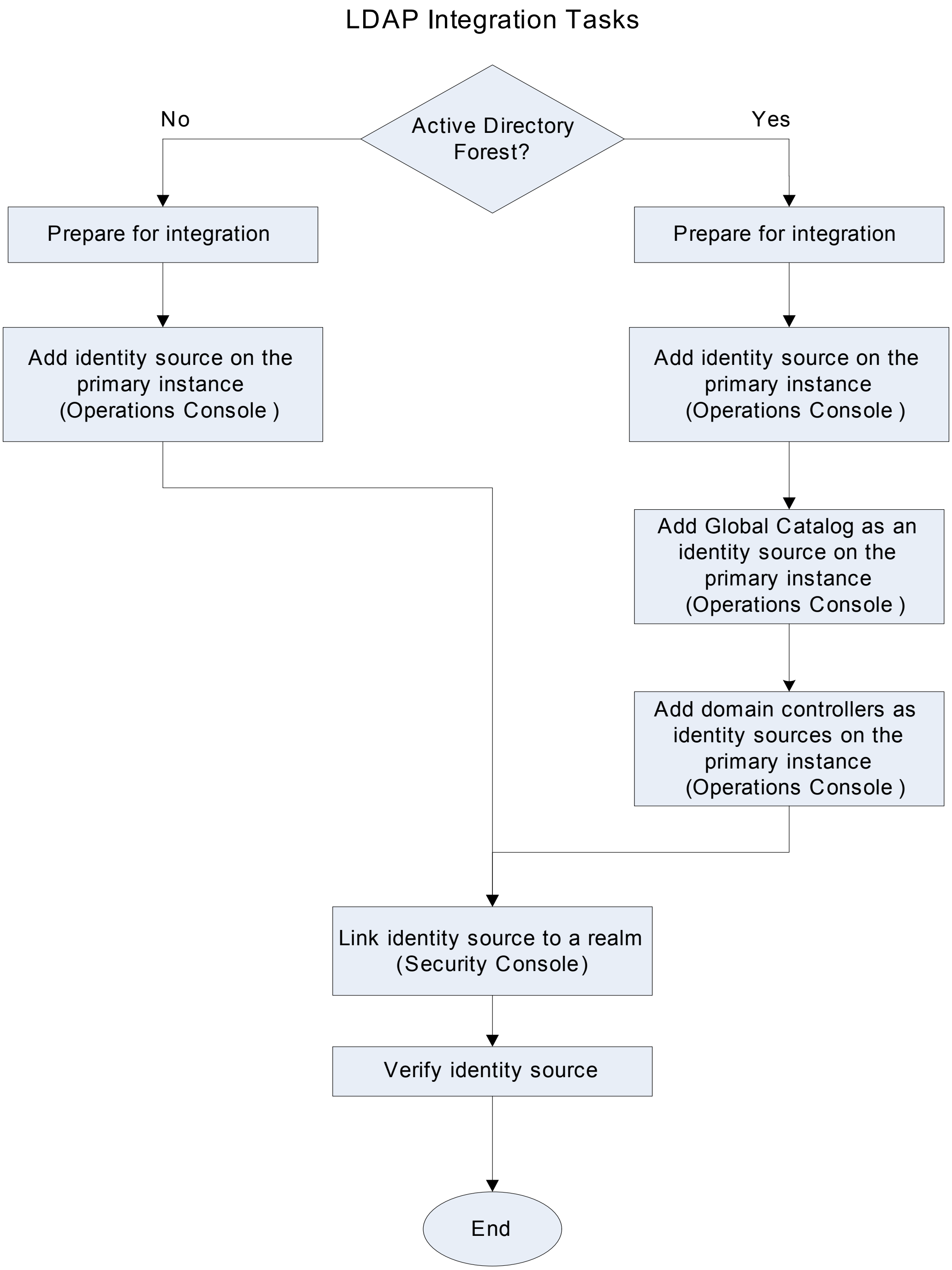
Important: Many of the tasks in the following sections require detailed knowledge of LDAP and your directory server deployment. RSA recommends that these tasks be performed by someone with LDAP experience and familiarity with the directory servers to be integrated.

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 130.
Consider the password policy (Active Directory only).	"Password Policy Considerations" on page 131.
Verify your domain functional level (Active Directory only).	"Supporting Groups" on page 131.
Verify that the Active Directory server name is a valid DNS name (Active Directory Forest only).	"Active Directory Forest Considerations" on page 131.
2. Add the identity source.	"Adding an Identity Source" on page 132.
3. Link the identity source to a realm.	"Linking an Identity Source to a Realm" on page 136.
4. Verify the LDAP integration.	"Verifying the LDAP Identity Source" on page 137.

The following figure illustrates the process flow for integrating an LDAP directory as an identity source.


LDAP Integration Tasks
Active Directory Forest?
No
Yes
Prepare for integration
Prepare for integration
Add identity source on the primary instance (Operations Console)
Add identity source on the primary instance (Operations Console)
Add Global Catalog as an identity source on the primary instance (Operations Console)
Add domain controllers as identity sources on the primary instance (Operations Console)
Link identity source to a realm (Security Console)
Verify identity source
End

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 132. Then, in case of 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 132.

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. Click **Deployment Configuration > 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 132, 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 name 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:
    1. 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.
    2. 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.
    3. In the **Directory User ID** field, enter the directory administrator user ID.
    4. 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.
    5. 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:
    1. In the **User Base DN** field, enter the base DN for directory user definitions.
    2. In the **User Group Base DN** field, enter the base DN for directory user group definitions.
    3. Optional. Select **Read-only** to prevent administrators from using the Security Console to edit the users and groups in the identity source.
    4. 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**.
    5. 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.
    6. 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.

11

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 Chapter 10, "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**.

12 Removing RSA Authentication Manager

- Removing RSA Authentication Manager Servers
- Removing a Server Node
- Removing a Replica Database Server
- Rebalancing Contact Lists
- Removing a Primary Database Server
- Removing an RSA RADIUS Server
- Removing a Standalone Database Server

Removing RSA Authentication Manager Servers

To remove all servers from a deployment, including server nodes, replica database servers, and the primary database server, remove the server nodes in this order:

1. Server nodes
2. Replica database servers
3. Primary database server

For example, if you are removing a replica instance with server nodes, first remove the server nodes and then the replica database server.

The order is important because you must remove server node information from the database server before removing the server node itself. In a replica database server removal, the reference information is removed automatically from the primary database server by the removal program.

After removing server nodes from a replica instance or removing a replica database server, perform the tasks described in "Rebalancing Contact Lists" on page 148.

Removing a Server Node

To remove a server node on Windows:

1. Make sure that you have stopped all Authentication Manager services on the server node server.
2. From a command prompt on the primary server, change directories to ***RSA_AM_HOME*/utils.**
3. Type:

```
rsautil manage-nodes --action rem-node --node-host
node_hostname
```

4. When prompted, enter your administration password.
5. When prompted, enter the master password.

   The message "Removing node from cluster" appears.
6. Switch to the server node that you want to uninstall.
7. From the Windows Control Panel, click **Add/Remove Programs**.
8. From the program list, select RSA Authentication Manager, and click **Remove**.

   The GUI uninstaller program displays on your screen.
9. Restart the host machine of the database server and the remaining server nodes.
10. Perform the tasks described in "Rebalancing Contact Lists" on page 148.

To remove a server node on Solaris or Linux:

1. Make sure that you have stopped all Authentication Manager services on the server node server.
2. From a command prompt on the primary server, change directories to ***RSA_AM_HOME*/utils.**
3. Type:

   ```
   rsautil manage-nodes --action rem-node --node-host
   node_hostname
   ```
4. When prompted, enter your Super Admin password.

   The message "Removing node from cluster" appears.
5. Switch to the server node.
6. Change directories to ***RSA_AM_HOME*/uninstall**.
7. Type:

   ```
   uninstall
   ```

   The GUI uninstaller program is displayed on your screen. The removal program runs and then prompts you to run an important script as root user.
8. Run this script to finish removing Authentication Manager.
9. Restart the host machine of the database server and the remaining server nodes.
10. Perform the tasks described in "Rebalancing Contact Lists" on page 148.

Removing a Replica Database Server

Make sure that Authentication Manager is running on the primary instance and the replica database server is able to connect to the primary database server before you begin removal.

Note: If you have RSA RADIUS installed on the replica server, it is automatically removed when you remove the replica database server.

To remove on Windows:

1. From the Windows Control Panel, click **Add/Remove Programs**.
2. From the program list, select RSA Authentication Manager, and click **Remove**.

   The GUI uninstaller program displays on your screen.
3. Click **Next** > **Uninstall**.
4. To verify that the replica database server has been successfully removed, at a command prompt on the primary database server change directories to ***RSA_AM_HOME*/utils**, and type:

   ```
   rsautil manage-replication -a list
   ```

   Make sure that the replica database server you removed does not display in this listing.
5. Restart the machine.
6. Perform the tasks described in "Rebalancing Contact Lists" on page 148.

To remove on Solaris or Linux:

1. Change directories to ***RSA_AM_HOME*/uninstall**.
2. Type:

   ```
   ./uninstall.sh
   ```

   The GUI removal program displays on your screen.
3. When prompted, select the components that you want to remove, and click **Finish**.

   The removal program runs and then prompts you to run an important script as root user.
4. Run the script to finish removing Authentication Manager.
5. To verify that the replica database server has been successfully removed, at a command prompt on the primary database server, change directories to ***RSA_AM_HOME*/utils**, and type:

   ```
   rsautil manage-replication -a list
   ```

   Make sure that the replica database server you removed does not display in this listing.
6. Restart the machine.
7. Perform the tasks described in "Rebalancing Contact Lists" on page 148.

Manual Cleanup for Unsuccessful Removal

If the primary database server is unavailable at removal time, the error message, “Replica uninstall failed. You may need to perform manual replica cleanup on the primary” may appear.

To perform manual cleanup:

1. At a command prompt on the primary database server, type:

   ```
   rsautil manage-replication –a remove-replica –n name of
   the replica site
   ```

2. To verify that the replica database server has been successfully removed and cleanup has succeeded, type:

   ```
   rsautil manage-replication –a list
   ```

   Make sure that the replica database server you removed does not display in this listing.

Rebalancing Contact Lists

After you remove the replica database server and any server nodes from the replica instance, rebalance the contact lists in the primary instance RSA Security Console. This removes the references to the removed replica instances.

To automatically update your contact lists:

1. Click **Access** > **Authentication Agents** > **Authentication Manager Contact List** > **Automatic Rebalance**.
2. Click **Rebalance**.

Removing a Primary Database Server

Make sure that Authentication Manager is running before you begin removal.

Note: If you have RSA RADIUS installed on the primary server, it is automatically removed when you remove the primary database server.

To remove on Windows:

1. From the Windows Control Panel, click **Add/Remove Programs**.
2. From the program list, select **RSA Authentication Manager**, and click **Remove**.

   The GUI-based uninstaller program is displayed on your screen.
3. Click **Next** > **Uninstall**.

To remove on Solaris or Linux:

1. Change directories to ***RSA_AM_HOME*/uninstall**.
2. Type:

   ```
   uninstall
   ```

   The GUI removal program displays on your screen.
3. Click **Next** > **Uninstall**.

   The removal program runs and then prompts you to run an important script as root user.
4. Run the script to finish removing Authentication Manager.
5. Restart the machine.

Removing an RSA RADIUS Server

The method of removing the RSA RADIUS server is the same as removing a database server.

Note: A RADIUS server installed on the same machine as the version 7.1 software is removed when you uninstall Authentication Manager. You cannot uninstall the RADIUS server itself without also uninstalling Authentication Manager.

Removing a Standalone Database Server

To remove a standalone database server on Windows:

1. Verify that the Authentication Server is running.
2. Click **Start** > **Control Panel** > **Add/Remove Programs**.
3. On the listing for RSA Authentication Manager, click **Remove**.

   The GUI uninstaller program is displayed on your screen.
4. When prompted, select the components that you want to remove, and click **Finish**.

To remove a standalone database server on Solaris or Linux:

1. Verify that the Authentication Server is running.
2. Change directories to ***RSA_AM_HOME*****/uninstall**.
3. Type:

   ```
   uninstall.sh
   ```

   The GUI removal program is displayed on your screen.
4. When prompted, select the components that you want to remove, and click **Finish**.
5. The removal program runs and then prompts you to run an important script as root user. Run this script to finish removing Authentication Manager.
6. Restart the machine.

13 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
- Multicast Network Communication Fails
- 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
- Unable to Receive Multicast Packets Sent to Self

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. If you attempt to install from a network drive on a Windows machine, or to copy the contents of the DVD or the ISO image from a non-Windows 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, you must perform the following procedure:

1. Copy the contents of the DVD, or the ISO image, to the network machine.
2. From the Windows sub-directory, change the permissions of the **ora10g2** directory using the following command:

   ```
   chmod -R a+rx ora10g2
   ```

3. Copy the 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.

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_*YYMMDDHHmmSS*/rsa_am_install.log**.
- Unsuccessful installation log (installation failures) - ***Temp*/rsa_am_*YYMMDDHHmmSS*/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_*YYMMDDHHmmSS*/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 Can Not 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. For example, if you installed "Documentation Only" on the machine previously, and you want to now add a primary instance on the same machine, you must first uninstall the "Documentation Only" component and then install the primary instance.

If you installed the database on a separate machine, before you uninstall and reinstall, back up the Authentication Manager database, restore the database after reinstalling, and generate a new database package before installing the primary or replica instance.

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 RSA Authentication Manager Servers" on page 145.

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 173.

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.

Multicast Network Communication Fails

It may be difficult to detect whether server nodes in a cluster are communicating properly over the network. You might notice large numbers of expired JMS messages in the application server logs. Check the ***RSA_AM_HOME*/server/servers/*servername*_server/ogs/*servername*_server.log** file.

You can use the Multicast Network Test utility, test-multicast, to troubleshoot problems that may occur as a result of deploying Authentication Manager in a clustered environment. For more information, see "Multicast Network Test Utility" on page 187.

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**.

Unable to Receive Multicast Packets Sent to Self

If the following error message appears during installation, you likely have a firewall running on the machine on which you are installing that is either blocking the Internet Group Management Protocol (IGMP) or blocking the range of ports used to multicast.

```
Unable to receive multicast packets sent to self. Please
check network configuration.
```

Multicast is used by version 7.1 for certain communications between server nodes and within a single server node. The installer checks to see if the multicast protocol, IGMP, can communicate on certain ports and displays this message when the test fails.

To fix this problem, you must do the following:

- Allow the IGMP to communicate through your firewall.
- Open ports 7000 to 8000 on the firewall.

Perform these tasks only on the firewall running on the installation machine. You do not need to allow the IGMP to communicate or open these ports on any firewall that protects your network from external threats.

Note: If you configure the firewall as described and still receive the error message, run the installer from a command prompt using the -V FORCE_CONTINUE=true command option. The GUI installer runs and allows you to choose to continue the installation.

A Deployment Checklist

Pre-Installation

Element	Description	Your Plan
License or option type	• Base Server • Enterprise Server • Business Continuity option • Credential Manager Provisioning option	
Platform	• 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) • Red Hat Enterprise Linux 4.0-1 ES (32-bit) • Red Hat Enterprise Linux 4.0-1 ES (64-bit) • Solaris 10 (64-bit) **Note:** RADIUS is not supported on 64-bit Windows and Linux systems.	
Master password		
Super Admin user name	Authentication Manager Super Admin user name	
Super Admin password	Authentication Manager Super Admin password	

Installation

Element	Description	Your Plan
Primary instance	Physical location	
	Name and IP address of the database server	
	Name and IP address of any server nodes	
Replica instance	Number of instances	
	Physical location(s)	
	Name and IP address of the database server	
	Name and IP address of any server nodes	

Identity Source Configuration

Element	Description	Your Plan
Identity source	Number and type For example: • RSA Authentication Manager internal database – Same machine as primary – Standalone machine • Active Directory • Sun Java System Directory Server Select the identity sources to make available for self-service and provisioning	
LDAP	User defined unique identity source name	
	URL of the LDAP identity source	
	URL of the failover identity source (optional)	
	LDAP server user name	
	LDAP server password	
	Read/write access or read-only access	

Administrative Configuration

Element	**Description**	**Your Plan**
Realm	Number	
	Names	
Security domain	Top-level name **Note:** The top-level security domain in a realm has the same name as the realm. This name cannot be changed.	
	Lower-level names	
Tokens	Number and type For example: • RSA SecurID token • RSA Smart Card • RSA SecurID Software Toolbar Token • RSA USB token	
	Contact person for obtaining token seed records	
Policies	Number of custom policies	
	Names of security domains requiring custom policies	

Element	Description	Your Plan
	Method of PIN creation For example: • System-generated • User-generated	
	Length of PINs (4-8 characters)	
	Character restrictions on PINs	
	Number of failed authentication attempts allowed before user lockout	
	Method of unlocking locked user. For example: • Automatic • Manual	
	Password lifetime	
	Maximum and minimum password length	
	Number of restricted old passwords	
	Excluded words dictionary	
	Character restrictions on password	
	Lifetime of Emergency Access Tokencodes	
	Behavior of Emergency Access Tokencode when token is recovered For example: • Deny authentication with the token • Allow authentication with the token and disable the Emergency Access Tokencode • Allow authentication with the token only after the Emergency Access Tokencode expires	

Administrative Configuration for Self-Service and Provisioning

Element	Description	Your Plan
Logon Method	• RSA password • LDAP password • SecurID token	
User Enrollment	• Select identity sources. • Select security domains. • Customize user profiles. • Customize the RSA Self-Service Console Home page.	
Self-Service Troubleshooting	Authentication methods: • Security questions • Passwords • None Number of self-service authentication attempts: • Allow an unlimited number of failed self-service troubleshooting authentication attempts. • Allow a specified number of failed attempts within a specified number of days, hours, or minutes. Method of unlocking locked user for self-service troubleshooting: • Unlock accounts after users have exceeded the number of failed attempts specified. • Allow the system to automatically unlock accounts after a specified number of days, hours, or minutes.	
Proxy Server for self-service requests	Set up proxy server in your network’s DMZ to protect Authentication Manager.	

Element	**Description**	**Your Plan**
Additional Administrative Configuration for Provisioning		
Workflows	For each type of request, set: • One or two approval steps • One distribution step for hardware token requests • Optionally, add one distribution step for software token requests	
Roles for Requests	• Create approvers • Create distributors	
User Group Membership	Select user group membership to make protected resources available for requests. For example: • HR • Finance	
Tokens	Select tokens to make available for provisioning requests. For example: • RSA SecurID token • RSA Smart Card • RSA SecurID Software Toolbar Token • RSA USB token Optionally, select a default token. Decide when to allow requests for replacement tokens. Optionally, make the on-demand tokencode service available. Optionally, make the on-demand tokencode service the default.	

Element	**Description**	**Your Plan**
Hardware token distribution	Plan distribution reports for tokens. Optionally, customize distribution reports. Plan how to collect shipping addresses from users. • Map an attribute in an directory server for the shipping address. • Create a custom attribute in an directory server. • Allow users to enter shipping addresses.	
Software token distribution	Protect token files. Decide the file format: • ZIP format • SDTID format	
E-mail notifications	Set up an e-mail server: • Determine which SMTP port to use. • Decide the e-mail address from which Credential Manager sends e-mail notifications. • Determine if the e-mail server requires User ID and password. Optionally, customize e-mail templates. Select e-mail notification recipients. • All workflow participants • Super Admins • Workflow participants in the parent security domain	

Element	Description	Your Plan
Emergency access	Allow users to get emergency access. Set method to authenticate: • Temporary fixed tokencode (TFT). • One-time tokencode (OTT). • Decide the number of one-time tokencodes to issue in a set. • On-demand tokencode. Set the lifetime of emergency access tokencodes. • For lost or broken tokens • For temporarily unavailable tokens Method if a missing token is recovered. • 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.	

Post-Installation

Element	Description	Your Plan
Resources to protect	For example: • File servers • Databases • Identity sources	
Agents	Number	
	Physical location of agents	
	Name and IP address of agents	

B

Command Line Utilities

- Overview
- Collect Product Information Utility
- Data Migration Utility
- Generate RADIUS Package Utility
- Manage Nodes Utility
- Manage Secrets Utility
- Manage SSL Certificate Utility
- Multicast Network Test Utility
- Setup Replication 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*/utils** 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
Multicast Network Test	master password
Register Custom Extension	master password & Super Admin
Restore Super Admin	master password
Set Trace	Super Admin
Setup Replication	master password

Utility	Required Credentials
Store	master password
Update Instance Nodes	master password
User Groups and Token Bulk Requests	master password & Super Admin
Verify Archive Log	master password

[1] The 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.

Flag	Alternate Flag	Description
	--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:

```
rsautil 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	Specifies an action to perform. Select one of the following: **initMigration.** Initialize RSA_MIGRATION_ADMIN and related migration packages. **enableAudit.** Enable data capture on all replica instances. **backupPrimary.** Back up primary instance data. **importPrimary.** Import primary instance data. **migratePrimary.** Migrate primary instance data. **initMigrationOnReplica.** Initialize additional migration configuration data on the replica instance. **backupAudit.** Back up captured runtime data on the replica instance. **backupReplica.** Back up replica instance data. **importReplica.** Import replica instance data. **migrateReplica.** Migrate replica instance data. **importAudit.** Import captured runtime data to the replica instance. **enableReplication.** Enable replication after reverting to the previous version. **rollbackAudit.** Import captured runtime data to the replica instance after reverting to the previous version. **reportPrimary.** Generate primary instance migration report. **validatePrimary.** Validate primary instance. **reportReplica.** Generate replica instance migration report. **validateReplica.** Validate replica instance.
-d	--scriptDir	The SQL script directory.

Flag	Alternate Flag	Description
-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.

Generate RADIUS Package Utility

Use the Generate RADIUS Package utility, gen-radius-pkg, to gather information from the Authentication Manager primary server and make it available to the RSA RADIUS primary and replica standalone servers in your deployment.

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

Using the Generate RADIUS Package Utility

To create a RADIUS package file:

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

   ```
   rsautil gen-radius-pkg -m master-password
   ```

   where *master-password* is the master password for the encrypted properties file, which you set when installing the Authentication Manager primary instance. (By default, this is the same as the Super Admin password, unless the Super Admin password was changed after installation.)

   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.

When the package file creation is complete, the message "Successfully generated *AMprimaryhost*-radius.pkg" appears and the package file is output to the ***RSA_AM_HOME*/utils** directory as ***AMprimaryhost*-radius.pkg**.

Options for gen-radius-pkg

The following table describes the options for this utility.

Flag	Alternate Flag	Description
-o	--overwrite-pkg	Overwrites RADIUS package file if one exists.
-I	--interactive	Enters all values interactively.
-m	--master-password	Master password for the encrypted properties file.
-v	--version	Displays the version and copyright information.
-h	--help	Displays help for this utility.

Manage Nodes Utility

Use the Manage Nodes utility, manage-nodes, to gather information from the primary or replica database server and make it available to the server node host.

Using the Manage Nodes Utility

To use manage-nodes:

1. From a command prompt on the host of the database server, change directories to ***RSA_AM_HOME*/utils**.
2. Type:

   ```
   rsautil manage-nodes --node-host hostname --action
   add-node
   ```

   where *hostname* is the fully qualified hostname of the server node host.

   For relevant options, see the following section, "Options for manage-nodes."

   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.

3. When prompted, enter your master password.

   The message "Adding node to cluster" appears.

4. Verify that the directory contains a file named ***hostname*-node.pkg**, where *hostname* reflects the hostname value you specified for the --node-host argument.

Options for manage-nodes

The following table describes the options for this utility.

Flag	Alternate Flag	Description
-n	--node-host	Fully qualified hostname of the new server node.
-i	--node-ip	IP address for the new server node (optional).
-m	--master-password	Master password for the encrypted properties file.
-u	--admin-uid	Administrator's User ID. Default: admin.
-p	--admin-password	Administrator's password.
-I	--interactive	Allows you to enter all values interactively.
-o	--overwrite	Overwrites the existing node package.
-a	--action	

Flag	Alternate Flag	Description
	add-node	Adds a server node to the cluster.
	rem-node	Removes a server node from the cluster.
	list-nodes	Lists the server nodes in this cluster.
-v	--version	Displays the version and copyright information.
-h	--help	Displays help for this utility.

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:

  ```
  rsautil manage-secrets --action change
  --new-password new-master-password
  ```

- To recover the system fingerprint-encrypted file after the host machine is reconfigured, type:

  ```
  rsautil manage-secrets --action recover
  ```

- To load a number of keys (in bulk) from a plain text file into an encrypted file, type:

  ```
  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	Specifies an action to perform. Select one of the following: **import**. Imports a password-protected file to be system fingerprint encrypted. A file can be imported to the same system or a different system. **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. **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. **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. **load**. Loads a plain text properties file into an encrypted file. **list**. Displays a subset of the secrets in the file. By default, this action only displays the CmdClient user name and password. **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. **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. **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.

Flag	Alternate Flag	Description
-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.
-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*/utils**.
2. Type:

   ```
   rsautil 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 key_entry_alias --keypass key_entry_password
  --dname "certificate_DN" --keystore keystore_path
  ```

  where:

  - *key_entry_alias* is the alias for the key entry, for example, myalias.
  - *key_entry_password* is the password for the key entry. The password must be at least six characters long, for example, mykeypass.
  - *"certificate_DN"* is the distinguished name of the certificate. This is usually the name of the server host, for example, "CN=myserver.mycompany.com,OU=AM,L=mycity,C=US".
  - *keystore_path* is the absolute path of the keystore file, for example, C:/bea/weblogic91/server/lib/wl_server_ keystore.jks.

- To create a certificate signing request (CSR), type:

  ```
  rsautil manage-ssl-certificate --certreq
  --alias key_entry_alias --keypass key_entry_password
  --keystore keystore_path
  --csr-file CSR_path
  ```

  where:

  - *key_entry_alias* is the alias for the key entry used in the previous task, for example, myalias.
  - *key_entry_password* is the password for the key entry, for example, mykeypass.
  - *keystore_path* is the absolute path of the keystore file, for example, C:/bea/weblogic91/server/lib/wl_server_ keystore.jks.
  - *CSR_path* is the absolute path of the CSR output file, for example, C:/certificates/mycertreq.pem.

- To import a CA root certificate to the keystore, type:

  ```
  rsautil manage-ssl-certificate --import --trustcacerts
  --ca-alias ca_alias
  --cert-file signed_certificate_file_path
  --keystore keystore_file_path
  ```

  where:

  - *ca_alias* is the alias for the CA certificate, for example, myCAalias.
  - *signed_certificate_file_path* is the absolute path of the signed certificate file from the CA, for example, C:/Certificates/certca187.cer.
  - *keystore_file_path* is the absolute path of the keystore file, for example, C:/bea/weblogic91/server/lib/DemoTrust.jks.

- To import a Signed Server Certificate to the keystore, type:

  ```
  rsautil manage-ssl-certificate --import
  --alias key_entry_alias
  --cert-file signed_certificate_file_path
  --keypass key_entry_password
  --keystore keystore_file_path
  ```

  where:

  – *key_entry_alias* is the alias for the key entry, for example, myalias.

  – *signed_certificate_file_path* is the absolute path of the signed certificate file from the CA, for example, C:/certificates/myServerCertificate.cer.

  – *key_entry_password* is the password for the key entry, for example, mykeypass.

  – *keystore_file_path* is the path of the keystore file, for example, C:/bea/weblogic91/server/lib/wl_server_keystore.jks.

- To configure the application server for the new key alias and password, type:

  ```
  rsautil manage-ssl-certificate --config-server
  --alias key_entry_alias --keypass key_entry_password
  --server-name server_node_name_server
  ```

  where:

  – *key_entry_alias* is the alias for the key entry, for example, myalias.

  – *key_entry_password* is the password for the key entry, for example, mykeypass.

  – *server_node_name*_server is the name of the server node to use the new private key, for example, abc_server.

  You must restart the application server for the changes to take effect.

Note: For the primary instance, you need to configure the proxy server and application server.

- To import certificates and configure the server at the same time, type:

```
rsautil manage-ssl-certificate --update-server-certs
--ca-alias CA_alias
--ca-cert-file CA_certificate_file_path
--alias key_entry_alias
--cert-file signed_certificate_file_path
--keypass key_entry_password
--keystore keystore_file_path
--server-name server_name
```

  where:

  - *CA_alias* is the alias for the CA certificate, for example, myCAalias.
  - *CA_certificate_file_path* is the absolute path of the CA certificate file*,* for example, C:/certificates/myCACertificate.cer.
  - *key_entry_alias* is the alias for the key entry, for example, myalias.
  - *signed_certificate_file_path* is the absolute path of the signed certificate file from the CA, for example, C:/certificates/myServerCertificate.cer.
  - *key_entry_password* is the password for the key entry, for example, mykeypass.
  - *keystore_file_path* is the absolute path of the keystore file, for example: C:/bea/weblogic91/ server/lib/wl_server_keystore.jks.
  - *server_name* is the application server node name, for example, myServerNode.

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.

Flag	Alternate Flag	Description
-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.
-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.

Multicast Network Test Utility

Use the Multicast Network Test utility, test-multicast, to troubleshoot problems that may occur as a result of deploying RSA Authentication Manager in a clustered environment. The utility verifies whether multiple machines can communicate with each other over the network using multicast.

Server nodes in a cluster must be in the same subnet as the primary database server and must be able to communicate. If the utility finds that two machines can communicate successfully, the problem does not lie in the network configuration.

Utility Messages

The utility displays ping-like messages verifying that the specified hosts can exchange messages. Normal execution messages are similar to these:

```
I (server100) sent message num 507
Received message 507 from server100
```

The utility displays an error message only if something is wrong, such as the port is in use or the resource is unavailable.

You must also know:

- If a host is misconfigured, the utility displays only the sending messages, not the receiving ones.
- The utility uses a multicast address which, unlike a regular IP address, is not assigned to a single machine. A multicast address causes the message to propagate throughout the subnet. Any host with a listener open on that multicast address can receive the message.

Examples

You can run the Multicast Network Test utility on multiple hosts in any order. For example, on the primary instance, you might type this command:

```
rsautil test-multicast --name Primary --address 237.1.2.3
```

The following messages appear:

```
I (Primary) sent message num 1
Received message 1 from Primary
```

On the replica instance, you might type this command:

```
rsautil test-multicast --name Replica --address 237.1.2.3
```

The following messages appear:

```
I (Replica) sent message num 1
Received message 1 from Replica
Received message 2 from Primary
```

The primary instance begins to receive these messages from the replica instance:

```
I (Primary) sent message num 2
Received message 1 from Replica
```

Using the Multicast Network Test Utility

To use test-multicast:

1. Open a new command shell, and change directories to ***RSA_AM_HOME*/utils**.
2. Type:

   ```
   rsautil test-multicast --name --address
   ```

   For relevant options, see the following section, "Options for test-multicast"

   For example, the command for a multicast test on MyServer on IP 237.1.2.3 and default port 7001:

   ```
   rsautil test-multicast --name MyServer --address 237.1.2.3
   ```

Note: To obtain the multicast address and port number, view the ***RSA_AM_HOME*/server/config/config.xml** file.

3. Review the output to verify that messages are sent and received. Normal output:

```
I (MyServer) sent message num 507
Received message 507 from Myserver
```

4. To stop testing, type:

```
CTRL-C
```

Until you stop it manually, the utility continues testing the connection.

Options for test-multicast

The following table describes the options for this utility.

Flag	Alternate Flag	Description
-n	--name	Required. Arbitrary system identifier used in test. Good values include the system hostname or IP address.
-a	--address	Required. The multicast IP address. Use the Authentication Manager multicast IP, 230.1.2.3, for testing.
-o	--port	The multicast port. Default: 7001.
-t	--timeout	The idle timeout.
-s	--send-pause	The pause between sending packets in seconds. Default: 2.
-c	--interface	Address of interface card (NIC) to use. If none is specified, attempts to use default NIC. Use this option if Authentication Manager is being deployed on multiple NICs.
-l	--time-to-live	Time-to-live of packets (number of hops). Default: 1.
-i	--interactive	Runs the utility in interactive mode.
-v	--version	Displays the version and copyright information.
-h	--help	Displays help for this utility.

Setup Replication Utility

Use the Setup Replication utility, setup-replication, to upgrade from RSA Authentication Manager 7.0 to RSA Authentication Manager 7.1.

Using the Setup Replication Utility

To use setup-replication:

1. On the primary instance, change directories to ***RSA_AM_HOME*/utils**.
2. Type:

   ```
   rsautil setup-replication options
   ```

   For relevant options, see the following section, "Options for setup-replication."

   For example, to view a list of currently configured replica instances, you specify the following option:

   ```
   rsautil setup-replication --action list
   ```

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 setup-replication

The following table describes the options for this utility.

Flag	Alternate Flag	Description
-a	--action	Specifies an action to perform. Select one of the following: **list**. Lists currently configured replica instances. **set-primary**. Sets up the primary instance for replication. **generate-data**. Generates the primary schema data dump file. **add-replica-online**. Adds a new replica instance to the deployment, synchronizing the data online. **add-replica-offline**. Adds a new replica instance to the deployment. You must synchronize the data offline in a separate step. **synch-online**. Reinitializes the replica instance with data from the primary instance and synchronizes the data online automatically. **synch-offline**. Reinitializes the replica instance with data from the primary instance. You must synchronize the data offline in a separate step.

Flag	Alternate Flag	Description
		report. Displays the status of replication for each instance. **cleanup**. Removes all replica configuration information from the primary instance and disconnects all instances in the replicated deployment. **cleanup-site**. Removes all replica information from a disconnected instance. **remove-primary**. Removes the primary instance from the deployment and disables replication. **remove-replica**. Removes the replica instance from the deployment and disconnects it from the primary instance. **attach-old-primary**. Adds a demoted primary instance to the deployment as a replica instance.
-f	--file	The location of configuration data files. Use a comma to separate each path. Enclose the path in double quotation marks. For example: "/dir/file1.sql, /dir1/file2.sql".
-G	--generate-sql	Generates SQL configuration scripts for each command, but does not execute the scripts. **Note:** Use this option only for an instance that is not yet configured. This applies to all action items. You can use these scripts as a reference to see how the system is configuring Oracle Streams for replication. However, do not use the scripts to set up an actual instance.
-h	--help	Displays help for this utility.
-i	--migration	Specifies migration mode. Used with the remove-replica and remove-primary actions when upgrading an installation.
-m	--master-password	Specifies the master password for the encrypted properties file.
-n	--name	Specifies the instance name of the replica being promoted, or the comma-separated instance name of replicas being removed. For example, "name1, name2".
-v	--version	Displays the version and copyright information.
-V	--verbose	Displays setup information during setup.

Glossary

Term	Definition
Active Directory	The directory service that is included with Microsoft Windows Server 2003 and Microsoft Windows 2000 Server.
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.
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.

Term	Definition
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.
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.

Term	Definition
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 and server nodes 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.
cluster	An instance consisting of a database server and one or more server nodes.
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.

Term	Definition
contact list	A list of server nodes 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.
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).

Term	Definition
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.
database server	The server where the database is installed.
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 tokencodes 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.
EAP	See extensible authentication protocol.

Term	**Definition**
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, multiple replica instances, and multiple server nodes.
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.
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.

Term	Definition
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.
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.)

Term	**Definition**
instance	One single database server, or a database server and one or more server nodes, acting as a single cohesive processing unit. An instance does not have to be a cluster, but a cluster is an instance.
instance ID	This ID identifies a single logical installation of a product or component. For example, in a non-clustered environment, it identifies the database server. In a clustered environment, it identifies the database server and the entire cluster of server nodes. Likewise for web agents, a single agent may have a unique instance ID or an entire server cluster may share a single instance ID.
instance name	The name assigned to an instance. It is either the hostname where a single server node is installed or the cluster name where the clustered instance is installed.
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.

Term	Definition
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.
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	A long-lived symmetric key that the agent uses to encrypt the data in the authentication request. 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.
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	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. An on-demand tokencode can only be used once, and you configure the lifetime of an on-demand tokencode. See on-demand tokencode service.

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.
server node	An installation of Authentication Manager on a single server host. Each instance has one server node that contains the internal database. You can add additional server nodes to an instance, if your license allows. The additional server nodes cannot operate alone because they do not contain the internal database.
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.

Term	**Definition**
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.
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	An administrator who has all permissions within the system. A Super Admin: • 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: • 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 *jdoe*.
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

- access control, 22
- Active Directory, 18
  - definition, 193
  - forest, 129
  - Global Catalog, 129
  - group membership, 131
  - large deployment example, 40, 41
  - MMC Extension, 139
  - password policy, 131
  - starting console, 143
- Active Directory forest
  - definition, 193
- Active Directory Global Catalog, 130
- AD. *See* Active Directory
- adjudicator
  - definition, 193
- administrative command
  - definition, 193
- administrative identity source, 129
- administrative role
  - definition, 193
- administrator
  - definition, 193
- Advanced Encryption Standard
  - definition, 193
- AES. *See* Advanced Encryption Standard
- agent
  - contact lists, 148
  - definition, 193
  - documentation, 24
  - download software, 22
  - supported, 22
- agent auto-registration utility
  - definition, 193
- agent host
  - definition, 193
- Agent Protocol Server
  - definition, 193
- approver
  - definition, 194
- attribute
  - definition, 194
- attribute mapping
  - definition, 194
- audit information
  - definition, 194
- audit log
  - definition, 194
- authentication
  - definition, 194
- authentication authority
  - definition, 194
- authentication broker
  - definition, 194
- Authentication Manager
  - certificate and key, 47, 58, 64, 70
  - installing with GUI, 45, 56, 63, 76
  - license, 22
  - pre-installation checklist, 30, 31, 33
  - security backup files, 49, 60, 65
  - server fails to start, 155
  - starting services
    - on Solaris and Linux, 109
    - on Windows, 108
  - stopping services
    - on Solaris and Linux, 110
    - on Windows, 109
  - system architecture, 23
- authentication method
  - definition, 194
- authentication policy
  - definition, 194
- authentication protocol
  - definition, 194
- Authentication Server, 23
  - definition, 194
- authenticator
  - definition, 194
- authorization
  - definition, 195
- authorization data
  - definition, 195
- auto-registration
  - definition, 195

B
backup
    post-installation, 49, 60, 65
    standalone primary instance, 105
Base Server license
    definition, 195
browser
    security, 19
    support, 19
Business Continuity option
    definition, 195

C
certificate
    definition, 195
    LDAP, 118
    SSL requirements, 115
    SSL-LDAP, 18
certificate DN
    definition, 195
certificate. See SSL
chained authentication
    definition, 195
checklists
    planning your deployment, 35
    pre-installation, 30, 31, 33
client time-out
    definition, 195
clocks, synchronizing, 44, 107
CLU
    Collect Product Information, 173
    Data Migration, 175
    Generate RADIUS Package, 178
    Manage Nodes, 179
    Manage Secrets, 180
    Manage SSL Certificate, 115, 183
    Multicast Network Test, 187
    Setup Replication, 190
CLU command
    collect-product-info, 174
    gen-radius-pkg, 178
    manage-nodes, 179
    manage-secrets, 182
    manage-ssl-certificate, 186
    migrate-amapp, 175
    setup-replication, 190
    test-multicast, 187
CLU. *See* command line utility
cluster
    definition, 195
Collect Product Information utility, 156, 173
collect-product-info command, 174
command line utility
    definition, 195
communication
    port usage, 19
compatibility, Authentication Agents, 22
components, 23
connection pool
    definition, 195
contact list
    definition, 196
    rebalancing, 60, 65, 148
context-based authentication
    definition, 196
core attributes
    definition, 196
Credential Manager Provisioning
    definition, 196
Cryptographic Token-Key Initialization Protocol
    client, 196
    enabled token, 196
    server, 196
    toolkit, 196
CT-KIP
    post-installation configuration, 119
CT-KIP. *See* Cryptographic Token-Key Initialization Protocol
customer name
    definition, 196

D
data encryption standard
    definition, 196
Data Migration utility, 175
data store
    definition, 197
    supported, 18
data transfer object
    definition, 197
data, user and group, 18
database, 18, 23, 30
    data replication, 26
    encryption, 107
    internal, 24
database package file
    generate, 71
    transfer, 72

database server
  definition, 197
  primary, 25
  replica, 25
  system requirements, 13
delegated administration
  definition, 197
delivery address
  definition, 197
denial of service
  definition, 197
deployment
  checklist, 35
  definition, 197
  example, 37
  large, 40
  medium, 38
  model, 35
  process illustration, 35
DES. *See* data encryption standard
DHCP, 30
directory server
  secure connections, 18
  supported directories, 18
disk space, 14
distribution file
  definition, 197
distribution file password
  definition, 197
distributor
  definition, 197
DN
  configuring, 23
download
  agents, 22
  software, 30, 32, 33
DTO. *See* Data Transfer Object
dump file
  definition, 197
DVD image. *See* ISO

E
EAP
  definition, 197
EAP-POTP
  client, 198
  definition, 198
e-mail notification
  definition, 198
e-mail template
  definition, 198
emergency access
  definition, 198
emergency access passcode
  definition, 198
emergency access tokencode
  definition, 198
Enterprise Server license
  definition, 198
Evaluation license
  definition, 198
event-based token
  definition, 198
example deployment, 37
excluded words dictionary
  definition, 198
extensible authentication protocol
  definition, 199

F
failover, 25, 38
failover mode
  definition, 199
Firefox, 19
firewall
  RADIUS, 74
  required open ports, 19
four-pass CT-KIP
  definition, 199

G
generate
  database package file, 71
  replica package file, 54
Generate RADIUS Package utility, 178
gen-radius-pkg command, 178
Global Catalog, 130
  definition, 199
  mapping to identity source, 129
graded authentication
  definition, 199
group data, 18
group membership
  definition, 199
GUI-based install, 45, 56, 63, 76, 78

H
hardware requirements, 14
hardware token
  definition, 199
high-water mark
  definition, 199

I

identity attribute
  definition, 199
Identity Management Services
  definition, 199
identity source, 23, 125
  adding, 132
  administrative, 129
  definition, 199
  linking to realm, 136
  runtime, 129
  supported, 18
IMS. *See* Identity Management Services
initial time-out
  definition, 199
installation
  fails to complete, 152
  logs, 152
  planning, 35
  primary instance, 43, 67
  process, 35
  RADIUS on a separate machine, 76
  RADIUS with Authentication Manager, 43, 51
  reinstallation cleanup script, 155
  replica instance, 51
  securing backup files, 49, 60, 65
  server node, 61
    network configuration, 27
  type, 24
instance, 24
  definition, 200
  primary, 24, 25
  replica, 24, 25, 26
instance ID
  definition, 200
instance name
  definition, 200
internal database, 18, 23, 30
  definition, 200
Internet Explorer, 19
interval
  definition, 200
ISO, 44

J

J2EE. *See* Java 2 Enterprise Edition
Java 2 Enterprise Edition
  definition, 200
Java Cryptographic Architecture
  definition, 200
Java Cryptographic Extensions
  definition, 200
Java keystore
  definition, 200
Java Management Extensions
  definition, 200
Java Messaging Service
  definition, 200
Java Server Pages
  definition, 200
JavaScript, 19
  enabling, 110
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, 201
Key Management services
  definition, 201
keystore
  definition, 201
  legacy compatibility, 118
  SSL requirements, 115

L

large deployment, 40
LDAP
  Active Directory, 129
  Active Directory forest, 129
  base DN, 23
  failover, 128
  identity source, 23, 125
  integration, 23, 38, 40, 125
  SSL setup, 130
  supported configurations, 23
  trusted root certificate, 118
LDAP directories
  Active Directory Global Catalog, 130
license
  Base Server, 195
  definition, 201
  Enterprise Server, 198
  Evaluation, 198
  files, 22
  general description, 22
  server node requirement, 27

- license category
  - definition, 201
- license creation date
  - definition, 201
- license deployment
  - definition, 201
- license file
  - definition, 201
- license file version
  - definition, 201
- license ID
  - definition, 201
  - determining, 11
- License Management Service
  - definition, 201
- license.rec
  - definition, 201
- link identity source to realm, 136
- Linux
  - requirements, 15
- LMS. *See* License Management Service
- Local Authentication Client
  - definition, 202
- locked license
  - definition, 202
- lockout policy
  - definition, 202
- log archival
  - definition, 202
- logging service
  - definition, 202
  - installation logs, 152
  - system logs, 155
- lower-level security domain
  - definition, 202

M

- Manage Nodes utility, 179
- Manage Secrets utility, 180
- Manage SSL Certificate utility, 115, 183
- Management Information Base
  - definition, 202
- manage-nodes command, 179
- manage-secrets command, 182
- manage-ssl-certificate command, 186
- master password, 30, 31, 33
- medium deployment, 38
- member user
  - definition, 202
- member user group
  - definition, 202
- memory requirements, 14
- MIB. *See* Management Information Base
- Microsoft Management Console
  - definition, 202
- migrate-amapp command, 175
- MMC
  - installing, 140
  - post-installation configuration, 142
  - purpose, 139
- MMC Extension, 157
- MMC. *See* Microsoft Management Console
- multicast network communication fails, 157
- Multicast Network Test utility, 157, 187

N

- namespace
  - definition, 202
- network address translation (NAT), 68
- network configuration
  - proxy service, 28, 29
  - server node, 27
- Network Management System
  - definition, 203
- NMS administrator
  - definition, 203
- NMS. *See* Network Management System
- node
  - fails to communicate, 157
  - installation, 27
  - manager, 108
  - package file, 61
  - test communication, 187
- node manager
  - troubleshooting, 157
- node secret
  - definition, 203
- NTP service, 22

O
object
    definition, 203
offset
    definition, 203
on-demand tokencode
    definition, 203
on-demand tokencode service
    definition, 204
one-time tokencode
    definition, 204
Operations Console
    definition, 206
options
    Business Continuity, 195
Oracle, 30

P
PAM Agent, 22
PAM. *See* Pluggable Authentication Module
passcode
    definition, 204
password
    Active Directory policy, 131
    encrypted properties file, 180
    internal system, 114
    master, 30, 31, 33, 112
    Super Admin, 30, 31, 33, 112
password policy
    definition, 204
    planning, 30, 31, 33
password-based encryption
    definition, 204
permissions
    definition, 204
Pluggable Authentication Module
    definition, 204
policy data, 18
ports, 19
ports reserved for Authentication Manager, 30, 32, 33
post-installation tasks
    changing passwords, 112
    SSL, 115
    starting services, 108
    stopping services, 108
pre-installation checklist, 30
primary connection pool
    definition, 204
primary database server, 25
    removing, 148, 149
primary instance, 25
    backing up standalone, 105
    definition, 204
    installing, 43
    installing RADIUS with Authentication Manager, 43
    removing, 145
    securing data over the network, 107
    synchronizing clocks, 44
private key
    definition, 204
PRN. *See* pseudorandom number
properties file, 180
protecting resources, 22
Protocol Data Unit
    definition, 204
provisioning
    definition, 204
provisioning data
    definition, 205
proxy servers, 119
proxy service, 28, 29
pseudorandom number
    definition, 205
public key
    definition, 205

R
RADIUS. *See* Remote Authentication Dial-In User Service
realm
    definition, 205
    identity source, 136
Red Hat Package Manager
    versions required, 16
regular time-out
    definition, 205
reinstallation cleanup script, 155

Remote Authentication Dial-In User Service
  adding clients, 122
  administrative access, 74
  and firewalls, 74
  copying a RADIUS package file, 75
  copying a RADIUS replica package file, 79
  creating a RADIUS package file, 74
  definition, 205
  installing primary server on a separate machine, 76
  installing replica server on a separate machine, 78
  installing with Authentication Manager primary instance, 43
  installing with Authentication Manager replica instance, 51
  platform requirements, 13
  post-installation configuration, 122
  pre-installation tasks for standalone server, 74
  replication of database changes, 122
  testing operation, 123
  uninstall server, 149
remote EAP
  definition, 205
remote post-dial
  definition, 205
Remote Token Key Generation Service, 119
replica instance, 25
  connection to primary instance, 26
  definition, 206
  installing, 51
  installing RADIUS with Authentication Manager, 51
  rebalancing contact lists, 60, 65
  removing, 147
  synchronizing clocks, 44, 107
replica package file
  generate, 54
  transfer, 55
Request Approver
  definition, 206
requests
  definition, 206
requirements
  system, 13
RPM. *See* Red Hat Package Manager
RSA ACE/Server, 30
RSA Authentication Manager. *See* Authentication Manager
RSA Credential Manager
  definition, 206
RSA EAP
  definition, 206
RSA Operations Console
  definition, 206
RSA Protected OTP
  definition, 206
RSA Security Console
  adding to trusted sites, 111
  definition, 206
  description, 23
  fails to start, 156
  identity source, 23
  MMC Extension configuration, 142
  on server, 28, 29
  read-only operations, 26
  starting service, 108
  stopping service, 108
  supported browsers, 19
RSA Self-Service Console
  definition, 206
runtime
  definition, 206
runtime command
  definition, 206
runtime identity source, 129
  definition, 206

S

scope
  definition, 207
secondary connection pool
  definition, 207
Secure Sockets Layer
  definition, 207
Secure Sockets Layer. See SSL
Security Console, 23
  adding to trusted sites, 111
  definition, 206
  description, 23
  fails to start, 156
  identity source, 23
  MMC Extension configuration, 142
  on server nodes, 28, 29
  read-only operations, 26
  starting service, 108
  stopping service, 108
  supported browsers, 19
security domain
  definition, 207

security questions
  definition, 207
self-service
  definition, 207
Self-Service Console
  definition, 206
self-service requests
  definition, 207
self-service troubleshooting policy
  definition, 207
server certificate and key, 47, 58, 64, 70
server node
  connection to primary instance, 28, 29
  definition, 207
  fails to communicate, 157
  function, 27
  installation type, 24
  installing, 61
  removing, 145
  test communication, 187
services
  defined, 19
  protocols used, 19
services, fail to start, 155
session
  definition, 207
session policy
  definition, 208
setting local time, 22
Setup Replication utility, 190
setup-replication command, 190
shipping address
  definition, 208
Short Message Service
  definition, 208
Simple Mail Transfer Protocol
  definition, 208
Simple Network Management Protocol
  definition, 208
single sign-on
  definition, 208
SMS
  definition, 208
SMTP
  definition, 208
snap-in
  definition, 208
SNMP agent
  definition, 208
SNMP trap
  definition, 208
SNMP. *See* Simple Network Management Protocol
Solaris
  requirements, 17
SSL
  LDAP, 130
  manage certificate, 183
  post-installation tasks, 115
SSL LDAP, 18
SSL. *See* Secure Sockets Layer
SSO. *See* single sign-on
starting RSA Authentication Manager services, 108
starting services
  on Solaris and Linux, 109
  on Windows, 108
stopping RSA Authentication Manager services, 108
stopping services
  on Solaris and Linux, 110
  on Windows, 109
subnet, 27
Sun Java System Directory Server, 18
Super Admin
  definition, 209
  planning password, 30, 31, 33
supported browsers, 19
symmetric key
  definition, 209
system
  architecture, 23
  components, 23
  fingerprint, 180
  logs, 155
  required packages, 16
system event
  definition, 209
system log
  definition, 209
system requirements
  Linux, 15
  Microsoft Windows, 14
  Solaris, 17
systemfields.properties, 30, 31, 33, 180

T

TACACS+. *See* Terminal Access Controller Access Control System+
TCP ports, 30, 32, 33
temporary directory for installation logs, 30

temporary fixed tokencode
  definition, 209
test-multicast command, 187
time settings, 22
time synchronization, 22
time-based token
  definition, 209
Token Distributor
  definition, 209
token provisioning
  definition, 209
tokencode
  definition, 209
tokens
  definition, 209
top-level security domain
  definition, 210
trace log, 155
  definition, 210
transfer
  database package file, 72
  replica package file, 55
troubleshooting
  accessing installation files on a network, 151
  Collect Product Information utility, 173
  message indicating Node Manager Service is not started, 157
  MMC Extension does not start, 157
  multicast network communication fails, 157
  RSA Security Console fails to start, 156
  Security Console times out when searching for users, 158
  server fails to start, 155
  starting node manager, 157
  unsuccessful authentication between RADIUS and Authentication Manager, 158
  unsuccessful end-to-end authentication on RADIUS, 158
  unsuccessful installation, 152
  unsuccessful installation or removal, 152
trust package
  definition, 210
trusted realm
  definition, 210
two-factor authentication
  definition, 210
two-pass CT-KIP
  definition, 210

U

UDP ports, 30, 32, 33
UDP. *See* User Datagram Protocol
uninstall
  primary database server, 148, 149
  RADIUS server, 149
  replica database server, 147
upgrade
  primary instance, 84
  replica instance, 95
  server node, 102
upgrade from version 7.0 to 7.1, 84
URL to access the RSA Security Console, 103
user and group data, 18
User Datagram Protocol
  definition, 210
user groups
  definition, 210
User ID
  definition, 210
users
  definition, 210
users and groups
  accessing from LDAP directory, 23, 125
utility
  Collect Product Information, 173
  Data Migration, 175
  Generate RADIUS Package, 178
  Manage Nodes, 179
  Manage Secrets, 180
  Manage SSL Certificate, 183
  Multicast Network Test, 187
  Setup Replication, 190

V

version number, determining, 11

W

Windows registry settings, 30, 32, 33
Windows requirements, 14
workflow
  definition, 210
workflow participant
  definition, 211