RSA Authentication Manager 6.1 Administrator's Guide

RSA SECURITY™

Contact Information

See our Web sites for regional Customer Support telephone and fax numbers.

RSA Security Inc.	RSA Security Ireland Limited
www.rsasecurity.com	www.rsasecurity.ie

Trademarks

License agreement

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 exporting this product.

Distribution

Limit distribution of this document to trusted personnel.

RSA notice

Protected by U.S. Patent #4,720,860, #4,885,778, #4,856,062, and other foreign patents.

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

First printing: September 2005

Contents

Preface

Intended Audience

This book is intended only for system administrators and other trusted personnel. For security reasons, do not make this book available to your general user population.

Documentation

The RSA Authentication Manager 6.1 CD contains all RSA Authentication Manager documentation and Help, which provide complete instructions for installation, configuration, administration, and troubleshooting. For information about all RSA Authentication Manager 6.1 resources available to you, see the printed *Getting Started* booklet in the RSA Authentication Manager package.

Note: For security reasons, RSA Security recommends that you obtain the latest version of Adobe Reader for your platform at **www.adobe.com**.

Getting Support and Service

RSA SecurCare Online	**https://knowledge.rsasecurity.com**
Customer Support Information	**www.rsasecurity.com/support**

Before You Contact Customer Support

Make sure that you have direct access to the computer running the RSA Authentication Manager software, and that you have the following information available:

- ❑ Your RSA Security Customer/License ID. You can find this number on the license distribution medium. Alternatively, you can run the Configuration Management application in Windows, or **sdinfo** in UNIX.
- ❑ RSA Authentication Manager software version number.
- ❑ The make and model of the machine on which the problem occurs.
- ❑ The name and version of the operating system under which the problem occurs.

1 Overview

RSA Authentication Manager works with RSA Authentication Agents to enhance native Windows security with the strong, two-factor authentication of time-based RSA SecurID tokens. In this software release, RSA Security introduces the RSA SecurID for Microsoft Windows solution, which includes:

- **RSA Authentication Manager 6.1** for administration, user authentication, password integration, and auditing
- **RSA Authentication Agent 6.0 or 6.1** to protect local computers, domain and terminal servers, and remote logons through Microsoft's Routing and Remote Access Service (RRAS) and Microsoft wireless LANs.
- **RSA Authentication Agent 5.3 for Web** to protect web servers and Microsoft Outlook web access.

With RSA Authentication Manager and RSA Authentication Agent 6.0 or 6.1, you can use RSA SecurID to enhance Windows password security on your computers and networks. On protected systems, the RSA Authentication Agent prompts users for their logon names and passcodes, requests authentication services from RSA Authentication Manager, and, based on Authentication Manager responses, enables or prevents logging on.

Versions of RSA Authentication Agent software run on other platforms as well, so that a variety of network resources can take advantage of RSA SecurID protection. For a list of supported platforms, see "RSA Authentication Agent Software" on page 222.

To provide for scalability to large numbers of users and tokens, RSA Authentication Manager integrates a commercial relational database developed by Progress Software.

To create custom administration applications to read and write to RSA Authentication Manager databases, the RSA Authentication Manager product set includes the Administration Toolkit. For more information, see the *Administration Toolkit Reference Guide* (**authmgr_admin_toolkit.pdf** in the ***ACEDOC*** directory or on the software CD).

This chapter discusses the RSA Authentication Manager and RSA SecurID solution, including security capabilities, system architecture, and new features.

RSA SecurID Tokens and Two-Factor Authentication

With RSA SecurID deployed in your organization, a user must enter a valid passcode to gain access to a protected system. A passcode consists of:

- A personal identification number, or PIN (something the user *knows*)
- The tokencode currently displayed on the user's token (something the user *has*)

Because user authentication requires these two factors, the RSA SecurID solution offers stronger security than traditional passwords (single-factor authentication).

Most RSA SecurID tokens are handheld devices containing microprocessors that calculate and display pseudorandom codes.

SID800 Token

PINPad

Key Fob

These *tokencodes* change at a specified interval, typically every 60 seconds. RSA Authentication Manager 6.1 supports the following token algorithms:

- **Traditional SID (64-bit algorithm)** tokens provide time-based authentication using the SID proprietary algorithm. SID seed records are available in ASCII and XML format.
- **AES (128-bit algorithm)** tokens provide time-based authentication using the Advanced Encryption Standard (AES) cryptographic algorithm. AES seed records are available in XML format.

Token Algorithm is included as a field or search criterion in many of the administration tasks in the RSA Authentication Manager Database Administration application. For example, when viewing token records in the database, you can list them by algorithms or by the SID or AES algorithm only.

RSA Security provides an authentication instructions template (**authmgr_authentication.doc** and **authmgr_authentication.pdf**) that you can customize and provide to your users.

If you are deploying the RSA SecurID Authenticator SID800 to your users, see the *RSA Security Center Help* and the *RSA Authenticator Utility 1.0 User's Quick Reference*, both of which are provided with the RSA Authenticator Utility 1.0, for end-user instructions.

Note: RSA Authentication Manager also supports authentication with hardware tokens that do not require a PIN. For more information, see "Tokens that Do Not Require PINs" on page 107.

RSA SecurID Software Token

The software token is a software file installed on a client workstation, an RSA SecurID Smart Card, a personal digital assistant (PDA), or a cell phone.

The RSA Authentication Manager Database Administration application provides a centralized administration interface for issuing RSA SecurID software tokens to the supported device types. You can add information to software tokens such as device type, device serial number, or token nickname using token extension fields.

For more information about the software token, see "RSA SecurID Software Tokens" on page 117, and the documentation that accompanies individual RSA SecurID software token products.

RSA SecurID Authenticator SID800

The RSA SecurID Authenticator SID800 is both an RSA SecurID authenticator and a USB smart card (USB token) with a built-in reader. The two sets of electronics operate independently of each other.

When disconnected, the SID800 generates and displays tokencodes used in RSA SecurID authentication. When connected to a computer, the token serves two functions:

- For RSA SecurID authentication, users obtain their tokencodes through the supporting software on their desktop instead of reading the number off the token.
- With the token's smart card capabilities, users can store credentials, including digital certificates and Windows logon accounts, for logging on to Windows.

For more information, see the RSA Authenticator Utility 1.0 documentation.

User Password Token

A user password token is a single password that the user enters instead of a PIN and tokencode. User passwords are less secure than other token types, but they allow administration of users with different security needs. For example, you might want to assign user passwords to employees who work in a physically secure facility.

Important: Because the user password token is less secure than other token types, RSA Security does not recommend user passwords as a long-term security solution.

Token Assignment Limits

You can assign up to three RSA SecurID tokens to each authorized user on a protected system. For example, employees can have different token types for different work locations—hardware tokens for telecommuting from home and RSA SecurID software tokens for working in the office.

RSA SecurID Code Generation and Time Synchronization

RSA Authentication Manager software and RSA SecurID tokens work together to authenticate user identity. The RSA Security patented time synchronization ensures that the pseudorandom code displayed by a user's token is the same code the RSA Authentication Manager software has generated for that moment.

An RSA SecurID token generates tokencodes with a calculation based on these elements:

- The token's unique identifier (also called a "seed"), which is stored in the token itself
- The current time according to the token's internal clock, shown in Coordinated Universal Time (UTC)

The RSA Authentication Manager generates tokencodes for a token using these elements:

- The token's unique identifier, which is stored in the token's record in the RSA Authentication Manager database
- The time, which is calculated by adding the offset stored in the token record to the current RSA Authentication Manager time, in Coordinated Universal Time (UTC)

To determine whether an access attempt is valid, the RSA Authentication Manager compares the tokencode it generates with the tokencode the user enters. If the tokencodes do not match or if the wrong PIN is entered, the user is denied access.

For a more detailed description of the RSA Security time-synchronization technique and an explanation of the time offset stored in the token record, see "Synchronization" on page 132.

Maintaining Accurate System Time Settings

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

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

To get UTC, call a reliable time service. In the U.S., call 303-499-7111.

Note: If you use a network time server (NTS) to maintain accurate time, enable it only on the Primary Authentication Manager. The Primary then automatically maintains the Replica's time synchronization. However, there is one exception. In a UNIX environment, for security reasons, some organizations do not allow Authentication Managers to be started by a root user. In this case, the Primary does *not* maintain accurate time on the Replicas, and you can use an NTS on the Primary and the Replicas.

Other RSA Authentication Manager Security Capabilities

Other security capabilities in RSA Authentication Manager include auditing, protection from intruders, and data encryption.

Accountability and Security Auditing

Because user accountability is a critical part of system security, the RSA Authentication Manager creates an audit trail. This audit trail tracks all logon requests and all operations performed with the Database Administration application.

When the RSA Authentication Manager is properly implemented, the audit trail reliably identifies which user was responsible for each logged action. User information that is based on two-factor authentication provides stronger legal evidence of who performed the recorded activity than information based solely on password authentication.

Instruct users to avoid unauthorized use of their identities and of the system. For more information, see "Educating Users About Security Responsibilities" on page 125.

You can examine the audit trail in the following ways:

- Through Database Administration application reports.
- Through the Report Creation Utility (see "RSA Authentication Manager Report Creation Utility (Windows)" on page 174).
- Through reports created with third-party software using the file generated by the automated log maintenance feature (see "Scheduling Automated Log Database Maintenance" on page 157).

You can also monitor activity in real time by requesting that records be displayed on the screen as soon as they are created. For more information, see "Monitoring Activity in Real Time" on page 220.

Protection from Intruders

If an unauthorized person tries to use a stolen PIN or RSA SecurID token to break into your system, the RSA Authentication Manager "evasion-of-attack" features can detect the attempted intrusion and deny access. Note that evasion-of-attack features do **not** replace the need to implement and use the product properly, and can offer **no** protection against an intruder who has both a user's PIN and RSA SecurID token.

Therefore, it is **essential** to observe the following policies:

- All users must protect the secrecy of their PINs and the physical security of their tokens.
- Administrators must respond immediately to disable compromised PINs and missing tokens.

- Primary and Replica machines should be set up for RSA Authentication Manager functions only. Avoid using these computers as web servers, file servers, firewalls, or for any other application.
- RSA Authentication Manager Primary and Replica machines must be kept physically secure.

Important: RSA Security recommends that administrators direct users to follow the directions in the "User Responsibilities" section of their authentication instructions.

Evasion-of-Attack Features

If an unauthorized user with a stolen PIN eventually succeeds in guessing a valid tokencode, this person is still not granted access because the Authentication Manager prompts for a second tokencode after a series of failed logon attempts. If the person does not correctly enter the next tokencode generated by the token, he or she is denied access. Additionally, after a certain number of consecutive failed logon attempts, the token used in these attempts is disabled automatically. For more information, see "Summary of Evasion-of-Attack Features" on page 130.

The number of incorrect passcodes allowed is configurable using the Configuration Management application (Windows) or the ***ACEPROG*/sdsetup -config** command (UNIX). For more information, see Chapter 12, "Configuring the RSA Authentication Manager (Windows)" or Chapter 14, "Configuring the RSA Authentication Manager (UNIX)."

The Lock Manager

The Lock Manager defends the RSA Authentication Manager against replay attacks in which an intruder attempts to reuse an old passcode or acquires the current passcode for a token. The Lock Manager service name is **sdlockmgr**, and the default service port is **5560**.

The Lock Manager coordinates data that was previously maintained in an RSA Authentication Manager work queue. The work queue is used to detect two simultaneous authentications occurring for the same authenticator (RSA SecurID token) within a time period referred to as the "Response Delay." In addition, the RSA Authentication Manager uses a token "high water mark" to prevent the replay of past tokencodes that fall within the authentication window and would therefore be accepted by the RSA Authentication Manager. When RSA Authentication Manager processes are replicated, you need a mechanism to coordinate the work queue data from all RSA Authentication Managers within a realm. The Lock Manager fills this role by:

- Locking a user's Default logon name when an RSA Authentication Agent sends a name lock request to the RSA Authentication Manager. If the Authentication Manager receives a second request, the request is denied.

- Tracking the "high water mark." The high water mark is a record of the last good passcode used for the token. The Authentication Manager accepts passcodes that occur *after* the last good passcode. The token record can still store the high water mark (as in previous releases), but you now have the option of leaving this task entirely to the Lock Manager. To configure your Authentication Manager not to record the high water mark in the token record, click **System** > **Edit System Parameters** and clear **Store time of last login in token records**.

Detecting a Replay Attack

In a replay attack, an intruder attempts to gain access with a captured passcode by setting the server system clock back, then reusing the passcode at the appropriate system time. The RSA Authentication Manager software warns you of any change in system time that may indicate a replay attack.

When the RSA Authentication Manager software detects that the server system clock has been set back, it puts the following warning message in the log database: "*** System clock setback detected". This message can be viewed through Database Administration application Activity or Exception reports. This message is also added by default to the Event log and can be tracked and identified with a commercial network management tool.

Note: Because this message may indicate a serious security breach, RSA Security recommends that it ***not*** be removed from the list of message types sent to the Event log.

Data Encryption

RSA Authentication Manager 6.1 uses data encryption in several ways to ensure the security of your system:

- All messages and data exchanged between the Primary and Replica are encrypted during transmission—the more sensitive data with the secure RC5 block cipher and the less sensitive data with a DES encryption key that changes every ten minutes.
- Communications between any Agent and a Primary or Replica are encrypted using a unique key (the "node secret") known only to the specific Agent and to the Authentication Manager. This prevents an unauthorized machine from passing for an Agent, a Primary, or Replica. For more information, see "Node Secret File" on page 228.
- Communications between separate RSA Authentication Manager systems (realms) are encrypted using a unique "realm secret" known only to the two Authentication Managers participating in the exchange. For more information about the realm secret, see "Creating and Modifying Realms" on page 85.
- Sensitive token data, for example, a user's PIN, is encrypted so that no one, including system administrators, can view it. Token serial numbers, which are not encrypted, enable administrators to specify tokens for administrative purposes.

Emergency Access

Even the most responsible user might lose a token. RSA Security recommends that you disable lost tokens. However, if your organization's security policy permits, you can assign *temporary* passwords (either a single fixed password or a set of one-time passwords) for authentication until a lost token is found or you determine that it must be disabled. For more information, see "Temporary Passwords to Replace Lost Tokens" on page 128.

Instruct your users to protect a temporary password as carefully as a token. For more information about using temporary passwords, see *Authenticating with an RSA SecurID Token* (**authmgr_authentication.pdf**)

RSA Authentication Manager Architecture

This section provides an overview of system architecture, including a discussion of the RSA Authentication Manager database, the Primary and Replica model, the cross-realm model, and Agent Host architecture.

RSA Authentication Manager Database

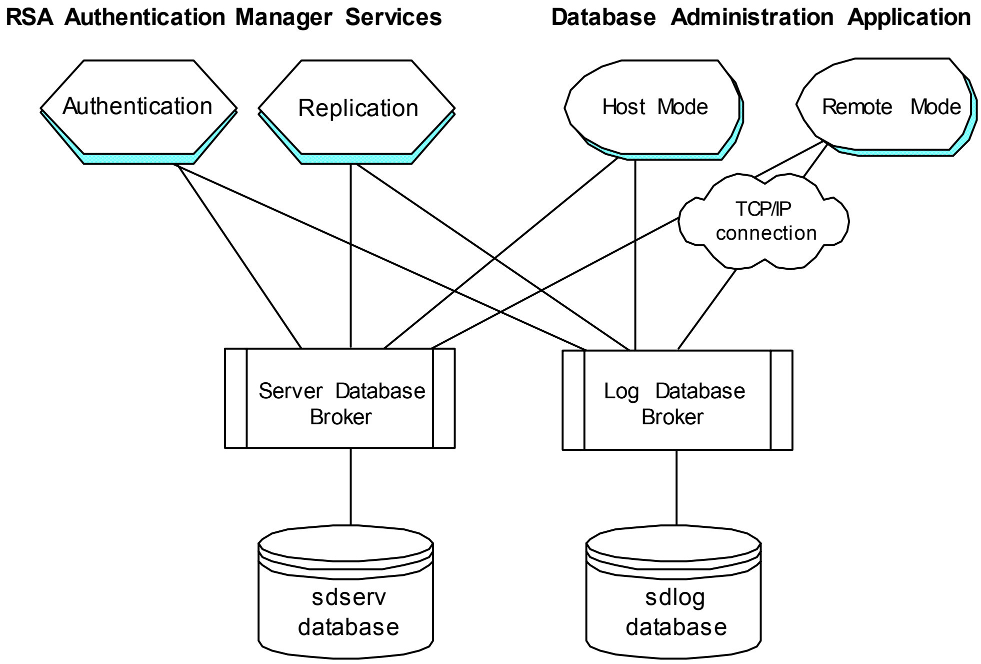
RSA Authentication Manager data is stored in a commercial relational database management sytem (RDBMS) developed by Progress Software Corporation and integrated into the RSA Authentication Manager software.

Two separate databases are maintained by the Authentication Manager: **sdserv** (the user database) and **sdlog** (the audit log database). The Authentication Manager databases include:

- A list of resources to be protected by RSA SecurID authentication
- Records for all tokens
- A registry of users
- Registries of realms for cross-realm authentication and for Remote Administration
- An audit trail of authentication and administrative activity

The following figure illustrates the relationships among the two databases (**sdserv** and **sdlog**), the RSA Authentication Manager Authentication and Replication Services, and the Database Administration application (both in Host Mode and in Remote Mode).

The brokers connect the services and Database Administration application sessions to the databases. When you start the RSA Authentication Manager Services or the Database Administration application in Host Mode, the Authentication Manager software checks to see if the brokers are running and starts them if necessary. At this point the software also starts the Remote Administration service (**sdadmind**), so that the Database Administration application can be run remotely.



When you stop all RSA Authentication Manager Services, the Authentication Manager software automatically stops the database brokers. Shutting down the brokers breaks the necessary connection between the databases and any active administration sessions.

When you exit a Database Administration application session, the brokers continue to run, even if the RSA Authentication Manager Services are not running.

If you are using Windows, you can start and stop the services through the RSA Authentication Manager Control Panel.

If you are using UNIX, you can stop the brokers by typing:

```
ACEPROG/sdconnect stop
```

at a command prompt, where *ACEPROG* is the location of the **ace/prog** directory.

Note: One RSA Authentication Manager service—External Authorization (**sdxauthd**)—is not discussed in this section because it is not essential to the Authentication Manager architecture.

Primary and Replica Model

RSA Authentication Manager 6.1 has one Primary and can have up to ten Replicas. The Primary functions as the administration Authentication Manager, replicates database changes to each Replica, authenticates users, and gathers the log messages it receives from all Replicas into a consolidated log database. The Replicas function as the authentication Servers with read-only access to the database.

Note: You must have an RSA Authentication Manager Advanced license to use more than one Replica. If you have an RSA Authentication Manager Base license, your system is limited to one Primary and one Replica. For more information about licensing, see Appendix A, "Licensing."

Database Replication

The Primary runs a separate instance of the replication service (**acesyncd** on UNIX or **syncserv** on Windows) for each Replica in your system. Each Replica runs a single instance of the replication service. The replication service enables the Primary and Replica to communicate and exchange information about changes to the database on a regular basis. Each exchange of these delta records between the Primary and a Replica is called a replication pass.

The first replication process begins a certain number of seconds after the Primary starts. The second replication process begins the same number of seconds after the first, and so on. This startup delay staggers the startup times of replication processes so that all the Replicas in your realm do not send their changes to the Primary at the same time.

After they start, the Primary and the Replicas exchange delta records at a specified frequency called the replication interval. You can define both the startup delay and replication interval with the **sdsetup -repmgmt** tool on UNIX or the Replication Management application on Windows.

Most changes in the Primary database are caused by administrator actions—for example, an administrator adds a user to the database and assigns an RSA SecurID token to that user. Changes in a Replica database are caused by user authentication attempts, successful or unsuccessful, and the log messages generated in connection with these attempts. For example, a new user logs in with a token for the first time and selects a new PIN. When the Replica that receives the authentication request accepts the new PIN and authenticates the user, that user's record in the Replica database is changed. The Replica sends this change to the Primary, and the Primary passes it to all other Replicas in the realm. The Replica also sends any messages logged as a result of the change to the Primary, but the Primary does not communicate these log messages to the other Replicas.

Replica Package

The Replica Package contains the database and license files necessary to install one or more Replicas. You create the Replica Package on the Primary and copy it to the Replica machine before installing the RSA Security software on the Replica.

If you specify multiple Replica machines when you are creating the Replica Package, you can use the same package for all of these machines. RSA Security recommends that you identify all of your Replica machines before you create the Replica Package. If you later need to add a Replica that was not specified in the original package, you can first add the Replica and then create a new Replica Package for it.

Push DB Assisted Recovery

Push DB is a System Parameters option that, when enabled, copies the latest database files to a Replica over your network.

You can specify Push DB during installation or as part of the recovery process after an Authentication Manager or the database on an Authentication Manager fails. In an installation, you must still create the initial Replica Package, copy the license files from the Replica Package to the Replica, and install the software, but the push database feature copies the database files from the Primary to the Replica when the Replica starts for the first time.

Copying large database files may slow down your network to an unacceptable level, depending on the network bandwidth, your speed requirements, and the size of the database. Decide whether you want to use the Push DB feature to copy the database from the Primary to the Replicas or whether you want to use a copying method that avoids using the network.

Nominate Replica

To keep your RSA Authentication Manager installation running while your original Primary machine is being repaired or replaced, you can use the **Nominate Replica** capability in the Replica Management utility.

From a Replica, you can run the Replica Management utility appropriate for your platform (Windows or UNIX), and nominate this Replica as the new Primary.

If your Authentication Managers are running on Windows 2000, Windows XP, or Windows 2003, see “Nominating a Replica to Replace Primary Hardware” on page 97. For UNIX, see “Nominating a Replica to Replace Primary Hardware” on page 148.

Agent Host/Authentication Manager Architecture

With RSA Authentication Manager software running on a Windows system, a variety of resources on your TCP/IP network can be configured for RSA SecurID protection: local machines, domain controllers, firewalls, routers, virtual private networks (VPNs), web servers, and so on.

To be protected by RSA SecurID authentication, a computer or other device running RSA Authentication Agent software must be registered as an Agent Host in the RSA Authentication Manager database.

Each Agent Host registered in the Authentication Manager database can have its own list of authorized RSA SecurID users. You create this list by activating users on the Agent Host or by making users members of groups that are activated on the Agent Host. You also have the option of designating "open" Agent Hosts without specific user or group activations.

The following table shows what categories of users are allowed access to each type of Agent Host. Note that an open Agent Host can optionally be instructed to search other realms for users who are not known locally. However, these users must belong to realms that are registered in your RSA Authentication Manager database.

Agent Host Configuration	Availability to Users in Local Database	Availability to Outside Users
Set up with lists of activated users and groups	Open to valid activated users and members of activated groups	Open to valid activated users and members of activated groups, provided users' realms are locally registered
Open, set to look up users in registered realms	Open to all valid users	Open to all valid users, provided users' realms are locally registered
Open, no lookup	Open to all valid users	No access

For more information about Agents and Agent Host activation, see Chapter 3, "Agents and Activation on Agent Hosts."

RSA Authentication Agent software installed on Agent Hosts or integrated into routers, communication servers, VPN servers, web servers, and firewalls performs the following functions as part of the authentication process:

- Responds to logon attempts with a request for an RSA SecurID passcode
- If the user's computer is online (connected to a network), sends the user's response to the Authentication Manager for verification that the user is authorized to use resources on the Agent Host
- If the user's computer is offline (disconnected from the network), works with other RSA Security software on the user's machine to perform an offline authentication (RSA Authentication Agent 6.1 only)
- After a user's machine reconnects to a network, sends offline authentication log data to the RSA Authentication Manager for incorporation into the log database
- Verifies the authenticity of the RSA Authentication Manager so that no other machine can masquerade as the Authentication Manager to capture security data
- Encrypts and decrypts messages sent between the Agent Host and the Authentication Manager

The RSA Authentication Manager provides:

- Continuous authentication service to Agent Hosts
- Offline authentication data to computers whose users are often disconnected from the network (computers with RSA Authentication Agent 6.1 only)
- Cross-realm authentication services for users visiting from other realms
- Administrative functions for the Authentication Manager system (on the Primary only—administrative functions are limited on Replicas)
- Real-time monitoring of RSA SecurID authentication and administrative activity

Automatic Load Balancing

Version 5.0 (and later) RSA Authentication Agents can do automatic load balancing by polling the Authentication Managers and selecting the one that responds most quickly to an authentication request. You can also balance the load manually by configuring Agents to give higher priority to different Authentication Managers. For more information, see "Load Balancing by Agent Hosts" on page 69.

Authentication Manager and Agent Host Communication Through Firewalls

An RSA Authentication Agent Host can use up to three alias Authentication Manager IP addresses to communicate with an RSA Authentication Manager that is located on the other side of one or more firewalls. When one of these firewalls intercepts an authentication request, it recognizes one of the Authentication Manager's alias IP addresses and uses an established protocol to match the alias with a valid IP address. For information on setting alias Authentication Manager IP addresses, see the *Windows Installation Guide*.

The configuration file of an Agent Host separated from the Authentication Manager by a firewall must contain the list of available aliases. If you have legacy Agent Hosts that must authenticate through a firewall, and you want to use an alias IP address that is not listed in the database as an available alias, you can use the Configuration Record Editor to edit the Acting Master and Slave Authentication Manager fields in any **sdconf.rec** file. For more information, see "Legacy Agent Hosts" on page 75.

Legacy Agent Support

Two changes in RSA Authentication Manager 5.0 (and later) architecture improved authentication rates over previous major versions: the use of multiple authenticating Replicas and the ability of the new RSA Authentication Agent software to select the Replica that will respond most quickly to an authentication request. The new Agent software is aware of all the Replicas in your realm and can send authentication requests to any one of them.

Lacking this ability, Agent Hosts running versions of RSA ACE/Agent software prior to 5.0 can authenticate users against only the Master or the Slave, because the Agent Host's configuration file (**sdconf.rec**) identifies only these two Authentication Managers.

For more information about legacy Agent issues, see "Legacy Agent Hosts" on page 75.

Cross-Realm Model

In the RSA Authentication Manager context, each instance of a Primary and its Replicas is called a realm. A single installation can include multiple realms, and you can configure a realm to authenticate and allow access to users from other realms. This is called "cross-realm" authentication.

Important: This section refers to implementations with multiple Realms and is applicable only to RSA Authentication Manager Advanced license customers. For a description of the licensing options, see Appendix A, "Licensing."

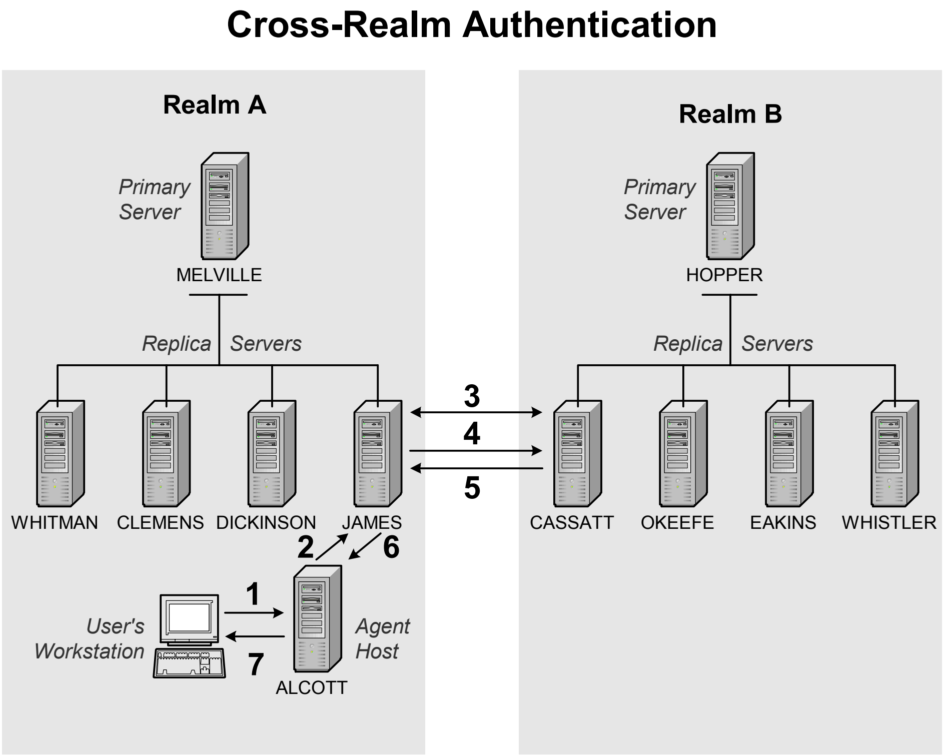
Multiple realms may not be needed in your installation. RSA Authentication Manager 6.1 allows each Primary to have up to 10 Replicas, greatly increasing the load one realm can handle. If your installation initially includes one Primary and two Replicas, you can add additional Replicas, at different physical locations, as your user base grows.

If you have a very large number of users or want to install Primary Authentication Managers at widely separated sites, you may decide to use multiple realms. If so, you have to configure each realm specifically to accept and authenticate users from other realms.

A user's *Home* realm is the realm where that user was added to the database and where his or her user record is stored. A *Remote* realm is any realm that authenticates a user whose record is not stored in its own database.

When you add a realm to your database, you must specify the Primary in the remote realm and one or two Authentication Managers in the remote realm that authenticate visitors from that realm. You must also specify one or two Authentication Managers in your own realm that authenticate users from your realm when they are visiting the remote realm. If, as RSA Security recommends, you specify two Authentication Managers in each realm for cross-realm authentications, one is designated the preferred Authentication Manager and the other the failover Authentication Manager, to be used when the preferred Authentication Manager is unavailable.

The following diagram illustrates the course of a cross-realm authentication.



1. A user from Realm B attempts to log on to Agent Host ALCOTT in Realm A.
2. The Agent Host passes the request to Replica JAMES, where the RSA Authentication Manager 6.1 software checks the database and does not find the user.
3. Authentication Manager JAMES polls the preferred Authentication Manager (or if it is unavailable, the failover Authentication Manager) in each realm registered in the Realm A database until it finds the Authentication Manager—CASSATT in Realm B—that has a user record for the visiting user.
4. Authentication Manager JAMES sends the authentication request to CASSATT. (If CASSATT is unavailable, the request goes to OKEEFE, which is listed in the realm record as the failover Authentication Manager.)
5. The RSA Authentication Manager 6.1 software on CASSATT in Realm B authenticates the user and passes this information back to JAMES in Realm A.
6. JAMES informs Agent Host ALCOTT that the user is authenticated.
7. The RSA Authentication Agent on ALCOTT admits the user to the network.

To Begin: Click **Realm** > **Add Realm**. Click **Help** for directions.

New Features in RSA Authentication Manager 6.1

RSA Authentication Manager Control Panel

From the expanded RSA Authentication Manager Control Panel, you can start and stop the RSA Authentication Manager services, view installation information, and perform various maintenance tasks, depending on what type of installation you are on.

To access the RSA Authentication Manager Control Panel, click **Start** > **Programs** > **RSA Security**> **RSA Authentication Manager Control Panel**.

For information about individual tasks, see the corresponding chapters in this book, the *Installation Guide* for your platform, and the Help.

Group Authentication Settings

When you add or edit a group, you can enable Offline Authentication and Windows Password Integration for all members of that group. To use these features, you must install RSA Authentication Agent 6.1 for Microsoft Windows and activate the group on that Agent.

RSA RADIUS Server 6.1 Powered by Funk Software

RSA Authentication Manager 6.1 features a new RSA RADIUS Server, powered by Funk Software, that provides extended capabilities, including:

- Support for traditional and wireless authentication using RSA SecurID two-factor authentication
- Support for PAP, EAP-PEAP-GTC, EAP-TTLS-PAP, and EAP-TTLS-GTC protocols
- Architecture that mirrors the RSA Authentication Manager Primary/Replica model

You perform most of the administration of the RSA RADIUS Server 6.1 through its own administration application, which you can launch from the RSA Authentication Manager Database Administration application by clicking **RADIUS** > **Manage RADIUS Server**. You assign profiles to users and groups through the RSA Authentication Manager. To start the RSA RADIUS server application, you must have a token or passcode assigned to you in the RSA Authentication Manager database.

Note: All profiles in the RSA RADIUS Server must have a matching profile name in the RSA Authentication Manager.

For more information about profiles, see the Help.

For information about upgrading to RSA RADIUS 6.1 as part of the upgrade to RSA Authentication Manager 6.1, see the *Installation Guide* for your platform. For information about installing and administering RSA RADIUS 6.1, see the *RSA RADIUS Server 6.1 Administrator's Guide.*

RSA Authentication Manager Licensing

RSA Authentication Manager enforces two types of permanent licenses—the Base license and the Advanced license—both during installation and in the normal course of daily operation and administration. (The Evaluation license, a temporary trial license, is also enforced by RSA Authentication Manager.)

The RSA Authentication Manager Base license provides the rights to use the RSA Authentication Manager software in the following environment:

- With as many active users in the RSA Authentication Manager database as specified by the active user tier that was purchased. For more information about active users, see Appendix A, "Licensing."
- On one Primary and one Replica in one Realm.

  Customers who want to deploy more than one Replica or more than one Primary (for example, multiple Realms) must purchase an Advanced license.

The RSA Authentication Manager Advanced license provides the rights to use the RSA Authentication Manager software in the following environment:

- With as many active users in the RSA Authentication Manager database as specified by the active user tier that was purchased.
- On one Primary and up to ten Replicas in up to six Realms.

  Multiple Advanced licenses may be purchased for customers who want to install the software in more than six Realms.
- Installed on a qualified High Availability hardware system. RSA Security currently supports Veritas Cluster Server on Sun Solaris 9.0 for high availability.

For more information about licenses and active users, see Appendix A, "Licensing."

2 Using RSA Authentication Manager Administration Applications

This chapter describes the tasks for setting up your RSA Authentication Manager, and introduces the Database Administration applications.

In Windows, all subdirectories, databases, and program files are installed in a directory specified during installation. The default installation directory is **c:\ace**. The subdirectory that contains the executable files is **prog**, and data files are in subdirectory **data**.

In UNIX, all directories, databases, and program files are installed in a top-level directory specified during installation. The subdirectory that contains the executable files must be **ace/prog**, and the subdirectory that contains the data must be **ace/data**.

In this guide, the following conventions are used:

- ***ACEPROG*** stands for the full pathname to the directory that contains the Authentication Manager executable files.
- ***ACEDATA*** stands for the full pathname to the directory that contains the Authentication Manager databases.

As the administrator for RSA Authentication Manager, you must perform the post-installation setup tasks described in this chapter. With these tasks completed properly, your network resources are protected by RSA SecurID authentication.

Administrative Roles

An administrative role is a template defining a set of tasks that a user can perform on a specific realm, site, or group. By assigning administrative roles, you limit administrators to specific kinds of actions and specific areas of the RSA Authentication Manager database. After a role is defined, you can assign it to as many administrators as you choose without having to specify the same tasks and limitations in each individual user record.

CAUTION: The privilege of defining or assigning administrative roles, if abused, can have serious consequences for the security of your network. This privilege must be given only to highly trusted members of your staff.

The two components of an administrative role are:

Administrative scope. Specifies which sites, Agent Hosts, groups, users, and tokens can be affected by administrators to whom the role is assigned. For details, see the following section, "Administrative Scope."

Administrative task list. A named set of tasks that administrators, who are assigned a particular role, can perform within their administrative scope. For details, see "Task Lists" on page 33.

By combining a specific administrative scope with a specific task list, you place precise limits on an administrator's control of RSA Authentication Manager data.

Administrative Scope

Administrative scope, one of the two components of an administrative role, specifies which sites, Agent Hosts, groups, users, and tokens can be affected by administrators to whom the role is assigned.

There are three categories of administrative scope: realm, site, and group. Each category defines an administrator's privileges on one or more levels in the system. Within categories, administrative scope can be varied by specifying the realms, sites, or groups to which it applies: a realm administrator may be given control over one realm or several, and the same principle applies to site and group administrators.

The categories of administrative scope are hierarchical, in that privileges on a higher level include privileges on the levels below it. For example, a realm administrator can affect sites and groups within the realm, while the privileges of a group administrator do not extend beyond the group. However, no realm administrator has privileges over sites and groups that are not within the realm or realms specifically included in the assigned administrative scope. The RSA Authentication Manager filters the names of sites, groups, users, Agent Hosts, and tokens that appear on any administrator's screen according to this scope definition so that administrators can access only data within their scopes.

The three basic administrative scope categories distribute administrative privileges as follows within the specific realms, sites, or groups assigned:

- **Realm administrators** can view and edit all sites, groups, users, Agent Hosts and tokens (assigned and unassigned) within their designated realms.
- **Site administrators** cannot add or delete a site. They can view and edit their designated sites as well as the groups, users, Agent Hosts and assigned tokens belonging to those sites. Site administrators can also view and edit all unassigned tokens in the Authentication Manager database. They can view and edit all Agent Hosts, users, and tokens not belonging to any group or site.
- **Group administrators** cannot add or delete a group. They can view and edit their designated groups as well as the users, Agent Hosts, and assigned tokens belonging to those groups. Group administrators can also view and edit all tokens that are assigned to users in their groups and all unassigned tokens in the Authentication Manager database. They can view and edit all Agent Hosts, users, and tokens not belonging to any group or site.

Task Lists

A task list is the second component of an administrative role. It is a named set of tasks that administrators, who are assigned a particular role, can perform within their administrative scope. Tasks correspond to commands in the user interface. Commands not included in the task list for an administrator's assigned role are disabled on the menus that the administrator sees.

RSA Authentication Manager provides three predefined task lists: Realm, Site, and Group. These task lists include tasks that are appropriate for realm, site, or group administrators.

You can also create modified versions or entirely new task lists and assign them to administrators in your realm. This ability to customize roles gives you precise control over the authority of your administrators. However, you cannot enable an administrator to perform a task that is forbidden by the assigned administrative scope. It is important to remember that administrators' privileges are limited according to the assigned administrative scope and that they can perform only those tasks allowed by the scope definition, whatever the contents of the task list.

Using Administrative Scope and Task Lists Together

An administrative role is the combination of the administrative scope and the task list that you assign to a user. Consider the example of assigning the administrative role of New York site administrator for a large corporation with multiple sites.

- First, you assign the administrative scope of a site administrator limited to the New York site. This gives the user the authority to administer groups, users, Agent Hosts, and tokens associated with the New York site, but prohibits him or her from administering similar resources associated with other sites.
- Second, you assign the user the predefined site administrator task list. This means the user can perform the tasks that are required of a site administrator. These tasks include assigning administrative roles, importing and exporting tokens, adding and deleting groups, and editing the site.

You can also assign a second, assistant administrator to the New York site, but with a more restricted task list, such as the predefined Group Administrator task list or a custom task list you create. This assignment enables the assistant administrator to perform a limited set of tasks on all resources associated with the New York site, such as editing users, tokens, and groups, but not the full range of tasks permitted to the primary site administrator.

For information about creating a task list and assigning a task list to a user, see the Help topics "Creating a Task List" and "Assigning Administrative Roles." For a list administrative tasks and their subtasks, see the Help topic "Categories of Tasks."

To Begin: Click **User > Edit User** > **Administrative Roles**. For instructions, click **Help**.

Important Administrative Tools

The following features will help you manage your RSA Authentication Manager Agent Hosts, tokens, and users more efficiently.

System Design Tools

Open Agent Hosts

Open Agent Hosts are supported for all Agent types. If an Agent Host is "open," users are not required to be directly activated on the Agent Host or to be members of a group activated on the Agent Host. Any user registered in your Authentication Manager database can be authenticated on an open Agent Host. For more information, see "Agent Host/Authentication Manager Architecture" on page 23.

Note: If you plan to use RSA Authentication Agent 6.0 or 6.1 to enable offline authentication, and you want only some users to have this capability, you can control this on an Agent Host basis. In this case, you would not want to use an open Agent Host. Offline authentication (and related) capabilities are discussed in more detail in "Setting Up Offline Authentication and Password Integration" on page 59.

Automated Agent Host Registration and Updating

Automated Agent Host registration and updating reduces administrative overhead by enabling new Agent Hosts to register themselves with the Authentication Manager and by enabling existing Agent Hosts to automatically update their own IP addresses and **sdconf.rec** files. See "Automated Agent Host Registration and Updating" on page 65.

Consolidated Logging

All log messages are consolidated to the Primary. When activity on a Replica generates a log message, the message is eventually sent to the Primary and logged in the Primary log database. During heavy periods of authentication, consolidation of these *delta records* to the Primary database have a lower priority, but eventually are consolidated.

External Authorization

You can use External Authorization to apply additional criteria before users can access network resources. External Authorization criteria supplement RSA Authentication Manager authentication—they do not replace it. See "Customizing Your Authorization Procedures" on page 216.

Report Creation Utility

You can run standard reports (reports that cannot be modified or removed) and you can create and run custom reports. Audit trail reports are run against the **sdlog** database. Token statistic reports are run against the **sdserv** database. For more information, see "RSA Authentication Manager Report Creation Utility (Windows)" on page 174 or "RSA Authentication Manager Report Creation Utility (UNIX)" on page 183.

Custom Queries

The Custom Queries capability enables you to use provided sample SQL queries, or to create your own queries, to gather and view data from the RSA Authentication Manager log and user databases. For complete information, see "Creating and Running Custom SQL Queries" on page 193.

Administrative Support Tools

RSA Authentication Manager Control Panel

From the RSA Authentication Manager Control Panel, you can start and stop the RSA Authentication Manager services, view installation information, and perform various maintenance tasks, depending on what type of installation you are on. To access the RSA Authentication Manager Control Panel, click **Start > Programs > RSA Security RSA Authentication Manager Control Panel**. For information about individual tasks, see the *Administrator's Guide*, the *Windows Installation Guide*, and the Help.

Batch Token Replacement

With Batch token replacement you can replace tokens for large groups of users efficiently (for example, users whose tokens are about to expire). For more information, see the Help topic, "Replacing Many Tokens Using a Batch Procedure."

RSA SecurID Software Token Management

You can issue and revoke RSA SecurID software tokens through the Token menu. A software token is a software-based security token that resides on a user's computer. For more information, see the Help topic, "Issuing Software Tokens."

Automated Log Database Maintenance

Through scheduling and definition options, you can configure the RSA Authentication Manager to delete and archive log records. Regular backups and maintenance take place automatically according to the schedule and methods that you specify. For more information, see "Scheduling Automated Log Database Maintenance" on page 157.

Temporary Passwords

If a user loses a token, you can assign a temporary password to use until you assign and deliver a new token to the user. For more information, see "Temporary Passwords to Replace Lost Tokens" on page 128.

Remote Administration

With Remote Administration you can administer RSA Authentication Manager databases without being directly connected to them. The Remote Administration software runs on Windows 2003 Server, Windows XP Professional, and Windows 2000 (Advanced, Server, and Professional) machines.

With Remote Administration you can administer Windows or UNIX databases in your local realm or in registered remote realms. For more information, see "Remote Administration" on page 40.

Quick Admin

With the RSA Authentication Manager Quick Admin application, a Help Desk administrator can use a web browser to view and modify user, token, and extension record data in the RSA Authentication Manager database. For more information, see "Web-Based Administration with Quick Admin" on page 46.

Audit Log Messages in the Event Log

You can specify that certain audit log messages be written to the Event Log, based on selection criteria such as current logon, user name, affected token, Agent Host name, and Authentication Manager name. For more information, see "Monitoring Authentication Manager Events in the System Log" on page 170.

Customer-Defined Extension Records

The database records that define elements of your RSA Authentication Manager system—tokens, users, groups, Agent Hosts, logs—can be augmented with extension records that include any additional information you want to specify. For example, you might create a record for a user's home telephone or badge number. For more information, see "Maintaining Customer-Defined Data (Extension Records)" on page 100.

Introduction to the Database Administration Application

The Database Administration application enables you to perform administrative tasks, such as adding and editing users, Agent Hosts, realms, sites and groups; enabling offline, domain, and terminal services authentication, and login password integration; and generating reports regarding RSA Authentication Manager activity. The application runs in host mode (on Windows only) or remote mode.

Note: On UNIX platforms, while with the **sdadmin** program you can access many of the features of the RSA Authentication Manager software, Remote Administration provides a graphical user interface for administering an RSA Authentication Manager database and provides the only supported method of accessing all of the administrative features. For more information, see "Remote Administration" on page 40.

In host mode, the Database Administration application must be run on the Primary because it needs a direct connection to the RSA Authentication Manager database. In remote mode, the application can be run on a Windows 2000, Windows XP, and Windows 2003 machines through the Remote Administration service. The application handles multiple sessions by locking records that are in use, so that they cannot be changed from more than one session.

Before you can administer the database remotely, you must perform certain tasks directly on the Primary. For information, see the *Installation Guide* for your platform.

For more information and for instructions on running the Database Administration application remotely, see "Remote Administration" on page 40.

To run the Database Administration application in host mode:

On a Windows machine, click **Start** > **Programs** > **RSA Security > RSA Authentication Manager Host Mode**.

The Database Administration application main menu opens.

Exiting the Database Administration Application

To exit the Database Administration application, from the File menu, click **Exit**.

Important: Do not leave a machine unattended while the Administration application is running on it, either in host mode or in remote mode. Instead, exit the Administration application and log off. If you leave the machine unattended, anyone with access to the machine can make changes to Authentication Manager data under your identity.

Language Support (Windows)

The RSA Authentication Manager software supports the character sets of a number of ISO Latin-1 and Asian languages. You must configure your Windows system to support a specific language, and the RSA Authentication Manager database includes some fields that support English characters only.

ISO Latin-1 Languages

- English
- Finnish
- French
- German
- Norwegian
- Spanish
- Swedish

Asian Languages

- Chinese (Simplified and Traditional)
- Japanese (Katakana, Hiragana, and Kanji)
- Korean

To enable Authentication Manager database support for one of the non-English ISO Latin-1 languages, you must configure your Windows 2000 or Windows 2003 system to use the language before you install the RSA Authentication Manager software. To enable Authentication Manager database support for Chinese, Japanese or Korean, your system must be running the appropriate version of Windows.

Once you install RSA Authentication Manager on a non-English system, you cannot change the language back to English. If you were to attempt such a change, the RSA Authentication Manager database would still contain non-English characters that could not be displayed on the English language system.

For information about configuring your system to use one of the supported Latin-1 languages, see the *Windows Installation Guide*.

Important: Language support and use must be uniform throughout an RSA Authentication Manager installation. All Primary Authentication Managers, Replica Authentication Managers, and Remote Administration machines across all realms must support the same language. The language of each Replica database must be the same as the language of its Primary database, and you cannot administer an Authentication Manager database that supports one language from a Remote Administration machine that supports a different language. Users in a non-English language realm cannot authenticate in an English language realm.

Applicable Data Fields

All text fields in the RSA Authentication Manager database are enabled for non-English character input except for the restricted fields listed in the following table. These text fields accept only single-byte English characters:

Dialog Boxes	Text Field
Add User, Edit User	Default Login
Add Agent Host, Edit Agent Host	Name
Add Realm, Edit Realm	Primary Name
Add Realm, Edit Realm	Replica Name

Numeric fields accept only single-byte Arabic numerals.

Entering Japanese Characters with MS-IME97

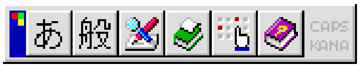
With the RSA Authentication Manager Database Administration application you can enter Japanese characters (Katakana, Hiragana, and Kanji) in all text fields of the Authentication Manager database, except those fields listed in the preceding section, "Applicable Data Fields."

To enter Japanese characters, you must use a machine running the Japanese version of Windows 2000, Windows XP, or Windows 2003 Server.

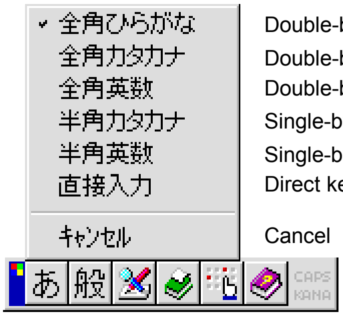
This section explains how to enter Japanese characters using the MS-IME97 (Microsoft Input Method Editor). For more detailed information on using MS-IME97, see the MS-IME97 System Help for Japanese Input.

Hiragana and Katakana

To enter Japanese characters in text fields in the RSA Authentication Manager Database Administration application from a workstation running a supported Japanese version of Windows, activate MS-IME97, and set the input mode to either Hiragana or Katakana. To activate the MS-IME97 (if it is not activated already), type Alt+~ on the standard 101-key keyboard or Alt+ [半角/全角] on the Japanese 106-key keyboard. When MS-IME97 is activated, a floating toolbar similar to the following illustration appears on the screen:



Click the leftmost button on the MS-IME97 toolbar to see a drop-down menu listing all the input modes supported by MS-IME97, as shown in the following illustration:



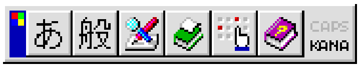
Double-byte Hiragana
Double-byte Katakana
Double-byte English alphanumeric
Single-byte Katakana
Single-byte English alphanumeric
Direct keyboard input (no Japanese conversion)

Cancel

To input Japanese characters, select double-byte Hiragana, double-byte Katakana, or single-byte Katakana while the input cursor is on a text field. There are two input modes: Kana and Romaji.

- Kana input maps each Hiragana/Katakana character to a key on your keyboard. When you press a key, a Hiragana or Katakana character, depending on the input mode, is displayed on your screen.
- For Romaji input, you must type a sequence of keystrokes, which MS-IME97 converts to a single Hiragana or Katakana character.

To choose Kana or Romaji input, click the fifth button on the toolbar, and select the first tab to change the basic settings for MS-IME97. Then use the drop-down list in the second field to change the input mode to the one you prefer. On the 106-key Japanese keyboard, you can toggle the input mode by pressing Alt+ [カタカナ ひらがな]. If you choose to use Kana input method, the KANA status on the toolbar is enabled and a floating toolbar similar to the following illustration appears on the screen:



Converting Hiragana and Katakana to Kanji

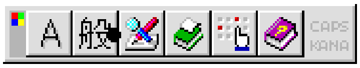
To enter Kanji characters, type the Katakana or Hiragana syllables that compose the sound of the equivalent Kanji characters. When you type Katakana or Hiragana syllables, they appear on your screen with a dotted underline. To convert them to Kanji characters, continue pressing the spacebar on the 101-key keyboard, or press either the spacebar or the [[illegible]] key on the 106-key Japanese keyboard until you find the Kanji characters you want. Press ENTER to place the selection in the input field.

During the Kanji conversion, if there are more than three candidates from which to choose, MS-IME97 displays a selection list with all the candidates. Press the up or down arrow key to highlight the one you want. Then press ENTER to put the selection in the input field.

Entering Characters in Single-Byte Fields

Note: For text fields that are not enabled for double-byte input, the RSA Authentication Manager Database Administration application does not prevent you from using MS-IME97. That is, even if the input focus is in these fields, you can switch the input mode to double-byte Hiragana, double-byte Katakana, double-byte English alphanumeric, or single-byte Katakana. However, if you enter any double-byte character or even a single-byte Katakana character in a field that is not enabled for double-byte input, an error message is displayed when you attempt to exit this field. Therefore, you must switch to Direct Keyboard Input mode when you are in any text fields not enabled for double-byte input.

To switch to Direct Keyboard Input mode from any other modes, press Alt+~ on the 101-key keyboard or Alt+ [半角/全角] on the Japanese 106-key keyboard. The leftmost button on the toolbar changes to indicate Direct Keyboard Input mode, as shown in the following illustration:



For information on using other features of MS-IME97, click the rightmost button on the toolbar to open the MS-IME97 System Help for Japanese Input.

Remote Administration

With Remote Administration you can connect to and manage the RSA Authentication Manager databases from a remote host. The remote host must have a copy of **sdconf.rec** in the **\ace\data\realms** directory. This directory is created on the host when you install Remote Administration.

Remote Administration connections to a Primary are read-write, so that you can change records in the database. Connections to Replicas are read-only. You can run reports and view the log and activity monitor, but you cannot change records.

After you authenticate and select the realm you want to administer, Remote Administration connects to the Primary using the name and IP address listed in **sdconf.rec**. Each Authentication Manager in the realm you are administering is listed in the upper left corner of the Database Administration application main menu. You can connect to a different Authentication Manager by clicking the radio button next to its name and IP address.

When you connect to the Primary or any Replica, the Authentication Manager sends a file named **failover.dat** to the realm directory on the remote host. This file has the IP address of the Authentication Manager, plus one alias IP address. The next time the remote host attempts to connect to that Authentication Manager, it uses the IP addresses specified in **failover.dat**.

Redirecting Remote Administration Connections

Remote Administration connections are redirected to a Replica when

- The IP address of the Primary has changed.
- A Replica is nominated to be the Primary.
- The Primary is unavailable.

In these situations, a message displays explaining that the connection cannot be established using the original Primary IP address specified in **failover.dat**. Remote Administration then connects to the next available Replica listed in **failover.dat**.

Managing Authentication Manager IP Aliases

You can update the alias IP address information for any Authentication Manager listed in **failover.dat** by selecting that Authentication Manager from the Remote Administration main window and clicking **Manage Server IP aliases**. The Manage Replica IP aliases dialog box lists all Authentication Managers in the realm. After you select an Authentication Manager, click one of the following buttons:

- **Auto Select**. Remote Administration automatically selects an alias IP address for that Authentication Manager.
- **Manually Select**. You select an alias from a list of possible corresponding IP addresses for the Authentication Manager you have chosen.

Note: The **Manage Server IP aliases** button does not appear on the Database Administration application main menu if you connect to an Authentication Manager that is configured to allow resolution of hosts and services by name. For more information, see "Enable Features" on page 237.

Remote Administration can be used in any of the following situations:

- If you are running the RSA Authentication Manager on Windows 2000 Professional, you can remotely administer its databases from a remote host running Windows 2000, Windows XP Professional, or Windows 2003 Server.
- If you are running the RSA Authentication Manager on UNIX, you can remotely administer its databases from a remote host running Windows 2000, Windows XP Professional, or Windows 2003 Server.

Note: On UNIX platforms, while with the **sdadmin** program you can access many of the features of the RSA Authentication Manager software, Remote Administration provides a graphical user interface for administering an RSA Authentication Manager database and provides the only supported method of accessing all of the administrative features.

If the Remote Administration session has remained idle for twelve or more hours, the error message "**Encryption Error: -1**" may appear. This message indicates that the session has timed out. Remote Administration supports 32 concurrent sessions.

Configuring a System for Remote Administration

By default, remote administration is *not* allowed on a UNIX system. To set up your UNIX system for remote administration, you must use the character-based version of the administration application. On the UNIX Primary, type:

```
./sdadmin
```

To set up an RSA Authentication Manager System for Remote Administration:

1. On the Primary, click **System** > **Edit System Parameters**.
   The System Parameter dialog box opens.
2. Select **Allow remote administration**.
3. Choose the authentication methods you want the RSA Authentication Manager to accept. (The following section describes your options.)
4. Close the dialog box, saving your changes.
5. Assign tokens to remote administrators.
6. Distribute these tokens.

Note: Each RSA Authentication Manager (Primary or Replica) that you intend to administer or work with remotely must have a record on the machine you use for remote administration. See the *Installation Guide* for your platform for instructions on installing Remote Administration software and adding records for the Authentication Managers or realms you want to administer or work with remotely.

Authentication of Remote Administrators

To administer an RSA Authentication Manager database remotely, an administrator must be authenticated by the Authentication Manager, which means that he or she must have a token record in its database.

RSA Security strongly recommends that administrators have a separate token for each realm. If an administrator were to use the same token in multiple realms, an attacker might be able to detect a tokencode as an administrator enters it in one realm and use this tokencode in another realm to gain access to the Database Administration application and, possibly, to other network resources.

Note: If an administrator *never* administers a database from any location outside the corporate firewall when authenticating, using a single token in more than one realm is less risky, but it is still not recommended.

Choosing Authentication Methods

The security administrator for each realm decides which administrator authentication methods to allow in the realm.

The kinds of tokens or passwords that can be used for authentication of remote administrators are set in the System Parameters dialog box within the Database Administration application.

Although any token or password type may be selected, RSA Security recommends that administrators use hardware tokens because these are most secure. The hardware tokens in this category are the RSA SecurID PINPad, standard card, and key fob.

Authentication Challenges

Remote administrators go through the same authentication process as other users. The only difference is in the screens they see. Therefore, if you are already familiar with authentication, you can omit the following instructions.

The instructions in the following section, "Normal Logon and Passcode Challenges," assume that you are using either an RSA SecurID standard card or key fob. If you are using a PINPad, when you are asked for a passcode (*except* at the beginning of the New PIN procedure):

1. Enter your PIN in the PINPad, and press the diamond near the bottom of the card.
2. At the keyboard, enter the tokencode displayed by the token, and click **OK**.

Normal Logon and Passcode Challenges

Usually, you see only one authentication dialog box with two challenges in it. If your token is in New PIN mode, go to "Authenticating When Your Token Is in New PIN Mode" on page 44.

To authenticate:

1. Click **Start** > **Programs > RSA Security > RSA Authentication Manager Remote Mode**.

   The Select Server to Administer dialog box opens.

2. Select the server you want to administer, and click **OK**.

   The Administrator Authentication dialog box opens.

3. Enter your user name in the Login field and your passcode in the passcode field.

   The passcode is your PIN followed by the tokencode displayed on the token.

4. Click **OK**.

   If your passcode is accepted, the main menu for the Database Administration application appears. The header shows the name of the Primary on which the database resides.

   If you are prompted for the Next Tokencode, see the following section, "Authenticating When Your Token Is in Next Tokencode Mode."

Authenticating When Your Token Is in Next Tokencode Mode

Occasionally, even after you enter your passcode correctly, the Authentication Manager prompts you for the next code displayed by your token because it needs to confirm that you have the token in your possession. This prompt indicates that your token is in Next Tokencode mode.

To authenticate when your token is in Next Tokencode mode:

1. Wait for the tokencode to change on your RSA SecurID token.
2. Enter *only* the tokencode.

   If the tokencode is correct, the passcode you originally entered is accepted and the main menu for the Database Administration application appears.

Authenticating When Your Token Is in New PIN Mode

The first time you log in with a specific token, the token is in New PIN mode. Depending on how your system is set up, you are required to take one of these actions:

- Choose between creating your own PIN and accepting a system-generated PIN (see the procedure that follows).
- Accept a system-generated PIN (see the procedure on page 45).
- Create your own PIN (see the procedure on page 46).

To authenticate in New PIN mode when you can choose the type of PIN:

1. Click **Start** > **Programs > RSA Security > RSA Authentication Manager Remote Mode**.

   The Select Server to Administer dialog box opens.
2. Select a server and click **OK**.
3. In the Administrator Authentication dialog box that opens next, enter the tokencode and click **OK**.

   You are asked if you want the system to generate your new PIN.
4. Do one of the following:
   - To have the system generate a PIN for you, enter **y** and click **OK**. You are asked if you are prepared to have the system generate your PIN.

     Being prepared means that you are ready to continue the procedure and that no one else can see the PIN when it appears on your screen.
   - To create your own PIN, enter **n**, click **OK**, and go to step 8.

   Note: Memorize your PIN. Do not write it down.

5. If you entered **y** in step 4, make sure you are prepared. Then enter **y** and click **OK**.

   The next dialog box displays your PIN with instructions to wait until your tokencode changes and then to enter a new passcode.

6. Following the instructions in the dialog box, enter a new passcode and click **OK**.

   Important: This dialog box remains open until you finish the authentication procedure. Therefore, to protect your PIN, finish the procedure immediately.

7. Follow the instructions on the screen to complete the authentication procedure with your system-generated PIN.
8. If you entered **n** in step 4, you are prompted to enter a new PIN.
9. Enter a PIN that matches the criteria in the prompt. Click **OK**.
10. Reenter your PIN to confirm it, and click **OK**.
11. Follow the instructions on the screen to complete the authentication procedure with the PIN you created.

To authenticate in New PIN mode when you must accept a system-generated PIN:

1. Click **Start** > **Programs > RSA Security > RSA Authentication Manager Remote Mode**.

   The Select Server to Administer dialog box opens.
2. Select a server and click **OK**.
3. In the Administrator Authentication dialog box that opens, enter the tokencode and click **OK**.

   A message informs you that you must accept a system-generated PIN and asks if you are prepared to have it generated.

   Being prepared means that you are ready to continue the procedure and that no one else will be able to see the new PIN when it appears on your screen.
4. Do one of the following:
   - To have the system generate a new PIN now, enter **y** and click **OK**.

     The next dialog box displays your PIN with instructions to wait until your tokencode changes and then to enter a new passcode. Continue with step 5.
   - If you do not want the system-generated PIN at this time, enter **n**, and click **OK**. The Remote Administration application closes.

   Note: Memorize your PIN. Do not write it down.

5. Following the instructions in the dialog box, enter a new passcode and click **OK**.

   Important: This screen will stay open until you finish the authentication procedure. To protect your PIN, finish the procedure immediately.

6. Follow the instructions on the screen to complete the authentication procedure.

To authenticate in New PIN mode when you must create your own PIN:

1. Click **Start** > **Programs** > **RSA Security** > **RSA Authentication Manager Remote Mode**.

   The Select Server to Administer dialog box opens.
2. Select a server and click **OK**.
3. In the Administrator Authentication dialog box that opens, enter the tokencode and click **OK**.

   A message prompts you to enter a new PIN.
4. Enter a PIN that matches the criteria in the message and click **OK**.

   Note: Memorize your PIN. Do not write it down.
5. Reenter your PIN to confirm it, and click **OK**.
6. Follow the instructions in the dialog box to complete the authentication procedure with the PIN you created.

Web-Based Administration with Quick Admin

With Quick Admin, administrators can use a web browser to view and modify user, token, and extension record data in the RSA Authentication Manager database. Because Quick Admin provides limited access to the database, it is ideal for help desks and for organizations that outsource help desk operations to a third party.

Quick Admin administrators can perform common tasks such as:

- Editing user and token information
- Deleting users
- Assigning a temporary password to a user
- Marking a token as Lost
- Resetting a token
- Editing user and token extension data
- Generating a user or token report

Quick Admin administrators *cannot* edit realm, site, group, or Agent Host records, create new user records, or import token records into the RSA Authentication Manager database.

In addition, in Quick Admin, administrators can access only user and token reports, and a subset of user and token extension data functionality.

Note: For a list of the specific tasks available through Quick Admin, see the Help topic "Categories of Tasks". Tasks marked with an asterisk (*) are available in Quick Admin.

Quick Admin Architecture

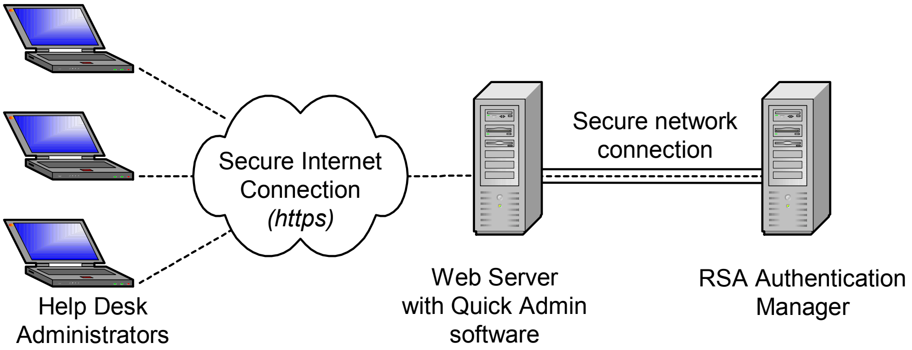
Quick Admin consists of:

- Java servlets accessible through a web server. These servlets are powered by the Apache Jakarta Tomcat 5.5.7 servlet engine.
- A back-end process that runs on the RSA Authentication Manager Primary Server. This process, named RSA Authentication Manager Quick Admin Daemon, manages the encrypted communication between the servlets and the Primary database.

Do not install the web server on the same machine as the RSA Authentication Manager. For complete installation and configuration information, see the *Installation Guide* for your platform.

Important: For security purposes, RSA Security strongly recommends that you follow the latest Apache Software Foundation guidelines and best practices. For more information, go to **http://jakarta.apache.org/tomcat**.

The following diagram illustrates the Quick Admin architecture.


Secure Internet Connection (https)
Secure network connection
Help Desk Administrators
Web Server with Quick Admin software
RSA Authentication Manager

Administrative Roles in Quick Admin

Quick Admin 6.1 enforces the administrative roles defined in the RSA Authentication Manager. An administrative role is a template defining a set of tasks that a user can perform on a specific realm, site, or group. By assigning administrative roles, you limit administrators to specific kinds of actions and specific areas of the RSA Authentication Manager database.

The two components of an administrative role are:

Administrative scope. Specifies the sites and groups (and therefore users and their tokens) that can be managed by administrators with the assigned role. You have the option of disabling administrative scoping for Quick Admin. For instructions, see "Disabling Quick Admin Administrative Scoping" on page 48.

Administrative task list. A named set of tasks that administrators, who are assigned a particular role, can perform within their administrative scopes. In Quick Admin, tasks not included in a Quick Admin administrator's defined task list are unavailable. For information, see "Setting Up Task Lists" on page 48.

Disabling Quick Admin Administrative Scoping

If you prefer that Quick Admin not enforce administrative scoping, you can configure Quick Admin to enforce administrative task lists only. This means that administrators using Quick Admin may perform their assigned tasks on records that are outside of their assigned scopes.

To disable Quick Admin scoping:

1. Make sure all Quick Admin administrators have logged off of their Quick Admin sessions.
2. On Windows machines, in the ***%SystemRoot%*\system32**\ directory on the Primary, open the **apidemon.ini** file.

   On UNIX machines, in the ***ACEPROG*** directory on the Primary, open the **apidemon.ini** file.

   The **apidemon.ini** file consists of one or more text lines, each defining one key. SCOPE is the key that determines whether or not Quick Admin enforces administrative scoping.

   For specific information about the **apidemon.ini** file, see "Configuring the apidemon" in the *Administration Toolkit Reference Guide* (**authmgr_admin_toolkit.pdf**).
3. In the **apidemon.ini** file, find the line that reads

   ```
   SCOPE=TRUE
   ```
4. To disable Quick Admin scoping, change "TRUE" to "FALSE" so that the line reads

   ```
   SCOPE=FALSE
   ```
5. Save and close the **apidemon.ini** file.
6. Restart Quick Admin by closing and relaunching the browser.

Quick Admin no longer enforces administrative scoping.

Setting Up Task Lists

To Begin:

- To add a task list, on the Primary click **System** > **Task Lists** > **Add Task List**. For instructions, click **Help**.
- To assign a task list to your Quick Admin administrators, click **User > Edit User > Administrative Role** and, from Task List options, select the task list that you set up for Quick Admin administrators. For more information, click **Help**.

To access Quick Admin, administrators *must* have either the List User task or the List Tokens task (or both) in their task list. The following table shows tasks that can be in a Quick Admin administrator's task list.

Note: The "Additional Tasks" column in the following table lists further actions that you can allow Quick Admin administrators to perform. However, because these tasks modify the user database, RSA Security recommends that you are careful about which ones to add to the task lists of Quick Admin administrators.

Type of Information	Required Tasks	Additional Tasks
Edit User Information	• List User • Edit User	• Edit Token-User Assignment **Note**: In Quick Admin, this task controls the Unassign Token operation. • Set/Change User Password • Remove User Password • Delete User • Replace Token • Edit User-Group Assignment **Note**: In Quick Admin, this task allows admins to only *view* group membership. It does not allow them to *edit* group membership. • Edit User Extension Data
User Reports	List User	N/A
Edit Token Information	• List Tokens • List Users • Edit Token	• Edit Token Extension Data • Edit Lost Status • Edit Token-User Assignment **Note**: In Quick Admin, this task controls the Unassign Token operation. • Enable/Disable token • Clear PIN **Note**: In Quick Admin, this task controls the Reset Token operation. • Resynchronize Token • Set New PIN Mode • Replace Token
Token Reports	List Tokens	N/A

Authentication of Quick Admin Administrators

To gain access to Quick Admin, administrators must authenticate to the Authentication Manager. Therefore, each administrator must have a user record with an assigned token in the RSA Authentication Manager database.

RSA Security strongly recommends that Quick Admin administrators have separate tokens for each realm. If an administrator were to use the same token in multiple realms, an attacker could detect a tokencode as an administrator enters it in one realm and could use this tokencode in another realm to gain access to Quick Admin.

Note: To access Quick Admin, administrators must have either the List User task or the List Tokens task (or both) in their task lists.

Choosing Administrator Authentication Methods

The security administrator for each realm decides which authentication methods to allow for administrators in the realm. The types of tokens that can be used for authentication of remote administrators are set in the System Parameters dialog box within the Database Administration application. The default setting is **SecurID Cards and Fobs**.

Although any token or password type can be selected, RSA Security recommends that administrators be required to use hardware tokens, because these are the most secure. Hardware tokens include the RSA SecurID PINPad, standard card, and key fob.

The least secure method for administrator authentication is the user password, which does not involve two-factor authentication.

Quick Admin administrators use the same basic authentication process as other users. For instructions, see the Quick Admin Help topic "Logging On and Off."

Guidelines for Searches and Reports

Searches

Quick Admin administrators can search for specific users and assigned tokens. The more specific the search query is, the less time it takes to retrieve the information. If your Authentication Manager database is very large, a search can take a long time to complete. You can limit the search result by configuring the **Max_Search** variable in the **quickadminconfig.properties** configuration file. This file is located in the ***Quick Admin installation directory*****\Tomcat\webapps\ quickadmin\WEB-INF\ properties** directory.

Note: To search for users, administrators must have the List User task in their task list. To search for assigned tokens, administrators must have the List Tokens task.

Reports

Quick Admin administrators can generate user and token reports. Reports are stored in text files in the ***Quick Admin installation directory*****\Tomcat\webapps\quickadmin\WEB-INF\reports** directory on the Quick Admin web server. To conserve disk space, clean out this directory periodically.

Advise Quick Admin administrators to restrict their reports as much as possible. The greater the number of records retrieved, the longer it takes to generate the report. If they need to generate large reports, RSA Security recommends that you turn off Quick Admin logging. To turn off logging, open ***Quick Admin installation directory*\\Tomcat\webapps\quickadmin\WEB-INF\properties\quickadminconfig.properties** in a text editor, and set the **Verbose** parameter to **no**.

Note: To generate user reports, administrators must have the List User task in their task list. To generate token reports, administrators must have the List Tokens task.

Reconfiguring Quick Admin

In certain situations, such as when you nominate a Replica to the Primary, you must reconfigure the Quick Admin settings to maintain functionality. To do that, follow the instructions in this section.

First, reconfigure the information in the **quickadminconfig.properties** file on the machine on which the Quick Admin software is installed**.** This file usually resides in the ***Quick Admin installation directory*\Tomcat\webapps\quickadmin\WEB-INF\properties** directory.

To reconfigure the quickadminconfig.properties file:

1. Change the **ACE_SERVER** parameter to the fully-qualified DNS name of the new Primary.

   For example, if the name of the new Primary is **oxygen**, the fully-qualified DNS name would be **oxygen.*yourdomainname***.

2. Change the **ACE_IP** parameter to the IP address of the new Primary.

Next, you must reconfigure the Primary directory located in the ***Quick Admin installation directory*\Tomcat\webapps\quickadmin\WEB-INF\certs** directory.

To reconfigure the Primary directory:

1. Go to the ***Quick Admin installation directory*\Tomcat\webapps\quickadmin\WEB-INF\certs** directory.
2. Delete the subdirectory that has the name of the old Primary.
3. Create a subdirectory with the name of the new Primary.
4. From the ***ACEDATA*** directory of the new Primary, copy the **sdti.cer** and **server.cer** files into the subdirectory that has the name of the new Primary.

For the change to take effect, stop and restart the Tomcat server on the machine on which Quick Admin is installed.

Finally, you must make some changes to the ***ACEPROG*\hosts.conf** file on the new Primary.

To change the hosts.conf file:

1. Open the ***ACEPROG*\hosts.conf** file.
2. Add the fully-qualified DNS name and IP address of the Quick Admin machine.
3. Stop and restart the RSA Authentication Manager.

   On Windows, perform the following steps:

   - On the Primary, click **Start > Programs >RSA Security > RSA Authentication Manager Control Panel**.
   - In the RSA Authentication Manager Control Panel window, in the left pane, select **Start & Stop RSA Auth Mgr Services**.
   - In the right pane, click **Stop All**. If a warning message appears, click **OK**.
   - When the RSA Authentication Manager is fully stopped, click **Start All**.
   - Click **Close**.

   On a UNIX machine, type:

   ```
   sdconnect stop
   aceserver stop

   sdconnect start
   aceserver start
   ```

Troubleshooting

For information about troubleshooting specific Quick Admin error messages, see Appendix C, "Troubleshooting."

If Quick Admin administrators experience problems logging on to Quick Admin, verify the following items:

- The correct token or user password is assigned to the UserID that the administrator entered when attempting to log on.
- The administrator with that UserID has sufficient RSA Authentication Manager administrative rights.
- Valid copies of the Primary **sdti.cer** and **server.cer** files are located in the ***Quick Admin installation directory*\Tomcat\webapps\quickadmin\WEB-INF\certs\*servername*** subdirectory on the web server host.

Also, look at the RSA Authentication Manager Activity log and the Tomcat log files (located in the ***Quick Admin installation directory*\ Tomcat\logs** subdirectory on the web server host).

Note: The Quick Admin software installed on your web server logs all transactions to a log file (**stdout_*date*.log** on Windows or **catalina.out** on Solaris) in the ***Quick Admin installation directory*\Tomcat\logs\** directory. Log files can grow large enough to completely fill the disk space on the web server. RSA Security recommends that you monitor the growth of the log files, periodically archive them, and then delete them from the web server.

Quick Admin Next Steps

- For information about installing or upgrading Quick Admin, see the chapter “Installing the RSA Authentication Manager Quick Admin Software” in the *Installation Guide* for your platform.
- For information about Quick Admin procedures, see the Quick Admin Help included with the product.
- For information about troubleshooting specific Quick Admin error messages, see “Messages” in Appendix C, “Troubleshooting.”
- For information about installing RSA SecurID Web Express on the same web server as Quick Admin, see the *Installation Guide* for your platform.

3 Agents and Activation on Agent Hosts

This chapter describes RSA Authentication Agent software and activation on Agent Hosts. For RSA SecurID authentication protection, a computer or other device running RSA Authentication Agent software must be registered as an Agent Host in the RSA Authentication Manager database, or must be a client of a registered Agent Host.

Using the RSA Authentication Manager Database Administration application, an authorized administrator can add an Agent Host record to the Authentication Manager database and modify it at any time.

During a typical user authentication, when a user attempts to gain access to a personal computer or other protected resource, the RSA Authentication Agent receives the request, prompts the user for a passcode, and sends the passcode to the RSA Authentication Manager. The Authentication Manager authenticates the user and sends back authentication access or denial to the RSA Authentication Agent. The Agent in turn sends back authentication access or denial to the protected device that the user is attempting to access.

With this release, RSA Security introduces new capabilities for RSA SecurID in the Microsoft Windows environment. You can use RSA Authentication Manager 6.1 and RSA Authentication Agent 6.0 or 6.1 to enable:

Offline Authentication. Whether connected to the network or offline, users can log on to protected resources with their RSA SecurID tokens. When the user is traveling, at home, or when the network connection to the RSA Authentication Manager is temporarily unavailable, offline authentication data stored on users' computers, or on domain and terminal servers, enables users to authenticate with RSA SecurID. If users misplace their tokens or forget their PINs, administrators can provide emergency tokencodes and passcodes that users can log on to their offline computers.

Windows Password Integration. With this option, when users enter an RSA SecurID passcode to log on to a protected resource, their logon password is automatically sent to the Windows authentication service. Users do not have to enter passwords manually. This can simplify and improve an organization's password security policies and reduce costs associated with password maintenance.

For more information about administering these capabilities, see "Setting Up Offline Authentication and Password Integration" on page 59.

For an overview of the system architectural options around these capabilities, and for references to the information you need to implement the RSA SecurID for Microsoft Windows solution, see the *RSA SecurID for Microsoft Windows Planning Guide*.

For information about installing and configuring the Agent on the various protected resources in your network environment, see the *RSA Authentication Agent 6.1 for Microsoft Windows Installation and Administration Guide*.

Downloading the Latest Agent for your Platform

RSA Security provides the latest RSA Authentication Agent software for your platform at **http://www.rsasecurity.com/node.asp?id=1174**. Included with the Agent download package is an installation and administration guide and a *Readme*. RSA Security recommends that you read the documents before installing the Agent.

Creating and Modifying Agent Hosts

After you or an Agent administrator installs and configures the Agent software, you must add an Agent Host record to the Authentication Manager database for each Agent Host in the realm. If you set up auto-registration of Agent Hosts, their records are added to the database automatically. For details, see "Automated Agent Host Registration and Updating" on page 65 and the following section, "Auto-Registered Agent Hosts."

If you do not plan to use auto-registration of Agent Hosts, you need to specify in the Authentication Manager database which local resources are running RSA Authentication Agent software and need to be protected by RSA SecurID authentication.

To Begin: Click **Agent Host > Add Agent Host**. For more information, click **Help**.

Note: To edit an Agent Host record after you have added it to the RSA Authentication Manager database, click **Agent Host > Edit Agent Host**.

Auto-Registered Agent Hosts

You can configure your system so that new Agent Hosts register themselves and update their own records in the RSA Authentication Manager database. For information on how to use auto-registration for Windows, HP-UX, AIX, and Solaris Agent Hosts on your system, see "Automated Agent Host Registration and Updating" on page 65.

Note: Standard auto-registration assumes that the Agent Host supports the DNS method of address/name resolution. If this is not true for the Agent Host you are adding, run the Configuration Management program and make sure that the **Resolve Hosts and Services By Name** box (in the Hosts panel) is *not* selected. If none of your Agent Hosts support DNS resolution, there is no reason to select this box again, but if some Agent Hosts support DNS and some do not, select or clear the box as required.

Default Agent Host Settings

When the auto-registration program is run on a newly installed, unregistered Agent Host, a record for the Agent Host is created in the Authentication Manager database. By default, the Agent Host has these characteristics:

- Open access
- Set to search other realms for users who are not known locally
- Type is UNIX Agent Host

- Uses DES encryption
- The Acting Master is set to the server that performed registration
- No Acting Slave is configured

If these default settings are not appropriate for the new Agent Host, edit the record to change the settings as appropriate. Click **Agent Host** > **Edit Agent Host** and select the record for modification. The Edit Agent Host dialog box opens.

Modifying Agent Host Extension Data

Use the **Edit Agent Host Extension Data** button in the Add or Edit Agent Host dialog box to modify information in Agent Host Extension records. These records contain information defined by your organization that can be accessed by custom administration programs.

For information on creating custom administration programs with the RSA Authentication Manager Administration Toolkit, see the *Administration Toolkit Reference Guide* (**authmgr_admin_toolkit.pdf** in the ***ACEDOC*** directory).

Generating and Editing an Agent Configuration Record

Every device defined as an RSA Authentication Agent Host has an RSA Authentication Manager configuration file (**sdconf.rec**) in the ***%SYSTEMROOT%*\system32** directory (on Windows machines) or the ***ACEDATA*** directory (on UNIX machines). RSA Authentication Manager creates the initial configuration file during the installation of the Primary and stores it in the ***ACEDATA*** directory on the Primary.

Under most circumstances, you can copy this **sdconf.rec** file to Agent Hosts before you install the RSA Authentication Agent software.

Note: A number of manufacturers use the RSA Authentication Agent toolkit to build their own Agents. Some of these third-party Agents do not use the **sdconf.rec** file.

For some types of Agent Hosts, you need to generate the **sdconf.rec** file. The process of generating the configuration file ensures that it includes configuration data that the Agent Host may need, for example:

- The identities of the Acting Master and Acting Slave, required to support legacy Agent Hosts (see "Legacy Agent Hosts" on page 75).
- Alias IP addresses for the Primary, required to support authentication through firewalls (see "Authentication Manager and Agent Host Communication Through Firewalls" on page 25).

To generate the configuration file for an Agent Host, open the Database Administration application (described in Chapter 2, "Using RSA Authentication Manager Administration Applications"), and click **Agent Host** > **Generate Configuration Files**. Click **Help** for details and instructions.

To edit a configuration file, you run the Configuration Management application on Windows systems or ***ACEPROG*/sdsetup -config** on UNIX systems. For more information, see Chapter 12, "Configuring the RSA Authentication Manager (Windows)" or Chapter 14, "Configuring the RSA Authentication Manager (UNIX)."

Note: If you add a legacy Agent Host *after* installing RSA Authentication Manager 6.1, you must enter the identities of the Acting Master and Acting Slaves manually. See "Load Balancing by Agent Hosts" on page 69.

You can also use the Configuration Record Editor (**sdcfgedit_ui.exe** in the ***ACEPROG*** directory) to edit the Acting Master and Slave specifications in any **sdconf.rec** file. For instructions, see "Legacy Agent Hosts" on page 75.

If your system is configured for automated Agent Host registration, running the auto-registration and update utility on a new Agent Host registers the Agent Host in the database, and an administrator does not need to create the Agent Host record.

You can also run this utility any time the Agent Host IP address has changed to update the IP address field of the Agent Host record in the Authentication Manager database. This update feature is especially useful for systems that use the Dynamic Host Configuration Protocol (DHCP) to assign IP addresses to Agent Host resources. For more information, see "Automated Agent Host Registration and Updating" on page 65.

An Agent Host can be configured as a restricted or an open Agent Host. A restricted Agent Host allows access only to those users who are specifically activated on the Agent Host, or who belong to groups that are specifically activated on the Agent Host.

Resources protected by a restricted Agent Host are considered to be more secure because, rather than allowing access to any user in the RSA Authentication Manager database, only users who are activated individually or as part of a group are allowed access.

If you plan to implement limited access to certain resources, you must protect those resources with a restricted Agent Host. An open Agent Host can be configured to allow access to users in these categories:

- Any user in the database that has authenticated with RSA SecurID, provided that the user is not specifically activated on the Agent Host with time restrictions that prohibit access at the current time, or does not belong to a group with similar time restrictions. (See "Restricting Access to Open Agent Hosts" on page 65.)
- Any user in the database that has authenticated with RSA SecurID, without other restrictions.

Another configuration setting, if positive, instructs the Agent Host to search other realms that are registered in the home realm database for unknown users, thereby opening the Agent Host to cross-realm authentication. If the setting is negative, only users in the Agent Host's home realm are admitted.

Any Agent Host, whether restricted or open, can have its own list of authorized users. You create this list by activating users on the Agent Host or by making users members of groups that are activated on the Agent Host. See "Activation on Agent Hosts" on page 122. (The only reason to activate users and groups on an open Agent Host is to place time restrictions on their access.)

Setting Up Offline Authentication and Password Integration

Working together, RSA Authentication Manager 6.1 and RSA Authentication Agent 6.1 enable local, domain, and Terminal Services authentication, as well as login password integration. Most of the installation and configuration of these features is done on the Agent side For more information, see *RSA Authentication Agent 6.1 for Microsoft Windows Installation and Administration Guide*.

On the Authentication Manager, using Database Administration, you can enable offline authentication and Windows password integration for the entire system, then enable or disable these capabilities for specific Agent Hosts.

Note: For offline authentication and password integration to work properly, users must have exactly the same login name in the RSA Authentication Manager database as in their Windows environment. If users are defined on a supported LDAP server, you can use RSA Authentication Manager LDAP synchronization feature to import users to the RSA Authentication Manager database. For more information, see "Synchronizing LDAP User Records" on page 108.

Specifying Offline Authentication at the System Level

You can set a number of offline authentication parameters at the system level. These parameters become the defaults for Agents. In addition, you can specify offline authentication and password integration settings for individual Agents. For more information, see "Setting Offline Authentication and Password Integration for Agents" on page 61.

The following table describes parameters that you can specify at the system level.

Parameter	Description
Enable offline authentication at system level	Determines whether offline authentication is allowed.
Offline Authentication Security Settings: • Provide enabled agents with a maximum of *nn* days of offline data • Require PIN + Tokencode entry to be at least *nn* characters • Allow offline authentication with alternate token types: PINPads, tokencode-only tokens, and static passwords	Controls the number (*nn*) of offline days that users can have on their system, the required length of their passcodes, and which, if any, alternate token types can be used with offline authentication. If your users have already downloaded offline authentication data, and you then reduce the maximum number of days of data, users will still be able to authenticate as long as they have offline data left. When users connect to the network, only then will the reduced number of offline days be downloaded. RSA Security recommends that a passcode be at least 12 characters. It is important to consider whether enabling the alternate token types will reduce your organization's required level of security for offline authentication. For example, with tokencode-only tokens, if a user's computer and token are stolen, the intruder can gain unrestricted access.

Parameter	Description
Offline Emergency Codes: • Generate offline emergency codes • Code Types: – Offline emergency tokencodes – Offline emergency passcodes – Both • Codes Contain: – Numbers – Characters – Punctuation Marks • Require emergency code after *nn* offline authentication failures • Emergency codes expire after *nn* days	If a user is locked out of his or her computer (for example, has entered too many bad passcodes), the RSA Authentication Manager administrator can provide an emergency code that the user can use to gain entry. These parameters control whether the emergency codes are allowed, the types of codes that are allowed, when they are required, and when they expire. Typically, when users are locked out, they call the administrator, who can look up and provide their emergency code to enable them to access their computers. For more information about the emergency code, see "Enabling Emergency Access for Offline Authentication Users" on page 62.
Warn users when only *nn* days of offline authentication data remain	You can specify that users be automatically warned when they have only a certain number of days of offline authentication data remaining.
Upload offline authentication log entries when user reconnects	Offline authentication log activity on users' computers can be sent back to the Authentication Manager's log database whenever the users reconnect to the network.
Enable verbose offline authentication logging	Provides more detailed logging of offline authentication activity and failures, for example, when users' PIN and Tokencode (passcode) combinations are not the required length.

To Begin: In the Database Administration application, click **System** > **System Configuration** > **Edit Offline Authentication**. For complete instructions, click **Help**.

Enabling Password Integration at the System Level

As with offline authentication, you can specify password integration at the system level. However, as described in the following section, "Setting Offline Authentication and Password Integration for Agents," you can disable this parameter for individual Agents.

To Begin: In the Database Administration application, click **System** > **Edit System Parameters**. Click **Enable Windows password integration at system level**.

Setting Offline Authentication and Password Integration for Agents

By default, computers running RSA Authentication Agent 6.1 use system-level parameters for offline authentication and password integration. However, in Database Administration, you can disable these parameters for specific Agents.

For example, if you have some Agent Hosts that are set as open Agent Hosts, you might want to disable one or both of these features.

To Begin: Click **Agent Host** > **Add Agent Host** (or **Edit Agent Host**). For instructions, see the Help topic "Adding an Agent Host" or "Editing an Agent Host."

Enabling Remote Access Agent Hosts to Function in Protected Domains

If your domain is protected with RSA Authentication Agent 6.1 for Microsoft Windows, and includes remote access applications, domain authentication and remote authentication are incompatible. To solve this problem, the Authentication Agent administrator must tell the Agent on the domain controller how to address the remote access application hosts during authentication. If the remote access application has another RSA SecurID application installed on it, the Agent administrator tells the Agent on the domain controller to verify whether the remote access application host recently made a valid authentication request to the RSA Authentication Manager. If the remote access application host did make a valid request, the Agent allows access to the domain. For more information, see "Using Domain Authentication With Remote Authentication" in the *RSA Authentication Agent 6.1 for Microsoft Windows Installation and Administration Guide*.

For verification to work, you must enable the RSA Authentication Manager to create verifiable authentications for the remote access application host.

To Begin: In the Database Administration application, click **Agent Host** > **Edit Agent Host**, and select **Create Verifiable Authentications**. For more information, see the Help topic "Editing an Agent Host."

Important: After you select **Create Verifiable Authentications** for an Agent Host, and save the changes, you must restart the RSA Authentication Manager to complete the configuration. If you are editing a number of Agent Hosts to specify this setting, you can configure them all before restarting the Authentication Manager.

Supporting Web Applications in Front-End/Back-End Environments

In protected front-end/back-end environments, the front-end web server performs the RSA SecurID challenge, and the back-end performs the Windows challenge.

To support these types of environments, you need to create an Agent Host record in RSA Authentication Manager for the front-end, copy the Agent Host record for the back-end, and ensure that both Agent Hosts are set up to create verifiable authentications. Both Agent Hosts need to have identical user and group activations.

To Begin: In the Database Administration application, for the front-end component, click **Agent Host > Add Agent Host**. Fully define Agent Host settings, including user and group activations, and be sure to select **Create Verifiable Authentications**. For the back-end component, click **Agent Host > Copy Agent Host**, and make a copy of the front-end component. Name the copy for the back-end component, and confirm that **Create Verifiable Authentications** is selected. For more information, see the Help topics "Adding an Agent Host" and "Copying an Agent Host."

To complete the configuration, place both the front-end and back-end Agent Hosts in the Verify Group of the Domain Agent Host running on the domain controller. For complete information, see "Configuring Web Servers for RSA SecurID Authentication" in the *RSA Authentication Agent 6.1 for Microsoft Windows Installation and Administration Guide*.

Enabling Emergency Access for Offline Authentication Users

Several unusual situations can lock users out of their computers:

- Users' systems have been disconnected from the network for a long period, causing the data to expire.
- Users type in more than the allowed number of incorrect passcodes.
- Users forget their PINs.
- Users lose their tokens.

In any of these situations, the user must contact the RSA Authentication Manager administrator, who can provide an emergency code.

Note: For security purposes, any time an administrator views an emergency code, RSA Authentication Manager logs the event.

There are two types of emergency codes: an offline emergency tokencode and an offline emergency passcode.

Offline Emergency Tokencode

If users of offline authentication misplace their RSA SecurID tokens, they must contact their RSA Authentication Manager administrators to receive an emergency tokencode. Users can then enter their regular PINs followed by the offline emergency tokencode to authenticate and gain access to their offline computers.

Note: Assuming the user finds the misplaced token, the token is put into New PIN mode the next time the user attempts to perform a connected authentication.

To view an offline emergency tokencode so that you can provide it to a user, start by editing the token from the RSA Authentication Manager Database Administration application.

To Begin: Click **Token** > **Edit Token**. For instructions, see the Help topic "Editing a Token."

Offline Emergency Passcode

If users of offline authentication forget their PINs, they will need an offline emergency passcode to authenticate to their offline computers. To view an offline emergency passcode so you can provide it to a user, start by editing the user from the RSA Authentication Manager Database Administration application.

To Begin: Click **User** > **Edit User**. For instructions, see the Help topic “Editing a User.”

Note: Because an offline emergency passcode does not require a PIN, be sure to confirm the user’s identity.

Configuring Agents to Handle Incorrect Passcodes

The RSA Authentication Manager system requires that some false passcode entries be tolerated. System security demands that intruders be prevented from trying one entry after another until a lucky guess results in a successful authentication. You can specify in RSA Authentication Manager the number of incorrect authentication attempts to accept before taking each of the following actions:

- Putting the token into Next Tokencode mode
- Disabling the token

For example, the RSA Authentication Manager system receives an authentication request from someone who appears to be a registered user. The user is asked for a passcode and enters a value that is incorrect. When informed of this error, the user continues to enter incorrect passcodes. When the number of incorrect passcodes entered reaches the limit set for the Agent, the token is disabled. The token must be enabled by an administrator before it can be used again.

Suppose again, however, that after entering several incorrect passcodes, the user enters one that happens to be correct. The Authentication Manager could accept it, but coming after a sequence of incorrect passcodes it could be a lucky guess. Putting the token into Next Tokencode mode tests whether the person entering the passcodes actually has the token in his or her possession. In this mode, the Agent requires the user to enter two consecutive passcodes. If this cannot be done correctly, and the false entries continue, the Authentication Manager disables the token as soon as the limit is reached.

Next Tokencode mode is not invoked unless the user enters a valid passcode. By default, the RSA Authentication Manager accepts three incorrect entries (prior to one correct entry) before putting a token in Next Tokencode mode, and ten incorrect entries before disabling a token.

To configure Agent management of incorrect passcodes on a Windows server:

1. Click **Start** > **Programs > RSA Security > RSA Authentication Manager Configuration Tools > RSA Authentication Manager Configuration Management**.
2. Click **Agent**.
3. Enter the configuration values for each Agent type.

4. Click **OK**.
5. Click **OK**.
6. Repeat these steps on all servers in the realm as this information is not replicated.

For more information, see "Agent Host Passcode Configuration" on page 242.

To configure Agent management of incorrect passcodes on a UNIX server:

1. Run ***ACEPROG*/sdsetup -config**.
2. Press RETURN to move through the prompts.
3. Enter the configuration values at the following prompts:

```
How many wrong PASSCODEs before a token is set to next
tokencode?

How many wrong PASSCODEs before a token is set to
disabled?
```

For more information on configuring the RSA Authentication Manager for UNIX, see Chapter 14, "Configuring the RSA Authentication Manager (UNIX)."

Open Agent Hosts

The open Agent Host feature decreases administrative overhead by eliminating the need to activate individual users on an Agent Host or put them in groups activated on the Agent Host. Any user who is registered in your Authentication Manager database can be authenticated on an open Agent Host, without being activated on it either directly or through group membership. However, you may want to activate users or groups even on open Agent Hosts in order to place time restrictions on their access. For information, see "Restricting Access to Open Agent Hosts."

Specifying an Open Agent Host

You can designate an Agent Host as open by selecting the **Open to All Locally Known Users** checkbox in the Add Agent Host or Edit Agent Host dialog box. You also have the option of selecting **Search Other Realms for Unknown Users**, which opens the Agent Host to cross-realm authentication by users from other realms registered in the local database.

If you use automated Agent Host registration, the new Agent Hosts will register themselves as open Agent Hosts by default. For more information, see "Load Balancing by Agent Hosts" on page 69.

Restricting Access to Open Agent Hosts

Users and groups may be activated on open Agent Hosts just as they are on restricted Agent Hosts. If a user is either directly activated on an Agent Host or activated through membership in a group that is enabled on the Agent Host, an open Agent Host may not be open to this user because of access time restrictions.

When the Authentication Manager authenticates a user, it checks to see if the user is directly activated on the Agent Host. If the user is directly activated, the Authentication Manager determines whether the user has access time restrictions. If there are no time restrictions or the user is authenticating at a permitted time, the user is granted access to the Agent Host.

If a user is not directly activated on the Agent Host, the Authentication Manager checks the user's group activations. If the user is activated on the Agent Host through one or more groups, the Authentication Manager checks to see if the groups have access time restrictions. For example, if the user is a member of Group 1, which can log on between 8 a.m. and 5 p.m, the user can log on only during these hours. If this user is also a member of Group 2, which can log on between 8 p.m. and 8 a.m., the user is denied access only between 5 p.m. and 8 p.m.

Automated Agent Host Registration and Updating

The Automated Agent Host Registration and Updating features of RSA Authentication Manager reduce administrative overhead in several ways:

- A new Agent Host can register itself in the Authentication Manager database rather than requiring an administrator to create an Agent Host record.
- An existing Agent Host can update its own IP address in the Authentication Manager database if the address is changed (for example, through DHCP).

Note: The name of the Agent Host must remain the same. If both the name and the IP address change, the Authentication Manager will create a new entry.

- An existing Agent Host can update its own **sdconf.rec** file with relevant changes from the Authentication Manager configuration file. Changes to the Acting Authentication Managers and alias IP address information are not sent.

These features are available for supported versions of Windows, HP-UX, AIX, and Solaris. For more information, see the *Installation Guide* for your platform. Auto-registration is fully supported on 5.0 (and later) Agent Hosts. Auto-registration is not supported on machines with more than one network interface. If you have configured existing Agents Hosts to use auto-registration, see "Auto-Registration Support for Legacy Agent Hosts" on page 78.

To accept registration information from new Agent Hosts, the existing Agent Hosts must have the auto-registration and update program installed, and the RSA Authentication Manager must be set to allow auto-registration. Use the following appropriate set of instructions to advise Agent Host administrators about installing and using the auto-registration and update program.

- Agent Hosts that use the Automated Agent Host Registration feature must register to the Primary. Both the Agent Host record on the Primary and the **sdconf.rec** file on the Agent Host must have the Primary designated as the Acting Master.

  In the Agent Host record on the Primary, assign the Primary as the Acting Master. Then, generate a new configuration file, and distribute it to the Agent Host.

- If you upgraded your Master to the Primary, existing Agent Hosts are already configured to register with the Primary. If you add the auto-registration feature to any other existing or new Agent Hosts, you must assign the Primary as the Acting Master for each Agent Host using auto-registration, generate a new **sdconf.rec** file, and distribute it to the Agent Host.

- If you did not upgrade your Master to the Primary, but instead, used a new machine as the Primary, you must assign the Primary as the Acting Master for each Agent Host using auto-registration, generate a new **sdconf.rec** file, and distribute it to the Agent Host.

- If you are merging multiple realms, you must assign the Primary as the Acting Master for any Agent Host from the merged realm that uses auto-registration, generate a new **sdconf.rec** file, and distribute it to the Agent Host.

For information on assigning Acting Authentication Managers and generating **sdconf.rec** files, see the Help topic "Assign Acting Authentication Managers."

Instructions for Microsoft Windows Agent Host administrators:

1. Copy the Primary's **sdconf.rec** and **server.cer** files to a temporary directory on a target Agent Host.

2. Copy **sdadmreg_install.exe** from the RSA Authentication Manager 6.1 CD (located in the **acesupp\sdadmreg\windows** directory) to the temporary directory that contains the **sdconf.rec** and **server.cer** files.

3. In Windows Explorer on the target Windows Agent Host, double-click **sdadmreg_install.exe** and follow the instructions on the screen.

   The **sdadmreg_install** utility installs **sdconf.rec**, **server.cer**, and **sdadmreg.exe** in the Agent Host's ***%SYSTEMROOT%*\system32** directory (for example, **winnt\system32**).

4. Start the database brokers on the Primary before you run **sdadmreg**.

   If you are using Windows, starting any RSA Authentication Manager program (for example, the Database Administration application) starts the database brokers automatically.

   If you are using UNIX, start the database brokers by issuing the ***ACEPROG*/sdconnect start** command on the Authentication Manager.

5. The auto-registration program runs whenever the Agent Host is restarted. To run the program at any time, double-click **sdadmreg.exe**.

   Note: If you run **sdadmreg** using a command-prompt, it will not print the results. Instead, you must view related messages in the Event Log. To open the Event Log, click **Start** > **Programs** > **Administrative Tools** > **Event Viewer**.

   You may want to run the program at the following times:

   - Before or immediately after installing RSA Authentication Agent software on a new Windows Agent Host. An Agent Host record is added to the Authentication Manager database if none exists already and if the Authentication Manager is set to allow auto-registration.
   - When the Agent Host has a new IP address. The new Agent Host IP address is written to the Authentication Manager database Agent Host record, provided that a node secret for this Agent Host has already been created.
   - When you want to have the Agent Host's **sdconf.rec** updated by the current **sdconf.rec** on the Authentication Manager. The updated **sdconf.rec** does not take effect until the Agent Host is restarted.

Instructions for UNIX Agent Host administrators:

1. Copy the Primary's **sdconf.rec** and **server.cer** files to a temporary directory on a target Agent Host.
2. Copy **sdadmreg_install** and **sdadmreg** from the RSA Authentication Manager 6.1 CD (located in the **acesupp\sdadmreg\*platform*** directory) to the temporary directory that contains the **sdconf.rec** and **server.cer** files.
3. Change to the temporary directory you used in steps 1 and 2.
4. Run the installation script by typing:

   ```
   sdadmreg_install
   ```

   at the UNIX command line prompt. Follow the instructions on the screen.

   The **sdadmreg_install** utility installs **sdconf.rec** and **server.cer** in the Agent Host's ***ACEDATA*** directory, and installs the **sdadmreg** program in the Agent Host's ***ACEPROG*** directory.
5. Start the database brokers on the Primary before you run **sdadmreg**.

   If you are using Windows, starting any RSA Authentication Manager program (for example, the Database Administration application) starts the database brokers automatically.

   If you are using UNIX, start the database brokers by issuing the ***ACEPROG/*sdconnect start** command on the Authentication Manager.
6. Run the auto-registration and update program on the Agent Host by typing:

   ```
   ACEPROG/sdadmreg
   ```

   at the UNIX command line prompt.

You may want to run the program at the following times:

- Before or immediately after installing RSA Authentication Agent software on a new UNIX Agent Host. An Agent Host record is added to the Authentication Manager database if none exists for it already and if the Authentication Manager is set to allow auto-registration.
- When the Agent Host has a new IP address. The new Agent Host IP address is written to the Authentication Manager database Agent Host record, provided that a node secret for this Agent Host has already been created.
- When you want to have the Agent Host's **sdconf.rec** updated by the current **sdconf.rec** on the Authentication Manager. The updated **sdconf.rec** does not take effect until the Agent Host is restarted. You may want to run **sdadmreg** for this purpose on a regular basis (for example, whenever the Agent Host is restarted).

Dynamic Host Configuration Protocol (DHCP) Support

Note: Agent Hosts that use RSA Authentication Manager DHCP support must have the **sdadmreg** program in their startup files.

The **sdadmreg** program automatically checks and updates the IP address field of an Agent Host's record in the Authentication Manager database to reflect address changes made by the Dynamic Host Configuration Protocol.

Note: The name of the Agent Host must remain the same. If both the name and the IP address change, the Authentication Manager will create a new entry.

For security reasons, a new RSA Authentication Manager Agent Host must have an uncontested IP address until after the first successful authentication from the Agent Host. You can ensure that an IP address is uncontested by temporarily assigning the new Agent Host an IP address that is not controlled by DHCP. After the first successful authentication, DHCP can take over assigning an IP address to the Agent Host when the Agent Host is restarted, as illustrated in the following example:

- Agent Host *hopper* is running RSA Authentication Agent software and registered in the RSA Authentication Manager database with IP address 192.168.10.23.
- Agent Host *hopper* is shut down, releasing IP address 192.168.10.23.
- Agent Host *eakins* joins the network and is assigned IP address 192.168.10.23 (*hopper*'s old address) by the DHCP server. The IP address entry in *hopper*'s Agent Host record becomes "DHCP_UNASSIGNED *Agent Host number*."
- Agent Host *hopper* is restarted and requests to rejoin the network.
- The DHCP server assigns *hopper* IP address 192.168.10.26.
- The **sdadmreg** program is executed automatically and writes the IP address change to *hopper*'s database record.

Load Balancing by Agent Hosts

RSA ACE/Agent software versions 5.1 and 5.2 can balance authentication request loads automatically. It does this by sending a time request to each Authentication Manager in the realm and determining a priority list based on the response time of each Authentication Manager. The Authentication Manager with the fastest response is given the highest priority and receives the greatest number of requests from that Agent Host, while other Authentication Managers get lower priorities and fewer requests. This is in effect until the Agent software sends another time request. If the Authentication Managers respond to the next time request in a different order, the Agent Host changes its priorities accordingly.

In addition, the Agent Host can connect to its Authentication Managers through firewalls if the alternate IP addresses (aliases) for those Authentication Managers are either specified in the Agent Host's configuration record file (**sdconf.rec**), or are provided by a 6.1 Authentication Manager upon request by the Agent Host. The RSA Authentication Agent software automatically checks the alias IP address information before using those aliases to send its authentication requests to the Authentication Managers.

As an alternative to this automatic load-balancing process, Agent administrators have the option of balancing the load manually by specifying exactly which Authentication Managers each Agent Host should use to process requests. The specification also assigns a priority to each Authentication Manager so that the Agent Host directs authentication requests to some Authentication Managers more frequently than to others. To use this option, the Agent administrator specifies priority settings in a flat text file named **sdopts.rec**, which resides on the Agent Host.

You can also indicate additional firewall IP addresses to be used to contact Authentication Managers. Finally, you can specify an overriding IP address for the Agent Host if that host is a multi-homed server. These depend on settings that you specify in an optional, flat text file named **sdopts.rec**.

As an RSA Authentication Manager administrator you are not directly responsible for load balancing by Agent Hosts. However, you should be aware of how the Agent administrators in your realm are managing this activity.

Knowing what Authentication Manager priorities the Agent administrators have set is especially important if they use **sdopts.rec** files. Because the priorities set in these files are not adjusted automatically, it is possible that too many Agent Hosts direct their requests to the same Authentication Manager, with adverse effects on performance, or that an effective set of priorities becomes ineffective as circumstances change. RSA Authentication Manager administrators should keep Agent administrators informed and work with them to ensure that the system runs as smoothly and efficiently as possible.

The following section, "Manual Load Balancing Through the sdopts.rec File," is addressed to Agent administrators. It provides instructions for using an **sdopts.rec** file to balance loads manually.

Manual Load Balancing Through the sdopts.rec File

To specify manual load balancing, you can create an **sdopts.rec** file. You can use any text editor to create and edit an **sdopts.rec** file.

After you set up the **sdopts.rec** file, save the file into the correct directory for your Agent Host platform. On Windows, store the file in ***%SYSTEMROOT%*\System32**. On UNIX, store the file in the **\var\ace** directory (or in the directory being pointed to by the **$VAR_ACE** system variable).

To protect the file from unintended changes, change the permission settings on your **sdopts.rec** file so that only administrators can modify it.

Important: Each time that you modify the **sdopts.rec** file, you must restart the Agent to register your changes.

The file can include the following types of lines:

- Comments, each line of which must be preceded by a semicolon
- Keyword-value pairs, which can be any of the following:

  CLIENT_IP=<*ip_address*>. This specifies an overriding IP address for the Agent Host. The **Client_IP** keyword can appear only once in the file. For information about overriding IP addresses, see "Setting an Overriding IP Address for an Agent Host" on page 74.

  USESERVER=<*ip_address*>, <*priority*>. This specifies an Authentication Manager that can or will receive authentication requests from the Agent Host according to the priority value specified. Use one setting for each Authentication Manager that the Agent Host is to use. Each **Useserver** keyword value must consist of the actual Authentication Manager IP address, separated by a comma from the assigned Authentication Manager *priority.* The priority specifies whether or how often an Authentication Manager will receive authentication requests.

  Important: The maximum number of Authentication Managers you can specify in the **sdopts.rec** and **sdconf.rec** files *combined* is 11.

  The priority value must be one of those listed in the following table.

Priority	Meaning
2-10	Send authentication requests to this Authentication Manager using a randomized selection weighted according to the assigned priority of the Authentication Manager. The range is from 2–10: the higher the value, the more requests the Authentication Manager receives. A Priority 10 receives about 24 times as many requests as a Priority 2.
1	Use this Authentication Manager as a last resort. A Priority 1 is used only if no Authentication Managers of higher priority are available.

Priority	Meaning
0	Ignore this Authentication Manager. A Priority 0 can be used only in special circumstances. First, it must be one of the four Authentication Managers listed in the **sdconf.rec** file. If so, the Priority 0 can be used only for the initial authentication of the Agent unless all Authentication Managers with priorities of 1-10 listed in the **sdopts.rec** file are known by the Agent Host to be unusable. Generally, a priority value of 0 allows you to put an entry in the file for a Authentication Manager without using that Authentication Manager. You can change the Authentication Manager's priority value if you later decide to use it.

Each Authentication Manager you add to the **sdopts.rec** file with the **USESERVER** keyword must be assigned a priority. Otherwise, the entry is considered invalid. The IP addresses in the file are verified against the list of valid Authentication Managers that the Agent receives as part of its initial authentication with a 6.1 Authentication Manager.

ALIAS=*ip_address*, *alias_ip_address_1*[, *alias_ip_address_2*, *alias_ip_address_3]*. This specifies one or more alternate IP addresses (*aliases*) for an Authentication Manager. Aliases for an Authentication Manager can be specified in the Agent **sdconf.rec** file. Use the **ALIAS** keyword to specify the IP addresses of up to three additional firewalls through which the specified Authentication Manager can be contacted by the Agent.

The value for the **ALIAS** keyword must consist of the Authentication Manager's actual IP address, followed by up to three alias IP addresses for that Authentication Manager. The Agent sends its timed requests to both the actual and the alias IP addresses.

Only the actual IP address specified by the **ALIAS** keyword must be known to the Authentication Manager that is being specified. In addition, the actual IP address must be included on any Authentication Manager *list* received by the Agent. The Authentication Manager list provides actual and alias IP address information about all known Authentication Managers in the realm, and the Agent receives the Authentication Manager list from a 6.1 Authentication Manager, after the Authentication Manager validates an authentication request.

ALIASES_ONLY[=*ip_address*]. If you use this keyword, make certain that at least one Authentication Manager has an alias IP address specified for it either in **sdconf.rec** or in **sdopts.rec**.

When used without a value, the **ALIASES_ONLY** keyword specifies that the Agent should send its requests only to Authentication Managers that have alias IP addresses assigned to them. Exceptions can be made by including in the **sdopts.rec** file no more than 10 **IGNORE_ALIASES** keywords to specify which Authentication Managers must be contacted through their actual IP addresses. For an example showing these exceptions, see "Examples Featuring the ALIAS, ALIASES_ONLY, and IGNORE_ALIASES Keywords" on page 73.

When you provide an Authentication Manager's actual IP address as the value of **ALIASES_ONLY**, the keyword specifies that only the alias IP addresses of the Authentication Manager must be used to contact that Authentication Manager.

IGNORE_ALIASES[=*ip_address*]. When used without a value, the **IGNORE_ALIASES** keyword specifies that all alias IP addresses found in the **sdopts.rec** file, the **sdconf.rec** file, or on the Authentication Manager list provided by 6.1 Authentication Managers are ignored. Exceptions can be made by including no more than 10 **ALIASES_ONLY** keywords in the **sdopts.rec** file to specify which Authentication Managers must be contacted through their alias IP addresses. For an example showing these exceptions, see "Examples Featuring the ALIAS, ALIASES_ONLY, and IGNORE_ALIASES Keywords" on page 73.

When you provide an Authentication Manager's actual IP address as the value of **IGNORE_ALIASES**, the keyword specifies that only the actual IP address of the Authentication Manager must be used to contact that Authentication Manager.

An Example Featuring the USESERVER Keyword

You can put the settings in the file in any order, but each setting must be listed separately in the file, one setting per line. Here is an example featuring only **USESERVER** keywords:

```
;Any line of text preceded by a semicolon is ignored
;(is considered a comment).
;Do not put a blank space between a keyword and its
;equal sign. Blank spaces are permitted after the
;equal sign, after the IP address, and after the
;comma that separates an IP address from a priority
;value.
USESERVER=192.168.10.23, 10
USESERVER=192.168.10.22, 2
USESERVER=192.168.10.20, 1
USESERVER=192.168.10.21, 0
```

The Authentication Manager identified by the actual IP address 192.168.10.23 receives many more authentication requests than Authentication Manager 192.168.10.22. Authentication Manager 192.168.10.20 is used only if the Authentication Managers of higher priority are unavailable, and Authentication Manager 192.168.10.21 is ignored except in rare circumstances (as explained in the definition of Priority 0 in the **USESERVER** keyword's description).

Note: You can use the **USESERVER** and **ALIAS** keywords together in the **sdopts.rec** file, just as you can include whichever keywords defined for use in the file as you want. However, **USESERVER** keywords do not affect the alias addresses used to connect to Authentication Managers, and **ALIAS** keywords have no effect on which Authentication Managers are specified for use.

Examples Featuring the ALIAS, ALIASES_ONLY, and IGNORE_ALIASES Keywords

You can put the settings in the file in any order, but each setting must be listed separately in the file, one setting per line. Here is an example featuring keywords related to Authentication Manager alias addresses:

```
;Any line of text preceded by a semicolon is ignored
;(is considered a comment).
;Do not put a blank space between a keyword and its
;equal sign. Blank spaces are permitted after the
;equal sign, after the IP address, and after the
;comma that separates an IP address from other IP
;addresses.
USESERVER=192.168.10.23, 10
USESERVER=192.168.10.22, 2
USESERVER=192.168.10.20, 1
USESERVER=192.168.10.21, 0
ALIAS=192.168.10.23, 192.168.4.1, 192.168.4.2, 192.168.4.3
ALIAS=192.168.10.22, 192.168.5.2, 192.168.5.3
ALIAS=192.168.10.20, 192.168.5.2
ALIAS=192.168.10.21, 192.168.1.1
ALIASES_ONLY=192.168.10.23
IGNORE_ALIASES=192.168.10.22
```

In this example, the default is to use alias or actual IP addresses, with a couple of exceptions. The Authentication Manager with the actual IP address 192.168.10.23 has three alias addresses specified for it, while Authentication Managers 192.168.10.20 and 192.168.10.21 have only one alias apiece, and Authentication Manager 192.168.10.22 has two alias addresses specified for it. The aliases specified by the **ALIAS** keywords are provided in addition to any aliases specified in **sdconf.rec** or on the Authentication Manager list.

Note: You can use the **USESERVER** and **ALIAS** keywords together in the **sdopts.rec** file, just as you can include whichever keywords defined for use in the file as you like. However, **USESERVER** keywords do not affect the alias addresses used to connect to Authentication Managers, and **ALIAS** keywords have no effect on which Authentication Managers are specified for use.

The exceptions are that Authentication Manager 192.168.10.23, as specified by the **ALIASES_ONLY** keyword, is contacted by the Agent through use of the Authentication Manager's alias IP addresses. Authentication Manager 192.168.10.22, specified by the **IGNORE_ALIASES** keyword, are only contacted by the Agent through use of the Authentication Manager's actual IP address.

Here is an example where the default is to ignore aliases, with two exceptions:

```
IGNORE_ALIASES
ALIASES_ONLY=192.168.10.23
ALIASES_ONLY=192.168.10.22
```

The **ALIASES_ONLY** exceptions specify that the Agent must send its requests to Authentication Manager 192.168.10.23 and Authentication Manager 192.168.10.22 only by using their alias IP addresses.

Here is an example where the default is to use aliases, with two exceptions:

```
ALIASES_ONLY
IGNORE_ALIASES=192.168.10.23
IGNORE_ALIASES=192.168.10.22
```

The **IGNORE_ALIASES** exceptions specify that the Agent must send its requests to Authentication Manager 192.168.10.23 and Authentication Manager 192.168.10.22 only by using their actual IP addresses.

Setting an Overriding IP Address for an Agent Host

When an RSA Authentication Agent runs on an Agent Host that has multiple network interface cards and therefore multiple IP addresses, the Agent administrator must specify a primary Agent Host IP address for encrypted communications between the Agent Host and the RSA Authentication Manager.

Agent Hosts typically attempt to discover their own IP addresses. An Agent Host with multiple addresses might select one that is unknown to the Authentication Manager, making communication between Agent and Authentication Manager impossible. The Agent administrator can use the **Client_IP=** keyword in an **sdopts.rec** file to ensure that the primary IP address specified as the keyword value is always used to communicate with the Authentication Manager.

Each Agent Host's primary IP address must be identified in its Agent Host record in the Authentication Manager database. The Agent Host's other IP addresses can also be listed there (as "secondary nodes") for failover purposes.

If your RSA Authentication Manager system uses auto-registration of Agent Hosts (for more information, see "Automated Agent Host Registration and Updating" on page 65), each Agent Host's primary IP address is entered in that Agent Host's record automatically and updated whenever it changes.

If Agent Hosts are registered manually, however, it is your responsibility as the Authentication Manager administrator to ensure that the Agent's primary IP address in the Agent Host record in the Authentication Manager database is identical to the primary IP address specified in the Agent Host's configuration records or in an **sdopts.rec** file. If these two settings do not match, communication between Agent Host and Authentication Manager will fail. If secondary IP addresses are also specified for the Agent Host, these too must be entered in the record, and all addresses must be updated if they change.

The instructions in the following section, "Using the Client_IP Keyword," are for RSA Authentication Agent administrators. They explain how to use the **Client_IP** keyword in an **sdopts.rec** file to identify an Agent Host's primary IP address, ensuring that this address is always used when the Agent Host communicates with the Authentication Manager.

Some RSA Authentication Agents for Microsoft Windows machines give administrators the option of specifying the overriding IP address for the Agent Host in the RSA Authentication Agent Control Panel. To use the Control Panel to specify the Agent Host's primary IP address, see the *RSA Authentication Agent 6.1 for Microsoft Windows Installation and Administration Guide*.

Using the Client_IP Keyword

You can either add the **Client_IP** keyword to an existing **sdopts.rec** file on the Agent Host or create an **sdopts.rec** file if none exists. For more information, see "Manual Load Balancing Through the sdopts.rec File" on page 70.

Note: The Dynamic Host Configuration Protocol allocates IP addresses to Agent Hosts dynamically. (For more information, see "Dynamic Host Configuration Protocol (DHCP) Support" on page 68.) To avoid address conflicts, DHCP must not be enabled for Agent Hosts with multiple IP addresses. Conversely, there is no reason to use the **Client_IP** keyword for Agent Hosts that have single IP addresses, because these Agent Hosts have no alternative addresses to override.

To specify an IP address override in the **sdopts.rec** file, use the **Client_IP** keyword, as in this example:

```
CLIENT_IP=192.168.10.19
```

This statement in the file ensures that the Agent Host always uses the specified IP address to communicate with the RSA Authentication Manager.

In the absence of Agent Host auto-registration, you, as the RSA Authentication Agent administrator, must ensure that the Authentication Manager administrator knows the Agent Host's primary and secondary IP addresses when the Agent Host is first configured on the RSA Authentication Manager system. If any Agent Host address changes at any time, inform the Authentication Manager administrator in time to update the Agent Host record in the Authentication Manager database.

Legacy Agent Hosts

RSA Authentication Manager 6.1 continues to support legacy Agent Hosts (those running versions of RSA ACE/Agent software prior to 5.0). This section discusses issues relating to legacy Agent Hosts.

Authentication Manager Designations Required By Legacy Agent Software

RSA Authentication Manager 6.1 is based on architecture introduced in version 5.0. Two changes in RSA ACE/Server 5.0 architecture improved authentication rates over previous major versions: the use of multiple authenticating Replicas and the ability of the new RSA Authentication Agent software to select the Replica that will respond most quickly to an authentication request. Agent software based on 5.0 architecture is aware of all the Replicas in your realm and can send authentication requests to any one of them.

Lacking the load balancing capability, legacy Agent Hosts can request authentication of users only from a Master or a Slave, because the Agent Host's configuration file (**sdconf.rec**) can identify only these two Authentication Managers.

If your installation includes legacy Agent Hosts, the RSA Authentication Manager 6.1 installation software saves the identities of the original Master and Slaves when it modifies the Authentication Manager configuration file, **sdconf.rec**. This information, which is in the configuration file of each legacy Agent Host, has the effect of assigning the original Master and Slaves (now configured as Replicas in the 6.1 environment), as the Acting Master and Slaves for legacy Agent Hosts in the new environment.

Note: If, after installation, you add a legacy Agent Host—that is, an Agent Host running RSA ACE/Agent software earlier than 5.0—you must enter the name of the Acting Master and Acting Slaves in the Agent Host configuration record manually. This is true even if the record was created through the auto-registration process. For information about modifying the Agent Host record, see "Legacy Agent Hosts" on page 75.

Merging Realms That Include Legacy Agent Hosts

After installing RSA Authentication Manager 6.1, you can merge your database with that of another realm that also includes legacy Agent Hosts. If you do this, you must ensure that these "imported" legacy Agent Hosts will continue sending authentication requests to their own original Master and Slaves.

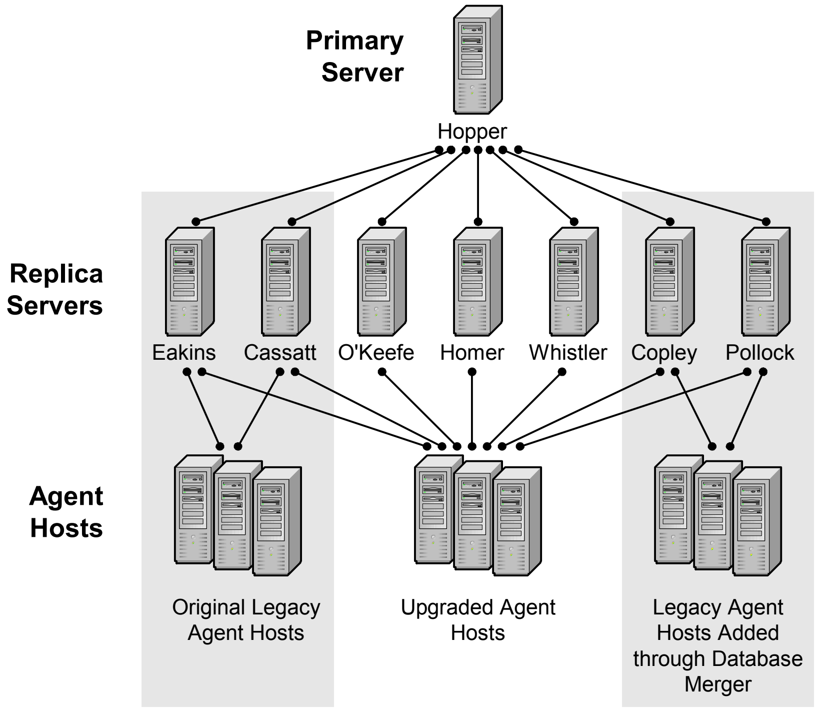
Before you begin the merge procedure, edit **sdconf.rec** on the Primary so that it specifies the Master and Slaves of the realm you are importing rather than the former Master and Slaves of your own realm.

This change does not affect the behavior of the legacy Agent Hosts already in your realm, which continue to direct authentication requests to the Acting Master and Slaves specified in their own configuration files. In the database merge procedure, however, the new Acting Master and Slaves are copied from **sdconf.rec** on the Primary to the Agent Host record of each new legacy Agent Host. If the specifications in that file have not been changed, authentication requests from all legacy Agent Hosts, including those just added to the realm, will be addressed to the same pair of Authentication Managers.

To Begin: See the database merge procedure described in the *Installation Guide* for your platform.

The following diagram illustrates the scenario described in this section.

Servers and Agent Host Connections in an Upgraded RSA ACE/Server 5.2 Realm



In the shaded area on the left are Agent Hosts that were part of the sample realm when it was upgraded to RSA Authentication Manager 6.1. Because Authentication Managers "Eakins" and "Cassatt" were the Master and Slaves prior to the upgrade, they are identified in each legacy Agent Host record as Acting Master and Slaves for this set of legacy Agent Hosts. The configuration file of each Agent Host, which is not changed in the RSA Authentication Manager upgrade process, specifies Eakins and Cassatt as the Master and Slave respectively, and the Agent Host must therefore address all authentication requests to these two Authentication Managers only.

In the center area are Agent Hosts that have been upgraded to RSA ACE/Agent 5.0 or later. These Agent Hosts can send authentication requests to any Replica in the realm.

The shaded area on the right identifies a set of legacy Agent Hosts that were added to the realm by merging its database with that of another realm. The former Master and Slaves in that realm, "Copley" and "Pollock," are now the Acting Master and Slaves to which the newly added Agent Hosts must direct all their authentication requests. If the Agent Host records did not identify Copley and Pollock in these roles, the legacy Agent Hosts would be unable to function, since these are the Master and Slaves specified in their configuration files.

Note: The illustrated system requires an RSA Authentication Manager Advanced license. The RSA Authentication Manager Base license allows a Primary and one Replica only.

Auto-Registration Support for Legacy Agent Hosts

Auto-registration is not fully supported on legacy Agent Hosts. The legacy Agent Host **sdconf.rec** file must contain a Master and Slave that matches the Acting Master and Slave assigned in the Agent Host record in the database. If the Agent Host **sdconf.rec** file and the database do not match, users cannot authenticate through the legacy Agent Host.

This is a problem for auto-registration, because it uses the Authentication Manager **sdconf.rec** file, which may or may not agree with the Master and Slave information in the Agent Host **sdconf.rec** file and the Acting Master and Slave information in the database. If a legacy Agent Host updates its own **sdconf.rec** file through auto-registration, it may be retrieving an **sdconf.rec** file that contains Acting Master and Slaves that are different than those assigned in the database. When the legacy Agent Host attempts to authenticate to the Acting Master and Slave in its updated **sdconf.rec** file, the authentication fails.

For this reason, if you have any legacy Agent Hosts using auto-registration, they must all use the same Acting Master and Slave. Additionally, the Authentication Manager **sdconf.rec** file must contain the same Acting Master and Slave as the Agent Host **sdconf.rec** file.

If at some time after installation you add another Agent Host running the same pre-5.0 version of the Agent software, you must enter the name and IP address of the Acting Master (and, optionally, the Acting Slave as well) in the Agent Host record before the Agent Host can handle authentications successfully. This is true whether the Agent Host record in the Authentication Manager database is created automatically through auto-registration or manually by an administrator. Until you edit the Agent Host record and supply the identity of the Acting Master, the Agent has no destination to direct authentication requests to.

To Begin: Click **Agent Hosts** > **Edit Agent Host**. Select the Agent Host whose record you want to edit and click **OK** to open the Edit Agent Host dialog box. Click **Assign Acting Servers** and, if you need instructions, click **Help**.

The Configuration Record Editor

With the Configuration Record Editor you can edit the Acting Master and Acting Slave fields of any Authentication Manager configuration file. For reasons why you might want to do this, see "Authentication Manager Designations Required By Legacy Agent Software" on page 75.

There are two versions of the Configuration Record Editor located in the ***ACEPROG*** directory: a GUI version for Windows (**sdcfgedit_ui.exe**) and a command line version for UNIX (**sdcfgedit**). You can use the command line version on Windows platforms as well.

Editing Master and Slave Data (GUI Version)

To edit the Acting Master and Acting Slave in an existing configuration file:

1. On the Authentication Manager, change to the ***ACEPROG*** directory, and double-click **sdcfgedit_ui.exe**.
2. Click **Select Configuration File**.
3. In the Open dialog box, select the configuration file you want to edit, and click **Open**.
4. Type the name and IP address for each Acting Authentication Manager in the **Name** and **IP Address** boxes.

   If you are using DNS, and the **Resolve host name and addresses** is selected, the IP address of the Authentication Manager automatically populates when you tab out of the **Name** box.
5. Click **OK** to save the configuration file.

Editing Master and Slave Data (Command-Line Version)

The command line version of the Configuration Record Editor requires specifying the location of the **sdconf.rec** file, and the name or IP address of the new Acting Master and Acting Slaves.

To edit the Acting Master and Acting Slave in an existing configuration file on UNIX:

Change to the ***ACEPROG*** directory and type:

```
sdcfgedit -ffilename -mname,IPAddress
-sname,IPaddress
```

This command includes the following option switches:

- **-f*filename*** specifies the full path and filename of the configuration file
- **-m*name*, *IP address*** specifies the name and IP address of the Acting Master
- **-s*name*, *IP address*** specifies the name and IP address of the Acting Slave

Note: To clear the Acting Master or Slave from the configuration file, use a dash in place of the name. For example, to clear the specified Slave, use **-s-**.

The names of the Authentication Managers are resolved to their fully-qualified names, unless you use the optional **-p** switch, which preserves the names exactly as you type them. (The **-p** switch must be entered immediately before the **-m** switch in the command line.) If you do not specify IP addresses for the Authentication Managers, the addresses are resolved using the method that is standard for the system.

4 Realm Administration

This chapter explains how to plan for, create, and modify realms in your RSA Authentication Manager installation.

The term "realm" refers to the Primary Authentication Manager and its Replica Authentication Managers, databases, users, tokens, and Agent Hosts. Realms support the exchange of messages for cross-realm authentication. This chapter refers to implementations with multiple realms and applies to customers with RSA Authentication Manager Advanced licenses only. For more information, see Appendix A, "Licensing."

Before your realm can participate in cross-realm authentication, you must create a list of participating realms on your Primary.

Cross-Realm Authentication

With minimal administration, users visiting from other realms can access your Agent Hosts after being authenticated by RSA SecurID. To enable cross-realm authentication, see the following section,"Creating Records for Visiting Users Automatically," or "Creating Remote User Records Manually" on page 82.

Creating Records for Visiting Users Automatically

Visiting users are authenticated and given access to an Agent Host if these conditions are true:

- The Agent Host is open to all known users.
- The Agent is configured to search other realms for unknown users who attempt to authenticate on the Agent Host.

With these Agent Host settings, an authentication attempt by a user whose login is not found in the local RSA Authentication Manager database causes an inquiry to be broadcast to all realms registered in the database. When the user's home realm is identified and the authentication information entered by the user is successfully validated, the Authentication Manager creates and stores a remote user record for the visiting user. Subsequent authentication attempts by this user are validated against the user's home realm directly, without an inquiry to all registered realms. For more information, see "Default Logins in Cross-Realm Authentication" on page 82.

Creating Remote User Records Manually

Remote user records can be created through an automatic process or you can create them manually. You can use remote user records to activate visiting users on any restricted Agent Host within your realm just as if they were local users. Explicit activation of this kind is unnecessary for open Agent Hosts in your realm, where the user identified in the record can be authenticated without the need for a broadcast to all registered realms.

To activate a remote user on a restricted Agent Host in your realm, create a user record in your Authentication Manager database for the remote user, then activate that user on the restricted Agent Host.

Your RSA Authentication Manager system uses remote aliases to prevent login conflicts. For details, see the following section, "Default Logins in Cross-Realm Authentication."

Default Logins in Cross-Realm Authentication

Within a realm, every user must have a unique default login, but users in different realms within a cross-realm may have the same default login. Having two or more users in different realms with the same default login can cause problems in the following circumstances:

- Users need to authenticate in realms other than their own and use resources that are protected by an RSA Authentication Manager.
- You merge two or more existing realms into one realm.

  With the database dump and load utilities (described in the *Installation Guide* for your platform) you can load the databases from different realms into a version 6.1 database, merging all data. Duplicate default logins generate errors during the merge operation.

When a user attempts to gain access to a protected resource in a remote realm, the Authentication Manager in that realm looks for a matching login name in its own database first. If the Authentication Manager finds a matching login name whose passcodes do not match those submitted by the user, it denies access to the remote user without informing other realms of the authentication attempts. If the visiting user continues trying to gain access, the local user's tokens are eventually disabled.

In this situation, the visiting user needs a different default login in the remote realm, but the Authentication Manager in the user's home realm—where authentication actually takes place—expects the default login that it knows. To resolve this conflict, an administrator in the remote realm must create a remote user record for the visiting user that substitutes a remote default login name for the user's home default login name. The two names must be different, and each must be unique within the realm where it is used. The remote default login name is said to be aliased to the home default login name.

For example, **Joshua Abrams** from realm *okeefe* visits realm *cassatt*. His default login in *okeefe* is **jba**. In *cassatt*, **Jane Anderson** already uses **jba**. An administrator in *cassatt* adds **Joshua Abrams** as a remote user with **jba1** as the default login he uses in the remote realm and enters **jba** as his remote alias. When the Authentication Manager in *cassatt* sends **Joshua Abrams's** authentication attempts to *okeefe*, it ignores the default login in the remote user record and sends his remote alias (**jba**), which is what the Authentication Manager in *okeefe* expects.

Note: There must be an entry in the **Remote Alias** field. The entry may be the same as the entry in the **Default Login** field.

Some Realms Not Upgraded to RSA ACE/Server 5.0.1 or Later

Until all realms in your cross-realm are upgraded to RSA ACE/Server 5.0.1 or later, additional administrative tasks may be required for cross-realm authentication support. Contact RSA Security Customer Support for more information.

Planning for Cross-Realm Authentication

When planning for cross-realm authentication, consider the following points:

- Cross-realm authentication requires an RSA Authentication Manager Advanced license, which supports up to six realms.
- Cross-realm authentication requires close coordination among realm administrators. For example, realm administrators must share their token serial numbers and tokencodes in order to establish trust between realms. Realm administrators need procedures so that they can work together on cross-realm-level issues.
- Login names must be unique across realms, or visiting users must have their remote logins aliased to their logins in their home realms.
- If an RSA Authentication Manager machine address changes, the security administrator must notify every realm. Administrators in the remote realms must then update the address using the Edit Realm dialog box. Any changes to the network configuration may temporarily increase your administrative overhead.
- Every realm must be configured to use the same UDP port for authentication requests.
- The Agent time-out interval is the same for a remote authentication request as for a local request—the default is five seconds. When the network is slow, the Agent Host can time out before the Authentication Manager gets a positive response. You may need to increase the Agent time-out setting in this case.
- You must either enable External Authorization or disable External Authorization in all participating realms. If External Authorization is enabled in some realms and disabled in others, cross-realm authentication fails. For information about External Authorization, see "Customizing Your Authorization Procedures" on page 216.

Note: For an overview of cross-realm authentication, see "Cross-Realm Model" on page 26.

Cross-realm authentication requires dynamically allocated UDP ports. The UDP ports are used for communication between the remote realm and the user's home realm, and for certain types of internal communication on the RSA Authentication Manager. There must be one available UDP port for each process (**acesrvc_be.exe** on the Windows platform or **_aceserver_be** on UNIX platforms) running on the RSA Authentication Manager.

If there is a firewall between the realms, you must leave open a range of at least 11 UDP ports from which the required port can be allocated during cross-realm authentication. You must configure the Authentication Manager to use the same range of port numbers by setting the maximum and minimum port number in the Windows registry (on an RSA Authentication Manager for Windows) or as environment variables (on an RSA Authentication Manager for UNIX). The maximum port number must be ten greater than the minimum port number. By default, the minimum port number is set to 0, which means that the first available port will be used for communication, and the maximum port number is set to 65,535. If there is no firewall between the realms, you do not need to restrict the range of port numbers that the RSA Authentication Manager uses for communication between realms.

Important: Make sure that the required range of port numbers is available at all times. If the RSA Authentication Manager cannot bind a port, a fatal exit will occur. Configure the correct range of port numbers, and restart the Authentication Manager.

To limit the range of port numbers on RSA Authentication Manager for Windows:

1. On the Primary, click **Start** > **Programs** > **RSA Security** > **RSA Authentication Manager Control Panel**.
2. From the **Start & Stop RSA Authentication Manager Services** panel, click **Stop Auth Service Only**.
3. From the **Configure Authentication Processes**, specify the desired port range, and click **OK**.
4. From the **Start & Stop RSA Authentication Manager Services** panel, click **Start All**.

To limit the range of port numbers on RSA Authentication Manager for UNIX:

1. Make sure that no Authentication Manager processes are running.
2. Set the **MINIMUM_BE_PORT** environment variable to the minimum open UDP port that you want to use.
3. Set the **MAXIMUM_BE_PORT** to the maximum open UDP port that you want to use.

You could also include lines in the Authentication Manager startup script (**/ace/prog/aceserver**) that set the environment variables. Include the lines in the section of the startup script that sets the values for VAR_ACE, USR_ACE, and DLC. For example, if you wanted the minimum port to be 10,000 and the maximum port to be 10,011, include the following lines:

```
MINIMUM_BE_PORT=10000
export MINIMUM_BE_PORT
MAXIMUM_BE_PORT=10011
export MAXIMUM_BE_PORT
```

If you do not set the variables, the default values (1024-9999) are used.

Note: If you reinstall RSA Authentication Manager 6.1, the minimum and maximum ports will be set to the default values. Reset the minimum and maximum values to reflect the range of ports that you want to use.

Creating and Modifying Realms

If you want your realm to participate in authentication with a remote realm, the remote realm must be registered in your Authentication Manager database and your realm must be registered in the remote Authentication Manager database. To add and modify realms, you must be a realm administrator or have a custom role that includes realm administrator privileges.

In the following discussion, "local realm" refers to the RSA Authentication Manager installation you are administering, and "remote realm" refers to the realm you are adding to your database.

Adding realm records requires close cooperation with other realm administrators in your organization. You need the following information about a remote realm in order to register the realm in your Authentication Manager database:

- The name and IP address of the Primary.
- The names and IP addresses of the one or two remote Authentication Managers that authenticate remote users visiting your local realm. If there are two, you must also know which is the Preferred Authentication Manager and which is the Failover Authentication Manager, as specified by the remote realm administrator.

Note: The realm secret must initially be established using the Primary as the Preferred Authentication Manager. The Preferred and Failover Authentication Managers can be updated once the realm secret is established. In addition, if you update the Preferred and Failover Authentication Managers, you must also update that information in the other realm as well.

When a visitor to your realm attempts to log on to an Agent Host, the Agent Host sends the authentication request to an Authentication Manager in your realm, which forwards the request to the Preferred Authentication Manager in the remote realm. If the Preferred Authentication Manager does not respond, the local Authentication Manager then tries the Failover Authentication Manager. If the Failover Authentication Manager does not respond, the cross-realm authentication fails. One of the Authentication Managers *must* be running in order to successfully process cross-realm authentication requests.

- The authentication service port number (which must match your Authentication Manager's authentication port number).
- The remote realm administrator's token serial number.
- A series of tokencodes from the remote realm administrator's token.

In addition to this information about the remote realm, you must also be prepared to specify the names and IP addresses of one or two local Authentication Managers that authenticate local users who visit the remote realm. RSA Security recommends that you designate one as the Preferred Authentication Manager and one as the Failover Authentication Manager. Give this information to the remote realm administrator.

The function of these servers in the local realm matches that of the Preferred and Failover Authentication Managers in the remote realm. When one of your users attempts to log on an Agent Host in the remote realm, the authentication request is forwarded first to the Preferred Authentication Manager in your local realm, and then, if that Authentication Manager does not respond, to the Failover Authentication Manager. One of the two Authentication Managers must respond so that the cross-realm authentication can succeed.

To Begin: Click **Add Realm** on the Realm menu to add a realm. Click **Help** for instructions.

When you input the set of tokencodes from the remote realm administrator's token, the initial authentication transaction does two important things:

- Establishes the realm secret between the local realm (your Authentication Manager) and the remote realm. A realm secret is a random string known only to the local realm and the remote realm. The realm secret is part of a key used for encrypting packets sent between the two machines. The realm secret must be established before authentication requests can be exchanged between local and remote realms.
- Automatically adds your local realm record to the remote realm database. The administrator in the remote realm does not have to take any action to add your realm record to the remote realm database. If your local realm record already exists in the remote realm database, you will see the error message "Remote error inserting realm." You must delete your local realm record from the remote database before you can establish the realm secret.

5 Database Maintenance (Windows)

This chapter provides instructions to back up, restore, and create offline storage of RSA Authentication Manager data, and how to update information in your extension data records. It also describes how to run external procedures directly from the Database Administration application.

Maintaining Adequate Disk Space

If writing to an RSA Authentication Manager database fails because the file system is full, Authentication Manager programs will abort. Take whatever measures are necessary to avoid having inadequate disk space.

Important: Do not allow a Primary or Replica Authentication Manager's disk to become more than 90% full.

Because disk space requirements vary depending on your particular implementation of the system, use the examples of database sizes in the following table as guidelines only.

Number of Users	Number of Agent Hosts	Audit Trail Entries per Day	Authentication Manager Database Size	Estimated Daily Growth of Log Database	Estimated Event Log Growth
100	50	1000	1.8 MB	1 MB	.1 MB
1000	500	10000	2.2 MB	5 MB	.5 MB
10000	5000	25000	19.2 MB	11 MB	1.1 MB

Reclaiming Disk Space with Database Compression

Periodically, you must compress the Authentication Manager and the log databases, so that disk space is used more efficiently. For this purpose, RSA Authentication Manager includes a compression utility to reclaim disk space used by the RSA Authentication Manager databases. For example, after you have completed a large number of deletions, such as purging old log records, use the compression utility to free the disk space that the log database is no longer using.

Do not run the database brokers on the Primary during compression. Use the compression utility only at a time when you can shut down authentication services and all other RSA Authentication Manager programs on the Primary.

To compress the database files:

1. Log on as a Windows administrator.
2. Terminate all Authentication Manager programs and the database brokers, if they are running.
3. Click **Start** > **Programs** > **RSA Security** > **RSA Authentication Manager Database Tools** > **Compress**.

   The Database Compression dialog box opens. This dialog box displays the available disk space and the pathname to one of the databases.
4. Select the checkbox for one or both of the databases, **Compress Log Database** and **Compress Server Database**.

   The disk space required for the compression and the amount of available space are displayed. If the drive where your Primary is installed does not have enough space, postpone the compression until you can create more space on the drive. Alternatively, if the space you need is available on another drive or partition, in the **Path** box enter the location and name of a directory on this drive or partition.

   Important: The **Do not load delta records** checkbox is provided to address certain database problems caused by faulty records. Do not select this box unless you are advised to do so by RSA Security Customer Support.
5. Click **OK**.

   While the database is being compressed, the screen lists ongoing compression activities. The last two lines report the original size of the database and the compressed size.
6. To save the complete contents of this activity list to a file, click **Save As**. Otherwise, click **Close**.

Backing Up and Restoring RSA Authentication Manager Data

Follow the directions in this section to create reliable, complete backup files:

- ***ACEDATA:***
  - Back up the log and Authentication Manager databases daily. (You can set up RSA Authentication Manager to save the log database to an archive file according to a schedule and method you select. See "Scheduling Automated Log Database Maintenance" on page 157.)
  - Back up the **sdconf.rec** file any time you make changes to it.
  - Back up the **license.rec** file after initial installation of the product or after you upgrade the license record for any reason.
  - Back up SSL files for remote administration, RADIUS remote administration, and LDAP synchronization (**sdti.cer**, **server.cer**, **server.key**, **radius.key**, **radius.cer**, **key3.db**, and **cert7.db**).
  - Back up custom queries (**queries****).

- *ACEPROG*
  - Back up the configuration file **hosts.conf**.
  - Backup the configuration file **sdcommdConfig.txt**.

Note: RSA Security recommends that you back up the databases when ***no*** RSA Authentication Manager programs are running. If you ***must*** make a backup under these conditions, see "Backing Up Data While RSA Authentication Manager Programs Are Running" on page 90.

Backing Up Data While RSA Authentication Manager Programs Are Not Running

If you have multiple Replicas, you can stop all RSA Authentication Manager programs on an Authentication Manager to back up data with no loss of authentication service.

To back up the databases:

1. Log on as a Windows administrator.
2. Make sure that no RSA Authentication Manager programs are running on the Authentication Manager you are backing up.
3. If the database brokers are running, use the RSA Authentication Manager Control Panel application to stop them.
4. Locate the data files you want to back up.

   The database files are stored in the ***ACEDATA*** directory (for example, ...**\ace\data**).

   To back up the log database, copy all **sdlog** files:

   sdlog.b1
   sdlog.d1
   sdlog.db
   sdlog.lg
   sdlog.st
   sdlog.vrs

   To back up the Authentication Manager database, copy all **sdserv** files:

   sdserv.b1
   sdserv.d1
   sdserv.db
   sdserv.lg
   sdserv.st
   sdserv.vrs

Backing Up Data While RSA Authentication Manager Programs Are Running

This section describes the database backup command, which you can use to back up databases on both Primary and Replicas. However, more reliable backup methods are listed at the beginning of "Backing Up and Restoring RSA Authentication Manager Data" on page 88.

Note: You can perform a backup while RSA Authentication Manager programs are running without endangering the integrity of the database, but the backup may be incomplete. This is because *delta records* (for example, recent authentications) from the various Replicas in your realm may not have been propagated to the Primary database. Before you begin, make sure that no one else is backing up a database at the same time. Simultaneous multiple backups can slow system performance significantly.

Syntax

The **sdbkup** command has the following syntax:

```
sdbkup [noprompt|prompt] [online] databasefile backupfile
```

The following table describes the options of the **sdbkup** command:

Option	Description
noprompt	Overwrites any existing backup file in the location you specify with *backupfile*.
prompt	Prompts you when a backup file exists. You can choose to overwrite or not overwrite the backup file. This is the default behavior.
online	Specifies that you want to perform the backup while RSA Authentication Manager programs are running.
databasefile	Specifies the full pathname of the database file you want to back up (usually a file in the **ACEDATA** directory).
backupfile	Specifies the full pathname (or the name only) of the backup file.

For example, the command to back up the Authentication Manager database to a file named **sdserv1** is as follows:

```
sdbkup online \ace\data\sdserv sdserv1
```

If there is a file named **sdserv1** already, the following prompt appears:

```
*** <backup-file> already exists ***
Press "Enter" to continue; <backup-file> will be
overwritten.
-- or -- Press CTRL_C to abort.
Press any key to continue . . .
```

You can overwrite the **sdserv1** file without being prompted by issuing the following command:

```
sdbkup noprompt online \ace\data\sdserv sdserv1
```

Note: If your command line does not specify a target directory for the backup file, the file is created in the directory from which you issue the command. If this is inconvenient, create a backup directory in the ***ACEDATA*** directory (for example, **\ace\data\backups**). You can then specify this directory path in the **sdbkup** command line (or run the command from this directory).

Restoring Databases Created by the Database Backup Command

Use the procedure described in this section to restore the databases created by the database backup command. See the preceding section "Backing Up Data While RSA Authentication Manager Programs Are Running."

Note: The **sdrest** command restores *only* those databases created with the **sdbackup online** command.

If you have backed up your Primary when RSA Authentication Manager programs were not running, see the following section, "Recovering Data From an Offline Backup or a Server."

To restore a database using sdrest:

1. Log on as a Windows administrator.
2. From the RSA Authentication Manager Control Panel, stop all services.
3. To restore a database, use the command:

   ```
   sdrest ACEDATA\filename pathname\backup_filename
   ```

   For example, to restore the server database from a file named **sdserv1** in a directory named **backups** in the **ace\data** directory, the command would be:

   ```
   sdrest \ace\data\sdserv \ace\data\backups\sdserv1
   ```

   To restore the log database from a file named **sdlog1** in a directory named **backups** in the **ace\data** directory, the command would be:

   ```
   sdrest \ace\data\sdlog \ace\data\backups\sdlog1
   ```

4. Generate a Replica Package for all Replicas, and distribute the new database files in the Replica Package to all Replicas.

   If **Push DB Assisted Recovery** is allowed, the Primary will push the new database files to the Replicas when you restart the Primary. Otherwise, copy the database files to the Replicas manually, and use the RSA Authentication Manager Control Panel to apply the Replica Package.

5. Restart the Primary.

Recovering Data From an Offline Backup or a Server

When you want to recover data that was not backed up through the **sdbkup** command (see "Backing Up Data While RSA Authentication Manager Programs Are Running" on page 90), the appropriate procedure depends on the location of the most up-to-date database:

- If the most up-to-date database available is one you produced by the method described in "Backing Up Data While RSA Authentication Manager Programs Are Not Running" on page 89, use the first procedure in this section to recover data.
- If the most up-to-date database is on one of your Replicas, use the second procedure in this section.
- If your Primary has the most up-to-date database, use the third procedure in this section.

To recover data from an offline backup:

1. Log on the Primary as a Windows administrator.
2. From the RSA Authentication Manager Control Panel, stop all services.
3. From the directory where you stored the offline backup files, copy the **sdserv** and **sdlog** databases to the ***ACEDATA*** directory.

   The **sdserv** files you copy are **sdserv.d1**, **sdserv.b1**, **sdserv.db**, **sdserv.lg**, **sdserv.st**, and **sdserv.vrs**. The **sdlog** files you copy are **sdlog.d1**, **sdlog.b1**, **sdlog.db**, **sdlog.lg**, **sdlog.st**, and **sdlog.vrs**.
4. Generate a Replica Package for all Replicas, and distribute the new database files in the Replica Package to all Replicas.

   If **Push DB Assisted Recovery** is allowed, the Primary will push the new database files to the Replicas. Otherwise, copy the database files to the Replicas manually, and use the RSA Authentication Manager Control Panel to apply the Replica Package.
5. Start the RSA Authentication Manager Authentication Services on the Primary.

To recover data on a Replica to the Primary:

1. Log on the Primary as a Windows administrator.
2. From the RSA Authentication Manager Control Panel, stop all services.
3. Repeat steps 1 and 2 on the Replica.
4. Copy the **sdserv** database on the Replica to the Primary.

   The files you copy from the Replica to the Primary are **sdserv.db**, **sdserv.lg**, **sdserv.lic**, and **sdserv.vrs**.
5. Generate a Replica Package for all Replicas, and distribute the new database files in the Replica Package to all Replicas.

   If **Push DB Assisted Recovery** is allowed, the Primary will push the new database files to the Replicas. Otherwise, copy the database files to the Replicas manually, and use the RSA Authentication Manager Control Panel to apply the Replica Package.

6. Start the RSA Authentication Manager Authentication Services on the Primary.
7. Start the RSA Authentication Manager Authentication Services on the Replica.

To recover data on the Primary to a Replica:

1. Log on the Replica as a Windows administrator.
2. From the RSA Authentication Manager Control Panel on the Replica, stop all services.
3. Repeat steps 1 and 2 on the Primary.
4. Generate a Replica Package for all Replicas, and distribute the new database files in the Replica Package to all Replicas.

   If **Push DB Assisted Recovery** is allowed, the Primary will push the new database files to the Replicas. Otherwise, copy the database files to the Replicas manually, and use the RSA Authentication Manager Control Panel to apply the Replica Package.
5. Start the RSA Authentication Manager Authentication Services on the Primary.
6. Start the RSA Authentication Manager Authentication Services on the Replica.

Importing and Exporting Database Records

Some RSA Authentication Manager data can be exported and stored in clear ASCII text files. These files are for offline viewing or processing rather than for backup purposes. They cannot be restored to the databases for use by the Authentication Manager.

You can use the RSA Authentication Manager Database Administration application to create text files containing the following kinds of data:

- Certain user data such as user name and login.

  Click **User** > **List Users** and click **Help** for instructions.
- Log records in the form of an RSA Authentication Manager report.

  For more information, see "Sending a Report to a File" on page 167.
- Log records in Comma-Separated Values (CSV) format for use with third-party software such as Microsoft Excel.

  For more information, see "Scheduling Automated Log Database Maintenance" on page 157.

Store these files in a secure area. The data they contain can pose serious threats to system security if unauthorized personnel gain access to it.

Using the Database Dump and Load Utilities

With the dump and load utilities you can export database records in a format that (unlike text files) you *can* import into the database. For more information, see the *Windows Installation Guide*.

Recovery Procedures

In the event of an Authentication Manager hardware failure or database problem, use the following procedures to recover or replace the failed hardware or database.

Some steps in the procedures depend on whether your system uses Push DB Assisted Recovery. RSA Security recommends that you enable this feature. For more information, see "Push DB Assisted Recovery" on page 23.

To configure your system to use Push DB Assisted Recovery, start the Database Administration application, click **System** > **Edit System Parameters**, and select **Allow Push DB Assisted Recovery**.

Determining Which Database is Most Up-To-Date

If you have an RSA Authentication Manager Advanced license and are using multiple Replicas, whenever you are instructed to use the most up-to-date database, use the following procedure to make that determination. If the Primary hardware is still functioning, check the Event Log on the Primary. If the Primary hardware is no longer functioning, check the Event Log on each of the Replicas.

To determine the most up-to-date database:

1. On the Authentication Manager, click **Start > Programs > Administrative Tools > Event Viewer**.
2. Click **Log > Application Log**.
3. On the Primary, look for the following message:

   ```
   Primary Successfully Received Replica Records
   ```

   This message includes a date and time and the IP address of a Replica. The Replica indicated by the IP address in the most recent message contains the most up-to-date database.

   On a Replica, look for the following message:

   ```
   Replica Successfully Reconciled Databases
   ```

   This message includes a date and time, and the IP address of the Primary. Check the Event Log on each of the Replicas. The Replica that contains the most recent message contains the most up-to-date database.

Replacing a Replica Database

If the database on a Replica needs to be replaced, you must create a new Replica Package on the Primary and specify that the Replica requires a new database.

To replace the database on a Replica:

1. Log on to the Primary as a Windows administrator.
2. From the RSA Authentication Manager Control Panel on the Replica, stop the RSA Authentication Manager only.

   All administrative sessions are disconnected.

3. Repeat steps 1 and 2 on the Replica whose database you are replacing, and then log on again to the Primary.
4. Click **Start** > **Programs** > **RSA Security > RSA Authentication Manager Configuration Tools > RSA Authentication Manager > Replica Management**.

   Note: If **Details** is the only active command button, either you are on a Replica, or you did not shut down the database brokers.

5. Select the Replica from the **Servers in This Realm** list.
6. Click **Generate Replica Package**.

   You are asked if you want to mark the selected Replica for database push.
7. Click **OK** when prompted to generate the Replica Package for the selected Replica.
8. Click **OK** when the Replica has been successfully marked for database push.

   You are prompted to confirm that you want to mark each Replica. Click **OK** each time you are prompted to confirm that you want to mark the Replica for push.
9. Click **OK** when the success message displays.

   The Replica Package is created in the **replica_package** directory in the ***ACEDATA*** directory.
10. Copy the files in the ***ACEDATA*\replica_package\database** directory and the ***ACEDATA*\replica_package\license** directory on the Primary to a directory outside of ***ACEDATA*** on the Replica.
11. On the Replica, use the RSA Authentication Manager Control Panel to apply the Replica Package.

Replacing Replica Hardware

If a Replica experiences a hardware failure and is no longer able to function, the recommended method for replacing that Replica is to use the **Replace** button in the Replica Management interface. You must first select a network machine to use as a replacement Replica.

To replace Replica hardware:

1. Select the Replica from the **Servers in This Realm** list, and click **Replace**.
2. In the **Name** box, type the name of the replacement Replica.
3. Place your cursor in the **IP Address** box.
4. The IP address of the replacement Replica displays in the **IP Address** box.
5. Click **OK**.
6. In the message that displays, click **OK**.
7. Generate a Replica Package and install the replacement Replica using the Replica Package.
8. For instructions on installing a Replica, see the *Installation Guide* for your platform.

9. As a result of replacing the Replica, you may need to perform the following tasks:
   - If the old Replica is specified as a Local Realm Authentication Manager or a Remote Realm Authentication Manager for cross-realm authentication, edit the realm record in the database, and in the database in the Remote realm to reflect the name and IP address of the new Replica. For more information, see the Help topic "Edit Realm."
   - If the Replica was specified as a RADIUS server, install the RADIUS server and make sure that all RADIUS clients are configured to use the new Replica.

     For information on installing the RADIUS server, see the *RSA RADIUS Server 6.1 Administrator's Guide*.
   - If the Replica is specified as an Acting Authentication Manager for legacy Agent Hosts, generate new **sdconf.rec** files for all legacy Agent Hosts that use this Authentication Manager as an Acting Master or Acting Slave, and distribute the **sdconf.rec** file to the Agent Hosts. For more information, see the Help topic "Assign Acting Servers."
   - If the Replica is specified in any **sdopts.rec** files for version 5.0 (or later) Agent Hosts, edit the **sdopts.rec** file on the Agent Host to reflect the name and IP address of the new Replica.

Replacing the Primary Database

If the database on the Primary is corrupted, you must replace the Primary database with the most up-to-date Replica copy of the database, and create a new Replica Package that will be distributed to all other Replicas.

To replace the Primary database:

1. From the RSA Authentication Manager Control Panel, stop the RSA Authentication Manager only.

   All administrative sessions are disconnected.
2. Dump the database from the Replica. On the Replica, click **Start** > **Programs > RSA Security > RSA Authentication Manager Database Tools** > **Dump**.
3. In the Database Dump dialog box, select **Dump Server Database** only, and click **OK**.

   The dump utility creates the **sdserv.dmp** file in the ***ACEDATA*** directory. Any existing dump file is overwritten. When the dump is complete, click **Done**.
4. Copy the **sdserv.dmp** file to the Primary.
5. From the RSA Authentication Manager Control Panel on the Primary, stop all services.
6. Create a new, empty database on the Primary. In the ***ACEPROG*** directory, double-click **sdnewdb.exe**.
7. Load the dump file into the new database. Click **Start** > **Programs > RSA Security > RSA Authentication Manager Database Tools** > **Load**.
8. Select **Server Database**.

9. Type the pathname of the **sdserv.dmp** file in the **Path of server dump file** box, or browse to the directory by clicking the **Browse** button, selecting the file, and clicking **OK**.
10. When the database load is complete, click **OK**.
11. On the Primary, create a Replica Package. Click **Start** > **Programs** > **RSA Security > RSA Authentication Manager Configuration Tools > RSA Authentication Manager Replica Management**.

    Note: If **Details** is the only active command button, either you are on a Replica, or you did not shut down the database brokers.

12. Select all the Replicas from the **Servers in This Realm** list.
13. Click **Generate Replica Package**.

    You are asked if you want to mark the selected Replica for database push.
14. Click **OK** when prompted to generate the Replica Package for the selected Replica.
15. Click **OK** when the Replica has been successfully marked for database push.

    You are prompted to confirm that you want to mark each Replica. Click **OK** each time you are prompted to confirm that you want to mark the Replica for push.
16. Click **OK** when the success message appears.

    The Replica Package is created in the **replica_package** directory in the ***ACEDATA*** directory.

    If your RSA Authentication Manager System Parameters are set to enable Push DB Assisted Recovery, the Primary will push the database files to the Replica when you restart the Primary and Replica, completing the process.

    If the System Parameters are *not* set to enable Push DB Assisted Recovery, go to step 17.
17. Copy the files in the ***ACEDATA*\replica_package\database** directory on the Primary to a directory outside of the ***ACEDATA*** directory on the Replica.
18. On the Replica, use the RSA Authentication Manager Control Panel to apply the Replica Package.

Nominating a Replica to Replace Primary Hardware

If your Primary hardware fails, you can nominate an existing Replica to the Primary. You must first select a Replica that you intend to nominate. Then, on the selected Replica, you can click the **Nominate** button in the Replica Management interface and automatically convert the Replica to the Primary. An updated Replica Package is created in the ***ACEDATA*\replica_package** directory of the new Primary.

Note: If you want to replace a functional Primary with newer hardware, you can add the new hardware as a Replica and then nominate it as the Primary. Then you can take the old Primary offline. However, you must follow a specific procedure to do this: first, stop the current Primary, add the new machine as a Replica and generate a Replica package for the new machine. Restart the current Primary back up, and let the Replicas fully reconcile. Now you can complete the standard nominate procedure for the new Replica, as described in the following subsections.

Before Nominating a Replica

Before you nominate a Replica, you must assess the condition of the failed Primary hardware. If the failed Primary will be inoperable for a prolonged period, you will need to nominate a Replica. If the necessary repairs can be completed in a short amount of time, you may decide that you *do not* need to nominate a Replica, and that instead, you will repair the original Primary. In either of these scenarios, each of the Replicas continue to process authentication requests during the time that the Primary is not running. If you repair the original Primary, you will most likely want to inform all Quick Admin and remote administrators of the situation, and explain to them that neither Quick Admin nor Remote Administration of any machine in the realm will be possible until the Primary has been restored.

To nominate a Replica:

1. Select a Replica to use as a replacement for the failed Primary.

   Note: RSA Security recommends that you select the Replica that contains the most up-to-date database. For more information, see "Determining Which Database is Most Up-To-Date" on page 94.

2. From the RSA Authentication Manager Control Panel on the Replica, stop the RSA Authentication Manager only.

   All administrative sessions are disconnected.

3. Click **Start** > **Programs** > **RSA Security > RSA Authentication Manager Configuration Tools > RSA Authentication Manager Replica Management**.

4. Click **Nominate**.

5. Click **OK** to nominate this Replica.

6. Start the RSA Authentication Manager services and database brokers on the new Primary.

   If your RSA Authentication Manager System Parameters are set to enable Push DB Assisted Recovery, the Replica Package is automatically distributed and applied to each Replica.

   If the System Parameters are *not* set to enable Push DB Assisted Recovery, repeat steps 7 through 13 on each Replica.

7. Stop all services on the Replica.

8. Copy the files in the ***ACEDATA*\replica_package\database** directory and the ***ACEDATA*\replica_package\license** directory on the new Primary to a directory outside of ***ACEDATA*** on the Replica.
9. On the Replica, use the RSA Authentication Manager Control Panel to apply the Replica Package.

Note: If you repair the old Primary and restore it to your network, it is automatically added as a Replica. If you want to restore it as the Primary, you must nominate it.

When you replace damaged Primary hardware by either nominating a Replica or installing the Primary on a new machine, be aware that there are resulting implications for Quick Admin, RADIUS servers, Agent Hosts, LDAP synchronization and Remote Administration. In order for these features to function properly with a new Primary, perform these tasks in order of importance, referring to the appropriate instructions.

1. If Quick Admin is installed, you must reconfigure the Quick Admin settings with the name and IP address of the new Primary. For instructions, see "Reconfiguring Quick Admin" on page 51.
2. If the Authentication Manager is specified as a Local Realm Authentication Manager or a Remote Realm Authentication Manager for cross-realm authentication, edit the realm record in the database, and in the database in the Remote realm to reflect the new name or IP address. For more information, see the Help topic "Edit Realm."
3. If the failed Primary was specified as a RADIUS server, you can either install the RADIUS server on the new Primary, another Replica or a separate host machine. So as not to impact the administrative capability of the new Primary, RSA Security recommends that you enable RADIUS on another Replica. Be sure to
   - Add the Authentication Manager you choose to use as the RADIUS server to the database as an Agent Host. For more information, see "Adding Servers as Agent Hosts to the Primary Database" in the *Windows Installation Guide*.
   - If you opt to use the new Primary as the RADIUS server, update the RADIUS Server configuration settings so that they are identical to those that were on the old Primary.
   - Configure all RADIUS clients to use the appropriate name and IP address of the designated RSA RADIUS server. See the NAS device manual for specific configuration instructions.
4. If the Authentication Manager is specified as an Acting Authentication Manager for legacy Agent Hosts, generate new **sdconf.rec** files for all legacy Agent Hosts that use this Authentication Manager as an Acting Master or Acting Slave, and distribute the **sdconf.rec** file to the Agent Hosts. For more information, see the Help topic "Assign Acting Servers."
5. If the Authentication Manager is specified in any **sdopts.rec** files for version 5 Agent Hosts, edit the **sdopts.rec** file on the Agent Host to reflect the new name or IP address of the Authentication Manager.

6. If the Authentication Manager was previously set up with LDAP synchronization jobs that use SSL to connect to the LDAP server, make sure that the new Primary has the required **cert7.db** file in the ***ACEDATA*/ldapjobs/sslcerts** directory. Otherwise, when LDAP synchronization runs, you will see the error:

   ```
   LDAP connection error - Failed to initialize LDAP session
   ```

   For information about setting up the **cert7.db** file, see "Using SSL" on page 114.

7. For all Remote Administration machines, copy the **sdconf.rec** and the **server.cer** file from the ***ACEDATA*** directory on the Primary to the Remote Administration machine, remove the Primary from the Remote Administration machine and then add the Primary using the new **sdconf.rec** file. For more information, see the *Windows Installation Guide*.

Maintaining Customer-Defined Data (Extension Records)

With the RSA Authentication Manager extension records you can define and manage database information that is useful to your organization, although it is not required to run RSA Authentication Manager programs. This customer-defined information is called **extension data**.

The RSA Authentication Manager Database Administration application provides menu options you can use to access and process extension records. The following table shows each type of extension data you can manage, the database table where it is stored, the menu you use to manage it, and a place to find further information.

Extension Data	Database Table	Menu	Page to See
RSA Authentication Manager system-related	CustSystemExtension	System	215
Agent Host-related	CustClientExtension	Agent Host	57
Group-related	CustGroupExtension	Group	122
Log entry-related	CustLogExtension	Log	101
Site-related	CustSiteExtension	Site	135
Token-related	CustTokenExtension	Token	120
User-related	CustUserExtension	User	See the Help

To create reports based on customer-defined data, click **Extension Data** on the Report menu.

Note: For additional information about extension fields and about creating custom administration programs, see the *Administration Toolkit Reference Guide* (**authmgr_admin_toolkit.pdf** in the *ACEDOC* directory).

Managing Log Extension Data

This section explains how to create, modify, and delete log-related extension data. You can find information on managing other kinds of extension data through the table in the preceding section, "Maintaining Customer-Defined Data (Extension Records)."

You can add information to existing log entries in the log entry extension fields. This information can be used afterward to select the log entries for a report.

To edit log extension data:

1. Click **Log** > **Edit Log Extension Data**.
2. Select the type of log message to which the extension data is related: Activity, Exception, or Incident.

   The Log Entry Selection Criteria dialog box opens.
3. Enter specifications in one or more fields in the Log Entry Selection Criteria dialog box. For an explanation of the fields, see "Selection Criteria for Report Content" on page 164.

   To reset all selection criteria to the default values, click **Clear**.
4. After choosing the selection criteria, click **OK**.

   The Select Log Entry dialog box opens and displays only log records that meet all the specifications you entered.

   For each entry, the dialog box shows the time (Coordinated Universal Time and local time), the user for whom the activity was recorded, and the log message. The selection values remain in effect until you or another administrator changes them or until you end the current administration session.
5. Select the log entry to which the extension data is related and click **Edit Log Extension Data**.

   The Edit Log Extension Data dialog box displays the log entry and the records defined for this entry. Each record consists of a secondary key (up to 48 characters) and data (up to 80 characters).
6. You can add, modify, or delete these records. You can create more than one record with the same key, but you cannot create duplicate records (records having the same key *and* the same data values) in one extension database table.

   - To change an existing record, select the record, modify the information displayed in the **Key** or **Data** fields, and click **Save**. (The **Save** button is unavailable until you make an entry in one of these fields.)

     To clear the fields without changing the record, click **Clear**.
   - To create a new record, click **Clear** if necessary to clear the **Key** and **Data** fields. Enter the information for the new record and click **Save**.
   - To delete a record, select the record and click **Delete**. Click **OK** to confirm.
7. Click **Exit** to close the Edit Log Extension Data dialog box.

Running External 4GL Procedures

If you are comfortable programming in 4GL, you can run custom 4GL procedures to process RSA Authentication Manager data directly from the Database Administration application. To run a procedure that updates RSA Authentication Manager data, you must be a realm administrator or be assigned the **Run Custom 4GL** task.

CAUTION: A 4GL procedure can overwrite or delete valid data, such as log records or extension data, and can even corrupt your database. RSA Security **strongly advises** that you use the Administration Toolkit to create custom applications to work with your RSA Authentication Manager database. For information, see the *Administration Toolkit Reference Guide* (**authmgr_admin_toolkit.pdf** in the ***ACEDOC*** directory).

There are a number of fields that cannot be modified by custom administration programs. For information about these fields and for additional information about creating custom administration programs, see the *Administration Toolkit Reference Guide* (**authmgr_admin_toolkit.pdf** in the ***ACEDOC*** directory).

To run a 4GL procedure from the Database Administration application:

1. Click **Administration** > **File** > **Run Custom 4GL**.

   The Run External Procedure dialog box opens.

2. In the **Procedure Name** field, enter the filename of the procedure to run or click **Browse** and select a filename from a list.

3. Use the **Automatically Connect to RSA Database** checkbox to indicate whether the specified procedure should be run against your RSA Authentication Manager database.

   This checkbox is provided for convenience. If you select it, you do not have to include lines of code in the 4GL procedure to identify your administrator privileges or target the RSA Authentication Manager database. The Database Administration application does this work for you.

   If you are running a procedure that accesses a database other than the RSA Authentication Manager database, do not select this box. Instead, include code for connecting to that database in the 4GL procedure.

4. You can run a procedure against all database records (with the exception of those that are marked by an asterisk in the database description in the *Administration Toolkit Reference Guide*), or you can use the **Object Type** field to limit the procedure to records of one specific kind (user records, token records, and so on.)

   To run a procedure against all kinds of records, use the default object type (**None**). To run the procedure against records of a specific kind, highlight one type of data (**User**, **Token**, **Group**, **Agent Host**, **Site**, or **Realm**) under **Object Type**. Then, select a specific record from the standard selection dialog box that opens and click **OK**.

The **Argument List** displays certain fields from the record you have chosen. These are the fields whose values the procedure can use. The Database Administration application extracts the value of each field and concatenates these values (in the order displayed) into a single string, separating them with pound signs (#). Your application can be written to parse the string in order to process records by field values.

The following table shows the fields from the record of each object type that the Database Administration application extracts and concatenates when you select it in the **Object Type** field.

Object Type	Contents of Argument List
User	First name, last name, default login, default shell
Token	Token serial number, last login date, last login time
Group	Site name, group name
Agent Host	Agent Host name, network address, protocol
Site	Site name
Realm	Primary name, Primary address, Replica name, Replica address

5. Click **OK**.

6 Registering Users for Authentication

This chapter describes user-related administrative tasks. The sections of the chapter are arranged in the order in which you should perform the tasks. When you complete all the tasks, your RSA Authentication Manager system is set up to authenticate your users, and your users can log on using their assigned RSA SecurID tokens.

Your responsibilities as an RSA Authentication Manager administrator include the following:

- Updating user information
- Responding promptly to a user's report of a stolen or missing token by disabling the token
- Responding promptly to a user's report of a compromised PIN by putting affected tokens into New PIN mode
- Backing up the Authentication Manager databases regularly
- Obtaining and installing replacements for tokens that expire or are destroyed

PIN Options

Before you assign and distribute tokens, you must define the following characteristics of users' PINs:

- Alphanumeric or numeric
- Fixed or varying lengths
- Generated by the user or by the system

When you have decided which PIN options are best for your system, set those options in the System Parameters dialog box.

To Begin: Click **System** > **Edit System Parameters**. For instructions, click **Help**.

Selecting Alphanumeric or Numeric PINs

RSA Security recommends the use of alphanumeric PINs with RSA SecurID standard cards and key fobs. PINs that include both numbers and letters provide greater security because they are more difficult to guess.

A potential disadvantage of using alphanumeric PINs is that long, system-generated alphanumeric PINs are usually difficult to memorize. A user who receives a PIN such as **kh8n4wo** is likely to write it down, thereby compromising security.

Note: If you change the system parameter from alphanumeric to numeric after PINs have been assigned or created, each token with letters in its PIN is put in New PIN mode. Then the user of the token must enter a new PIN at the next authentication attempt.

PINs for RSA SecurID PINPads and software tokens must be numeric. A PINPad cardholder must enter his or her PIN in the card itself to generate a passcode. Because the PINPad has no letter keys, the New PIN operation does not allow these users to create or be given alphanumeric PINs.

Selecting PINs of Fixed or Varying Lengths

The RSA Authentication Manager system can be configured to require PINs that are all the same length or to accept PINs that vary in length between four and eight characters.

Some system administrators prefer fixed-length PINs for conformity with pre-existing systems or for ease of administration. Varying-length PINs offer more flexibility to users who create their own PINs because users can choose PINs of any length between the minimum and maximum specified by their system administrator.

Determining the Best PIN Length

RSA Authentication Manager PINs may have no fewer than four characters and no more than eight characters. RSA Security recommends PINs with at least six characters. Longer PINs provide greater security, but users find shorter PINs more convenient. Six characters provide a good balance between security and convenience.

Within the RSA Authentication Manager limits, you specify the range of allowable lengths. (To require PINs of a uniform length, set the minimum and the maximum length to the same value.) The New PIN operation neither generates nor accepts a PIN that violates the limits you set.

Selecting User-Created or System-Generated PINs

You must specify one of these three PIN assignment modes:

- All users have their PINs generated by the system.
- All users must create their own PINs.
- Designated users are permitted to create their own PINs but can elect to have the system generate them instead.

The RSA Authentication Manager system has both user-created and system-generated PINs enabled—in the Edit System Parameters dialog box, the **User-created PINs allowed** checkbox is selected, and the **User-created PINs required** box is clear. This configuration allows user-created PINs but does not require them. When you add users to the database, you specify for each user individually whether the user can create his or her own PIN or must use a system-generated PIN.

System-generated PINs have the advantage of preventing users from selecting obvious PINs like **1234**, or their phone extensions. System generation also prevents a user, whose token has been put in New PIN mode because someone has learned the PIN, from selecting the same—now compromised—PIN.

Although system-generated PINs offer these benefits, there can also be good reasons for users creating their own PINs. If a user's RSA SecurID token is registered on another RSA Security access control product used by your organization (for example, an ACM/1600), the user can elect to use the same PIN on that system. A user who has more than one token might want to use the same PIN for both. Using system-generated PINs would prevent such duplication, but it may be safer to allow it by letting users choose their own PINs. Users often find more than one PIN hard to remember and may therefore be tempted to write their PINs down.

You can also configure the RSA Authentication Manager system to require all users to create their own PINs. If you do this, the New PIN prompt does not give users the option of having the system generate a PIN.

Tokens that Do Not Require PINs

RSA Authentication Manager supports authentication with tokens that do not require PINs. To authenticate, instead of entering the PIN followed by the tokencode, the user enters just the tokencode currently displayed on his or her token.

Authenticating with just a tokencode is ideal for situations such as tokens on smart cards that a user has to unlock with a PIN or tokens on a desktop that a user has to unlock with a password. In these situations, the resource is protected by two-factor authentication without the user having to enter two different PINs.

You can configure both traditional and software tokens to not require a PIN.

To Begin: Click **Token** > **Change Tokens to Authenticate With...**. For instructions, see the Help. For information about configuring software tokens to not require a PIN, see "Issuing Software Tokens" on page 118.

Creating and Modifying a User Record

Each RSA SecurID tokenholder must have a user record in the RSA Authentication Manager database. There are four ways to create these records:

- Add data for individual users in the **Add User** dialog box.

  Click **User** > **Add User** to open the Add User dialog box. Click **Help** for instructions.
- Copy and edit an existing user record to make a template with group membership and Agent Host activation lists that you can use for many new users.

  Click **User** > **Copy User** to select a user record for a model and open the Add User dialog box. Click **Help** for instructions.

- Import user data from a SAM database.

  For more information, see "Importing Users from a SAM Database" in the *Windows Installation Guide* (**authmgr_install_windows.pdf** in the ***ACEDOC*** directory).

- Import user data from an LDAP directory.

  You can create user records in the RSA Authentication Manager database from data in an existing LDAP directory. Run the LDAP compare utility (**sdaceldap** in the ***ACEUTILS*** directory) to create a comma-separated value (.csv) file containing a list of LDAP users, and import the file into the database using the **Manage LDAP Users** option on the User menu. For more information, see the following section, "Importing LDAP User Data from the Command Line."

The data in user records, whether you type it into the record, derive it from a template, or import it in a file, can be modified through the **Edit User** option.

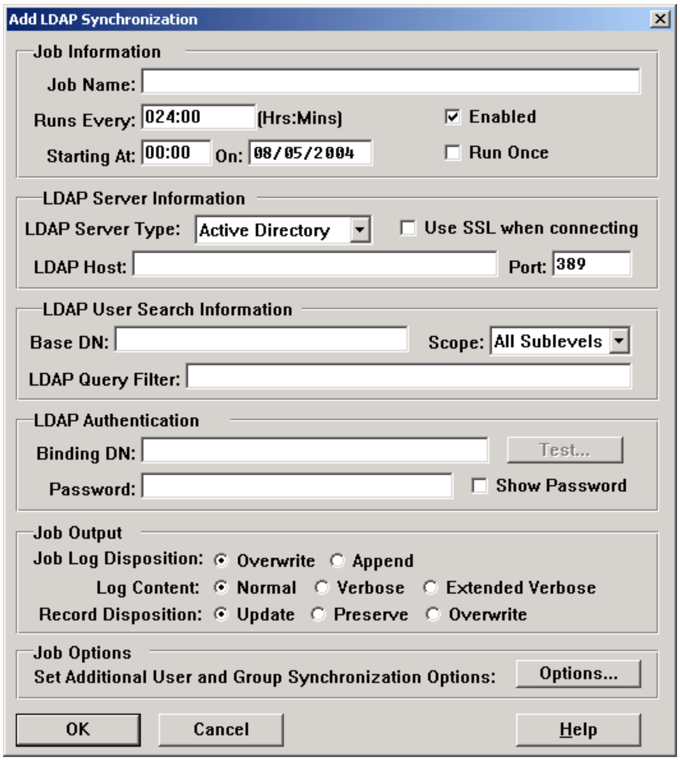
Synchronizing LDAP User Records

The Database Administration application provides LDAP synchronization tools that you can use to populate the Authentication Manager's user database and keep it synchronized with your LDAP directory server.

The RSA Authentication Manager supports the following LDAP directory servers: Microsoft Active Directory, Sun ONE Directory Server, and Novell NDS eDirectory.

Using commands in Database Administration, you can add, edit, copy, list, delete, and run synchronization jobs to automatically maintain LDAP user records in the RSA Authentication Manager database.

To Begin: On the Primary Authentication Manager, click **User** > **LDAP Users** and select **Add Synchronization**. For instructions, click **Help**.



Add LDAP Synchronization

Job Information

Job Name:

Runs Every: 024:00 (Hrs:Mins) ☑ Enabled

Starting At: 00:00 On: 08/05/2004 ☐ Run Once

LDAP Server Information

LDAP Server Type: Active Directory ☐ Use SSL when connecting

LDAP Host: Port: 389

LDAP User Search Information

Base DN: Scope: All Sublevels

LDAP Query Filter:

LDAP Authentication

Binding DN: Test...

Password: ☐ Show Password

Job Output

Job Log Disposition: ● Overwrite ○ Append

Log Content: ● Normal ○ Verbose ○ Extended Verbose

Record Disposition: ● Update ○ Preserve ○ Overwrite

Job Options

Set Additional User and Group Synchronization Options: Options...

You can run a synchronization job on demand or schedule it to run at specific times. During a synchronization job, the RSA Authentication Manager connects with, and examines user data in, the specified LDAP directory. A synchronization job can:

- Delete users that are no longer in LDAP.
- Enable or disable users in the Authentication Manager that are enabled or disabled in LDAP.
- Assign LDAP users to an existing Authentication Manager group.

You can also configure synchronization jobs to create groups and sites in the Authentication Manager database for new LDAP users. Groups that a synchronization job creates in the Authentication Manager database use the name of corresponding LDAP groups in which new users are found. If new users do not belong to a group in LDAP, the synchronization job does not create a group in the Authentication Manager database. You can also create a site for a new group. Sites created by a synchronization job use the same name as the corresponding OU level in LDAP.

Note: You can configure synchronization jobs locally or remotely on the Primary only.

When you add a synchronization job, a subdirectory with the name of the job is created under **/ldapjobs** in ***ACEDATA***. When the job completes, an output file named **ldapsync.log** is generated and stored in **/ldapjobs**. This file provides a summary of changes that occurred in the Authentication Manager database involving LDAP users.

Note: If you plan to administer LDAP users previously added to the database using **sdaceldap import**, first run **sdaceldap compare** to delete any of those users that are no longer in LDAP. Then you can run a synchronization job to update those users that remain in LDAP. For more information, see “The sdaceldap Utility” on page 111.

The sdldapsync Utility

With the **sdldapsync** utility you can run synchronization jobs from the command line. You can use the **sdldapsync** utility to run any synchronization job that is enabled in the database. Before you use this utility, use the **Edit Synchronization** command in Database Administration to change the date in the **Starting At** field to a date in the past. This prevents you from accidentally running the job using **sdldapsync** at the same time that the RSA Authentication Manager runs the job. You may want to add new jobs that you plan to run using **sdldapsync** only and schedule their run time in the past. To do so, type:

```
sdldapsync -j jobnumber
```

where *job number* is the number of the job in the database.

Importing LDAP User Data from the Command Line

As in prior releases, you can still create user records and import them from LDAP directory entries using the import and compare utilities. These existing utilities are supported on the same LDAP directory servers as is the LDAP synchronization interface.

Library Path Setting

The LDAP comparison utility uses the shared object libraries from the RSA Authentication Manager administration toolkit. When you run the comparison utility, the directory containing the shared object libraries must be in the user's library path environment variable. To ensure that the environment variables are set correctly, RSA Security provides the **admenv** utility, which displays the correct environment variable settings for your system. In the **/ace/utils** directory, run **admenv**, and set your environment variables according to the displayed information.

LDAP Map Files

RSA Authentication Manager includes a map file for each of the supported LDAP directory servers. The **sdaceldap** utility uses these files to map the entries in an LDAP directory to fields in the RSA Authentication Manager database. The map files (**active.map**, **sunone.map** and **novell.map**) are located in the **toolkit** directory in the ***ACEUTILS*** directory.

You can edit the map files to map up to four additional LDAP directory entries to data extension fields in the RSA Authentication Manager database. As a minimum, you must map the Default Login field in the RSA Authentication Manager database to an LDAP field.

Note: You must be on the Primary to edit LDAP map files.

To Begin: On the Primary, click **System** > **LDAP Maps** and click the name of the map file that corresponds to your LDAP directory service. For instructions, click **Help**.

The sdaceldap Utility

The **sdaceldap** utility is located in the **c:\ace\utils\toolkit** directory on Windows and the **/ace/utils/toolkit** directory on UNIX systems. It compares an LDAP directory with the RSA Authentication Manager database and generates a comma-separated values (**.csv**) file with user information that you can import into the database through the **Manage LDAP Users** menu item. (You can choose to import only the information that the user is an LDAP user, or to add certain user extension information such as an e-mail address or telephone extension.)

You can run this utility on a Primary or a Replica, but you must import the file on a Primary.

Two options determine the contents of the file generated by the **sdaceldap** utility: **import** and **compare**. The **import** option generates a file that lists the following:

- Users whose default logins are found in the LDAP directory, but not in the RSA Authentication Manager database. Importing this file into the database creates a user record for each user in which he or she is designated an LDAP user.
- Users whose default logins are found in both locations, but whose records in the Authentication Manager database do not identify them as LDAP users. You can handle these "conflicting" users individually or globally. Your global options are as follows:
  - Do not import them into the RSA Authentication Manager database.
  - Import them by overwriting everything in their current user records.
  - Import them by leaving current user data untouched and updating only the **LDAP User** field (plus any extension data fields you may have specified for the import).

The **compare** option generates a file that lists users who have been designated as LDAP users in the database, but whose entries in the LDAP directory have changed in some way—either some information in the LDAP entry for that user has changed, or the entry has been deleted. Only users whose records in the RSA Authentication Manager database identify them as LDAP users are compared with the users in the LDAP directory

The first time you run the utility, use the **import** option. (The **compare** option is ineffective until the RSA Authentication Manager database contains some LDAP users.) After the first time, choose the **import** or the **compare** option according to your purpose:

- To add to the Authentication Manager database users whose entries in the LDAP directory are new since your last import operation, choose **import**.
- To update the records of users who were previously imported from the LDAP directory, choose **compare**.

  When you import the .csv file created through this option, the user extension information you originally imported from the LDAP entry is updated if it has changed. For users who are no longer in the LDAP directory, you can choose (for individual users or for all users in this category) to remove the LDAP user designation from the user record in the Authentication Manager database or to delete the record completely.

Syntax

The following table describes the options and arguments for the **sdaceldap** utility.

Option	Argument	Description
-b	*basedn*	Specifies a base level LDAP directory containing a distinguished user name for comparison.
-D	*binddn*	A distinguished user name located in a specified LDAP server directory. This must be the name of an authorized administrator. With Microsoft Active Directory, you must use the **-D** option with a user recognized by the Windows domain. Otherwise 0 errors, 0 users are returned.
-d	*import* *compare*	Compares entries in the Authentication Manager database with entries from a corresponding LDAP directory, and generates an output file. • The **import** option generates a file that contains a list of users who have entries in the LDAP directory, but do not have user records in the RSA Authentication Manager database. • The **compare** option generates a file that contains a list of users that have been designated as LDAP users in the RSA Authentication Manager database, but whose entries in the LDAP directory have changed in some way.
-h	*hostname* or *IP Address*	The LDAP server name or IP address.

Option	Argument	Description
-m	*mapfile*	The map file required during comparison that is used to map the LDAP directory entries with the RSA Authentication Manager database fields. RSA Security provides map files for the following LDAP servers: Sun ONE Directory Server (**sunone.map**) Novell NDS eDirectory (**novell.map**) Microsoft Active Directory (**active.map**)
-o	*filename*	The name of the CSV output file.
-P	*pathname*	The pathname to a certificate database containing certificates for use with an SSL connection.
-p	*ldap port*	The TCP port number used by **sdaceldap** to connect to an LDAP directory server. The default is 389.
-s	*base* *one* *sub*	Specifies the levels of the LDAP directory that you want to search: **base** – search the base DN **one** – search one level below the base **sub** – search all levels below the base
-w	*password*	Specifies the password to be used with a distinguished name.
-Z	None	Specifies an SSL encrypted connection to the LDAP directory. When establishing the SSL connection, you must supply the **-P** argument to access the certificate database.

Example

The following example creates a file that contains a list of all the users in the LDAP directory who do not have user records in the Authentication Manager database.

This example is run on the AIX platform against a Microsoft Active Directory server, using a Secure Socket Layer (SSL) connection. The certificate from the Microsoft Active Directory server was imported into a Netscape browser, and then the **cert7.db** and **key3.db** were copied into the directory path designated by the **-P** option.

```
sdaceldap -h active -p 636 -Z -P "/ace/data/ldapjobs/sslcerts"
-D "user@rsa.com" -w passwd -b "cn=Users,DC=hixville,DC=com"
-d import -m active.map -s sub -o aixact.csv "objectclass=user"
```

Note: The example constitutes a single command line. In this listing, line breaks are placed to keep options with their arguments.

When this command is run on an RSA Authentication Manager, the command points to an LDAP directory server named **active** and connects using port number **636**. The **-Z** option indicates that an SSL connection should be used, and that the **cert7.db** and **key3.db** files that are needed to make the SSL connection are located in the **/ace/data/ldapjobs/sslcerts** directory. The user attempting to connect to the LDAP directory server is **user@rsa.com** with the password **passwd**. The utility searches in all sub (**-s sub**) levels under the base level **cn=Users,DC=hixville,DC=com**. The utility uses the map file for a Microsoft Active Directory server (**-m active.map**) to generate a file named **aixact.csv**. The filter **objectclass=user** limits the file to all users in the LDAP directory who do not have user records in the RSA Authentication Manager database.

Note: Filters apply only when importing (using the **-d import** option). They do not apply when using the **-d compare** option. For information about supported filters, see your LDAP directory documentation.

Using SSL

To establish an SSL connection to your LDAP directory server, the **sdaceldap** and **sdldapsync** utilities require a properly configured **cert7.db** (certificate database). To enable this, RSA Authentication Manager 6.1 includes the open source utility, **certutil.exe**, from www.mozilla.org. With this utility, you can create a **cert7.db** file and import your LDAP directory server's certificate (.cer or .crt) file into it.

The **certutil.exe** utility is located in the ***ACEUTILS*/toolkit** directory. Certificates from Microsoft Active Directory, Sun ONE Directory, and Novell NDS eDirectory can be imported. The following sample command creates a **cert7.db** file and imports a Microsoft Active Directory certificate file to the certificate database.

```
certutil.exe -A -n ace_ads -t P -i /data/LDAP/ADS_1.cer -d
/top/ace/data/ldapjobs/sslcerts
```

The following table describes the options used in this sample command. For complete information about the **certutil.exe** utility, go to **http://www.mozilla.org/projects/security/pki/nss/tools/certutil.html**.

Option	Argument	Description
-A	None	Specifies that a certificate is to be added to the certificate database. If **cert7.db** does not exist, it will be created.
-n	*name*	Specifies a nickname for the LDAP server certificate (in this case, "ace_ads"). The nickname does not have to match the actual certificate file name, but it must be unique in the certificate database.
-t	*trustedargs*	Specifies the trust attributes to apply to a certificate when creating it. For RSA Authentication Manager purposes, only the **P** option (valid peer/trusted peer) needs to be specified.
-i	*pathname*	Specifies the full pathname of the LDAP directory server's certificate file to be added to the certificate database.
-d	*path*	Specifies the directory in which the **cert7.db** and associated files will be created. For RSA Authentication Manager purposes, this must be ***ACEDATA*/ldapjobs/sslcerts**.

After you create the certificate database and import your server's certificate into it, you can copy the **cert7.db** to any RSA Authentication Manager Primary or Replica on which you intend to run the **sdaceldap** or **sdldapsync** utilities.

Manage LDAP Users

With **Manage LDAP Users** on the User menu you can import the file generated by the **sdaceldap** utility into the Authentication Manager database. While the compare utility can be run on any Authentication Manager (Primary or Replica), you can import the file only on a Primary. Once you process the generated file, the database contains a user record for each user processed. Optionally, you can assign a group to the users before processing the file, and the database contains a group with the processed users as members.

To Begin: Click **Manage LDAP Users** on the User menu. For instructions, click **Help**.

Contents of a User Record

Each user record can contain the following information about an RSA SecurID tokenholder (some of the information, such as the default shell, is optional):

- Name of the user
- Default login
- Default shell (when on a UNIX Agent Host other than AIX)
- If the user is a local user, the Token Type, whether the user authenticates with a passcode or just a tokencode, token status, and serial numbers of the user's assigned tokens
- Administration authority level
- Whether or not the user can create his or her own PIN
- Start and end dates of the period during which the user can be authenticated
- If the user is directly activated on one or more Agent Hosts, the times when the user can be authenticated on each Agent Host

To Begin: Click **User > Add User**. For information, click **Help**.To modify the user information, click **User > Edit User**.

Sharing Token Record Data with Other Installations

With the RSA Authentication Manager export option you can move token records among different Authentication Manager installations. The export option creates a dump file (.dmp) of the token records. Optionally, you can export user information associated with the token.

Note: In RSA Authentication Manager 6.1, you can no longer export tokens to ASCII (.asc) format. RSA ACE/Server software prior to version 5.0 can import *only* ASCII format files.

To use the token records on another system, use one of the Export Token options on either the Token or the User menu. Then, use the **Import Tokens** option on the Token menu to import the records to another system.

Assigning Tokens

When you first install the RSA Authentication Manager database it is empty, and the token records you received from RSA Security are unassigned. You must import the token records to the database and create a record for each authorized user before you can assign tokens to users.

The act of assigning a token to a user activates that user. A user is considered active if one or more tokens (or User Passwords) are assigned to the user. Every active user counts against the number of active users allowed by your license—that is, if you are licensed for 900 active users, you can assign up to three tokens (or User Passwords) to each of 900 users.

For more information about licensing and active users, see Appendix A, "Licensing."

Important: The more tokens a user is assigned, the longer it takes the Authentication Manager to process that user's authentication request because it tries to match the input against each of the user's tokens in turn. If no match is found, the Authentication Manager updates the bad login count for *all* of the user's tokens, increasing the chance that the tokens might be disabled or put into Next Tokencode mode. For examples, see "Evasion of Attack with a Token" on page 127.

RSA SecurID Software Tokens

An RSA SecurID Software Token is a software-based security token that resides on a user's computer, an RSA SecurID Smart Card, or other devices such as Palm Pilots, Pocket PCs, and cell phones. This software uses a two-factor authentication method when users access a network or a standalone resource that is protected by an RSA Authentication Manager.

Software tokens are available running SID (64-bit) or AES (128-bit) algorithms. RSA Security ships all software token records as .sdtid files. The Software Token application determines the type of tokens being delivered and reads the file accordingly.

AES (128-bit) software tokens are shipped with a predefined extension field named **DeviceSerialNumber** so that you can restrict the number of devices on which they are installed to one device. When you enter a serial number in the **DeviceSerialNumber** field, that number is included in the token file that an end user installs using the Software Token application. If the serial number the user enters does not match the number in the file, the token does not install.

Important: RSA Security highly recommends that you use passwords to protect software token XML files. In addition, store all software token files in a secure directory on a secure machine.

Issuing Software Tokens

When you issue software tokens, they are automatically enabled and assigned to the user or group of users you select in the RSA SecurID Issue Software Tokens dialog box. During this process, a file is generated which contains the software tokens, and you can specify a location for the file on your network. Administrators can then use the RSA Security software token application to install the software tokens on a supported device. For more information on software tokens, see the documentation distributed with that product.

To Begin: Click **Token** > **Issue Software Tokens**. Click **Help** for instructions.

Revoking Software Tokens

When you revoke software tokens, they are automatically disabled and unassigned from the associated users.

To Begin: Click **Token** > **Revoke Software Tokens**. For instructions, click **Help**.

Reissuing Software Tokens

Under certain circumstances, you may want to reissue a software token. When you reissue a token, the previously issued token no longer generates the correct codes and no longer functions. If you want to reissue the same token to the same user, you must select **Retain token information** in the Issue Software Token dialog box when you issue the token for the first time.

Contents of a Token Record

The Edit Token dialog box displays information from the token record for the specified token. To open the Edit Token dialog box, click **Token** > **Edit Token**.

The following paragraphs explain the fields in the Edit Token dialog box.

Serial Number. The serial number on the back of a hardware token or on the software token GUI.

Algorithm. SID tokens provide time-based authentication using the SID proprietary algorithm, while AES tokens provide time-based authentication using the Advanced Encryption Standard (AES) cryptographic algorithm.

Assigned to. If the token is assigned, this field displays the name of the person to whom the token is assigned. This name can be the user's name or login.

Next tokencode mode. If this value is turned on, the next time this token's PIN and code are used in an authentication attempt, the user is prompted to provide the next code displayed by the token before being given access to the system.

Replacement serial number. This field appears only if the token selected for editing has been assigned a replacement token. The field displays the serial number and type of the token that has been assigned as a replacement.

Lost Status. Whether or not the token is lost. Only tokens with Lost status can be assigned temporary passwords. If the token is lost, the following temporary password information appears:

- The type of password (Fixed or One-Time password set).
- The expiration date and time.

For fixed passwords, "AUTO" indicates that the status of the token changes to **Not Lost** when the fixed password expires. The RSA Authentication Manager performs this change if you select **When lost status expires, mark token as Not Lost** in the Lost Token dialog box.

Software Token. If the token is an issued software token, the following information appears:

- The password assigned to protect the token file.
- The copy protection status of the token.
- The number of times the token has been issued.
- Whether the token is currently issued.

Last login date. The date and time of the last successful authentication or resynchronization with this token is displayed in Coordinated Universal Time. If the token has never been assigned or is newly assigned, this field has no meaning and contains an initial date value of 1/1/1986.

Enabled status. If the Enabled checkbox is selected, the token is enabled. If a token is disabled, it cannot be used for authentication. This value is set by an administrator using the Enabled checkbox or by a series of unsuccessful authentication attempts, which disable the token. For more information, see "When a Token Is Stolen or Otherwise Missing" on page 126.

Token start and shutdown dates. The dates (in format *mm/dd/yyyy*) and times when the token started and when it will stop displaying codes. After the shutdown date, the token will no longer function.

Note: Because Token Reports reflect Coordinated Universal Time as opposed to local time, the token shutdown date and time may differ by several hours from the token shutdown date and time shown in the Edit Token dialog box.

New PIN mode. If the New PIN mode checkbox is selected, an administrator has set the token to New PIN mode. The user must complete the New PIN operation to gain access to a resource protected by RSA SecurID.

Token Assignment Date. The date on which the token was assigned to a user. If the token is unassigned, "NONE" appears in place of a date. If the assigned token was imported from an .asc file or from a .dmp file from a previous version of the RSA Authentication Manager, or was upgraded from a version earlier than 5.2, "UNDEFINED" appears in place of a date.

User Authenticates With. Specifies whether the user authenticates with a passcode or with a tokencode only. For more information, see "Tokens that Do Not Require PINs" on page 107.

Token records also contain the following information that is never displayed:

- A synchronization offset value. See "Synchronization" on page 132.
- The unique key used to generate the token's pseudorandom codes.
- The PIN for the token, known only to the assigned user.
- The number of consecutive failed authentication attempts with the token.

  The system disables any token used in a specified number of consecutive failed authentication attempts.

  A standard card or key fob is disabled before this number of failed attempts is reached if the attempts are made with an invalid PIN but with valid tokencodes. The Authentication Manager assumes that an unauthorized user has obtained the token and is using it with guessed PINs. After the third consecutive attempt of this kind, the token is disabled.

  This number is reset to zero when the user authenticates successfully with the token, when an administrator resynchronizes or unassigns the token, or when an administrator enables a token that was disabled following a series of failed authentication attempts.

  Note: If more than one token is assigned to a user, a failed authentication attempt counts against all tokens assigned to that user. Therefore, a token that does not have any failed authentication attempts could be disabled or put in Next Tokencode mode.

Modifying Token Extension Data

You can click **Edit Token Extension Data** in the Edit Token dialog box to edit the information in Token Extension records. These records contain customer-defined token information that can be accessed by custom administration programs.

Creating and Modifying Groups

This section describes an administrative tool for activating groups of users on restricted Agent Hosts.

Note: If all Agent Hosts on your system are open Agent Hosts, you do not need this information. The Groups feature is useful only for Agent Hosts that are restricted to a specified list of users and groups of users.

Organizing users into groups can save time and make administration more convenient. Rather than activate many individual users directly on an Agent Host, you can group users together and activate the entire group by a single action. Subsequent changes to a group are effective on all Agent Hosts on which the group is activated. For example, adding or removing a member adds or removes the member's access to all of those Agent Hosts at once. You can activate a single group on any number of Agent Hosts.

To provide another level of organization, you can associate groups with sites. A site can have any number of groups. For information about using sites, see "Creating and Modifying Sites" on page 135.

To Begin: To create a group, on the Group menu, click **Add Group** to open the Add Group dialog box. For directions, click **Help**.

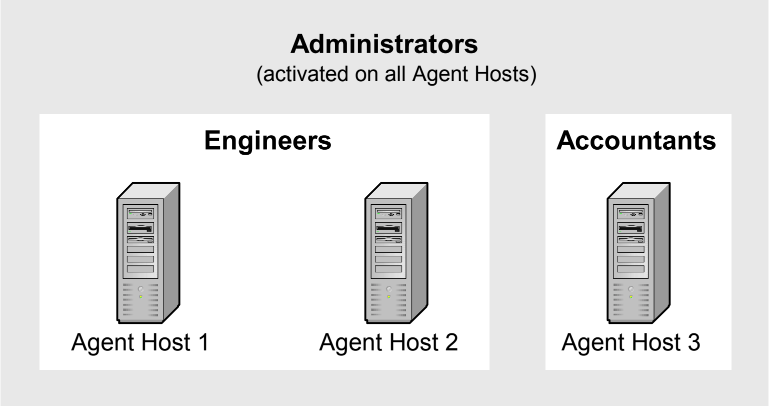
Example of Using Groups to Activate Users on an Agent Host

You can create groups that correspond to departments, to each floor in an office building, or to any set of similarly situated users.

Example: Grouping users by privilege level can be useful. You could create a group called **Administrators**, made up of all users who are realm administrators, and activate this group on all machines, including the Primary and Replicas (which should be set up for protection as RSA Authentication Agent Hosts).

You could then group the remaining users, who do not need access to the Authentication Manager, by department or by some other criterion. For example, an engineering department might need access to two Agent Hosts while an accounting department might need access to only one. You could create a group called **Engineers**, put all the members of the engineering department in this group, and activate the group on the two Agent Hosts. Then, you could create another group called **Accountants**, put all the members of the accounting department in this group, and activate it on one Agent Host.

The following diagram illustrates the implementation of group activations described in the preceding example.



Creating and Modifying Group Membership Lists

To add members to a group, you can use the **Group Memberships** button in either the Add User or Edit User dialog box, as described in "Creating and Modifying a User Record" on page 107. You can also use the **Members** button in either the Add Group or Edit Group dialog box.

Modifying Group Extension Data

Use the **Edit Group Extension Data** button in the Add or Edit Group dialog box to modify information in Group Extension records. These records contain information defined by your organization that can be accessed by custom administration programs.

For information on creating custom administration programs with the RSA Authentication Manager Administration Toolkit, see the *Administration Toolkit Reference Guide* (**authmgr_admin_toolkit.pdf** in the ***ACEDOC*** directory).

Activation on Agent Hosts

Depending on how an Agent Host is configured, you may need to explicitly associate users or groups with the Agent Host by placing an entry in the user or group record. The user or group is then said to be activated on the Agent Host. Whether you need to do this depends on how the Agent Host is configured.

An Agent Host can be **restricted** to a specified set of users and groups or **open** to all locally known users. Open Agent Hosts can even be set up to admit users from other realms that are registered in the local RSA Authentication Manager database. For more information about open and restricted Agent Hosts, see page 58.

Every properly installed Agent Host responds to an attempted login by challenging the user to enter a valid passcode. Whether a valid passcode is sufficient for access depends on the Agent Host configuration, as shown in the following table. (Assume that all users enter valid passcodes.)

Agent Host Configuration	Local Users Given Access	Outside Users Given Access
Restricted to directly activated users and groups.	Only users who are directly activated or members of directly activated groups.	Only users who are directly activated or members of directly activated groups and whose home realms are locally registered.
Open, configured to look up users in registered realms.	All.	All users whose home realms are locally registered.
Open, no lookup.	All.	None.

Note: Although it is not indicated in the table, you can restrict the access times of users and groups on an open Agent Host by activating them directly just as you would on a restricted Agent Host, and then defining their access times (see "Editing User and Group Access Times" on page 124).

Activating and Deactivating Users

To activate and deactivate users on an Agent Host, click **Agent Host Activations** in either the Add User or Edit User dialog box, or click **User Activations** in either the Add Agent Host or the Edit Agent Host dialog box.

Activating and Deactivating Groups

Although individual users can be activated directly on an Agent Host, it is often more convenient for administrative purposes to group the users and activate all of them on the Agent Host at the same time.

For an introduction to groups and instructions for creating groups and adding members to them, see "Creating and Modifying Groups" on page 121 and "Creating and Modifying Group Membership Lists" on page 122.

You can activate or deactivate a group on an Agent Host in either of two ways:

- In the Add Group or Edit Group dialog box, click **Agent Host Activations**.
- In the Add Agent Host or Edit Agent Host dialog box, click **Group Activations**.

Editing User and Group Access Times

By default, users can be authenticated at any time on protected Agent Hosts where the users are activated. The same is true for members of activated groups. With the **Edit Access Times** feature, however, an administrator can restrict the authentication access of users or groups to certain periods (for example, 8 a.m. to 5 p.m., Monday through Friday, or only on weekends).

Only *authentication* is affected by the **Edit Access Times** feature. A user who has been authenticated before the end of the designated time period continues to have access until some action on the user's part, such as logging out and logging back in, triggers a new passcode prompt.

To Begin:

- For users, click **User** > **Add User** > **Edit Access Times** or **User** > **Edit User** > **Edit Access Times**.
- For groups, click **Group** > **Add Group** > **Edit Access Times** or **Group** > **Edit Group** > **Edit Access Times**.

For instructions, click **Help**.

Distributing Hardware Tokens to Users

Use secure methods such as the following to distribute hardware tokens to users:

- Distribute tokens that are assigned but disabled.
- Enable a token only after you are satisfied that it is in the possession of the assigned user and that the user is ready log in for the first time using this token.
- If you must distribute enabled tokens to assigned users, do so through secure channels (such as having them delivered in person by trusted staff members).

Give each user the tokens assigned to him or her with a copy of the authentication instructions that explain how to use tokens. For information on locating and printing authentication instructions for users, see "Documentation" on page 11. Instructions for the care of RSA SecurID hardware tokens accompany each token purchased by your company. For information about planning the distribution of tokens, see the *Deployment Guide*.

Note: Instructions for distributing and using RSA SecurID Software Tokens are provided in the *RSA SecurID Software Token 3.0 for Windows® Workstations Administrator's Guide* and the *RSA SecurID Software Token 3.0 for Windows® Workstations User's Guide.*

Preventing and Handling User Authentication Problems

Problems related to tokens and authentication are likely to occur as RSA SecurID authentication becomes a regular part of your users' routine. This section describes some remedial tasks you will need to perform from time to time in the course of administering the RSA Authentication Manager. First, however, it suggests some educational measures you can take to minimize problems.

Educating Users About Security Responsibilities

A critical part of implementing a secure system is educating users about their security responsibilities. No security product can protect your system fully if your authorized users do not perform their security duties and take their responsibilities seriously.

Users and administrators must understand that the RSA Authentication Manager can offer **no** protection against an intruder who has been allowed to obtain both a user's PIN and RSA SecurID token. Therefore, it is essential to make sure that all users are aware of the following obligations on their part:

- To protect the secrecy of their PINs
- To protect the physical security of their tokens
- To notify an administrator immediately if their PINs are compromised (learned by anyone else)
- To notify an administrator immediately if one of their tokens is missing
- To protect their tokens from physical abuse
- To follow standard logoff procedures so that no opening is left through which an intruder can enter the system
- To reserve their accounts for their own use

Unassigning a Token

Unassigning a token breaks the link between the user record and the token record and clears the PIN. An unassigned token cannot be used for authentication.

A token is usually unassigned when its user leaves the organization. At that time the token is unassigned, rather than deleted, so that the token record remains in the database and the token can be assigned to another user. Deleting the token would permanently remove its record from the database.

To Begin: Click **Token** > **Edit Token**. Select the token to open the Edit Token dialog box, and click **Unassign Token**. Click **Help** for instructions.

Note: You can revoke a user's RSA SecurID Software Token by selecting the **Revoke Software Tokens** option on the Token menu. When a software token is revoked, it is automatically unassigned.

If a token is misplaced, do not unassign it. Instead, disable it. See the following section, "Disabling a Token."

Disabling a Token

When a token is disabled, all the information—including the user’s PIN—is preserved in the token record. When the token is found by its authorized user, it can be re-enabled and put into use again. A disabled token cannot be used for authentication, but the association between the user record and the token record is not broken. An administrator can enable the token at any time.

Disable a token when its authorized user reports it missing. If the lost token is found later, it can be re-enabled by an administrator and used again without any other administrator or user action required.

To Begin: Click **Token** > **Edit Token**. Select the token to open the Edit Token dialog box and clear the **Enabled** checkbox. For instructions, click **Help**.

When the RSA Authentication Manager Disables a Token

Sometimes the Authentication Manager disables a token without administrator intervention. After a series of three authentication attempts with a valid code from an RSA SecurID standard card or key fob, but with an incorrect PIN, the Authentication Manager disables the token. The assumption is that an unauthorized person has possession of the token and is using it with guessed PINs in attempts to gain access.

The Authentication Manager also disables ***any*** token that has been used in a certain number of consecutive failed authentication attempts. You can set the number of consecutive failed attempts that must occur before tokens are disabled. For more information, see “Configuring Agents to Handle Incorrect Passcodes” on page 63.

When a Token Is Stolen or Otherwise Missing

Important: You should disable lost or stolen tokens **immediately**. If an RSA SecurID token **and** its PIN are stolen, an unauthorized user will be able to gain access to your system.

All users must be instructed to report a stolen or missing token to an administrator without delay. *RSA Security recommends that the administrator disable the token immediately.* (Another, less secure, option is to assign the user a temporary password. Use of this feature depends on your security policy. For more information, see “Temporary Passwords to Replace Lost Tokens” on page 128.)

Unfortunately, an unauthorized person may gain possession of a token and start using it before the authorized user reports it missing. The RSA Authentication Manager evasion-of-attack features help maintain security in such a case.

If someone tries to use a stolen token to break into your system, the Authentication Manager can detect the attack, deny access, and disable the token. However, this feature offers ***no protection*** against an intruder who manages to obtain both a user’s PIN and RSA SecurID token.

Therefore, the following measures are **essential**:

- All users must protect the physical security of their tokens and the secrecy of their PINs.
- You must respond immediately to disable missing tokens and compromised PINs.

To Begin: Click **Token** > **Edit Token**. Select the token to open the Edit Token dialog box.

- To disable a token, clear the **Enabled** checkbox.
- To disable a PIN, click **Clear PIN**. (For more information, see "When a PIN Is Stolen or Otherwise Compromised" on page 129.)

For directions, click **Help**.

Evasion of Attack with a Token

The RSA Authentication Manager disables tokens used in consecutive failed authentication attempts as follows:

- Tokens that require the tokencode and PIN to be entered separately (the RSA SecurID standard card and key fob) are disabled after three consecutive attempts in which a valid tokencode is entered with an incorrect PIN. (This limit cannot be changed.)
- *All* tokens regardless of type are disabled after a certain number of consecutive failed authentication attempts. This number can be set for each Agent Host type, but setting it higher than three does not change the rule described in the previous item.

Note: These features are not supported on legacy Agent Hosts.

If a user has multiple tokens, the Authentication Manager does not distinguish which token has been used improperly. A failed authentication attempt with one token is counted against all tokens. A successful authentication clears the count ***only*** for the token that was authenticated successfully. Failed attempts can therefore accumulate and cause all or nearly all of a user's tokens to be disabled at the same time.

Consider two examples with multiple tokens. In each example, the Authentication Manager is configured to disable a token after four consecutive failed authentication attempts, and the user has three tokens, A, B, and C, each with three consecutive failed attempts already counted against it.

- The user attempts to log on with token A and mistypes the passcode. The Authentication Manager disables all three tokens (A, B, and C), because the failed attempt increases the count for each token from three to four.
- The user logs on with token C and is authenticated successfully. The system clears the failed authentication attempt count for token C, but tokens A and B still have three failed attempts counted against them.

  On the next attempt, the user again logs on with token C, but mistypes the passcode. Token C now has one failed authentication attempt counted against it, but tokens A and B now have four. The Authentication Manager therefore disables tokens A and B.

Temporary Passwords to Replace Lost Tokens

When a user loses a token, RSA Security recommends that you disable the token. However, depending on your organization's security policy and the user's security requirements, you can allow a user continued access while looking for a lost token by assigning the user a temporary password. There are two types of temporary passwords:

- A single "fixed" temporary password that can be used repeatedly until it expires
- A set of several "one-time" temporary passwords that can be used only one time each and that all expire on a specified date

A user authenticates with a temporary password by entering his or her PIN and the temporary password at the **Enter passcode** prompt. Procedures and requirements associated with the use of PINs still apply.

Not gaining access with a temporary password updates the count of consecutive failed logon attempts for the Lost token. Successfully authenticating resets this count to zero. Like any other token, a Lost token is automatically disabled after a certain number of consecutive failed authentication attempts.

Before you can assign a temporary password, you must define the token status as **Lost**. When the token is found, you must change the token status to **Not Lost** before the token can be used for authentication. Changing the token to **Not Lost** also disables any temporary passwords you may have created for the token. When you change a token status from **Lost** to **Not Lost**, the Authentication Manager informs you of any one-time passwords that were removed.

To Begin: On the Token menu, click **Edit Token** to select the token and open the Edit Token Dialog box. For instructions, click **Help**.

- To change token status, click **Edit Lost Status**.
- To assign passwords, select either **Fixed Password** or **One-Time Password Set** as the authentication method. Then click **Set up Passwords**.

Lost tokens are counted as part of the token statistics and can be listed in a separate report. Lost tokens can be exported, but their **Lost** status is not preserved.

Note: A temporary password is different from a user password, which the Authentication Manager treats as a type of token. You can assign a user password as the user's standard means of authentication. For more information, see "User Password Token" on page 15.

Emergency Access for Users of Offline Authentication

If you have deployed offline authentication for offsite users whose computers are not connected to your organization's network, there are a number of situations in which you can provide them emergency access. For information, see "Enabling Emergency Access for Offline Authentication Users" on page 62.

When a PIN Is Stolen or Otherwise Compromised

Instruct all users to tell an administrator immediately if they believe that someone has learned the PIN for a token assigned to them. The administrator must immediately put this token into New PIN mode.

An unauthorized person who learns a PIN may begin using it before the authorized user reports that the PIN has been compromised. The RSA Authentication Manager evasion-of-attack features can help maintain security in such a case.

If someone tries to use an authorized user's PIN to break into your system, the Authentication Manager can detect the attack and deny access. However, this feature offers no protection against an intruder who has managed to obtain both the PIN RSA SecurID token associated with it.

Therefore, the following measures are **essential** to the security of your system:

- All users must protect the secrecy of their PINs and the physical security of their tokens.
- You must respond immediately to disable a compromised PIN (by putting the token in New PIN mode) or to disable a missing token.

To Begin: Click **Token** > **Edit Token** and select the token to open in the Edit Token dialog box. For instructions, click **Help**.

- To disable the PIN and put the token in New PIN mode, check **New PIN Mode** and click **Clear PIN**.

Note: If you place an offline authentication user's PIN in New PIN Mode, it will clear emergency access data from the token record. If an offline user contacts you for emergency access reasons, you will have to provide them with an emergency access passcode.

- To disable the token, clear the **Enabled** checkbox.

Evasion of Attack with a Stolen PIN

If an unauthorized person with a stolen PIN does succeed eventually in guessing a tokencode, this person is still not granted access. After a series of failed authentication attempts, the Authentication Manager prompts for a second code. If the user does not enter the next code generated by the token, access is denied.

You can set the number of invalid attempts allowed before tokens are put into Next Tokencode mode. Use the Configuration Management application (on Windows) or ***ACEPROG*/sdsetup** (on UNIX). For more information, see the *Windows Installation Guide* or the *UNIX Installation Guide*.

Summary of Evasion-of-Attack Features

The following table summarizes the evasion-of-attack features.

RSA SecurID PINPads	
Event detected	**RSA Authentication Manager response**
Attempted login with guessed passcodes.	Puts token in Next Tokencode mode after a specified number of attempts.
Tokenholder exceeds allowed number of consecutive wrong passcodes.	Disables token immediately.
RSA SecurID Standard Cards and Key Fobs	
Event detected	**RSA Authentication Manager response**
Three incorrect passcodes with an invalid PIN but valid SecurID tokencodes.	Assumes that an unauthorized person has the token and is guessing PINs and disables the token immediately.
Attempted logon with guessed passcodes.	Puts token in Next Tokencode mode after a specified number of attempts.
Tokenholder exceeds allowed number of consecutive wrong passcodes.	Disables token immediately.
RSA SecurID Software Tokens	
Event detected	**RSA Authentication Manager response**
Entry of one incorrect passcode.	Puts token in Next Tokencode mode.
Tokenholder exceeds allowed number of consecutive wrong passcodes.	Disables token immediately.

Note: The Authentication Manager also puts the token into Next Tokencode mode when its clock and the system clock are no longer synchronized. For more information, see "Synchronization" on page 132.

Setting New PIN Mode

With RSA SecurID authentication, it is not necessary to change PINs on a regular basis. However, the PIN associated with a token must be changed under any of the following conditions:

- The authorized user has forgotten the PIN.
- An unauthorized person has learned the PIN.
- You see one of the following log messages: **PASSCODE REUSE ATTACK DETECTED** or **Simultaneous Login Detected**.

Important: Put the token in New PIN mode ***immediately*** if you learn that an unauthorized person may have learned a user's PIN or if you see either of these log messages, meaning an attempt has been made to break into your network. Notify the authorized user that the token's status is changed.

Helping a User with the New PIN Procedure

After the system is set up, users must complete the New PIN procedure. This procedure is also required whenever a user's token is set to New PIN mode.

Note: The New PIN procedure is not necessary if you have imported or converted token records that already contain PINs, or if you set the user's token to authenticate with the tokencode only.

New Users

The first time a new user is prompted for an RSA SecurID passcode, the user enters just the tokencode code currently displayed on the assigned token.

PIN Cleared When New PIN Mode Set

A user whose PIN has been cleared is treated as a new user during the authentication process. When prompted for the passcode, a new user must enter just the tokencode displayed on the token. If a user whose PIN has been cleared enters the old PIN along with the tokencode, the Authentication Manager responds with an **Access denied** message.

Token in New PIN Mode but Old PIN not Cleared

If a user's token is in New PIN mode but you have not cleared the old PIN, the user must enter the old PIN and the tokencode currently displayed on the token.

All Users

If users are creating their own PINs, emphasize the following points:

- If a PIN is compromised, the user must create a new PIN.
- PINs that contain both letters and numbers are more secure than PINs with numbers only. If your system allows alphanumeric PINs, encourage users of standard cards and key fobs to use them.

Resynchronizing a Token

RSA Security's patented, time-synchronization technology ensures that the pseudorandom tokencode displayed by a user's RSA SecurID token is the same code generated by the RSA Authentication Manager software for the prescribed time period.

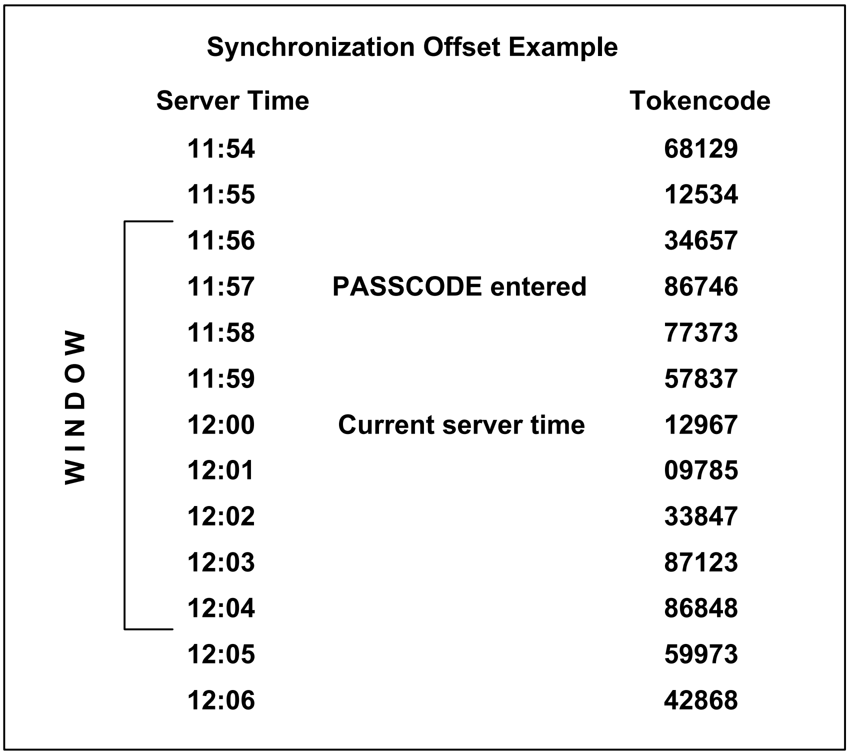
If a user is entering valid passcodes but is consistently being denied access, the token clock and the system clock may be out of synchronization. If the system time is correct and the user is being denied access, perform the **Resynchronize Token** operation described in the Help. This operation expands, temporarily, the number of tokencodes the Authentication Manager generates to find a match. If the operation produces a match, the token is resynchronized with the system clock.

The following section, "Synchronization," describes how synchronization works and provides examples to show when the system calculates a wider range of valid tokencodes.

Synchronization

Whenever a user attempts to authenticate, the Authentication Manager computes passcodes for the user's token over a range of time. The first time a user authenticates, this range (or "window") is based on the Authentication Manager's system time. If a value is found that matches the entered passcode, the difference between the Authentication Manager system time and the time corresponding to this passcode—called the "synchronization offset"—is stored in the token record in the Authentication Manager database. The Authentication Manager system time is also stored in the token record as the time of last logon.

The following example shows how a synchronization offset is calculated. This token is three minutes behind the server time, so the token has a synchronization offset of -180. When -180 is added to the current Authentication Manager time, the codes must match.



Synchronization Offset Example

Server Time		Tokencode
11:54		68129
11:55		12534
11:56		34657
11:57	PASSCODE entered	86746
11:58		77373
11:59		57837
12:00	Current server time	12967
12:01		09785
12:02		33847
12:03		87123
12:04		86848
12:05		59973
12:06		42868

On subsequent authentication attempts, the token synchronization offset is added to the RSA Authentication Manager system time, and the sum is used as the center of the range of passcodes to be computed. For example, if the user makes another attempt at 12:20 using the same token, the center of the range is determined as follows:

12:20 + (-180) = 12:17

The size of the window is usually equal to three code display intervals. (A code display interval is typically 60 seconds, but tokens can be purchased with longer or shorter intervals.) There are conditions that will cause the system to open the window wider.

Note: The window for RSA SecurID Software Tokens can be wider than for standard cards, PINPads, and key fobs. For more information, see the Software Token documentation.

The window is widened under any of the following conditions:

- A long time has passed since the last logon.

  The size of the window is directly proportional to the difference between the RSA Authentication Manager system time and the time of the last logon (that is, the longer the time since the last logon, the wider the window). This allows for access even if the token clock is no longer synchronized with the Authentication Manager clock.

- The token is put into Next Tokencode mode by a series of failed logons.

  When this happens, the Authentication Manager searches to see if the invalid codes are actually valid codes for a somewhat earlier or later time.

- The token is in New PIN mode.

  For a token in this mode, the Authentication Manager widens the range of its search in case the token has never been synchronized with the system clock or it has not been used for some time and is now out of synch with the system clock.

- The user is logging on through an Agent Host that is a communications server.

  The authentication procedure can take longer on this type of Agent Host. Therefore, the Authentication Manager scans a wider window to match codes.

If a token is so far out of synchronization with the RSA Authentication Manager system clock that its code is outside the expanded window, the token can no longer be used. Contact RSA Security Customer Support or local distributor for a replacement token.

When a matching passcode is found, both the synchronization offset and time of last login are updated in the token record. The authentication services process returns to using only the standard-sized window (that is, plus or minus one code display interval).

The window is expanded so that access is not denied to an authorized user who has entered a valid passcode. However, to ensure that allowing for matches in the widened window does not weaken security, the user is prompted for a second tokencode.

The Next Tokencode prompt appears if the token is in Next Tokencode mode because of a series of failed login attempts or if a code match was made in a widened window. Users need help getting out of this mode if the Agent Host device they are using cannot display the Next Tokencode prompt.

To Begin: Click **System** > **Edit System Parameters** and click **Help** for instructions.

Creating and Modifying Sites

As your user population and the number of protected Agent Hosts increase, consider using sites to organize Agent Hosts and groups for activation on Agent Hosts that are not open to all authorized users.

You can create one or more sites, and then associate Agent Hosts and groups with a site. Association with a site does not restrict the Agent Hosts on which a group can be activated. Any group can be activated on any Agent Host.

Unlike Agent Host names, group names do not need to be unique across sites. Because the site name becomes part of the group identifier, you can have a group called **Operations** at site **Denver** and a different group called **Operations** at site **Austin**.

If you use sites, you can run reports selected by site name and see if any of the following activities have been logged:

- Changing the name of the site
- Deleting the site
- Associating a group or Agent Host with the site
- Removing a group or Agent Host from the site
- Deleting a group or Agent Host associated with the site

To Begin: To create a site, on the Site menu, click **Add Site** to open the Add Sites dialog box. Click **Help** for directions.

Note: Reports selected by site do *not* include any logon activity, not even for Agent Hosts associated with the site. For more information about generating reports with selection criteria, see Chapter 9, "Reports."

Modifying Site Extension Data

Use the **Edit Site Extension Data** button in the Add or Edit Site dialog box to modify information in Site Extension records. These records contain user-defined information that can be accessed by custom administration programs.

For information on creating custom administration programs with the RSA Authentication Manager Administration Toolkit, see the *Administration Toolkit Reference Guide* (**authmgr_admin_toolkit.pdf** in the ***ACEDOC*** directory).

7 Database Maintenance (UNIX)

This chapter provides instructions to back up, restore, and create offline storage of RSA Authentication Manager data. It also describes how to manage the audit trail database by deleting or archiving old log records, and how to update information in your extension data records. Finally, it provides instructions to run external procedures directly from the Database Administration application.

This chapter describes some tasks that you do by entering UNIX commands at the command line prompt on the UNIX RSA Authentication Manager machine. It describes other tasks for which you need the Database Administration application. Run this application on your Remote Administration machine.

Before you begin, read the following section, "Maintaining Adequate Disk Space," for important information about maintaining adequate disk space on RSA Authentication Managers.

Maintaining Adequate Disk Space

If writing to an RSA Authentication Manager database fails because the file system is full, Authentication Manager programs will abort. Take whatever measures are necessary to avoid having inadequate disk space.

Important: Do not allow a Primary or Replica Authentication Manager's disk to become more than 90% full.

Because disk space requirements vary depending on your particular implementation of the system, use the examples of database sizes in the following table as guidelines only.

Number of Users	Number of Agent Hosts	Audit Trail Entries per Day	Authentication Manager Database Size	Estimated Daily Growth of Log Database	Estimated Syslog Growth
100	50	1000	1.8 MB	1 MB	.1 MB
1000	500	10000	2.2 MB	5 MB	.5 MB
10000	5000	25000	19.2 MB	11 MB	1.1 MB

Reclaiming Disk Space with Database Compression

Periodically, you must compress the Authentication Manager and log databases so that disk space is used more efficiently. RSA Security provides a database compression utility that enables you to reclaim disk space used by the RSA Authentication Manager databases. For example, after you have done a large number of deletions, such as purging old log records, use the compression utility to free the disk space the log database is no longer using.

Use the database compression utility also to shrink the **sdserv.bi** and **sdlog.bi** files. These files are created by the software for use in rolling back transactions if a group of transactions cannot be completed successfully. They are never automatically purged and can become quite large, especially after operations, such as importing tokens, that make a large number of changes to the databases.

No RSA Authentication Manager programs or database brokers can be allowed to run during the compression operation. It may therefore be most convenient to use this utility when you have stopped the **aceserver** process and the brokers to do your daily backup.

With multiple Replicas, authentication services continue to be available even if you shut down the Primary in order to back up data and compress the files.

To compress the database files on either the Primary or a Replica:

1. If you are not logged in as **root** or as the owner of the RSA Authentication Manager files, **su** to one of these two accounts.

   If you are unsure who was designated as file owner, run ***ACEPROG/*sdinfo** to view the configuration values.

2. Terminate all RSA Authentication Manager programs, including the **aceserver** process.

3. Stop the database brokers with the command:

   ```
   sdconnect stop
   ```

4. Run **sdcompress**, specifying which database is to be compressed:

   ```
   ACEPROG/sdcompress -l | -s
   ```

   where **-s** ("server") compresses **sdserv** and **-l** ("log") compresses **sdlog**.

   The **sdcompress** script automatically creates a backup of the database that is stored until the compression operation is successfully concluded. In cases of depleted disk space so extreme that there is not enough room to store this temporary backup, run **sdcompress** with the **-n** option. *This command creates no backup and should only be used when absolutely necessary.* If you must use it, first make a tape backup of the databases.

   ```
   ACEPROG/sdcompress -db -n
   ```

Backing Up and Restoring RSA Authentication Manager Data

Follow the instructions in this section to create reliable, complete backup files:

- ***ACEDATA:***
  - Back up the log and Authentication Manager databases daily. (You can set up RSA Authentication Manager to save the log database to an archive file according to a schedule and method you select. For more information, see "Scheduling Automated Log Database Maintenance" on page 157.)
  - Back up the **sdconf.rec** file any time you make changes to it.
  - Back up the **license.rec** file after initial installation of the product or after you upgrade the license record for any reason.
  - Back up SSL files for remote administration and LDAP synchronization (**sdti.cer**, **server.cer**, **server.key**, **key3.db**, and **cert7.db**).
  - Back up custom queries (**queries***).
  - Back up **sdtacplus.cfg** if you are using TACACS+.
- ***ACEPROG***
  - Back up the configuration file **hosts.conf**.
  - Backup the configuration file **sdcommdConfig.txt**.

Note: RSA Security recommends that you back up the databases when ***no*** RSA Authentication Manager programs are running. If you ***must*** make a backup without closing all of the programs, see the section, "Backing Up Data While RSA Authentication Manager Programs Are Running" on page 140.

Backing Up Data While RSA Authentication Manager Programs Are Not Running

If you have multiple Replicas, you can stop all RSA Authentication Manager programs on an Authentication Manager to back up data with no loss in authentication.

To back up the databases while they are not in use:

1. Make sure that no one is running any RSA Authentication Manager program.
2. At a command prompt, type:

   ```
   rptconnect stop
   aceserver stop
   sdconnect stop
   ```

   If you do not run **sdconnect stop**, your backups will include the lock files **sdserv.lk** and **sdlog.lk**. If you make and then restore database backups that contain lock files, **sdconnect start** fails.

3. Locate the data files you want to back up.

   The database files are stored in the ***ACEDATA*** directory (for example, **/top/ace/data**).

   These are the log database (**sdlog**) files:

   sdlog.b1
   sdlog.d1
   sdlog.db
   sdlog.lg
   sdlog.st
   sdlog.vrs

   These are the Authentication Manager database (**sdserv**) files:

   sdserv.b1
   sdserv.d1
   sdserv.db
   sdserv.lg
   sdserv.st
   sdserv.vrs

4. Use the UNIX command **tar -p** or **cp -p** to copy the log and Authentication Manager database files.

   Use the **tar** command to copy files to tape and the **cp** command to copy files to another directory. Preserve the file permissions by using the **-p** option.

Backing Up Data While RSA Authentication Manager Programs Are Running

This section describes the database backup command, which you can use to back up databases on both Primary and Replicas. However, a better backup method is described in the preceding section, "Backing Up Data While RSA Authentication Manager Programs Are Not Running,"

Note: *Do not use this backup method if you are in single-user mode.* You can back up while RSA Authentication Manager programs are running without endangering the integrity of the database, but the backup you get may not be complete. Before you begin, make sure that no one else is backing up a database at the same time. Simultaneous multiple backups can slow system performance significantly.

Syntax

The **sdbkup** command has the following syntax:

```
sdbkup [online] databasefile backupfile
```

The following table describes the options of the **sdbkup** command:

Option	Description
online	Specifies that you want to perform the backup while RSA Authentication Manager programs are running.
databasefile	Specifies the full pathname of the database file you want to back up (usually a file in the **ACEDATA** directory).
backupfile	Specifies the full pathname (or the name only) of the backup file.

For example, to back up the Authentication Manager database to a file named **sdserv1**, the command line would be:

```
sdbkup online /ace/data/sdserv /dev/rst0/sdserv1
```

If there is a file named **sdserv1** already, the following prompt appears:

```
*** backup_file already exists ***
Do you want to continue and overwrite the file? (y/n) [y]:
```

If you want to overwrite the **sdserv1** file, the command line would be:

```
sdbkup online /ace/data/sdserv dev/rst0/sdserv1
```

Restoring Databases Created by the Database Backup Command

Use the procedure described in this section to restore the databases created by the database backup command.

To restore a database:

1. Make sure that no RSA Authentication Manager program is running.
2. Stop the Report Creation Utility (if it is running), the **aceserver** process, and the database broker:

   ```
   rptconnect stop
   aceserver stop
   sdconnect stop
   ```

3. To restore the Authentication Manager database:

   ```
   sdrest /top/ace/data/sdserv /dev/rst0
   ```

4. To restore the log database:

   ```
   sdrest /top/ace/data/sdlog /dev/rst0
   ```

5. Generate a Replica Package for all Replicas, and distribute the new database files in the Replica Package to all Replicas.

   If **Push DB Assisted Recovery** is allowed, the Primary will push the new database files to the Replicas when you restart the Primary. Otherwise, copy the database files to the Replicas manually.

6. Restart the Primary.

Recovering Data From an Offline Backup or a Server

When you need to recover data that was not backed up through the **sdbkup** command, (for more information, see "Backing Up Data While RSA Authentication Manager Programs Are Running" on page 140), the appropriate procedure depends on the location of the most up-to-date database:

- If the best database available is one you produced by the method described in "Backing Up Data While RSA Authentication Manager Programs Are Not Running" on page 139, use the first procedure in this section to recover data.
- If the most up-to-date database is on one of your Replicas, use the second procedure in this section.
- If your Primary has the most up-to-date database, use the third procedure in this section.

To restore data from an offline backup:

1. If you are not logged in as **root** or as the owner of the RSA Authentication Manager files, **su** to one of these two accounts.
2. Stop all RSA Authentication Manager programs running on the Primary.

   Stop the Report Creation Utility (if it is running), the **aceserver** process, and the database broker by entering the following commands at a command prompt:

   ```
   rptconnect stop
   aceserver stop
   sdconnect stop
   ```

3. Using the command appropriate to the backup file format, copy the backup **sdlog** and **sdserv** databases to the ***ACEDATA*** directory.

   These are the log database (**sdlog**) files:

   sdserv.b1
   sdserv.d1
   sdserv.db
   sdserv.lg
   sdserv.st
   sdserv.vrs

   These are the Authentication Manager database (**sdserv**) files:

   sdserv.b1
   sdserv.d1
   sdserv.db
   sdserv.lg
   sdserv.st
   sdserv.vrs

4. Generate a Replica Package for all Replicas, and distribute the new database files in the Replica Package to all Replicas.

   If **Push DB Assisted Recovery** is allowed, the Primary will push the new database files to the Replicas. Otherwise, copy the database files to the Replicas manually.

5. Start the **aceserver** on the Primary.

To restore data on a Replica to the Primary:

1. If you are not logged on as **root** or as the owner of the RSA Authentication Manager files, **su** to one of these two accounts.
2. Stop all RSA Authentication Manager programs running on the Primary.

   Stop the Report Creation Utility (if it is running), the **aceserver** process, and the database broker by entering the following commands at a command prompt:

   ```
   rptconnect stop
   aceserver stop
   sdconnect stop
   ```

3. Repeat steps 1 and 2 on the Replica.

4. Using the command appropriate to the backup file format, copy the Replica database to the Primary.

   The files to copy from the Replica to the Primary are **sdserv.bi**, **sdserv.db**, **sdserv.lg**, **sdserv.lic**, and **sdserv.vrs**.

5. Generate a Replica Package for all Replicas, and distribute the new database files in the Replica Package to all Replicas.

   If **Push DB Assisted Recovery** is allowed, the Primary will push the new database files to the Replicas. Otherwise, copy the database files to the Replicas manually.

6. Start the **aceserver** on the Primary.

7. Start the **aceserver** on the Replica.

To restore data on the Primary to a Replica:

1. If you are not logged on as **root** or as the owner of the RSA Authentication Manager files, **su** to one of these two accounts.

2. Make sure that no RSA Authentication Manager programs are running on the Replica.

   Stop the Report Creation Utility (if it is running), the **aceserver** process, and the database broker by entering the following commands at a command prompt:

   ```
   rptconnect stop
   aceserver stop
   sdconnect stop
   ```

3. Repeat steps 1 and 2 on the Primary.

4. Generate a Replica Package for all Replicas, and distribute the new database files in the Replica Package to all Replicas.

   If **Push DB Assisted Recovery** is allowed, the Primary will push the new database files to the Replicas. Otherwise, copy the database files to the Replicas manually.

5. Start the **aceserver** on the Primary.

6. Start the **aceserver** on the Replica.

Importing and Exporting Database Records

Some RSA Authentication Manager data can be exported and stored in clear ASCII text files. These files are for offline viewing or processing rather than for backup purposes. They cannot be restored to the databases for use by the Authentication Manager.

You can use the RSA Authentication Manager Database Administration application on your Remote Administration machine to create text files containing the following kinds of data:

- Certain user data such as user name and login. Click **User** > **List Users** and click **Help** for instructions.
- Log records in the form of an RSA Authentication Manager report.

  For more information, see "Sending a Report to a File" on page 167.
- Log records in Comma-Separated Values (CSV) format for use with third-party software such as Microsoft Excel.

  For more information, see "Scheduling Automated Log Database Maintenance" on page 157.

Store these files in a secure area. The data they contain can pose serious threats to system security if unauthorized personnel gain access to it.

Using the Database Dump and Load Utilites

The dump and load utilities enable you to export database records in a format that (unlike text files) you *can* import into the database. For more information, see the *UNIX Installation Guide*.

Recovery Procedures

In the event of an Authentication Manager hardware failure or database problem, use the following procedures to recover or replace the failed hardware or database.

Some steps in the procedures depend on whether your system uses Push DB Assisted Recovery. RSA Security recommends that you enable this feature. For more information, see "Push DB Assisted Recovery" on page 23.

To configure your system to use Push DB Assisted Recovery, start the Database Administration application, click **System** > **System Configuration > Edit System Parameters**, and select **Allow Push DB Assisted Recovery**.

Determining Which Database is Most Up-To-Date

If you have an RSA Authentication Manager Advanced license and are using multiple Replicas, whenever you are instructed to use the most up-to-date database, use the following procedure to make that determination. If the Primary hardware is still functioning, check the syslog on the Primary. If the Primary hardware is no longer functioning, check the syslog on each of the Replicas.

To determine the most up-to-date database:

On the Authentication Manager, check the syslog for the most recent successful replication.

- On the Primary, look for the following message:

  ```
  Primary Successfully Received Replica Records
  ```

  This message includes a date and time, and the IP address of a Replica. The Replica indicated by the IP address in the most recent message contains the most up-to-date database.

- On a Replica, look for the following message:

  ```
  Replica Successfully Reconciled Databases
  ```

  This message includes a date and time, and the IP address of the Primary. Check the syslog on each of the Replicas. The Replica that contains the most recent message contains the most up-to-date database.

Replacing a Replica Database

If the database on a Replica needs to be replaced, you must create a new Replica Package on the Primary and specify that the Replica requires a new database.

To replace the database on a Replica:

1. Log on the Primary as **root** or as the owner of the RSA Authentication Manager files.

2. Stop all RSA Authentication Manager programs and database brokers running on the Replica and on the Primary. Change to the ***ACEPROG*** directory and type the following commands at a command prompt:

   ```
   aceserver stop
   sdconnect stop
   ```

3. On the Primary, create a Replica Package. Type:

   ```
   ACEPROG/sdsetup -package
   ```

4. At the **Name of replica** prompt, type the full name of the same Replica and press RETURN.

5. At the **Confirm** prompt, type **y** and press RETURN again.

6. Repeat Steps 4 and 5 for each database that needs to be replaced. When you have entered all the Replicas, press RETURN at the **Name of replica** prompt, and press RETURN again at the **Have you entered all the Replicas you would like included in this package (y/n/q) [y]:** prompt.

   If your RSA Authentication Manager System Parameters are set to enable Push DB Assisted Recovery, the Primary will push the database files to the Replica when you restart the Primary and Replica in the next step.

   If the System Parameters are *not* set to enable Push DB Assisted Recovery, copy the files in the ***ACEDATA*/replica_package/database** directory on the Primary to the ***ACEDATA*** directory on the Replica.

7. Start the RSA Authentication Manager and database brokers on both the Primary and Replica. On each system, type the following commands at a command prompt:

   ```
   ACEPROG/sdconnect start
   ACEPROG/aceserver start
   ```

   If Push DB Assisted Recovery is enabled, the Primary begins the assisted recovery process by pushing the new database to the Replica.

   If Push DB Assisted Recovery is not enabled, the recovery process is complete.

Replacing Replica Hardware

If a Replica experiences a hardware failure and is no longer able to function, you must replace the Replica in the database with another machine. Use the Replica Management utility to replace Replica hardware. The utility prompts you to enter the name and IP address of the Replica that you want to replace, and then prompts you to enter the name and IP address of the new Replica.

To replace Replica hardware:

1. Select a network machine to use as the replacement Replica.
2. Log on the Primary as **root** or as the owner of the RSA Authentication Manager files.
3. Stop all RSA Authentication Manager programs and database brokers running on the Primary. Change to the ***ACEPROG*** directory and type the following at a command prompt:

   ```
   aceserver stop
   sdconnect stop
   ```

4. On the Primary, run the replica management utility and replace the failed Replica. Type:

   ```
   ACEPROG/sdsetup -repmgmt replace
   ```

5. At the prompt, type the full name of the Replica you want to replace and press RETURN.
6. At the prompt, enter the new system name and IP address, and press RETURN.

   A replica package is generated in the ***ACEDATA*/replica_package** directory on the Primary.

7. Start the RSA Authentication Manager and database brokers on the Primary by entering the following commands at a command prompt:

   ```
   ACEPROG/sdconnect start
   ACEPROG/aceserver start
   ```

8. Copy the replica package directory to the new Replica. If your System Parameters are configured to allow Push DB Assisted Recovery, you need to copy only the license directory. If your System Parameters are *not* configured to allow Push DB Assisted Recovery, you need to copy both the license and database directories.

9. Perform a new installation of the Replica software on the new Replica using the new replica package. See the *UNIX Installation Guide* for full instructions on installing a Replica.

   If Push DB is enabled, the Primary begins the assisted recovery process by pushing the new database to the replica.

   If Push DB is not enabled, restart the RSA Authentication Manager services and database brokers on the Replica.

Repeat this procedure for any additional Replicas that need to be replaced.

Replacing the Primary Database

If the database on the Primary is corrupted, you must replace the Primary database with the most up-to-date Replica copy of the database, and create a new Replica Package that will be distributed to all other Replicas.

To replace the Primary database:

1. Log on the Primary as **root** or as the owner of the RSA Authentication Manager files.
2. Dump the database from one of the Replicas. On the Replica, change to the ***ACEPROG*** directory and type:

   ```
   sddump -s
   ```

   The dump utility creates the **sdserv.dmp** file in the ***ACEDATA*** directory. Any existing dump file is overwritten.
3. Copy the **sdserv.dmp** file to the Primary.
4. Stop all RSA Authentication Manager programs and database brokers running on the Primary. Change to the ***ACEPROG*** directory and type:

   ```
   aceserver stop
   sdconnect stop
   ```
5. Create a new, empty database on the Primary. Type:

   ```
   sdnewdb server
   ```
6. Load the dump file into the new database. Type:

   ```
   sdload -s -f pathname/sdserv.dmp
   ```

   For *pathname* enter the location of the dump file.
7. On the Primary, create a Replica Package. Type:

   ```
   ACEPROG/sdsetup -package
   ```
8. At the **Name of replica** prompt, type the full name of the Replica and press RETURN.
9. At the **Confirm** prompt, type **y** and press RETURN again.
10. Repeat Steps 7 and 8 for each Replica. When you have entered all the Replicas, press RETURN at the **Name of replica** prompt, and press RETURN again at the **Have you entered all the Replicas you would like included in this package (y/n/q) [y]:** prompt.

11. Start the RSA Authentication Manager and database brokers on the Primary. Type:

    ```
    ACEPROG/sdconnect start
    ACEPROG/aceserver start
    ```

    If Push DB is enabled, the Primary begins the assisted recovery process by pushing the new database to the replica.

    If Push DB Assisted Recovery is not enabled, copy the files in the **/replica_package/database** directory to each Replica. On the Replica, stop all RSA Authentication Manager programs and database brokers, move the database files to the ***ACEDATA*** directory, and restart the RSA Authentication Manager and database brokers.

Nominating a Replica to Replace Primary Hardware

If your Primary hardware fails, you can nominate an existing Replica to the Primary. You must first select a Replica that you intend to nominate. Then, on the selected Replica, click the **Nominate** button in the Replica Management interface and automatically convert the Replica to the Primary. An updated Replica Package is created in the ***ACEDATA*\replica_package** directory of the new Primary.

Note: If you want to replace a functional Primary with newer hardware, you can add the new hardware as a Replica and then nominate it as the Primary. Then you can take the old Primary offline. However, you must follow a specific procedure to do this: first, stop the current Primary, add the new machine as a Replica, and generate a Replica package for the new machine. Restart the current Primary, and let the Replicas fully reconcile. Now you can complete the standard nominating procedure for the new Replica, as documented in the following subsections.

Before Nominating a Replica

Before you nominate a Replica, you must assess the condition of the failed Primary hardware. If the failed Primary will be inoperable for a prolonged period, you need to nominate a Replica. If the necessary repairs can be completed in a short amount of time, you may decide that you *do not* need to nominate a Replica, and that instead, you will repair the original Primary. In either of these scenarios, each of the Replicas will continue to process authentication requests during the time that the Primary is not working. If you repair the original Primary, you will most likely want to inform all Quick Admin and remote administrators of the situation, and explain to them that neither Quick Admin nor Remote Administration of any machine in the realm will be possible until the Primary has been restored.

Note: RSA Security recommends that you select the Replica that contains the most up-to-date database. For more information, see "Determining Which Database is Most Up-To-Date" on page 144.

To nominate a Replica:

1. On the Replica, type:

   ```
   ACEPROG/sdsetup -repmgmt nominate
   ```

2. Type **y** and press RETURN to nominate the Replica as the new Primary.

3. Start the RSA Authentication Manager services and database brokers on the new Primary.

   If your RSA Authentication Manager System Parameters are set to enable Push DB Assisted Recovery, the updated Replica Package is automatically distributed to each Replica. When you restart the new Primary, the recovery process is complete.

   If Push DB Assisted Recovery is *not* enabled, repeat steps 5, 6, and 7 on each Replica.

4. Stop all RSA Authentication Manager services and database brokers on the Replica.

5. Copy the files in the ***ACEDATA*****/replica_package/database** directory and then in the ***ACEDATA*****/replica_package/license** directory on the new Primary to a directory outside of ***ACEDATA*** on the Replica.

6. Apply the Replica Package. On the Replica, type:

   ```
   ACEPROG/sdsetup -apply_package pathname
   ```

   The following message is displayed.

   ```
   Replica Package was successfully applied.
   ```

Note: If you repair the old Primary and bring it back on to your network, it is automatically added as a Replica. If you want to restore it as the Primary, you must nominate it.

When you replace damaged Primary hardware by either nominating a Replica or installing the Primary on a new machine, be aware that there are resulting implications for Quick Admin, RADIUS servers, Agent Hosts, and Remote Administration. In order that these features function properly with a new Primary, perform the following tasks, referring to the appropriate instructions.

Note: RSA Security recommends that you use Remote Administration to perform these tasks so that, where necessary, you may view associated Help topics. To enable Remote Administration, you must first perform task 1 on the Primary. Then, on a Remote Administration machine, you can perform task 2 through task 7 in any order.

1. For all Remote Administration machines, copy the **sdconf.rec** and the **server.cer** files from the ***ACEDATA*** directory on the Primary to the Remote Administration machine, remove the Primary from the Remote Administration machine, and then add the Primary using the new **sdconf.rec** file. For more information, see the *Windows Installation Guide*.

2. If Quick Admin is installed, you must reconfigure the Quick Admin settings with the name and IP address of the new Primary. For instructions, see "Reconfiguring Quick Admin" on page 51.
3. If the Authentication Manager is specified as a Local Realm Authentication Manager or a Remote Realm Authentication Manager for cross-realm authentication, edit the realm record in the database, and in the Remote realm database to reflect the new name or IP address. For more information, see the Help topic "Edit Realm."
4. If the failed Primary was specified as a RADIUS server, you can either install the RADIUS server on the new Primary, another Replica, or a separate host machine. So as not to impact the administrative capability of the new Primary, RSA Security recommends that you enable RADIUS on another Replica. Be sure to
   - Add the Authentication Manager you choose to use as the RADIUS server to the database as an Agent Host. For more information, see "Adding Servers as Agent Hosts to the Primary Database" in the *Windows Installation Guide*.
   - If you opt to use the new Primary as the RADIUS server, update the RADIUS Server configuration settings so that they are identical to those that were on the old Primary.
   - Configure all RADIUS clients to use the appropriate name and IP address of the designated RSA RADIUS server. See the NAS device manual for specific configuration instructions.
5. If the Authentication Manager is specified as an Acting Server for legacy Agent Hosts, generate new **sdconf.rec** files for all legacy Agent Hosts that use this Server as an Acting Master or Acting Slave, and distribute the **sdconf.rec** file to the Agent Hosts. For more information, see the Help topic "Assign Acting Servers."
6. If the Authentication Manager was previously set up with LDAP synchronization jobs that use SSL to connect to the LDAP server, make sure that the new Primary has the required **cert7.db** file in the ***ACEDATA*/ldapjobs/sslcerts** directory. Otherwise, when LDAP synchronization runs, you will see the error:

   ```
   LDAP connection error - Failed to initialize LDAP session
   ```

   For information about setting up the **cert7.db** file, see "Using SSL" on page 114.
7. If the Authentication Manager is specified in any **sdopts.rec** files for version 5.0 Agent Hosts, edit the **sdopts.rec** file on the Agent Host to reflect the new name or IP address of the Authentication Manager.

Maintaining Customer-Defined Data (Extension Records)

The RSA Authentication Manager extension records enable you to define and manage database information that is useful to your organization although it is not required to run RSA Authentication Manager programs. This customer-defined information is called **extension data**.

The RSA Authentication Manager Database Administration application, which you run on your Remote Administration machine, provides menu options that you can use to access and process extension records.

The following table shows each type of extension data you can manage, the database table where it is stored, the menu you use to manage it, and a place to find further information.

Extension Data	Database Table	Menu	See Page
RSA Authentication Manager system-related	CustSystemExtension	System	215
Agent Host-related	CustClientExtension	Agent Host	57
Group-related	CustGroupExtension	Group	122
Log entry-related	CustLogExtension	Log	152
Site-related	CustSiteExtension	Site	135
Token-related	CustTokenExtension	Token	120
User-related	CustUserExtension	User	See the Help

To create reports based on customer-defined data, click **Extension Data** on the Report menu.

Note: For additional information about extension fields and about creating custom administration programs, see the *Administration Toolkit Reference Guide* (**authmgr_admin_toolkit.pdf** in the ***ACEDOC*** directory).

Managing Log Extension Data

This section explains how to create, modify, and delete log-related extension data. You can find information on managing other kinds of extension data through the table in the preceding section, "Maintaining Customer-Defined Data (Extension Records)."

You can add information to existing log entries in log entry extension fields. This information can then be used to select the log entries for a report.

To edit log extension data:

1. Start the Database Administration application on your Remote Administration machine.
2. Click **Log** > **Edit Log Extension Data**.
3. Select the type of log message to which the extension data is related: Activity, Exception, or Incident.

   The Log Entry Selection Criteria dialog box opens.
4. Enter specifications in one or more fields. For an explanation of the fields, see "Selection Criteria for Report Content" on page 164.

   To reset all selection criteria to the default values, click **Clear**.
5. After choosing the selection criteria, click **OK**.

   The Select Log Entry dialog box opens and displays only log records that meet all the specifications you entered.

   For each entry, the dialog box shows the time (Coordinated Universal Time and local time), the user for whom the activity was recorded, and the log message. The selection values remain in effect until you or another administrator changes them or until you end the current administration session.
6. Select the log entry to which the extension data is related, and click **Edit Log Extension data.**

   The Edit Log Extension Data dialog box opens and displays the log entry and the records defined for this entry. Each record consists of a secondary key (up to 48 characters) and data (up to 80 characters).
7. You can add, modify, or delete these records. You can create more than one record with the same key, but you cannot create duplicate records (records having the same key *and* the same data values) in one extension database table.

   - To change an existing record, select the record, modify the information displayed in the **Key** or **Data** fields, and click **Save**. (The **Save** button is unavailable until you make an entry in one of these fields.)

     To clear the fields without changing the record, click **Clear**.
   - To create a new record, click **Clear** if necessary to clear the **Key** and **Data** fields, enter the information for the new record, and click **Save**.
   - To delete a record, select the record, and click **Delete**. Click **OK** to confirm.
8. Click **Exit** to close the Edit Log Extension Data dialog box.

Running External 4GL Procedures

If you are comfortable programming in 4GL, you can run custom 4GL procedures to process RSA Authentication Manager data directly from the Database Administration application. To run a procedure that updates RSA Authentication Manager data, you must be a realm administrator or be assigned the **Run Custom 4GL** task.

CAUTION: A 4GL procedure can overwrite or delete valid data, such as log records or extension data, and can even corrupt your database. RSA Security ***strongly advises*** that you use the Administration Toolkit to create custom applications to work with your RSA Authentication Manager database. For information, see the *Administration Toolkit Reference Guide* (**authmgr_admin_toolkit.pdf** in the ***ACEDOC*** directory).

There are a number of Authentication Manager database fields that cannot be modified by custom administration programs. For information about these fields and for additional information about creating custom administration programs, see the *Administration Toolkit Reference Guide* (**authmgr_admin_toolkit.pdf** in the ***ACEDOC*** directory).

To run a 4GL procedure from the Database Administration application:

1. On the Administration menu, select **File** and click **Run Custom 4GL**.

   The Run External Procedure dialog box opens.

2. In the **Procedure Name** field, enter the filename of the procedure to run, or click **Browse** and select a filename from a list.

3. Use the **Automatically Connect to RSA Database** checkbox to indicate whether the specified procedure should be run against your RSA Authentication Manager database.

   This checkbox is provided for convenience. If you select it, you do not have to include lines of code in the 4GL procedure to identify your administrator privileges or target the RSA Authentication Manager database. The Database Administration application does this work for you.

   If you are running a procedure that accesses a database other than the RSA Authentication Manager database, do not select this box. Instead, include code for connecting to that database in the 4GL procedure.

4. You can run a procedure against all database records (with the exception of those that are marked by an asterisk in the database description in the *Administration Toolkit Reference Guide*), or you can use the **Object Type** field to limit the procedure to records of one specific kind (user records, token records, and so on).

   To run a procedure against all kinds of records, use the default object type (**None**). To run the procedure against records of a specific kind, highlight one type of data (**User**, **Token**, **Group**, **Agent Host**, **Site**, or **Realm**) under **Object Type**. Then select a specific record from the standard selection dialog box that opens and click **OK**.

The **Argument List** displays certain fields from the record you have chosen. These are the fields whose values the procedure can use. The Database Administration application extracts the value of each field and concatenates these values (in the order displayed) into a single string, separating them with pound signs (#). Your application can be written to parse the string in order to process records by field values.

The following table shows the fields from the record of each object type that the Database Administration application extracts and concatenates when you select it in the **Object Type** field.

Object Type	Contents of Argument List
User	First name, last name, default login, default shell
Token	Token serial number, last login date, last login time
Group	Site name, group name
Agent Host	Agent Host name, network address, protocol
Site	Site name
Realm	Primary name, Primary address, Replica name, Replica address

5. Click **OK**.

8 Maintaining the Log Database

This chapter describes log database maintenance tools and procedures.

The instructions in this chapter apply only to the *log database*, which contains the RSA Authentication Manager audit trail. They do not apply to the Authentication Manager *database* in which user, token, group, Agent Host, and other records are stored.

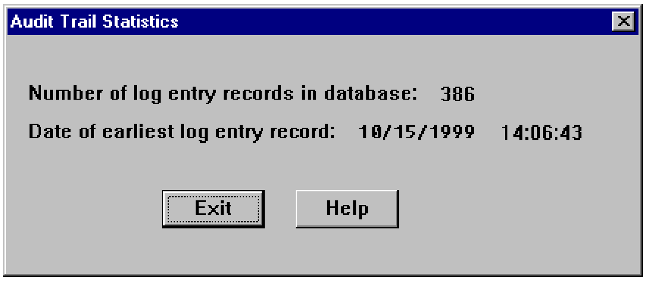
When activity on a Replica Authentication Manager generates a log message, the message is sent to the Primary Authentication Manager. The Primary gathers the log messages it receives from all of the Replicas into a consolidated log database.

The Log Menu

In the Database Administration application, the Log menu provides commands to maintain and control the RSA Authentication Manager log database. Five of the commands, **Log Statistics**, **Delete by Percentage, Delete Before a Date**, **Automate Log Maintenance**, and **Log Filtering** are associated with the audit trail and are discussed in this section. For information about the other commands in the Log menu, see the Help.

Viewing Log Database Statistics

To view the number of entries currently in the log record database, on the Log menu, click **Log Statistics**. The Audit Trail Statistics dialog box opens.



Number of log entry records in database: 386

Date of earliest log entry record: 10/15/1999 14:06:43

This dialog box also displays the time stamp for the oldest log record (in local time, based on a 24-hour clock). This information can be useful when you want to base log record deletions on a date. For more information, see the following section, "Deleting Log Records."

Deleting Log Records

The log database grows continually until database records are deleted or until the Authentication Manager runs out of disk space. It is important never to let the log record file grow too large. When the log database exhausts the available disk space, users are denied access because the Authentication Manager does not authenticate a user unless it can log the event.

You can purge old log records by deleting a certain percentage of the log records in the database or by deleting all the log records created before a certain date. You can also set the Authentication Manager to delete records according to a schedule. See "Scheduling Automated Log Database Maintenance" on page 157.

When you delete log records, disk space is made available for new log records. This disk space is ***not*** freed for other uses unless you run the database compression utility. Therefore, it is a good practice to compress the database after deleting a large number of log records.

To delete log records by percentage:

1. From the Log menu, select **Delete by Percentage**.

   You are prompted for a percentage of the total number of log entries.

2. To delete all records in the database, enter **100**, and click **OK**.

   To delete only some of the records, enter a percentage of the total number of log records currently in the database. The total is displayed by this dialog box along with the date and local time of the oldest log record.

3. Click **OK**.

   If you entered a number between 1 and 100, inclusive, a confirmation box opens, showing you the number of log records selected for deletion. The selected records are the oldest in the database.

4. To delete the selected log records, click **OK**.

When the delete operation is complete, the total number of log records in the database is reduced, and the dialog boxes are closed.

To delete log records by date and time:

1. From the Log menu, select **Delete Before a Date**.

   The Audit Trail Delete Before a Date dialog box opens.

   The dialog box displays the date and local time of the oldest log record and the total number of log records currently in the database.

2. Enter a date that falls within the time period covered by the database in the month, day, year format (***mm/dd/yyyy***).

   You can also include a particular time of day (in local time, not in Coordinated Universal Time). If you do not specify a time, the system assumes 00:00:00 (midnight) local time and deletes only records logged before the date you specified.

For example, if you enter **02/02/2001**, the latest record that can be deleted is time-stamped 02/01/2001 23:59:59.

If you entered a valid date, a confirmation box opens, showing you the number of log records selected for deletion (that is, the number of log records in the database with a time stamp earlier than the date [and time] you entered).

3. To delete the log records, click **OK**.

When the delete operation is complete, the total number of log records in the database is reduced and the dialog boxes are closed. For more information, see "Reclaiming Disk Space with Database Compression" on page 87 (for Windows) or "Reclaiming Disk Space with Database Compression" on page 138 (for UNIX).

Scheduling Automated Log Database Maintenance

You can use the Automated Log Maintenance feature to schedule regular backup and maintenance of the audit log database. The Authentication Manager deletes and archives audit log records according to the schedule and methods that you specify.

Deleting removes the log records from the audit log. Archiving saves the log records to a file in Comma-Separated Value (CSV) format, but does not delete any records. When log records have been deleted, you must use the compression utility described in "Reclaiming Disk Space with Database Compression" on page 87 (for Windows) or "Reclaiming Disk Space with Database Compression" on page 138 (for UNIX) if you want to recover the disk space for uses other than the log database.

Archive Files

Archive files are not like backup copies of the log database. You cannot restore archive files to the log database for use by the Authentication Manager as you can backup files. To create backup copies of the log database, see "Backing Up and Restoring RSA Authentication Manager Data" on page 88 (for Windows) or "Backing Up and Restoring RSA Authentication Manager Data" on page 139 (for UNIX).

Archive files are saved in Comma-Separated Value (CSV) format, in which columns are separated by commas and rows are separated by end-of-line characters. You can use CSV-formatted files with Microsoft Excel or other third-party software to view audit log records or to create reports.

Each time Automated Log Maintenance archives log records to a file, it saves a second file dedicated to customer-defined extension data. This file, which has the same name as the archive file with an *x* appended to it, is created whether or not any extension data has been defined.

For example, if you use the default archive filename **logcsv** to archive log records, the extension data is saved in a file named **logcsvx**. For more information on extension data, see "Maintaining Customer-Defined Data (Extension Records)" on page 100 (for Windows) or "Maintaining Customer-Defined Data (Extension Records)" on page 151 (for UNIX).

All versions of the archive file reside on the Authentication Manager in the ***ACEDATA*** directory. When the number of versions of the archive file equals the number entered in the **Cycle Through** field, Automated Log Maintenance overwrites the oldest version. To determine which version is the most recent, you must check the file dates.

For example, if you enter **3** in the **Cycle Through** field and use the default archive filename **logcsv**, the file **logcsv.1** is overwritten the fourth time Automated Log Maintenance is run.

To Begin: Click **Log** > **Automate Log Maintenance**. For instructions, click **Help**.

Log Filtering

Log filtering provides a way to select the log messages that go into the RSA Authentication Manager log database. By filtering out certain messages, you can slow the growth of the log database and increase the replication, authentication and administration performance of the RSA Authentication Manager. For example:

- You can increase authentication rates by filtering out the "PASSCODE Accepted" message that is logged to the database every time the Authentication Manager authenticates a user.
- For cross-realm authentications, you may want to log cross-realm messages (those messages that begin with XR) only on Authentication Managers that accept cross-realm authentication requests.

  For more information, see Chapter 4, "Realm Administration."

Once you configure the Primary to filter certain log messages, you can save the configuration settings to a file and import them to Replicas.

CAUTION: Filtered log messages cannot be recovered. Filter only those messages that you are certain you do not need to log.

To Begin: Click **Log** > **Log Filtering** > **Configure**. For instructions, click **Help**.

9 Reports

This chapter contains information about producing reports on RSA Authentication Manager activities and data. It also describes SQL-based custom query tools for retrieving data from the user and log databases. This chapter is organized as follows:

Audit Trail Reports. The RSA Authentication Manager logs a record for each login attempt and for actions taken through the Database Administration application. An administrator can run a variety of reports to view this audit trail. This section describes the Database Administration application audit trail reports and explains how to format and produce them.

Extension Data Reports. This section describes how to produce reports on user-defined information in the Authentication Manager extension records.

Log Monitoring and Reporting. This section describes the Database Administration application log monitor, which displays log entries as soon as they are written to the audit trail. It also discusses the format of the log archive file and options for log monitoring and reporting.

Report Creation Utility. Two sections describe a utility that enables you to create and run custom reports and to run additional ready-made reports. There are two versions of the report creation utility: one for Windows, and one for the UNIX platforms. Using the report creation utility requires no programming knowledge.

Creating and Running Custom SQL Queries. This section describes querying tools built into the Database Administration program. These tools enable the creation and management of SQL-based queries of the user and log databases to output and view data in a variety of industry-standard text formats.

Audit Trail Reports

Contents of a Log Record

This section describes the information contained in the fields of each log record. The columns of a log report correspond to these fields. Each event or action is logged in a record that is displayed on two or three lines.

The First Line of a Log Record

Date and Time. The date and time of the recorded event in Coordinated Universal Time.

Current User. The login of the person who performed the action. No user is listed for system events that occur automatically (for example, if a token was put in Next Tokencode mode after a series of failed login attempts). Because an authentication log record records an event that changes the user's record, the name of the person logging in appears in the **Affected User** field instead of the **Current User** field, which is blank.

Agent Host. The name of the Agent Host on which the event occurred. Even if the action took place on an Authentication Manager, an Agent Host name is listed because all Authentication Managers are defined as Agent Hosts.

(Group). If the action affected group information (for example, membership data), the group name appears in parentheses after the Agent Host name. A user's group name is not given in authentication log records.

Affected User. If a token was directly affected by an action, its serial number appears in the right-hand column. If the token is assigned, the user's login name may appear in addition to or instead of the serial number. Which identifier appears is based on a formatting specification. (For more information, see page 164.) In an authentication log record, because authentication changes the user's record, the person who logs in is listed as the Affected User instead of the Current User.

The Second Line of a Log Record

Date and Time. The date and time of the recorded event in local time.

Description of the Event or Action. For explanations of selected log descriptions, see Appendix C, "Troubleshooting."

(Site). If applicable, a site name appears in parentheses in the right-hand column. This is the site with which the current Agent Host is associated. Site information is not given in authentication log records.

Authentication Manager **Name or Realm Name.** This name appears in the right-hand column.

- For local authentication events, the Authentication Manager name is shown.
- For cross-realm authentication events, the name of the remote realm is shown.

The Third Line of a Log Record

Date and Time. The date and time of the recorded event in local time.

Affected User Name. This line appears only if you select the **Full User Names** checkbox in the Report Format dialog box. When this feature is enabled, the affected user's full first and last names (up to 48 characters) appear in the third line of each event entry.

Report Types

Each log record contains an internally stored severity code. **Activity**, **Exception**, and **Incident** reports are defined by which types of records they include. **Activity** reports include records of all severity levels. The content of **Exception** and **Incident** reports is more limited.

A fourth type of report is the **Usage Summary**, which gives counts of certain types of activities that have occurred on the system. A **Usage Summary** does not contain log messages.

Restrictions on All Reports

In addition to content restrictions based on report type, the following restriction applies to all reports: selection criteria that are set during the current Database Administration application session are applied to determine which records are included in a report. (For more information, see "Selection Criteria for Report Content" on page 164.)

Activity Reports

All types of log records are included in an **Activity** report. Log records are excluded from an **Activity** report only as described in the preceding section, "Restrictions on All Reports."

Exception Reports

Exceptions are events that are important to a security administrator. Exceptions are not necessarily security breaches, but they may indicate attempts to breach security. For example, errors that occur when a user requests authentication or an administrator attempts to edit data may indicate an intruder's attempt to guess a PIN or to modify the database using tools with which he or she is unfamiliar.

Incident Reports

Incidents are groups of related events that end in an important occurrence (for example, a series of events that triggers an evasion–of–attack action). Incidents are not necessarily security breaches, but they are events that could be of interest to a security administrator. Sequences of events that conclude in any of the following actions are included in **Incident** reports:

- New PIN Received
- PIN Created by User

- Next Tokencode On
- Token Disabled, Many Failures
- Token Disabled, Suspect Stolen

If a precursor event is outside the range of the report being run, the report will indicate **Preceding events not included**.

Usage Summaries

A Usage summary shows how many times certain activities were performed in the period covered by the report.

A Usage summary is divided into two sections: **General Activity**, which lists all login, token, infrastructure failure, and report record activity, and **Filtered Activity**, which lists login and token record activity for an entity (group, user, site, or realm) that you specify in the Log Entry Selection Criteria dialog box before you generate the Usage summary.

The following information appears in the Usage summary:

Denied accesses. The number of failed access attempts.

Allowed accesses. The number of successful access attempts.

Average accesses per day. The total number of successful access attempts recorded for the period of the report, divided by the total number of days in the period.

New tokens assigned. The number of times a token assignment operation was performed.

New PIN modes set. The number of times an administrator puts tokens into New PIN mode.

System time changes. The number of times one of the **Set server clock offset** buttons in the Edit System Parameters dialog box was used.

Report Records. How many times each type of report was generated.

Generating Reports

To generate an RSA Authentication Manager report:

1. Select **Report Format** on the Report menu.

   The Report Format dialog box opens.

   The report you are about to run will use the values that appear here. These formatting specifications are saved across Database Administration application sessions. To make modifications, see the following section, "Report Formatting."

   If you are using reports for the first time, consider setting the **Output to** value to **Screen**, so you can see what a report looks like.
2. Click **OK**.

3. From the Report menu, select the report by type (**Activity**, **Exception**, **Incident**, **Usage Summary**).

   The Selection Criteria box opens. The values are based on the last ones set during this Database Administration application session.

4. To accept the values and generate the report, click **OK**.

   If selection criteria have been set but you want to see a report for all users, all Agent Hosts, all servers, and so on, click **Clear**. All selection criteria are set to "*" so that all items will be included. Click **OK**.

   For more information about criteria, see "Selection Criteria for Report Content" on page 164.

   When the report is displayed, its first page shows what selection criteria are in effect. The following pages show the selected log records in chronological order from oldest to most recent.

   If the report is a log monitor report, select the **Hold** checkbox if you want to stop scrolling (for more information, see "Log Monitoring and Reporting" on page 169).

5. To close the report, click **Exit**.

Report Formatting

When you run a report, the values in the Report Format dialog box are applied. Unlike content selection criteria, changes in formatting variables are saved from one Database Administration application session to the next. If another administrator has made format changes since your last session, these changes are now the default. Before you run a report, always check the Report Format variables to see if they are set as you want them.

To change the Report Format variables:

1. From the Report menu, select **Report Format**.

   The Report Format dialog box opens.

2. Set the report format according to the following criteria:

   Turn header printing on or off. This value applies only if the report is being sent to a file. When the **Header** checkbox is selected, the following information appears at the top of each page:

   - Number of this page and total number of pages in the report
   - Report title
   - Time selection criteria used
   - Date and time when the report was generated

   Turn page breaks on or off. This value applies only if the report is being sent to a file. When the **Page break** checkbox is selected, a page break character is included after each page. If the **Page break** checkbox is cleared, the report is essentially one page long with a single header and no page breaks.

Specify the number of lines each page should include. This value applies only if the report is being sent to a file and page breaking is turned on. A page can be set to have as many as 98 lines before the page break. Enter an even number of lines per page. If you enter an odd number, it will be rounded to the previous even number.

Specify how user names are shown. If the **Full User names** checkbox is selected, each affected user's full first and last names (up to 48 characters) appear in the third line of each recorded event. If the **Full User names** box is not selected, the user's full name appears in the first line of the recorded event and no third line appears.

Specify how affected tokens/users are identified. When a token is identified in the Affected User column of a report, its serial number, its assigned user's name, or both, can be listed. Select the appropriate Affected token identifier button: **Serial No./Name** for both to display, **Serial No. only**, or **Name only**.

Customize report titles. The default report titles indicate the report type. You can enter different text in the title fields of the Report Format dialog box. Each title can contain up to 34 characters, and all characters are allowed.

Selection Criteria for Report Content

To limit what records are included in a report, from the Report menu, select the **Selection Criteria** option.

The Report Selection Criteria dialog box opens.

Specify the report range in the **Specify report by** area.

- To limit the report to a specific number of pages, click **Pages** and specify the number of pages in the **Last pages** box. The page size is calculated depending on the number of lines per page you specify in the Report Format dialog box. For more information, see "Report Formatting" on page 163.

  Note: The number of pages is calculated with the assumption that the report will appear on the screen. This number may differ if you output the report to a file.

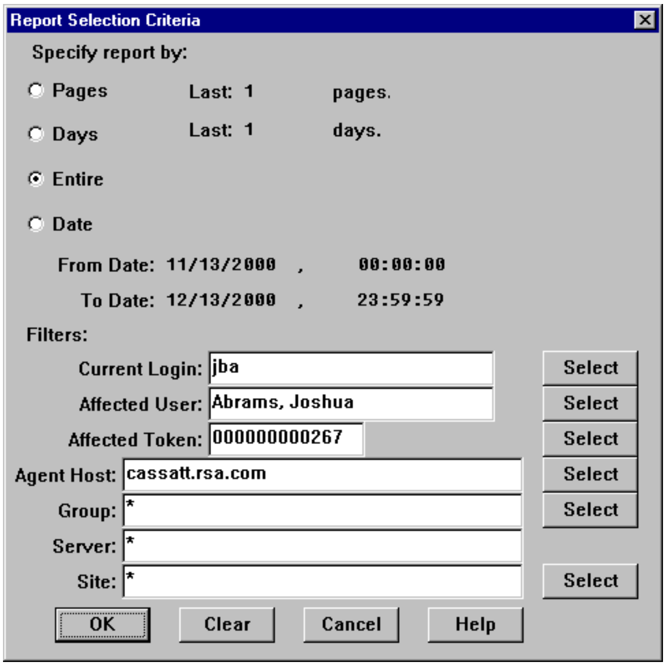
- To limit the report to a specific number of days, click **Days** and enter the number of days in the **Last days** box.
- To see all records from the start of the log database to the present, click **Entire**.
- To limit the report to a specific range of dates, click **Date**. The default date range for the report is 30 days prior to the current day. To enter a different range, enter a time period based on a 24-hour clock in local time (not Coordinated Universal Time) in the **From Date** and **To Date** boxes. Use the ***mm/dd/yyyy*** format (***mm*** for the month, ***dd*** for the date, and ***yyyy*** for the year). In the **From Date** fields, enter the date and time of the oldest record you want included. In the **To Date** fields, enter the date and time of the most recent record you want included. To see the latest records stored in the database, leave this field blank.

Enter specifications in one or more of the selection fields. An asterisk (*) alone in a selection field indicates that no restrictions based on this variable apply.

Note: When generating an activity, exception, incident, or usage summary report, you can improve query response time by entering criteria in only ***one*** field. You can enter an exact match in a field or use a wildcard. For example, in the **Affected User** field, if you entered (**Joshua Abr***), you would generate a report for all users in the database whose first name is **Joshua** and whose last name begins with the letters **Abr**. If you entered an exact match (**Joshua Abrams**), you would generate a report for all users in the Authentication Manager database named **Joshua Abrams**.

The selection criteria shown in the screen illustration will produce a report of activities that share *all* of the following characteristics:

- Were performed by a user whose login is "jba"
- Changed the record of a user named "Abrams, Joshua"
- Changed the record of a token with serial number 000000000267
- Were performed on an Agent Host named "cassatt"



Report Selection Criteria

Specify report by:

○ Pages Last: 1 pages.

○ Days Last: 1 days.

● Entire

○ Date

From Date: 11/13/2000 , 00:00:00

To Date: 12/13/2000 , 23:59:59

Filters:

Current Login: jba

Affected User: Abrams, Joshua

Affected Token: 000000000267

Agent Host: cassatt.rsa.com

Group: *

Server: *

Site: *

No log records are excluded on the basis of server or site information. Details about each selection field are presented later in this section.

You can also generate a report restricted to a particular time period, not just the most recent events. Select the **Date** button. Enter a time period based on a 24-hour clock in local time (not Coordinated Universal Time). Use the ***mm/dd/yyyy*** format (***mm*** for the month, ***dd*** for the date, and ***yyyy*** for the year.) In the **From Date** fields, enter the date and time of the oldest record you want included. To see all records from the start of the log database, leave this field blank. In the **To Date** fields, enter the date and time of the most recent record you want included. To see the latest records stored in the database, leave this field blank.

You can select log records for inclusion in a report using a variety of criteria. There are **Select** buttons next to each box for this. If you type in the fields instead of using the **Select** buttons, enter the specifications carefully. The system does not verify that the names or serial numbers you enter are valid identifiers. For example, if you enter **Market** in the **Group** field and the group name is **Marketing**, the system will find no records to report, but you will not know this until you run a report.

Selection Criterion	Activities Included
Current Login	Activity performed by the specified user. Enter the user's login, not the user's name.
Affected User	Records for operations that affected a specific user. Enter the user's name, not the user's login.
Affected Token	Records for operations that affected a specific token. Specify the token serial number.
Agent Host	Activity that relates to the named Agent Host. Login attempts on the named Agent Host and changes to the Agent Host information stored in the Authentication Manager's **sdserv** database are reported.
Group	Administrative actions that affect the specified group (for example, adding or deleting group members). A report selected by group will not include the login activity of the group's members.
Authentication Manager	Activity on the specified Primary or Replica or in a specified realm.
Site	All administrative actions that affect the specified site (for example, creating a group or Agent Host within the site). A report selected by site will not include any login activity.

To reset all selection criteria to the default values, click **Clear**.

After choosing the selection criteria, click **OK** to close the dialog box.

The next report you run will contain only records that meet all the specifications you entered. The selection values will remain in effect until you or another administrator changes them or until you end the current Database Administration application session.

Sending a Report to a File

You can save all types of audit trail reports, including the log monitor, as ASCII text files.

To save a report as a file:

1. From the Report menu, select **Report Format**.

   The Report Format dialog box opens.
2. Select **File** for the **Output**.
3. If you want a particular filename to be the default filename in step 6, enter this name in the **Report Filename** field.

   Be sure to comply with operating system character restrictions.
4. Set other formatting specifications.

   For more information, see "Report Formatting" on page 163.
5. Click **OK**.
6. From the Report menu, select the report that you want generated.

   The Report Filename dialog box opens, prompting you for the name of the report file. If you entered a filename in the Report Format dialog box in step 3, this name is displayed in the box. You can specify a different path and filename. To select an existing file or view the available paths, click the **Browse** button.
7. When you have specified the path and filename, click **OK** to close the Report Filename dialog box and generate the report.

When you save a report to a file, a message box confirms that the report was saved under the filename you specified.

Store this report file in a secure location. Reports contain a good deal of information about your system, including server names, Agent Host names, and user names. Protect this information from unauthorized users.

Extension Data Reports

To generate reports that list extension records:

1. From the Report menu, select **Extension Data**.

   The Report Selection Criteria dialog box opens.
2. Specify the report format:

   Output to. Click **Screen** to display the report on your monitor or **File** to save the report to an ASCII text file.

   Need. These values apply only if you are sending the report to a file. Click **Header** to include the report title in the file. Click **Page break** to include a page break character after each page. (The next item, **Lines per page**, sets the page length.) If **Page break** is cleared, the report is essentially one page long, with a single header and no page breaks.

Lines per page. This value applies only if you are sending the report to a file and **Page break** is selected. You can set a page to have from 9 to 60 lines before a page break.

Report Title. The default report title indicates the report type. You can change the default title in the Report Title field. The title can have up to 60 characters, and all characters are allowed.

3. Specify the report content.

   To specify the type of extension data to be reported, click a category in the **Extension Type** list.

4. Enter specifications in one or more of the selection fields:

   - For Agent Host, group, site, or user extension data, specify the Agent Host, group, site, or user name, respectively, to which the extension data is related. For token extension data, specify the token serial number. For log extension data, specify the message.
   - To report extension records that include a specific key value, enter the value in the **Key** field.
   - To report extension records that include a specific data value, enter the value in the **Data** field.

   There are **Select** buttons next to each box for specifications. If you type specifications in the fields instead of using the **Select** buttons, enter your data carefully. The system does not verify that the names or serial numbers you enter are valid identifiers.

   An asterisk (*) alone in a selection field indicates that no records will be eliminated from the report based on this variable. All values encountered in the field are accepted.

5. To accept the settings displayed and generate the report, click **OK**.

Extension Data Report Content

Each report includes the following information:

- The report selection criteria
- The date and time the report was created
- Depending on the type of extension data being reported, the following information:
  - **Agent Host:** the Agent Host name and network address
  - **Group:** the group name and site name
  - **Log message:** the log message and local time message was created
  - **Site:** the site name
  - **Token:** the token serial number and user name
  - **User:** the first name, last name, and default login of the user
- All records that match the selection criteria.

Log Monitoring and Reporting

This section describes how you can monitor activity on the RSA Authentication Manager system. It also discusses the log file to which system activity is archived on a periodic basis.

By starting a log monitor session from the Database Administration application, you can monitor access attempts, database administration and other activity in real time as the records are written to the audit trail.

RSA Authentication Manager also provides the ability to send log events to the system log, which you can monitor with third-party tools that alert you to system trouble.

For log maintenance, the Authentication Manager can be set up to archive system activity to a log file on a regular basis. By accessing this text file, you can view a historical record of RSA Authentication Manager activity. Because this log file is written as CSV (comma-separated values), you can also import it to third-party tools to view the data and create custom reports.

Log Monitor Options

From the Report menu, select **Log Monitor** to view the submenu of monitor types (**Activity**, **Exception**, or **Incident**). Use this submenu to initiate a session that monitors all activity or just noteworthy activity (exceptions or incidents). See "Report Types" on page 161.

Note: To use the log monitor, you must be connected to the database on the Primary.

When you select a log monitor type, the Report Selection Criteria dialog box opens. Set selection criteria to monitor the activity of only one user or on certain Agent Hosts, and then click **OK**. A live report window opens to report on activity as it happens. (For more information, see "Selection Criteria for Report Content" on page 164.)

When the report window opens, continuous real-time monitoring begins. To temporarily stop log monitoring without closing the report window, select the **Hold** checkbox. When monitoring is on hold, the navigation buttons (**Previous**, **Next**, and **Go To**) are enabled. Use these buttons to page through the report.

The log monitor can display a maximum of 100 pages per session.

To end the log monitoring session, click **Exit**. The monitor window closes, and you are returned to the Database Administration application main menu.

Using the sdlogmon Command

On a UNIX server, you can also initiate log monitoring from outside the Database Administration application. At the command line prompt of the Primary, enter this command:

```
sdlogmon [-type] [-t] [-f filename]
```

Argument	Description
-type	Use this argument to specify the type of monitoring you want to run: **-a** for all activity (the default if this argument is omitted), **-e** for exceptions only, **-i** for incidents only.
-t	Use the "tail" argument to see new activity displayed at the end of a long file. You can scroll upward to see previous activity. If you omit this argument, the log monitor runs in a character-mode version of the live report window described on page 169. This argument is appropriate only when the output is sent to the screen (that is, when the **-f** argument is not used).
-f *filename*	Use this argument to indicate that the output should be sent to a file instead of the screen. Specify the filename immediately after **-f**. The **-t** argument should not be used when the **-f** argument is used.

End the log monitoring session by pressing CTRL+C. You return to the command line.

Monitoring Authentication Manager Events in the System Log

Another way to track RSA Authentication Manager activity is to monitor the events that it sends to the Event Log (Windows) or System Log (UNIX) of the host machines that are part of your system.

Many third-party SNMP (Simple Network Management Protocol) tools for network management can be set up to monitor system logs of various computers. These same tools can be configured to send e-mail or pager alerts to the appropriate person when critical events occur (such as the RSA Authentication Manager failing).

In RSA Authentication Manager operation, there are two general types of events:

- Events sent to the audit log database
- Other events related to RSA Authentication Manager processes, which, with a few exceptions described below, are *automatically* logged to the system log of the host machine (generally a Primary or Replica server)

The Database Administration application provides tools to enable you to specify the audit log database messages that are sent to the system log. For information, see "Sending Audit Log Messages to the Event or System Log" on page 287.

To avoid duplication, you can filter those messages from the log database and use the system log as your primary logging mechanism. Filtering prevents the specified types of messages from appearing in the log database. For information, see "Log Filtering" on page 158.

In RSA Authentication Manager, you can specify filtering or system logging of events from ***all*** processes. Because RSA Authentication Manager has a multiple-server architecture, you need to set up filtering and system logging on the Primary and all Replicas in your installation.

Note: For a description of all RSA Authentication Manager processes, see Appendix B, "Services and Processes." For a list and description of all important system log messages related to RSA Authentication Manager, see "Messages" in Appendix C, "Troubleshooting."

There are two categories of system logging: local and remote. Local system logging is done on the host machine running the process, and is performed by all processes connected to the RSA Authentication Manager database except Remote Administration, RADIUS (local or remote) and Job Executor (JSED) processes. System logging of these exceptions, which RSA Authentication Manager performs remotely, is described in the following subsections.

System Logging for Remote Administration

When you use the **Database Administration - Remote Mode** command, system logging for the remote session is performed on the remote host computer, not on the computer from which you launched Remote Administration.

The host computer can be any Primary or Replica in a realm. System logging is handled by the **sdadmind** process of the Authentication Manager to which the Remote Administration process *originally* connects. This means that if you switch to a different Authentication Manager in the realm, system logging continues to be handled on the first Authentication Manager (the one on which you initially authenticated).

System Logging for the RADIUS Server

For information about logging RADIUS server activity, see the *RSA RADIUS Server 6.1 Administrator's Guide*.

System Logging for the Job Executor

The Job Executor (JSED) process handles LDAP synchronization as well as periodic license validation.

For logging, it uses the same model as a local RADIUS server. It sends two events to the database audit log: **Job Executor server started** and **Job Executor server stopped**. You can filter these events from the audit log, but cannot specify them to be sent to the system log.

However, JSED automatically sends separate messages to the system log when the server is started or stopped.

Using Log Archive Files

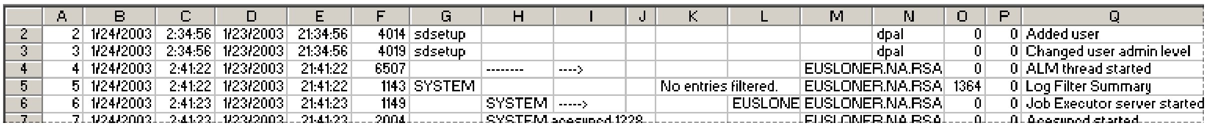
With automatic log maintenance enabled, the RSA Authentication Manager audit trail is regularly offloaded to one or more log archive files. (For more information, see "Scheduling Automated Log Database Maintenance" on page 157.)

You can open and view a log archive file anytime. For example, for security reasons or statistical purposes, you might want to research the history of certain types of transactions within your Authentication Manager installation.

The default name of a log archive file is **logcsv**. Log data in the archive file is formatted as CSV (comma-separated values), which can be imported to Microsoft Excel or other third-party applications.

After you import the log archive data to your application, you can filter, format, organize, and output the data in a variety of custom reports, depending on the application that you are using.

This section describes the format of the **logcsv** file. The **logcsv** file is made up of multiple records each containing 17 fields separated by commas. Each record ends with a line feed. Imported into a spreadsheet, each record would be formatted as a row with 17 columns (A–Q):



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
2	2	1/24/2003	2:34:56	1/23/2003	21:34:56	4014	sdsetup							dpal	0	0	Added user
3	3	1/24/2003	2:34:56	1/23/2003	21:34:56	4019	sdsetup							dpal	0	0	Changed user admin level
4	4	1/24/2003	2:41:22	1/23/2003	21:41:22	6507		--------	---->				EUSLONER.NA.RSA		0	0	ALM thread started
5	5	1/24/2003	2:41:22	1/23/2003	21:41:22	1143	SYSTEM				No entries filtered.		EUSLONER.NA.RSA		1364	0	Log Filter Summary
6	6	1/24/2003	2:41:23	1/23/2003	21:41:23	1149		SYSTEM	----->			EUSLONE	EUSLONER.NA.RSA		0	0	Job Executor server started
7	7	1/24/2003	2:41:23	1/23/2003	21:41:23	2004		SYSTEM	acesuned 1228				EUSLONER.NA.RSA		0	0	Acesuned started

The following table describes the contents of each column.

Column	Description
A	Log entry ID (unique identifier).
B	GMT Date.
C	GMT Time.
D	Local Date.
E	Local Time.
F	Message number.
G	Name of the administrator who performed the operation. Alternatively, this field can contain the name of a service or utility that performed the operation.
H	Default login of the person who performed the operation. Alternatively, this field can contain a string that identifies a service or utility that performed the operation.
I	Token Serial Number. (If the operation does not involve token activity, the field is left empty or filled with a placeholder.)
J	Site name involved in the administrative operation. This field is left empty during authentication activity.
K	Group name involved in the administrative operation. This field is left empty during authentication activity.
L	Agent Host name (or in some cases the Agent Host IP address) involved in the operation. This field is populated during authentication activity.
M	Authentication Manager name that performed the operation or to which the operation was related.
N	User name affected by the operation.
O	Process ID of the application that logged the event (in most cases not populated).
P	Error level of the message.
Q	Message text.

RSA Authentication Manager Report Creation Utility (Windows)

The RSA Authentication Manager software includes a Report Creation Utility, which enables you to create and run audit trail reports against the **sdlog** database and token statistic reports against the **sdserv** database. The utility also includes a way to select a user and display on your screen information from the corresponding user record.

Installing the Report Creation Utility

When you install the RSA Authentication Manager, the Report Creation Utility software is copied to the ***ACEUTILS*** directory. No separate installation procedure is required.

Starting and Stopping the Report Creation Utility

To run the Report Creation Utility:

1. At a command prompt, start the report database server by typing:

   ```
   ACEUTILS\rptconnect start
   ```

2. Run the Report Creation Utility by typing:

   ```
   ACEUTILS\sdreport
   ```

   Note: The Report Creation Utility can also be run in batch mode. In this mode, the RSA Authentication Manager Reports dialog box does not open. To connect to the database in batch mode, enter **ACEUTILS\rptconnect start batch**.

   The RSA Authentication Manager Reports dialog box opens.

To stop the Report Creation Utility:

1. From the File menu, select **Exit** in the RSA Authentication Manager Reports dialog box.

2. At a command prompt, stop the report database server:

   ```
   ACEUTILS\rptconnect stop
   ```

   Important: If you do not stop the Report Creation Utility in this manner, the utility may become locked with a lock file, ***ACEUTILS*\sdrpt.lk**. Remove this file, and try again.

Selecting Reports to Run

In the RSA Authentication Manager Reports dialog box, you can select reports to run from two lists: **Standard Reports** and **Custom Reports**.

- **Standard Reports** are predefined reports that cannot be modified or deleted. The set of standard reports includes four histogram and four token list reports.
- **Custom Reports** are reports you can create, modify, and delete. Until you or another administrator creates one or more custom reports, the **Custom Reports** list is empty.

Using the Run List

The Report Creation Utility is designed so that reports can be run only from the **Run List**. In order to run a report, you must first move it from the **Standard List** or **Custom List** to the **Run List**.

- To move reports to the **Run List**, highlight the reports in the **Standard List** or **Custom List** and click **Add**. You can highlight multiple reports by clicking each selection while you press CTRL.
- To remove a report from the **Run List**, highlight it and click **Remove**. When you remove reports from the **Run List**, each report returns to the list from which it was taken.

You can use the **Run List** for the reports you select to run during a single session, or you can save the list contents so that the same set of files are ready to be run whenever you start the Report Creation Utility. If you never save the list, it is always empty when the utility opens. Otherwise, the list contains the same files that it contained when last saved.

Although the utility comes with eight standard reports and no custom reports, you may over time create large numbers of custom reports—some that you run regularly and others that you need only on rare occasions. By saving the **Run List**, you can keep the reports that you run most often in a place where they are easy to find. Rarely needed reports are not lost—they remain on the **Standard List** and **Custom List**.

To save the **Run List**, click **File** > **Save Run List**. When you want to change the contents of your standard run list, create a new version and save it in place of the old one.

Saving the Report Run List

To save the list of reports that you want to run:

On the File menu, click **Save Run List** of the RSA Authentication Manager Reports dialog box.

The list of reports in the **Run List** is saved.

To run reports from the Run List:

1. Enter the **From** and **To** log dates to define the date range for the report or reports you are going to run.

   If you do not specify a date range, all available relevant information is included without regard to the log record dates.
2. Highlight the report or reports you want to run.
3. Click **Run Report(s)**.

Standard Report Types

Histogram Reports

A **Histogram** report is a series of numbers that represents an hourly count of activity. This count is useful for plotting peak activity or load by time. The output file (with extension .xls) can be imported into a spreadsheet and graphed.

- **Histogram – Accepted** shows the number of successful authentications during each hour of the specified period.
- **Histogram – Attempts** shows the number of access attempts, both successful and unsuccessful, during each hour of the specified period.
- **Histogram – Bad PASSCODE** shows the number of login attempts that failed because of an invalid passcode during each hour of the specified period.
- **Histogram – Bad PIN** shows the number of login attempts that failed because a valid tokencode was entered with an incorrect PIN during each hour of the specified period. (This count applies to RSA SecurID standard cards and key fobs only.)

Token List Reports

The following token lists can help you troubleshoot users' authentication problems. Use the Token Statistics Report Builder described in "Creating Token Statistics Reports" on page 180 to create similar listings specific to your needs.

- **Token – Disabled** lists the token serial number and the assigned user's name and login for each disabled token.
- **Token – New PIN** lists the token serial number and the assigned user's name and login mode for each token in New PIN mode.

- **Token – Wait 1 Tokencode** lists the tokens that are in Next Tokencode mode with one good tokencode already entered. Each token serial number and the assigned user’s name and login are identified.
- **Token – Wait 2 Tokencodes** lists the tokens for which the system needs two good tokencodes before granting access to their users. Each token is identified by serial number and assigned user’s name and login.

Report Output Files

When you run a report from the Reports dialog box, the output is stored in two text files. One of the files has a .txt extension and is in an easy-to-read format. The other file has an .xls extension and is in a format compatible with spreadsheets.

For standard reports, the full filename is based on the report content and format. For example, complete filenames for **Histogram – Attempts** output are **attempts.txt** and **attempts.xls**. Each standard report type has a unique, predefined name. For a custom report, you specify the filename and the Report Creation Utility adds the extension. You must ensure that the filename you supply is not used for any other report regardless of type.

Report output files are stored in a subdirectory of the ***ACEUTILS*****\output** directory. The subdirectory is created automatically if it does not exist, and it is named for the date on which the report was run (in ***yyyymmdd*** format). If the same report type is run more than once during a single day, the latest output overwrites the previous output.

Example: On March 1, 2001, you highlight **Histogram – Accepted** on the **Run List** and click **Run Report(s)**. Two files are created, **accepted.txt** and **accepted.xls**, both stored in ***ACEUTILS*****\output\20010301**.

Creating and Managing Custom Reports

The Report Creation Utility provides three custom report definition dialog boxes. You can use these dialog boxes not only to create new reports but also to edit or delete existing reports.

To create, edit, or delete custom reports:

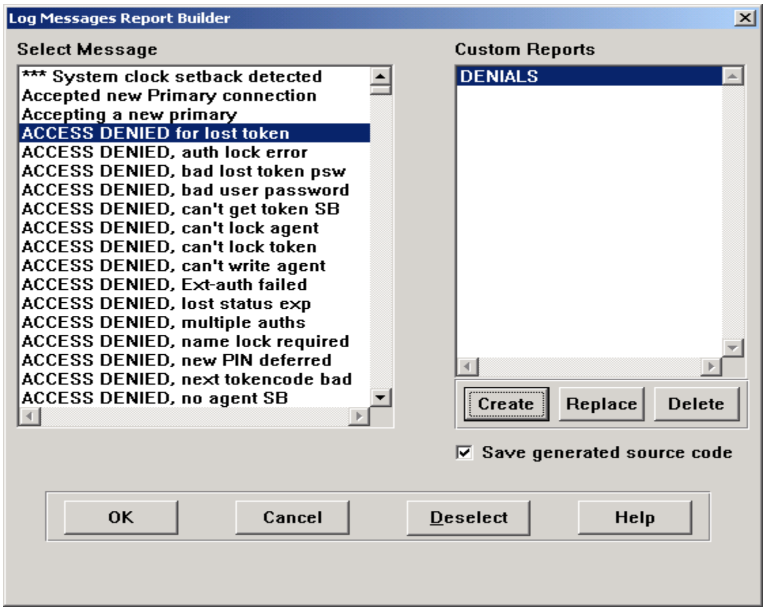
1. In the RSA Authentication Manager Reports dialog box, click **Create Report**.

   The Select Report Type dialog box opens.

2. Select one of three types: **Log Entry**, **Histogram**, or **Token Statistics**. Depending on your selection, one of the following dialog boxes opens:

   - Log Messages Report Builder
   - Log Messages Histogram Builder
   - Token Statistics Report Builder

One feature common to all of these dialog boxes is the **Custom Reports** list, which lists by name any custom reports of the type you selected that are currently defined. For example, see the right side of the Log Messages Report Builder dialog box.



```
*** System clock setback detected
Accepted new Primary connection
Accepting a new primary
ACCESS DENIED for lost token
ACCESS DENIED, auth lock error
ACCESS DENIED, bad lost token psw
ACCESS DENIED, bad user password
ACCESS DENIED, can't get token SB
ACCESS DENIED, can't lock agent
ACCESS DENIED, can't lock token
ACCESS DENIED, can't write agent
ACCESS DENIED, Ext-auth failed
ACCESS DENIED, lost status exp
ACCESS DENIED, multiple auths
ACCESS DENIED, name lock required
ACCESS DENIED, new PIN deferred
ACCESS DENIED, next tokencode bad
ACCESS DENIED, no agent SB
```

Custom Reports: DENIALS

☑ Save generated source code

3. One way to create a new report is to select an existing report and change the definition. When you select any report, the settings that define it are displayed on the screen. (In the Log Messages Report Builder dialog box, for example, the log messages specified as the report contents are highlighted in the **Select Message** list.) You can change these settings and click **Replace** to save the new report definition in place of the old one.

4. To create a new report without using an existing one, click **Create**. New reports are added to the **Custom Reports** list. (Full procedures for creating the three types of report are provided in the next three sections.)

5. To delete a report from the **Custom Reports** list, select it and click **Delete**.

6. To save editable 4GL code for a report you create, select **Save generated source code**.

   When this box is not selected, only compiled 4GL code is generated. When this box is selected, readable and editable 4GL source code is generated in addition to the compiled code.

Creating Log Entry Reports

The Log Messages Report Builder dialog box enables you to create reports that include all log records of one or more event types by selecting the corresponding log messages from the **Select Message** box. For example, you could define a report showing every instance of the RSA Authentication Manager disabling a token. Another report might include all log records that represent changes to a user record or a token record.

Log reports include the detailed information available from the Authentication Manager audit trail. Entries show the time and date of the event, the current and affected users (as appropriate), and a one-line description of the event.

To define a custom log entry report:

1. In the RSA Authentication Manager Reports dialog box, click **Create Report** to open the Select Report Type dialog box.
2. Click **Log Entry** > **OK**.

   The Log Messages Report Builder dialog box opens.
3. Select one or more messages by highlighting them in the **Select Message** list. (If you change your mind about a message, put the cursor on it and click **Deselect**.)

   Each occurrence of an event indicated by one of the selected messages is reported (for the dates you specify) when this report is run.
4. Click **Create**.

   The Create a New Report dialog box opens and prompts you for a description and a filename for the new report.
5. Enter a short, descriptive name (up to 25 characters) by which users of the Report Generation Utility can identify the new report. This name will appear in the **Custom Reports** list or **Run List**.

   In addition to the descriptive name, enter a filename (up to eight characters) to be used for the report output files (and for the report source code file if you requested one).

   Note: Do not use a description or a filename that is already used for another report, even if the report type is different.
6. Click **OK**.

   The new report appears in the **Custom Reports** list in the Log Messages Report Builder dialog box.
7. Click **OK** in the Log Messages Report Builder dialog box.

   The new report appears on the **Custom Reports** list in the RSA Authentication Manager Reports dialog box.

Creating a Histogram of Log Activity

A histogram is a count of activity by the hour. This report does not show any event details, such as user name or Agent Host name.

The Log Messages Histogram Builder dialog box resembles the Log Messages Report Builder dialog box exactly except for its title. You define a report in the same way—by selecting the log messages that correspond to the events you want reported. The only difference between these two report types is in the output: complete, detailed log entries in one report, statistics without details in the other.

To create a histogram of log activity:

1. In the RSA Authentication Manager Reports dialog box, click **Create Report** to open the Select Report Type dialog box.
2. Select **Histogram**, and click **OK**.

   The Log Messages Histogram Builder dialog box opens.
3. Select one or more messages by highlighting them in the **Select Message** list. (If you change your mind about a message, put the cursor on it and click **Deselect**.)

   The number of occurrences of each event indicated by one of the selected messages is reported (for the dates you specify) when this report is run.
4. Click **Create** to add the new report and open the Create a New Report dialog box.
5. Enter a short, descriptive name (up to 25 characters) by which users of the Report Generation Utility can identify this new report. This name will appear in the **Custom Reports** list or **Run List**.

   Also, enter a filename (up to eight characters) to be used for the report output files (and for the report source code file if you requested one).

   Note: Do not use a description or a filename that is already used for another report, even if the report type is different.
6. Click **OK**.

   The new report appears in the **Custom Reports** list in the Log Messages Histogram Builder dialog box.
7. Click **OK** in the Log Messages Histogram Report Builder dialog box.

   The new report appears on the **Custom Reports** list in the main Report dialog box.

Creating Token Statistics Reports

Token statistics reports display the number of tokens in each category that you specify in the report definition. In addition to these numbers, the output data lists the token serial number, the user's first name, and the user's last name for each token included. The default settings in the Token Statistics dialog box define the report so that it includes every token in your realm. Your selections and entries modify these settings and restrict the report to a more closely defined set of tokens.

To create a token statistics report:

1. In the RSA Authentication Manager Reports dialog box, click **Create Report** to open the Select Report Type dialog box.
2. Select **Token Statistics**, and click **OK**.

   The Token Statistics Report Builder dialog box opens.

3. Select criteria to specify the tokens you want to include in the custom report. Make sure that criteria you do not want to include are cleared.

   Tokens which shut down before. All tokens that will shut down (expire) before this date are included in the report.

   Logins which occurred after. All logins made after this date are included in the report.

   Bad tokencode counts greater than. When the number of incorrect tokencodes entered in a single login attempt exceeds the number you enter in this field, the event is included in the report.

   Bad PIN counts greater than. When the number of incorrect PINs entered in a single login attempt exceeds the number you enter in this field, the event is included in the report.

   Token type. Select one or more token types that you want to include in this report.

   Token Enabled, **New PIN Mode**, **Token Lost**, and **Next Tokencode Status**. Click the selections you want to include in the report.

4. Click **Create**.

   Enter a description and a filename for the new report.

5. Enter a short, descriptive name (up to 25 characters) by which users of the Report Generation Utility can identify this new report. This name will appear in the **Custom Reports** list or **Run List**.

   Also, enter a filename (up to eight characters) to be used for the report output files (and for the report source code file if you requested one).

   Note: Do not use a description or a filename that is already used for another report, even if the report type is different.

6. Click **OK**.

   The new report appears in the **Custom Reports** list in the Token Statistics Report Builder dialog box.

7. Click **OK** in the Token Statistics Report Builder dialog box.

   The new report appears on the **Custom Reports** list in the main Report dialog box.

Displaying User Information

To display user information:

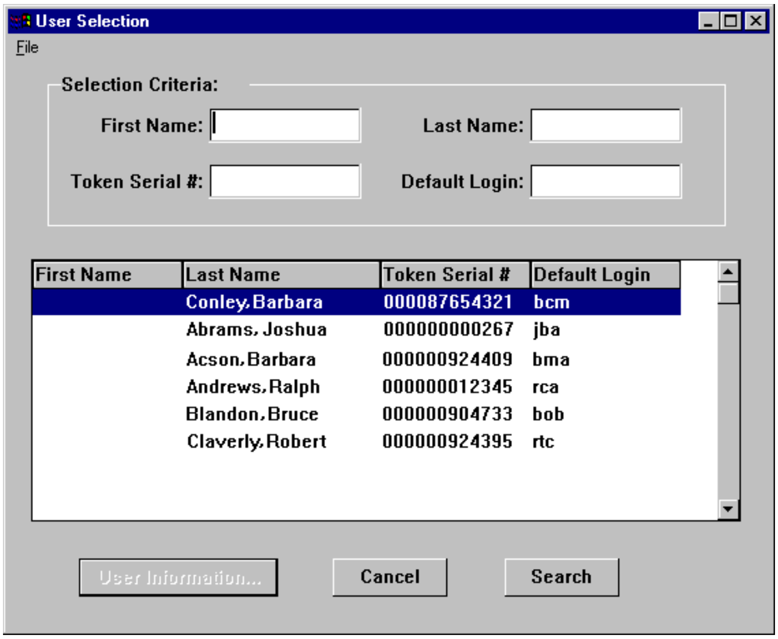
1. On the Users menu, click **User Information** in the RSA Authentication Manager Reports dialog box.

   The User Selection dialog box opens with a list of the entries in the user list.

2. To locate a user in the list, enter information in the selection criteria fields at the top of the dialog box.

3. Click **User Information** to see information about the selected user.

   The User Selection dialog box opens with detailed information about the selected user.



First Name	Last Name	Token Serial #	Default Login
	Conley, Barbara	000087654321	bcm
	Abrams, Joshua	000000000267	jba
	Acson, Barbara	000000924409	bma
	Andrews, Ralph	000000012345	rca
	Blandon, Bruce	000000904733	bob
	Claverly, Robert	000000924395	rtc

Running Reports from a Command Line

Use the **rptrun** utility to run any report from a command line. The first argument to **rptrun** must be the complete path and filename of the report 4GL code. The path for standard reports 4GL code is ***ACEUTILS*\std_rpt**, and the path for custom reports 4GL code is ***ACEUTILS*\cust_rpt**. The 4GL code filenames for custom reports are those specified when the report was created, followed by a .p extension.

Start Date and End Date Command Line Arguments

If you include a start date and an end date in the **rptrun** command, the log reports and histograms cover only the specified period, rather than the whole audit trail. For example, the following command generates a standard report of successful login attempts for the month of September 2001:

```
rptrun ACEUTILS\std_rpt\accepted.p 09/01/2001 09/30/2001
```

Token Expiration Date and Last Login Date Command Line Arguments

When you use the **rptrun** utility to run Token Statistics reports, two input arguments are required following the path and filename of the 4GL code. The first argument is the token expiration date and the second argument is the last login date. These dates must be supplied, even if the expiration date and last login date are not criteria in the report. (The dates are ignored if the report does not require them.) When the expiration date is a criterion, the date is used to select tokens for the report that expire on this date and earlier. When the last login date is a criterion, the date is used to select tokens that were used for authentication on this date and later.

The command syntax is:

```
rptrun full_path expiration_date last_login_date
```

For example, the date is not a criterion in the following command:

```
rptrun ACEUTILS\std_rpt\disabled.p 01/01/2001 01/01/2001
```

The token expiration date is a criterion in the following command:

```
rptrun ACEUTILS\cust_rpt\expire.p 01/31/1999 01/01/2003
```

RSA Authentication Manager Report Creation Utility (UNIX)

The RSA Authentication Manager software includes a Report Creation Utility, which enables you to create and run audit trail reports against the **sdlog** database and token statistic reports against the **sdserv** database. The utility also includes a way to select a user and display on your screen information from the corresponding user record.

UNIX Interface Conventions

The Report Creation Utility runs in character mode (TTY mode) on UNIX systems. The interface conventions are as follows:

- Enter the menu bar by pressing the F3 or PF3 key.
- Once the menu bar is activated, you can move from menu to menu with the arrow keys or by typing the underlined letter in the menu title.
- Once a menu is activated and displayed, select an option by typing the underlined letter in the option name or by moving to the option with the arrow keys and by pressing RETURN.
- In an option box, actions can be initiated with a keystroke only in the currently active area of the box. A rectangle highlights the area of focus.
- To move forward from one area of an option box to another, press TAB. To move backward, press CTRL+U.
- To move from item to item within an area, press the arrow keys.
- To highlight a list item, use the arrow keys.
- To select a list item, radio button, or checkbox, press the spacebar or the RETURN key.
- If a checkbox or radio button is highlighted, pressing RETURN turns it on or off.
- Pressing RETURN executes the action of a highlighted command button. If you have not highlighted a different button, the action associated with the default button is executed when you press RETURN. (Frequently, the default button is **OK**, which may close the dialog box.)
- Pressing RETURN in a box is equivalent to pressing TAB. It moves the cursor out of the field.
- When you click **Cancel** or press **F4** or **PF4**, you cancel any unsaved modifications made in the dialog box and close the dialog box.
- The ESC key cannot be used to close a box.

- Using the BACKSPACE key in a date field has no effect other than moving the cursor. To modify a date field, type over the contents of the field.
- Inactive buttons look no different from activated buttons, but you cannot move the cursor to a button unless it is activated.

Installing the Report Creation Utility

During installation of the RSA Authentication Manager, the Report Creation Utility software is copied to the ***ACEUTILS*** directory.

If you are upgrading and you have used the Report Creation Utility, use the following procedure to restore the database for the Report Creation Utility and custom reports you have created.

- To restore custom report output files, copy the files in the **ace_tmp/utils/cust_rpt** directory back to ***ACEUTILS*/cust_rpt**.
- To restore the database, copy **sdrpt.db** from the **ace_tmp/utils** directory back to the ***ACEUTILS*** directory.

Starting and Stopping the Report Creation Utility

To run the Report Creation Utility:

1. Verify that an RSA Authentication Manager database broker is running on the Primary. If no database broker is running, start one by typing:

   ```
   ACEPROG/sdconnect start
   ```

2. Start the report database server by typing:

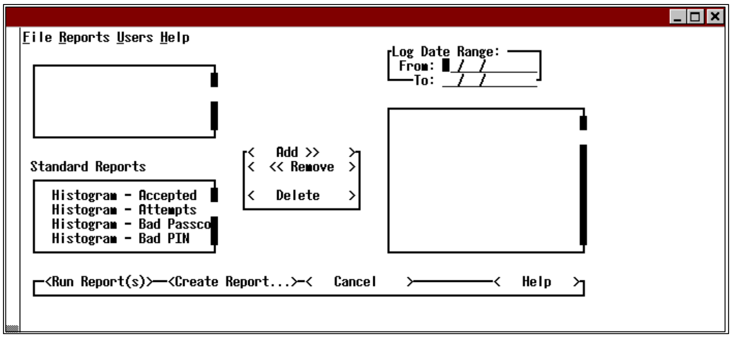
   ```
   ACEUTILS/rptconnect start
   ```

3. Run the Report Creation Utility by typing:

   ```
   ACEUTILS/sdreport
   ```

   Note: The Report Creation Utility may also be run in batch mode. When running the Report Creation Utility in batch mode, the RSA Authentication Manager Reports dialog box does not open. To connect to the database in batch mode, type **ACEUTILS/rptconnect start batch.**

   The RSA Authentication Manager Reports dialog box opens.



To stop the Report Creation Utility:

1. Press **F3** to enter the RSA Authentication Manager Reports dialog box menu bar.
2. Type **F** to open the File menu and **x** to select **Exit**.
3. At the command prompt, stop the report database server by typing:

```
ACEUTILS/rptconnect stop
```

Important: If you do not stop the Report Creation Utility in this manner, the utility may become locked with a lock file, ***ACEUTILS*/sdrpt.lk**. Remove this file, and try again.

Selecting a Report to Run

In the RSA Authentication Manager Reports dialog box, you can select reports from two lists: **Standard Reports** and **Custom Reports**.

- **Standard Reports** are ready-made reports that cannot be modified or removed. The set of standard reports includes four histogram reports and four token list reports.
- **Custom Reports** are reports that you can create, modify, and delete. Until you or another administrator creates one or more custom reports, the **Custom Reports** list is empty.

Using the Run List

The Report Creation Utility is designed so that reports can be run only from the **Run List**. In order to run a report, you must first move it from the **Standard List** or **Custom List** to the **Run List**.

- To move reports to the **Run List**, highlight the reports in the **Standard List** or **Custom List** and click **Add**. You can highlight multiple reports by clicking each selection while you press CTRL.
- To remove a report from the **Run List**, highlight it and click **Remove**. When you remove reports from the **Run List**, each report returns to its original list.

You can use the **Run List** for the reports you select to run during a single session, or you can save the list contents so that the same set of files are ready to be run whenever you start the Report Creation Utility. If you never save the list, it is always empty when the utility opens. Otherwise, the list contains the same files that it contained when last saved.

Although the utility comes with eight standard reports and no custom reports, you may, over time, create large numbers of custom reports—some that you run regularly and others that you run infrequently. By saving the **Run List** you can keep the reports that you run most often in a place where they are easy to find. Reports run infrequently are not lost—they remain on the **Standard List** and **Custom List**.

To save the **Run List**, click **File** > **Save Run List**. When you want to change the contents of your standard run list, create a new version and save it in place of the old one.

To run reports from the Run List:

1. Enter the **From** and **To** log dates to define the date range for the report or reports you are going to run.

   If you do not specify a date range, all available relevant information is included without regard to the log record dates.

2. Highlight the report or reports you want to run.
3. Select **Run Report(s)**.

Standard Report Types

Histogram Reports

A **Histogram** report is a series of numbers that represents an hourly activity count. This count is useful for plotting peak activity or load by time. The output file (with extension .xls) can be imported into a spreadsheet and graphed.

- **Histogram – Accepted** shows the number of successful authentications during each hour of the specified period.
- **Histogram – Attempts** shows the number of access attempts, both successful and unsuccessful, during each hour of the specified period.
- **Histogram – Bad PASSCODE** shows the number of login attempts that failed because of an invalid passcode during each hour of the specified period.
- **Histogram – Bad PIN** shows the number of login attempts that failed because a valid tokencode was entered with an incorrect PIN during each hour of the specified period. (This count applies to RSA SecurID standard cards and key fobs only.)

Token List Reports

The following token lists can help you troubleshoot users’ authentication problems. Use the Token Statistics Report Builder, described in “Creating Token Statistics Reports” on page 190, to create similar listings specific to your needs.

- **Token – Disabled** lists the token serial number and the assigned user’s name and login for each disabled token.
- **Token – New PIN** lists the token serial number and the assigned user’s name and login mode for each token in New PIN mode.
- **Token – Wait 1 Tokencode** lists the tokens that are in Next Tokencode mode with one good tokencode already entered. Each token serial number and the assigned user’s name and login are identified.
- **Token – Wait 2 Tokencodes** lists the tokens for which the system needs two good tokencodes before granting access to their users. Each token is identified by serial number and assigned user’s name and login.

Report Output Files

When you run a report from the Reports dialog box, the output is stored in two text files. One of the files has a .txt extension and is in an easy-to-read format. The other file has a .xls extension and is in a format compatible with spreadsheets.

For standard reports, the full filename is based on the report content and format. For example, complete filenames for **Histogram – Attempts** output are **attempts.txt** and **attempts.xls**. Each standard report type has a unique, predefined name. For a custom report, you specify the filename and the Report Creation Utility adds the extension. You must ensure that the filename you supply is not used for any other report regardless of type.

Report output files are stored in a subdirectory of the ***ACEUTILS*\output** directory. The subdirectory is created automatically if it does not exist, and it is named for the date on which the report was run (in ***yyyymmdd*** format). If the same report type is run more than once during a single day, the latest output overwrites the previous output.

Example: On March 1, 2005, you highlight **Histogram – Accepted** on the **Run List** and select **Run Report(s)**. Two files are created, **accepted.txt** and **accepted.xls**, both stored in ***ACEUTILS*/output/20050301**.

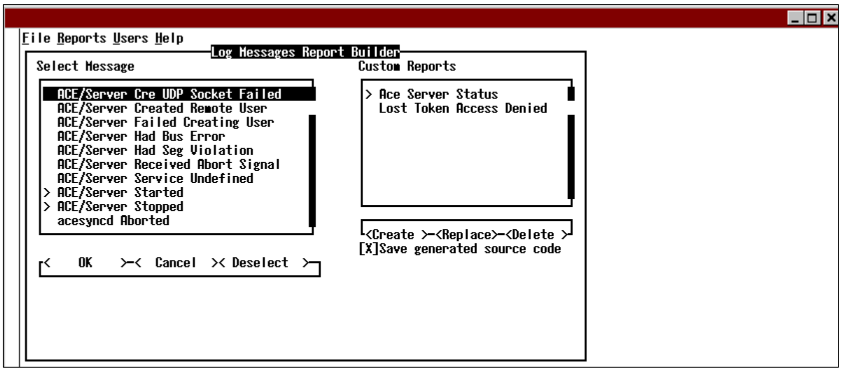
Creating and Managing Custom Reports

The Report Creation Utility provides three custom report dialog boxes. You can use these dialog boxes not only to create new reports but also to edit or delete existing reports.

To create, edit, or delete custom reports:

1. Press **F3** to enter the RSA Authentication Manager Reports dialog box menu bar and **R** to open the Reports menu.
2. Select **Create New Report** and press RETURN.
   The Select Report Type dialog box opens.
3. Select one of three types: **Log Entry**, **Histogram**, or **Token Statistics**.
   Depending on your selection, one of the following dialog boxes opens:
   - Log Messages Report Builder
   - Log Messages Histogram Builder
   - Token Statistics Report Builder

One feature common to all of these dialog boxes is the **Custom Reports** list, which lists by name any custom reports of the selected type that are currently defined. For an example, see the right side of the Log Messages Report Builder dialog box.



```
File Reports Users Help
                  Log Messages Report Builder
 Select Message                           Custom Reports
    ACE/Server Cre UDP Socket Failed       > Ace Server Status
    ACE/Server Created Remote User           Lost Token Access Denied
    ACE/Server Failed Creating User
    ACE/Server Had Bus Error
    ACE/Server Had Seg Violation
    ACE/Server Received Abort Signal
    ACE/Server Service Undefined
  > ACE/Server Started
  > ACE/Server Stopped
    acesyncd Aborted
                                          <Create >-<Replace>-<Delete >
                                          [X]Save generated source code
  < OK  >-< Cancel  >< Deselect  >
```

4. One way to create a new report is to select an existing report and change the definition. When you select any report, the settings that define it are displayed on the screen. (In the Log Messages Report Builder dialog box, for example, the messages specified as the report contents are highlighted in the **Select Message** list.) You can change these settings and select **Replace** to save the new report definition in place of the old one.
5. To create a new report without using an existing one, select **Create**. New reports are added to the **Custom Reports** list. (Complete procedures for creating the three types of report are provided in the next three sections.)
6. To delete a report from the **Custom Reports** list, highlight it and select **Delete**.
7. To save editable 4GL code for a report you create, press TAB to move to the **Save generated source code** box and press RETURN to mark it.

   When this box is not marked, only compiled 4GL code is generated. When this box is marked, readable and editable 4GL source code is generated in addition to the compiled code.

Creating Log Entry Reports

The Log Messages Report Builder dialog box enables you to create reports that include all log records of one or more event types by selecting the corresponding log messages from the **Select Message** box. For example, you could define a report showing every instance of the RSA Authentication Manager disabling a token. Another report might include all log records that represent changes to a user record or a token record.

Log reports include the detailed information available from the Authentication Manager audit trail. Entries show the time and date of the event, the current and affected users (as appropriate), and a one-line description of the event.

To define a custom log entry report:

1. Press **F3** to enter the RSA Authentication Manager Reports dialog box menu bar and **R** to open the Reports menu.
2. Select **Create New Report** and press RETURN.

   The Select Report Type dialog box opens.
3. Select **Log Entry** and then **OK**.

   The Log Messages Report Builder dialog box opens.
4. In the **Select Message** list, select a message for inclusion in the report by highlighting the message and pressing RETURN. To select additional messages, repeat the procedure.

   The number of occurrences of each event indicated by one of the selected messages is reported (for the dates you specify) when this report is run.
5. When you have made all of your message selections, highlight **OK** below the **Select Message** list and press RETURN.
6. Highlight **Create** below the **Custom Reports** list and press RETURN.

   The Create a New Report dialog box opens and prompts you for a description and a filename for the new report.
7. Enter a short, descriptive name (up to 25 characters) by which users of the Report Generation Utility can identify the new report. This name will appear in the **Custom Reports** list or **Run List**.

   In addition to the descriptive name, enter a filename (up to eight characters) for the report output files (and for the report source code file if you requested one).

   Note: Do not use a description or a filename that is already used for another report, even if the report type is different.
8. Select **OK** and press RETURN.

   The new report appears in the **Custom Reports** list in the Log Messages Report Builder dialog box.
9. Select **OK** in the Log Messages Report Builder dialog box and press RETURN.

   The new report appears on the **Custom Reports** list in the RSA Authentication Manager Reports dialog box.

Creating a Histogram of Log Activity

A histogram is an activity account by the hour. This report does not include event details, such as user name or Agent Host name.

The Log Messages Histogram Builder dialog box is identical to the Log Messages Report Builder dialog box *except* for its title. You define a report in the same way—by selecting the log messages that correspond to the events you want reported. The only difference between these two report types is in the output: detailed log entries in one report, statistics without details in the other.

To create a histogram of log activity:

1. Press **F3** to enter the RSA Authentication Manager Reports dialog box menu bar and **R** to open the Reports menu.
2. Select **Create New Report** and press RETURN.

   The Select Report Type dialog box opens.
3. Select **Histogram** and then **OK**.

   The Log Messages Histogram Builder dialog box opens.
4. Press TAB to move into the **Select Message** list.
5. Select a message by pressing the arrow keys to highlight the message, and then press RETURN to select the message. To select more than one message, repeat the procedure for each message you want to select.

   Each occurrence of the selected messages is counted in the report output.
6. When you have made all of your message selections, highlight **OK** below the **Select Message** list and press RETURN.
7. Highlight **Create** below the **Custom Reports** list and press RETURN.

   The Create a New Report dialog box opens and prompts you for a description and a filename for the new report.
8. Enter a short, descriptive name (up to 25 characters) by which users of the Report Generation Utility can identify the new report. This name will appear in the **Custom Reports** list or **Run List**.

   In addition to the descriptive name, enter a filename (up to eight characters) for the report output files (and for the report source code file if you requested one).

   Note: Do not use a description or a filename that is already used for another report, even if the report type is different.
9. Select **OK** and press RETURN.

   The new report appears in the **Custom Reports** list in the Log Messages Histogram Builder dialog box.
10. Select **OK** in the Log Messages Histogram Builder dialog box and press RETURN.

    The new report appears on the **Custom Reports** list in the RSA Authentication Manager Reports dialog box.

Creating Token Statistics Reports

Token statistics reports display the number of tokens in each category that you specify in the report definition. In addition to these numbers, the output data lists the token serial number, the user's first name, and the user's last name for each token included. The default settings in the Token Statistics dialog box define the report so that it includes every token in your realm. Your selections and entries modify these settings and restrict the report to a more closely defined set of tokens.

To create a token statistics report:

1. Press **F3** to enter the RSA Authentication Manager Reports dialog box menu bar and **R** to open the Reports menu.
2. Select **Create New Report** and press RETURN.

   The Select Report Type dialog box opens.
3. Select **Token Statistics** and then **OK**.

   The Token Statistics Report Builder dialog box opens.
4. Indicate the criteria you want to include in the custom report:

   Tokens which shut down before. All tokens that will shut down (expire) before this date are included in the report.

   Logins which occurred after. All logins made after this date are included in the report.

   Bad tokencode counts greater than. When the number of incorrect tokencodes entered in a single login attempt exceeds the number you enter in this field, the event is included in the report.

   Bad PIN counts greater than. When the number of incorrect PINs entered in a single login attempt exceeds the number you enter in this field, the event is included in the report.

   Token type. Mark one or more token types that you want to include in this report. For more information about token types, see "RSA SecurID Tokens and Two-Factor Authentication" on page 14.

   Token Enabled, New PIN Mode, Token Lost, and **Next Tokencode Status.** Mark the selections you want to include in the report.
5. When you have indicated all the report criteria, select **OK** below your selections and press RETURN.
6. Select **Create** below the **Custom Reports** list and press RETURN.

   You are prompted to provide a description and a filename for the new report.
7. Enter a short, descriptive name (up to 25 characters) by which users of the Report Generation Utility can identify the new report. This name will appear in the **Custom Reports** list or **Run List**.

   In addition to the descriptive name, enter a filename (up to eight characters) for the report output files (and for the report source code file if you requested one).

   Note: Do not use a description or a filename that is already used for another report, even if the report type is different.
8. Select **OK** and press RETURN.

   The new report appears in the **Custom Reports** list in the Token Statistics Report Builder dialog box.
9. Select **OK** in the Token Statistics Report Builder dialog box and press RETURN.

   The new report appears on the **Custom Reports** list in the RSA Authentication Manager Reports dialog box.

Displaying User Information

To display user information:

Press **F3** to enter the RSA Authentication Manager Reports dialog box menu bar and **U** to open the Users menu.

1. Select **User Information** and press RETURN.

   The User Selection dialog box opens with a list of the entries in the **User** list.
2. To locate a user in the list, enter information in the selection criteria fields at the top of the dialog box.
3. To see data about the selected user, select **User Information** and press RETURN.

   The User Information dialog box opens with detailed information about the selected user, such as first and last name, token serial number, and so on.

Running Reports from the Command Line

Use the **rptrun** utility to run any report from the command line. The first argument to **rptrun** must be the complete path and filename of the report 4GL code. The path for standard reports 4GL code is ***ACEUTILS*/std_rpt**, and the path for custom reports 4GL code is ***ACEUTILS*/cust_rpt**. The 4GL code filenames for custom reports are those specified when the report was created, followed by a .p extension.

Start Date and End Date Command Line Arguments

If you include a start date and an end date in the **rptrun** command, the log reports and histograms will cover only the specified period, rather than the whole audit trail. For example, the following command generates a standard report of successful login attempts for the month of January 2005:

```
rptrun ACEUTILS/std_rpt/accepted.p 01/01/2005 01/31/2005
```

Token Expiration Date and Last Login Date Command Line Argument

When you use the **rptrun** utility to run Token Statistics reports, two input arguments are required following the path and filename of the 4GL code. The first argument is the token expiration date and the second argument is the last login date. These dates must be supplied, even if the expiration date and last login date are not criteria in the report. (The dates are ignored if the report does not require them.) When the expiration date is a criterion, the date is used to select tokens for the report that expire on this date and earlier. When last login date is a criterion, the date is used to select tokens that were used for authentication on this date and later.

The command syntax is:

```
rptrun full_path expiration_date last_login_date
```

For example, the date is not a criterion in the following command:

```
rptrun ACEUTILS/std_rpt/disabled.p 01/01/1999 01/01/2003
```

The token expiration date is a criterion in the following command:

```
rptrun ACEUTILS/cust_rpt/expire.p 01/31/1999 01/01/2003
```

Creating and Running Custom SQL Queries

RSA Authentication Manager maintains its data in a Progress Software relational database management system (RDBMS). Two databases—**sdserv** (the user database) and **sdlog** (the audit log database)—are available in RSA Authentication Manager.

With Custom Queries, you can use SQL (Structured Query Language) to query the databases, and specify data output to CSV, HTML or XML files. Using third-party software, you can import the data and build a range of useful reports.

If you are unfamiliar with SQL, you can still run the sample queries provided with RSA Authentication Manager.

If you or someone in your organization has experience with SQL, you can create your own queries to run against the RSA Authentication Manager databases. Over time, you can build up a library of custom queries for your organization.

Note: For security purposes, only realm administrators can create, compile and, optionally, share custom queries. For more information, see "Administrative Scoping in Custom Queries" on page 207.

Getting Started with Custom Query Tools

This section describes the basic tasks you can perform to compile, run, and otherwise manage the sample queries provided with RSA Authentication Manager.

For information about developing custom queries, which requires some SQL experience, see "Creating and Editing Custom Queries" on page 195 and "SQL Syntax and Grammar in Custom Queries" on page 196.

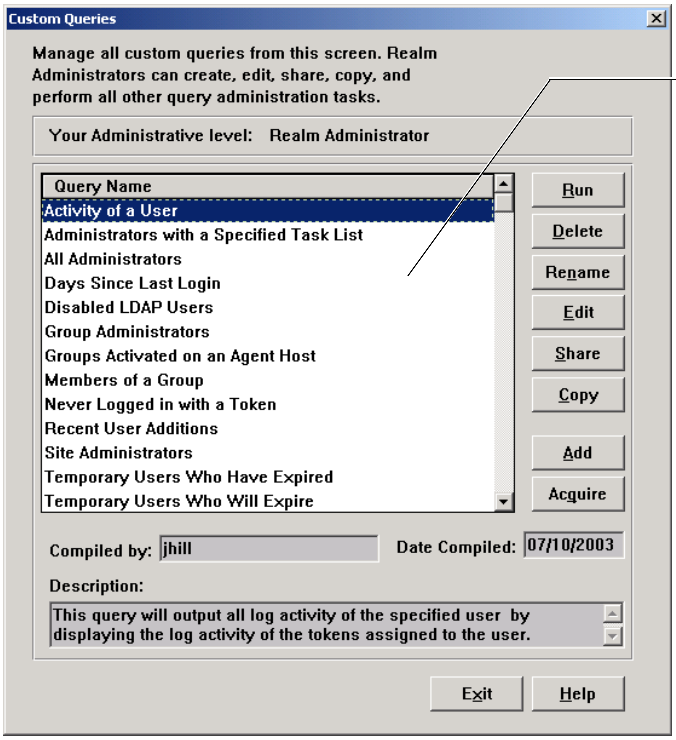
Custom Query tools are available in the Database Administration program.

To Begin:

1. Click **Start** > **Programs** > **RSA Security > RSA Authentication Manager Host Mode (or Remote Mode).**
2. Select **Report** > **Custom Queries**.

   The Custom Queries dialog box (shown on page 194) appears. This is the control center for all custom query activities in RSA Authentication Manager.

Note: In all custom query dialog boxes, you can access context-sensitive and step-by-step information by clicking **Help**.



Custom Queries

Manage all custom queries from this screen. Realm Administrators can create, edit, share, copy, and perform all other query administration tasks.

Your Administrative level: Realm Administrator

Query Name
- Activity of a User
- Administrators with a Specified Task List
- All Administrators
- Days Since Last Login
- Disabled LDAP Users
- Group Administrators
- Groups Activated on an Agent Host
- Members of a Group
- Never Logged in with a Token
- Recent User Additions
- Site Administrators
- Temporary Users Who Have Expired
- Temporary Users Who Will Expire

Compiled by: jhill

Date Compiled: 07/10/2003

Description:

This query will output all log activity of the specified user by displaying the log activity of the tokens assigned to the user.

List of sample queries

Administrative Levels and Query Privileges

For security reasons, only Realm Administrators have access to the full functionality of custom query tools, including creating, editing, and sharing queries.

When a Site or Group Administrator runs the Custom Queries command, RSA Authentication Manager detects the administrative level and displays a different version of the Custom Queries dialog box. In that version, only four options are available: **Acquire**, **Run**, **Rename** and **Delete**.

In addition, Site and Group Administrators can only run queries that they have acquired from the list of shared queries.

For security purposes, scoping features enable the Realm Administrator to define the administrative level (Realm, Site, or Group) that is required to run a shared query. For more information, see "Administrative Scoping in Custom Queries" on page 207.

Using the Sample Queries

If you are a Realm Administrator, the uncompiled sample queries appear in your view of the Custom Queries dialog box. You can compile, copy, edit, run, and share the sample queries.

To use a sample query, you first must compile it. Highlight the query in the list, then click **Edit**. Follow the instructions in each successive dialog box. When you "finish" the compilation, the query is now bound to your installation and can only be used within the realm. (For more information, see "Editing a Query" on page 196. If you have multiple realms, see "Managing Queries Among Multiple Realms" on page 211.)

Note: Sample queries are listed and described in the Help. If you want to modify a sample query, RSA Security recommends that you make a copy of it first and modify the copy.

Creating and Editing Custom Queries

If you are a Realm Administrator familiar with SQL, you can create custom queries or edit existing queries for your own purposes.

Creating a New Query

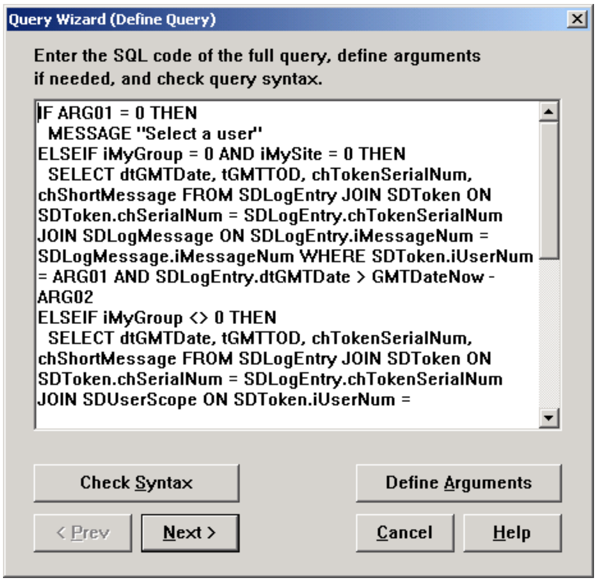
Use the **Add** button to create a new query. A **Query Wizard** guides you through the process.

To Begin: Click **Report** > **Custom Queries** > **Add**. This opens the Query Wizard (Query Name) dialog box. See the Help for the details of each step.

For more information, see "SQL Syntax and Grammar in Custom Queries" on page 196 and "Advanced Application Notes for Custom Queries" on page 207.

Editing a Query

You must be a Realm Administrator to use the Edit option (as described in “Administrative Levels and Query Privileges” on page 194). Select the query name from the Custom Queries dialog box, and click **Edit**. The Query Wizard takes you directly to the Define Query screen.



Enter the SQL code of the full query, define arguments if needed, and check query syntax.

```
IF ARG01 = 0 THEN
  MESSAGE "Select a user"
ELSEIF iMyGroup = 0 AND iMySite = 0 THEN
  SELECT dtGMTDate, tGMTTOD, chTokenSerialNum,
chShortMessage FROM SDLogEntry JOIN SDToken ON
SDToken.chSerialNum = SDLogEntry.chTokenSerialNum
JOIN SDLogMessage ON SDLogEntry.iMessageNum =
SDLogMessage.iMessageNum WHERE SDToken.iUserNum
= ARG01 AND SDLogEntry.dtGMTDate > GMTDateNow -
ARG02
ELSEIF iMyGroup <> 0 THEN
  SELECT dtGMTDate, tGMTTOD, chTokenSerialNum,
chShortMessage FROM SDLogEntry JOIN SDToken ON
SDToken.chSerialNum = SDLogEntry.chTokenSerialNum
JOIN SDUserScope ON SDToken.iUserNum =
```

After you finish editing the SQL code and query arguments, you can check syntax and complete the other Query Wizard tasks.

For related information, see the following section, “SQL Syntax and Grammar in Custom Queries” and “Advanced Application Notes for Custom Queries” on page 207.

SQL Syntax and Grammar in Custom Queries

This section discusses SQL usage in Custom Queries and provides a number of SQL code examples to illustrate valid syntax. RSA Security recommends that you review and understand the sample queries that are provided with RSA Authentication Manager.

Database Schema

The RSA Authentication Manager database is organized as a set of interrelated tables, or **schema**. To use the custom query feature effectively, you need to become familiar with the schema table names and the data they contain.

For example, the **SDUser** table contains over 30 fields relating to every user defined in the database—fields such as first and last name (**chFirstName**, **chLastName**), login (**chDefaultLogin**), and so on. **SDUser** is one of over 100 tables in the RSA Authentication Manager database schema.

Note: Refer to the Help for a comprehensive reference of all the schema tables and their contents. A schema section is also included in the *Administration Toolkit Reference Guide* (**authmgr_admin_toolkit.pdf**).

General Rules About Query Length and Syntax

In Custom Queries, for a query to be valid, it must meet the following conditions:

- There must be at least one **SELECT** statement. For more information, see the following section, "SELECT Statement Syntax."
- Up to 32 statements in a single query are allowed, and a query can be up to 4,096 characters in length.
- If there is more than one **SELECT** statement in a query, they all must return the same set of fields in the same order. Selected fields in different SELECT statements can be identical. Alternatively, selected fields can be from different database tables if they have the same name, type and, in the case of character fields, the same size (for example, **chDefaultLogin** from the **SDUser** table and **chDefaultLogin** from the **SDUserScope** table). In addition, in all SELECT statements in a query, the fields must be in the same position.
- Custom queries are not *case-sensitive* and allow any combination of capital and lowercase letters.
- **MESSAGE** statements are optional and can only be used in conditional clauses (IF/THEN, ELSEIF, ELSE). For more information, see "Using Conditional Clauses to Validate User Input" on page 205.

SELECT Statement Syntax

In Custom Queries, you are limited to *reading* from the RSA Authentication Manager user and log databases, **sdserv** and **sdlog**. You cannot use queries to write to or modify the databases. Consequently, the sample queries primarily make use of the **SELECT** statement.

In Custom Queries, the syntax of the SELECT statement is as follows. Entries in square brackets ([ ]) are optional:

```
SELECT {*|column-list} FROM {table-name|explicit-join}
[WHERE search-condition]
[GROUP BY column[,column]...]
[HAVING search-condition]
[ORDER BY sort-criteria]
```

In a SELECT statement, you identify the *column list*, or fields of data, you want to search and the **FROM** clause to identify the database table containing the data. For example:

```
SELECT chDefaultLogin, chLastName, chFirstName FROM SDUser
```

In this example, all users' default logins, last and first names are retrieved from the SDUser table (which is in the **sdserv** database).

Note: Because all table names in the **sdserv** (user) and **sdlog** (audit log) databases are unique, you do not need to include the database name in the query.

To retrieve all fields in a table, you can use the asterisk (*) as a wildcard for the column list in the SELECT statement: For example:

```
SELECT * FROM SDUser
```

The asterisk cannot be used as a wildcard in other constructions. For example, the following is *not* allowed and generates an error:

```
SELECT SDUser.*
```

Using Expressions to Retrieve Data

Another way to specify the column list in a SELECT statement is to use an **expression**. Expressions provide ways to retrieve data by using a function. Custom Queries supports only functions that retrieve a numeric result. These include:

COUNT. This function provides a count of all rows in the results list. For example:

```
SELECT COUNT(DISTINCT chLastName) FROM SDUser
```

This example counts the number of distinct last names in the SDUser table.

MAX. This function retrieves the highest number from a particular field. For example:

```
SELECT MAX(iUserNum) FROM SDUser
```

This example retrieves the highest user number, or the last user added to the database.

MIN. This function retrieves the smallest number in a particular field. For example:

```
SELECT MIN(iUserNum) + 1 FROM SDUser
```

This example retrieves the second lowest active user number from the SDUser table.

Note: You can use **operands** (for example, " + 1") to modify functions. In such cases, be sure to include spaces to separate the operand from the function, or a syntax error appears.

Using Joins in SELECT Statements

When using the SELECT statement, you can retrieve data from a single table or from multiple tables. To retrieve data from multiple tables, use a table join. There are three types of joins:

INNER. An inner join returns the records selected for the table on the left side combined with the related records from the table on the right. (The first table specified in the SELECT statement is said to be on the left side.) With an inner join, only the fields that match the selection criteria are output. For example:

```
SELECT chDefaultLogin FROM SDUser JOIN SDToken ON
SDUser.iUserNum=SDToken.iUserNum
```

This statement would output the login names of only those users who have tokens (including passwords) assigned to them. Note that using the JOIN clause by itself implies an inner join. You can also use the explicit INNER JOIN clause.

LEFT[OUTER]. With a left join, all records from the first (left) table are put into the result set and then they are joined by only those fields in the second (right) table that match the selection criteria. For example:

```
SELECT chLastName, chFirstName, chSerialNum FROM SDUser LEFT
JOIN SDToken ON (SDUser.iUserNum = SDToken.iUserNum)
```

This statement would output the names of all users in the SDUser table. For users with an assigned token, the token serial number would also be output. Note that using LEFT JOIN by itself implies an outer join. You can also use the explicit LEFT OUTER JOIN clause.

RIGHT[OUTER]. With a right join, all records from the second (right) table are put into the result set, then they are joined by only those fields in the first (left) table that match the selection criteria. For example, in contrast to the preceding LEFT JOIN example, if you want to retrieve all serial numbers of tokens in the database, whether they are assigned or not, you can use this query:

```
SELECT chLastName, chFirstName, chSerialNum FROM SDUser
RIGHT JOIN SDToken ON (SDUser.iUserNum = SDToken.iUserNum)
```

Note that using RIGHT JOIN by itself implies an outer join. You can also use the explicit RIGHT OUTER JOIN clause. Also note that a RIGHT JOIN is limited to two tables.

To further define the column list in a SELECT statement, you can use multiple joins. For example, to list all Group Administrators in the database, you can use this query:

```
SELECT chDefaultLogin, chLastName, chFirstName,
SDGroup.chName, SDSite.chName FROM SDAdministrativeRole
JOIN SDUser ON SDUser.iUserNum =
SDAdministrativeRole.iUserNum
JOIN SDGroup ON SDAdministrativeRole.iGroupNum =
SDGroup.iGroupNum
LEFT OUTER JOIN SDSite ON SDGroup.iSiteNum = SDSite.iSiteNum
ORDER BY chDefaultLogin
```

Note: You can use inner joins and left joins together, or inner and right joins, but you should *not* use right and left joins in the same SELECT statement.

In addition, in Custom Queries, the fields on which the table join is to occur must include the table name followed by a period followed by the column name. For example:

Correct:

```
JOIN SDAdministrativeRole ON SDUSer.iUserNum =
SDAdministrativeRole.iUserNum
```

Incorrect:

```
JOIN SDAdministrativeRole ON iUserNum
```

The SELECT statement examples shown in this section use *explicit* joins (some form of the JOIN clause is included). Table joins can be also be *implicit*. For example:

```
SELECT chDefaultLogin FROM SDUser, SDToken WHERE
SDUser.iUserNum=SDToken.iUserNum
```

Note: Implicit joins can take a long time to process and are *not* recommended. When you have the choice, use explicit joins, which are generally more efficient.

The following section goes into more detail about search conditions in table joins. For additional information about table joins, see "Best Practices for Table Joins" on page 209.

Using the 'ON' Search Condition

Explicit table joins must use the **ON** search condition. This conditional clause can serve one of two purposes in a join:

Relating tables. In the RSA Authentication Manager database, like most relational databases, tables often have relationships to other tables. For example, both the SDUser and SDToken tables have an **iUserNum** field, which relates users to their assigned tokens. An example of using this relationship in a SELECT statement is:

```
SELECT chLastName, chFirstName, chDefaultLogin FROM SDUser
JOIN SDToken ON SDUser.iUserNum=SDToken.iUserNum
```

There are a number of other relationships among tables in the RSA Authentication Manager database. Relationship types are one-to-one, zero-to-one, one-to-many, and zero-to-many. For more information about relationships among tables, see the descriptions of the database schema in the Help.

Filtering tables. You can also use the ON search condition to select only those records that meet the search criteria. This sort of filter condition contains one or more logical expressions connected by a logical operator (AND, OR, NOT). For example:

```
SELECT chDefaultLogin, chLastName, chFirstName, chSerialNum
FROM SDUser JOIN SDToken ON SDUser.iUserNum =
SDToken.iUserNum AND SDUser.chLastName BEGINS "A" AND
SDUser.bTempUser = YES
```

This statement would output the login, last and first names, and token serial numbers of all temporary users whose last names begin with "A".

Using the ‘WHERE’ Search Condition

Use the WHERE clause to set up filter conditions for the output of a query. Unlike the ON clause, you can use WHERE when no join is required. For example:

```
SELECT chDefaultLogin, chLastName, chFirstName FROM SDUser
WHERE SDUser.chLastName BEGINS "A" AND SDUser.bTempUser =
YES
```

In the example, the login, last and first names of temporary users whose last names begin with “A” are output. Only the SDUser table is searched for the information.

You can also use WHERE inside the ON clause in a table join. For example:

```
SELECT chDefaultLogin, chLastName, chFirstName,
dateLastLogin, todLastLogin FROM SDUser JOIN SDToken ON
SDUser.iUserNum = SDToken.iUserNum WHERE
SDToken.DateLastLogin < GMTDateNow ORDER BY chDefaultLogin
```

In the example, the login, last and first names of users, along with the dates and times of their last logins would be output.

Using ‘GROUP BY’ and ‘HAVING’ Clauses

Use the GROUP BY clause to merge a set of rows that have the same value for a specified column or columns into a single row. For example:

```
SELECT chLastName, chFirstName FROM SDUser JOIN SDToken ON
SDUser.iUserNum = SDToken.iUserNum GROUP BY SDToken.iUserNum
HAVING COUNT(DISTINCT SDToken.iTokenNum) > 2
```

This example searches for users who have more than two tokens assigned to them. Since you might want only a simple list of users with multiple tokens, the GROUP BY clause enables only one row per user to be output (rather than one row per token).

As shown in the example, you can use the HAVING clause to specify one or more qualifying conditions, typically for the GROUP BY clause.

Using the ‘ORDER BY’ Clause to Specify Sort Order

Use the ORDER BY clause to sort query results by the values in one or more columns. For example:

```
SELECT chDefaultLogin, chLastName, chFirstName FROM SDUser
ORDER BY chLastName
```

In the example, the records will be ordered alphabetically by users’ last names.

Using Operators to Form Logical Expressions

To qualify the JOIN, ON, WHERE and HAVING clauses, you can use **operators** to form logical expressions. There are three types of operators:

Comparison. These operators enable you to qualify numeric, binary, date, and other functions:

<	greater than
>	less than
=	equal to
<>	not equal to

For example:

```
SELECT chDefaultLogin, chLastName, chFirstName, dateEnd,
todEnd FROM SDUser WHERE SDUser.bTempUser = TRUE AND
dateEnd < GMTDateNow AND SDUser.iJobNum = 0 ORDER BY
chDefaultLogin
```

In this example, the login, and the last and first names of all expired temporary users are output, along with the dates and times that they expired.

Boolean. The AND, OR, and NOT operators enable you to combine, include, or exclude search conditions.

For example:

```
SELECT chDefaultLogin, chLastName, chFirstName, iType,
chSerialNum FROM SDUser JOIN SDToken ON SDUser.iUserNum =
SDToken.iUserNum WHERE SDToken.iType = 2 AND dateDeath >
GMTDateNow AND NOT dateDeath < 12/31/2006 ORDER BY
chDefaultLogin
```

In this example, the login, last and first names of all users with assigned, active key fob tokens that will expire before 12/31/2006 are output along with the token type and serial numbers.

Matching. With these operators you can qualify search conditions by specifying a variety of matching criteria:

BEGINS
BETWEEN
IN
LIKE
MATCHES

For example:

```
SELECT chDefaultLogin, chLastName, chFirstName, chSerialNum
FROM SDUser JOIN SDToken ON SDUser.iUserNum =
SDToken.iUserNum WHERE SDToken.chSerialNum BEGINS
"000029949" AND SDToken.chSerialNum NOT BEGINS "000029950"
ORDER BY chSerialNum
```

In this example, the login, last and first names of all users with tokens whose serial numbers fall within the range 000029949000–000029949999, are output along with the serial numbers themselves. (Actual serial numbers are 12 characters in length.)

You could use the BETWEEN operator to construct the same query. Note that BETWEEN can be used only with integers.

```
SELECT chDefaultLogin, chLastName, chFirstName, iType,
chSerialNum FROM SDUser JOIN SDToken ON SDUser.iUserNum =
SDToken.iUserNum WHERE SDToken.chSerialNum BETWEEN
"000029949000" AND "000029949999" ORDER BY chSerialNum
```

The LIKE operator could similarly be used to construct the query:

```
SELECT chDefaultLogin, chLastName, chFirstName, iType,
chSerialNum FROM SDUser JOIN SDToken ON SDUser.iUserNum =
SDToken.iUserNum WHERE SDToken.chSerialNum LIKE "000029949%"
ORDER BY chSerialNum
```

In this example, note the use of the percent (%) sign acting as a wildcard matching zero or more characters. Similarly, the underscore (_) wildcard can be used to match a single character.

Using 'LENGTH' and 'DATE' Functions in Expressions

To qualify expressions in the JOIN, WHERE or HAVING clause, you can use the LENGTH and DATE functions.

LENGTH: Use this function to qualify a search condition by, for example, selecting only those fields that are have a certain number of characters. For example:

```
SELECT chDefaultLogin, chLastName, chFirstName FROM SDUser
WHERE LENGTH(chDefaultLogin) < 6
```

This example finds all users whose login is less than six characters in length.

DATE. This function can qualify a search condition by specifying a date. The syntax of the DATE function can be:

```
DATE(month,day,year)
DATE(mm/dd/yyyy)
```

For example:

```
SELECT chDefaultLogin, chLastName, chFirstName,
chSerialNum, dateDeath FROM SDUserScope JOIN SDToken ON
SDUserscope.iUserNum = SDToken.iUserNum WHERE
SDToken.dateLastLogin = DATE(01,01,1986)
```

In this example, the logins and names of users with assigned tokens who have never used the tokens to authenticate are output along with their token serial numbers and the dates the tokens expire. January 1, 1986 is the birthdate (or "clock-zero" date) assigned to new tokens.

Using Arguments to Enable User Input

Rather than including fixed data in queries, such as dates, numbers, and so on, you can define **arguments**, the values of which the query user would specify at runtime. In the body of the query, you can use argument placeholders (for example, "ARG01").

To define arguments for a query, you navigate to the Define Query dialog box (shown on page 196) in the Query Wizard.

To Begin: Click **Report** > **Custom Queries** > **Add** (or **Edit** for an existing query). See the Help for the details of each step.

You can define up to 12 arguments for each query. Arguments have predefined names: **ARG01**, **ARG02**, ... **ARG12**.

In the previous section, the example shown for the LENGTH function uses an expression with a fixed number ("< 6").

However, to make the query more useful, you could create an argument that would enable the query user to specify a number. The query might look like this instead:

```
SELECT chDefaultLogin, chLastName, chFirstName FROM SDUser
WHERE LENGTH(chDefaultLogin) < ARG01
```

This example finds all users whose login is less than the number of characters the user running the query enters. When defining ARG01, you could specify a prompt that users would see when they run the query. For example:

```
Enter the minimum character count in users' logins
```

Two categories of arguments can be defined:

Arguments of a specific type: The argument can be NUMBER, STRING, LOGICAL (true or false), or DATE. The user running the query sees a dialog box allowing entry of the argument value.

Selectable arguments: The argument can be one of the selections in the following table, which return an integer value. The user running the query sees a dialog box with a drop-down list from which to select the argument.

Selection	Return Value (an Integer)
Users	iUserNum in SDUser
Tokens	iTokenNum in SDToken
Groups	iGroupNum in SDGroup
Sites	iSiteNum in SDSite
Profile	iProfileNum in SDProfile
Agent Hosts	iClientNum in SDClient
Task Lists	iTaskNum in SDTaskList

Note: You cannot use arguments as columns in a SELECT statement.

Using Conditional Clauses to Validate User Input

If you have a query that requires the user to enter an argument before continuing, you need a way to validate the input provided by the user.

To do so, you can use conditional clauses IF, THEN, ELSEIF and ELSE. The general construction of conditional statements is:

```
IF condition THEN
  statement
[ELSEIF condition THEN
  statement]
ELSE
  statement
```

As shown, a conditional statement must have an IF clause, a THEN clause, and an ELSE clause. The ELSEIF clause is optional, and can be used to add multiple conditions to the construct. You are limited to a maximum of 32 clauses in a conditional statement.

To understand how a conditional construct might be used to validate user input, recall an example used in one of the previous sections:

```
SELECT chDefaultLogin, chLastName, chFirstName FROM SDUser
WHERE LENGTH(chDefaultLogin) < ARG01
```

This simple query outputs users whose default login is less than the number of characters specified by the person who runs the query.

To prevent too large or too small a number from being entered by the query user, however, you could use conditional clauses. For example:

```
IF ARG01 < 1 OR ARG01 > 16 THEN
MESSAGE "Please enter a number between 1 and 16"
ELSE
SELECT chDefaultLogin, chLastName, chFirstName FROM SDUser
WHERE LENGTH(chDefaultLogin) < ARG01
```

This query ensures that a reasonable argument is entered by the user, generating reasonable output from the query.

Because conditions are evaluated in order from top to bottom, it is important to implement input checking clauses at the beginning of the condition. You can then follow them with the conditions that execute the actual SELECT statements. The sample query, “Administrators with a Specified Task List,” is a good example of this:

```
IF ARG01 = 0 THEN
MESSAGE "Select a Task List"
ELSEIF iMyGroup <> 0 OR iMySite <> 0 THEN
MESSAGE "You must be a Realm Administrator to run this query"
ELSE
SELECT chDefaultLogin, chLastName, chFirstName FROM SDUser
JOIN SDAdministrativeRole ON SDUSer.iUserNum =
SDAdministrativeRole.iUserNum WHERE
SDAdministrativeRole.iListNum = ARG01 ORDER BY
SDUser.chDefaultLogin
```

The query verifies that the user has selected a task list and verifies that the user is a realm administrator. Only then is the SELECT statement executed.

Conditional clauses can also be used for more than input validation. You can construct complex queries that execute one of multiple possible SELECT statements based on user input. A number of the sample queries use conditional clauses for this purpose. An excellent example is the query named "Users with Tokens (with Wildcards)."

Another use of conditional clauses is to implement administrative scoping in your queries. This is described in more detail in "Administrative Scoping in Custom Queries" on page 207.

Using Global Constants in Expressions

In addition to arguments, the Custom Query tools include a defined set of global constants that you can use in expressions. These are listed in the following table:

Name	Type	Value
iMyLogin	number	iUserNum of the current administrator.
iMyGroup	number	The **iGroupNum** of the current administrator's group (if he or she has group scope). Otherwise, a value of zero for realm and site administrators is returned.
iMySite	number	The **iSiteNum** of the current administrator's site (if he or she has site scope). Otherwise, a value of zero for realm and site administrators is returned.
chMyLogin	string	Default login of the current administrator.
chMyGroup	string	Group name of the current administrator's group (if he or she has group scope). Otherwise, an empty string is returned.
chMySite	string	Site name of the current administrator's site (if he or she has site scope). Otherwise, an empty string is returned.
LocalTimeNow	number	The number of seconds after midnight of local time.
LocalDateNow	date	The current local date in mm/dd/yyyy format.
GMTTimeNow	number	The number of seconds since midnight of Greenwich Mean Time (also known Coordinated Universal Time, or UTC)
GMTDateNow	date	GMT date in mm/dd/yyyy format.

See the sample queries for numerous examples employing these global constants. For more information about constants used for administrative scoping, see "Administrative Scoping in Custom Queries" on page 207.

Note: You cannot use global constants as columns in a SELECT statement.

Advanced Application Notes for Custom Queries

This section provides additional tips, techniques, and recommendations for best practices in using Custom Queries.

Administrative Scoping in Custom Queries

For security reasons, creating and sharing custom queries with other administrators can only be done by Realm Administrators (those with the highest access level). This is mainly to prevent lower-level (Site and Group) administrators from having access to sensitive data.

There are two ways to employ administrative scoping in custom queries:

Including scoping conditions in the actual SQL code of the query. You can build administrative scoping directly into the SQL code of the custom query. Depending on the administrative level of the person running the query, the query can be structured to perform different activities. There are three levels of administrator in the RSA Authentication Manager environment—Realm, Site, and Group administrators (in descending order of **scope**).

To build scoping into a query, you can use the global constants, iMySite and iMyGroup with the following logic:

- To determine that the current user is a Realm Administrator, verify that both iMySite and iMyGroup are equal to zero (0).
- To determine that the current user is a Site Administrator, verify that iMySite is not equal to zero and iMyGroup is equal to zero.
- To determine that the current user is a Group Administrator, verify that iMyGroup is not equal to zero.
- If both iMySite and iMyGroup are not equal to zero, then the current user is the Group Administrator of the group within the site. Fields **chMyGroup** and **chMySite** would then contain the group and site names of this particular Group Administrator.

The **SDUserScope** table in the RSA Authentication Manager user database keeps track of the scope of all users. You can use this table in queries to select the user records of Site and Group Administrators. For Site Administrators, use the following syntax:

```
SELECT chDefaultLogin, chLastName, chFirstName FROM
SDUserScope WHERE SDUserScope.iSiteNum = iMySite
```

Similarly, for Group Administrators, you could use this syntax:

```
SELECT chDefaultLogin, chLastName, chFirstName FROM
SDUserScope WHERE SDUserScope.iGroupNum = iMyGroup
```

For examples of administrative scoping in queries, refer to the sample queries, "Administrators with a Specified Task List," "All Administrators," "Group Administrators" and "Site Administrators."

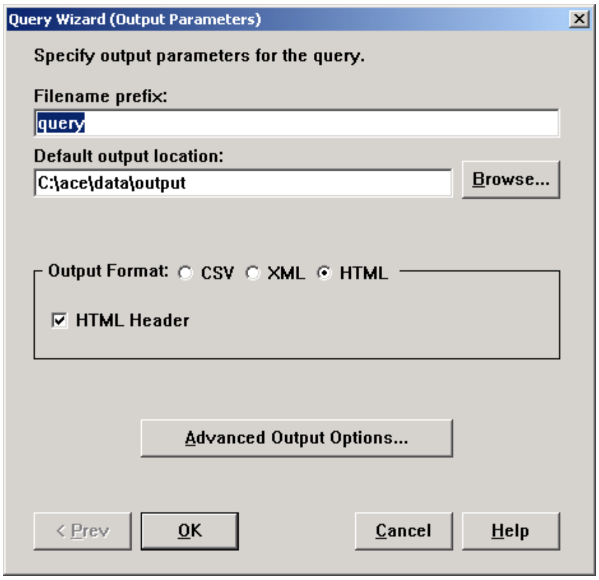
Specifying query access level in the Query Wizard. In the Query Wizard, you can specify the site and group administrators allowed access to a query that you share out to a common location on your network.

In the **Query Access Level** dialog box, you can specify **None** or **All** for Site and Group Administrators, or select a specific site and group whose administrators can access the query. Then, even if you share the query to a common location on your network, only those administrators who have access can see and run the query.

For information about setting scope in the Query Access Level screen, see the Help. For information about sharing queries, see the Help and "Creating a Central Repository for Shared Queries" on page 210.

Formatting Output for Use with Third-Party Reporting Tools

When you create or edit a query, or when you run a compiled query, the Query Wizard's Output Parameters screen appears.



Query Wizard (Output Parameters)

Specify output parameters for the query.

Filename prefix: query

Default output location: C:\ace\data\output

Output Format: ○ CSV ○ XML ● HTML

☑ HTML Header

This Output Parameters screen enables you to specify the default output format of the data, as well as other advanced options. At the basic level, you can specify the output format—CSV, HTML, or XML.

When running the query, the user can accept the defaults, or specify their own parameters.

The format to select depends on the program with which you want to view the data. The CSV (comma-separated values) format is ideal for importing into spreadsheet programs such as Microsoft Excel.

For viewing the data in a web browser, select HTML as the output format. For viewing in reporting products such as Crystal Decisions' Crystal Reports, select XML.

When you select an output format, the options specific to the format change, as described in the following table:

Format	Options	Description
CSV	CSV Header	Determines whether the column names defined in the query appear in the output file.
	Separator	Defines the character used to separate the values in the CSV output. The default is the comma character.
	Qualifier	Defines the character used to denote the beginning and the end of each field in the CSV output.
HTML	HTML Header	Determines whether the column names defined in the query appear in the HTML output file.
XML	XML Tag	Defines the XML title of the report. This is useful for an XML processing application such as Crystal Decisions' Crystal Reports.
	Column names as tags	Specifies that column names will be included as XML tags. If not selected, the column tags will be fields from the database.

From the Output Parameters screen, click **Advanced Output Options** to display another dialog box with additional selections. Here, you can specify:

- A limit to the number of records that will be output
- The program to launch for viewing the data immediately after running the query
- Whether special characters not valid for the specific output format are to be removed or substituted

Best Practices for Table Joins

In general, running a query that uses multiple JOIN statements can use a great deal of a computer's CPU cycles, particularly when the joins involve large tables in your database.

If you run such queries directly on a Primary or Replica, this could impact overall Authentication Manager performance in database reconciliation, replication, and authentication.

Following are some guidelines for using table joins efficiently:

- Use explicit joins. Avoid implicit joins, because they are slower and less efficient.
- When joining two tables, join the table with fewer records to the table with more records. A good example is the "Activity of a User" sample query, which joins the SDToken table to the SDLogEntry table.
- Do not mix left and right joins.

- You can mix inner and left outer joins to join multiple tables. The most efficient mix specifies inner joins all together in one series first (on the left), followed by all left outer joins in a second series (on the right).

How Queries Are Stored and Organized

By default, queries are stored in a subdirectory in the ***ACEDATA*** folder, typically:

```
c:\ace\data\queries
```

Each query is in a subdirectory to that pathname. The name that you specify for a new query actually determines the name of the subdirectory in which it is stored. For example, a query named "my_first_query" would be located at:

```
c:\ace\data\queries\my_first_query
```

The actual files related to the query, in this example, would be stored in the "my_first_query" folder. Files related to a query are described in the following table.

Filename	Contains	Comments
definition.txt	The uncompiled query, including the arguments, conditions, statements, description, access level and configuration information	This is a fixed name. It is created in the query name folder when you click **Finish** from the Query Wizard. Only an uncompiled query can be shared with other realms or for compilation on another platform (by manually sharing the **definition.txt** file).
query.r	The compiled query	Only a compiled query can be run.
runtime.txt	Instructions entered the last time the query was run, such as output format, output folder, and so on.	The query must be run at least once for this file to appear.
acquery.r	A query acquired from a shared location	Only a compiled query shared by its creator (a Realm Administrator) can be acquired, and a new subdirectory is created under **c:\ace\data\queries** to store it. No **definition.txt** is included. After the query is run, a **runtime.txt** file appears.

Creating a Central Repository for Shared Queries

If you are the Realm Administrator, and intend to share compiled queries in your organization, you need to set up a directory on your network to which other administrators have access.

In general, the shared repository should be outside of the RSA Authentication Manager installation directory. For example, in Windows the default installation directory for RSA Authentication Manager is **C:\ACE**. Do not create the shared directory in or below this directory tree.

Important: Queries created and compiled on one OS platform cannot be shared and run on computers running a different OS. For example, suppose your Primary and Replicas are running Sun Solaris, and your Remote Administration machines are running Microsoft Windows. Users on the Windows machines will not be able to acquire and run the queries compiled on the Solaris machines.

Running Queries on a Replica

When you install a Replica in your RSA Authentication Manager environment, its primary purpose is to perform authentications.

However, a Replica maintains a copy of the user database locally, and includes the database administration program (both local and remote).

Therefore, you can run Custom Queries on the Replica. You might want to do this if your Primary is temporarily out of service, is under heavy load, and so on.

If you use the Database Administration - Host Mode command on a Replica, any queries that you run search the local copy of the database.

When running queries on a Replica, note the following:

- Because reconciliation of the databases is a background process, the user database (**sdserv**) on the Replica may be somewhat out-of-date with the Primary (typically only a few minutes, but possibly longer during heavy authentication periods).
- The log database (**sdlog**) only holds data related to activity on this specific Replica. Only the log database on the Primary reconciles all activity on all Authentication Managers in the realm.
- The Replica has all the sample queries, but queries developed on other Authentication Managers are not automatically be available.

Managing Queries Among Multiple Realms

After a query is compiled, it is linked to a specific realm. If your site has multiple realms, and you want to share queries across realms, you cannot use the standard Share/Acquire method built into the Custom Queries feature.

In such cases, you could provide the **definition.txt** file to the Realm Administrator of the second realm, who could create a new query based on the definition file. For a procedure to create a query from a **definition.txt** file, see the Help.

If you are the Realm Administrator for multiple realms, however, and want to share your own queries across realms, you need to do some preparation.

Typically, you would manage your realms by logging into each one as necessary using Remote Administration.

Suppose you are logged into one realm, access Custom Queries and compile one of the sample queries, for example, "**Recent User Additions**."

When you log on to a different realm within the same Remote Administration session, and access Custom Queries, you would notice that "**Recent User Additions"** is not shown as one of the available queries. It is only available to the first realm.

To better manage this process, you could make multiple copies of an uncompiled query. For example:

```
Recent User Additions (Realm 1)
Recent User Additions (Realm 2)
Recent User Additions (Realm 3)
```

Now, in Remote Administration, you can log on to each realm and compile the copy that is reserved for the current realm.

Troubleshooting Custom Queries

If you encounter an error message when working with Custom Queries, and the solution is not obvious, see "Messages" on page 300.

10 Additional Administrative Tasks

This chapter discusses additional administrative tasks that you may need to perform, including changing system parameters, modifying system extension data, and customizing authorization procedures.

Changing System Parameters

RSA Security recommends that you familiarize yourself with your RSA Authentication Manager system-level settings, found in the System Parameters dialog box. To view and change these settings, on the System menu, click **System Configuration > Edit System Parameters**. The System Parameters dialog box opens.

The options and fields in the System Parameters dialog box are described in the following list:

Allow agent host auto-registration. This option enables the system to accept information from new Agent Hosts, and to register the new Agent Hosts in the Authentication Manager database without an administrator creating Agent Host records.

This checkbox does *not* control the system's ability to use the other auto-registration features. Even if this checkbox is cleared, Agent Hosts can update their own IP addresses in the Authentication Manager database and update their own **sdconf.rec** files with new configuration information from the Authentication Manager.

For a complete explanation of how to set up your system to enable auto-registration, see "Auto-Registered Agent Hosts" on page 56.

Store time of last login in token records. This setting instructs RSA Authentication Manager to store the last login time of each user in the token record of the token assigned to the user. By viewing the token record, you can determine when the user's last successful authentication occurred. Disabling this feature can improve authentication rates. However, the token record will not be updated when the user authenticates, and you will not be able to determine when the user's last successful authentication occurred.

Allow Push DB Assisted Recovery. If this box is selected, the database files are written automatically ("pushed") whenever a Replica package is generated to the Replica or Replicas specified in the package. This feature can be used to distribute the initial database to newly installed Replicas. It is also useful in recovering the database. See "Recovery Procedures" on page 94 for Windows 2000, Windows XP, or Windows 2003, or "Recovery Procedures" on page 144 for UNIX.

Allow remote administration. This setting enables administration of the RSA Authentication Manager databases from a Windows 2000 Professional, Server, or Advanced Server (Service Pack 4), Windows XP Pro, or Windows 2003 Server machine.

Note: On UNIX platforms, while with the **sdadmin** program you can access most of the features of the RSA Authentication Manager software, Remote Administration provides a graphical user interface for administering an RSA Authentication Manager database and provides the only supported method of accessing all of the administrative features.

Enable Windows password integration at system level. With this option enabled, when users enter an RSA SecurID passcode to a protected resource, and they are authenticated, their login password is automatically sent to the Windows authentication service. This is a system-wide setting and applies to all Agent Hosts running RSA Authentication Agent 6.0 or 6.1 for Microsoft Windows software. For information about overriding this parameter on an Agent-by-Agent basis, see “Setting Offline Authentication and Password Integration for Agents” on page 61.

Administrator Authentication Methods. This setting specifies the methods administrators can use to authenticate. For more information about token types, see “RSA SecurID Tokens and Two-Factor Authentication” on page 14.

PIN Options

- **User-created PINs allowed.** This setting allows both user-created and system-generated PINs.
- **User-created PINs required.** This specifies that users must create their own PINs.
- **Alphanumeric PINs allowed.** This setting enables the system to generate PINs containing letters as well as numbers, and allows users to create PINs that contain letters. Existing PINs, if any, will not be affected. (PINs for RSA SecurID PINPads and software tokens can never contain letters.)
- **Min PIN length: [4].** With this setting, you specify the number of characters the shortest PIN on the system may contain. This number cannot be smaller than four; RSA Security recommends six.
- **Max PIN length: [8].** With this setting, you specify the number of characters the longest PIN on the system may contain. The maximum cannot be greater than eight.

  For information to help you decide the best PIN settings for your system and for step-by-step instructions on how to set the PIN parameter, see “PIN Options” on page 105.

RSA Authentication Manager Date and Time. The Authentication Manager date and time fields show the current date and time. You may need to change the offset on the server if the system clock is out of synchronization with the token clock by more than a few minutes.

> **Note:** Inform all users of any changes made to the system clock offset. In addition, instruct any user attempting to authenticate to wait 60 seconds, so that their tokens can properly synchronize with the Authentication Manager.

- **Set clock offset to 0.** Select this option to remove the system clock offset.
- **Set clock offset by token.** When you click the **Set clock offset by token** button, a browser opens, listing the token serial numbers from which you can select to set the offset. The complete procedure is described in the Help.

  After you have entered a value for the offset, the **Computed offset currently applied** field displays this value.

Modifying System Extension Data

Use the **Edit System Extension Data** option on the System menu to modify information in system extension records. These records contain customer-defined information that can be accessed by custom administration programs.

For information on creating custom administration programs with the RSA Authentication Manager Administration Toolkit, see the *Administration Toolkit Reference Guide* (**authmgr_admin_toolkit.pdf** in the ***ACEDOC*** directory).

To edit system extension data:

1. From the System menu, select **Edit System Extension Data**.

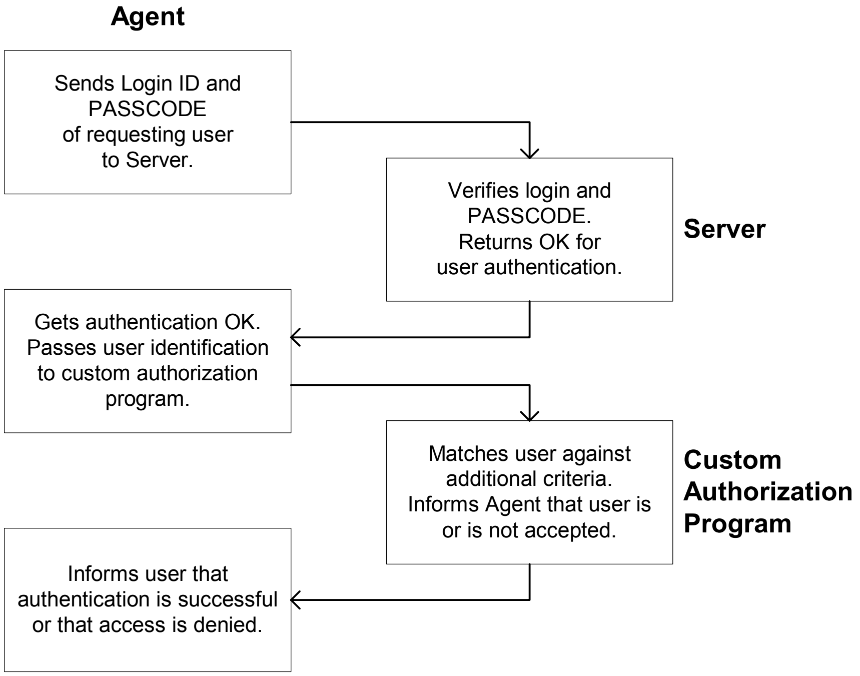
   The Edit System Extension Data dialog box opens and displays the system name and the records defined for the system. Each record consists of a secondary key (up to 48 characters) and data (up to 80 characters).
2. You can add, modify, or delete these records. You can create more than one record with the same key, but you cannot create duplicate records (same key and data values) in one extension database table.
   - To change an existing record, select the record, modify the information displayed in the **Key** and **Data** fields, and click **Save**. (The **Save** button is unavailable until you make an entry in one of these fields.)

     To clear the fields without changing the record, click **Clear**.
   - To create a new record, click **Clear**, if necessary, to clear the **Key** and **Data** fields, enter the information for the new record, and click **Save**.
   - To delete a record, select the record and click **Delete**. Click **OK** to confirm.
3. Click **Exit** to close the Edit System Extension Data dialog box.

Customizing Your Authorization Procedures

External Authorization allows you to use a generic Application Programming Interface (API) to customize criteria for authorizing users within your organization. This customized authorization is an addition to RSA Authentication Manager authentication, not a replacement for it. When External Authorization is enabled, users attempting access must meet additional criteria before they are permitted access to your system.

The following diagram illustrates the way an RSA Authentication Agent handles an authentication request in a system that includes External Authorization:


Agent
Sends Login ID and PASSCODE of requesting user to Server.
Verifies login and PASSCODE. Returns OK for user authentication.
Server
Gets authentication OK. Passes user identification to custom authorization program.
Matches user against additional criteria. Informs Agent that user is or is not accepted.
Custom Authorization Program
Informs user that authentication is successful or that access is denied.

When a user tries to access the system, the Agent and Authentication Manager conduct the usual authentication exchange. After the user is authenticated, the External Authorization process begins. Using criteria that you have defined, the program determines whether or not the authenticated user is granted access.

For example, the authenticated user might be checked against a list of employees who are currently checked in on a secure site.

If the External Authorization remote login option is enabled, the same custom criteria can be applied to users who request authentication from a remote realm.

Note: In a cross-realm authentication environment, you must either enable External Authorization or disable External Authorization in all participating realms. If External Authorization is enabled in some realms and disabled in others, cross-realm authentication will fail. For information about cross-realm authentication, see Chapter 4, "Realm Administration."

RSA Security does *not* provide specific External Authorization code. You must first create your own External Authorization routines based on a template source file, then substitute your customized routines for the four stubbed routines supplied by RSA Security. Your customized routines must meet these requirements:

- They must conform to the External Authorization API.
- They must define an authorization scheme that integrates closely with the RSA Authentication Manager authentication process.

For more information on installing and customizing External Authorization, see the *External Authorization API Guide* (**authmgr_authorization_api.pdf** in the ***ACEDOC*** directory).

Choosing External Authorization Options

When you choose one or both of the options in the Authorization Information dialog box, you enable authorization criteria that have already been defined for your system.

To enable External Authorization:

1. Click **System** > **Edit Authorization Parameters**.

   The Authorization Information dialog box opens. By default, External Authorization is disabled.

2. Select **Enable External Authorization** so that users can log on the local system.

   When only the **Enable External Authorization** option is enabled, users who meet the authorization criteria can log on the local system. Users cannot log on from remote systems.

3. Select **Enable Authorization of Remote Login Requests** so that users can log on from a remote location as well as from a local one.

   Note: You must select **Enable External Authorization** before you can select **Enable Authorization of Remote Login Requests**.

   When **Enable Authorization of Remote Login Requests** is selected, users from remote realms are first authenticated, then checked locally against custom criteria retrieved from their home realms before they are granted access.

4. Before the options you chose can take effect, the Authentication Manager must be stopped and restarted. Click **Start** > **Settings** > **RSA Security > RSA Authentication Manager Control Panel**.

Stopping and Restarting External Authorization

If External Authorization fails, subsequent requests for authentication are denied until External Authorization is disabled or the Authentication Manager is restarted.

To stop External Authorization:

1. From the System menu, select **Edit Authorization Parameters**.

   The Authorization Information dialog box opens.
2. Clear the **Enable External Authorization** checkbox.
3. Restart the Authentication Manager from the Control Panel.

To restart External Authorization:

1. Enable External Authorization.

   For instructions, see “Choosing External Authorization Options” on page 217.
2. Restart the Authentication Manager from the Control Panel.

   External Authorization is now enabled.

11 Program and Data Files

This chapter describes the components that work together to protect your system, including RSA Authentication Manager programs, RSA Authentication Agent programs, and RSA Authentication Manager data.

RSA Authentication Manager Software

Installed on the RSA Authentication Manager machines are programs that provide

- Configuration tools
- Continuous authentication service for protected network resources
- Tools for administering the RSA Authentication Manager system and its data
- Real-time monitoring of authentication and administrative activity

This section describes the functions performed by the RSA Authentication Manager programs.

Configuration Management

The Configuration Management application is used to configure an RSA Authentication Manager system and to modify configuration values. For information about changing configuration data, see Chapter 12, "Configuring the RSA Authentication Manager (Windows)."

Authenticating Users

The RSA Authentication Manager Authentication service works with RSA Authentication Agent software to authenticate users. The Replication service is launched when the Authentication service is started on the Primary Authentication Manager.

The Agent Host prompts a user for an RSA SecurID passcode and sends the user's response to the Authentication service, which checks to see if the user is registered in the Authentication Manager database and if the passcode is valid for one of the user's tokens. On the basis of this information, the Authentication service directs the Agent Host to grant or deny access.

Administering the Database

An authorized RSA Authentication Manager administrator can perform tasks such as adding users, assigning tokens, running activity reports, and purging old log records. Administrative tasks can be performed on a Primary machine or on a machine set up to do Remote Administration.

RSA SecurID authentication is not required to run the Database Administration application in host mode on the Primary. Instead, the program checks to make sure that the user has permission to access the directory in which the Authentication Manager software is installed. However, anyone who attempts to administer an Authentication Manager database remotely must first pass authentication. This is impossible unless the administrator uses an RSA SecurID token that is registered in the RSA Authentication Manager database he or she wants to administer.

The functions of the Database Administration application are described throughout this manual. To find instructions for a specific administrative task, use the Table of Contents or the Index.

Programmers can use the Administration Toolkit to create customized administration programs. For more information, see the *Administration Toolkit Reference Guide* (**authmgr_admin_toolkit.pdf** in the ***ACEDOC*** directory).

Monitoring Activity in Real Time

Real-time log monitoring can be initiated from within the Database Administration application. From the Report menu, select **Log Monitor**. You can also run log monitoring on the Primary.

To Begin: Click **Start** > **Programs** > **RSA Security > RSA Authentication Manager Log Monitor**. For more information, click **Help**.

Determining Realm Status

Use the **_aceping** command to send a message to each realm in the database of an RSA Authentication Manager. The **_aceping** command determines whether realm-to-realm communication is working and whether encryption and decryption are being performed correctly. Each pinged realm responds with its realm status. The **_aceping** output is displayed on the screen.

You can run **_aceping** only from the command line prompt of the Primary.

Note: On UNIX systems, the command is **aceping**.

Command Line Arguments

To run **_aceping**, type:

```
ACEPROG\_aceping number_of_times interval 0
```

The italicized words represent values you supply. The following table explains each parameter.

Parameter	Explanation
number_of_times	Number of times a **ping** request is broadcast. Execution stops after the last ping request is sent. A zero (0) setting repeats the command until you stop it.
interval	Number of seconds between pings.
0	Use zero (0) to represent the port number. The **_aceping** command fills in the authentication port number that is registered in the **sdconf.rec**.

For example, if the ***ACEPROG*** directory is **ace\prog**, enter:

```
ace\prog\_aceping 0 5 0
```

This command pings the realms every five seconds until you stop the command.

The _aceping Output

The output of **_aceping** consists of information about ping requests and ping responses.

Each request packet includes the following items:

- Time sent
- Request ID
- Information about the pinged realm (realm name, whether the Authentication Manager is a Preferred or a Failover Server, the primary network address, and the port number).

Each response packet includes the following items:

- Time received
- Request ID
- Responding realm name, whether the Server is a Preferred or a Failover Server, the network address from which the response was sent, the port number, and the primary network address if the response was received from a secondary node.
- Round trip time
- **_aceping** port number
- Status and error messages

RSA Authentication Agent Software

The following types of hardware and software resources can run RSA Authentication Agent software and be configured for RSA SecurID protection:

- Windows NT, Windows 2000, Windows XP, and Windows 2003 workstations and servers
- Sun Solaris, HP-UX and IBM AIX UNIX workstations
- Novell NetWare Connect and Novell NMAS (Novell Modular Authentication Service) servers
- iPlanet web servers
- Lotus Domino web servers
- Custom applications that call the RSA Authentication Manager Authentication API
- Communication servers, VPN servers, firewalls, routers, and other devices and applications with integrated RSA Authentication Agent code

For more information about RSA Authentication Agents, go to the RSA Security web site at **www.rsasecurity.com/node.asp?id=1174**.

The RSA Authentication Agent software is made up of several programs, including an authentication dialog program and a program that displays configuration information. This section briefly describes the functions performed by these programs. For more information about Agent software, see the documentation that came with the downloaded file.

User Authentication Dialog

RSA Authentication Agent 6.1 software works with the RSA Authentication Manager to identify and authenticate users. Rather than the standard Windows logon screen, the user is prompted for their logon name and an RSA SecurID passcode.

Note: With older Agents, when a user logs in to an Agent Host machine, he or she provides a login (and password if required). The Agent Host checks to see if this login has been designated for RSA SecurID authentication. If so, it prompts the user to enter a passcode.

The user's response is sent to the Server for verification that the user is authorized to use the Agent Host machine. If the passcode is valid and the user is activated on this Agent Host, the Server sends this information to the Agent Host. The Agent Host displays this message to the user:

```
PASSCODE accepted
```

If the passcode is invalid or if there is any reason why the user should not be granted access (if, for example, the token is disabled or the Agent Host is restricted and the user has not been activated on it), the Agent Host displays this message:

```
Access denied
```

For help in dealing with access denials, see Appendix C, "Troubleshooting."

Displaying Configuration Information

On an RSA Authentication Manager machine, the Configuration Management application displays the contents of the **sdconf.rec** file. On an RSA Authentication Agent for Microsoft Windows, use the Authentication Test feature to see this information. On an Agent for UNIX, run **sdinfo**. On other Agents, run the appropriate utility.

If both the RSA Authentication Manager and Agent software are installed on one Windows 2000, Windows XP, or Windows 2003 machine there are two **sdconf.rec** files, one in the ***ACEDATA*** directory and one in the ***%SYSTEMROOT%*\system32** directory.

For information about the full contents of the configuration record, see Chapter 12, "Configuring the RSA Authentication Manager (Windows)".

Automated Agent Host Registration and Updating

The **sdadmreg** utility enables new Agent Hosts to register themselves in the Server database. It also enables existing Agent Hosts to update their own IP address in the Server database if the address is changed through DHCP and to update their own **sdconf.rec** files if they detect Authentication Manager configuration changes. For details, see "Automated Agent Host Registration and Updating" on page 65.

Encryption and Decryption of Communications

Communications between Agent Hosts and RSA Authentication Managers and between realm Authentication Managers for cross-realm authentication are encrypted to protect against masquerading and electronic eavesdropping. Before an Agent Host sends an authentication request message to the Authentication Manager, it encrypts the data using a "node secret," which is a string of pseudorandom data known only to the Agent Host and the Authentication Manager. For more information about the realm secret, see "Node Secret File" on page 228.

A realm Authentication Manager encrypts authentication request messages that it sends to another realm Authentication Manager using a "realm secret" that is known only to the two Authentication Managers. For more information about the realm secret, see "Creating and Modifying Realms" on page 85.

When an Authentication Manager receives a request, it can decrypt the request because it knows the node or realm secret (and certain other information). The same process is followed for communication in either direction. Both parties (whether they are both Authentication Managers or one is an Authentication Manager and the other an Agent Host) use the same secret for encryption and decryption.

A mismatch between the node secret stored on an Authentication Manager and the one stored on an Agent Host can occur if you delete and re-create an Agent Host or if you accidentally delete a node secret file. The mismatch prevents messages between the devices from being decrypted and causes the Agent Host to deny access to all users who attempt to log in. **Node Verification Failed** is recorded in the audit trail. If this occurs, see "Node verification failed (137)" on page 358.

Similarly, the realm secret for a remote realm can be lost if the local realm record is removed and reinstalled. The local Authentication Manager denies access to all users attempting to log in from the other realm, and **Could not decrypt XR message** is recorded in the audit trail. If this occurs, see "Could Not Decrypt XR Message (8220)" on page 330.

RSA Authentication Manager Data

RSA Authentication Manager data is stored on the Authentication Manager machine in the Authentication Manager and log databases and in the **sdconf.rec** and **license.rec** files. These databases and files are described in this section.

Authentication Manager Database

The Authentication Manager database contains system parameters; token and user records; and Agent Host, realm, site, and group information. The Authentication Manager database contains these files:

sdserv.b1
sdserv.d1
sdserv.db
sdserv.lg
sdserv.st
sdserv.vrs

An additional file, **sdserv.lk**, exists when the database is in use.

These **system parameters** are stored in the Authentication Manager database:

- Whether or not auto-registration of Agent Hosts is allowed
- Whether or not replaced tokens will be deleted automatically from the database
- The number of days until all user passwords expire
- Whether or not the database can be administered remotely
- Which administrator authentication methods are allowed
- Whether PINs are of a fixed length or of varying lengths
- Whether PINs are alphanumeric or numeric

The database stores **Agent Host** records that include the following information for each Agent Host:

- Agent Host name and IP address
- Whether or not the Agent Host is open to all users
- Lists of authorized users and groups of the Agent Host if it is not open to all users

Token records are stored in the Authentication Manager database. Each RSA SecurID token record contains unmodifiable information about the token itself, such as the following:

- Token type: RSA SecurID standard card, PINPad, key fob, software token (formerly SoftID)
- Serial number

- Length of the code the token displays
- How frequently the code changes
- Whether or not the token is in New PIN mode

For a complete list of token record contents, see "Contents of a Token Record" on page 118.

Realm records include information about other realms in the cross-realm network, such as the following:

- Primary network name and IP address
- Replica network name and IP address
- A text description of the realm
- Whether or not realm trust has been established

User records, also stored in the Authentication Manager database, contain the following information that can be set by an administrator through the Database Administration application:

- Assigned user's name
- User's login
- Between what dates the user can log in
- Home realm information for remote users

For a complete list of user record contents, see "Contents of a User Record" on page 116.

Log Database

The RSA Authentication Manager logs a record for each authentication attempt and for each action taken through the Database Administration application. This audit trail is stored in the log database, made up of the following files:

sdlog.b1
sdlog.d1
sdlog.db
sdlog.lg
sdlog.st
sdlog.vrs

An additional file, **sdlog.lk**, exists when the database is in use.

Using the Database Administration application, an administrator can run a variety of reports on log data for such purposes as the following:

- To learn of potential security problems
- To investigate security breaches
- To help a user who is having trouble logging in

For information about producing reports, see Chapter 9, "Reports."

Important: The only limit on the size of the log database is the disk space available on your Authentication Manager machine. *Do not allow the database files to grow indefinitely nor allow the disk to become more than 90 percent full.* Back up the files regularly and then purge old log records. For more information, see Chapter 8, "Maintaining the Log Database."

The sdconf.rec File

The RSA Authentication Manager configuration file, **sdconf.rec**, is created by the installation process. Information in the file can be viewed and modified on the Authentication Managers using the Configuration Management application. The **sdconf.rec** file is stored in the ***ACEDATA*** directory on each Authentication Manager.

To Begin: Click **Start** > **Programs >RSA Security > RSA Authentication Manager Configuration Tools > RSA Authentication Manager Configuration Management**. For information about configuration values, click **Help** or see Chapter 12, "Configuring the RSA Authentication Manager (Windows)," or Chapter 14, "Configuring the RSA Authentication Manager (UNIX)."

Configuration Files for Agent Hosts

When an Agent Host is installed, you must generate a configuration file and copy it to the Agent Host (unless the Agent Host is a third-party device with integrated RSA Authentication Agent code and its own configuration record). The configuration file in the Authentication Manager's ***ACEDATA*** directory is the template for all configuration files that you generate for Agent Hosts.

To Begin: After starting the RSA Authentication Manager Database Administration application, click **Agent Host** > **Generate Configuration Files**. For instructions, click **Help**.

Configuration files for legacy Agent Hosts must contain information about the Acting Master and Acting Slave Authentication Managers that process authentication requests from legacy Agent Hosts. You must designate an Acting Master and an Acting Slave Authentication Manager for legacy Agent Hosts. For more information, see "Authentication Manager and Agent Host Communication Through Firewalls" on page 25.

To Begin: Click **Agent Host** > **Edit Agent Host** > **Assign Acting Servers**. For instructions, click **Help**.

You can also use the **sdcfgedit_ui.exe** utility in the ***ACEPROG*** directory to designate the Acting Master and Acting Slave in a configuration file. For more information, see "Legacy Agent Hosts" on page 75.

The Primary, Replica, and all Agent Hosts must have compatible configurations or the machines cannot communicate. For more information, see the explanation of the error message "Cannot initialize Agent Host-server communications" on page 320.

The license.rec File

When your organization purchases RSA Authentication Manager, the package includes a diskette containing your site-specific license file (**license.rec**). The settings in the **license.rec** file are based on your organization's license agreement with RSA Security.

RSA Authentication Manager 6.1 uses the Version 4 license record, which enables license compliance to be checked and enforced. Releases of RSA ACE/Server prior to 5.1 used Version 3 **license.rec** files. If you upgraded from one of those releases, the Setup program converts your original **license.rec** to a Version 4 format.

To display the data in your license.rec file in RSA Authentication Manager 6.1:

Do one of the following:

- On Windows:

  From the Primary or a Replica, or from a machine configured for Remote Administration, click **Start > Programs > RSA Security > RSA Authentication Manager Configuration Tools > RSA Authentication Manager Configuration Management**.
- On UNIX, type:

  ```
  Run ACEPROG/sdinfo
  ```

The Configuration Management settings contain the following information about your license:

Note: For the exact license information contained in the RSA Authentication Manager 6.1 for UNIX Configuration Management settings, see "Understanding Your RSA Authentication Manager Configuration" on page 252.

License. The type of license you have been issued—**Base** or **Advanced**.

Status. Whether your license is **Permanent** or **Evaluation**.

Expiration Date. Usually **None**, but can also be an actual date if the license has Violation or Evaluation status.

Licensed Active Users. The number of RSA SecurID active users that can be within your realm at any one time.

For information about active users, see "Upgrading or Converting Your License" on page 280.

Licensed Replicas. The number of Replica servers you are allowed—**1** with a Base License, **10** with an Advanced License.

Licensed Realms.The number of Realms you are allowed—**1** with a Base License, **6** with an Advanced License.

On Windows, the Configuration Management dialog box also has a **More** button under License Information. When you click **More**, another dialog box opens with these additional entries:

License Created. The date (*mm/dd/yy*) on which the license was created.

License ID. This is your unique customer identifier. You may be asked for this number when you contact RSA Security Customer Support.

Licensee. Your organization's name and address.

For a complete overview of RSA Authentication Manager licensing, see Appendix A, "Licensing."

Node Secret File

Packets exchanged between an Agent Host and the Authentication Manager are encrypted using a node secret, which is a pseudorandom string known only to the Agent Host and the Authentication Manager, in combination with other data. You create and send the node secret file through Automatic or Manual Delivery.

Note: A missing or mismatched node secret makes communications between the Agent Host and the RSA Authentication Manager impossible. If such a mismatch occurs, the system logs a **Node Verification Failed** error. For information on how to correct the error, see "Node verification failed (137)" on page 358.

Best Practices for Automatic Delivery

If you use Automatic Delivery, which is the default setting, the Authentication Manager automatically creates and sends the node secret to the Agent Host in response to the first successful authentication on the Agent Host. The transmission containing the node secret is encrypted with a key derived from the user's passcode in combination with other information.

- Windows Agents with a version of 4.4.0 or later store the node secret file in the system registry.
- Windows legacy Agents (other than 4.4.0) store the node secret file in the ***%SYSTEMROOT%*\system32** directory.
- All UNIX Agents store the node secret file in the in the ***ACEDATA*** directory.

The default name of the node secret file is **securid**.

In the case of Automatic Delivery, capture of the node secret is possible if you are not careful to control the circumstances in which the first authentication on each Agent Host occurs.

- The Agent Host should *not* be set to **Open to All Locally Known Users** until the node secret delivery has taken place. Only the administrator should be able to authenticate on that Agent Host. This parameter can be set in the Add Agent Host dialog box. For instructions, see Chapter 3, "Agents and Activation on Agent Hosts."

- If your system uses **telnet** or **rlogin** for remote users, prevent theft of the node secret by ensuring that the first authentication on a new Agent Host is never done remotely. If the first user to be authenticated is connected to the Agent Host remotely, through an application such as **telnet** or **rlogin**, the user's passcode is sent in the clear, where an attacker can easily intercept it and use it to derive the node secret.
- You can greatly increase the decryption time and significantly diminish your vulnerability to attack by ensuring that the first authentication is done with the longest possible passcode — 12 characters or more.

As the administrator, you can maximize your protection against attack by performing the first authentication yourself, making sure to do it locally and to use a token with a sufficiently long PIN.

Best Practices for Manual Delivery

If you choose to send the node secret manually, you must prompt the Authentication Manager to create the node secret. You then deliver the node secret to the Agent Host (on a disk, for example) and use the Node Secret Load utility to load the node secret onto the Agent Host. The node secret is password protected.

When you run the Node Secret Load utility on the Agent Host, the utility decrypts the node secret file, renames the file after the authentication service name (usually **securid**), and then stores the the renamed file in the ***%SYSTEMROOT%*\system32** directory on Windows machines and the ***ACEDATA*** directory on UNIX machines.

- 4.4.0 and later Agents copy the renamed node secret file from the ***%SYSTEMROOT%*\system32** directory to the system registry and delete it from the ***%SYSTEMROOT%*\system32** directory.
- Legacy Agents (other than 4.4.0) leave the renamed node secret file in the***%SYSTEMROOT%*\system32** directory.
- All UNIX Agents leave the renamed node secret file in the in the ***ACEDATA*** directory.

With manual delivery, once you have created the node secret it is up to you to deliver it to the Agent Host. For security purposes, follow these guidelines:

- Use the longest possible, *alphanumeric* password—12 characters or more.
- If possible, deliver the node secret on a *floppy disk* to the RSA Authentication Agent administrator, and verbally deliver the password. Do not write down the password. If you choose to deliver the node secret through e-mail, deliver the password separately.
- Make sure all personnel involved in the node secret delivery are *trusted* personnel.

For additional information about creating and sending the node secret file, see the Help topic "Creating a Node Secret."

Database Reconciliation

When communication is reestablished between the Primary and Replicas after an interruption during which one or both Authentication Managers have operated independently, the databases are reconciled. Once reconciliation is complete, the **sdserv** databases on the Primary and Replicas contain the same information.

Note: The reconciliation process does not give the record updates and counts unless the **SDI_ASD_SYSLOG** environment variable is set. If data was altered, by default the reconciliation process provides a message indicating that a reconciliation pass was completed. To enable detailed system event log messages, set the **SDI_ASD_SYSLOG** environment variable before starting the database broker servers. To set the **SDI_ASD_SYSLOG** environment variable, click **Control Panel > System Properties > Environment.** On Windows, set this as a system variable, and restart your system for the changes to take effect.

To reconcile databases, the synchronization service (**syncsrvc**) follows these rules:

Log record changes. All log records written by the Replica are added to the Primary database during reconciliation. The Primary sends no log records to the Replica database.

Agent Host record changes. After reconciliation, Agent Host records contain the most recent node secret status information, whether it comes from the Primary or the Replica. All other information in Agent Host records is taken from the Primary database.

Token record changes. During reconciliation, **syncsrvc** compares the Primary copy of each token record with the Replica copy. If the copies do not match, the action depends on which items differ:

- If **token assignment** differs, the Primary version is preferred. The entire token record is sent to the Replica database. No more fields are compared.
- If **last login attempt** differs, the token record with the more recent last login attempt determines the post-reconciliation values for the following fields: **Bad PIN count**, **Bad PASSCODE count**, **Next Tokencode mode**, and **Time Synchronization value**.

  This rule has one exception: if the last login attempts on both the Primary and the Replica were unsuccessful, each field is compared and the greater **Bad PIN** and **Bad PASSCODE** counts are stored, the Synchronization value in the Primary copy is stored, and **Next Tokencode mode** is turned on if either copy has it on.
- If the token's **enabled status** differs, the more recent change becomes the post-reconciliation status.
- If the token's **New PIN status** differs, the more recent change becomes the post-reconciliation status.
- If **PIN** information differs, the more recent PIN is preferred.

Note: Using similar rules, **syncserv** also reconciles user records and one-time password records.

Errors. If an error occurs during reconciliation (for example, a transmission time-out or locking error), the current transaction is not written to the database.

Summary and status messages are sent to the Event log during reconciliation. For example:

```
...Primary Sent 1 System Changes to the Replica
...Primary Sent 100 User Changes to the Replica
...Primary Sent 200 User Changes to the Replica
...Primary Sent 342 User Changes to the Replica
...Primary Sent 100 Token Changes to the Replica
...Primary Sent 200 User Changes to the Replica
...Primary Sent 300 User Changes to the Replica
...Primary Sent 403 User Changes to the Replica
...Primary Sent 11 Agent Host Changes to the Replica
...Primary Sent 10 Group Changes to the Replica
```

A more complete sample Event log of reconciliation transactions appears in "Sample Event/System Logs" on page 291.

Viewing RSA Authentication Manager Installation and Patch Information

From the RSA Authentication Manager Control Panel on any Primary, Replica, or Remote Administration machine, you can view

- Details about your current installation
- Details about any patches or hot fixes you have installed

To view installation and patch information:

1. Click **Start** > **Programs** > **RSA Security** > **RSA Authentication Manager Control Panel**.
2. From the Control Panel menu, select **View Installation & Patch Information**.

12 Configuring the RSA Authentication Manager (Windows)

This chapter describes RSA Authentication Manager configuration management.

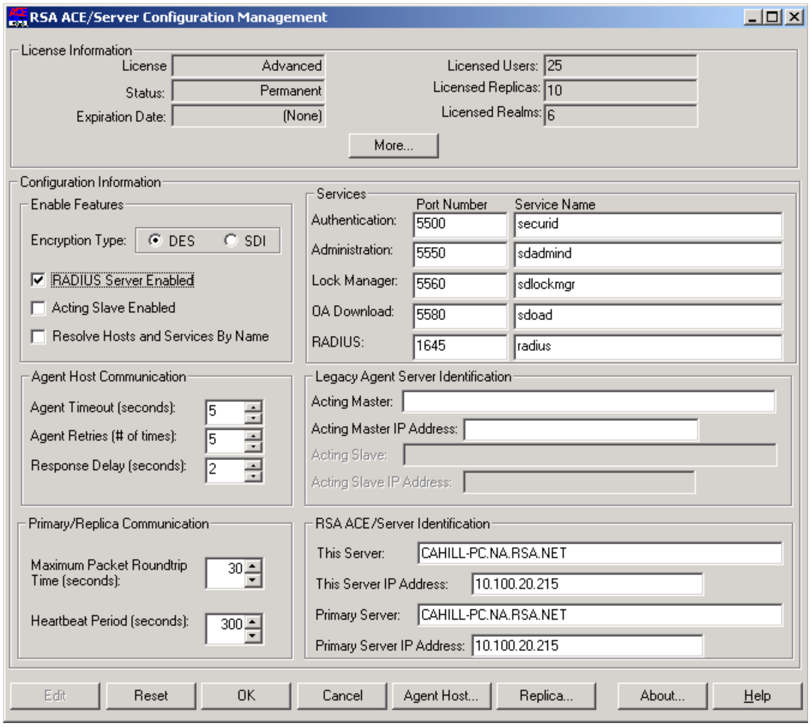
RSA Authentication Manager configuration information is stored in the **sdconf.rec** file in the Authentication Manager's ***ACEDATA*** directory. The configuration record contains information about RSA Authentication Manager services, Agent Host and Authentication Manager communication, Authentication Manager identification, and the features you have enabled on your system.

When an Agent Host is installed, you must use the Database Administration application to generate a configuration file and copy that file to the Agent Host (unless it is a third-party device with RSA Authentication Agent code and its own configuration record). The **sdconf.rec** file stored in the ***ACEDATA*** directory on the Primary Authentication Manager is the template for the configuration files you distribute to Agent Hosts.

CAUTION: Do not copy the **sdconf.rec** file directly from the ***ACEDATA*** directory to an Agent Host. By generating a new configuration record, you ensure that the **sdconf.rec** file on the new Agent Host includes needed information that you may have entered, such as Acting Master/Acting Slave information (required to support legacy Agent Hosts) or alias IP address information (required to support authentication through firewalls).

To display or modify the current configuration settings of your RSA Authentication Manager system, click **Start** > **Programs > RSA Security > RSA Authentication Manager Configuration Tools > RSA Authentication Manager Configuration Management**.

The Configuration Management dialog box opens. This chapter describes the contents of each panel.



RSA ACE/Server Configuration Management

License Information
License: Advanced
Status: Permanent
Expiration Date: (None)
Licensed Users: 25
Licensed Replicas: 10
Licensed Realms: 6

Configuration Information

Enable Features
Encryption Type: ● DES ○ SDI
☑ RADIUS Server Enabled
□ Acting Slave Enabled
□ Resolve Hosts and Services By Name

Services

	Port Number	Service Name
Authentication:	5500	securid
Administration:	5550	sdadmind
Lock Manager:	5560	sdlockmgr
OA Download:	5580	sdoad
RADIUS:	1645	radius

Agent Host Communication
Agent Timeout (seconds): 5
Agent Retries (# of times): 5
Response Delay (seconds): 2

Legacy Agent Server Identification
Acting Master:
Acting Master IP Address:
Acting Slave:
Acting Slave IP Address:

Primary/Replica Communication
Maximum Packet Roundtrip Time (seconds): 30
Heartbeat Period (seconds): 300

RSA ACE/Server Identification
This Server: CAHILL-PC.NA.RSA.NET
This Server IP Address: 10.100.20.215
Primary Server: CAHILL-PC.NA.RSA.NET
Primary Server IP Address: 10.100.20.215

Whenever you are instructed to copy the configuration file (**sdconf.rec**) to a Replica, you must first run Configuration Management on the Replica, and change the value of **This Server** (in the **RSA Authentication Manager Identification** panel at the lower right) from the name of the Primary to the name of the Replica. For more information, see "Distributing the Configuration Update" on page 243.

Note: The **sdconf.rec** file is created by the Configuration Management application. Agents can use either **DES** or **SDI** encryption, and each Agent Host must have an **sdconf.rec** file that accurately specifies the type of encryption it uses. If you have some agents that use **DES** encryption and other agents that use **SDI** encryption, make sure that the **sdconf.rec** file you distribute to each Agent Host has the correct encryption setting.

License Information

The top panel of the Configuration Management dialog box displays data about your current license, as determined by the **license.rec** file you specified at installation time. Because RSA Security creates your license, you cannot change the information in this dialog box.

Additional Information

- For information about modifying your license, see the Help topic, "Upgrading the RSA Authentication Manager License."
- For descriptions of the data fields displayed in the License Information panel, see "The license.rec File" on page 238.

For information about license options and enforcement, and how to convert from a temporary evaluation license, see Appendix A, "Licensing".

Updating Your License Record in RSA Authentication Manager

During installation and, periodically, during normal operation, RSA Authentication Manager 6.1 checks for license compliance. If, for example, you have more active users in the database than your license allows, you will receive warning messages and will be unable to activate additional users.

If you anticipate user or site growth beyond your current license limits, you need to obtain a new license from RSA Security.

After you have obtained a new license, use the procedure outlined in this section to update your license record in RSA Authentication Manager. If you are running RSA Authentication Manager on a UNIX system, see "Updating Your License Record in RSA Authentication Manager for UNIX" on page 251.

Important: If you have more than one realm, you must have an Advanced license from RSA Security, which will supply you with six separate **license.rec** files on six diskettes. Label and assign each diskette for use with only one of your realms. Then, for each realm, repeat the following upgrade procedure using the **license.rec** you have assigned to it.

To upgrade the license:

1. On the Primary for the realm, log on as a Windows administrator.
2. Make sure that no RSA Authentication Manager processes are running. If the Authentication Manager or database brokers are running, open the RSA Authentication Manager Control Panel on the Authentication Manager machine, and double-click the **RSA Authentication Manager** icon.

   The RSA Authentication Manager dialog box opens.

3. Under **Stop Services**, click **Stop All** to stop both the Authentication Manager and the database brokers. If only the database brokers are running, click **Stop** under **ACE Brokers**. When the "ACE/Server stopped" (or "ACE/Broker stopped") message appears, click **OK**, then click **OK** again to close the RSA Authentication Manager control panel dialog box.
4. Click **Start** > **Settings** > **Control Panel** > **Add/Remove Programs**.

   The standard Windows Add/Remove Programs dialog box opens.
5. Scroll down to and select **RSA Authentication Manager**, and click **Add/Remove**.

   The RSA Authentication Manager Maintenance dialog box opens.
6. Select **Modify**, and click **Next**.
7. Select **Upgrade License,** and click **Next**.
8. If necessary, browse to the path where your new **license.rec** file for the current realm is located (the default is A:). Click **Next**.

   Assuming that you specified the location of a valid **license.rec** file, a message appears informing you that the:

   ```
   License has been successfully upgraded.
   ```
9. Click **OK** in the message dialog box. Click **Finish** in the next dialog box to complete the process and close the RSA Authentication Manager Maintenance program.
10. Click **Close** to close the Windows Add/Remove Programs dialog box.

Note: The next time you start RSA Authentication Manager, it automatically propagates the new license to its Replicas within the realm.

Configuration Information

The main part of the screen (below the license information) displays configuration information. You can edit these parameters on the Primary or Replicas only. On a Remote Administration machine, you can view but not edit them. To view this information on an RSA Authentication Agent for Microsoft Windows, use the Test Authentication Test feature. To view this information on a UNIX Agent Host, use the **sdinfo** command.

Note: When you make changes to the **sdconf.rec** file, you need to restart the RSA Authentication Manager for the changes to take effect. If any Agent Hosts are using auto-registration, you also need to stop the database brokers to ensure that the Agent Host **sdconf.rec** file is updated.

Enable Features

Parameter	Description
Encryption Type	The encryption method used for Agent Host/Authentication Manager communication, DES or SDI. If your system was previously configured for SDI encryption, click **SDI**. Otherwise, click **DES**.
Acting Slave Enabled	If this box is selected, you have the option of specifying an Acting Slave as well as an Acting Master for a legacy Agent Host. For more information, see "Resolving Hosts and Services" on page 240.
Resolve Hosts and Services by Name	This option determines how the RSA Authentication Manager and its Agents resolve hosts and services names. If the **Resolve Hosts and Services By Name** checkbox is not selected, the Authentication Manager resolves by IP Address. If the **Resolve Hosts and Services By Name** checkbox is selected, the Authentication Manager resolves by hostname.

The **Encryption Type** setting is used *only* by RSA Authentication Agents. If some Agents use SDI encryption, change the **Encryption Type** from DES to SDI and save the configuration record. Then copy the new **sdconf.rec** file only to the Agent Hosts that use SDI to communicate with the Authentication Manager. After doing this, return to the Configuration Management application and change the **Encryption Type** back to **DES** so that the default setting is preserved.

Agent Host Communication

Parameter	Description
Agent Time-out	Number of seconds between attempts to establish communications between the Agent Host and the Authentication Manager. The value can be from 1 to 20. The default is 5.
Agent Retries	Number of times the Agent should attempt to establish communication with the Authentication Manager before returning the error message “Cannot initialize agent host-Server communication.” The value can be from 1 to 6. The default is 5.
Response Delay	Number of seconds that an authentication request is held before the response is returned to the Agent. This delay is used to trap certain kinds of attacks on networks where logins are performed through unencrypted telnet connections. For this setting to have any effect, choose a value lower than **Agent Time-out** multiplied by **Agent Retries**. The value can be from 0 to 15. The default is 1.

If you change the **Agent Time-out**, **Agent Retries**, or **Response Delay**, distribute copies of the updated **sdconf.rec** file to all the Agent Hosts.

Primary and Replica Communication

If you change either of these values, distribute copies of the updated **sdconf.rec** file to all Replicas and apply it using the RSA Authentication Manager Control Panel. For more information, see "Distributing the Configuration Update" on page 243.

Parameter	Description
Maximum Packet Roundtrip Time	Packet-acknowledgment time-out period. The number of seconds that one Authentication Manager is to wait for the other to acknowledge that it has received a data packet. At the end of this period, the sending Authentication Manager attempts to reestablish the connection. The time-out period can be from 1 to 300 seconds. The default value is 30.
Heartbeat Period	This value is used to monitor the connectivity of the Replication service. When there has been no replication activity for the length of time specified as the Replica Heartbeat, the Authentication Manager assumes that the connection is lost. If the Primary detects a lost connection, it attempts to reestablish the connection. If a Replica detects a lost connection, it continues to listen on the Replication service port. The Heartbeat period can be from 15 to 1800 seconds. The lower limit of this range is always twice the **Maximum Packet Roundtrip Time**, so this value must always be set to *at least* twice the value of the **Maximum Packet Roundtrip Time**.

Services Configuration

Parameter	Description
Authentication	Port number and name of the authentication service as specified in the **services** file. The default name for the Authentication Service process is *securid*, and the default port number for this process is 5500.
Administration	Port number and name of the administration service as specified in the **services** file. The default name for the administration service process is *sdadmind*, and the default port number for this process is 5550. The Administration Service is used for Remote Administration.
Lock Manager	Port number and name of the Lock Manager as specified in the **services** file. The default name for the Lock Manager process is *sdlockmgr*, and the default port number for this process is 5560.
OA Download	Port number and name of the Offline Authentication Download service as specified in the **services** file. The default name for the OA Download process is *sdoad*, and the default port number for this process is 5580.

Resolving Hosts and Services

The **Resolve Hosts and Services by Name** checkbox determines how the RSA Authentication Manager resolves server identity. The Authentication Manager checks information in the **sdconf.rec** file (when identifying itself or communicating with the Primary) or the RSA Authentication Manager database (when communicating with a Replica), and compares it to information from the DNS server or entries in the hosts and services files.

- If the box is selected, the Authentication Manager resolves processes running on the RSA Authentication Manager and RSA Authentication Agent authentication requests by hostname. Names are resolved through the **/etc/hosts** file, the **/etc/services** file, or a name server. Resolving by hostname requires that your system use a consistent naming scheme. For example, if you use fully-qualified names on your network or in your hosts and services files, you must use fully-qualified names in the **sdconf.rec** file and the RSA Authentication Manager database. If you use short names on your network or in your hosts and services files, you must use short names in the **sdconf.rec** file and in the RSA Authentication Manager database.

- If the box is not selected, the Authentication Manager resolves processes running on the RSA Authentication Manager and RSA Authentication Agent authentication requests by IP address. For RSA Authentication Manager processes, the Authentication Manager uses the IP address found in the **sdconf.rec** file. If the IP address in the **sdconf.rec** file does not match the local machine's IP address, the Authentication Manager checks the **/etc/hosts** file and, if necessary, the name server for the IP address. For RSA Authentication Agent authentication requests, the Authentication Manager uses the IP address in the UDP packet to look up the RSA Authentication Agent in the RSA Authentication Manager database. Resolving by IP address is the most flexible method. For example, if the host file uses the short name and the DNS name server uses the fully-qualified name, the RSA Authentication Manager will still be able to resolve its identity by checking the IP addresses.

If you use both a **hosts** file and a DNS server, the entries for each Authentication Manager must be the same in both places and must be the fully-qualified name (for example, **okeefe.painter.com** rather than just **okeefe**). The name on the computer itself need not be fully qualified, but it must otherwise be the same (that is, it can be just **okeefe**, but it cannot be **okeefe_pc**).

If you change the name of an Authentication Manager, distribute copies of the updated **sdconf.rec** file to the Replica and to all the Agent Hosts.

Legacy Agent Server Identification

Parameter	Description
Acting Master	Name of the Acting Master.
Acting Master IP Address	IP address of the Acting Master.
Acting Slave	Name of the Acting Slave.
Acting Slave IP Address	IP address of the Acting Slave.

If you assign the role of Acting Master or Acting Slave to a Replica, distribute copies of the new **sdconf.rec** file to all machines with legacy agent software. If you use the Add Agent Host menu to add additional legacy Agent Hosts and specify a different set of Replicas to be the Acting Master and Acting Slave for those legacy agents, copy the **sdconf.rec** file to the***%SYSTEMROOT%*\system32** directory of each Windows Agent Host and the ***ACEDATA*** directory of each UNIX Agent Host. For more information, see Chapter 3, "Agents and Activation on Agent Hosts."

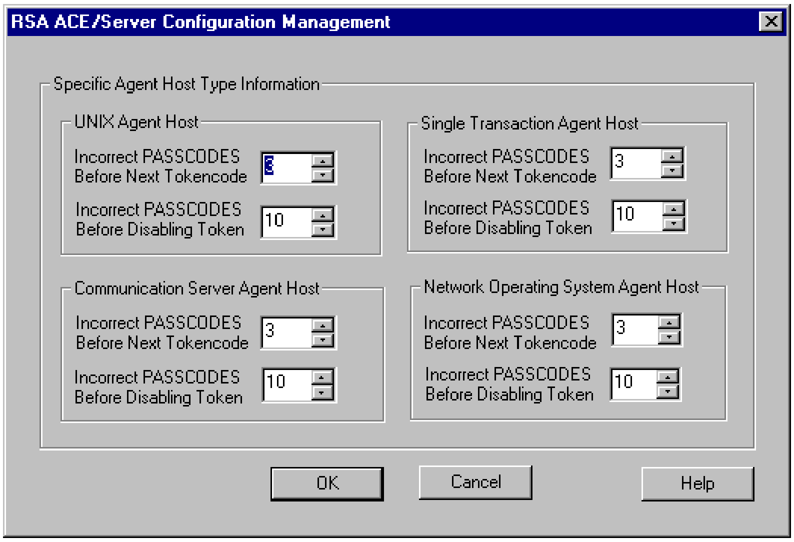
Note: If the **Acting Slave Enabled** box (see page 237) is not selected, you can specify only an Acting Master. The Acting Slave boxes are unavailable, as shown in the following illustration.

Primary and Replica Identification

Parameter	Description
This Authentication Manager	Name of the Authentication Manager on which you are running the Configuration Management application.
This Authentication Manager IP Address	IP address of the Authentication Manager on which you are running the Configuration Management application.
Primary Authentication Manager	Name of the Primary Authentication Manager.
Primary Authentication Manager IP Address	IP address of the Primary Authentication Manager.

Agent Host Passcode Configuration

To set the number of incorrect passcode attempts an Agent Host is to accept before it puts a token in Next Tokencode mode or disables the token, click **Agent Host** in the Configuration Management dialog box. The Configuration Management window containing the Specific Agent Host Type Information opens.



RSA ACE/Server Configuration Management

Specific Agent Host Type Information

UNIX Agent Host
Incorrect PASSCODES Before Next Tokencode: 3
Incorrect PASSCODES Before Disabling Token: 10

Single Transaction Agent Host
Incorrect PASSCODES Before Next Tokencode: 3
Incorrect PASSCODES Before Disabling Token: 10

Communication Server Agent Host
Incorrect PASSCODES Before Next Tokencode: 3
Incorrect PASSCODES Before Disabling Token: 10

Network Operating System Agent Host
Incorrect PASSCODES Before Next Tokencode: 3
Incorrect PASSCODES Before Disabling Token: 10

The window lists the four types of Agent Hosts. You can set the parameters separately for each type. The procedure is described in "Configuring Agents to Handle Incorrect Passcodes" on page 63.

Note: The RSA Authentication Agent for Microsoft Windows is a Network Operating System Agent.

If you change any of the settings in this dialog box, distribute copies of the updated **sdconf.rec** file to all Replicas, and apply it using the RSA Authentication Manager Control Panel. See the following section, "Distributing the Configuration Update."

Parameter	Description
Incorrect PASSCODEs Before Next Tokencode	Number of failed authentication attempts to allow before putting token into Next Tokencode mode. The value can be from 1 to 5. The default value is 3, but you may want to set it lower if you use unencrypted telnet.
Incorrect PASSCODEs Before Disabling Token	Number of failed authentication attempts to allow before a token is disabled. The range of possible values is 2 to 25. The default value is 10, but you may want to set this value lower if you use unencrypted telnet. Unless this value is at least one greater than the **Incorrect PASSCODEs Before Next Tokencode** value, tokens are never put in Next Tokencode mode.

Distributing the Configuration Update

Whenever you modify the Authentication Manager configuration file by using the Configuration Management application on the Primary, you must distribute the updated **sdconf.rec** to affected Replicas and Agent Hosts.

For instructions, see the Help topic "Distributing the Configuration Update."

Note: The **sdconf.rec** file is created by the Configuration Management application. Agents can use **DES** or **SDI** encryption, and each Agent Host must have an **sdconf.rec** file that contains a match for the encryption it uses. If you have some Agents that use **DES** encryption and other Agents that use **SDI** encryption, make sure that the **sdconf.rec** file you distribute to each Agent Host has the correct encryption setting.

Whenever you modify the Authentication Manager configuration file by using the Configuration Management application on the Primary, take the following steps:

1. Copy the new **sdconf.rec** file to the ***ACEDATA*** directory on each Replica affected by the change. On the Replica, using a DOS command prompt, change to the ***ACEPROG*** directory and type:

   ```
   sdconfig -update
   ```

   Running this command updates the name and IP address for **This Server** in the configuration file on the Replica.

2. Stop and restart the Primary and Replicas so that the new configuration takes effect.

3. Do one of the following:
   - Copy the new **sdconf.rec** file to the ***ACEDATA*** directory on affected RSA Authentication Agents; or make the new **sdconf.rec** available, and instruct administrators to update configurations as described in the appropriate Agent manual.
   - If you have legacy Agent Hosts, generate new configuration files for each Acting Master/Acting Slave pair using the **Generate Configuration Files**.

If you changed any configuration value other than these four, you must install the new **sdconf.rec** on the Agent Host workstations:

- Maximum Roundtrip Time
- Communications
- Incorrect PASSCODEs Before Next Tokencode
- Incorrect PASSCODEs Before Disabling Token

If you changed no values other than these, it is not necessary to install the new **sdconf.rec** on Agent Host workstations.

Note: A Windows machine that runs both an RSA Authentication Manager and an RSA Authentication Agent needs two copies of the **sdconf.rec** file, one in the ***ACEDATA*** directory and one in the ***%SYSTEMROOT%*\system32** directory.

Agents that are not RSA Authentication Agents developed by RSA Security may not be able to store and read the **sdconf.rec** file. Typically, third-party devices that integrate RSA Authentication Agent code use a configuration file specific to the device type. To distribute new configuration information to these Agents, reconfigure the device following the instructions in the manufacturer's documentation.

Authenticating Across Multiple Network Interfaces

To set up your RSA Authentication Manager to authenticate across multiple network interfaces, you must create an alias IP address list and then generate new configuration files for each alias IP address. RSA Security recommends that you specify IP addresses that are unique across your network.

For information about authenticating across multiple network interfaces for UNIX, see Chapter 15, "Replica Management Utility (UNIX)."

To create an alias IP address list:

1. From the RSA Authentication Manager Control Panel, shut down all processes on the Primary.
2. On the Primary, click **Start** > **Programs** > **RSA Security** > **RSA Authentication Manager Configuration Tools** > **RSA Authentication Manager Replication Management**.
3. Select the Authentication Manager that you want to modify. This Authentication Manager will be the *multihomed* Authentication Manager.

4. Click **Details**.

   The RSA Authentication Manager Replica Information dialog box opens.

5. Under Alias Information, in the IP Address box, enter the alias IP address, and click **Add**.

6. Repeat step 5 for all alias IP addresses you want to assign to the multihomed Authentication Manager.

   Note: The maximum number of alias IP addresses allowed is three.

7. When you are finished adding alias IP addresses, click **OK**.

8. Restart the Primary.

To generate configuration files for each alias IP address:

1. From the Database Administration interface, click **Agent Host** > **Add Agent Host**.
2. Add the RSA Authentication Agent to which you will assign the alias IP address. For instructions, see the Help topic "Add Agent Host."
3. When you have finished adding the RSA Authentication Agent as an Agent Host, click **Assign Acting Servers**.
4. Where the multihomed Authentication Manager is an Acting Master or Acting Slave, from the **IP Address** drop-down menu, select the appropriate alias IP address.
5. Click **Generate Config File**.
6. If prompted, click **Yes**.
7. Save the new **sdconf.rec** file in the desired location.
8. Copy the new **sdconf.rec** to the ***%SYSTEMROOT%*\system32** directory (Windows) or ***ACEPROG*** (UNIX) directory on the RSA Authentication Agent for which it was created.
9. Repeat steps 1 through 8 for each alias IP address you added.

13 Replica Management Utility (Windows)

With the RSA Authentication Manager Replica Management utility you can configure the Replicas in your realm. From a Primary, you can

- Add and delete Replicas from your realm.
- Display and edit information about the Replicas.
- Create Replica Packages for Replicas.

On a Replica, you can only display information about the Primary and the Replicas.

For Replica Management procedures, see the Replica Management utility Help.

Note: Some Replica Management procedures modify the **sdconf.rec** file. Make sure that you or another administrator does not have the Configuration Management utility running, as changes made in that utility can overwrite the changes you make with Replica Management.

To start the Replica Management utility:

1. Using the RSA Authentication Manager Control Panel, shut down all services on the RSA Authentication Manager (Primary or Replica).

   All administrative sessions are disconnected.

2. Click **Start** > **Programs** > **RSA Security** > **RSA Authentication Manager Configuration Tools** > **RSA Authentication Manager Replica Management**.

   If you are connected to a Replica or did not shut down the database brokers, the **Details** button is the only active button, and "READ ONLY Access to database" appears above the list of Authentication Managers.

Viewing Replica Authentication Manager Information

The following table describes the information displayed in the RSA Authentication Manager Replica Information dialog box. To open the RSA Authentication Manager Replica Information dialog box, click **Details from the main Replica Management screen**.

Information	Description
This Authentication Manager is a Replica or This Authentication Manager is a Primary	Whether the selected Authentication Manager is the Primary or a Replica.
Authentication Manager Information	
Hostname	The hostname of the Authentication Manager.
IP Address	The IP address of the Authentication Manager.
Service Name	The name of the service that the Primary and the Replica use to communicate. The default name is **securidprop**_##, where ## is a two digit number from 00 to 10. On a new Primary, the default name is **securidprop_00**.
Service Port Number	The port number that the Primary and Replica use to communicate. On a new Primary, the default port number is 5505.
Begin Replication Service	The number of seconds after Primary startup that the replication service starts.
Replicate Database Changes Every	How often databases changes are replicated, in seconds.
Alias Information	
Alias List	The list of alias IP addresses that you have assigned to this Authentication Manager. If you want to delete an alias, select it from the list, and click **Remove**.
IP Address	Enter the alias IP address that you want to assign to the Authentication Manager, and click **Add**. If this box and the **Add** button are not active, then the Authentication Manager has the maximum number of aliases assigned already.

Information	Description
Replica Status Information	
Replica Number	The number of the Replica. Possible values are 0 to 10.
Replica Sequence Number	The Replica Sequence Number is used to ensure that the correct database is being used by the Primary and the Replica. This number is incremented at various times (for example, when you add a Replica or generate a Replica Package). When the Replica starts and attempts to connect to the Primary, both Authentication Managers check the value of the Replica Sequence Number and whether the initial Primary/Replica communication has occurred. Matching Replica Sequence Numbers indicate that the correct Replica Package was installed on the Replica. If the two numbers do not match, the Replica shuts down, and a new Replica Package must be created on the Primary and sent to the Replica.
Able to Authenticate	If **Yes**, the Replica is capable of authenticating users and replicating database changes with the Primary. If **No**, the Replica is not capable of authenticating users and replicating database changes with the Primary.
Initial Primary/Replica Communication Has Occurred	If **Yes**, the Primary and Replica have successfully performed the initial communication pass. Successful initial communication between the Primary and the Replica indicates that the Replica Sequence Numbers on each Authentication Manager match. If **No**, the Primary and Replica have not yet performed the initial communication pass.
Replica Marked for Unconditional Push	If **Yes**, you recovered your Primary by restoring a backup copy of the database to the Primary. The new database must be delivered to all existing Replicas through Push DB Assisted Recovery. You must allow Push DB Assisted Recovery in the System Parameters of the Primary so that the Primary can push the database. Applying full or partial Replica Package to the Replicas is not required. Otherwise, the value is **No**.

For instructions, see the Replica Management utility Help.

14 Configuring the RSA Authentication Manager (UNIX)

This chapter describes how to modify your RSA Authentication Manager configuration.

Updating Your License Record in RSA Authentication Manager for UNIX

If you need to upgrade your RSA Authentication Manager license limits, you must purchase a new license record from RSA Security through your sales representative or local distributor. Reasons to upgrade may include increasing the number of allowed active users, adding Replica Authentication Managers, or increasing the number of Realms.

When you receive the new license record (**license.rec**) file, follow the instructions in this section to install it.

For general information about licensing in RSA Authentication Manager, see Appendix A, "Licensing." For troubleshooting information, see "Messages" on page 300.

To update the license record:

1. Log on as **root** on the Primary Authentication Manager.
2. Change to a directory that is outside your top-level RSA Authentication Manager directory.
3. Insert the 3.5-inch diskette that contains the new **license.rec** file into the diskette drive on the Authentication Manager or other workstation. Following your usual procedures for copying from this drive, copy the **license.rec** file to the current directory.

   Important: If you purchased a multiserver license, you received a package of six license diskettes individually labeled for Authentication Managers one through six. Reserve a single diskette for each Primary, write the name of the Authentication Manager on the diskette label, and *always* use this diskette for any installations on this Authentication Manager.

4. To create a backup of the existing **license.rec** (to **license.old**) automatically and to install the new license record, type:

   ```
   ACEPROG/sdsetup  -license
   ```

   You do not need to back up the existing **license.rec** manually before you run ***ACEPROG*/sdsetup**. However, if you do choose to create a backup file manually, do not name it **license.old**.

Note: The **1version** file, which was copied into your current working directory, is included for internal purposes only. You do not need to take any action relative to this file.

5. Stop and restart **aceserver** for the new license to take effect.

   When RSA Authentication Manager restarts, the Primary attempts to reestablish communication with the Replicas in the Realm. After communication is reestablished, the Primary will automatically propagate the new license record to the Replicas.

Understanding Your RSA Authentication Manager Configuration

The installation program stored values in the configuration file and displayed those values along with license information when the program was completed.

Each value in the configuration file (***ACEDATA*/sdconf.rec**) is one of the following:

- A value specified by the installer (for example, the name of the RSA Authentication Manager file owner)
- A default value the Authentication Manager selects and sets because the value represents a balance between system security and user convenience
- A value derived from information in an existing Authentication Manager configuration file in the ***ACEDATA*** directory

To display your system's current configuration settings, run ***ACEPROG*/sdinfo**. The following table describes the information that can be displayed.

Parameter	Description
License Creation	The date the license was created.
License ID	The license ID number generated when the license was created.
RSA Authentication Manager version	The complete version number of the current software, as stored in ***ACEDATA*/version.txt**.
Evaluation	This field appears only if your license is a trial license. A trial license has a fixed expiration date, which when reached causes your RSA Authentication Manager to stop working. For information about converting to a permanent license, see "Upgrading or Converting Your License" on page 280.
Violation	This field appears only if your license is in *upgrade violation* mode (established during installation). For more information, see "Upgrading or Converting Your License" on page 280.

Parameter	**Description**
Expiration	This field appears only if your license is a temporary license, either because you are using an evaluation (temporary) version of RSA Authentication Manager, or your license is in upgrade violation mode.
Config File Version	The complete version number of the current configuration file.
File ownership	The login of the administrator who owns the RSA Authentication Manager program and data files.
Agent retry *value*	The number of times an Agent Host attempts to establish communications with the Authentication Manager before returning **Cannot initialize Agent Host-server communication**.
Agent retry *interval* ("Agent time-out")	Number of seconds between attempts to establish Agent Host/Authentication Manager communications.
DES/RC5 Encryption	Encryption method used for Agent Host/Authentication Manager communications: DES, the Data Encryption Standard; or RC5, the RSA Security proprietary encryption.
TACACS Plus	If enabled, the TACACS+ server is started automatically when you run **aceserver**.
Primary Authentication Manager information	The name and IP address of the Primary Authentication Manager.
Current Authentication Manager information	The name and IP address of the Authentication Manager on which you are running **sdinfo**.
Acting Master Authentication Manager Information	The name and IP address of the Acting Master.
Acting Slave Authentication Manager Information	The name and IP address of the Acting Slave.
Replica Time-out	The Primary-to-Replica and Replica-to-Primary packet-acknowledgment time-out period—the number of seconds (1-300) that one Authentication Manager waits for another to acknowledge that it has received a data packet. The sending Authentication Manager attempts to reestablish the Primary and Replica connection when the period ends.

Parameter	Description
Replica Heartbeat	The value used to detect connectivity of the Replication service. When there has been no replication activity for the length of time specified for the **Replica Heartbeat**, the Authentication Manager assumes that the connection is lost. If the Primary detects a lost connection, it attempts to reestablish the connection. If a Replica detects a lost connection, it continues to listen on the Replication service port. You can set the interval from 15 through 1800 seconds. The lower limit of this range is always twice the **Replica Time-out**, so the value of the **Replica Heartbeat** must always be set to *at least* twice the value of the **Replica Time-out**.
Authentication service name and port number	The service name and port number of Agent Host and Authentication Manager communications. They must match what appears in all **/etc/services** files on the system (default service name is **securid**; default port number is **5500**).
Addresses	How IP addresses are resolved. **By IP address in ACE/Server database** means that Authentication Manager programs and Agent Hosts do not look at the **/etc/hosts** file, **/etc/services** file, or a name server to resolve the names of servers and services. Instead, they look in the Authentication Manager's **sdconf.rec** file. **By name in host file or name service** means that names are resolved through the **/etc/hosts** file, **/etc/services** file, or name server. This method may be more convenient, but is only as secure as your **/etc/hosts** file, **/etc/services** files, or name server. You must secure these.
Administration service name and port number	The service name and port number for the administration service. They must match what appears in all **/etc/services** files on the system and must also match the services entry on the Remote Administration machine. (The default name is **sdadmind**; the default port number is **5550**.)
Lock Manager service name and port number	The service name and port number for the lock manager. (The default name is **sdlockmgr**; the default port number is **5560**.)
Bad PASSCODEs before setting Next Tokencode	The number of unsuccessful authentication attempts allowed for each Agent type before a token is put into Next Tokencode mode.
Bad PASSCODEs before Disabling Token	The number of unsuccessful authentication attempts allowed for each Agent type before a token is disabled.
Response delay	The time in seconds that an authentication request is held before the response is returned to the Agent Host. This setting traps certain kinds of attacks on networks where logons are performed over unencrypted telnet connections.

Parameter	Description
Alias IP Address List	The actual and alias IP addresses of all the Authentication Managers in the realm. You specify alias IP addresses using the Replica Management utility. There is a maximum of three alias IP addresses allowed per Authentication Manager.
License	The license level—Base or Advanced.
Number Licensed Users	The number of users that your license allows in the RSA Authentication Manager database. (Because each user can be assigned up to three tokens, the number of tokens allowed by the license can be greater.)
Number Licensed Replicas	If you have a Base license, this will be **1**. If you have an Advanced license, this will be **10**.
Number Licensed Realms	If you have a Base license, this will be **1**. If you have an Advanced license, this will be **6**.

Changing the Configuration

The information in this section helps you select the most appropriate configuration values for your installation. Whenever you copy the configuration file (**sdconf.rec**) to a Replica, you must run **sdconfig -update** on the Replica.

Note: When you make changes to the **sdconf.rec** file, you need to restart the RSA Authentication Manager for the changes to take effect. If any Agent Hosts are using auto-registration, you also need to stop the database brokers to ensure that the Agent Host **sdconf.rec** file is updated.

To modify the RSA Authentication Manager configuration:

1. Log on to the Primary as **root**.
2. Run ***ACEPROG*/sdsetup -config**.
3. You are asked a series of configuration questions that enable you to change the values currently stored in the **sdconf.rec** file in the Primary ***ACEDATA*** directory. The prompts that appear depend on the options you purchased with the system. Use the descriptions that follow for help answering each prompt that appears.

   How many seconds should an agent wait before retrying?

   Enter the number of seconds that should pass between attempts to establish Agent Host/Authentication Manager communications. This is stored in **sdconf.rec** as the "Agent Time-out" value. The range of acceptable values is 1 to 20, and the default is 5.

How many times should an agent retry before reporting failure?

Specify the number of times the Agent Host should attempt to establish communications with the Authentication Manager before returning **Cannot initialize Agent Host-server communication**. The range of possible values is one to six, and the default value is five.

Do you want to use DES/RC5 encryption?

Specify whether Authentication Manager communications with Agent Hosts are to be protected by DES/RC5 or SDI encryption. The default encryption type is DES/RC5. If all your Agent Host workstations are set to use SDI encryption instead, specify SDI here.

If some but not all Agent Hosts are registered as using SDI encryption, you must either change the encryption type in those Agent Host records or else create two versions of **sdconf.rec**: one with the default value of DES/RC5, the other with this value set to SDI. For more information, see “Distributing the Configuration Update” on page 259.

How many wrong PASSCODEs before a token is set to Next Tokencode?

Set the number of failed login attempts with incorrect RSA SecurID passcodes before a token is put into Next Tokencode mode. When this mode is turned on, the Authentication Manager prompts for a second code after it sees a series of invalid passcodes. If the user does not enter the next code generated by the token, access is denied. You can set the number for the four types of Agent Hosts (UNIX Agents, Communication servers, Single transaction agents, and NOS agents).The range of possible values is one to five. The default value is three, but you can set this value lower if you do not use encrypted telnet or telnet in line mode.

How many wrong PASSCODEs before a token is set disabled?

Set the number of failed login attempts with incorrect RSA SecurID passcodes before a token is disabled. You can set the number for the four types of Agent Hosts (UNIX Agents, Communication servers, Single transaction agents, and NOS agents). The range of possible values is 2 to 25, with the default set at 10. This value must always be at least one greater than the Bad passcodes before Next Tokencode mode value (described above). You may want to set both of these values lower if you use unencrypted telnet.

Which administrator should own the RSA Authentication Manager files?

Specify a member of the UNIX group of RSA Authentication Manager administrators to be the owner of all Authentication Manager files.

Which port number should be used for authentication?

Enter the port number you specified for the authentication service in **/etc/services**. The default value is 5500.

What is the service name you will use?

Enter the name of the authentication service (by default, **securid**). This is the name you specified in the **/etc/services** file or information server.

Do you want to resolve hosts and services by name?

If True, the Authentication Manager resolves processes running on the RSA Authentication Manager and RSA Authentication Agent authentication requests by hostname. Names are resolved through the **/etc/hosts** file, the **/etc/services** file, or a name server. Resolving by hostname requires that your system use a consistent naming scheme. For example, if you use fully qualified names on your network or in your hosts and services files, you must use fully qualified names in the **sdconf.rec** file and the RSA Authentication Manager database. If you use short names on your network or in your hosts and services files, you must use short names in the **sdconf.rec** file and in the RSA Authentication Manager database.

If False, the Authentication Manager resolves processes running on the RSA Authentication Manager and RSA Authentication Agent authentication requests by IP address. For RSA Authentication Manager processes, the Authentication Manager uses the IP address found in the **sdconf.rec** file. If the IP address in the **sdconf.rec** file does not match the local machine's IP address, the Authentication Manager checks the **/etc/hosts** file and, if necessary, the name server for the IP address. For RSA Authentication Agent authentication requests, the Authentication Manager uses the IP address in the UDP packet to look up the RSA Authentication Agent in the RSA Authentication Manager database. Resolving by IP address is the most flexible method. For example, if the host file uses the short name and the DNS name server uses the fully-qualified name, the RSA Authentication Manager will still be able to resolve its identity by checking the IP addresses.

What is the name or address of the Primary RSA Authentication Manager?

Enter the name or IP address of the Primary. The value you enter must be in the hosts file, and the machine must exist on the network.

Which port number should administration use?

Enter the port number you specified for this purpose in **/etc/services**.

What is the service name you will use?

Enter the name of the Remote Administration service (by default, **sdadmind**). This is the name you specified in the **/etc/services** file or information server. This name must match the services entry on the Remote Administration machine.

Which port number should the lock manager use?

Enter the name of the you specified for this purpose in **/etc/services**.

What is the service name you will use?

Enter the name of the Lock Manager service (default is **sdlockmgr**). This is the name you specified for this purpose in the **/etc/services** file or information server.

Do you want to use TACACS Plus?

If you answer **y**, a TACACS+ daemon starts automatically whenever you start **aceserver**.

Do you want to specify an acting master server?

Answer **y** if some Agent Hosts in your system use RSA Authentication Agent software earlier than version 5.0.

Legacy Agents running older software use the **sdconf.rec** file to identify the Authentication Managers. This file, however, identifies only two Authentication Managers: the Master and the Slave. For RSA Authentication Manager 6.1 to accept authentication requests from legacy Agents, a Replica must act as the Master, so you must specify a Replica as the "acting" Master. If the Acting Master is not working, the Acting Slave responds to requests from legacy Agents.

Answer **n** if no Agent Hosts in your system use legacy Agent software.

What is the name or address of the acting master server?

If you want to specify an Acting Master, enter the name or IP address of the Replica that you want to use as the Acting Master. The value you enter must be in the hosts file, and the machine must exist on the network.

Do you want to specify an acting slave server?

Answer **y** if some Agent Hosts in your system use legacy Agent software. (For a definition, see "Do you want to specify an acting master server?".)

The Acting Slave responds to legacy Agent requests when the Acting Master is not working.

Answer **n** if no Agent Hosts in your system use legacy Agent software.

What is the name or address of the acting slave server?

If you want to specify an Acting Slave, enter the name or IP address of the Replica that you want to use as the Acting Slave. The value you enter must be in the hosts file, and the machine must exist on the network.

The Primary expects an acknowledgment for each packet it sends to a Replica. How many seconds should the Replica wait for this acknowledgment?

Enter the number of seconds the Primary must wait for a packet receipt from a Replica before it assumes that the connection is lost. At the end of this acknowledgment time-out interval, the "disappointed" Authentication Manager tries to reestablish the connection. This value is labeled the **Replica Time-out** interval. The time-out period may be from 1 through 300 seconds.

Heartbeat in seconds

This value is used to detect connectivity of the Replication service. When there has been no replication activity for the length of time specified for the **Replica Heartbeat**, the Authentication Manager assumes that the connection is lost. If the Primary detects the lost connection, it attempts to reestablish the connection. If a Replica detects the lost connection, it continues to listen on the Replication service port. You may set the interval from 15 through 1800 seconds. The lower limit of this range is always twice the **Replica Time-out**, so the value of the **Replica Heartbeat** must always be set to *at least* twice the value of the **Replica Time-out**. The prompt shows the appropriate range.

How many seconds should the Authentication Manager queue agent responses?

Enter number of seconds that an authentication request should be held before a response is returned to the Agent Host. This option is used to trap certain kinds of attacks on networks where logins are performed over unencrypted telnet connections. There is no performance degradation when the value is 2 seconds. Although the maximum allowed value is 15 seconds, do not enter a value that is greater than the Agent Retries value multiplied by Agent Time-out value. For example, if the Agent Retries setting is 2 and the Agent Time-out setting is 2, the delay value must not be greater than 4.

If a service name or service port number as stored in **sdconf.rec** cannot be found in the **/etc/services** file, a warning message appears. The unresolvable service name and port numbers are displayed. Review them carefully. If they are incorrect, type **r** (reconfigure) to change these values in **sdconf.rec**. If they are correct as displayed, type **s** to go to a shell and edit **/etc/services** to add or modify these lines.

Distributing the Configuration Update

Note: The **sdconf.rec** file is created by the Configuration Management application. Agents can use **DES** or **SDI** encryption, and each Agent Host must have an **sdconf.rec** file that contains a match for the encryption it uses. If some but not all Agent Hosts are registered as using SDI encryption, you must either change the encryption type in those Agent Host records or else create two versions of **sdconf.rec**: one with the default value of DES/RC5, the other with this value set to SDI. Make sure that the **sdconf.rec** file you distribute to each Agent Host has the correct encryption setting.

Whenever you modify the Authentication Manager configuration file by running ***ACEPROG*/sdsetup -config** on the Primary, stop and restart **aceserver** for the new configuration to take effect.

If the only configuration values you changed were Replica Time-out value, Replica Heartbeat value, the number of bad passcodes before Next Tokencode, or the number of bad passcodes before Token Disabled, then it is not necessary to install the new **sdconf.rec** on Agent Host workstations. If you changed any other configuration value, however, you must install the new **sdconf.rec**. Use the following procedure.

To install the new sdconf.rec file on the Replica and on Agent Host workstations:

1. Copy the new configuration file, ***ACEDATA*/sdconf.rec**, from the Primary to the target UNIX workstation.
2. On the target workstation, log in as **root**.
3. Go to the directory into which you copied **sdconf.rec**.
4. Type:

   ```
   ACEPROG/sdsetup -config
   ```

   This installs the new configuration file into the ***ACEDATA*** directory of the target workstation. Using a command that simply copies the file into the ***ACEDATA*** directory is not sufficient. Use the ***ACEPROG*/sdsetup -config** command instead.

5. On Agent Host workstations, the new configuration file takes effect as soon as it is installed. On a Replica, however, to put the new configuration into effect after it is installed, you must stop and restart **aceserver** on that machine.

If you have Agent Hosts that are not UNIX workstations and are not RSA Authentication Agents developed by RSA Security, the Agent Hosts may not be able to store and read **sdconf.rec**. Typically, third-party devices that integrate RSA Authentication Agent code use a configuration file particular to that device type. To distribute new configuration information to those Agent Hosts, you must reconfigure the device, following the instructions in the manufacturer's documentation.

RSA Authentication Agents that are developed by RSA Security for non-UNIX platforms, such as the RSA Authentication Agent for Microsoft Windows, do store and read **sdconf.rec** for configuration information. Make the new **sdconf.rec** available to all Agent Host administrators and instruct them to update Agent Host configurations as described in the applicable RSA Authentication Agent documentation.

Changing an Agent Host Name or IP Address

If you are not using the Agent Host auto-registration and update program, **sdadmreg**, follow the directions in this section to update the RSA Authentication Manager database when an Agent Host's IP address changes. For information on installing and using **sdadmreg**, see the *UNIX Installation Guide*.

To change an Agent Host name or IP address:

1. Update the Authentication Manager **/etc/hosts** file or the system information service with the Agent Host's new name or IP address.
2. On the administration machine, run the Authentication Manager Database Administration application.
3. On the Agent Host menu, click **Edit Agent Host**.
4. If the Agent Host machine name has changed, edit the **Name** field and press TAB.

   If the name is the same but the IP address has changed, press TAB to move the cursor out of the **Name** field.

   In either case, the **Network address** field is updated automatically when you press TAB, based on the entry you made in **/etc/hosts** or the information service in step 1.

Multiple Agent Host IP Addresses

When you add an Agent Host to the RSA Authentication Manager database, you enter the primary name of the machine in the **Name** field of the **Add Agent Host** dialog box. When you press TAB to exit the **Name** field, the Agent Host IP address is displayed in the **Network address** field automatically, based on the information in the local hosts file or name server. This network address is the same as the one that displays when you run **sdinfo** (or **clntchk**) on the Agent Host.

If an Agent Host has more than one node name and IP address, you can register multiple names in the Authentication Manager database as Secondary Nodes.

To register an Agent Host that has more than one node name and IP address:

1. On the administration machine, run the RSA Authentication Manager Database Administration application.
2. On the Agent Host menu, click **Edit Agent Host** and select the Agent Host whose record you want to update.
3. Click the **Secondary Nodes** button.

   The **Select Secondary Node** dialog box opens, displaying any secondary nodes that already exist.
4. To add a new name to the list of secondary nodes, type the name in the box. Press TAB to exit the field, or click **OK** to close the dialog box.
5. If the name you entered exists in the local hosts file or name server, the **Add Secondary Node** dialog box opens to display the primary name, the new secondary name, and secondary network address of the Agent Host. Click **OK** to add this node information to the list.

15 Replica Management Utility (UNIX)

With the RSA Authentication Manager Replica Management utility (**sdsetup -repmgmt**) you can configure the Replicas in your realm. From a Primary, you can

- Add and delete Replicas from your realm.
- Change the name or IP address of the Replica or Primary.
- Display and edit information about the Replicas.
- Push the Primary database to a Replica.

On a Replica, you can display only information about the Primary and the Replicas.

Running the Replica Management Utility

You can run the Replica Management utility at any time to view the information about the Authentication Managers. However, to make changes to the Authentication Manager information, you must shut down the database brokers. Shutting down the brokers disconnects all administrative sessions connected to the database. At the command line, type:

```
ACEUTILS/rptconnect stop
```

to stop the Report Creation utility, if it is running, and then type:

```
ACEPROG/aceserver stop
ACEPROG/sdconnect stop
```

Interactive Mode vs. Command Line Mode

You can run the utility in two ways: in interactive mode, which prompts you to enter each piece of information separately, or in command line mode, where you can enter all required information with one command, using the options and arguments described in "Syntax" on page 271. Interactive mode is available only when you are adding, modifying, deleting, or replacing a Replica. Command line mode is available for all Replica Management tasks.

To run the utility in interactive mode, type only the command, as described in the following sections. To run in command line mode, you must provide all the required options and arguments. If you do not include all the required options and arguments, the utility does not execute the command and displays a failure message.

Adding a Replica

In interactive mode, the Replica Management utility prompts you to enter the information about the Replica. To add a Replica in interactive mode, at the command prompt, type:

```
sdsetup -repmgmt add
```

Follow each of the prompts to complete the process.

Name of the Replica

When you enter a Replica name, the RSA Authentication Manager attempts to resolve it in the database. If the name is not resolved you can choose to use it anyway, or enter a different name.

IP Address

If the Replica name was resolved, a valid IP address displays. You can use this address or specify a different one. If the address you specify is invalid, you are prompted again.

Alias IP Addresses

You can specify up to three alias IP addresses. If the Replica is communicating with the Primary through a firewall, at least the main IP address or one alias must be valid and known by the Primary Authentication Manager.

Service Name

Use the default or specify a different service name. Any service name that you use must be added as an entry in the services file. The default is **securidprop_##**, where ## is a two digit number from 00 to 10.

Service Port

Use the default or specify a different port number. Any port number that you use must be added as an entry in the services file. For a Primary, the default is 5505. The number is incremented for each Replica that you add. For example, the first Replica you add uses the number 5506.

Delay

The number of seconds after Primary start up that the replication service starts. The default value is 10 for the first Replica you add. For each subsequent Replica, the value is incremented by 10.

Interval

The number of seconds between replication of database changes. The default value is 100 seconds.

Modifying a Replica

To modify Replica information, at the command prompt type:

```
sdsetup -repmgmt modify
```

At the first prompt, specify the name of the Replica that you want to modify. The remaining prompts are the same as the prompts for adding a Replica. For more information, see the preceding section, "Adding a Replica."

Replacing a Replica

To replace a Replica, type:

```
sdsetup -repmgmt replace
```

The utility prompts you to enter the name or IP address of the Replica that you want to replace, and then prompts you to enter the name of the new Replica. For more information on replacing a Replica, see "Replacing Replica Hardware" on page 146.

Note: RSA Security recommends that you shut down the Replica before you replace it. If you replace a Replica without first shutting it down, the Replica is removed from the database, but is not disabled. In this state, the Replica is unable to communicate with the Primary.

Deleting a Replica

To delete a Replica, type:

```
sdsetup -repmgmt delete Replica name
```

Deleting a Replica removes the entry for the Replica from the database.

Important: Shut down the Replica to stop it from authenticating users, and uninstall the RSA Authentication Manager software from the Replica machine if you do not plan to use the Replica again.

Displaying the Authentication Manager Information

To display information about all Replicas, type:

```
sdsetup -repmgmt list
```

To display information about one Replica, type:

```
sdsetup -repmgmt list Replica name
```

The following table describes the information displayed by the **list** option.

Information	Description
Replica #	The Replica number of the selected Authentication Manager and the hostname of the Authentication Manager.
Internet Address	The IP address of the Authentication Manager.
Service Name	The name of the service that the Primary and the Replica use to communicate. The default name is **securidprop_##**, where ## is a two digit number from 00 to 10.
Service Number	The port number that the Primary and Replica use to communicate.
Startup Delay Interval	The number of seconds after Primary startup that the replication service starts. On a Primary, this field is not used.
Replication Interval	How often databases changes are replicated, in seconds.
Enabled	Whether or not the Replica is able to authenticate users and replicate database changes with the Primary. Possible values: **0**: the Replica is not able to authenticate users or replicate changes. **1**: the Replica is capable of authenticating users and replicating database changes with the Primary.
Primary	Whether the Authentication Manager is the Primary or a Replica. Possible values: **0**: Replica **1**: Primary
Connected	Whether or not the Primary and Replica have successfully performed the initial communication pass. Possible values: **0**: initial communication between the Primary and Replica has not occurred. **1**: initial communication between the Primary and the Replica was successful.

Information	Description
Replica Marked for Unconditional Push	If **1**, you recovered your Primary by restoring a backup copy of the database to the Primary. The new database must be delivered to all existing Replicas through Push DB Assisted Recovery. You must allow Push DB Assisted Recovery in the System Parameters of the Primary so that the Primary can push the database. Applying full or partial Replica Package to the Replicas is not required. Otherwise, the value is **0**.
Replica Sequence Number	The Replica Sequence Number is used to ensure that the correct database is being used by the Primary and the Replica. This number is incremented at various times (for example, when you add a Replica or generate a Replica Package). When the Replica starts and attempts to connect to the Primary, both Authentication Managers check the value of the Connected flag, and the value of the Replica Sequence Number. Matching Replica Sequence Numbers indicate that the correct Replica Package was installed on the Replica. If the two numbers do not match, the Replica shuts down, and a new Replica Package must be created on the Primary and sent to the Replica.

Changing the Name or IP Address of the Primary

To rename or change the IP address of the Primary:

1. On the Primary, change to the ***ACEPROG*** directory.
2. To change the name of the Primary, type:

   ```
   sdsetup -repmgmt modify old name name new name
   ```

   To change the IP address of the Primary, type:

   ```
   sdsetup -repmgmt modify old address address new address
   ```

   To change both the name and the IP address of the Primary, type:

   ```
   sdsetup -repmgmt modify old name name new name address
   new address
   ```

3. Change the name or IP address on the Primary system, and restart the machine.
4. At the prompt, type:

   ```
   ACEPROG/sdsetup -repmgmt list
   ```

   When Replication Management runs, it detects whether or not the system name (or IP address) and the Primary name in the database match.

When you see the following message, type **y** to confirm the change.

```
The name and/or IP address of this Primary Server has
changed

from:
old_namenn.nn.nn.nn
to:
new_namenn.nn.nn.nn
Type 'No' to cancel:
```

If you see either of the following messages, you either did not change the system information, or you changed the system information to something different than what you specified in step 2.

```
You are about to complete the change of this Primary
Server's name and/or IP address, however, the name
previously specified does not match the name of this
system.
Do you want to accept this name? [new_name]
Enter 'YES' to continue or \NO' to cancel

You have initiated the procedure to change the name
and/or IP address of this primary RSA ACE/Server. The
name and/or IP address of this system has not yet changed.
Follow the instructions for changing the name and reboot
the system.
```

5. If Push DB is enabled on the Primary, copy only the ***ACEDATA*\replica_package\license** directory to all Replicas. If Push DB is disabled on the Primary, copy the ***ACEDATA*\replica_package** directory to all Replicas.

   For more information about Push DB, see the *UNIX Installation Guide*.

6. Apply the Replica Package. On the Replica, type:

   ```
   ACEPROG/sdsetup -apply_package pathname
   ```

   where *pathname* is the location of the Replica Package files.

As a result of changing the name of the Primary, you may need to perform the following tasks.

Note: RSA Security recommends you use Remote Administration to perform these tasks so that, where necessary, you may view associated Help topics. To enable Remote Administration, you must first perform, on the Primary, the task described in the first bulleted item. Then, on a Remote Administration machine, you can perform the other tasks in any order. For information about Remote Administration, see the *UNIX Installation Guide* or Chapter 2, "Using RSA Authentication Manager Administration Applications."

- For all Remote Administration machines, copy the **sdconf.rec** and the **server.cer** file from the ***ACEDATA*** directory on the Primary to the Remote Administration machine, remove the Primary from the Remote Administration machine, and then add the Primary using the new **sdconf.rec** file. For more information, see the *UNIX Installation Guide*.

- If the Authentication Manager is specified as a Local Realm Authentication Manager or a Remote Realm Authentication Manager for cross-realm authentication, edit the realm record in the local and remote realm databases to reflect the new name or IP address. For more information, see the Help topic "Edit Realm."
- If the Authentication Manager is specified as a RADIUS server, configure all RADIUS clients to use the new name or IP address. For specific configuration instructions, see the NAS device manual. In addition, you must modify the RSA RADIUS server's Agent Host record to reflect the new name or IP address. For instructions, see "Adding Servers as Agent Hosts to the Primary Database" in the *UNIX Installation Guide*.
- If the Authentication Manager is specified as an Acting Authentication Manager for legacy Agent Hosts, generate new **sdconf.rec** files for all legacy Agent Hosts that use this Authentication Manager as an Acting Master or Acting Slave, and distribute the **sdconf.rec** file to the Agent Hosts. For more information, see the Help topic "Assign Acting Servers."
- If the Authentication Manager is specified in any **sdopts.rec** files for version 5 Agent Hosts, edit the **sdopts.rec** file on the Agent Host to reflect the new name or IP address of the Authentication Manager.

Authenticating Across Multiple Network Interfaces

Note: For information about authenticating across all network interfaces for Windows, see "Authenticating Across Multiple Network Interfaces" on page 244.

To configure your RSA Authentication Manager to authenticate across multiple network interfaces, you must create an alias IP address list and then generate new configuration files for each alias IP address.

To create an alias IP address list:

1. Shut down all processes on the Primary. For directions, see "Command Line Tasks" on page 271.
2. On the Primary, change to the ***ACEPROG*** directory.
3. At the prompt, type:
   ```
   sdsetup -repmgmt modify
   ```
4. At the prompt, enter the name of the Authentication Manager you are modifying. This Authentication Manager will be the *multihomed* Authentication Manager.
5. Accept the defaults for **Replica Service Name**, **Startup Delay Interval**, and **Replication Interval**.
6. At the **Alias1** prompt, enter the alias IP address for the Authentication Manager.
7. Repeat step 6 for the **Alias2** and **Alias3** prompts.

Note: The maximum number of alias IP addresses allowed is three.

8. Restart the Primary.

Although you can perform the following procedure in TTY mode, RSA Security recommends that you perform the procedure through Remote Administration. For information about Remote Administration, see the *UNIX Installation Guide* or Chapter 2, "Using RSA Authentication Manager Administration Applications."

To generate configuration files for each alias IP address:

1. Through a Remote Administration interface, click **Agent Host > Add Agent Host**.
2. Add the RSA Authentication Agent to which you will assign the alias IP address. For instructions, see the Help topic "Add Agent Host."
3. When you have finished adding the RSA Authentication Agent as an Agent Host, click **Assign Acting Servers**.
4. Where the multihomed Authentication Manager is an Acting Master or Acting Slave, from the IP Address drop-down menu, select the appropriate alias IP address.
5. Click **Generate Config File**.
6. If prompted, click **Yes**.
7. Save the new **sdconf.rec** file in the desired location.
8. Copy the new **sdconf.rec** to the **%*SYSTEMROOT*%\system32** directory (Windows) or ***ACEPROG*** (UNIX) directory on the RSA Authentication Agent for which it was created.
9. Repeat steps 1 through 8 for each alias IP address you added.

Command Line Tasks

You can run the Replica Management utility at any time to view the information about the Authentication Managers. However, to make changes to the Authentication Manager information, you must shut down the database brokers. Shutting down the brokers disconnects all administrative sessions connected to the database.

Syntax

The **sdsetup -repmgmt** utility has the following syntax:

```
sdsetup -repmgmt [add|modify [Replica name|IP address]]
[name|address|servicename|port|delay|interval|alias IP
address, IP address, IP address]
sdsetup -repmgmt [list|delete] Replica_name
```

The following table describes the options of the **sdsetup -repmgmt** utility.

Option	Argument	Description
add	name *Replica name* or address *Replica IP address*	Adds a Replica Authentication Manager to the database.
list	*Replica name* or *Replica IP address* or None	Lists detailed information about all Replica Authentication Managers when no argument is provided or lists information about the Replica Authentication Manager you specify as the argument.
delete	*Replica name* or *Replica IP address*	Deletes the Replica Authentication Manager you specify.

Option	Argument	Description
modify		Where you can change configuration information for a particular Replica. You must specify the Replica by its fully qualified name or IP address. You can change the following information:
	Replica name or ***Replica IP address***	The name of the Replica (or Primary) Authentication Manager.
	address ***IP address of the Replica (or Primary)***	The IP address of the Replica (or Primary) Authentication Manager.
	name ***name of the Replica (or Primary)*** **servicename** ***name of the service***	The name of the service used for Primary/Replica communication. If you change the service name on the Primary, you must use the **sdsetup -port_config** command to change the service name on the Replica.
	port ***port number***	The port number used for Primary/Replica communication. If you change the service port number on the Primary, you must use the **sdsetup -port_config** command to change the service port number on the Replica.
	delay ***number of seconds***	The number of seconds after Primary startup that the replication service starts.
	interval ***number of seconds***	The amount of time the Primary and Replica wait before attempting to reconcile.
	alias ***ip1*****,** ***ip2*****,** ***ip3***	The alias IP addresses of the Authentication Manager. Alias IP addresses can be used to allow Agent Hosts to send authentication requests through firewalls. A maximum of three aliases is allowed.

Adding a Replica (Command Line)

To add a Replica, type:

```
sdsetup -repmgmt add name Replica name
```

The Replica is added to the RSA Authentication Manager database, and the name and information about the Replica displays when you use the **list** option.

Optionally, you can assign alias IP addresses to the Replica when you add the Authentication Manager to the database. Type:

```
sdsetup -repmgmt add name Replica name alias IP address, IP
address, IP address
```

You can add up to three alias addresses per Authentication Manager. You can assign aliases after adding the Replica by using the **modify** option, but you are still limited to three aliases.

When you have finished adding Replicas, you still need to create a Replica Package. For information, see the *UNIX Installation Guide*.

Assigning an Alias IP Address (Command LIne)

You can assign up to three alias IP addresses to an Authentication Manager. To assign an alias IP address to an Authentication Manager, type:

```
sdsetup -repmgmt modify Replica_name alias IP address, IP
address, IP address.
```

If you need to change one of the IP addresses, you must retype each alias that you want to keep in the list, and substitute the new IP address for the deleted IP address.

For example, if the list of aliases includes the following IP addresses:

```
1.2.3.4
1.2.3.5
1.2.3.6
```

and you want to replace alias **1.2.3.6** with **1.2.3.7**, type:

```
sdsetup -repmgmt 1.2.3.4, 1.2.3.5, 1.2.3.7
```

If you then want to clear **1.2.3.5**, and keep the other aliases, type:

```
sdsetup -repmgmt 1.2.3.4, 1.2.3.7
```

If you want to clear all aliases, type:

```
sdsetup -repmgmt ,,
```

Note: You can also assign alias IP addresses when you add the Replica, using the **add** option.

Modifying Replica Information (Command Line)

When you modify Replica information (for example, the service name or service port number), the changes are not be viewable on any Replica until the next replication pass. To view the most up-to-date information about a Replica, run the Replication Management utility on the Primary. To display information about all Replicas, type:

```
sdsetup -repmgmt list
```

To display information about one Replica, type:

```
sdsetup -repmgmt list Replica name
```

The following example illustrates how to change the startup delay interval from the default value of 10 to a new value of 15. For a full description of the arguments for the **modify** option, see the *UNIX Installation Guide*.

To change the startup delay interval:

1. Change to the ***ACEPROG*** directory.
2. At the command line, type:

   ```
   sdsetup -repmgmt modify Server_name delay 15
   ```

To change the service name or service port number:

1. Change to the ***ACEPROG*** directory.
2. At the command line, type:

   ```
   sdsetup -port_config portnum "new_portname" "new_portnum"
   ```

   where *portnum* is the original port number, *portname* is the new port name, and *new_portnum* is the new port number. If want to retain the name or port number, include empty quotes in place of the new name or number. For example, to change the information for port 5508 from securidprop_03 to securidprop_20, type:

   ```
   sdsetup -port_config 5508 "" "securidprop_20"
   ```

To change the name or IP address of the Replica:

1. Change the name or IP address of the Replica system in the OS, and restart the machine.
2. On the Primary, change to the ***ACEPROG*** directory.
3. Use the **ping** or **telnet** command to make sure the Primary can access the Replica that you are modifying.
4. Change the Replica name, the Replica IP address, or both, in the RSA Authentication Manager, as follows:

   To change the name of the Replica, type:

   ```
   sdsetup -repmgmt modify oldname name newname
   ```

   To change the IP address of the Replica, type:

   ```
   sdsetup -repmgmt modify oldaddress address newaddress
   ```

   Note: When you change the name of the Replica, the RSA Authentication Manager resolves the IP address automatically. Likewise, if you change the IP address of the Replica, the RSA Authentication Manager resolves the name automatically.

5. At the prompt, type:

   ```
   sdsetup -repmgmt list Replica_name
   ```

   where *Replica_name is the new Replica name.*

   When Replication Management runs, it detects whether or not the system name (or IP address) and the Replica name in the database match.

   If the information does not match, you either did not change the system information, or you changed the system information to something different than what you specified in step 4.

6. If Push DB is enabled on the Primary, copy only the ***ACEDATA*\replica_package\license** directory to the Replica. If Push DB is disabled on the Primary, copy the ***ACEDATA*\replica_package** directory to the Replica.

   For more information about Push DB, see the *UNIX Installation Guide*.

7. Apply the Replica Package. On the Replica, type:

   ```
   ACEPROG/sdsetup -apply_package pathname
   ```

   where *pathname* is the location of the Replica Package files.

As a result of changing the name of the Replica, you may need to perform the following tasks.

Note: RSA Security recommends that you use Remote Administration to perform these tasks so that, where necessary, you may view associated Help topics. For information about Remote Administration, see the *UNIX Installation Guide* or Chapter 2, "Using RSA Authentication Manager Administration Applications."

- If the Authentication Manager is specified as a Local Realm Authentication Manager or a Remote Realm Authentication Manager for cross-realm authentication, edit the realm record in the local and remote realm databases to reflect the new name or IP address. For more information, see the Help topic "Edit Realm."
- If the Authentication Manager is specified as a RADIUS server, configure all RADIUS clients to use the new name or IP address. For specific configuration instructions, see the NAS device manual. In addition, you must modify the RSA RADIUS server's Agent Host record to reflect the new name or IP address. For instructions, see "Adding Servers as Agent Hosts to the Primary Database" in the *UNIX Installation Guide*.
- If the Authentication Manager is specified as an Acting Authentication Manager for legacy Agent Hosts, generate new **sdconf.rec** files for all legacy Agent Hosts that use this Authentication Manager as an Acting Master or Acting Slave and distribute the **sdconf.rec** file to the Agent Hosts. For more information, see the Help topic "Assign Acting Servers."
- If the Authentication Manager is specified in any **sdopts.rec** files for version 5.0 (or later) Agent Hosts, edit the **sdopts.rec** file on the Agent Host to reflect the new name or IP address of the Authentication Manager.

A Licensing

This appendix describes RSA Authentication Manager licensing, including the following topics: active user, license types, license enforcement, licensing for cross-realm environments, and the procedure for upgrading a license.

Active Users

RSA Authentication Manager uses the concept of active user in license enforcement. An active user has

- A user record in the RSA Authentication Manager database
- At least one and as many as three tokens (or a combination of a user password and up to two tokens) assigned to the user

For example, a user who has two assigned tokens and one assigned user password counts as *one* active user. A user who is listed in the RSA Authentication Manager database but does not have an assigned token or user password is *not* an active user.

Note: A user with an assigned expired token counts as an active user. For information about unassigning expired tokens, see the Help topic "Unassigning a Token."

License Types

RSA Authentication Manager enforces two types of permanent licenses: the Base license and the Advanced license.

Note: RSA Authentication Manager also enforces the Evaluation license, which is a temporary trial license.

With the RSA Authentication Manager Base license your organization can use the RSA Authentication Manager software

- With the number of active users specified by the active-user tier that your organization purchased.
- On only one Primary and one Replica in one realm.

With the RSA Authentication Manager Advanced license your organization can use the RSA Authentication Manager software

- With the number of active users, throughout your installation, specified by the active-user tier that your organization purchased.

  Note: The number of active users is per installation, *not* per realm. For example, if you have a 1000-user limit and two realms, you can have a maximum of 1000 users across both realms. You cannot have 1000 users in each realm. For more information, see "Cross-Realm Environments" on page 280.

- On 1 Primary and up to 10 Replicas in up to 6 realms. You must purchase multiple Advanced licenses if you want to install the software in more than 6 Realms. For example, if you want 10 realms, purchase 2 Advanced licenses.
- Installed on a qualified High Availability hardware system. Currently, the only qualified High Availability platform is Veritas Cluster Server on Solaris 9.

Enforcement of License Limits

RSA Authentication Manager 6.1 software enforces license limits both during installation and in the normal course of daily operation and administration.

License Enforcement During Installation

Whether you are upgrading from an older version of RSA Authentication Manager or performing a new installation, you must specify the location of your license file (**license.rec**). This can be a Version 3 (pre-5.1 format) or Version 4 (5.1, 5.2, and 6.0) license file on the original diskette or copied to a hard drive location.

If you are upgrading from a previous version of RSA Authentication Manager, the setup program verifies that your current installation is valid under the terms of your current license. If the database exceeds the licensed number of active users or Replicas, the upgrade places your RSA Authentication Manager in *upgrade violation* mode. Upgrade violation mode effectively turns your license into a 90-day temporary license. When your license expires, it goes into *violation* mode, meaning you are prevented from activating additional users and/or adding new Replicas.

You must bring your RSA Authentication Manager 6.1 into compliance within 90 days by doing one of the following:

- Removing Replicas or reducing the number of active users, depending on your upgrade violation
- Purchasing a new license from RSA Security

To purchase a new license, contact your RSA Security sales representative or local distributor, or go to **www.rsasecurity.com/contact/**.

The table on page 279 describes the different license modes for the RSA Authentication Manager.

License Enforcement During Daily Operation and Administration

During normal RSA Authentication Manager 6.1 administration, a valid license can go into *violation* mode. Periodically, the RSA Authentication Manager checks for license compliance. If, for example, you activate more users than your license allows, RSA Authentication Manager detects this and displays a warning message:

```
There are too many active users in the database
```

When your license is in violation mode, you cannot activate additional users or add new Replicas.

You must bring your RSA Authentication Manager 6.1 into compliance immediately by doing one of the following

- Removing Replicas or reducing the number of active users, depending on your upgrade violation
- Purchasing a new license from RSA Security

To purchase a new license, contact your RSA Security sales representative or local distributor, or go to www.rsasecurity.com/contact/.

The following table describes the different license modes for the RSA Authentication Manager.

Mode	Why You Are In This Mode	What You Can Do In This Mode
License Compliant	The number of active users and Replicas in the RSA Authentication Manager database is within license limits.	You can activate additional users and, if you have an Advanced license, add new Replicas.
Upgrade Violation	You have upgraded from a previous version of RSA Authentication Manager, and the number of active users and Replicas in the RSA Authentication Manager database exceeds license limits.	Upgrade Violation mode converts your license into a 90-day temporary license. For 90 days, you can continue to activate additional users and add new Replicas.
Violation	• The 90-day *upgrade violation* period has expired. • During normal RSA Authentication Manager 6.1 administration, you activated more users and added more Replicas than your license allows.	You cannot activate additional users or add new Replicas.

Cross-Realm Environments

To support a cross-realm environment, your organization must have one or more Advanced licenses that support the total number of active users across all realms.

The following table describes some example cross-realm situations and the licenses needed to support them.

Situation	License Requirement
Your company wants to set up a cross-realm relationship between two divisions. One division has an Advanced license, and the other one has a Base license.	One of the following: • The division with a Base license must upgrade to its own Advanced license. • The division with the Base license can upgrade to the other division's Advanced license, provided the Advanced license can support the additional users and realms. (One Advanced license can be used for up to six realms.)
Your company wants to set up a cross-realm relationship between two divisions, both of which have Base licenses.	One of the following: • Both divisions can upgrade to separate Advanced licenses. • Both divisions can upgrade to one Advanced license that supports the total number of users across both realms.
Your company wants to establish a cross-realm relationship with another company.	Each company must have its own Advanced license.

Upgrading or Converting Your License

If you have exceeded your license limits or your evaluation license has expired, you must obtain a new **license.rec** from RSA Security. Contact your RSA Security sales representative or local distributor, or go to **www.rsasecurity.com/contact/**.

For information about updating the **license.rec** on the RSA Authentication Manager, see "License Information" on page 267 or "Updating Your License Record in RSA Authentication Manager for UNIX" on page 251.

B Services and Processes

Note: For information about RSA RADIUS Server services and processes, see the *RSA RADIUS Server 6.1 Administrator's Guide*.

Services With Network Ports (Windows and UNIX)

The following table contains information about the default network ports that the RSA Authentication Manager uses.

Service Name	Port Number	Protocol	Direction	Use
securid	5500	UDP	• From RSA Authentication Agents to RSA Authentication Manager • From RSA Authentication Manager to RSA Authentication Manager in cross-realm environment	• RSA Authentication Agent communication for RSA SecurID authentication, including applications that are built with the RSA Authentication Agent API. For example, Remote RADIUS Server. • Cross Realm Authentication

securidprop_00 to **securidprop_10,** where **securidprop_00 = 5505, securidprop_01 =5506**, etc.	5505 to 5515	TCP	From Primary to Replica	Database replication between the Primary and all Replicas, where
				securidprop_00 = 5505 (Primary),
				securidprop_01 = 5506 (first Replica),
				securidprop_02 = 5507 (second Replica), and so on

sdlockmgr	5560	TCP	Any Primary or Replica to other Authentication Managers in the realm	Lock Manager communication with all other Authentication Managers in the realm. The Primary and Replicas require this service, which is used for the high-speed propagation of authentication information when RSA SecurID authentication occurs.

Service Name	Port Number	Protocol	Direction	Use
sdreport	5540	TCP	Local	Local report database communication. You do not have to open this port in the firewall.
sdadmind	5550	TCP	From Remote Administration or Agent Host auto-registration to the RSA Authentication Managers	Remote Administration authentication and Agent Host auto-registration.
sdcommd	5570	TCP	From Web Server to Primary Server	Communication between the **ACECOMPROXY** running on a Web server and the RSA Authentication Manager database. For example, Quick Admin, RSA SecurID Web Express.
sdlog and sdserv	5520 and 5530	TCP	From Remote Administration to any Primary or Replica in the realm	Remote Admin ports, used for connections to the **sdlog** and **sdserv** databases. Once the initial connection is established, the Progress Software database broker hands the connection to a dynamically allocated port (for instance, **-minport**, **-maxport**) for continued processing by the database broker.
sdlog and sdserv	-minport to -maxport	TCP	From Remote Administration to any Primary or Replica in the realm	Remote Admin database connection, which uses two ports per session. Configure in **/ace/rdbms32/startup.pf** on Windows and **/ace/prog/sdserv.pf** and **/ace/prog/sdlog.pf** on UNIX. On Windows the **–minport** must be greater than 3000. On all systems the **–maxport** must be less than the maximum port range that the system supports.

Service Name	Port Number	Protocol	Direction	Use
sdoad	5580	TCP	From RSA Authentication Agent 6.1 to the Primary From the Primary to RSA Authentication Agent 6.1	Offline authentication events (OA data download requests, password integration and updates, log uploads, and so on)
tacacs	49	TCP	From TACACS+ client to all RSA Authentication Managers	(UNIX only) TACACS+ communication.
aceserv_be.exe (Windows) **_aceserver_be** (UNIX)	MinimumBE port MaximumBE port	UDP	Local only or cross-realm	Define the range of ports on which the RSA Authentication Manager **acesrvc_be.exe** (Windows) and **_aceserver_be** (UNIX) communicate. You must define a range of at least 11 ports and configure the ranges in the firewall. Use any available ports. For example: MINIMUM_BE_PORT=10000 MAXIMUM_BE_PORT=10010 On Windows, set up through the RSA Authentication Manager Control Panel. On UNIX, set up through the environment variables **MINIMUM_BE_PORT** and **MAXIMUM_BE_PORT**.

RSA Authentication Manager Processes (Windows and UNIX)

You can view the RSA Authentication Manager processes in the Windows Task Manager or by running the **ps** command on a UNIX machine.

Process	Description
_mprshut	Performs tasks related to the **sdserv** and **sdlog** databases. Multiple instances of this process run on the system.
jsed	Enables the RSA Authentication Manager to schedule system maintenance tasks. Commonly referred to as the job scheduler.
logmaintthd	Performs log maintenance tasks.
_mprosrv	Controls the database broker and database server processes. The broker controls the database and its shared memory. When the network requests a connection to the database, such as in a Remote Administration connection, the broker starts a database server process. The **sdlog** and **sdserv** databases each have one database broker process. Any number of server processes can be running at one time, depending on the number of network requests.
sdadmind	Connects Remote Administration authentication and Agent Host auto-registration to the RSA Authentication Manager.
_aceserver_fe (UNIX) **acesrvc (Windows)**	RSA Authentication Manager authentication engine processes referred to as the *front end*. For authentication, one front end process can be associated with multiple back end processes. Authentication attempts go to the front end process first. The front end process then distributes the authentication attempts to back end processes as they become available. You can configure authentication processes through the RSA Authentication Manager Control Panel on the Primary or Replica.
_aceserver_be (UNIX) **aceservc_be (Windows)**	RSA Authentication Manager authentication engine processes referred to as the *back end*. Multiple back end processes, which receive authentication requests from the front end process, can run at one time. You can configure authentication processes through the RSA Authentication Manager Control Panel on the Primary or Replica.
sdcommd	Represents the Quick Admin daemon, which provides Quick Admin and Web Express with access to the RSA Authentication Manager database.

Process	Description
acesyncd (UNIX) **syncservc (Windows)**	Represents the replication process. On the Primary, one **acesyncd** process runs for each active Replica. On each Replica, only one **acesyncd** process runs.
brksrv (Windows only)	Starts and stops the RSA Authentication Manager brokers.
sdoad	Receives and services offline authentication events from RSA Authentication Agents (OA data download requests, password integration and updates, log uploads, and so on).

Service Control Manager Services (Windows Only)

The following table contains information about RSA Authentication Manager services that control the startup and shutdown of various elements of the RSA Authentication Manager. To administer these services, go to **Start > Programs > RSA Security > RSA Authentication Manager Control Panel**.

Service Name	Description
RSA Authentication Manager Administration Daemon	Handles Remote Administration requests
RSA Authentication Manager Authentication Engine	Provides authentication services
RSA Authentication Manager Broker	Provides database access
RSA Authentication Manager Job Executor Daemon	Performs job scheduling
RSA Authentication Manager Log Maintenance Daemon	Performs log maintenance
RSA Authentication Manager QuickAdmin Daemon	Provides Quick Admin and Web Express with access to the RSA Authentication Manager database

Service Name	Description
RSA Authentication Manager Replication Engine 0 to **RSA Authentication Manager Replication Engine 10**	Provides replication between the Primary and Replicas, where RSA Authentication Manager Replication Engine 0 = Primary, RSA Authentication Manager Replication Engine 1= first Replica, RSA Authentication Manager Replication Engine 2= second Replica, and so on The Primary runs one instance of the service for each Replica. On the Replica, only one instance of the service runs.
RSA RADIUS Server	Provides RSA RADIUS services. **Note**: This service is listed only if you have RSA RADIUS installed and it is a local installation.

C Troubleshooting

This appendix helps you understand and solve the most common RSA Authentication Manager problems. It includes the following sections:

- Sending Audit Log Messages to the Event or System Log
- Sample Event/System Logs
- Filtering Messages Using SNMP
- Error Conditions
- Procedures to Resolve Problems
- Messages (listed in alphabetical order)
- Message ID Numbers

Note: Authentication Manager and Agent Host data directories are referred to as the ***ACEDATA*** directory, and the executables directory is referred to as the ***ACEPROG*** directory. When these names appear in bold italics (***ACEDATA***, ***ACEPROG***), they stand in place of the actual directory name.

Sending Audit Log Messages to the Event or System Log

You can use the **Log to System Log** option to direct Authentication Manager-related audit log messages to your Event log (on Windows) or system log (on UNIX). Only Authentication Manager-related messages can be sent to the log. You can specify criteria to select the kinds of messages sent to the log so that it captures only the information you need. On Windows, messages from the RSA Authentication Manager appear in the Application log portion of the Event log.

Note: Database Administration application messages cannot be directed to the Event log.

You can use the **Log to System Log** feature in several ways:

- Set your selection criteria, and then activate **Log to System Log** at peak times to collect messages for monitoring purposes.
- Activate **Log to System Log** with certain criteria, and then change criteria while the Authentication Manager is running to collect information for troubleshooting a specific condition.
- Configure your Event log to send all messages captured from the audit log to a particular file, or to send different types of audit log messages to different files.
- Use a commercial network management tool to monitor Authentication Manager activities by checking for particular audit log messages in the Event log.

You can turn the **Log to System Log** feature on and off from the Database Administration main menu and change message selection criteria whether the RSA Authentication Manager is running or stopped. If the Authentication Manager is running, new selection criteria take effect only after you stop and restart it. If the Authentication Manager is not running, your changes take effect the next time you start it.

Note: Messages are sent to the Event log or system log only when the Authentication Manager is running.

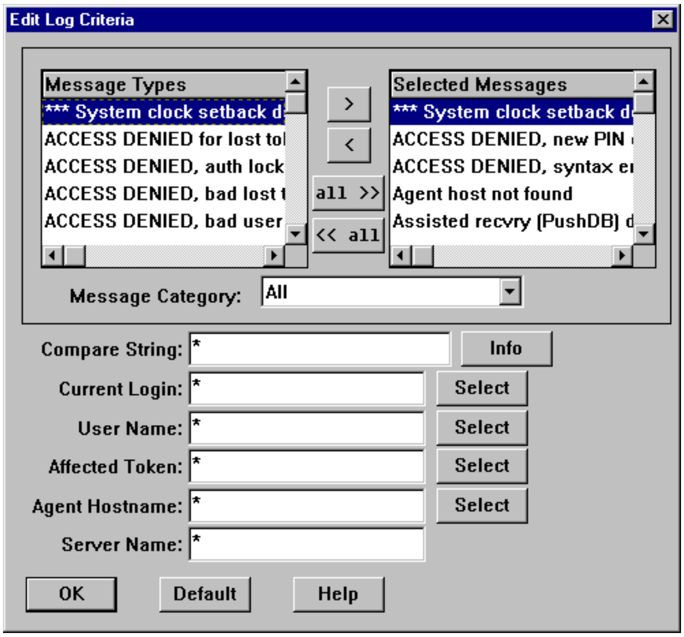
You can apply the following criteria when selecting messages for the Event log: message type, current login, affected user name, affected token, Agent Host, or Authentication Manager. You can also match messages against a string. Depending on how complex you make your selection criteria, you may notice a slight decrease in Authentication Manager performance as the system evaluates messages against the criteria and writes messages to the Event log or system log.

To use this feature, click **Log** > **Log to System Log**.

To set selection criteria for sending audit log messages to the Event log or system log:

1. Click **Log** > **Edit System Log Parameters**.

   The Edit Log Criteria dialog box opens, displaying a list of message types for selection, a list of messages already selected to be sent to the Event Log or system log, and additional selection criteria.



Message Types
*** System clock setback d
ACCESS DENIED for lost to
ACCESS DENIED, auth lock
ACCESS DENIED, bad lost t
ACCESS DENIED, bad user

Selected Messages
*** System clock setback d
ACCESS DENIED, new PIN
ACCESS DENIED, syntax er
Agent host not found
Assisted recvry (PushDB) d

Message Category: All

Compare String: *

Current Login: *

User Name: *

Affected Token: *

Agent Hostname: *

Server Name: *

Note: When RSA Authentication Manager is installed, messages in the Exception/Incident category are set to be sent to the Event log.

2. To change the message types available for selection in the **Message Types** list, select a **Message Category** from the drop-down list.

   The following table describes the **Message Category** options:

Message Category	Activities Included
Exception/Incident	Illegal authentication activity and attempts
Authentication Manager	Authentication activity and operations
Syncsrvc	Reconciliation activity
Realm	Cross-realm activity
Radius	RADIUS server activity
Offline Authentication	Offline authentication events, such as viewing emergency passcodes, failed downloads, and so on.

3. To add a message type to the list of selected messages, highlight the message type in the **Message types** list, and click > . To select all message types in the current category, click **all** >> .

   To remove a message type from the **Selected Messages** list, highlight the message type, and click < . To remove all messages in the current category, click << **all**.

4. Use the selection fields to apply additional criteria to the message types that you have selected.

   Click the **Select** buttons to select from a list of identifiers. If you type in the fields instead of using the **Select** buttons, enter the specifications carefully. The system does not verify that you have entered valid identifiers. For example, if you type user name **Jon Smith** and the correct user name is **John Smythe**, you are not told that user name **Jon Smith** does not exist.

Select Messages By	To Send These Messages to the Event Log
Current Login	Messages regarding operations performed by the specified user. Enter the user's login, not the user's name.
User Name	Messages regarding operations that affected a specific user. Enter the user's name, not the user's login.
Affected Token	Messages regarding operations that affected a specific token. Specify the token serial number.
Agent Host Name	Messages that reflect activity related to the named Agent Host.
Authentication Manager Name	Messages that reflect activity on a specific Authentication Manager (the Primary, the Replica, or a remote realm).

If you leave a selection field blank, the field is not used in determining which messages are sent to the Event Log or system log.

To reset all selection criteria to the default values, click **Set To Defaults**. The default is to select all Exception/Incident messages. No other criteria are used.

5. To select log messages created by activities of more than one login, user, token, Agent Host, or Authentication Manager, enter the names or token serial numbers as strings in the **Compare String** field. Enter the names or serial numbers *exactly* as they appear in the Authentication Manager database.

   Click **Info** for assistance in using this field. You can enter one or more strings, delimited by the pipe character (|). Do not include any spaces on either side of the delimiter, and place a delimiter after the last string.

6. To reset all selection criteria to the default values, click **Default**. The default behavior sends all Exception/Incident messages to the Event log or system log.

7. When you have finished setting your selection criteria, click **OK**. If you have changed any criteria since you opened the Edit Log Criteria dialog box (in step 1), **Log to System Log** is toggled on automatically.

To start or stop sending audit log messages to the Event log:

- On the Log menu, click **Log to System Log** to turn this feature on or off. When **Log to System Log** is on, the menu item is preceded by a check mark.
- Before Log to System Log can be turned on, at least one message type must be selected to send to the system log. If no message type is selected, use **Edit System Log Parameters** to select at least one.

Note: When RSA Authentication Manager processes write more than 10,000 records to the Event Log or system log in one day, the message "Too Many Syslog Messages Per Day" appears in the log and the log count is reset to 0.

Sample Event/System Logs

This section provides sample Primary and Replica Authentication Manager Event logs (system logs on UNIX) that show typical transactions. General descriptions of error messages that appear in the Event Log for Replica Authentication Manager operation and database reconciliation follow the sample logs. If you need additional help in understanding the logs of **syncsrvc** (**acesyncd** on UNIX) events, contact RSA Security Customer Support. Be prepared to read the contents of the Event Log entry to the customer service representative.

Sample Event/System Log on the Primary Authentication Manager

```
Acesyncd Primary Started  0 0. [acesyncd.c.529.1]
Primary Unable To Connect To Replica 145.1.5.40 Port 7512 MsgLib Connect()....
Primary Will Retry Every 30 Seconds  0 0. [mloop.c.87.3]
Primary Has Connected To Replica  0 0. [mloop.c.66.4]
Primary Requesting LogEntry Changes From Replica  0 0. [mscomm.c.1264.5]
Primary Received 2 Modified LogEntry Records From Replica  0 0. [mscomm.c.1....
Primary Requesting Token Changes From Replica  0 0. [mscomm.c.1264.7]
Primary Received 0 Modified Token Records From Replica  0 0. [mscomm.c.135....
Primary Requesting Agent Host Changes From Replica  0 0. [mscomm.c.1264.9]
Primary Received 0 Modified Agent Host Records From Replica  0 0. [mscomm.c.135....
Primary Requesting System Changes From Replica  0 0. [mscomm.c.1264.11]
Primary Received 1 Modified System Records From Replica  0 0. [mscomm.c.13....
Primary Requesting LogEntry Changes From Replica  0 0. [mscomm.c.1264.13]
Primary Received 0 Modified LogEntry Records From Replica  0 0. [mscomm.c.1....
Primary Successfully Received Replica Records  0 0. [mloop.c.195.15]
Primary Sent 1 System Changes To The Replica  0 0. [perelt.c.409.16]
Primary Sent 100 User Changes To The Replica  0 0. [perelt.c.914.17]
Primary Sent 200 User Changes To The Replica  0 0. [perelt.c.914.18]
Primary Sent 300 User Changes To The Replica  0 0. [perelt.c.914.19]
Primary Sent 400 User Changes To The Replica  0 0. [perelt.c.914.20]
Primary Sent 500 User Changes To The Replica  0 0. [perelt.c.914.21]
Primary Sent 566 User Changes To The Replica  0 0. [perelt.c.970.24]
Primary Sent 100 Token Changes To The Replica  0 0. [perelt.c.1475.25]
Primary Sent 200 Token Changes To The Replica  0 0. [perelt.c.1475.26]
Primary Sent 300 Token Changes To The Replica  0 0. [perelt.c.1475.27]
Primary Sent 400 Token Changes To The Replica  0 0. [perelt.c.1475.28]
Primary Sent 500 Token Changes To The Replica  0 0. [perelt.c.1475.29]
Primary Sent 600 Token Changes To The Replica  0 0. [perelt.c.1475.30]
Primary Sent 700 Token Changes To The Replica  0 0. [perelt.c.1475.31]
Primary Sent 754 Token Changes To The Replica  0 0. [perelt.c.1531.35]
Primary Sent 21 Agent Host Changes To The Replica  0 0. [perelt.c.3214.36]
Primary Sent 24 Group Changes To The Replica  0 0. [perelt.c.4336.37]
Primary Sent 9 Administrator Changes To The Replica  0 0. [perelt.c.4897.38]
Primary Sent 100 EnabledGroup Changes To The Replica  0 0....
Primary Sent 131 EnabledGroup Changes To The Replica  0 0....
Primary Sent 100 GroupMember Changes To The Replica  0 0....
Primary Sent 200 GroupMember Changes To The Replica  0 0....
Primary Sent 300 GroupMember Changes To The Replica  0 0....
Primary Sent 400 GroupMember Changes To The Replica  0 0....
Primary Sent 479 GroupMember Changes To The Replica  0 0....
Primary Successfully Reconciled Databases  0 0. [mscomm.c.1019.49]
```

Sample Event Log on the Replica Authentication Manager

```
Replica Successfully Bound To Port 7512  0 0. [acesyncd.c.463.1]
Acesyncd Replica Started  0 0. [acesyncd.c.534.2]
Primary Has Connected To Replica  0 0. [sloop.c.79.3]
Replica Correcting Clock By -137 Seconds  0 0. [mscomm.c.736.4]
Primary Requesting Modified Log Entries From Replica  0 0. [mscomm.c.1812.5]
Replica Sent 2 Modified Log Entries To Primary  0 0. [mscomm.c.1834.6]
Primary Requesting Modified Token Records From Replica  0 0.
[mscomm.c.161....
Replica Sent 0 Modified Token Records To Primary  0 0. [mscomm.c.1639.8]
Primary Requesting Modified Agent Host Records From Replica  0 0.
[mscomm.c.167....
Replica Sent 0 Modified Agent Host Records To Primary  0 0.
[mscomm.c.1694.10]
Primary Requesting Modified System Records From Replica  0 0.
[mscomm.c.17....
Replica Sent 1 Modified System Record To Primary  0 0. [mscomm.c.1790.12]
Replica Sent 2 Modified Log Entries To Primary  0 0. [mscomm.c.1834.13]
Replica Successfully Reconciled Databases  0 0. [mscomm.c.1038.14]
```

Filtering Messages Using SNMP

To ease the burden of administrators who are using SNMP trapping, some of the messages include identification numbers, which can simplify the task of specifying which messages to trap. You can trap only the messages that the RSA Authentication Manager sends to the Event Log. In this appendix, the message numbers are in parentheses immediately following the message. Additionally, the section "Message ID Numbers" on page 390 contains tables that list the numbers of messages that share a common format, such as the "Cannot Check Dependency for *NAME*" messages.

Error Conditions

This section describes error conditions that can occur when

- users, including remote administrators, attempt to authenticate
- administrators use the Database Administration application

Important: If the RSA Authentication Manager system time is offset by any number of minutes, users who have never before authenticated to the RSA Authentication Manager or who have new tokens may not be able to gain access. **Do not** change the system time to accommodate new users, because this results in existing users being denied access. Instead, contact RSA Security Customer Support for assistance.

Authentication Error Conditions

A User Is Denied Access

If the Authentication Manager does not recognize a passcode as valid, it responds with **Access Denied**. For security purposes, no reason for failure is given to a person whose login attempts are unsuccessful. An authorized user who is being denied access needs your help to solve the problem.

To generate a report of a user's login attempts:

1. Run the Administration application.
2. Click **Report** > **Activity** to open the Report Selection Criteria dialog box.
3. Click **Date**.
4. Use the **From Date** and **To Date** fields to define the time period for which the user reported being denied access.

5. Click **OK** to close the Selection Criteria dialog box and generate the Activity report.

   If the report does not list any log records that correspond to the user's failed login attempts, see "No log record exists for the login attempt" on page 297.

   If the report contains log records that represent the user's failed login attempts, look in these records for the text of the message that was logged for the authentication attempt. This text is followed by a more detailed explanation of the problem and directions for solving it.

Under two kinds of circumstances, a positive log message is recorded in the audit trail (saying, for example, that the passcode was accepted or that the New PIN operation was completed successfully) even though the user sees a message reporting failure and is denied access:

- With the Authentication Manager and network under a heavy load, the Authentication Manager accepts the passcode or new PIN and attempts to inform the Agent Host, but the Agent Host times out before it receives the message. The Agent Host therefore displays **Access Denied** (or **PIN rejected**) to the user.

  Note: When a user has more than one token, access denials caused by Agent time-out may be more frequent because the Authentication Manager checks each token in turn until a match is found.

  When this occurs, either instruct the user to wait for the tokencode to change and then to try again until successful, or increase the **Agent Timeout** value and generate and distribute a new **sdconf.rec** file to each Agent Host. On Windows, use the Configuration Management application to increase the **Agent Timeout** value. On UNIX, use the **sdsetup -config** command.

- The encryption value in the **sdconf.rec** file (or other configuration method) on the Agent Host does not match the encryption type in the Agent Host record.

  If the encryption type is set incorrectly in the Agent Host record, on the Agent Host menu, click **Edit Agent Host** to change the setting. If the setting in the **sdconf.rec** file is incorrect, generate and distribute a new **sdconf.rec** file to the Agent Host.

For more information on distributing the **sdconf.rec** file, see "Distributing the Configuration Update" on page 243 (for Windows) or on page 259 (for UNIX).

All Users, Including Administrators, Are Denied Access

If all RSA SecurID tokenholders are being denied access, the Authentication Manager clock has probably been set inaccurately by more than a few minutes. Log on as an administrator on Windows or as root on UNIX, and follow the directions in the following section, "All Users Are Denied Access."

If administrator accounts are protected by RSA SecurID and administrators are also being denied access, contact RSA Security Customer Support.

All Users Are Denied Access

If no tokenholders can be authenticated, log on as an administrator on Windows or as root on UNIX, and check that the system clock is set accurately. Set it to the correct time and try again to authenticate. If administrator accounts are protected by RSA SecurID and administrators are also being denied access, contact RSA Security Customer Support.

If your system time cannot be set accurately for some reason, you must enter an offset into the RSA Authentication Manager database. The Authentication Manager then generates codes for authentication based on the system time as adjusted by this offset.

To set a system clock offset based on the difference between the Authentication Manager clock and a token clock:

1. Open the Database Administration application.
2. Click **System** > **Edit System Parameters**, and click **Set clock offset by token**.
3. A window listing token serial numbers opens. Highlight the token you will use to set the offset, and click **OK**.

   The Set Clock Offset by Token dialog box opens, prompting you for one tokencode from the selected token.
4. Enter the code currently displayed by the token, and click **OK**.

   A second prompt and box appear in the Set Clock Offset by Token dialog box. This second prompt instructs you to wait for the code to change.
5. Enter the next code that the token displays, and click **OK**. Click **OK** a second time to close the message box.
6. Click **OK** in the System Parameters dialog box.

   A value appears in the **Computed offset currently applied** field.
7. Click **OK** to close the System Parameters dialog box.
8. You are asked whether you want to save the changes to the system record. Click **Yes** to store the clock offset. If you click **No**, the offset and other system parameters remain unchanged.

To remove a system clock offset:

1. Click **System > Edit System Parameters**.
2. Click the **Set Server Clock Offset to 0** button.
3. Click **OK** to close the System Parameters dialog box.

   You are asked whether you want to save the changes to the system record.
4. Click **Yes** to store 0 as the clock offset. If you click **No**, the offset and other system parameters remain unchanged.

Agent Host hangs while trying to authenticate

Several conditions can prevent the Authentication Manager from responding to an Agent Host during an authentication attempt. Note that this problem sometimes causes the error message "Cannot initialize Agent Host-server communications" (page 320) to appear. At other times the system appears inactive and does not display a message.

To find the cause of the problem and enable Agent Host-Authentication Manager communications:

1. Verify that there is a network connection between the Authentication Manager and its Agent Hosts by issuing the **ping** command (in the **system32** directory) from the Authentication Manager to each of its Agent Hosts.
2. Make sure that the RSA Authentication Manager services are running.

   On Windows, click **Start** > **Programs** > **RSA Security** > **RSA Authentication Manager Control Panel**, and from the left-hand menu, click **Start & Stop** RSA Authentication Manager **Services**.

   On UNIX, as **root**, type:

   ```
   ps -ax | grep aceserver (For BSD)
   ps -ef | grep aceserver (For System V)
   ```

   If this command does not show an **aceserver** process, you must start one. First, start a database broker if one is not running already:

   ```
   ACEPROG/sdconnect start
   ```

   Then, start the aceserver process:

   ```
   ACEPROG/aceserver start
   ```
3. If the Authentication Manager process is running but this error occurs and the problem is with a UNIX Agent Host, check the permissions on the file **sdshell** on the Agent Host. Use the **ls -al** command to list the ***ACEPROG*** directory on the Agent Host. The permissions should be **--s--x--x**. If they are not, as **root**, change them by typing:

   ```
   chmod 4111 sdshell
   ```

Note: If there is no problem with the RSA Authentication Manager services or sdshell permissions, check the Agent Host information about the server. This problem is most likely to occur if the server is a gateway with two IP addresses.

4. If the problem is not with the RSA Authentication Manager services or **sdshell** permissions, check that the Agent Host has accurate information about the location of the Authentication Manager. Use the Configuration Management application to display the IP address. Review the contents of the Agent Host **sdconf.rec** file, using the utility appropriate to the Agent Host (for example, use the Authentication Test feature on a Windows Agent Host and the **sdinfo** command on a UNIX Agent Host).

   On a legacy Agent Host, when the information is displayed, note the Authentication Manager names and addresses. Log in as an administrator on the RSA Authentication Manager Primary or a Remote Administration machine, and run the Database Administration application. Click **Agent Host** > **Edit Agent Host** > **Assign Acting Servers**. The Current Server Assignments should match the designated Master and Slaves in the Agent Host configuration file unless the Agent Host record uses an alias IP address of the designated Acting Authentication Manager. Click **Help** for more information.

   If it is the Agent Host that lists inaccurate information, generate a new configuration file for the Agent Host and copy it to the Agent Host.

Administration Error Conditions

Deleting or listing items gives error message

If you receive an error message when you try to use a list option (for example, **List Agent Hosts** or **List Groups**) or a delete option (for example, **Delete Users** or **Delete Tokens**), try the operation again. One or more records were probably locked because they were being used for authentication or by another administrator. If the problem persists, verify that your Authentication Manager has not run out of disk space.

Names changed by conversion or import

You may notice minor modifications in some names after records are imported or converted from an earlier version of the RSA Authentication Manager. The import and conversion procedures use the following rules to translate illegal characters to valid characters for use with the Authentication Manager:

- A TAB is changed to a space.
- Nonprintable characters are changed to spaces.
- Leading and trailing spaces are discarded.
- A percent sign (%) is changed to a space.

These modifications can affect the user name, shell, Agent Host name, and group name fields.

No log record exists for the login attempt

If unsuccessful login attempts are not being recorded and a terminal server is being used, it is possible that the terminal server has no RSA Authentication Manager definition. Refer to your terminal server documentation to find out how to configure it properly.

Server times out during a login procedure

On some platforms, the Authentication Manager may time out during the New PIN or Next Tokencode procedures. If this happens, instruct the user to wait until the stack of countdown indicators on his or her token is low, and then to try again.

Illegible Characters Appear in Log Messages

Illegible characters can result from cross-realm authentications between a realm with a Japanese RSA Authentication Manager installation and a realm with an English RSA Authentication Manager installation. Japanese characters in authentication messages are not displayed correctly in an English log database.

Procedures to Resolve Problems

Probable Loss of Network Connection or Authentication Manager Is Down

If you find any of the messages in this section in your event log or system log, take the following steps:

1. Make sure a connection to the database exists through a database broker. On Windows, click **Start** > **Programs** > **RSA Security** > RSA Authentication Manager **Control Panel**, and from the left-hand menu, click **Start & Stop** RSA Authentication Manager **Services**. On UNIX, run **sdconnect start**.
2. Check your network connection. If the network is not working, you will get one or more of these messages, followed closely by a Primary Breaking Connection or Replica Breaking Connection message.
3. If neither of the first two steps help, you may be experiencing database corruption, and receive the **Daemon Stopping...** message, indicating a Fatal Error. Contact RSA Security Customer Support for instructions.

LDAP Synchronization Error Messages

If a synchronization job that connects with any of the three supported LDAP directory servers contains a query that returns a large number of user records (more than 1,000), either of the following messages appears:

```
Timelimit exceeded
Sizelimit exceeded
```

The issue typically results from the settings in place on your LDAP server. On your LDAP Directory Server, to accommodate for larger queries run by a synchronization job, increase the default values for connection time-out, maximum connection idle time, maximum page size, maximum query duration and maximum table size. The actual names of these settings, as well as the steps to change them, depend on your LDAP server. Consult the LDAP server documentation for information.

Note: Information about LDAP servers is available at http://www.openldap.org.

In RSA Authentication Manager, on the Primary machine, there are two environment variables that you can also increase:

```
RSA_LDAP_SEARCH_TIMEOUT
RSA_LDAP_BIND_TIMEOUT
```

The default values for these variables built in RSA Authentication Manager are 1200 seconds (20 minutes) and 300 seconds (five minutes). These values are optimized, and should be sufficient even for large queries. However, you can increase these settings by adding the environment variables with larger time-out values (in seconds). Consult Windows Help for information about adding environment variables.

You can also restrict the database search by editing the LDAP query filter associated with each synchronization job.

External Authorization Timeout Messages

If the External Authorization **iSDExtAuthorCheck()** or **iSDExtAuthorGetHomeData()** routines take too long to process, the Authentication Manager will time out an authentication request and display a message to users.

To resolve External Authorization time-out messages:

1. Start the Database Administration application.
2. Click **System > Edit Authorization Parameters**.
3. Turn off the External Authorization options.

   Then the Authentication Manager uses the default authentication routine to process access requests while you correct problems.
4. Determine why the **iSDExtAuthorCheck()** and **iSDExtAuthorGetHomeData()** routines take too long to process. Then, modify the routines to shorten their process times.
5. In the Database Administration application, click **System > Edit Authorization Parameters**.
6. Turn the External Authorization options back on.
7. Restart the Authentication Manager so that the External Authorization options take effect.

For more information about the External Authorization routines, see the *External Authorization API Guide* (**authmgr_authorization_api.pdf** in the ***ACEDOC*** directory).

Resolving Problems Starting Primary and Replica Communication

When the process that handles Primary and Replica communications (**syncsrvc** on Windows; **acesyncd** on UNIX) is having trouble starting, use the following procedure to correct the problem.

To correct a problem with syncsrvc (acesyncd):

1. Make sure a connection to the database exists through a database broker. Click **Start** > **Programs** > **RSA Security** > RSA Authentication Manager **Control Panel**, and from the left-hand menu, click **Start & Stop** RSA Authentication Manager **Services**.
2. Verify that the Primary and Replicas are the same type of computer and are running the same version of the operating system.

Messages

This section contains an alphabetical list of messages that you may see on your screen, in the RSA Authentication Manager audit log, and in the Event Log (on Windows) or the system log (on UNIX). The numbers in parentheses indicate the error number, which you can use to filter messages using SNMP. For more information, see "Filtering Messages Using SNMP" on page 293.

ACCESS DENIED,OA previous tokcode (8961)

A user attempted to reuse an old tokencode during an offline authentication. This is typically a user error.

Agent Request for Passwd Denied (8973)

The Authentication Manager has denied an Agent's request for a user's Windows password, possibly because Windows password integration is disabled at the system level or for this particular Agent Host, or because the Authentication Manager does not have the user's Windows password in its database.

A process timeout occurred while performing database broker management (15042)

If this message appears, restart the Authentication Manager. If the message persists, contact RSA Security Customer Support.

A Progress Utility error occurred while performing database broker management. (15043)

If this message appears, restart the Authentication Manager. If the message persists, contact RSA Security Customer Support.

A SELECT statement can select valid column names only. Arguments, numbers, or predefined variables are not allowed

This is a syntax error caused by the use of something other than a valid table field name in the column list. For more information, see the Help topic "RSA Authentication Manager Database Schema."

AALM failed to connect to log database (%1) (15994)

Stop the RSA Authentication Manager, verifying that all RSA Authentication Manager processes are stopped. Also verify that no administrators are performing a database dump or load. Restart the RSA Authentication Manager. If this message persists, contact RSA Security Customer Support.

AALM failed to daemonize (15993)

This message is logged when the Automated Log Maintenance daemon fails to start during the RSA Authentication Manager start. This message is usually preceded by one of the following messages:

```
Log Maintenance Had Seg Violation
Log Maintenance Had a Bus Error
Log Maintenance Aborted
Log Maintenance Stopped
```

Verify that Automated Log maintenance is enabled. In the Database Administration application, click **Log** > **Automate Log Maintenance** and make sure that **Enable Automatic Audit Log Maintenance** is selected, and then stop and restart the Authentication Manager.

AALM failed to get maintenance schedule (15998)

This message is logged when the Automated Log Maintenance daemon cannot connect to the log database. Restart the database broker.

AALM failed to initialize database context (%1) (15992)

Stop the RSA Authentication Manager, verifying that all RSA Authentication Manager processes are stopped. Also verify that no administrators are performing a database dump or load. Restart the RSA Authentication Manager. If this message persists, contact RSA Security Customer Support.

AALM failed to UPDATE maintenance schedule (15999)

The log maintenance daemon could not write to the database. Restart the Primary. If this message persists, contact RSA Security Customer Support.

AALM unable to set logmaintsvr credentials (15997)

Contact RSA Security Customer Support.

ACCESS DENIED, auth lock error (1140)

The Authentication Manager could not lock either the user's name or the user's token before acting on the authentication request. A lock on the name or token may already exist.

ACCESS DENIED, Bad Lost Token PSW (1083)

The user has been assigned a temporary password, but entered the password incorrectly during authentication. If the user has forgotten the password, create a new password and inform the user.

ACCESS DENIED, Bad User Password (1091)

If the log record lists the correct login, the user has been assigned a user password, but entered the password incorrectly during authentication. Use the **Set/Change User Password** button on the Edit User dialog box to change the user password and set the user password in Change Required mode.

For other circumstances in which this message might occur, see "ACCESS DENIED, PASSCODE Incorrect (1008)" on page 304.

ACCESS DENIED, Can't Get Token SB (1041)

Contact RSA Security Customer Support for assistance.

ACCESS DENIED, Can't Lock Token (1038)

The token could not be used to log on because the Authentication service could not lock the token.

ACCESS DENIED, Can't Write [Lock] Agent (1039)

The user could not log on because the Authentication service could not lock or write to the Agent Host record in order to update the node secret status.

ACCESS DENIED, Ext-auth failed *login user Agent Host server token* (1110)

This message appears if you have activated External Authorization on your RSA Authentication Manager. An External Authorization routine denied a user's access attempt. Review the Event Log for messages that indicate which External Authorization routine returned the error. If these messages are not sufficient to explain the error, ask the programmer who created the messages for more information.

ACCESS DENIED, Lost Password Exp

An attempt was made to log on with a fixed password assigned to a Lost token. However, the fixed password has expired. Create a new password for this Lost token.

ACCESS DENIED, Lost Token

An attempt was made to log on with a tokencode from a token that has been assigned Lost status. Now that the token has been found, verify that it is in the possession of the assigned user, and change the status to Not Lost.

ACCESS DENIED, multiple auths (1141)

This message is written to the RSA Authentication Manager audit trail to alert you that an attempt was made to break into your network. The Authentication service has detected the attempt and prevented access.

If you see this message, ***immediately set the token into New PIN mode and clear the old PIN***. For instructions, see "Setting New PIN Mode" on page 131.

ACCESS DENIED, name lock required (1142)

Before it sends an authentication request to a Authentication Manager, an Agent Host must issue a name lock request for the user name. This lock did not exist when the Authentication Manager received the authentication request. The name may already be locked, or a lock on it may have just been removed.

Some third-party Agents do not require a name lock. To prevent the Authentication Manager from expecting such a lock and denying access because it does not exist, open the Edit Agent Host dialog box for the Agent Host and if necessary clear the **Requires Name Lock** checkbox.

ACCESS DENIED, New PIN Deferred (147)

At the New PIN prompt, the user canceled the operation without specifying or receiving a new PIN. The user’s token is still in New PIN mode.

ACCESS DENIED, Next Tokencode Bad (1000)

The user attempted to answer the Next Tokencode prompt but entered a code that was not valid for the token. The user was therefore denied access. For a more detailed description of the Next Tokencode feature, see “When a PIN Is Stolen or Otherwise Compromised” on page 129.

ACCESS DENIED, No Agent SB (1042)

Contact RSA Security Customer Support for assistance.

ACCESS DENIED, No Token Assigned

The user attempted to log in but was not granted system access because that user has not been assigned a token. Before assigning this user a token, check with other system administrators to make sure that no security threat exists.

ACCESS DENIED, Node Verification Failed

This message may be logged under the following circumstances:

- The encryption value in the **sdconf.rec** file (or other configuration method) on the Agent Host does not match the encryption type in the Agent Host record.

  If the encryption type is set incorrectly in the Agent Host record, on the Agent Host menu, click **Edit Agent Host** to change the setting. If the setting in the **sdconf.rec** file is incorrect, see “Distributing the Configuration Update” on page 243 (for Windows) or on page 259 (for UNIX) for more information on distributing the **sdconf.rec** file.

- The Agent Host was deleted, then reinserted in the Authentication Manager database, or the Agent Host was previously associated with a different Authentication Manager. To solve the problem, perform the procedure in “Node verification failed (137)” on page 358.

- The node secret file has been deleted from the Agent Host. To solve the problem, follow steps 2 and 3 of the procedure in “Node verification failed (137)” on page 358.

If you need further assistance, contact RSA Security Customer Support.

ACCESS DENIED, Outside User Time (1003)

The user attempted to log on during a time that was outside the start and end time and date specified in the user's record.

ACCESS DENIED, PASSCODE Incorrect (1008)

Log record lists correct login. A record giving this description of the event but listing the user's login correctly can be logged for a number of reasons. The most common reason is the user entered his or her passcode incorrectly. If the user tried to authenticate only once or twice before calling you, tell him or her to try again.

If the user tries again and still is denied access, it may be that the token clock and the system clock are out of synch. If the system time is correct and the user is being denied access, perform the Resynchronize Token operation. For instructions, see "Resynchronizing a Token" on page 132.

If resynchronizing the token does not solve the problem, the user might be entering the wrong PIN. Put the token into New PIN mode and have the user receive (or create) a new PIN and log on with it.

Log record lists wrong logon. If there is no log record for the user who is being denied access but such records are being falsely recorded for another user, the problem is one of identifiers. It is likely that the wrong logon was specified when the user was activated on an Agent Host or added to a group. List direct users or group members (whichever is applicable to the user on this Agent Host), and see if the correct logon is listed for the serial number of the user's token. If it is not, perform the activation operation again to specify the user's logon correctly.

This message also appears when a user has been activated with a logon that is already being used on the Agent Host. If two different users have the same logon in an Agent Host, one tokenholder is unable to log on to the Agent Host because the Authentication service is expecting the passcode of the other tokenholder. Change the logon of one of the users.

ACCESS DENIED, PIN Rejected (1007)

The user did not complete the New PIN operation successfully because the PIN entered did not meet system specifications for length or allowable characters. The token is still in New PIN mode. The user must try again, this time selecting a PIN that meets the system requirements.

ACCESS DENIED, Previous Tokencode (1003)

The passcode entered is based on a tokencode that the token displayed at some time in the past (whether or not it was used to gain access). This is prohibited so that an unauthorized person cannot obtain (for example, through electronic eavesdropping) and then reuse a valid tokencode or passcode.

Access Denied (RSA Authentication Manager Quick Admin)

If you cannot log on to Quick Admin, verify the following items:

- Make sure the user ID you entered in the logon page is in the RSA Authentication Manager database and that the user is activated on the Agent Host (the Quick Admin web server host).
- Make sure a token or user password has been assigned to the user ID you entered.
- Make sure the user ID you entered has sufficient RSA Authentication Manager administrative rights.
- Make sure you have valid copies of the Primary Authentication Manager's **sdti.cer** and **server.cer** files in the ***Quick Admin installation directory*\Tomcat\webapps\quickadmin\WEB-INF\certs\*servername*** subdirectory on the web server host.
- Look at the RSA Authentication Manager Activity log to diagnose the problem further.

ACCESS DENIED, Syntax Error (146)

A user did not supply a valid string at the **Enter PASSCODE** prompt. For example, the user may have pressed RETURN without entering a passcode.

ACCESS DENIED, Token Disabled (1004)

The user attempted to log on but was not granted system access because his or her token had been disabled (either by the system or by an administrator). See "Disabling a Token" on page 126 and "When a Token Is Stolen or Otherwise Missing" on page 126. Before re-enabling the token, check with other system administrators to make sure that no security threat exists.

To enable a token:

In the Database Administration application, click **Token** > **Edit Token**. Select the disabled token to open the Edit Token dialog box and select the **Enabled** checkbox. Click **Help** if you need instructions.

ACCESS DENIED, Token Expired (1072)

The user attempted to log on but was not granted system access because that user's token has expired. An expired token must be replaced.

ACCESS DENIED, Token ToD Bad (1001)

The user attempted to log on with a token that has expired, or the user attempted to log in outside of his or her Temporary User period as specified in the user record. Use the **Add User** or **Edit User** option to set these dates.

ACCESS DENIED, Tokencode Repeated

The user entered a passcode that had already been used to gain system access. This is prohibited so that an unauthorized person cannot obtain (for example, through electronic eavesdropping), and then reuse, a valid passcode.

ACCESS DENIED, Write Token Failed (1006)

The token could not be used to log on because the Authentication service could not write to the token record.

ACE/Server attempted start from *hostname*: Unknown host

The machine does not correspond to the Authentication Manager named in the **sdconf.rec** file. On Windows, use the Configuration Management application to verify the hostname and IP address of your Primary. On UNIX, use the **sdsetup -config** command.

ACE/Server Error: calloc failed errno = ...

The RSA Authentication Manager services could not allocate memory. Check the memory resources allocated on your machine.

ACE/Server Can't Bind UDP Socket (1053)

Someone has tried to start the Authentication service when another process was running on the port specified for the Authentication service in the file ***%SYSTEMROOT%*\system32\drivers\etc\services** (**etc/services** on UNIX). For instructions on resolving the problem, see "ACM ERROR: Unable to bind the socket for ACE/Server" on page 308.

ACE/Server Can't Set UDP Sock Opt (1054)

The Authentication Manager cannot set the UDP socket options. See your system administrator.

ACE/Server Create UDP Socket Fail (1051)

There is a system problem, such as too few sockets available to start the Authentication service. See your system administrator.

ACE/Server error %d from errSDLicenseRead errno . . . .

The RSA Authentication Manager services could not read the license record. Make sure the **license.rec** file is in the ***ACEDATA*** directory, and check that the permissions on the file are correct.

ACE/Server error closing system handle . . . .

Progress error: look in the Event Log on Windows or system log on UNIX for other errors from the RSA Authentication Manager services and Progress Software database software.

ACE/Server Error: strdup failed errno = ...

It is possible that the RSA Authentication Manager services could not allocate memory. Check the memory resources allocated on your machine.

ACE/Server error updating the system record . . . . (15021)

Progress error: look in the Event Log on Windows or system log on UNIX for other errors from the RSA Authentication Manager services and Progress Software database software.

ACE/Server exiting: setsockopt() call failed

Check your network connections and settings.

ACE/Server failed to fetch system handle . . . .

Progress error: look in the Event Log on Windows or system log on UNIX for other errors from the RSA Authentication Manager services and Progress Software database software.

ACE/Server failed to get exclusive lock on system record . . . .

Another application has an exclusive lock on the system record. Try closing all administration sessions and then running the RSA Authentication Manager services again.

ACE/Server failed to open system record . . . .

Progress error: look in the Event Log on Windows or system log on UNIX for other errors from the RSA Authentication Manager services and Progress Software database software.

ACE/Server Primary will handle authentication requests

The connection between the Primary and Replicas has been restored, and the Primary is answering authentication requests from Agent Hosts.

ACE/Server recvfrom failed

Check your network connections and settings.

ACE/Server Replica started

The RSA Authentication Manager services started on the Replica.

ACE/Server service exited abnormally . . . .

Look in the Event Log on Windows or system log on UNIX for other messages from the RSA Authentication Manager services and the database for additional information about why the Authentication service failed.

ACE/Server service exited normally

The RSA Authentication Manager services stopped.

ACE/Server service started

The RSA Authentication Manager services started.

ACE/Server service stopped

The RSA Authentication Manager services stopped.

ACE/Server unable to set ACE/Server credentials

Make sure that the **license.rec** file exists and that the permissions on the file are correct.

Acesyncd aborted (2001)

Check the log for other messages which may indicate the exact nature of the problem. If this message persists, contact RSA Security Customer Support.

Acesyncd had a bus error (2002)

Check the log for more specific messages. If the message persists, contact RSA Security Customer Support.

Acesyncd had seg violation (2003)

Check the log for more specific messages. If the message persists, contact RSA Security Customer Support.

Acesyncd had seg violation (2003)

Check the log for more specific messages. If the message persists, contact RSA Security Customer Support.

Acesyncd Primary Started

This is a status message indicating that the replication process on the Primary has started.

Acesyncd Replica Started

This is a status message indicating that the replication process on the Replica has started.

ACM ERROR: Unable to bind the socket for ACE/Server

This message may mean that the operating system did not give up the socket quickly enough between your stopping and restarting the services, or it may mean that some other process was started on the ports specified for the RSA Authentication Manager services in the file ***%SYSTEMROOT%*\system32\drivers\etc\services** (where ***%SYSTEMROOT%*** stands for the root directory, for example **winnt**).

To change the port number used by one of the RSA ACE/Server Services:

1. Stop the RSA Authentication Manager services on the Primary and Replicas.
2. Make the port number change(s) in the **services** file. On Windows, the file is in the ***%SYSTEMROOT%*\system32\drivers\etc\services** directory. On UNIX, the file is in the **/etc** directory.

3. Make the change in the RSA Authentication Manager configuration file (**sdconf.rec**). On Windows, use the Configuration Management application to change the port numbers. On UNIX, use the **sdsetup -config** command.
4. Generate and distribute a new configuration file to the Replica and Agent Hosts. Copy the file (**sdconf.rec** in ***ACEDATA*** on the Primary) to the ***ACEDATA*** directory on the Replica and run the Configuration Management application to update the **sdconf.rec** file.

   For more information on distributing the **sdconf.rec** file, see "Distributing the Configuration Update" on page 243 (for Windows) or on page 259 (for UNIX).

   Note: The **sdconf.rec** file is created by the Configuration Management application. Agent Hosts may use **DES** or **SDI** encryption, and each Agent Host must have an **sdconf.rec** file that contains a match for the encryption it uses. If you have some Agent Hosts that use **DES** encryption and other Agent Hosts that use **SDI** encryption, make sure that the **sdconf.rec** file you distribute to each Agent Host has the correct encryption setting.

5. If you use **ftp** to copy the file, be sure to select binary mode.
6. Restart the RSA Authentication Manager services on the Primary and Replicas.

Admin Server (sdadmind) and remote administrative client (Host: %1) are not the same version (16197)

An administrator attempted to connect to the database using an incompatible version of the Remote Administration software. Most likely, the Remote Administration software is an older version. Upgrade the Remote Administration software to the same version as the RSA Authentication Manager.

Agent Host has no Acting Servers (1138)

No Acting Master and Slaves have been assigned in the database for the Agent Host, which is running RSA Authentication Manager software prior to 5.0. For information, see "Authentication Manager and Agent Host Communication Through Firewalls" on page 25 and "Resolving Hosts and Services" on page 240.

Agent Host not found (130)

Each machine on the network, including the Authentication Manager itself, must be listed as an Agent Host in the Authentication Manager database before its users can be authenticated. This log message means that the RSA Authentication Manager could not find in its list of Agent Hosts the name of the machine on which the user attempted to log on.

If this message contains the IP address of the Agent Host but not its hostname, the Authentication Manager is having a problem resolving the IP address. Make sure that this address is defined in the hosts file or name server database and that the Agent Host is in the Authentication Manager database. If the Agent Host is not listed in the database, on the Agent Host menu, click **Add Agent Host**. Once the Agent Host is created, activate users on it either directly or through groups. For detailed instructions on how to perform these operations, see Chapter 3, "Agents and Activation on Agent Hosts."

If you get this message but the Agent Host has, in fact, been created and is shown when you list Agent Hosts (using the Agent Host menu option), stop and restart the Authentication Manager. On Windows, use the RSA Authentication Manager Control Panel. On UNIX, use the **aceserver start** and **aceserver stop** commands. This should resolve the problem because the Agent Host database is reread on startup.

Agent Host not found in Server database, but cannot delete Agent Host delta (15249)

During a replication pass, the replication service attempted to apply a change to a database record, but the service could not access the record. This may happen when an administrator is editing the record during the replication pass. If this message persists, create a new replica package and apply it to the Replica.

Agent Host record is locked and cannot be updated. Will attempt to update at next replication pass. %1 (15118)

If you see this message repeatedly, restart the Replica. If the message persists after restarting, contact RSA Security Customer Support.

Aggregate functions other than COUNT, MIN or MAX are not supported

You tried to use an unsupported aggregate function (for example, AVG) in your query. Only COUNT, MIN and MAX are supported aggregate functions in Custom Queries.

ALL is not supported in the list of output fields

The ALL option is not allowed in SELECT statements when your column list contains more than one field. The default selection is to select all data from the fields in the column-list anyway, so ALL is unnecessary.

All SELECT statements must return same set of fields in the same order

In a complex query with multiple SELECT statements, you must specify the same column list in the same order in all SELECT statements.

An error occurred while creating a process for database broker management (15041)

If this message appears, reboot the Authentication Manager. If the message persists, contact RSA Security Customer Support.

An error occurred while reading the registry for database broker management (15040)

If this message appears, contact RSA Security Customer Support.

An Error Occurred While Reconciling Databases (15192)

This message indicates that the network connection was lost or that the Primary is not working. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

An Error Occurred While Walking Databases

This message indicates that the network connection was lost or that the Primary is not working. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

An unexpected word was encountered in the query

This error is typically caused when a known word was encountered in an unexpected place in the SQL code. For example, in an IF-THEN-ELSE conditional statement, the syntax checker encounters a SELECT when it was expecting a THEN.

An unknown error was encountered

This condition might be caused by a corrupted or missing file in the Custom Queries file hierarchy. If you get this error, contact RSA Security Customer Support.

Application Log is Full

Every action by a user, an administrator, or an RSA Authentication Manager process causes an RSA Authentication Manager application to write an entry to the Application Log, a facility of the Windows Event Log. The log size is fixed, and when these entries have filled it completely, this message appears on your screen when you start the RSA Authentication Manager.

Application Log entries are not generally useful except in debugging. To prevent this message from appearing, RSA Security recommends the following measures:

- If possible, expand the size of the log from the default 512 KB.
- Set the log to overwrite the oldest entries as new entries are added. This keeps the log from becoming full but ensures that the most recent entries are available if you need them for debugging.

To set Windows Event Log options:

1. Click **Start** > **Programs** > **Administrative Tools** > **Event Viewer** to display the Event Log.
2. Click **Log** > **Log Settings** to open the Event Log Settings dialog box.
3. In the **Change Settings for** box, select **Application**.
4. If you have enough disk space to expand the size of the log, type a new value (number of kilobytes) in the **Maximum Log Size** box, or click the Up arrow on the box to increase the size in 64 KB increments. RSA Security recommends that you make the new log size at least 1 MB (1024 KB).
5. Click **Overwrite Events as Needed**.
6. Click **OK** and exit from the Event Viewer.

Archive Error: %1 failed; errno %2 (15996)

The log maintenance daemon could not access the database to archive data. If this message persists, contact RSA Security Customer Support.

Assisted recvry (PushDB) disabled (2288)

A Replica was marked as needing a new database, but the System Parameters are not set to allow Push DB Assisted Recovery. As long as Push DB is disabled, the Primary cannot send Replica packages to the Replicas. To enable Push DB, click **System** > **Edit System Parameters** and select **Allow Push DB Assisted Recovery**.

If you want to use the Push DB Assisted Recovery feature to send the database Replica Package to the Replica, configure the System Parameters on the Primary to Allow Push DB Assisted Recovery, and then create a new Replica Package on the Primary and restart the Replica. The Primary sends the Replica Package to the Replica when you restart the Replica.

If you do not want to use the Push DB Assisted Recovery feature, create a Replica Package, copy the files in the Replica Package to the ***ACEDATA*** directory on the Replica, and restart the Replica.

Attempt To Start Demon On Unauthorized Host

If this message appears, the process that handles Primary and Replica communications (**syncsrvc** on Windows; **acesyncd** on UNIX) is having trouble starting. To correct the problem, see "Resolving Problems Starting Primary and Replica Communication" on page 300.

AUTH IGNORED, TRIAL EXPIRED (1009)

Your RSA Authentication Manager software was enabled for a trial period that has now expired. Although users continue to be authenticated, you cannot restart the Authentication service if it is stopped, and you cannot run the Administration application. The trial software should be removed or converted to the standard product. Contact your RSA Security distributor or sales representative to find out how to purchase RSA Authentication Manager software.

AUTHENTICATION Failed to get socket desc from server context. (15076)

There is a problem with the authentication service. The front end service, which accepts authentication requests, and the back end service, which processes the requests, are experiencing some kind of communication problem. Restart the Authentication Manager. On Windows, use the RSA Authentication Manager Control Panel to stop and start the Authentication Manager. On UNIX, use the **aceserver stop** and **aceserver start** commands.

Breaking connection with message %1 (15151)

An error occurred when the Replica attempted to break communication with the Primary. If this message occurs when the Primary is pushing the database to a Replica, stop the Replica and restart it.

Broker for sdlog started

The **sdlog** broker has started.

Broker for sdserv started

The **sdserv** broker has started.

Broker service started

The service responsible for the database brokers has started.

Broker service stopped

The service responsible for the database brokers has stopped. Check for other Event Log messages.

Brokers restarted (2292)

This message is logged after the **Start rep pack reinstall** message when the Push DB process is proceeding normally.

Bus Error (%1) (16202)

This message displays when an RSA Authentication Manager process dies (**syncsrvc** on Windows, **acesyncd** on UNIX, **sdadmind**, **acesrvc**, **acesrvc_be**, **logmainthd**). Look up the error listed in the message. If the problem is not related to RSA Authentication Manager software, take appropriate action, and restart the RSA Authentication Manager when the problem is resolved. If the problem is related to RSA Authentication Manager software, contact RSA Security Customer Support.

Can't Share Lock System On Replica (15205)

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Cannot acquire query and save it with the specified name. Query with same name already exists locally or provided name includes invalid symbols

You are attempting to acquire a shared query and assign a name to it that is already used by another shared query, or the name you are attempting to use contains invalid characters.

Cannot Check Delete Dependency for *NAME* (for specific messages, see page 390)

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Cannot Check Dependency for *NAME* (for specific messages, see page 391)

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Cannot Close System Table %1 (15263)

If you see this message repeatedly, stop and start the Primary. If the message persists, reboot the Replica. If the message persists after restarting, contact RSA Security Customer Support.

Cannot Close System Table (15263)

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Cannot close trace file. It is not open

Trace files can be used to help troubleshoot Primary and Replica communication problems. For instructions on enabling the packet trace and viewing the results, contact RSA Security Customer Support.

Cannot compare Agent last modified dates for merge (15117)

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Cannot Compare System L Dates for Merge (15203)

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Cannot Compare Token E Dates for Merge

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Cannot Compare Token L Dates for Merge

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Cannot Compare Token LE Dates for Merge

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Cannot Compare Token P Dates for Merge

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Cannot Copy Delta To *NAME* To Delete On Replica (for specific messages, see page 392)

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Cannot copy file (*OS error code*)

The file you are attempting to copy is missing or could be corrupted.

Cannot Copy *NAME* Delta (for specific messages, see page 394)

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Cannot copy query using specified name. Query with same name already exists locally or provided name includes invalid symbols

You are attempting to copy a query and assign a name to it that is already used by another query, or the name you are attempting to use contains invalid characters.

Cannot create destination folder (*OS error code*)

There was a problem creating the query folder while performing a Copy operation. The parent folder (queries) may have been renamed, or there may be a more serious OS error.

Cannot Create (Update) *NAME* On Replica (for specific messages, see page 395)

If this message appears and you do not see "Primary Successfully Reconciled Database" or "Replica Successfully Reconciled Databases," your databases may be corrupted or grossly mismatched. This message is likely to be accompanied by other messages identified as trigger errors.

See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298. Contact RSA Security Customer Support if you see this message without reconciliation success messages.

Cannot Decode Primary Agent Host SB for Merge

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Cannot Decode Primary Token SB

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Cannot Decode Replica Agent Host SB for Merge

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Cannot decode Replica token SB

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Cannot Decrypt Primary System SB for Merge (15201)

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Cannot Decrypt Replica System SB for Merge (15202)

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Cannot decrypt system record (15026)

There was a problem decrypting sensitive data in your database. Verify that you have the correct license record in the ***ACEDATA*** directory.

Cannot Delete Log Entry (15230)

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Cannot Delete *NAME* Delta (for specific messages, see page 397)

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Cannot Delete *NAME* On Replica (for specific messages, see page 398)

If this message appears and you do not see "Primary Successfully Reconciled Database" or "Replica Successfully Reconciled Databases," your databases may be corrupted or grossly mismatched. This message is likely to be accompanied by other messages identified as trigger errors.

See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298. Contact RSA Security Customer Support if you see this message without reconciliation success messages.

Cannot delete query (*OS error code*)

There was a problem deleting the specified query. The query may have been renamed, deleted through regular OS means, or there may be a more serious OS error.

Cannot determine number of attempted authentications associated with this token. Delete the token, and then reimport it to the database. (15214)

The RSA Authentication Manager could not update a token record during a replication pass. Delete the token from the database, and reimport it. If this message persists, the database may be corrupt. Contact RSA Security Customer Support.

Cannot determine the correct ETC Date associated with this token. Delete the token, and then reimport it to the database (21000)

The Authentication Manager is unable to determine the correct emergency tokencode date for a token, possibly because of clock drift or some internal problem. As indicated, delete and reimport the token record to the Authentication Manager database. If this problem persists, contact RSA Security Customer Support.

Cannot determine the correct PIN number associated with this token. Delete the token, and then reimport it to the database (15215)

The RSA Authentication Manager could not update a token record during a replication pass. Delete the token from the database, and reimport it. If this message persists, the database may be corrupt. Contact RSA Security Customer Support.

Cannot determine the last successful authentication associated with this user (15217)

A user record could not be updated during a replication pass.

Cannot determine the last successful EAP date associated with this user (21003)

A user record could not be updated during a replication pass because of a conflict merging Emergency Passcode dates. If this message persists, create a new Replica Package and apply it manually or by using Push DB. If applying the Replica Package does not solve the problem, contact RSA Security Customer Support.

Cannot determine when the last login occurred with this token. Delete the token, and then reimport it to the database (15213)

The RSA Authentication Manager could not update a token record during a replication pass. Delete the token from the database, and reimport it. If this message persists, the database may be corrupt. Contact RSA Security Customer Support.

Cannot determine when token was enabled. Delete the token, and then reimport it into the database (15212)

The RSA Authentication Manager could not update a token record during a replication pass. Delete the token from the database, and reimport it. If this message persists, the database may be corrupt. Contact RSA Security Customer Support.

Cannot determine when token was marked lost. Delete the token, and then reimport it into the database

The RSA Authentication Manager could not update a token record during a replication pass. Delete the token from the database, and reimport it. If this message persists, the database may be corrupt. Contact RSA Security Customer Support.

Cannot Exclusive Lock Agent Host for Merge

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Cannot Exclusive Lock *NAME* Delta (for specific messages, see page 400)

This message indicates that the network connection was lost or that the Primary is not working. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Cannot Exclusive Lock System (15264)

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Cannot Exclusive Lock System for Merge (15199)

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Cannot Exclusive Lock Token for Merge

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Cannot execute query. Output directory does not exist

The standard query output directory (by default named **output**) does not exist in ***ACEDIR***, preventing the query from running.

Cannot execute query. Query file is missing or corrupt

When you create a new query (or edit a sample query), RSA Authentication Manager compiles it for your realm. The compiled version is named **query.r** and is placed in the query folder. When this error appears, there is some problem with the **query.r** file. It may have been deleted, renamed, or corrupted.

Cannot Fetch *NAME* Delta (for specific messages, see page 401)

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Cannot Fetch System Record (15262)

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Cannot Find *NAME* To Delete On Replica (for specific messages, see page 403)

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Cannot Find Pending Delete for *NAME* (for specific messages, see page 404)

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Cannot find the user record for token serial number 000000*nnnnnn*

This message appears in the following circumstances:

- The token record is corrupted.
- The user was deleted, but the token record has not been updated.

  Verify that the user is still available. If so, unassign the original token to be replaced. Then assign a different token to the user.

Cannot fully read query data. Using default values for undefined and improperly configured parameters

When you create a new query (or edit a sample query), RSA Authentication Manager compiles it for your realm and places necessary files in the query folder. In addition to the compiled query (**query.r**), RSA Authentication Manager creates a **runtime.txt** file which specifies items such as output format. When this error appears, there is some problem with the **runtime.txt** file. It may have been deleted, renamed, or corrupted.

Cannot get system time (%1) (15063)

If this message appears, restart the Authentication Manager. If the message persists, contact RSA Security Customer Support.

Cannot get the local database directory

You are attempting to create or run a new query, and the Custom Queries feature cannot determine the location of the RSA Authentication Manager database directory. The ***ACEDATA*** directory is typically **c:\ace\data**. This error would be generated if the directory was deleted, renamed, or somehow corrupted.

Cannot initialize Agent Host-server communications

This is the same problem as the one described under the heading "Agent Host hangs while trying to authenticate" on page 296. See the resolution instructions for that error condition.

Cannot Locate *NAME* To Delete On Replica (for specific messages, see page 406)

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Cannot Mark Agent Host Delta for Merge

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Cannot Mark System Delta for Merge (15200)

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Cannot Mark Token Delta for Merge

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Cannot Match Delta State for *NAME* (for specific messages, see page 407)

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Cannot merge Agent Host record from the Primary because the security block could not be decrypted. Delete the Agent Host and then re-add it to the Primary database (15115)

An Agent Host record could not be updated during a replication pass. Delete the Agent Host from the database and add it again. If this message persists, the database may be corrupt. Contact RSA Security Customer Support.

Cannot merge Agent Host record to the Primary because the security block could not be decrypted. Delete the Agent Host and then re-add it to the Replica database (21001)

An Agent Host record could not be updated during a replication pass. Delete the Agent Host from the database and add it again. If this message persists, the database may be corrupt. Contact RSA Security Customer Support.

Cannot merge token record from the Primary because the security block could not be decrypted. Delete the token, and then reimport it to the database (15210)

The RSA Authentication Manager could not update a token record during a replication pass. Delete the token from the database, and reimport it. If this message persists, the database may be corrupt. Contact RSA Security Customer Support.

Cannot merge token record from the Replica because the security block could not be decrypted. Delete the token, and then reimport it to the database (15211)

The RSA Authentication Manager could not update a token record during a replication pass. Delete the token from the database, and reimport it. If this message persists, the database may be corrupt. Contact RSA Security Customer Support.

Cannot merge token record to the Primary because the security block could not be decrypted

The RSA Authentication Manager could not update a token record during a replication pass. Delete the token from the database, and reimport it. If this message persists, the database may be corrupt. Contact RSA Security Customer Support.

Cannot merge User record from Primary because its security block could not be decrypted. Delete the User (record) and then re-add it to the Primary database (21002)

The Authentication Manager has encountered an internal problem with the security block of a user record during a replication pass and could not continue. Delete the user record and recreate it. It the problem persists, contact RSA Security Customer Support.

Cannot merge User record to Primary because its security block could not be decrypted. Delete the User and then re-add it to the database (21001)

The Authentication Manager has encountered an internal problem with the security block of a user record during a replication pass and could not continue. Delete the user record and recreate it. It the problem persists, contact RSA Security Customer Support.

Cannot Open *NAME* Delta Cursor (for specific messages, see page 409)

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Cannot Open System Table

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Cannot Open System Table %1 (15261)

If you see this message repeatedly, restart the Primary. If the message persists, reboot the Replica. If the message persists after restarting, contact RSA Security Customer Support.

Cannot Read *NAME* Commit Response (for specific messages, see page 410)

This message indicates that the network connection was lost or that the Primary is not working. See “Probable Loss of Network Connection or Authentication Manager Is Down” on page 298.

Cannot read system record (15027)

Progress error: look in the Event Log on Windows or system log on UNIX for other errors from the RSA Authentication Manager services and Progress database software.

Cannot rename query using specified name. Query with same name already exists locally or provided name includes invalid symbols

You are attempting to use an existing name or one with invalid characters (shown below).

{} ~ " ; ' [ ] , / @ < > ^ |

Cannot resolve service %1 by name (15023)

There is a conflict with the name of the service specified in the message. Confirm that the name and port number for the service are configured correctly in the Configuration Management utility. On UNIX, run **sdsetup -repmgmt list**.

Cannot Save *NAME* On Replica (for specific messages, see page 412)

If this message appears and you do not see “Primary Successfully Reconciled Database” or “Replica Successfully Reconciled Databases,” your databases may be corrupted or grossly mismatched. This message is likely to be accompanied by other messages identified as trigger errors.

See “Probable Loss of Network Connection or Authentication Manager Is Down” on page 298. Contact RSA Security Customer Support if you see this message without reconciliation success messages.

Cannot send Agent Host delta to Primary. Agent Host record may be locked by another administrator. Will attempt to send delta at next replication pass. %1 (15114)

If you see this message repeatedly, restart the Replica. If the message persists after rebooting, contact RSA Security Customer Support.

Cannot send Agent Host delta to Primary. Will attempt to send at next replication pass. %1 (15251)

If you see this message repeatedly, stop and start the Replica. If the message persists, reboot the Replica. If the message persists after restarting, create a new Replica Package and apply it manually or by using Push DB.

Cannot Send Agent Host To Primary

This message indicates that the network connection was lost or that the Primary is not working. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Cannot send log entry record to Primary. Will attempt to send at next replication pass. %1 (15229)

If you see this message repeatedly, stop and start the Replica. If the message persists, reboot the Replica. If the message persists after restarting, contact RSA Security Customer Support.

Cannot Send Log Entry To Primary

This message indicates that the network connection was lost or that the Primary is not working. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Cannot Send *NAME* Commit Request to Replica (for specific messages, see page 413)

This message indicates that the network connection was lost or that the Primary is not working. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Cannot Send *NAME* To Replica (for specific messages, see page 415)

This message indicates that the network connection was lost or that the Primary is not working. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Cannot send one-time password delta. One-time password record may be locked by another administrator. Will attempt to send at next replication pass. %1 (15244)

If you see this message repeatedly, stop and start the Primary. If the message persists, reboot the Replica. If the message persists after restarting, contact RSA Security Customer Support.

Cannot send one-time password record to Primary. Will attempt to send at next replication pass. %1 (15245)

If you see this message repeatedly, stop and start the Replica. If the message persists, reboot the Replica. If the message persists after restarting, create a new Replica Package and apply it manually or by using Push DB.

Cannot Send System To Primary

This message indicates that the network connection was lost or that the Primary is not working. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Cannot send token delta to Primary. Token record may be locked by another administrator. Will attempt to send delta at next replication pass. %1 (15209)

If you see this message repeatedly, restart the Replica. If the message persists, reboot the Replica. If the message persists after restarting, contact RSA Security Customer Support.

Cannot send token delta. Token record may be locked by another administrator. Will attempt to send at next replication pass. %1 (15207)

If you see this message repeatedly, stop and start the Primary. If the message persists, reboot the Replica. If the message persists after restarting, contact RSA Security Customer Support.

Cannot send token record to Primary. Will attempt to send at next replication pass. %1 (15239)

If you see this message repeatedly, stop and start the Replica. If the message persists, restart the Replica. If the message persists after restarting, create a new Replica Package and apply it manually or by using Push DB.

Cannot Send Token To Primary

This message indicates that the network connection was lost or that the Primary is not working. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Cannot send user delta to Primary. User record may be locked by another administrator. Will attempt to send delta at next replication pass. %1 (15208)

If you see this message repeatedly, stop and start the Replica. If the message persists, reboot the Replica. If the message persists after restarting, contact RSA Security Customer Support.

Cannot send user delta. Token record may be locked by another administrator. Will attempt to send at next replication pass. %1 (15206)

If you see this message repeatedly, stop and start the Primary. If the message persists, reboot the Replica. If the message persists after restarting, contact RSA Security Customer Support.

Cannot send user record to Primary. Will attempt to send at next replication pass. %1 (15234)

If you see this message repeatedly, stop and start the Replica. If the message persists, reboot the Replica. If the message persists after restarting, contact RSA Security Customer Support.

Cannot share query and save it with the specified name. Query with same name or a folder with same name includes invalid symbols

You are attempting to use an existing name or one with invalid characters (shown below).

{} ~ " ; ' [ ] , / @ < > ^ |

Cannot start default application for the output file

When you run a query, you have the option of specifying the output format and whether a default application should launch automatically after the query output is generated. RSA Authentication Manager has encountered a problem attempting to launch the default application. The path may be wrong, the application may be corrupted or missing, or there could be another more serious problem.

Cannot Update Agent Host for Merge

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Cannot update locked system record

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Cannot update locked system record %1 (15274)

Stop and start the RSA Authentication Manager. If the message persists, contact RSA Security Customer Support.

Cannot Update *NAME* On Replica (for specific messages, see page 416)

If this message appears and you do not see "Primary Successfully Reconciled Database" or "Replica Successfully Reconciled Databases," your databases may be corrupted or grossly mismatched. This message is likely to be accompanied by other messages identified as trigger errors.

See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298. Contact RSA Security Customer Support if you see this message without reconciliation success messages.

Cannot Update System for Merge (15204)

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Cannot update token (%1) (15064)

Look up the specific error indicated in the message and check the log for additional messages that may be related to this problem. If the message persists, contact RSA Security Customer Support.

Cannot Update Token for Merge

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Cannot Update(Create) *NAME* On Replica (for specific messages, see page 418)

If this message appears and you do not see "Primary Successfully Reconciled Database" or "Replica Successfully Reconciled Databases," your databases may be corrupted or grossly mismatched. This message is likely to be accompanied by other messages identified as trigger errors.

See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298. Contact RSA Security Customer Support if you see this message without reconciliation success messages.

Cannot upgrade license...There are too many active users and Replicas in the database

The utility is unable to apply the specified **license.rec** file because it does not provide sufficient limits for your current installation. Your installation already has more than the licensed number of active users and Replicas.

Make sure that you are specifying the correct **license.rec** file during the upgrade process. If this still does not resolve the problem, contact RSA Security to obtain a new Advanced license with a higher active user limit.

For additional information about licensing, see Appendix A, "Licensing."

Cannot upgrade license...There are too many active users in the database

The utility is unable to apply the specified **license.rec** file because it does not provide sufficient limits for your current installation. Your installation already has more than the licensed number of active users.

Make sure that you are specifying the correct **license.rec** file during the upgrade process. If this still does not resolve the problem, contact RSA Security to obtain a new license with a higher active user limit.

For additional information about licensing, see Appendix A, "Licensing."

Cannot upgrade license...There are too many Replicas in the database

The utility is unable to apply the specified **license.rec** file because it does not provide sufficient limits for your current installation. In this case, your current installation already has more than the allowed number of Replicas in the RSA Authentication Manager database.

Make sure that you are specifying the correct **license.rec** file during the upgrade license process. If this still does not resolve the problem, contact RSA Security to obtain an Advanced license, which allows up to 10 Replicas per realm.

For additional information about licensing, see Appendix A, "Licensing."

Cannot upgrade license...You are attempting to upgrade your Permanent license with an Evaluation license

The utility is unable to apply the specified **license.rec** file because it is an evaluation license. Evaluation licenses have a fixed lifespan, which is usually 90 days from the time they are issued, not from the time they are installed. Make sure that you are specifying the correct **license.rec** file during the upgrade license process. If this still does not resolve the problem, contact RSA Security to obtain a valid license.

For additional information about licensing, see Appendix A, "Licensing."

Cannot upgrade license...You cannot apply a license that is in violation

The utility is unable to apply the specified **license.rec** file because it is in *upgrade violation* mode. Upgrade violation mode effectively turns your license into a 90-day temporary license.

Make sure that you are specifying the correct **license.rec** file during the upgrade license process. If this still does not resolve the problem, contact RSA Security to obtain a valid license.

For additional information about licensing, see Appendix A, "Licensing."

Cannot use a wildcard while joining tables

The wildcard character (*) can only be used when selecting from one table. You cannot use wildcards when selecting from multiple tables (table joins).

Cannot Write Push Response %1 (15272)

If you see this message repeatedly, stop and start the Replica. If the message persists after restarting, create a new Replica Package and manually apply it.

Can't get server context, FIND REALM FAILED (15082)

If this message appears, restart the Authentication Manager. If the message persists, contact RSA Security Customer Support.

Can't get server context, OPEN REALM FAILED (15081)

If this message appears, restart the Authentication Manager. If the message persists, contact RSA Security Customer Support.

Certificate verification failed and RSA ACE/Server will not start. The server.cer file either is corrupt or does not match the embedded root certificate (15030)

The **server.cer** file is invalid. Copy the **server.cer** file from a Replica or from the original license diskette that shipped with RSA Authentication Manager.

Certificate verification failed and RSA ACE/Server will not start. The server.cer file was not found (15029)

During startup, the Authentication Manager requires a **server.cer** file in the ***ACEDATA*** directory. Verify that the **server.cer** file is located in the ***ACEDATA*** directory. If you cannot find the file, copy it from a Replica or from the original license diskette that shipped with RSA Authentication Manager.

Close realm cursor failed (%1) (15070)

If this message appears, restart the Authentication Manager. If the message persists, contact RSA Security Customer Support.

Close token cursor failed (%1) (15069)

If this message appears, restart the Authentication Manager. If the message persists, contact RSA Security Customer Support.

COLLISION, agt rec, Accepting Rem (162)

A conflict occurred during a replication pass or authentication. A change to an Agent Host record in another Authentication Manager’s database conflicted with the Agent Host record in the database of the Authentication Manager that logged this message. The conflict was resolved by updating this Authentication Manager’s database.

COLLISION, agt rec, Local IP

A conflict occurred during a replication pass or authentication. A change to the IP address in the Agent Host record in another Authentication Manager’s database conflicted with the IP address in the Agent Host record in the database of the Authentication Manager that logged this message. The conflict was resolved by updating the other Authentication Manager’s database.

COLLISION, agt rec, Local Secret (173)

A conflict occurred during a replication pass or authentication. A change to the node secret in the Agent Host record in another Authentication Manager’s database conflicted with the node secret in the Agent Host record in the database of the Authentication Manager that logged this message. The conflict was resolved by updating the other Authentication Manager’s database.

COLLISION, agt rec, Remote IP

A conflict occurred during a replication pass or authentication. A change to the IP address in the Agent Host record in another Authentication Manager’s database conflicted with the IP address in the Agent Host record in the database of the Authentication Manager that logged this message. The conflict was resolved by updating this Authentication Manager’s database.

COLLISION, agt rec, Remote Secret (172)

A conflict occurred during a replication pass or authentication. A change to the node secret in the Agent Host record in the database of another Authentication Manager conflicted with the node secret in the Agent Host record in the database of the Authentication Manager that logged this message. The conflict was resolved by updating this Authentication Manager's database.

COLLISION, multiple node secrets (177)

The RSA Authentication Manager has received more than one node secret for Agent Hosts using the same IP address. Because this condition may be caused by an attempt to breach the security of your network, the Authentication Manager will not enter any node secret in the Agent Host record. To enable communication between the Authentication Manager and the Agent Host, you must clear the node secret and establish a new one.

1. Clear the node secret file on the Agent Host.

   For instructions on clearing the node secret on the Agent Host, see the documentation for your RSA Authentication Manager software.

2. If you are using Automatic Delivery, clear the node secret file on the Authentication Manager. If you are using Manual Delivery, this step is not necessary.

   To clear the node secret on the RSA Authentication Manager, open the Edit Agent Host dialog box for the Agent Host, and clear the **Node Secret Created** checkbox.

3. When the node secret is cleared on both the Agent Host and the Authentication Manager:

   - If you are using Automatic Delivery to create a new node secret, set up a controlled initial authentication to establish a new node secret. For information, see "Data Encryption" on page 19.
   - If you are using Manual Delivery to create a new node secret, see the Help topic "Creating a Node Secret."

   For information about the different types of node secret delivery, see "Node Secret File" on page 228.

COLLISION, tok rec, Enabled on Remote

A token was most recently enabled on another Authentication Manager. The token record on the Authentication Manager that logged this message was updated with the enabling information from the other Authentication Manager.

COLLISION, tok rec, Failed Logins (164)

Failed authentication attempts occurred with this token on both the Authentication Manager that logged this message and another Authentication Manager. The token record was updated with the total number of failed authentications added together from both Authentication Managers.

COLLISION, tok rec, Last Login on Remote

The most recent successful authentication with this token occurred on another Authentication Manager. The token record on this Authentication Manager was updated with this information.

COLLISION, tok rec, Pin set Last on Remote

The most recent PIN setting for this token occurred on another Authentication Manager. The token record on the Authentication Manager that logged this message was updated with this PIN setting.

COLLISION, tok rec, Rep Used (168)

A replacement token was issued on another Authentication Manager. The original token issued on the Authentication Manager that logged this message was unassigned.

Connection closed even though passcode accepted

This message appears if the user's UNIX shell is invalid. Check what shell was specified when the user was added to a group or activated on the Agent Host. Make sure it is a valid shell and is spelled correctly.

If you find that the shell on the Agent Host is incorrect, also check the shell specified in the user record.

Could Not Decrypt XR Message (8220)

The realm secrets in the local and remote realm no longer match. Click **Establish Realm Secret** in the Edit Realm dialog box to reestablish the realm secret.

Created User Password (4539)

A new user password was created by a user.

CSV separator cannot be empty

In the Query Wizard Output Parameters dialog box, the Separator field must have a specified character. The default is the comma, but other characters are accepted.

Database Inconsistency. Replica Rejecting *NAME* Delta (for specific messages, see page 419)

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Date range for fixed PSW modified (3556)

This is a status message indicating that the range of expiration days has changed for fixed passwords assigned to lost tokens.

date time Ext-auth Check error *-nnnnn login user Agent Host server token* (8401)

This message appears if you have activated External Authorization on your RSA Authentication Manager. You should have received a list explaining the return value assigned to this message from the programmer who created it for the **iSDExtAuthorCheck()** routine. Refer to this list. The **iSDExtAuthorCheck()** routine authorizes users to log in to an Agent Host.

date time Ext-auth Home-data error *-nnnnn login user Agent Host server token* (8403)

This message appears if you have activated External Authorization on your RSA Authentication Manager. You should have received a list explaining the return value assigned to this message from the programmer who created it for the **iSDExtAuthorGetHomeData()** routine. Refer to this list. The **iSDExtAuthorGetHomeData()** routine gets local information to be returned as part of a cross-realm authentication.

Definition.txt file is corrupted and cannot be loaded

The **definition.txt** file, which contains the SQL code and other information about the query, is corrupted.

Delete Error: %1 failed; errno %2 (15995)

The log maintenance daemon could not access the database to delete a record. If this message persists, contact RSA Security Customer Support.

Delta Record Exists Without Agent Host. Deleting

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Delta Record Exists Without Token. Deleting

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Destination folder has invalid permissions (OS error code)

While copying a query, or specifying output to a particular directory, you have selected a destination for which you do not have the appropriate access privileges.

DISTINCT is not supported in the list of output fields

You are attempting to use the DISTINCT clause in the column list of the SELECT statement. DISTINCT can only be used to qualify the output of the query (for example, after a WHERE clause or in a table join).

Domain Secret Update Failed (8957)

The domain secret for the specified Agent could not be updated in the Authentication Manager database. The Agent record could be corrupted, or there may have been a decryption failure on the security block. To fix the issue, first try restarting the Agent Host. If the problem still exists, try deleting and re-adding the Agent Host and clearing the node secret. If the problem persists, contact RSA Security Customer Support.

Entered Log Monitoring (7008)

An administrator started a log monitoring session. For more information about log monitoring, see "Log Monitoring and Reporting" on page 169.

err in get a token record (%1) (15073)

If this message appears, contact RSA Security Customer Support.

err in get an admin record (%1) (15074)

If this message appears, contact RSA Security Customer Support.

Error %1 setting Response Delay (15100)

If this message appears, contact RSA Security Customer Support.

Error accepting connection (2006)

This message can display when starting or stopping the RSA Authentication Manager. If this message persists, contact RSA Security Customer Support.

Error closing system to get SB Keys (15129)

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Error comparing agent host L dates (2283)

This message can display during the merging of database records during a replication pass. If the message persists, contact RSA Security Customer Support.

Error comparing lost dates (2334)

The RSA Authentication Manager cannot determine the date on which a token was marked Lost. If you see one instance of this message, delete the token and reimport it into the database. If you see the message logged more than once, this Authentication Manager's database may be corrupt. Contact RSA Security Customer Support.

Error comparing token ETC dates (2331)

The Emergency Token Code expiration dates for this token cannot be determined. If you see one instance of this message, export the token, and then reimport it to the database. If you see the message logged more than once, it may indicate that the Authentication Manager database is corrupted. Contact RSA Security Customer Support.

Error comparing user EAP dates (2330)

There is a conflict merging the offline emergency passcode dates of a user record. If this message persists, create a new Replica Package and apply it manually or by using Push DB. If applying the Replica Package does not solve the problem, contact RSA Security Customer Support.

Error Committing Data on Replica (2007)

This error is caused by corruption of the Replica Authentication Manager database, probably because of unsupported access to this database. Custom administration programs must be used only on the Primary database. Accessing the Replica Authentication Manager database directly is not supported and may cause corruption.

Error comparing system dates (2009)

This message can appear during the merging of database records during a replication pass. If the message persists, contact RSA Security Customer Support.

Error Comparing Tkn Enable Dates (2011)

The enable time for a token cannot be determined. If you see one instance of this message, export the token, and then reimport it to the database. If you see the message logged more than once, it may indicate that this Authentication Manager's database is corrupted. Contact RSA Security Customer Support.

Error Comparing Token Last Dates (2010)

The number of attempted authentications made with this token cannot be determined. If you see one instance of this message, export the token, and then reimport it to the database. If you see the message logged more than once, it may indicate that this Authentication Manager's database is corrupted. Contact RSA Security Customer Support.

Error Comparing Token Last Logins (2012)

The last login made with this token cannot be determined. If you see one instance of this message, export the token, and then reimport it to the database. If you see the message logged more than once, it may indicate that this Authentication Manager's database is corrupted. Contact RSA Security Customer Support.

Error Comparing Token PIN Dates (2013)

The PIN number for this token cannot be determined. If you see one instance of this message, export the token, and then reimport it to the Authentication Manager database on which you see the message. If you see the message logged more than once, it may indicate that this Authentication Manager's database is corrupted. Contact RSA Security Customer Support.

Error comparing user R A dates (2282)

There is a conflict merging the remote access dates of a remote user record. If this message persists, create a new Replica Package and apply it manually or by using Push DB. If applying the Replica Package does not solve the problem, contact RSA Security Customer Support.

Error: connection timed out (2015)

This message can appear when starting or stopping the RSA Authentication Manager. If this message persists, contact RSA Security Customer Support.

Error copying integer field from buffer

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Error creating agent delta (2016)

Back up the database on the Replica, generate a replica package, and apply it to the Replica, either through Push DB or manually. If this does not solve the problem, contact RSA Security Customer Support.

Error Creating Record (15137)

This message indicates that the network connection was lost or that the Primary is not working. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Error creating record on replica (2017)

This message indicates that the network connection was lost or that the Primary is not working. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Error creating system delta (2018)

Back up the database on the Replica, generate a replica package and apply it to the Replica, either through Push DB or manually. If this does not solve the problem, contact RSA Security Customer Support.

Error decrypting Primary agent SB (2019)

This error message appears when decryption (for reading from or writing to the security block) fails during a replication pass. The Primary cannot decrypt the security block on an Agent Host record, and cannot send an updated Agent Host record to a Replica. Contact RSA Security Customer Support.

Error decrypting primary sys SB (2020)

This error message appears when decryption (for reading from or writing to the security block) fails during a replication pass. The Authentication Manager could not decrypt the security block that is used to encrypt certain fields in the database. Contact RSA Security Customer Support.

Error decrypting Primary token SB (2021)

This error message appears when decryption (for reading from or writing to the security block) fails during a replication pass. A Primary cannot decrypt the security block on a token record, and cannot propagate changes from the Agent Host record to a Replica. Contact RSA Security Customer Support.

Error decrypting replica agent SB (2022)

This error message appears when decryption (for reading from or writing to the security block) fails during a replication pass. A Replica cannot decrypt the security block on Agent Host record, and cannot propagate changes from the Agent Host record to a Replica. Contact RSA Security Customer Support.

Error decrypting replica sys SB (2023)

This error message appears when decryption (for reading from or writing to the security block) fails during a replication pass. The Authentication Manager could not decrypt the security block that is used to encrypt certain fields in the database. Contact RSA Security Customer Support.

Error Decrypting Replica Token SB (2024)

This error message appears when decryption (for reading from or writing to the security block) fails during a replication pass. A Replica cannot decrypt the security block on a token record, and cannot send the changes made on the Agent Host record to a Replica. Contact RSA Security Customer Support.

Error decrypting system sec-blk (2025)

This error message appears when decryption (for reading from or writing to the security block) fails during a replication pass. The Authentication Manager could not decrypt the security block that is used to encrypt certain fields in the database. Contact RSA Security Customer Support.

Error decrypting system security block (15130)

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Error decrypting primary user SB (2333)

This error message appears when decryption (for reading from or writing to the security block) fails during a replication pass. A Primary cannot decrypt the security block on a user record, and cannot propagate changes from the Agent Host record to a Replica. Contact RSA Security Customer Support.

Error decrypting replica user SB (2332)

This error message appears when decryption (for reading from or writing to the security block) fails during a replication pass. A Replica cannot decrypt the security block on a token record, and cannot send the changes made on the Agent Host record to a Replica. Contact RSA Security Customer Support.

Error deleting delta *NAME* (for specific messages, see page 421)

If this message appears, contact RSA Security Customer Support.

Error deleting delta task item (2270)

If this message appears, contact RSA Security Customer Support.

Error deleting delta tasklist (2258)

If this message appears, contact RSA Security Customer Support.

Error Deleting *NAME* (for specific messages, see page 421)

This message indicates that the network connection was lost or that the Primary is not working. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Error Deleting Record %1 (15139)

An error occurred when the Replica attempted to respond to a request to delete a record. Check the log for other messages. Create a new Replica Package and apply it manually or use Push DB.

Error exporting token by user (7521)

Possible database collision. Stop and restart Database Administration application (or **sdadmin** on UNIX), and try to export the token again. If the message persists, contact RSA Security Customer Support.

Error exporting token by user (7521)

Possible database collision. Stop and restart Database Administration application (or **sdadmin** on UNIX), and try to export the token again. If the message persists, contact RSA Security Customer Support.

Error fetching system to get SB Keys (15128)

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Error handling heartbeat (2072)

If this message appears, contact RSA Security Customer Support.

Error loading security block keys (2073)

This error message appears when decryption (for reading from or writing to the security block) fails during a replication pass. This message appears when there is an error loading the database encryption keys. Contact RSA Security Customer Support.

Error Modifying Record (15138)

This message indicates that the network connection was lost or that the Primary is not working. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Error modifying record on replica (2074)

This message indicates a replication issue. Create a new Replica Package for the Replica and apply it manually or by using Push DB. If the message persists, contact RSA Security Customer Support.

Error non HB received in vASDProcessHBs!

This message indicates that the network connection was lost or that the Primary is not working. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Error occurred while parsing line *line number* of the runtime parameters file. Do you want to ignore error and continue parsing?

A problem with the **runtime.txt** file was encountered, usually as a result of file corruption. You can try to continue. If there are further problems running the query, try editing and recompiling the query.

Error on start of sdlog broker (15036)

There was an error starting the broker for the **sdlog** database. Check the Event Log for other messages.

The connection to the **sdlog** database has been lost. Because the RSA Authentication Manager services cannot write log messages, they exit.

Error on start of sdserv broker (15035)

There was an error starting the broker for the **sdserv** database. Check the Event Log for other messages.

The connection to the **sdserv** database has been lost. Because the RSA Authentication Manager services cannot write log message, they exit.

Error opening license.rec file (2308)

During startup, the Authentication Manager requires a valid **license.rec** file in the ***ACEDATA*** directory. The **license.rec** file is missing or corrupt. Contact RSA Security Customer Support.

Error opening rep pack file (2296)

Either the Replica Package does not exist on the Primary where the Primary expects to find it, or the Replica could not write the Replica Package files it received from the Primary. If the Primary cannot find the Replica Package, then create the Replica Package in the directory specified as **ACEREP** on Windows or **REP_ACE** on UNIX. If the Replica cannot write the packets received from the Primary, then disable Push DB Assisted Recovery in the System Parameters and manually copy the Replica Package files to the ***ACEDATA*** directory on the Replica.

Error opening system to get SB Keys (15127)

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. For assistance, contact RSA Security Customer Support.

Error operating with folder browser

The Query Wizard uses a common folder browser in the Add, Acquire and Share dialog boxes. During a folder browsing operation, the Query Wizard was unable to continue. This can result from you or someone else changing file or folder names in the operating system while this operation was ongoing. It can also result from more serious problems with the hardware or in the OS.

Error past end of buff in errCopyBuffStrToStr

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Error past end of string in errCopyStrToBuffStr

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Error processing modified Agent Host records on Replica (15260)

This message indicates that the network connection was lost or that the Primary is not working. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Error Processing Modified Log Entries On Replica (15269)

This message indicates that the network connection was lost or that the Primary is not working. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Error Processing Modified OneTimePassword Records On Replica %1 (15258)

This message indicates an error during replication. If you see this message repeatedly, stop and start the Replica. If the message persists, restart the Replica. If the message persists after restarting, create a new Replica Package and apply it manually or by using Push DB.

Error Processing Modified System Records On Replica (15266)

This message indicates that the network connection was lost or that the Primary is not working. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Error Processing Modified Token Records On Replica (15256)

This message indicates that the network connection was lost or that the Primary is not working. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Error Processing Modified User Records On Replica %1 (15255)

This message indicates an error during replication. If you see this message repeatedly, restart the Replica. If the message persists, restart the Replica. If the message persists after restarting, create a new Replica Package and apply it manually or by using Push DB.

Error Processing New Log Entries On Replica (15271)

This message indicates that the network connection was lost or that the Primary is not working. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Error propagating license rec (2307)

The Primary could not send the **license.rec** file to the Replica. Restart the Replica. If this message persists, restart the Primary. If restarting the Primary does not fix the problem, contact RSA Security Customer Support.

Error Reading Heartbeat Response

This message indicates that the network connection was lost or that the Primary is not working. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Error Reading Heartbeat Response (15198)

This message indicates that the network connection was lost or that the Primary is not working. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Error Reading Packet (15132)

This message indicates that the network connection was lost or that the Primary is not working. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Error reading rep pack file (2297)

The Primary found the Replica Package, but could not read it. The Primary may fail to open the Replica Package for either of the following reasons: the Replica Package is corrupt, or the Replica Package does not exist in the expected location. The Replica shuts down automatically. Create a new Replica Package on the Primary and restart the Replica.

Error Receiving Heartbeat (15136)

This message indicates that the network connection was lost or that the Primary is not working. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Error: replica clock can't be set (2086)

Verify that the clock on the Replica is synchronized with the clock on the Primary. The time on the Replica must be set to within 30 seconds of the time on the Primary. On UNIX, this error appears when the RSA Authentication Manager is started by a user who is not root. Log on as root and restart the Authentication Manager.

Error Responding To Agent Host Request

This message indicates that the network connection was lost or that the Primary is not working. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Error responding to Agent request %1 (15147)

An error occurred when the Replica attempted to respond to a request to modify an Agent Host record. Check the log for other messages. Create a new Replica Package and apply it manually or use Push DB.

Error Responding to Commit Request Record (15140)

This message indicates that the network connection was lost or that the Primary is not working. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Error Responding To Log Entry Request (15142)

This message indicates that the network connection was lost or that the Primary is not working. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Error Responding To OneTimePassword Request %1 (15146)

An error occurred when the Replica attempted to respond to a request to modify a one-time password record. Check the log for other messages. Create a new Replica Package and apply it manually or use Push DB.

Error Responding To Push Query %1 (15141)

The Primary could not push the database to the Replica. Restart the Replica. If the message persists, apply the Replica Package manually.

Error responding to push request (2075)

The Primary could not push the database to the Replica. Restart the Replica. If the message persists, apply the Replica Package manually.

Error Responding To Reconcile Done Msg (15148)

This message indicates that the network connection was lost or that the Primary is not working. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Error Responding To System Request (15145)

This message indicates that the network connection was lost or that the Primary is not working. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Error Responding To Token Request (15144)

This message indicates that the network connection was lost or that the Primary is not working. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Error Responding To User Request %1 (15143)

An error occurred when the Replica attempted to respond to a request to modify a user record. Check the log for other messages. Create a new Replica Package and apply it manually or use Push DB.

Error saving query

There was a problem saving the query. This could indicate problems with your file system. If you get this error, contact RSA Security Customer Support.

Error selecting packet (2079)

The Replica may be listening for the Primary on the wrong Service Port Number. Verify the port numbers and names using the Replication Management utility.

Error searching database (2078)

If this message appears, contact RSA Security Customer Support.

Error sending heartbeat (2080)

If this message appears, contact RSA Security Customer Support.

Error sending replica agent hosts (2081)

This message indicates a replication issue. Create a new Replica Package for the Replica and apply it manually or by using Push DB. If the message persists, contact RSA Security Customer Support.

Error sending replica log entries (2082)

This message indicates a replication issue. Create a new Replica Package for the Replica and apply it manually or by using Push DB. If the message persists, contact RSA Security Customer Support.

Error sending replica OTPs (2191)

During a replication pass, one or more used one-time user passwords (OTPs) could not be sent from the Replica to the Primary. If this message persists, create a new Replica Package for the Replica and apply it manually or by using Push DB. If the new Replica Package does not solve the problem, contact RSA Security Customer Support.

Error sending replica system (2083)

This message indicates a replication issue. Create a new Replica Package for the Replica and apply it manually or by using Push DB. If the message persists, contact RSA Security Customer Support.

Error sending replica tokens (2084)

This message indicates a replication issue. Create a new Replica Package for the Replica and apply it manually or by using Push DB. If the message persists, contact RSA Security Customer Support.

Error sending replica users (2278)

Error responding to a request for users. Create a new Replica Package for the Replica and apply it manually or by using Push DB. If the message persists, contact RSA Security Customer Support.

Error Setting Replica Clock (2085)

This error message appears when decryption (for reading from or writing to the security block) fails during a replication pass. A communications error occurred while **syncsrvc** was attempting to set the Replica clock.

Error Status *error number*

These error messages appear when you attempt to log on to Quick Admin and there is a problem with Tomcat, or the Tomcat server cannot communicate with the RSA Authentication Manager Quick Admin Daemon. To troubleshoot these errors, verify the following:

- Make sure the web server is running.
- Make sure the Tomcat server is running on the web server.

  To test the Default server, go to **http://*QuickAdmin host*/servlets-examples** and run the sample servlets.
- Make sure the RSA Authentication Manager Quick Admin Daemon service is running on the Primary RSA Authentication Manager.
- Make sure the RSA Authentication Manager and its database brokers are started.

Also, examine the Tomcat event log file: on the web server host, go to the ***Quick Admin installation directory*\Tomcat\logs** subdirectory. On a Windows host, the log file name is **stdout_*date*.log**. On Solaris, the log file name is **catalina.out**.

To view the error messages without re-creating them, open the **quickadmin\WEB-INF\properties\errormsg.properties** file.

Error swapping comm params (2088)

Create a new Replica Package and manually apply it.

Error swapping comm params 2 (2087)

Create a new Replica Package and manually apply it.

Error Swapping Communication Parameters (15135)

This message indicates that the network connection was lost or that the Primary is not working. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Error Swapping Encryption Keys (15133)

This message indicates that the network connection was lost or that the Primary is not working. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Error swapping encryption keys (2089)

The Primary and the Replica cannot communicate because there is a problem with the encryption keys. Verify that the following files are in the Primary ***ACEDATA*** directory: **server.cer**, **server.key**. **sdti.cer**. If the files are present, generate a new Replica Package for the Replica and manually apply it. If the message persists, contact RSA Security Customer Support.

Error Swapping Protocol Versions (15134)

If this message appears, the process that handles Primary and Replica communications (**syncsrvc** on Windows; **acesyncd** on UNIX) is having trouble starting. To correct the problem, see "Resolving Problems Starting Primary and Replica Communication" on page 300.

Error synching comm params (2090)

Create a new Replica Package and manually apply it.

Error Transferring *NAME*

An error occurred during a replication pass. *NAME* indicates the database field that was being transferred when the error occurred. For specific messages, see page 423.

Error: unexpected packet received (2077)

This message indicates a replication issue. Create a new Replica Package for the Replica and apply it manually or by using Push DB. If the message persists, contact RSA Security Customer Support.

Error updating agent host record (2116)

This message indicates a replication issue. Create a new Replica Package for the Replica and apply it manually or by using Push DB. If the message persists, contact RSA Security Customer Support.

Error updating system record (2117)

This message indicates a replication issue. Create a new Replica Package for the Replica and apply it manually or by using Push DB. If the message persists, contact RSA Security Customer Support.

Error updating token (2119)

This message indicates a replication issue. Create a new Replica Package for the Replica and apply it manually or by using Push DB. If the message persists, contact RSA Security Customer Support.

Error updating token delta (2118)

This message indicates a replication issue. Create a new Replica Package for the Replica and apply it manually or by using Push DB. If the message persists, contact RSA Security Customer Support.

Error updating user (2279)

During a replication pass, the Primary sent user record changes to the Replica, but the Replica could not update the database. If this message persists, create a new Replica Package and apply it manually or by Push DB. If the message still persists, contact RSA Security Customer Support.

Error updating user delta (2281)

This message indicates a replication issue. Create a new Replica Package for the Replica and apply it manually or by using Push DB. If the message persists, contact RSA Security Customer Support.

Error waiting for response (2120)

Verify that the information (hostname, IP address) for the Replica is the same in the Replication Management utility and your DNS server or the system's hosts file. You may need to contact your IT department to resolve network issues.

Error While Traversing Database

This message indicates that the network connection was lost or that the Primary is not working. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Evading Trial and Error Attack (135)

The RSA Authentication Manager authentication process detected a series of failed login attempts and slowed down the authentication dialog in order to thwart a possible break-in attempt.

Expired lost status cleared (1703)

The RSA Authentication Manager has cleared a token's expired lost status and has deleted a fixed password assigned to the token, because a user has attempted to authenticate with that token.

Expressions other than those containing COUNT, MAX or MIN functions are not supported in the list of output fields

You can only use COUNT, MAX, or MIN in the column list of a SELECT statement. Other expressions (for example, BEGINS, MATCHES, HAVING, and so on) can only be used in the part of the SELECT statement that qualifies the output (for example, after a WHERE clause or in a table join).

External Authorization Initialization error, *errstring*

This message appears if you have activated External Authorization on your RSA Authentication Manager. You should have received a list explaining the return value assigned to this message from the programmer who created it for the **iSDExtAuthorInit()** routine. For more information, refer to this list. The **iSDExtAuthorInit()** routine performs External Authorization initialization tasks.

External Authorization Shutdown error, *errstring*

This message appears if you have activated External Authorization on your RSA Authentication Manager. You should have received a list explaining the return value assigned to this message from the programmer who created it for the **iSDExtAuthorShutdown()** routine. For more information, refer to this list. The **iSDExtAuthorShutdown()** routine shuts down External Authorization.

Failed inserting realm record (%1) (15079)

The RSA Authentication Manager could not insert a realm record into the database. Delete the remote realm record in the local realm, the local realm record in the remote realm, and then reestablish the realm relationship. If the message persists, contact RSA Security Customer Support.

Failed signal setup, Daemon Stopping (%1) (16203)

This message appears when an RSA Authentication Manager process dies (**syncsrvc** on Windows, **acesyncd** on UNIX, **sdadmind**, **acesrvc**, **acesrvc_be**, **logmainthd**). Look up the error listed in the message. If the problem is not related to RSA Authentication Manager software, take appropriate action, and restart the RSA Authentication Manager when the problem is resolved. If the problem is related to RSA Authentication Manager software, contact RSA Security Customer Support.

Failed to allocate memory (%1) (15009)

If you see this message, look up the specific error indicated in the message and check the log for additional messages that may be related to this problem. If the message persists, contact RSA Security Customer Support.

Failed to clear the PIN for token serial number 000000*nnnnnn*. The token replacement process will stop

The token record may be corrupted. Delete the token record from the database, and assign a different token.

Failed to close system table cursor (%1) (15020)

If this message appears, restart the Authentication Manager. If the message persists, contact RSA Security Customer Support.

Failed to connect to the [RSA ACE/Server *IP Address*] with port = 5570. Wrong ACE/Server port number or ACE Web Admin service is down. Error code: 109

You have an incorrect system name or IP address in the ***ACEPROG*\hosts.conf** file on RSA Authentication Manager. Edit the **hosts.conf** file to make sure the Quick Admin Web server system name is spelled correctly and is entered as both a host name (for example, **cassatt**) and a fully-qualified DNS name (for example, **cassatt.rsasecurity.com**). Also make sure the IP address is correct.

Failed to connect to the card reader

The card reader is not properly connected to the computer, or the card reader is not working properly. Verify that the card reader is securely connected to the computer. Replace the card reader if necessary.

Failed to create socket (%1) (15008)

If you see this message, look up the specific error indicated in the message and check the log for additional messages that may be related to this problem. If the message persists, contact RSA Security Customer Support.

Failed to daemonize process (%1) (15016)

If this message appears, restart the Authentication Manager. If the message persists, contact RSA Security Customer Support.

Failed to fetch system record (%1) (15019)

If this message appears, restart the Authentication Manager. If the message persists, contact RSA Security Customer Support.

Failed To fully Send Database to Replica %1 (15191)

The Primary could not push the database to the Replica. Restart the Replica. If the message persists, apply the Replica Package manually.

Failed to get the PIN for token serial number 000000*nnnnnn*

The token record for this serial number has been corrupted. Assign a different token.

Failed to load the seed in file filename. This file is bound to a different device. Please contact your RSA SecurID administrator.

When you issue software tokens, users may install the token file on a PC or other device. If a user attempts to install a software token on a device that is different than the device to which you bind the token, this message displays to the user.

Verify that the serial number in the token record extension field **DeviceSerialNumber** matches the serial number of the device on which the user is installing the token file. Instruct the user to install the file on the correct device, or, if the user needs to install the token on a different device, reissue the token and specify the new device's serial number in the token extension field. For more information on reissuing software tokens, see the Help topic "Reissue Software Token."

Failed to Lock *recordtype* Record

If an authorized user was denied access and this is the log message for the event, a record required for authenticating the user was in use. The record type named ***recordtype*** may be an Agent Host, System, or Token Record. The inability to authenticate is temporary and should last only until the other operation using the record is completed.

This message may also be logged when **syncsrvc** has tried to put an exclusive lock on a record but could not.

This error also occurs if a custom administration program is accessing the Replica database. Custom administration programs must be used only on the Primary database. Accessing the Replica database directly is not supported and may cause corruption. For specific messages, see page 425.

Failed to open system table cursor (%1) (15018)

If this message appears, restart the Authentication Manager. If the message persists, contact RSA Security Customer Support.

Failed to read license (15010)

If this message appears, the process that handles Primary and Replica communications (**syncsrvc** on Windows; **acesyncd** on UNIX) is having trouble starting. To correct the problem, see "Resolving Problems Starting Primary and Replica Communication" on page 300.

Failed to read system record (1158)

If this message appears, restart the Authentication Manager. If the message persists, contact RSA Security Customer Support.

Failed to retrieve the config record (15077)

If this message appears, the process that handles Primary and Replica communications (**syncsrvc** on Windows; **acesyncd** on UNIX) is having trouble starting. To correct the problem, see "Resolving Problems Starting Primary and Replica Communication" on page 300.

Failed to set socket options (%1). (15017)

If you see this message, look up the specific error indicated in the message and check the log for additional messages that may be related to this problem. If the message persists, contact RSA Security Customer Support.

Failed to start offline authentication Download Manager (20006)

A component of the **sdoad** service failed to start. If this message appears, restart the Authentication Manager. If the message persists, contact RSA Security Customer Support.

Failed to start offline authentication Ticket Manager (20005)

A component of the **sdoad** service failed to start. If this message appears, restart the Authentication Manager. If the message persists, contact RSA Security Customer Support.

Failed to Stop Brokers %1 (15178)

Stop and start the Replica.

Failed to Stop Replica %1 (15175)

Stop and start the Replica.

Failed updating realm record (%1). (15080)

The RSA Authentication Manager could not update a realm record into the database. Delete the remote realm record in the local realm, the local realm record in the remote realm, and then reestablish the realm relationship. If the message persists, contact RSA Security Customer Support.

Fatal error execing acesyncd (%1) (15012)

The replication process (**acesyncd**) did not start. Look up the specific message in your operating system or networking resources.

Fatal Error: %1 (15109)

If you see this message, look up the specific error indicated in the message and check the log for additional messages that may be related to this problem. If the message persists, contact RSA Security Customer Support.

Fewer BEs (%1) (16221)

There is a problem with the authentication service. As part of normal operation, the RSA Authentication Manager creates two back end authentication processes (**acesrvc_be**) for each processor on the system. For some reason, one of the processes is not running. Restart the Authentication Manager. On Windows, use the RSA Authentication Manager Control Panel to stop and start the Authentication Manager. On UNIX, use the **aceserver stop** and **aceserver start** commands.

General error in broker server. %1 (15037)

If you see this message, restart the Authentication Manager. If the messages persists, contact RSA Security Customer Support.

General error in RSA ACE/Server acesrvc service %1 (15046)

Look up the specific error indicated in the message and check the log for additional messages that may be related to this problem. If the message persists, contact RSA Security Customer Support.

General error in RSA ACE/Server acesrvc service %1 (15046)

Look up the specific error indicated in the message and check the log for additional messages that may be related to this problem. If the message persists, contact RSA Security Customer Support.

General error in RSA ACE/Server syncsrvc service %1 (15827)

Look up the specific error indicated in the message and check the log for additional messages that may be related to this problem. If the message persists, contact RSA Security Customer Support.

Get Agent host failed (%1) (15052)

Look up the specific error indicated in the message and check the log for additional messages that may be related to this problem. If the message persists, contact RSA Security Customer Support.

Get enabled user failed (%1) (15067)

Look up the specific error indicated in the message and check the log for additional messages that may be related to this problem. If the message persists, contact RSA Security Customer Support.

Get node by name failed (%1) (15053)

An error occurred while attempting to find an Agent Host. If the message persists, verify that the information (hostname, IP address) for the Agent Host is the same in the database and in your DNS server or the system's hosts file.

Get node by net addr failed (%1) (15051)

Verify that the information (hostname, IP address) for the Replica is the same in the Replication Management utility and your DNS server or the system's hosts file. You may need to contact your IT department to resolve network issues.

Good Tokencode/Bad PIN Detected (1010)

The passcode sent to the RSA Authentication Manager contained a good tokencode, but an incorrect PIN. This may mean that an unauthorized user has acquired an authorized user’s token and is attempting to guess the correct PIN. Tokens that require the tokencode and PIN to be entered separately (the RSA SecurID standard card and key fob) are disabled after three consecutive attempts in which a valid tokencode is entered with an incorrect PIN. (You cannot change this limit.)

Group and Site administrators do not have permission to delete queries that are not acquired

You are a Group or Site administrator attempting to delete a query from the Custom Queries folder. However, since you did not personally acquire the query, you do not have permission to delete it.

Group and Site administrators do not have permission to rename queries that are not acquired

You are a Group or Site administrator attempting to rename a query in the Custom Queries folder. However, since you did not personally acquire the query, you do not have permission to rename it.

grp-mem db close error (%1) (15071)

If this message appears, restart the Authentication Manager. If the message persists, contact RSA Security Customer Support.

grp-mem db fetch error (%1) (15072)

If this message appears, restart the Authentication Manager. If the message persists, contact RSA Security Customer Support.

grp-mem db open error (%1) (15068)

If this message appears, restart the Authentication Manager. If the message persists, contact RSA Security Customer Support.

If you go back, you will lose changes to this screen. Do you want to continue? (This message will not appear again)

In the Query Wizard, each time you click **Back** in one of the dialog boxes, you lose the changes (for example, argument definitions) you have made to the current dialog box.

Incorrect order of the sections in the definition file

This message appears if the **definition.txt** is corrupted or was manually edited by someone, which is not recommended.

Insert Realm Bad Tokencode (8229)

When attempting to establish a realm secret, an administrator entered an invalid tokencode. This message might be logged if, due to network-related delays, the realm secret message did not reach the remote administrator's realm until after the tokencode changed. Other reasons why this message might appear are that the token clock and the system clock are out of synch (see "Resynchronizing a Token" on page 132) or that the administrator initiating the realm secret typed the tokencodes incorrectly.

Insert Realm Failed (8230)

The RSA Authentication Manager was unable to establish the realm secret with the target realm. Consequently, the local realm may not have been added to the remote realm database. This could occur if the network connection between the two realms was broken, the token clock and the system clock were out of synch, or the administrator initiating the realm secret entered the wrong tokencodes. Check the log message database in the remote realm for a more detailed error. The administrator attempting to establish the realm secret should obtain new tokencodes from the remote administrator and try again.

Insert Realm Not Allowed (8225)

An administrator attempted to establish the realm secret transaction while a Replica was running in the remote realm.The realm secret must initially be established using the Primary server (or Master in legacy realms) as the preferred server. The Preferred and Failover servers can be changed or updated once the realm secret has been established.

Insert Realm Not Authorized (8228)

When attempting to establish a realm secret, an administrator entered a tokencode belonging to an unauthorized user. A realm administrator’s tokencode must be used to encrypt a realm secret transaction.

Insert Realm Succeeded (8201)

The RSA Authentication Manager inserted the new realm in the database.

Insert Realm Token Not Found (8227)

When attempting to establish a realm secret, an administrator entered an invalid token serial number. The administrator establishing the realm secret should contact the remote administrator and obtain the correct serial number and tokencodes.

Insert Realm Tokencode Repeated (8226)

When attempting to establish a realm secret, the administrator entered a tokencode that had already been used. A tokencode that has been used for any purpose (for example, to log on, establish a realm, or resynch a token) cannot be used to establish a realm secret. Passcode or tokencode reuse is prohibited under any circumstances.

Internal error generating argument file

An internal error was encountered by the query compiler. If you get this message, contact RSA Security Customer Support.

Internal Error. Report to RSA Security Inc.

An internal error was encountered somewhere in the query creation or compilation process. If you get this message, contact RSA Security Customer Support.

Invalid condition

There is a syntax error in the SQL condition (IF, THEN, ELSEIF, ELSE). The error is somewhere in the highlighted string. Review the SQL condition, and correct the error.

Invalid default. For DATE enter date in MM/DD/YYYY format

In the Query Wizard Argument Details dialog box, there is a syntax error in the DATE argument. Make sure to enter a date using the MM/DD/YYYY format.

Invalid default. For LOGICAL enter TRUE or FALSE

In the Query Wizard Argument Details dialog box, there is a syntax error in the LOGICAL argument. The entry must be either TRUE or FALSE.

Invalid default. For NUMBER enter digits only; maximum is 9 digits

In the Query Wizard Argument Details dialog box, there is a syntax error in the NUMBER argument. The entry must be one or more numbers (to a maximum of nine numbers).

Invalid default. For STRING enter valid characters only. See help for details

In the Query Wizard Argument Details dialog box, there is a syntax error in the STRING argument. Any valid ASCII character or characters can be entered except:

{} ~ " ; ' [ ] , / @ < > ^ |

Invalid message statement

There is a syntax error in the MESSAGE statement in the SQL code. The error is somewhere in the highlighted string. Review the MESSAGE statement, and correct the error.

Invalid query name or query with such name already exists

In the Query Wizard, while attempting to name a query, you have entered either a query name that already is in use, or which has one or more of the following illegal characters:

\ / : * ? " < > |

Invalid range of the Back End ports. (15014)

Restart the Authentication Manager. If the message persists, contact RSA Security Customer Support.

Invalid SELECT statement

There is a syntax error in your SELECT statement. The error is somewhere in the highlighted string. Review the SELECT statement, and correct the error. This message is often the result of a misspelled or invalid table name.

Invalid SELECT statement has been specified in the query definition

This error would only be generated in the case of someone manually editing the **definition.txt** file of a query, which is not recommended.

Invalid symbols in the command line

In the Query Wizard, you entered invalid symbols in the Launch External Application command line field. Verify the entry in the field and make the necessary corrections.

Invalid symbols in the field. See the Help for details

In the Query Wizard, in one of the text fields (which is identified), you have entered one or more of the following illegal characters:

{} ~ " ; ' [ ] , / @ < > ^ |

Iteration count out of range

The number of iterations used by a RADIUS client to generate an RSA EAP Protected OTP credential is out of range. You can edit credential configuration settings on either the RSA Authentication Manager or the RADIUS client. For information on configuring RSA EAP Protected OTP on the RSA Authentication Manager, see the Help. To change credential settings on a RADIUS client, see your client software documentation.

License active user limit being approached

When you exceed the limits of your license, you will be in *violation* mode.

Violation mode occurs under either of the following circumstances:

- You have installed a new RSA Authentication Manager and have exceeded your license limits.
- Your license was in upgrade violation mode and is now in violation mode.

When your license is in violation mode, you cannot activate additional users.

When you exceed the limits of your license, to bring your system back into compliance, contact RSA Security to obtain a new license. Alternatively, you can deactivate a sufficient number of users to bring your system back into compliance.

For additional information about licensing, see Appendix A, "Licensing."

License Copy Failed %1 (15158)

If this message persists, restart the Primary and the Replica. If this does not solve the problem, reinstall the Replica.

License copy failed (2310)

The Primary could not send the **license.rec** file to the Replica. Restart the Replica. If this message persists, restart the Primary. If restarting the Primary does not fix the problem, contact RSA Security Customer Support.

License Packet Send Failed %1 (15157)

If this message persists, restart the Primary and the Replica. If this does not solve the problem, reinstall the Replica.

License packet send failed (2309)

The Primary could not send the **license.rec** file to the Replica. Restart the Replica. If this message persists, restart the Primary. If restarting the Primary does not fix the problem, contact RSA Security Customer Support.

Lock manager network error reading operation from: %1 Error: %2 Connection closed (15095)

This message appears during startup and shutdown of the RSA Authentication Manager, and also when the Primary pushes a database to a Replica. If you see this message at any other time, contact RSA Security Customer Support.

Lock manager network error sending operation to: *SERVER NAME* (15096)

This message is logged on a Replica when the lock manager on the Replica attempts to establish a connection to another Replica, but the second Replica refuses to acknowledge the connection because certain changes to the database have not yet been replicated to the second Replica.

For example, you have two Replicas, A and B. You have just generated a new Replica Package for Replica A and the Primary has pushed the new database to Replica A. As part of the Push DB process, Replica A restarts the lock manager, which attempts to establish connections with all Replicas in the database. If the lock manager on Replica A attempts to connect with Replica B before the Primary performs the next replication pass to Replica B, Replica B will drop the connection, because it does not yet know of the change to the database on Replica A. This message will be logged until the Primary replicates the changes to Replica B.

Lock manager server rejected client connection from: %1 (15097)

If this message appears, contact RSA Security Customer Support.

Lost Token Authenticated (1080)

This message is logged when a user enters a valid PIN and temporary password at the **Enter PASSCODE** prompt.

Lost token status cleared (1702)

This message appears after a user successfully authenticates with a token that was previously marked as Lost with a fixed password assigned to it. The RSA Authentication Manager marks the token as Not Lost and deletes the fixed password.

Missing ELSE condition

In the query, you have used the IF clause of a conditional statement without completing the statement with the required ELSE clause.

NAME Already Exists On Replica (for specific messages, see page 425)

If this message appears and you do not see "Primary Successfully Reconciled Database**"** or "Replica Successfully Reconciled Databases," your databases may be corrupted or grossly mismatched. This message is likely to be accompanied by other messages identified as trigger errors.

See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298. Contact RSA Security Customer Support if you see this message without reconciliation success messages.

Next Tokencode Accepted (1057)

A successful login attempt was followed by a system request for a second code in order to verify that the user had possession of the token. The user entered a valid second code at the prompt. For a more detailed description of Next Tokencode procedures and their use in evading attacks, see "When a PIN Is Stolen or Otherwise Compromised" on page 129.

Next Tokencode On (144)

Following a series of unsuccessful login attempts, the system put the token into Next Tokencode mode so that two sequential valid passcodes will be required before this user is granted access. See the note on the preceding item, "Next Tokencode Accepted."

Next Tokencode Requested (1002)

A successful login attempt was followed by a system request for a second code in order to verify that the user had possession of the token. See the note on the item "Next Tokencode Accepted."

Two circumstances cause the "Next Tokencode Requested" message to be logged even though the user is not granted access:

- With the Authentication Manager and network under a heavy load, the Authentication Manager accepts the passcode or new PIN and attempts to inform the Agent Host, but the Agent Host times out before it receives the message. The Agent Host therefore displays **Access Denied** (or **PIN rejected**) to the user.

  When this happens, either instruct the user to wait for the tokencode to change and then to try again until successful, or increase the **Agent Timeout** value and generate and distribute a new **sdconf.rec** file to each Agent Host. On Windows, use the Configuration Management application to increase the **Agent Timeout** value. On UNIX, use the **sdsetup -config** command.

  For more information on distributing the **sdconf.rec** file, see "Distributing the Configuration Update" on page 243 (for Windows) or on page 259 (for UNIX).

  Note: When a user has more than one token, access denials due to Agent time-out may be more frequent, since the Authentication Manager checks each token in turn until a match is found.

- The encryption value in the **sdconf.rec** file (or other configuration method) on the Agent Host does not match the encryption type in the Agent Host record.

  If the encryption type is set incorrectly in the Agent Host record, on the Agent Host menu, click **Edit Agent Host** to change the setting. If the setting in the **sdconf.rec** file is incorrect, for instructions on providing a new configuration file to the Agent Host, see Chapter 12, "Configuring the RSA Authentication Manager (Windows)".

No Agent Host Access Times Enabled

The user was directly activated on the Agent Host, but the access time information did not permit authentication.

No Agent Host/Group Times Enabled (1084)

The user was activated on an Agent Host both directly and through a group, but neither activation allowed the user to authenticate due to access time restrictions.

No authentication service. No RSA ACE/Server Back Ends registered (16210)

There is a problem with the authentication service. The front end service, which accepts authentication requests, and the back end service, which processes the requests, are experiencing some kind of communication problem. Restart the Authentication Manager. On Windows, use the RSA Authentication Manager Control Panel to stop and start the Authentication Manager. On UNIX, use the **aceserver stop** and **aceserver start** commands.

No CONDITION section has been specified in the query definition

A required section of the **definition.txt** file is missing. This error could be generated in the case of someone manually editing the **definition.txt** file of a query, which is not recommended. Alternatively, the file has somehow become corrupted. To fix this, try editing and recompiling the query.

No Group Access Times Enabled (1086)

The user was activated on the Agent Host through a group, but the access time information did not permit authentication.

No group has been selected

In the Query Access Level dialog box in the Query Wizard, you have chosen to set the access level to group level, but did not specify a group.

No name has been specified for the query in the 'Copy as' line

You are attempting to make a copy of an existing query, but have not entered the name for the copy.

No name has been specified for the query in the 'Save as' line

In the Acquire Shared Queries dialog box, you are acquiring a query but have not entered the name to which the query should be saved.

No One-Time Passwords (1088)

A user attempted to pass authentication with a one-time password, but has no passwords remaining. This message may be seen in conjunction with One-Time Password Set Expired, especially if the user has only one set of one-time passwords and the set has expired.

No query has been selected for acquisition

In the Acquire Shared Queries dialog box, you must select a query to acquire before clicking **OK**.

No Realm Secret Established (8219)

No realm secret has been established between the local Authentication Manager and the realm requesting authentication. Click **Establish Realm Secret** in the Edit Realm dialog box to establish the realm secret.

No Response From Remote Realm

The realm that received the authentication request did not respond before the local Agent Host timed out. The remote realm Authentication Manager may not be working or the network connection may be broken. If the problem occurs consistently, consider increasing the **Agent Timeout** value. For instructions, see "PASSCODE Accepted (1011)" on page 361.

No SELECT section has been specified in the query definition

A required section of the **definition.txt** file is missing. This error could be generated in the case of someone manually editing the **definition.txt** file of a query, which is not recommended. Alternatively, the file has somehow become corrupted. To fix this, try editing and recompiling the query.

No site has been selected

In the Query Access Level dialog box in the Query Wizard, you have chosen to set the access level to site level, but did not specify the actual site.

Node Secret Sent to Agent Host (1045)

If Automatic Delivery is used, after the Authentication Manager receives its first successful authentication from an identified Agent Host, it logs this message. For information about the different types of node secret delivery, see "Node Secret File" on page 228.

A missing or mismatched node secret makes Agent Host-Authentication Manager communications impossible. If there is a problem with the node secret, a **Node Verification Failed** error is logged. For details, see "ACCESS DENIED, Bad Lost Token PSW (1083)" on page 301.

Node verification failed (137)

If communication packets cannot be decrypted, this message is logged. Packets sent between an Agent Host and the Authentication Manager are encrypted with a key that includes the Agent Host's IP address and a node secret, which is a random string known only to the Agent Host and the Authentication Manager.

Deleting and re-creating an Agent Host or deleting a node secret file causes this problem by creating a mismatch between the node secret recorded on the Authentication Manager and the one recorded on the Agent Host. When this happens, no authentication attempts from this Agent Host will succeed.

To solve the problem:

1. Clear the node secret file on the Agent Host.
   - On an Agent Host running RSA ACE/Agent for Windows 5.2 (or later) software, open the RSA Authentication Manager application, and click **Advanced Settings** > **Clear Node Secret**.
   - On an Agent Host running older RSA ACE/Agent software for Windows (other than 4.4.x), delete the node secret file in the ***%SYSTEMROOT%*\system32** directory. By default, the file is named **securid**.
   - On an Agent Host running RSA ACE/Agent software for Windows 4.4.x software, delete the node secret file in the system registry. By default, the file is named **securid**.
   - On an Agent Host running RSA Authentication Manager software for UNIX, delete the node secret file stored in the ***ACEDATA*** directory. By default, the file is named **securid**.
2. If you are using Automatic Delivery, clear the node secret file on the Authentication Manager. If you are using Manual Delivery, this step is not necessary.

   To clear the node secret on the RSA Authentication Manager, open the Edit Agent Host dialog box for the Agent Host, and clear the **Node Secret Created** checkbox.
3. When the node secret is cleared on both the Agent Host and the Authentication Manager:
   - If you are using Automatic Delivery, which is the default, the node secret file will be resent to the Agent Host the next time there is a successful authentication on the Agent Host. The **Node Secret Created** checkbox is selected when this process takes place.
   - If you are using Manual Delivery to create a new node secret, see the Help for instructions.

   For information about the different types of node secret delivery, see "Node Secret File" on page 228.

The "Node verification failed" message is also logged in the following circumstances:

- The encryption type specified in the Agent Host's **sdconf.rec** file does not match the encryption type in the Authentication Manager's Agent Host record.

  If the encryption type is set incorrectly in the Agent Host record, on the Agent Host menu, click **Edit Agent Host** to change the setting. If the setting in the **sdconf.rec** file is incorrect, for more information on distributing the **sdconf.rec** file, see "Distributing the Configuration Update" on page 243 (for Windows) or on page 259 (for UNIX).
- When a remote user attempts authentication on a cross-realm authentication Agent Host before the node secret has been created. If the requesting user is not activated on the Agent Host, **User Not on Agent Host** is logged together with the **Node Verification Failed** message.
- You created the node secret file on the Authentication Manager but did not manually deliver it to the Agent Host. For instructions, see the Help.

Not Acting Server for this Agent (1139)

The Authentication Manager that received the request is not the assigned Acting Master or Slave for the Agent Host. For more information, see "Agent Host has no Acting Servers (1138)" on page 309.

No User Password in DB (8976)

An Agent request for a user's Windows login password has been denied because the user's password is not in the database. If an authorized user is prevented from logging in as a result, place the user in New PIN Mode, and have the user attempt to authenticate again. If the problem persists, contact RSA Security Customer Support.

Number of records cannot be a negative number

In the Query Wizard Advanced Parameters dialog box, you attempted to enter a negative number (for example, "-100") in the record limit field. You can only enter a positive number (for example, "100" or "+100").

OA PIN+Tokencode Length Invalid (8967)

The user cannot be authenticated because the length of the PIN+Tokencode combination is shorter than allowed in the Edit Offline Authentication dialog box. Place the user in New PIN Mode and instruct the user to log on again and create a new PIN that meets the specified security policy. For example, if the setting is for 12 characters, and your tokens display a six-digit tokencode, the user's PIN must be six characters.

Offline authentication service failed to initialize context (20002)

A component of the **sdoad** service failed to start. If this message appears, restart the Authentication Manager. If the message persists, contact RSA Security Customer Support.

Offline authentication service configuration error (20003)

A component of the **sdoad** service failed to start. If this message appears, restart the Authentication Manager. If the message persists, contact RSA Security Customer Support.

Offline authentication service DB initialization error (20004)

A component of the **sdoad** service failed to start. If this message appears, restart the Authentication Manager. If the message persists, contact RSA Security Customer Support.

Offline-Auth Download Failed (8953)

OA download failed for the specified user. In the Edit Offline Authentication dialog box, select **Enable verbose offline authentication logging**, launch the log monitor, and instruct the user to attempt to download offline days again. If the operation fails, the Log Monitor should provide a description of the problem. If you cannot correct the problem, contact RSA Security Customer Support.

Offl-Auth PASSCODE REUSE detected (8960)

A user attempted to use the same passcode more than once to authenticate. This is typically a user error. Instruct users to wait until the tokencode changes on their token before attempting to authenticate again.

Offline-Auth Policy Failed (8959)

An Agent encountered a problem when requesting offline authentication policy data from the Authentication Manager. Delete and re-create the Agent Host record in the Authentication Manager database, and try again. If the problem persists, contact RSA Security Customer Support.

Offline-Auth Request Denied (8963)

This message may appear when offline authentication has been disabled at the system or Agent level, when the token type has been disabled, or when the user already has enough offline authentication data.

Old Primary. Shutting down (2322)

This message appears when you have nominated a new Primary and the old Primary attempts to communicate with the new one. If you see this message and you have not nominated a new Primary, contact RSA Security Customer Support.

One-time password not found in Server database, but cannot delete one-time password delta.

During a replication pass, the replication service attempted to apply a change to a database record, but the service could not access the record. This may happen when an administrator is editing the record during the replication pass. If this message persists, create a new replica package and apply it to the Replica.

One-Time Password Set Expired (1087)

A set of one-time passwords reached the expiration date and was removed by the RSA Authentication Manager. The user may have other one-time password sets that could be used for authentication.

One-time Password used to authenticate twice (%1) (15087)

If this message appears, contact RSA Security Customer Support.

PASSCODE Accepted (1011)

This message is logged when a user enters a valid passcode at the **Enter PASSCODE** prompt.

Two circumstances cause the "PASSCODE Accepted" message to be logged even though the user is not granted access:

- With the Authentication Manager and network under a heavy load, the Authentication Manager accepts the passcode or new PIN and attempts to inform the Agent Host, but the Agent Host times out before it receives the message. The Agent Host therefore displays **Access Denied** (or **PIN rejected**) to the user.

  When this happens, either instruct the user to wait for the tokencode to change and then to try again until successful, or increase the **Agent Timeout** value and generate and distribute a new **sdconf.rec** file to each Agent Host. On Windows, use the Configuration Management application to increase the **Agent Timeout** value. On UNIX, use the **sdsetup -config** command.

  For more information on distributing the **sdconf.rec** file, see "Distributing the Configuration Update" on page 243 (for Windows) or on page 259 (for UNIX).

  Note: When a user has more than one token, access denials due to Agent time-out may be more frequent, since the Authentication Manager checks each token in turn until a match is found.

- The encryption value in the **sdconf.rec** file (or other configuration method) on the Agent Host does not match the encryption type in the Agent Host record.

  If the encryption type is set incorrectly in the Agent Host record, use **Edit Agent Host** on the Agent Host menu to change the setting. If the setting in the **sdconf.rec** file is incorrect, for instructions on providing a new configuration file to the Agent Host, see Chapter 12, "Configuring the RSA Authentication Manager (Windows)," or Chapter 14, "Configuring the RSA Authentication Manager (UNIX)."

PASSCODE REUSE ATTACK Detected (149)

The passcode entered is based on a tokencode that the token has displayed at some time in the past and has previously been used to gain access. This is prohibited so that an unauthorized person cannot obtain (for example, through electronic eavesdropping) and then reuse a valid tokencode or passcode.

Password Authentication (1092)

This message is logged when a user enters a valid user password at the **Enter PASSCODE** prompt. In the audit log, the serial number of a user password always begins with UPW.

Pepper length out of range (1156)

The length of an RSA EAP Protected OTP credential sent from a RADIUS client is out of range. You can edit credential configuration settings on either the RSA Authentication Manager or the RADIUS client. For information on configuring RSA EAP Protected OTP on the RSA Authentication Manager, see the Help. To change credential settings on a RADIUS client, see your client software documentation.

Press spacebar to continue

If this message appears while you are running the Administration application, you may have run into a problem with the software. Note what you were doing when the message appeared and contact RSA Security Customer Support or your local distributor.

Prev Tokencode/Bad PIN Detected (1144)

The passcode sent to the RSA Authentication Manager contained a tokencode that the token displayed at some time in the past, but with an incorrect PIN. This may indicate that an unauthorized person learned a valid tokencode through some means such as electronic eavesdropping and is now attempting to guess the correct PIN.

Primary and Replica Sent XR Response (8223)

Both the Primary and the Replica for a realm sent a response to an authentication request. This indicates that the network connection between the Primary and Replica is broken.

Primary Breaking Connection %1 (15219)

This message appears when the authentication process is stopped on the Primary, and is followed by the "ACE/Server Replica will handle authentication requests" message.

Primary cannot connect to replica (2121)

Verify that the information (hostname, IP address) for the Replica is the same in the Replication Management utility and your DNS server or the system's hosts file. You may need to contact your IT department to resolve network issues.

Primary Has Connected To Replica

This is a status message that indicates that communication between the Primary and the Replica has been established.

Primary Received ... Changes From Replica

This is a status message that appears during a replication pass.

Primary Received ... Modified ... Records From Replica

This is a status message that appears during a replication pass.

Primary Requesting ... Changes From Replica

This is a status message that appears during a replication pass.

Primary Shut Down Connection %1 (15197)

The connection between the Primary and a Replica has stopped.

Primary Successfully Received Replica Records

Changes to the Replica database were received by the Primary during a replication pass.

Primary Unable To Connect To Replica

The network connection was lost or that the Primary is not working. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Primary unable to connect to Replica %1 (15119)

This message can appear when the Primary attempts to connect to the Replica during a database push, or when the Replica is starting or shutting down.

Primary Will Retry Every ... Seconds

The network connection was lost or that the Primary is not working. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Progress brokers are busy. If the brokers aren't running, delete .lk files in the data directory (15039)

If deleting the .lk files does not solve the problem, restart the Authentication Manager. If the message persists, contact RSA Security Customer Support.

PushDB failed after receipt (2289)

This message is logged after the **Start rep pack reinstall** message when the Replica successfully received the Replica Package from the Primary, but could not install it. Copy the Replica Package from the Replica's default Replica Package directory to the ***ACEDATA*** directory, and restart the Replica.

PushDB failed on replica (2286)

This message is logged on the Primary when the Primary attempts to send the database to the Replica, but fails. A diagnostic message appears prior to this message. For example, you may see "Error opening rep pack file" or "Error reading rep pack file" immediately before this message in the log. If there is a problem with a packet while the Primary is sending the Replica Package to the Replica, the Rep Pack send failed message appears on the Replica.

PushDB-Assisted Recovery (PushDB) Disabled. Replica Package must be applied manually. %1 (15163)

Manually apply the Replica Package, or turn on Push DB Assisted Recovery in the System Parameters.

PushDB-Error Reading Replica Package File %1 (15169)

The Primary could not push the database to the Replica. Stop and start the Replica. If the message persists, apply the Replica Package manually.

PushDB-Failed After Replica Received Replica Package %1 (15165)

The Replica could not apply the Replica Package pushed by the Primary. Stop and start the Replica. If the message persists, apply the Replica Package manually.

PushDB-failed on Replica %1 (15161)

The Primary could not push the database to the Replica. Restart the Replica. If the message persists, apply the Replica Package manually.

PushDB-Replica Server Restart Failed %1 (15171)

The Replica did not restart after receiving the pushed database from the Primary. Stop and start the Replica.

PushDB-SDSERV Copy Failed on Replica Package Install %1 (15166)

The Replica could not apply the Replica Package pushed by the Primary. Stop and start the Replica. If the message persists, apply the Replica Package manually.

Realm Responded Late (8221)

A realm responded after the local Agent Host timed out. The remote realm Authentication Manager may not be working, or the network connection may be broken. If the problem happens consistently, consider increasing the **Agent Timeout** value. For instructions, see "PASSCODE Accepted (1011)" on page 361.

Received Abort Signal (%1) (16201)

This message appears when an RSA Authentication Manager process dies (**syncsrvc** on Windows, **acesyncd** on UNIX, **sdadmind**, **acesrvc**, **acesrvc_be**, **logmainthd**). Look up the error listed in the message. If the problem is not related to RSA Authentication Manager software, take appropriate action, and restart the RSA Authentication Manager when the problem is resolved. If the problem is related to RSA Authentication Manager software, contact RSA Security Customer Support.

Remote error inserting realm

This message appears when a realm record for your local realm already exists in a remote database, and you attempt to add the remote realm to your database or establish a realm secret with the remote realm. If you see this message, you must delete your local realm record from the remote database.

Removed User Password (4541)

An administrator removed this user password from this user record. It cannot be used for authentication by the indicated user, and the user does not have the opportunity to create or accept a new password.

Rep authenticating prematurely (2304)

Verify that the Primary and Replica are running and that the connection between them is working. If they are not running, start them. If that does not work, generate a new Replica Package for the Replica and apply it manually.

Rep name in DB doesn't match host (2303)

The Primary cannot communicate with the Replica because there is a conflict between the name and IP address in the database and the name and IP address on the network. Verify that the name and IP address of the Replica as configured in the Replication Management utility matches the name and IP address designated on your DNS server or in the local hosts file.

Rep name in DB doesn't match host (2303)

The Primary cannot communicate with the Replica because there is a conflict between the name and IP address in the database and the name and IP address on the network. Verify that the name and IP address of the Replica as configured in the Replication Management utility matches the name and IP address designated on your DNS server or in the local hosts file.

Rep needs initial primary connect (2305)

The Primary has not communicated with the Replica. Perform each of the tasks in the following list, checking to see if the problem is resolved after each one. If this message persists after performing each task, contact RSA Security Customer Support for further assistance.

- Verify that the Primary and Replica are running and that the connection between them is working. If they are not running, start and stop them.
- Generate a new Replica Package for the Replica and push it or apply it manually.
- Check the configuration information on each Authentication Manager to make sure that the names and IP addresses are configured correctly.

Rep pack not for this replica (2306)

Create a new Replica Package for the Replica and apply it. If the message persists, verify that the information (hostname, IP address) for the Replica is the same in the Replication Management utility and your DNS server or the system's hosts file.

Rep pack packet send failed (2298)

This message indicates that there was a problem with a packet sent from the Primary to the Replica. The Replica shuts down, and the Push DB process stops. If you see this message repeatedly, restart the Replica. If the message persists after restarting, create a new Replica Package and manually apply it.

Rep pack processed by replica (2287)

A Replica Package was installed on a Replica, creating a new, updated database. After processing the Replica Package, the Replica restarts and connects to the Primary. This message is logged after the "Start rep pack reinstall" message when the Push DB process is proceeding normally.

Repeated Failures to Lock System Record (15273)

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Replica Breaking Connection %1 (15220)

This message appears when the authentication process is stopped on a Replica, and is followed by the "ACE/Server Primary will handle authentication requests" message.

Replica Correcting Clock By ... Seconds

This message indicates that the Replica is setting the time on its clock to match the time on the Primary.

Replica Is Not Currently Configured

If this messages appears, the process that handles Primary and Replica communications (**syncsrvc** on Windows; **acesyncd** on UNIX) is having trouble starting. To correct the problem, see "Resolving Problems Starting Primary and Replica Communication" on page 300.

Replica Received Unexpected Packet (15149)

If this message appears and you do not see "Primary Successfully Reconciled Database" or "Replica Successfully Reconciled Databases," your databases may be corrupted or grossly mismatched. This message is likely to be accompanied by other messages identified as trigger errors.

See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298. Contact RSA Security Customer Support if you see this message without reconciliation success messages.

Replica Rejecting *NAME* Delta

The Primary was unable to send a change (for example, the creation of an Agent Host or the deletion of a user record) to the Replica database. Use the RSA Authentication Manager Control Panel on both the Primary and Replicas to stop the services and the database brokers. Create a Replica Package and copy or push it to the Replica. Then restart the RSA Authentication Manager services on both machines. For specific messages, see page 427.

Replica reqs re-connect (2284)

This a status message that indicates that the Replica needs to connect to the Primary after the successful installation of the database on the Replica. This message appears after the "Shutting down Replica" message when the Push DB process is proceeding normally.

Replica requires PushDB (2285)

This message appears when you have created a new Replica Package using the Replica Management utility. If you have configured your System Parameters to Allow Push DB Assisted Recovery, and have created a new Replica Package, the Primary will push the database to the Replica. If Allow Push DB Assisted Recovery is not allowed, this message will be followed by the "Assisted recvry (PushDB) disabled" message.

Replica restart failed (2293)

This message is logged after the "Start rep pack reinstall" message when the Replica could not restart after installing the Replica Package. Restart the Replica manually. On Windows, use the RSA Authentication Manager Control Panel. On UNIX, use the **aceserver stop** and **aceserver start** commands.

Replica Shut Down Connection %1 (15196)

The connection between the Replica and the Primary has stopped.

Replica Unable To Bind To Port ...

If this message appears, the process that handles Primary and Replica communications (**syncsrvc** on Windows; **acesyncd** on UNIX) is having trouble starting. To correct the problem, see "Resolving Problems Starting Primary and Replica Communication" on page 300.

Replica Unable To Correct Clock %1 (15222)

A Replica could not reset the time on its system clock. Reset the clock manually.

Request Recvd From Unknown Realm (8216)

An authentication request was received from a realm not listed in the local Authentication Manager database. The realm record may have been corrupted or inadvertently deleted from the database. Use the Add Realm dialog box to add the realm and establish a new realm secret.

Response Delay cannot be increased. Adjust client timing parameters. Max. Avg. Latency: %1 secs (to %2) (15099)

Verify that the information (hostname, IP address) for the Replica is the same in the Replication Management utility and your DNS server or the system's hosts file. You may need to contact your IT department to resolve network issues.

Restarting replica (2294)

The Replica is restarting after installing the Replica Package. This message is logged after the **Start rep pack reinstall** message when the Push DB process is proceeding normally.

RSA ACE/Server Back End cannot get Front End sockaddr (16211)

There is a problem with the authentication service. The front end service, which accepts authentication requests, and the back end service, which processes the requests, are experiencing some kind of communication problem. Restart the Authentication Manager. On Windows, use the RSA Authentication Manager Control Panel to stop and start the Authentication Manager. On UNIX, use the **aceserver stop** and **aceserver start** commands.

RSA ACE/Server Back End cannot get IP address (16215)

There is a problem with the authentication service. The front end service, which accepts authentication requests, and the back end service, which processes the requests, are experiencing some kind of communication problem. Restart the Authentication Manager. On Windows, use the RSA Authentication Manager Control Panel to stop and start the Authentication Manager. On UNIX, use the **aceserver stop** and **aceserver start** commands.

RSA ACE/Server Back End cannot get its own port data (16214)

There is a problem with the authentication service. The front end service, which accepts authentication requests, and the back end service, which processes the requests, are experiencing some kind of communication problem. Restart the Authentication Manager. On Windows, use the RSA Authentication Manager Control Panel to stop and start the Authentication Manager. On UNIX, use the **aceserver stop** and **aceserver start** commands.

RSA ACE/Server Back End cannot get the FE process handle (16217)

There is a problem with the authentication service. The front end service, which accepts authentication requests, and the back end service, which processes the requests, are experiencing some kind of communication problem. Restart the Authentication Manager. On Windows, use the RSA Authentication Manager Control Panel to stop and start the Authentication Manager. On UNIX, use the **aceserver stop** and **aceserver start** commands.

RSA ACE/Server Back End cannot get the FE socket data (16213)

There is a problem with the authentication service. The front end service, which accepts authentication requests, and the back end service, which processes the requests, are experiencing some kind of communication problem. Restart the Authentication Manager. On Windows, use the RSA Authentication Manager Control Panel to stop and start the Authentication Manager. On UNIX, use the **aceserver stop** and **aceserver start** commands.

RSA ACE/Server Back End cannot set the FE socket data (16216)

There is a problem with the authentication service. The front end service, which accepts authentication requests, and the back end service, which processes the requests, are experiencing some kind of communication problem. Restart the Authentication Manager. On Windows, use the RSA Authentication Manager Control Panel to stop and start the Authentication Manager. On UNIX, use the **aceserver stop** and **aceserver start** commands.

RSA ACE/Server Back End noticed Front End is down (16212)

There is a problem with the authentication service. The front end service, which accepts authentication requests, and the back end service, which processes the requests, are experiencing some kind of communication problem. Restart the Authentication Manager. On Windows, use the RSA Authentication Manager Control Panel to stop and start the Authentication Manager. On UNIX, use the **aceserver stop** and **aceserver start** commands.

RSA ACE/Server Back End unable to connect to the Offline Authentication Data Daemon (22000)

A component of the **sdoad** service failed to start. If this message appears, restart the Authentication Manager. If the message persists, contact RSA Security Customer Support.

RSA ACE/Server cannot decrypt system security block. . . . (15022)

There was a problem decrypting sensitive data in your database. Verify that you have the correct license record in the ***ACEDATA*** directory.

RSA ACE/Server cannot retrieve Back End information (16209)

There is a problem with the authentication service. The front end service, which accepts authentication requests, and the back end service, which processes the requests, are experiencing some kind of communication problem. Restart the Authentication Manager. On Windows, use the RSA Authentication Manager Control Panel to stop and start the Authentication Manager. On UNIX, use the **aceserver stop** and **aceserver start** commands.

RSA ACE/Server Fatal - current system date precedes license creation date (16253)

The system clock is set to a date and time that is earlier than the creation date of the license. Reset the clock on the system.

RSA ACE/Server Fatal - License Expired (16252)

If this message appears, the process that handles Primary and Replica communications (**syncsrvc** on Windows; **acesyncd** on UNIX) is having trouble starting. To correct the problem, see "Resolving Problems Starting Primary and Replica Communication" on page 300.

RSA ACE/Server Fatal Error forking %1 (15054)

If you see this message, start the Authentication Manager. If the message persists, contact RSA Security Customer Support.

RSA ACE/Server Fatal Error Starting sdradiusd %1 (16185)

After the Primary pushes the database to a Replica, the Replica restarts. In this case, the RADIUS server could not restart on the Replica. Stop and restart the Replica. If the message persists, contact RSA Security Customer Support.

RSA ACE/Server Front End cannot get a work queue entry (16219)

There is a problem with the authentication service. The front end service, which accepts authentication requests, and the back end service, which processes the requests, are experiencing some kind of communication problem. Restart the Authentication Manager. On Windows, use the RSA Authentication Manager Control Panel to stop and start the Authentication Manager. On UNIX, use the **aceserver stop** and **aceserver start** commands.

RSA ACE/Server Front End cannot get back end info (16220)

There is a problem with the authentication service. The front end service, which accepts authentication requests, and the back end service, which processes the requests, are experiencing some kind of communication problem. Restart the Authentication Manager. On Windows, use the RSA Authentication Manager Control Panel to stop and start the Authentication Manager. On UNIX, use the **aceserver stop** and **aceserver start** commands.

RSA ACE/Server Front End cannot get socket data (16218)

There is a problem with the authentication service. The front end service, which accepts authentication requests, and the back end service, which processes the requests, are experiencing some kind of communication problem. Restart the Authentication Manager. On Windows, use the RSA Authentication Manager Control Panel to stop and start the Authentication Manager. On UNIX, use the **aceserver stop** and **aceserver start** commands.

RSA ACE/Server No Back Ends registered with the Front End (16208)

There is a problem with the authentication service. The front end service, which accepts authentication requests, and the back end service, which processes the requests, are experiencing some kind of communication problem. Restart the Authentication Manager. On Windows, use the RSA Authentication Manager Control Panel to stop and start the Authentication Manager. On UNIX, use the **aceserver stop** and **aceserver start** commands.

RSA ACE/Server out of memory (15078)

The system memory is full or insufficient. Check which processes are using available memory. Verify that your system meets the minimum memory requirements as described in the *Installation Guide* for your platform.

sdserv copy failed on reinstall (2291)

On the Replica, the Replica Package installation could not copy the Authentication Manager database files to the *ACEDATA* directory. The Replica restart failed message is logged immediately after this message.

Segmentation violation (%1) (16200)

This message appears when an RSA Authentication Manager process dies (**syncsrvc** on Windows, **acesyncd** on UNIX, **sdadmind**, **acesrvc**, **acesrvc_be**, **logmainthd**). Look up the error listed in the message. If the problem is not related to RSA Authentication Manager software, take appropriate action, and restart the RSA Authentication Manager when the problem is resolved. If the problem is related to RSA Authentication Manager software, contact RSA Security Customer Support.

Select Error On Connection (15195)

The network connection was lost or that the Primary is not working. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Select Error On Well Known Port (15150)

The network connection was lost or that the Primary is not working. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Set User Password (4540)

An administrator defined a user password for a user, and the password was placed in Change Required mode.

Shutting down replica (2299)

The Replica shuts down when the Push DB process succeeds, but also whenever there is a problem with the database or the Replica Package on a Replica. When the Push DB process succeeds, this message is preceded by the "Rep pack processed by Replica" message. When there is a problem, this message might be preceded by the "Push DB failed on Replica" message and other error messages related to the Push DB process. The additional messages indicate the exact nature of the problem.

SIGPIPE, write with no one to read, resending (%1) (16204)

This message appears when an RSA Authentication Manager process dies (**syncsrvc** on Windows, **acesyncd** on UNIX, **sdadmind**, **acesrvc**, **acesrvc_be**, **logmainthd**). Look up the error listed in the message. If the problem is not related to RSA Authentication Manager software, take appropriate action, and restart the RSA Authentication Manager when the problem is resolved. If the problem is related to RSA Authentication Manager software, contact RSA Security Customer Support.

Simultaneous Login Detected (148)

This message is written to the RSA Authentication Manager audit trail to alert you that an attempt was made to break into your network. The Authentication service has detected the attempt and prevented access.

If you see this message, ***immediately set the token into New PIN mode and clear the old PIN***. For instructions, see "Setting New PIN Mode" on page 131.

Sizelimit exceeded

This message appears if a synchronization job that connects with any of the three supported LDAP directory servers contains a query that returns a large number of user records (more than 1,000). For more information, see "date time Ext-auth Check error -nnnnn login user Agent Host server token (8401)" on page 331.

Socket initialization failed %1 (15025)

Restart the Authentication Manager. If the message persists, contact RSA Security Customer Support.

Space symbol cannot be used as a text qualifier

In the Query Wizard Advanced dialog box, you attempted to use the space character in the Qualifier field for the CSV format. The default is the double-prime (") symbol, but you can choose from other symbols to specify the qualifier in CSV. (Make sure your target application to open CSV supports alternative qualifiers.)

ST Agent Host - No New PIN (1031)

Access is denied and this message is logged when someone attempts to log on through an Agent Host that cannot handle the interactive New PIN operation (a single-transaction Agent Host).

Verify that the token is in New PIN mode by running the Administration application and clicking **Token > Edit Token**.

If the token is in New PIN mode, the user must create or be given a new PIN in order to log on. Users who can log on directly rather than remotely can get new PINs immediately and proceed.

However, if it is impossible or inconvenient for the user to log on directly, you must perform the **Set PIN to Next Tokencode** operation. With this procedure, the user gets a numeric PIN that (like all PINs) is known only to that user. See "Setting New PIN Mode" on page 131.

ST Agent Host - No Next Tokencode (1032)

Access is denied and this message is logged when someone attempted to log on through an Agent Host that cannot handle the interactive Next Tokencode operation (a single-transaction Agent Host).

There are two ways to solve this problem:

- If the user can log on through a different Agent Host type, that user will be prompted for a second tokencode and can complete the Next Tokencode operation.
- If it is not possible or convenient for the user to log on directly, you need to perform the **Resynchronize Token** operation. See "Resynchronizing a Token" on page 132.

Start rep pack reinstall (2290)

The Replica has received a Replica Package and is attempting to install it. This message is logged after **Shutting down Replica** when the Push DB process is proceeding normally.

Starting PushDB (2295)

The Primary is attempting to send the Replica Package to the Replica. This message is logged after **Replica Receives Push DB** when the Push DB process is proceeding normally.

System clock setback detected (150)

The Authentication Manager has detected that the system clock has been set back. This may indicate a replay attack and, possibly, a breach in your system security. In a replay attack, an intruder attempts to gain access with a captured passcode by setting the system clock back and reusing the passcode at the appropriate time.

The database has rejected acesyncd's credentials

If this message appears, the process that handles Primary and Replica communications (**syncsrvc** on Windows; **acesyncd** on UNIX) is having trouble starting. To correct the problem, see "Resolving Problems Starting Primary and Replica Communication" on page 300.

The default output location cannot be empty

In the Query Wizard Output Parameters dialog box, you have left the Default output location field blank. Specify a valid pathname in this field.

The entry securid/securidprop ...... is invalid

If you see this message, make sure that the file ***%SYSTEMROOT%*\system32\drivers\etc\services** or the DNS name server contains lines that correctly provide the names of the Authentication service and the Replication service.

The default name of the Authentication service is **securid**, and its default port number is 5500. The name of the Replication Communication service is the Authentication service name plus prop; the default name of the Primary is **securidprop_00**, and the default port number is 5505. Each Replica has its own service name and port number.

By default, Replicas are assigned the service names **securidprop_01**, **securidprop_02**, and so on, and the port numbers 5506, 5507 and so on.

To find out the correct service name and port number for the Authentication service:

Click **Start > RSA Security >** RSA Authentication Manager **Configuration Tools** > **RSA Authentication Manager Replica Management**, then click **Details**.

The information appears in the **Authentication** fields under **Services**.

To find out the correct service name and port number for the Primary and Replica Communication service:

Click **Start** > RSA Authentication Manager **6.1 > Replication Management > Server** > **Details**.

The information appears in the **Service Name** and **Service Port Number** fields.

The file name prefix cannot be empty

In the Query Wizard Output Parameters dialog box, you have left the **Filename prefix** field blank. The term "query" is the default. Specify any valid character string in this field. Any character except the following is acceptable:

{} ~ " ; ' [ ] , / @ < > ^ |

The group specified in the query definition does not exist. The access level will be reset to default

The query access level for the query that you are running was set to a particular group. However, the group no longer exists. It was probably deleted from the Authentication Manager database since the query was last compiled.

The name of this Server in the sdconf.rec file does not match the name of any Server in the database (16260)

Run Configuration Management to view the name of this Authentication Manager in the **sdconf.rec** file and Replication Management to view the name of this Authentication Manager in the database. To resolve the conflict, edit the name of the Authentication Manager in the configuration file or the database.

The query DESCRIPTION data is too long and will be truncated

This error would only be generated in the case of someone manually editing the **definition.txt** file of a query, which is not recommended.

The RSA ACE/Server on this system has established a connection with an old Primary, %1. The connection was refused (16181)

A newly nominated Primary connected to the old Primary. The old Primary shuts down. Create a new Replica Package and apply it to the old Primary manually.

The RSA ACE/Server on this system has established a connection with an old Primary, %1. The connection was refused. Pushing database to that RSA ACE/Server (16180)

A newly nominated Primary connected to the old Primary. No action is required. The new Primary will push the database to the old Primary.

The SELECT statement is too long

This error would only be generated in the case of someone manually editing the **definition.txt** file of a query, which is not recommended.

The site specified in the query definition does not exist. The access level will be reset to default

The query access level for the query that you are running was set to a particular site. However, the site no longer exists. It was probably deleted from the Authentication Manager database since the query was last compiled.

The system call gethostname() failed, error = %1 (15024)

Look up the specific error indicated in the message and check the log for additional messages that may be related to this problem. If the message persists, contact RSA Security Customer Support.

There are multiple asterisks in the query. Only one is allowed

The asterisk can be used as a wildcard character in the column list of a query; however, only one wildcard character can be used.

There are too many active users and Replicas in the database/Number of active users and Replicas in the database exceeds license limit

Your system is either in *violation* mode or *upgrade violation* mode.

Violation mode occurs under either of the following circumstances:

- You have installed a new RSA Authentication Manager and have exceeded your license limits.
- Your license was in upgrade violation mode and is now in violation mode.

When your license is in violation mode, you cannot activate additional users and/or add new Replicas.

Upgrade Violation mode occurs when you upgrade your RSA Authentication Manager and have exceeded your license limits. Upgrade violation mode effectively turns your license into a 90-day temporary license. When your license expires, it goes into violation mode, meaning you are prevented from activating additional users and/or adding new Replicas.

To bring your system back into compliance, contact RSA Security to obtain a new license. Alternatively, you can deactivate a sufficient number of users or remove one or more Replicas from your database to bring your system back into compliance.

For additional information about licensing, see Appendix A, "Licensing."

There are too many active users in the database/Number of active users in the database exceeds license limit/ Number of active users in the database reached license limit

Your system is either in *violation* mode or *upgrade violation* mode.

Violation mode occurs under either of the following circumstances:

- You have installed a new RSA Authentication Manager and have exceeded your license limits.
- Your license was in upgrade violation mode and is now in violation mode.

When your license is in violation mode, you cannot activate additional users.

Upgrade Violation mode occurs when you upgrade your RSA Authentication Manager and have exceeded your license limits. Upgrade violation mode effectively turns your license into a 90-day temporary license. When your license expires, it goes into violation mode, meaning you are prevented from activating additional users.

To bring your system back into compliance, contact RSA Security to obtain a new license. Alternatively, you can deactivate a sufficient number of users to bring your system back into compliance.

For additional information about licensing, see Appendix A, "Licensing."

There are too many Replicas in the database/Number of Replicas in the database exceeds license limit

Your system is either in *violation* mode or *upgrade violation* mode.

Violation mode occurs under either of the following circumstances:

- You have installed a new RSA Authentication Manager and have exceeded your license limits.
- Your license was in upgrade violation mode and is now in violation mode.

When your license is in violation mode, you cannot add new Replicas.

Upgrade Violation mode occurs when you upgrade your RSA Authentication Manager and have exceeded your license limits. Upgrade violation mode effectively turns your license into a 90-day temporary license. When your license expires, it goes into violation mode, meaning you are prevented from adding new Replicas.

To bring your system back into compliance, contact RSA Security to obtain a new license. Alternatively, you can remove one or more Replicas from your database to bring your system back into compliance.

For additional information about licensing, see Appendix A, "Licensing."

This is an old Primary. Receiving DB Push. %1 (16183)

The old Primary is receiving the database from the new Primary. No action is required.

This is an old Primary. Shutting down. Replica Package should be applied. %1 (16182)

An old Primary logs this message when the new Primary connects to it, but Push DB is not enabled in the System Parameters. Create a new Replica Package and apply it to the old Primary manually.

This query is from an older version of the ACE/Server. It must recompiled by a Realm Administrator

Because of changes in versions of RSA Authentication Manager, backward compatibility of queries cannot be guaranteed. Therefore, recompiling queries created in one major version of RSA Authentication Manager is necessary when you have upgraded to a new major version of the Authentication Manager.

This query is not valid in this realm

This query was compiled in another realm and therefore cannot be run in the current realm.

This tool must be run on the same machine as the ACE/Server

If you are on an Authentication Manager and get this message:

1. Open the Control Panel and double-click **Network** to see the name of the computer.

   The **Computer Name** that you see should be in the list of aliases for the Authentication Manager machine in the **hosts** file, the database of a DNS server, or both.

2. If the name does not appear, edit the ***%SYSTEMROOT%*\system32\drivers\etc\hosts** file, the DNS server database, or both.

Make sure also that the Authentication Manager name is specified correctly in the **sdconf.rec** file by opening the Configuration Management application on the Primary. If the names do not match, use the **Edit** option to change the **sdconf.rec** file. Then distribute the new **sdconf.rec** file to the Replica and to all the Agent Hosts.

For more information on distributing the **sdconf.rec** file, see "Distributing the Configuration Update" on page 243 (for Windows) or on page 259 (for UNIX).

Note: The **sdconf.rec** file is created by the Configuration Management application. Agent Hosts may use **DES** or **SDI** encryption, and each Agent Host must have an **sdconf.rec** file that contains a match for the encryption it uses. If you have some Agent Hosts that use **DES** encryption and other Agent Hosts that use **SDI** encryption, make sure that the **sdconf.rec** file you distribute to each Agent Host has the correct encryption setting.

Timed out trying to insert realm

The RSA Authentication Manager was unable to establish the realm secret with the remote Primary. To establish a realm secret, the Primary in the local realm and the Primary in the remote realm must have the same port number, and the Primary in the remote realm must be running. Contact the administrator in the remote realm for the correct port number. You must first update the port number in the ***%SYSTEMROOT%*\system32\drivers\etc\services** file. Then, use the Configuration Management application to change the port number of your Primary.

Timelimit exceeded

This message appears if a synchronization job that connects with any of the three supported LDAP directory servers contains a query that returns a large number of user records (more than 1,000). For more information, see "date time Ext-auth Check error -nnnnn login user Agent Host server token (8401)" on page 331.

Token Disabled, Many Failures (145)

The token was disabled automatically because either the system detected three consecutive login attempts with a valid tokencode but an invalid PIN, or the system detected a specified number of consecutive invalid passcodes. (It does not matter which factor, PIN or tokencode, was incorrect.) This number can be any value between 1 and 10.

Note: When a user has more than one token, an invalid login counts against all of the tokens assigned to that user.

For a more detailed description of this evasion-of-attack feature, see "When a Token Is Stolen or Otherwise Missing" on page 126.

Token Disabled, Suspect Stolen (143)

The token was disabled automatically because the system detected three consecutive login attempts with valid tokencodes but an invalid PIN. This is possible only with RSA SecurID standard cards and key fobs, where the user enters the tokencode and PIN separately instead of entering a passcode.

Note: When a user has more than one token, an invalid login counts against all of the tokens assigned to that user.

For a more detailed description of this evasion-of-attack feature, see "When a Token Is Stolen or Otherwise Missing" on page 126.

Token not found in Server database, but cannot delete token delta.

During a replication pass, the replication service attempted to apply a change to a database record, but the service could not access the record. This may happen when an administrator is editing the record during the replication pass. If this message persists, create a new replica package and apply it to the Replica.

Token not found in Server database, but cannot delete user delta. %1 (15237)

This message indicates an error during replication. Create a new Replica Package for the Replica and apply it manually or by using Push DB. If the message persists, contact RSA Security Customer Support.

Token record is locked and cannot be updated. Will attempt to update at next replication pass.%1 (15218)

If you see this message repeatedly, stop and start the Primary. If the message persists, restart the Replica. If the message persists after restarting, contact RSA Security Customer Support.

Too many statements to process. The limit is 32 statements to a query

The query contains more than 32 SQL statements, over the allowable limit in RSA Authentication Manager Custom Queries.

Trace file closed

Trace files can be used to help troubleshoot Primary and Replica communication problems. For instructions on enabling the packet trace and viewing the results, contact RSA Security Customer Support.

Trace File Opened

Trace files can be used to help troubleshoot Primary and Replica communication problems. For instructions on enabling the packet trace and viewing the results, contact RSA Security Customer Support.

Trigger: %1 (15275)

If this message appears, contact RSA Security Customer Support.

Two different node secrets created for a single agent. Delete agent's secret and re-authenticate %1 (16226)

The node secret on the Agent Host does not match the node secret for that Agent Host in the database. Delete the node secret from the Agent Host and clear the node secret from the Agent Host record in the database.

Unable to access common query storage. Check folder name

In the Share Queries dialog box, the folder name you entered in the Folder containing shared queries field is not valid, or you might not have the proper permissions to access the folder.

Unable to access query data

In the Query Wizard Query Name dialog box, the folder name you specified was invalid, or you do not have the proper permissions to access it.

Unable to access query repository

The Query Wizard is unable to create the query subdirectory because there was a problem accessing the **ace/data/queries** directory. You might not have the proper permissions to access this directory, or the directory might be missing or corrupted.

Unable to assign a replacement for the current token

This message appears if the user record for the token is unavailable or cannot be retrieved. Verify that the token's user record is still available in the database. If the record is not available, assign a different token.

This message can also appear in the following circumstances:

- The token record is corrupted.
- The PIN for the token to be replaced could not be retrieved.
- The PIN for the replacement token could not be retrieved, copied, or cleared.

Assign a different replacement token.

Unable to assign a replacement token for token serial number 000000*nnnnnn*

This message appears if the user record for the token is unavailable or cannot be retrieved. Verify that the token's user record is still available in the database. If the record is not available, assign a different token.

This message can also appear in the following circumstances:

- The token record is corrupted.
- The PIN for the token to be replaced could not be retrieved.
- The PIN for the replacement token could not be retrieved, copied, or cleared.

Assign a different replacement token.

Unable to chdir to running directory

If this message appears, the process that handles Primary and Replica communications (**syncsrvc** on Windows; **acesyncd** on UNIX) is having trouble starting. To correct the problem, see "Resolving Problems Starting Primary and Replica Communication" on page 300.

Unable to connect to sdlog

If this message appears, the process that handles Primary and Replica communications (**syncsrvc** on Windows; **acesyncd** on UNIX) is having trouble starting. To correct the problem, see "Resolving Problems Starting Primary and Replica Communication" on page 300.

Unable to connect to sdserv

If this message appears, the process that handles Primary and Replica communications (**syncsrvc** on Windows; **acesyncd** on UNIX) is having trouble starting. To correct the problem, see “Resolving Problems Starting Primary and Replica Communication” on page 300.

Unable to create running directory

If this message appears, the process that handles Primary and Replica communications (**syncsrvc** on Windows; **acesyncd** on UNIX) is having trouble starting. To correct the problem, see “Resolving Problems Starting Primary and Replica Communication” on page 300.

Unable to delete used one-time password (%1) (15086)

If this message appears, contact RSA Security Customer Support.

Unable to determine IP address of Replica

If this message appears, the process that handles Primary and Replica communications (**syncsrvc** on Windows; **acesyncd** on UNIX) is having trouble starting. To correct the problem, see “Resolving Problems Starting Primary and Replica Communication” on page 300.

Unable To Determine Local IP Address

If this message appears, the process that handles Primary and Replica communications (**syncsrvc** on Windows; **acesyncd** on UNIX) is having trouble starting. To correct the problem, see “Resolving Problems Starting Primary and Replica Communication” on page 300.

Unable to find selected group in the database

This error only occurs if the group that you selected in the Query Wizard's Query Access Level dialog box is deleted by another administrator immediately after you selected it, but before you exited from the dialog box.

Unable to find selected site in the database

This error only occurs if the site that you selected in the Query Wizard's Query Access Level dialog box is deleted by another administrator immediately after you selected it, but before you exited from the dialog box.

Unable to find site related to the selected group

This error only occurs if the site that you selected in the Query Wizard's Query Access Level dialog box is deleted by another administrator immediately after you selected it, but before you began selecting a group from the site.

Unable to initialize connection to Lock Manager. Check configuration settings (16222)

The port number or service name for the lock manager may be incorrect. Run the Configuration Management application and verify that the Lock Manager is using the correct Port Number and Service Name.

Unable to load security block encryption keys

If this message appears, the process that handles Primary and Replica communications (**syncsrvc** on Windows; **acesyncd** on UNIX) is having trouble starting. To correct the problem, see "Resolving Problems Starting Primary and Replica Communication" on page 300.

Unable to locate ACE/Server host

RSA Authentication Manager host names must appear in the local hosts file or in a name server. This message appears when a Primary, Replica, or Agent Host name cannot be found.

Unable to locate current query configuration

There was a problem loading the query data into the Query Wizard. The **definition.txt** file could be corrupted, or there is some other more serious problem. If you get this message, contact RSA Security Customer Support.

Unable to locate definition.txt file in the specified location

While importing a **definition.txt** file, you specified a location that did not contain a definition file.

Unable to locate *service name* in the services file....

If you see this message, make sure that either the file ***%SYSTEMROOT%*\system32\drivers\etc\services** (where ***%SYSTEMROOT%*** stands for the root Windows NT directory, for example **winnt**) or the DNS name server contains lines that correctly provide the names and port numbers of the RSA Authentication Manager services. (For instructions on finding this information, see the message "The entry securid/securidprop ...... is invalid" on page 374.)

The default name of the Authentication service is **securid**, and its default port number is 5500. The name of the Replication Communication service is the Authentication service name plus **prop**; the default name of the Primary is **securidprop_00**, and the default port number is 5505. Each Replica has its own service name and port number. By default, Replicas are assigned the service names **securidprop_01**, **securidprop_02** and so on, and the port numbers 5506, 5507 and so on. The other RSA Authentication Manager services and their defaults are External Authorization (**sdxauthd**, 5540); Remote Administration (**sdadmind**, 5550); and RADIUS (**radius**, 1645).

You can change these default service names and port numbers, but you must make sure that the information in the **services** file and the DNS name server matches. For more information, see the *Installation Guide* for your platform.

Unable to log in to database

If this message appears, the process that handles Primary and Replica communications (**syncsrvc** on Windows; **acesyncd** on UNIX) is having trouble starting. To correct the problem, see "Resolving Problems Starting Primary and Replica Communication" on page 300.

Unable To Resolve Port Number Of Service...

If this message appears, the process that handles Primary and Replica communications (**syncsrvc** on Windows; **acesyncd** on UNIX) is having trouble starting. To correct the problem, see "Resolving Problems Starting Primary and Replica Communication" on page 300.

Unable to Retrieve the system record. (15061)

Restart the Authentication Manager. If the message persists, contact RSA Security Customer Support.

Unable To Send Heartbeat %1 (15193)

Stop and start the Replica. If this message persists, contact RSA Security Customer Support.

Unable to Send License to Replica %1 (15156)

If this message persists, restart the Primary and the Replica. If this does not solve the problem, reinstall the Replica.

Unable To Swap Encryption Keys %1 (15154)

The Primary and Replica could not exchange encryption keys. Restart the Replica. If this message persists, restart the Primary. If restarting the Primary does not fix the problem, contact RSA Security Customer Support.

Unable To Swap Encryption Keys %1 (15154)

The Primary and Replica could not exchange encryption keys. Restart the Replica. If this message persists, restart the Primary. If restarting the Primary does not fix the problem, contact RSA Security Customer Support.

Unable To Sync Replica Clock %1 (15153)

The system cannot automatically reset the time on the Replica. Verify that the clock on the Replica is synchronized with the clock on the Primary. The time on the Replica must be set to within 30 seconds of the time on the Primary. On UNIX, this error appears when the RSA Authentication Manager is started by a user who is not root. Log on as root and restart the Authentication Manager.

Unable To Transfer Agent Hosts From Replica

The network connection was lost or the Primary is not working. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Unable to transfer Agents from Replica %1 (15125)

Back up the Replica database, create a new Replica Package for the Replica, and manually apply it.

Unable To Transfer Log Entries From Replica

This message indicates that the network connection was lost or that the Primary is not working. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Unable to transfer log entries from Replica %1 (15121)

Back up the Replica database, create a new Replica Package for the Replica, and manually apply it.

Unable to transfer one-time-passwords from Replica %1 (15124)

Back up the Replica database, create a new Replica Package for the Replica, and manually apply it.

Unable To Transfer System From Replica

The network connection was lost or the Primary is not working. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Unable To Transfer Tokens From Replica

The network connection was lost or the Primary is not working. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Unable to transfer tokens from Replica %1 (15123)

Back up the Replica database, create a new Replica Package for the Replica, and manually apply it.

Unable to transfer user from Replica %1 (15122)

Back up the Replica database, create a new Replica Package for the Replica, and manually apply it.

Unable to update system start time (15055)

Restart the Authentication Manager. If the message persists, contact RSA Security Customer Support.

Unassigning Primary Server token because a replacement token was issued on a Replica Server (16235)

The replacement token of a user was enabled when the user authenticated through a Replica. As a result, the Primary database is being updated to reflect that the token was enabled through the Replica.

Unexpected error from errSDDemonize()

If this message appears, the process that handles Primary and Replica communications (**syncsrvc** on Windows; **acesyncd** on UNIX) is having trouble starting. To correct the problem, see "Resolving Problems Starting Primary and Replica Communication" on page 300.

Unexpected packet received %1 (15194)

Stop and start the Primary. If this message persists, contact RSA Security Customer Support.

Unexpected Packet. *NAME* Commit Response Expected (for specific messages, see page 430)

If this message appears, there is probable database corruption, gross mismatch between databases, or missing or corrupted files. See "Probable Loss of Network Connection or Authentication Manager Is Down" on page 298.

Unknown Lost Token Auth Method (1089)

If you find this message in your audit log, contact RSA Security Customer Support for assistance.

Unknown word encountered

This message appears in some cases when you have misspelled an entry in the SQL. For example, "MESSAG" instead of "MESSAGE".

Upgrade license check...You are attempting to upgrade an Advanced license with a Base license

You are attempting to apply a Base license, which has less potential to scale than your current Advanced license. Make sure you are using the newest version license that RSA Security has issued to you, and retry the upgrade. You should not proceed with the downgrade unless RSA Security Customer Support instructs you to do so.

For additional information about licensing, see Appendix A, "Licensing."

Upgrade license check...Your current license has a higher active user limit than its replacement

You are attempting to apply a license that allows fewer active users than your current license. Make sure you are using the newest version license that RSA Security has issued to you, and retry the upgrade. You should not proceed with the downgrade unless RSA Security Customer Support instructs you to do so.

For additional information about licensing, see Appendix A, "Licensing."

Upgrade Replica To Match Primary

If this message appears, the process that handles Primary and Replica communications (**syncsrvc** on Windows; **acesyncd** on UNIX) is having trouble starting. To correct the problem, see "Resolving Problems Starting Primary and Replica Communication" on page 300.

User not found in Server database, but cannot delete user delta (15232)

During a replication pass, the replication service attempted to apply a change to a database record, but the service could not access the record. This may happen when an administrator is editing the record during the replication pass. If this message persists, create a new replica package and apply it to the Replica.

User Not on Agent Host (131)

Access is denied and this message is logged when a user tries to log on to an Agent Host on which the user is not activated. If appropriate under your security policy, activate the user directly or through a group by following the directions in Chapter 3, "Agents and Activation on Agent Hosts."

This message also appears if the requesting user is activated on the Agent Host but has no assigned token. If no user is identified in the log record, the requesting user may not yet have a user record.

If an Agent Host is configured for cross-realm authentication, and a user from another realm who has not been activated on the Agent Host attempts to log on before the node secret is established, this message is logged together with the "Node Verification Failed" message.

User Password Update Failed (8955)

The user's Windows password could not be updated in the Authentication Manager database. Check to see whether another administrator disabled Windows password integration in the System Parameters dialog box. Otherwise, there may be a problem with the Agent Host record in the Authentication Manager database. Try deleting and re-adding the Agent Host and clearing the node secret. The next time the user authenticates, the Agent must re-prompt for the Windows password, and must attempt to resend the password to the Authentication Manager. If the problem persists, contact RSA Security Customer Support.

User record has been updated, but is currently locked. The updated record cannot be sent to Primary. Will attempt to update at next replication pass.%1 (15216)

If you see this message repeatedly, stop and start the Replica. If the message persists, restart the Replica. If the message persists after restarting, contact RSA Security Customer Support.

Warning: Unable to open syslog

If this message appears, the process that handles Primary and Replica communications (**syncsrvc** on Windows; **acesyncd** on UNIX) is having trouble starting. To correct the problem, see "Resolving Problems Starting Primary and Replica Communication" on page 300.

Work queue cannot allocate memory (16223)

The system memory is full or insufficient. Verify that your system meets the minimum memory requirements as described in the *Installation Guide* for your platform.

Write failed, file system is full

If you have insufficient disk space on your servers, the Authentication Manager cannot function. ***Do not allow your disk to become more than 90% full or you will experience problems with all applications***, including RSA Authentication Manager programs.

XR ACCESS DENIED, Bad Passcode (8212)

The user entered an incorrect passcode. This message might be logged if, because of network-related delays, the authentication request did not reach the user's home realm until after the user's tokencode changed. For other reasons why this message might appear, see "ACCESS DENIED, PASSCODE Incorrect (1008)" on page 304.

XR ACCESS DENIED, Ext-auth failed *login user Agent Host server token* (8235)

This message appears if you have activated External Authorization on your RSA Authentication Manager. This message appears in the following circumstances:

- A user's attempt to access his or her home Authentication Manager from a remote realm failed because the **Enable Authorization of Remote Requests** option is not enabled on the home Authentication Manager. Enable this option if you want to let users access their home Authentication Manager from remote realms.
- A user's attempt to access his or her home Authentication Manager from a remote realm failed because the **iSDExtAuthorGetHomeData()** request failed. (The **iSDExtAuthorGetHomeData()** routine gets local information to be returned as part of a cross-realm authentication.) Review the Event Log for messages that might indicate why the request failed.
- The **iSDExtAuthorGetHomeData()** request failed. Review the Event Log for messages that might indicate why the request failed.

XR ACCESS DENIED, Next Code Bad (8207)

The user attempted to answer the Next Tokencode prompt but entered a code that was not valid for the token. Therefore, the authentication request was denied.

This message might be logged if the user typed the wrong tokencode, or, due to network-related delays, the authentication request did not reach the user's home realm until after the user's next tokencode changed. For other reasons why this message might appear, see "When a PIN Is Stolen or Otherwise Compromised" on page 129.

XR Agent Host Not Found (8217)

An authentication request was received from a remote realm, but the local Authentication Manager could not find an Agent Host record corresponding to the remote Agent Host that initiated the request. When a remote realm is running an RSA Authentication Manager version earlier than 3.1, the remote Agent Hosts must be registered in your RSA ACE/Server 3.1 or later database in order for your users to access them. For more information, see "Some Realms Not Upgraded to RSA ACE/Server 5.0.1 or Later" on page 83.

XR Good Tokencode/Bad PIN Detected (8238)

The passcode sent to the RSA Authentication Manager from a remote realm contained a good tokencode, but a bad PIN. This could be a sign that an unauthorized user has acquired an authorized user's token and is attempting to guess the correct PIN.

XR New PIN Created by User (8210)

A user created a new PIN while attempting to pass authentication in a remote realm.

XR New PIN Rejected (8211)

The user attempting to pass authentication in a remote realm did not complete the New PIN operation successfully. Either the new PIN did not meet system specifications for length or allowable characters, or the user canceled the New PIN process. The token is still in New PIN mode.

XR New PIN Required (8208)

A user was required to create a new PIN while attempting to pass authentication in a remote realm.

XR New System Generated PIN (8209)

A user accepted the system-generated PIN while attempting to pass authentication in a remote realm.

XR Next Tokencode On (8214)

This was the last of a (user-specified) number of consecutive failed login attempts by a user attempting to log in to a remote realm. The user entered a valid PIN but an invalid tokencode. The token was put into Next Tokencode mode so that two sequential valid passcodes will be required before this user is granted access. For a more detailed description of Next Tokencode mode, see "When a PIN Is Stolen or Otherwise Compromised" on page 129.

XR Next Tokencode Required (8206)

A user attempting to pass authentication in a remote realm was required to enter a second tokencode in order to verify possession of the token. For a more detailed description of Next Tokencode mode, see "When a PIN Is Stolen or Otherwise Compromised" on page 129.

XR PASSCODE Accepted (8202)

A user entered a valid passcode while passing authentication in a remote realm.

Under certain circumstances this message is logged even though the user is not granted access. If there is a heavy load on the remote Authentication Manager, on the network, or on the Authentication Manager in the user's home realm, the Agent Host may time out before receiving the authentication response. Therefore, the Agent Host displays an "Access Denied" message to the user.

You should increase the **Agent Timeout** to the maximum value. For instructions, see "PASSCODE Accepted (1011)" on page 361.

XR Request Timed Out (8224)

An authentication request from another realm has not been resolved and the request is older than the Agent Timeout.

XR Token Disabled, Many Failures (8213)

A user's token was disabled automatically during an attempt to authenticate in a remote realm because either the system detected three consecutive login attempts with a valid tokencode but an invalid PIN or the system detected a user-specified number of consecutive invalid passcodes (regardless of which factor, PIN or tokencode, was incorrect). For a more detailed description of this evasion-of-attack feature, see "When a Token Is Stolen or Otherwise Missing" on page 126.

When a user has more than one token, an invalid login counts against all of the tokens assigned to that user.

XR User Not On Agent Host (8218)

Access is denied and this message is logged when a user visiting from a realm running RSA ACE/Server 3.0 or 3.0.1 attempts to pass authentication on one of your Agent Hosts but is not activated on the corresponding Agent Host record in the user's home realm. The security administrator for the local realm should activate the user on the Agent Host record, if appropriate.

In the case where the user is not activated on the Agent Host and the node secret is not established, this message is logged along with the Node Verification Failed message.

You are not authorized to run this query

You are attempting to run a query for which you do not have the appropriate scoping level. The administrator who compiled and shared the query has restricted the use of this query to administrators above your administrative level. For example, you might be a Group Administrator, and the query could be limited to Site and Realm Administrators.

You have not specified an application to launch

In the Query Wizard's Advanced Parameters dialog box, you selected the radio button "Launch specified application" but left the field empty. Specify a valid pathname to the intended application.

Your RSA ACE/Server has an evaluation license...Your license will expire on *month day year.*

Evaluation licenses have a fixed lifespan, which is usually 90 days from the time they are issued, not from the time they are installed. When the license expires, you cannot restart the Authentication Manager. To bring your system back into compliance, contact RSA Security to obtain a valid permanent license.

For additional information about licensing, see Appendix A, "Licensing."

Your RSA ACE/Server has an expired evaluation license...Your license expired on *month day year*.

Evaluation licenses have a fixed lifespan, which is usually 90 days from the time they are issued, not from the time they are installed. When the license expires, you cannot restart the Authentication Manager. To bring your system back into compliance, contact RSA Security to obtain a valid permanent license.

For additional information about licensing, see Appendix A, "Licensing."

Message ID Numbers

The following tables contain the ID number and text of event, system, and database log messages that share a common format. You can use the ID number to perform SNMP filtering of the messages that are sent to the event log (on Windows) or the system log (on UNIX). For more information, see "Filtering Messages Using SNMP" on page 293.

Cannot Check Delete Dependency for *NAME*

Number	Message
16150	Cannot Check Delete Dependency for AdministrativeRole
15439	Cannot Check Delete Dependency for Administrator
15436	Cannot Check Delete Dependency for Agent Host
15443	Cannot Check Delete Dependency for Agent Host Extension
15434	Cannot Check Delete Dependency for AgentType
15440	Cannot Check Delete Dependency for EnabledGroup
15441	Cannot Check Delete Dependency for EnabledUser
15438	Cannot Check Delete Dependency for Group
15444	Cannot Check Delete Dependency for GroupExtension
15442	Cannot Check Delete Dependency for GroupMember
15449	Cannot Check Delete Dependency for LogMessage
16024	Cannot Check Delete Dependency for Profile
15985	Cannot Check Delete Dependency for Realm
15989	Cannot Check Delete Dependency for RealmEnabledGroup
15987	Cannot Check Delete Dependency for RealmEnabledUser
15991	Cannot Check Delete Dependency for RealmExtension

Number	Message
15437	Cannot Check Delete Dependency for SecondaryNode
15435	Cannot Check Delete Dependency for Site
15448	Cannot Check Delete Dependency for SiteExtension
15431	Cannot Check Delete Dependency for System
15447	Cannot Check Delete Dependency for SystemExtension
16126	Cannot Check Delete Dependency for TaskList
16175	Cannot Check Delete Dependency for TaskListItem
15433	Cannot Check Delete Dependency for Token
15445	Cannot Check Delete Dependency for TokenExtension
15432	Cannot Check Delete Dependency for User
15446	Cannot Check Delete Dependency for UserExtension

Cannot Check Dependency for *NAME*

Number	Message
16151	Cannot Check Dependency for AdministrativeRole
15420	Cannot Check Dependency for Administrator
15417	Cannot Check Dependency for Agent Host
15424	Cannot Check Dependency for Agent Host Extension
15415	Cannot Check Dependency for AgentType
16095	Cannot Check Dependency for AttributeValue
15421	Cannot Check Dependency for EnabledGroup
15422	Cannot Check Dependency for EnabledUser
15419	Cannot Check Dependency for Group
15425	Cannot Check Dependency for GroupExtension
15423	Cannot Check Dependency for GroupMember
15430	Cannot Check Dependency for LogMessage
15822	Cannot Check Dependency for OneTimePassword

Number	Message
16023	Cannot Check Dependency for Profile
15411	Cannot Check Dependency for RealmEnabledGroup
15410	Cannot Check Dependency for RealmEnabledUser
15412	Cannot Check Dependency for RealmExtension
15418	Cannot Check Dependency for SecondaryNode
15416	Cannot Check Dependency for Site
15429	Cannot Check Dependency for SiteExtension
15409	Cannot Check Dependency for System
15428	Cannot Check Dependency for SystemExtension
16176	Cannot Check Dependency for TaskListItem
15414	Cannot Check Dependency for Token
15426	Cannot Check Dependency for TokenExtension
15413	Cannot Check Dependency for User
15427	Cannot Check Dependency for UserExtension
16071	Cannot Check Dependency for Value

Cannot Copy Delta To *NAME* To Delete On Replica

Number	Message
16145	Cannot Copy Delta To AdministrativeRole To Delete On Replica
15744	Cannot Copy Delta To Administrator To Delete On Replica
15748	Cannot Copy Delta To Agent Host Extension To Delete On Replica
15741	Cannot Copy Delta To Agent To Delete On Replica
15739	Cannot Copy Delta To AgentType To Delete On Replica
16044	Cannot Copy Delta To Attribute To Delete On Replica
16091	Cannot Copy Delta To AttributeValue To Delete On Replica
15745	Cannot Copy Delta To EnabledGroup To Delete On Replica
15746	Cannot Copy Delta To EnabledUser To Delete On Replica
15743	Cannot Copy Delta To Group To Delete On Replica

Number	Message
15749	Cannot Copy Delta To GroupExtension To Delete On Replica
15747	Cannot Copy Delta To GroupMember To Delete On Replica
15754	Cannot Copy Delta To LogMessage To Delete On Replica
15757	Cannot Copy Delta To LogMessage To Delete On Replica
15756	Cannot Copy Delta To LogReportFormat To Delete On Replica
15755	Cannot Copy Delta To OneTimePassword To Delete On Replica
16019	Cannot Copy Delta To Profile To Delete On Replica
15846	Cannot Copy Delta To Realm To Delete On Replica
15957	Cannot Copy Delta To RealmEnabledGroup To Delete On Replica
15935	Cannot Copy Delta To RealmEnabledUser To Delete On Replica
15979	Cannot Copy Delta To RealmExtension To Delete On Replica
15868	Cannot Copy Delta To Replica To Delete On Replica
15890	Cannot Copy Delta To SchedJob To Delete On Replica
15742	Cannot Copy Delta To SecondaryNode To Delete On Replica
15740	Cannot Copy Delta To Site To Delete On Replica
15753	Cannot Copy Delta To SiteExtension To Delete On Replica
15913	Cannot Copy Delta To SysLogCriteria To Delete On Replica
15736	Cannot Copy Delta To System To Delete On Replica
15752	Cannot Copy Delta To SystemExtension To Delete On Replica
16121	Cannot Copy Delta To TaskList To Delete On Replica
16170	Cannot Copy Delta To TaskListItem To Delete On Replica
15738	Cannot Copy Delta To Token To Delete On Replica
15750	Cannot Copy Delta To TokenExtension To Delete On Replica
15737	Cannot Copy Delta To User To Delete On Replica
15751	Cannot Copy Delta To UserExtension To Delete On Replica
16067	Cannot Copy Delta To Value To Delete On Replica

Cannot Copy *NAME* Delta

Number	Name
16127	Cannot Copy AdministrativeRole Delta
15284	Cannot Copy Administrator Delta
15281	Cannot copy Agent delta
15288	Cannot copy Agent host extension delta
15279	Cannot copy AgentType delta
16026	Cannot Copy Attribute Delta
16073	Cannot Copy AttributeValue Delta
15285	Cannot Copy EnabledGroup Delta
15286	Cannot Copy EnabledUser Delta
15283	Cannot Copy Group Delta
15289	Cannot Copy GroupExtension Delta
15287	Cannot Copy GroupMember Delta
15294	Cannot Copy LogMessage Delta
15297	Cannot Copy LogMessage Delta
15295	Cannot Copy LogReportFormat Delta
15296	Cannot Copy OneTimePassword Delta
16001	Cannot Copy Profile Delta
15828	Cannot Copy Realm Delta
15939	Cannot Copy RealmEnabledGroup Delta
15917	Cannot Copy RealmEnabledUser Delta
15961	Cannot Copy RealmExtension Delta
15282	Cannot copy SecondaryNode delta
15280	Cannot Copy Site Delta
15293	Cannot Copy SiteExtension Delta
15895	Cannot Copy SysLogCriteria Delta
15276	Cannot Copy System Delta

Number	Name
15850	Cannot Copy System Delta
15872	Cannot Copy System Delta
15292	Cannot Copy SystemExtension Delta
16103	Cannot Copy TaskList Delta
16152	Cannot Copy TaskListItem Delta
15278	Cannot Copy Token Delta
15290	Cannot Copy TokenExtension Delta
15277	Cannot Copy User Delta
15291	Cannot Copy UserExtension Delta
16049	Cannot Copy Value Delta

Cannot Create(Update) *NAME* On Replica

Number	Message
16143	Cannot Create(Update) AdministrativeRole On Replica
15700	Cannot Create(Update) Administrator On Replica
15704	Cannot Create(Update) Agent Host Extension On Replica
15697	Cannot Create(Update) Agent On Replica
15695	Cannot Create(Update) AgentType On Replica
16042	Cannot Create(Update) Attribute On Replica
16089	Cannot Create(Update) AttributeValue On Replica
15701	Cannot Create(Update) EnabledGroup On Replica
15702	Cannot Create(Update) EnabledUser On Replica
15699	Cannot Create(Update) Group On Replica
15705	Cannot Create(Update) GroupExtension On Replica
15703	Cannot Create(Update) GroupMember On Replica
15710	Cannot Create(Update) LogMessage On Replica
15713	Cannot Create(Update) LogMessage On Replica

Number	Message
15712	Cannot Create(Update) LogReportFormat On Replica
15711	Cannot Create(Update) OneTimePassword On Replica
16017	Cannot Create(Update) Profile On Replica
15844	Cannot Create(Update) Realm On Replica
15955	Cannot Create(Update) RealmEnabledGroup On Replica
15933	Cannot Create(Update) RealmEnabledUser On Replica
15977	Cannot Create(Update) RealmExtension On Replica
15866	Cannot Create(Update) Replica On Replica
15888	Cannot Create(Update) SchedJob On Replica
15698	Cannot Create(Update) SecondaryNode On Replica
15696	Cannot Create(Update) Site On Replica
15709	Cannot Create(Update) SiteExtension On Replica
15911	Cannot Create(Update) SysLogCriteria On Replica
15692	Cannot Create(Update) System On Replica
15708	Cannot Create(Update) SystemExtension On Replica
16119	Cannot Create(Update) TaskList On Replica
16168	Cannot Create(Update) TaskListItem On Replica
15694	Cannot Create(Update) Token On Replica
15706	Cannot Create(Update) TokenExtension On Replica
15693	Cannot Create(Update) User On Replica
15707	Cannot Create(Update) UserExtension On Replica
16065	Cannot Create(Update) Value On Replica

Cannot Delete *NAME* Delta

Number	Message
16133	Cannot Delete AdministrativeRole Delta
15480	Cannot Delete Administrator Delta
15477	Cannot Delete Agent Host Delta
15475	Cannot Delete AgentType Delta
16079	Cannot Delete AttributeValue Delta
15481	Cannot Delete EnabledGroup Delta
15482	Cannot Delete EnabledUser Delta
15479	Cannot Delete Group Delta
15485	Cannot Delete GroupExtension Delta
15483	Cannot Delete GroupMember Delta
15490	Cannot Delete LogMessage Delta
15493	Cannot Delete LogMessage Delta
15492	Cannot Delete LogReportFormat Delta
15491	Cannot Delete OneTimePassword Delta
15246	Cannot delete one-time password delta. One-time password record may be locked by another administrator. Primary Authentication Manager attempts to delete at next replication pass.
16007	Cannot Delete Profile Delta
15834	Cannot Delete Realm Delta
15945	Cannot Delete RealmEnabledGroup Delta
15923	Cannot Delete RealmEnabledUser Delta
15967	Cannot Delete RealmExtension Delta
15856	Cannot Delete Replica Delta
15878	Cannot Delete SchedJob Delta
15478	Cannot Delete SecondaryNode Delta
15476	Cannot Delete Site Delta
15489	Cannot Delete SiteExtension Delta

Number	Message
15901	Cannot Delete SysLogCriteria Delta
15472	Cannot Delete System Delta
15488	Cannot Delete SystemExtension Delta
16109	Cannot Delete TaskList Delta
16158	Cannot Delete TaskListItem Delta
15420	Cannot delete token delta. Token record may be locked by another administrator. Primary Authentication Manager attempts to delete at next replication pass.
15474	Cannot delete token delta. Token record may be locked by another administrator. Attempts to delete at next replication pass.
15486	Cannot Delete TokenExtension Delta
15235	Cannot delete user delta. User record may be locked by another administrator. Primary Authentication Manager attempts to delete at next replication pass.
15473	Cannot delete user delta. User record may be locked by another administrator. Attempts to delete at next replication pass.
15487	Cannot Delete UserExtension Delta
16055	Cannot Delete Value Delta

Cannot Delete *NAME* On Replica

Number	Message
16148	Cannot Delete AdministrativeRole On Replica
15810	Cannot Delete Administrator On Replica
15484	Cannot Delete Agent Host Extension Delta
15814	Cannot Delete Agent Host Extension On Replica
15807	Cannot Delete Agent On Replica
15805	Cannot Delete AgentType On Replica
16032	Cannot Delete Attribute Delta
16047	Cannot Delete Attribute On Replica
16094	Cannot Delete AttributeValue On Replica

Number	Message
15811	Cannot Delete EnabledGroup On Replica
15812	Cannot Delete EnabledUser On Replica
15809	Cannot Delete Group On Replica
15815	Cannot Delete GroupExtension On Replica
15813	Cannot Delete GroupMember On Replica
15820	Cannot Delete LogMessage On Replica
15824	Cannot Delete LogMessage On Replica
15823	Cannot Delete LogReportFormat On Replica
15821	Cannot Delete OneTimePassword On Replica
16022	Cannot Delete Profile On Replica
15849	Cannot Delete Realm On Replica
15960	Cannot Delete RealmEnabledGroup On Replica
15938	Cannot Delete RealmEnabledUser On Replica
15982	Cannot Delete RealmExtension On Replica
15871	Cannot Delete Replica On Replica
15893	Cannot Delete SchedJob On Replica
15808	Cannot Delete SecondaryNode On Replica
15806	Cannot Delete Site On Replica
15819	Cannot Delete SiteExtension On Replica
15916	Cannot Delete SysLogCriteria On Replica
15802	Cannot Delete System On Replica
15818	Cannot Delete SystemExtension On Replica
16124	Cannot Delete TaskList On Replica
16173	Cannot Delete TaskListItem On Replic
15804	Cannot Delete Token On Replica
15816	Cannot Delete TokenExtension On Replica
15803	Cannot Delete User On Replica

Number	Message
15817	Cannot Delete UserExtension On Replica
16070	Cannot Delete Value On Replica

Cannot Exclusive Lock *NAME* Delta

Number	Message
16130	Cannot Exclusive Lock AdministrativeRole Delta
15350	Cannot Exclusive Lock Administrator Delta
15347	Cannot Exclusive Lock Agent Delta
15345	Cannot exclusive lock AgentType delta
16029	Cannot Exclusive Lock Attribute Delta
16076	Cannot Exclusive Lock AttributeValue Delta
15351	Cannot Exclusive Lock EnabledGroup Delta
15352	Cannot Exclusive Lock EnabledUser Delta
15349	Cannot Exclusive Lock Group Delta
15355	Cannot Exclusive Lock GroupExtension Delta
15353	Cannot Exclusive Lock GroupMember Delta
15360	Cannot Exclusive Lock LogMessage Delta
15362	Cannot Exclusive Lock LogReportFormat Delta
15363	Cannot Exclusive Lock LogReportFormat Delta
15361	Cannot Exclusive Lock OneTimePassword Delta
16004	Cannot Exclusive Lock Profile Delta
15831	Cannot Exclusive Lock Realm Delta
15942	Cannot Exclusive Lock RealmEnabledGroup Delta
15920	Cannot Exclusive Lock RealmEnabledUser Delta
15964	Cannot Exclusive Lock RealmExtension Delta
15853	Cannot Exclusive Lock Replica Delta
15875	Cannot Exclusive Lock SchedJob Delta

Number	Message
15348	Cannot Exclusive Lock SecondaryNode Delta
15346	Cannot Exclusive Lock Site Delta
15359	Cannot Exclusive Lock SiteExtension Delta
15898	Cannot Exclusive Lock SysLogCriteria Delta
15342	Cannot Exclusive Lock System Delta
15358	Cannot Exclusive Lock SystemExtension Delta
16106	Cannot Exclusive Lock TaskList Delta
16155	Cannot Exclusive Lock TaskListItem Delta
15344	Cannot Exclusive Lock Token Delta
15356	Cannot Exclusive Lock TokenExtension Delta
15343	Cannot Exclusive Lock User Delta
15357	Cannot Exclusive Lock UserExtension Delta
16052	Cannot Exclusive Lock Value Delta
15354	Cannot Exclusively Lock Agent Host Extension Delta

Cannot Fetch *NAME* Delta

Number	Message
16129	Cannot Fetch AdministrativeRole Delta
15328	Cannot Fetch Administrator Delta
15325	Cannot fetch Agent delta
15332	Cannot fetch Agent host extension delta
15323	Cannot fetch AgentType delta
16028	Cannot Fetch Attribute Delta
16075	Cannot Fetch AttributeValue Delta
15329	Cannot Fetch EnabledGroup Delta
15330	Cannot Fetch EnabledUser Delta
15327	Cannot Fetch Group Delta
15333	Cannot Fetch GroupExtension Delta

Number	Message
15331	Cannot Fetch GroupMember Delta
15338	Cannot Fetch LogMessage Delta
15341	Cannot Fetch LogMessage Delta
15340	Cannot Fetch LogReportFormat Delta
15339	Cannot Fetch OneTimePassword Delta
16003	Cannot Fetch Profile Delta
15830	Cannot Fetch Realm Delta
15941	Cannot Fetch RealmEnabledGroup Delta
15919	Cannot Fetch RealmEnabledUser Delta
15963	Cannot Fetch RealmExtension Delta
15852	Cannot Fetch Replica Delta
15874	Cannot Fetch SchedJob Delta
15326	Cannot Fetch SecondaryNode Delta
15324	Cannot Fetch Site Delta
15337	Cannot Fetch SiteExtension Delta
15897	Cannot Fetch SysLogCriteria Delta
15320	Cannot Fetch System Delta
15336	Cannot Fetch SystemExtension Delta
16105	Cannot Fetch TaskList Delta
16154	Cannot Fetch TaskListItem Delta
15322	Cannot Fetch Token Delta
15334	Cannot Fetch TokenExtension Delta
15321	Cannot Fetch User Delta
15335	Cannot Fetch UserExtension Delta
16051	Cannot Fetch Value Delta
15262	Cannot Fetch System Record

Cannot Find *NAME* To Delete On Replica

Number	Message
16146	Cannot Find AdministrativeRole To Delete On Replica
15766	Cannot Find Administrator To Delete On Replica
15770	Cannot Find Agent Host Extension To Delete On Replica
15763	Cannot Find Agent To Delete On Replica
15761	Cannot Find AgentType To Delete On Replica
16045	Cannot Find Attribute To Delete On Replica
16092	Cannot Find AttributeValue To Delete On Replica
15767	Cannot Find EnabledGroup To Delete On Replica
15768	Cannot Find EnabledUser To Delete On Replica
15765	Cannot Find Group To Delete On Replica
15771	Cannot Find GroupExtension To Delete On Replica
15769	Cannot Find GroupMember To Delete On Replica
15776	Cannot Find LogMessage To Delete On Replica
15779	Cannot Find LogMessage To Delete On Replica
15778	Cannot Find LogReportFormat To Delete On Replica
15777	Cannot Find OneTimePassword To Delete On Replica
16020	Cannot Find Profile To Delete On Replica
15847	Cannot Find Realm To Delete On Replica
15958	Cannot Find RealmEnabledGroup To Delete On Replica
15936	Cannot Find RealmEnabledUser To Delete On Replica
15980	Cannot Find RealmExtension To Delete On Replica
15869	Cannot Find Replica To Delete On Replica
15891	Cannot Find SchedJob To Delete On Replica
15764	Cannot Find SecondaryNode To Delete On Replica
15762	Cannot Find Site To Delete On Replica
15775	Cannot Find SiteExtension To Delete On Replica

Number	Message
15914	Cannot Find SysLogCriteria To Delete On Replica
15758	Cannot Find System To Delete On Replica
15774	Cannot Find SystemExtension To Delete On Replica
16122	Cannot Find TaskList To Delete On Replica
16171	Cannot Find TaskListItem To Delete On Replica
15760	Cannot Find Token To Delete On Replica
15772	Cannot Find TokenExtension To Delete On Replica
15759	Cannot Find User To Delete On Replica
15773	Cannot Find UserExtension To Delete On Replica
16068	Cannot Find Value To Delete On Replica

Cannot Find Pending Delete for *NAME*

Number	Message
16149	Cannot Find Pending Delete for AdministrativeRole
15396	Cannot Find Pending Delete for Administrator
15391	Cannot Find Pending Delete for Agent Host
15400	Cannot Find Pending Delete for Agent Host Extension
15389	Cannot Find Pending Delete for AgentType
16048	Cannot Find Pending Delete for Attribute
16096	Cannot Find Pending Delete for AttributeValue
15397	Cannot Find Pending Delete for EnabledGroup
15398	Cannot Find Pending Delete for EnabledUser
15395	Cannot Find Pending Delete for Group
15401	Cannot Find Pending Delete for GroupExtension
15399	Cannot Find Pending Delete for GroupMember
15406	Cannot Find Pending Delete for LogMessage
15408	Cannot Find Pending Delete for LogMessage

Number	Message
15392	Cannot Find Pending Delete for LogReportFormat
15407	Cannot Find Pending Delete for OneTimePassword
16025	Cannot Find Pending Delete for Profile
15984	Cannot Find Pending Delete for Realm
15988	Cannot Find Pending Delete for RealmEnabledGroup
15986	Cannot Find Pending Delete for RealmEnabledUser
15990	Cannot Find Pending Delete for RealmExtension
15983	Cannot Find Pending Delete for Replica
15894	Cannot Find Pending Delete for SchedJob
15394	Cannot Find Pending Delete for SecondaryNode
15390	Cannot Find Pending Delete for Site
15405	Cannot Find Pending Delete for SiteExtension
15393	Cannot Find Pending Delete for SysLogCriteria
15386	Cannot Find Pending Delete for System
15404	Cannot Find Pending Delete for SystemExtension
16125	Cannot Find Pending Delete for TaskList
16174	Cannot Find Pending Delete for TaskListItem
15388	Cannot Find Pending Delete for Token
15402	Cannot Find Pending Delete for TokenExtension
15387	Cannot Find Pending Delete for User
15403	Cannot Find Pending Delete for UserExtension
16072	Cannot Find Pending Delete for Value

Cannot Locate *NAME* To Delete On Replica

Number	Message
16147	Cannot Locate AdministrativeRole Record To Delete On Replica
15788	Cannot Locate Administrator Record To Delete On Replica
15792	Cannot Locate Agent Host Extension Record To Delete On Replica
15785	Cannot Locate Agent Record To Delete On Replica
15783	Cannot Locate AgentType Record To Delete On Replica
16046	Cannot Locate Attribute Record To Delete On Replica
16093	Cannot Locate AttributeValue Record To Delete On Replica
15789	Cannot Locate EnabledGroup Record To Delete On Replica
15790	Cannot Locate EnabledUser Record To Delete On Replica
15787	Cannot Locate Group Record To Delete On Replica
15793	Cannot Locate GroupExtension Record To Delete On Replica
15791	Cannot Locate GroupMember Record To Delete On Replica
15798	Cannot Locate LogMessage Record To Delete On Replica
15800	Cannot Locate LogReportFormat Record To Delete On Replica
15799	Cannot Locate OneTimePassword Record To Delete On Replica
15801	Cannot Locate OneTimePassword Record To Delete On Replica
16021	Cannot Locate Profile Record To Delete On Replica
15848	Cannot Locate Realm Record To Delete On Replica
15959	Cannot Locate RealmEnabledGroup Record To Delete On Replica
15937	Cannot Locate RealmEnabledUser Record To Delete On Replica
15981	Cannot Locate RealmExtension Record To Delete On Replica
15870	Cannot Locate Replica Record To Delete On Replica
15892	Cannot Locate SchedJob Record To Delete On Replica
15786	Cannot Locate SecondaryNode Record To Delete On Replica
15784	Cannot Locate Site Record To Delete On Replica
15797	Cannot Locate SiteExtension Record To Delete On Replica

Number	Message
15915	Cannot Locate SysLogCriteria Record To Delete On Replica
15780	Cannot Locate System Record To Delete On Replica
15796	Cannot Locate SystemExtension Record To Delete On Replica
16123	Cannot Locate TaskList Record To Delete On Replica
16172	Cannot Locate TaskListItem Record To Delete On Replica
15782	Cannot Locate Token Record To Delete On Replica
15794	Cannot Locate TokenExtension Record To Delete On Replica
15781	Cannot Locate User Record To Delete On Replica
15795	Cannot Locate UserExtension Record To Delete On Replica
16069	Cannot Locate Value Record To Delete On Replica

Cannot Match Delta State for *NAME*

Number	Message
16131	Cannot Match Delta State for AdministrativeRole
15372	Cannot Match Delta State for Administrator
15369	Cannot Match Delta State for Agent
15376	Cannot Match Delta State for Agent Host Extension
15367	Cannot Match Delta State for AgentType
16030	Cannot Match Delta State for Attribute
16077	Cannot Match Delta State for AttributeValue
15373	Cannot Match Delta State for EnabledGroup
15374	Cannot Match Delta State for EnabledUser
15371	Cannot Match Delta State for Group
15377	Cannot Match Delta State for GroupExtension
15375	Cannot Match Delta State for GroupMember
15382	Cannot Match Delta State for LogMessage
15385	Cannot Match Delta State for LogMessage

Number	Message
15384	Cannot Match Delta State for LogReportFormat
15383	Cannot Match Delta State for OneTimePassword
16005	Cannot Match Delta State for Profile
15832	Cannot Match Delta State for Realm
15943	Cannot Match Delta State for RealmEnabledGroup
15921	Cannot Match Delta State for RealmEnabledUser
15965	Cannot Match Delta State for RealmExtension
15854	Cannot Match Delta State for Replica
15876	Cannot Match Delta State for Replica
15370	Cannot Match Delta State for SecondaryNode
15368	Cannot Match Delta State for Site
15381	Cannot Match Delta State for SiteExtension
15899	Cannot Match Delta State for SysLogCriteria
15364	Cannot Match Delta State for System
15380	Cannot Match Delta State for SystemExtension
16107	Cannot Match Delta State for TaskList
16156	Cannot Match Delta State for TaskListItem
15366	Cannot Match Delta State for Token
15378	Cannot Match Delta State for TokenExtension
15365	Cannot Match Delta State for User
15379	Cannot Match Delta State for UserExtension
16053	Cannot Match Delta State for Value

Cannot Open *NAME* Delta Cursor

Number	Message
16128	Cannot Open AdministrativeRole Delta Cursor
15306	Cannot Open Administrator Delta Cursor
15303	Cannot open Agent host delta cursor
15310	Cannot open Agent host extension delta cursor
15301	Cannot open AgentType delta cursor
16027	Cannot Open Attribute Delta Cursor
16074	Cannot Open AttributeValue Delta Cursor
15307	Cannot Open EnabledGroup Delta Cursor
15308	Cannot Open EnabledUser Delta Cursor
15305	Cannot Open Group Delta Cursor
15311	Cannot Open GroupExtension Delta Cursor
15309	Cannot Open GroupMember Delta Cursor
15316	Cannot Open LogMessage Delta Cursor
15318	Cannot Open LogReportFormat Delta Cursor
15319	Cannot Open LogReportFormat Delta Cursor
15317	Cannot Open OneTimePassword Delta Cursor
16002	Cannot Open Profile Delta Cursor
15829	Cannot Open Realm Delta Cursor
15940	Cannot Open RealmEnabledGroup Delta Cursor
15918	Cannot Open RealmEnabledUser Delta Cursor
15962	Cannot Open RealmExtension Delta Cursor
15851	Cannot Open Replica Delta Cursor
15873	Cannot Open SchedJob Delta Cursor
15304	Cannot Open SecondaryNode Delta Cursor
15302	Cannot Open Site Delta Cursor
15315	Cannot Open SiteExtension Delta Cursor

Number	Message
15896	Cannot Open SysLogCriteria Delta Cursor
15298	Cannot Open System Delta Cursor
15314	Cannot Open SystemExtension Delta Cursor
16104	Cannot Open TaskList Delta Cursor
16153	Cannot Open TaskListItem Delta Cursor
15300	Cannot Open Token Delta Cursor
15312	Cannot Open TokenExtension Delta Cursor
15299	Cannot Open User Delta Cursor
15313	Cannot Open UserExtension Delta Cursor
16050	Cannot Open Value Delta Cursor

Cannot Read *NAME* Commit Response

Number	Message
16135	Cannot Read AdministrativeRole Commit Response
15524	Cannot Read Administrator Commit Response
15521	Cannot Read Agent Commit Response
15528	Cannot Read Agent Host Extension Commit Response
15519	Cannot Read AgentType Commit Response
16034	Cannot Read Attribute Commit Response
16081	Cannot Read AttributeValue Commit Response
15525	Cannot Read EnabledGroup Commit Response
15526	Cannot Read EnabledUser Commit Response
15523	Cannot Read Group Commit Response
15529	Cannot Read GroupExtension Commit Response
15527	Cannot Read GroupMember Commit Response
15057	Cannot read log filtering configuration.
15534	Cannot Read LogMessage Commit Response

Number	Message
15537	Cannot Read LogMessage Commit Response
15536	Cannot Read LogReportFormat Commit Response
15535	Cannot Read OneTimePassword Commit Response
16009	Cannot Read Profile Commit Response
15836	Cannot Read Realm Commit Response
15947	Cannot Read RealmEnabledGroup Commit Response
15925	Cannot Read RealmEnabledUser Commit Response
15969	Cannot Read RealmExtension Commit Response
15858	Cannot Read Replica Commit Response
15880	Cannot Read SchedJob Commit Response
15522	Cannot Read SecondaryNode Commit Response
15520	Cannot Read Site Commit Response
15533	Cannot Read SiteExtension Commit Response
15056	Cannot read syslog criteria.
15903	Cannot Read SysLogCriteria Commit Response
15516	Cannot Read System Commit Response
15532	Cannot Read SystemExtension Commit Response
16111	Cannot Read TaskList Commit Response
16160	Cannot Read TaskListItem Commit Response
15518	Cannot Read Token Commit Response
15530	Cannot Read TokenExtension Commit Response
15517	Cannot Read User Commit Response
15531	Cannot Read UserExtension Commit Response
16057	Cannot Read Value Commit Response

Cannot Save *NAME* On Replica

Number	Message
16141	Cannot Save AdministrativeRole On Replica
15656	Cannot Save Administrator On Replica
15660	Cannot Save Agent Host Extension On Replica
15653	Cannot Save Agent On Replica
15651	Cannot Save AgentType On Replica
16040	Cannot Save Attribute On Replica
16087	Cannot Save AttributeValue On Replica
15657	Cannot Save EnabledGroup On Replica
15658	Cannot Save EnabledUser On Replica
15655	Cannot Save Group On Replica
15661	Cannot Save GroupExtension On Replica
15659	Cannot Save GroupMember On Replica
15666	Cannot Save LogMessage On Replica
15669	Cannot Save LogMessage On Replica
15668	Cannot Save LogReportFormat On Replica
15667	Cannot Save OneTimePassword On Replica
16015	Cannot Save Profile On Replica
15842	Cannot Save Realm On Replica
15953	Cannot Save RealmEnabledGroup On Replica
15931	Cannot Save RealmEnabledUser On Replica
15975	Cannot Save RealmExtension On Replica
15864	Cannot Save Replica On Replica
15886	Cannot Save SchedJob On Replica
15654	Cannot Save SecondaryNode On Replica
15652	Cannot Save Site On Replica
15665	Cannot Save SiteExtension On Replica

Number	Message
15909	Cannot Save SysLogCriteria On Replica
15647	Cannot Save System On Replica
15664	Cannot Save SystemExtension On Replica
16117	Cannot Save TaskList On Replica
16166	Cannot Save TaskListItem On Replica
15650	Cannot Save Token On Replica
15662	Cannot Save TokenExtension On Replica
15649	Cannot Save User On Replica
15663	Cannot Save UserExtension On Replica
16063	Cannot Save Value On Replica

Cannot Send *NAME* Commit Request to Replica

Number	Message
16134	Cannot Send AdministrativeRole Commit Request to Replica
15502	Cannot Send Administrator Commit Request to Replica
15499	Cannot Send Agent Commit Request to Replica
15506	Cannot Send Agent Host Extension Commit Request to Replica
15497	Cannot Send AgentType Commit Request to Replica
16033	Cannot Send Attribute Commit Request to Replica
16080	Cannot Send AttributeValue Commit Request to Replica
15503	Cannot Send EnabledGroup Commit Request to Replica
15504	Cannot Send EnabledUser Commit Request to Replica
15501	Cannot Send Group Commit Request to Replica
15507	Cannot Send GroupExtension Commit Request to Replica
15505	Cannot Send GroupMember Commit Request to Replica
15512	Cannot Send LogMessage Commit Request to Replica
15515	Cannot Send LogMessage Commit Request to Replica

Number	Message
15514	Cannot Send LogReportFormat Commit Request to Replica
15513	Cannot Send OneTimePassword Commit Request to Replica
16008	Cannot Send Profile Commit Request to Replica
15835	Cannot Send Realm Commit Request to Replica
15946	Cannot Send RealmEnabledGroup Commit Request to Replica
15924	Cannot Send RealmEnabledUser Commit Request to Replica
15968	Cannot Send RealmExtension Commit Request to Replica
15857	Cannot Send Replica Commit Request to Replica
15879	Cannot Send SchedJob Commit Request to Replica
15500	Cannot Send SecondaryNode Commit Request to Replica
15498	Cannot Send Site Commit Request to Replica
15511	Cannot Send SiteExtension Commit Request to Replica
15902	Cannot Send SysLogCriteria Commit Request to Replica
15494	Cannot Send System Commit Request to Replica
15510	Cannot Send SystemExtension Commit Request to Replica
16110	Cannot Send TaskList Commit Request to Replica
16159	Cannot Send TaskListItem Commit Request to Replica
15496	Cannot Send Token Commit Request to Replica
15508	Cannot Send TokenExtension Commit Request to Replica
15495	Cannot Send User Commit Request to Replica
15509	Cannot Send UserExtension Commit Request to Replica

Cannot Send *NAME* to Replica

Number	Message
16132	Cannot Send AdministrativeRole to Replica
15458	Cannot Send Administrator to Replica
15113	Cannot send agent host delta. Token record may be locked by another administrator. Will attempt to send at next replication pass.
15462	Cannot Send Agent Host Extension to Replica
15455	Cannot Send Agent to Replica
15453	Cannot Send AgentType to Replica
16031	Cannot Send Attribute to Replica
16078	Cannot Send AttributeValue to Replica
15459	Cannot Send EnabledGroup to Replica
15460	Cannot Send EnabledUser to Replica
15457	Cannot Send Group to Replica
15463	Cannot Send GroupExtension to Replica
15461	Cannot Send GroupMember to Replica
15468	Cannot Send LogMessage to Replica
15471	Cannot Send LogMessage to Replica
15470	Cannot Send LogReportFormat to Replica
15469	Cannot Send OneTimePassword to Replica
16006	Cannot Send Profile to Replica
15833	Cannot Send Realm to Replica
15944	Cannot Send RealmEnabledGroup to Replica
15922	Cannot Send RealmEnabledUser to Replica
15966	Cannot Send RealmExtension to Replica
15855	Cannot Send Replica to Replica
15877	Cannot Send SchedJob to Replica
15456	Cannot Send SecondaryNode to Replica

Number	Message
15454	Cannot Send Site to Replica
15467	Cannot Send SiteExtension to Replica
15900	Cannot Send SysLogCriteria to Replica
15265	Cannot Send System To Primary
15450	Cannot Send System to Replica
15466	Cannot Send SystemExtension to Replica
16108	Cannot Send TaskList to Replica
16157	Cannot Send TaskListItem to Replica
15452	Cannot Send Token to Replica
15464	Cannot Send TokenExtension to Replica
15451	Cannot Send User to Replica
15465	Cannot Send UserExtension to Replica
16054	Cannot Send Value to Replica

Cannot Update *NAME* On Replica

Number	Message
16144	Cannot Update AdministrativeRole On Replica
15722	Cannot Update Administrator On Replica
15726	Cannot Update Agent Host Extension On Replica
15719	Cannot Update Agent On Replica
15717	Cannot Update AgentType On Replica
16043	Cannot Update Attribute On Replica
16090	Cannot Update AttributeValue On Replica
15723	Cannot Update EnabledGroup On Replica
15724	Cannot Update EnabledUser On Replica
15721	Cannot Update Group On Replica
15727	Cannot Update GroupExtension On Replica

Number	Message
15725	Cannot Update GroupMember On Replica
15732	Cannot Update LogMessage On Replica
15735	Cannot Update LogMessage On Replica
15734	Cannot Update LogReportFormat On Replica
15733	Cannot Update OneTimePassword On Replica
16018	Cannot Update Profile On Replica
15845	Cannot Update Realm On Replica
15956	Cannot Update RealmEnabledGroup On Replica
15934	Cannot Update RealmEnabledUser On Replica
15978	Cannot Update RealmExtension On Replica
15867	Cannot Update Replica On Replica
15889	Cannot Update SchedJob On Replica
15720	Cannot Update SecondaryNode On Replica
15718	Cannot Update Site On Replica
15731	Cannot Update SiteExtension On Replica
15912	Cannot Update SysLogCriteria On Replica
15714	Cannot Update System On Replica
15730	Cannot Update SystemExtension On Replica
16120	Cannot Update TaskList On Replica
16169	Cannot Update TaskListItem On Replica
15716	Cannot Update Token On Replica
15728	Cannot Update TokenExtension On Replica
15715	Cannot Update User On Replica
15729	Cannot Update UserExtension On Replica
16066	Cannot Update Value On Replica

Cannot Update(Create) *NAME* On Replica

Number	Message
16140	Cannot Update(Create) AdministrativeRole On Replica
15634	Cannot Update(Create) Administrator On Replica
15638	Cannot Update(Create) Agent Host Extension On Replica
15631	Cannot Update(Create) Agent On Replica
15629	Cannot Update(Create) AgentType On Replica
16039	Cannot Update(Create) Attribute On Replica
16086	Cannot Update(Create) AttributeValue On Replica
15635	Cannot Update(Create) EnabledGroup On Replica
15636	Cannot Update(Create) EnabledUser On Replica
15633	Cannot Update(Create) Group On Replica
15639	Cannot Update(Create) GroupExtension On Replica
15637	Cannot Update(Create) GroupMember On Replica
15644	Cannot Update(Create) LogMessage On Replica
15648	Cannot Update(Create) LogMessage On Replica
15646	Cannot Update(Create) LogReportFormat On Replica
15645	Cannot Update(Create) OneTimePassword On Replica
16014	Cannot Update(Create) Profile On Replica
15841	Cannot Update(Create) Realm On Replica
15952	Cannot Update(Create) RealmEnabledGroup On Replica
15930	Cannot Update(Create) RealmEnabledUser On Replica
15974	Cannot Update(Create) RealmExtension On Replica
15863	Cannot Update(Create) Replica On Replica
15885	Cannot Update(Create) SchedJob On Replica
15632	Cannot Update(Create) SecondaryNode On Replica
15630	Cannot Update(Create) Site On Replica
15643	Cannot Update(Create) SiteExtension On Replica

Number	Message
15908	Cannot Update(Create) SysLogCriteria On Replica
15626	Cannot Update(Create) System On Replica
15642	Cannot Update(Create) SystemExtension On Replica
16116	Cannot Update(Create) TaskList On Replica
16165	Cannot Update(Create) TaskListItem On Replica
15628	Cannot Update(Create) Token On Replica
15640	Cannot Update(Create) TokenExtension On Replica
15627	Cannot Update(Create) User On Replica
15641	Cannot Update(Create) UserExtension On Replica
16062	Cannot Update(Create) Value On Replica

Database Inconsistency. Replica Rejecting *NAME* Delta

Number	Message
16137	Database Inconsistency: Replica Rejecting AdministrativeRole Delta
16036	Database Inconsistency: Replica Rejecting Attribute Delta
16083	Database Inconsistency: Replica Rejecting AttributeValue Delta
16011	Database Inconsistency: Replica Rejecting Profile Delta
15838	Database Inconsistency: Replica Rejecting Realm Delta
15949	Database Inconsistency: Replica Rejecting RealmEnabledGroup Delta
15927	Database Inconsistency: Replica Rejecting RealmEnabledUser Delta
15971	Database Inconsistency: Replica Rejecting RealmExtension Delta
15860	Database Inconsistency: Replica Rejecting Replica Delta
15905	Database Inconsistency: Replica Rejecting SysLogCriteria Delta
16113	Database Inconsistency: Replica Rejecting TaskList Delta
16162	Database Inconsistency: Replica Rejecting TaskListItem Delta
16059	Database Inconsistency: Replica Rejecting Value Delta
15882	Database Inconsistency: SchedJob Rejecting SchedJob Delta

Number	Message
15568	Database Inconsistency: Replica Rejecting Administrator Delta
15565	Database Inconsistency: Replica Rejecting Agent Delta
15572	Database Inconsistency: Replica Rejecting Agent Host Extension Delta
15563	Database Inconsistency: Replica Rejecting AgentType Delta
15569	Database Inconsistency: Replica Rejecting EnabledGroup Delta
15570	Database Inconsistency: Replica Rejecting EnabledUser Delta
15567	Database Inconsistency: Replica Rejecting Group Delta
15573	Database Inconsistency: Replica Rejecting GroupExtension Delta
15571	Database Inconsistency: Replica Rejecting GroupMember Delta
15578	Database Inconsistency: Replica Rejecting LogMessage Delta
15581	Database Inconsistency: Replica Rejecting LogMessage Delta
15580	Database Inconsistency: Replica Rejecting LogReportFormat Delta
15579	Database Inconsistency: Replica Rejecting OneTimePassword Delta
15566	Database Inconsistency: Replica Rejecting SecondaryNode Delta
15564	Database Inconsistency: Replica Rejecting Site Delta
15577	Database Inconsistency: Replica Rejecting SiteExtension Delta
15560	Database Inconsistency: Replica Rejecting System Delta
15576	Database Inconsistency: Replica Rejecting SystemExtension Delta
15562	Database Inconsistency: Replica Rejecting Token Delta
15574	Database Inconsistency: Replica Rejecting TokenExtension Delta
15561	Database Inconsistency: Replica Rejecting User Delta
15575	Database Inconsistency: Replica Rejecting UserExtension Delta

Error deleting delta *NAME*

Number	Message
2264	Error deleting delta admin role
2252	Error deleting delta ALM
2240	Error deleting delta ATTR
2242	Error deleting delta AV
2220	Error deleting delta CRX
2239	Error deleting delta PROF
2219	Error deleting delta realm
2222	Error deleting delta REG
2221	Error deleting delta REU
2241	Error deleting delta VAL

Error deleting *NAME*

Number	Message
2238	Error deleting AV
2026	Error deleting admin
2263	Error deleting admin role
2029	Error deleting agent host
2027	Error deleting agent host extnsn
2028	Error deleting agent host type
2251	Error deleting ALM
2236	Error deleting attribute
2208	Error deleting CRX
2030	Error deleting delta admin
2036	Error deleting delta agent host
2031	Error deleting delta CCX
2032	Error deleting delta CGX
2049	Error deleting delta csite-x

Number	Message
2033	Error deleting delta CTX
2034	Error deleting delta CType
2035	Error deleting delta CUX
2037	Error deleting delta EG
2038	Error deleting delta EU
2039	Error deleting delta GM
2040	Error deleting delta group
2042	Error deleting delta logmsg
2041	Error deleting delta LRF
2043	Error deleting delta node
2044	Error deleting delta site
2198	Error deleting delta syslog CR
2046	Error deleting delta system
2045	Error deleting delta sys-x
2047	Error deleting delta token
2048	Error deleting delta user
2050	Error deleting enabled group
2051	Error deleting enabled user
2054	Error deleting group
2052	Error deleting group extnsn
2053	Error deleting group member
2055	Error deleting log entry
2056	Error deleting log message
2057	Error deleting log rpt format8
2058	Error deleting node
2192	Error deleting one time pswrd
2235	Error deleting profile

Number	Message
2203	Error deleting realm
2059	Error deleting record on replica
2218	Error deleting REG
2275	Error deleting replica
2213	Error deleting REU
2061	Error deleting site
2060	Error deleting site extnsn
2197	Error deleting syslog CR
2062	Error deleting system extnsn
2063	Error deleting system record
2269	Error deleting task item
2257	Error deleting tasklist
2065	Error deleting token
2064	Error deleting token extnsn
2067	Error deleting user
2066	Error deleting user extnsn
2237	Error deleting value

Error Transferring *NAME*

Number	Message
2199	Error transferring realm
2109	Error transfer replica tokens
2091	Error transferring admin
2259	Error transferring admin role
2094	Error transferring agent host
2092	Error transferring agent host ext
2093	Error transferring agent type
2247	Error transferring ALM

Number	Message
2244	Error transferring ATTR
2246	Error transferring AV
2204	Error transferring CRX
2095	Error transferring enabled group
2096	Error transferring enabled user
2099	Error transferring group
2097	Error transferring group extnsn
2098	Error transferring group member
2327	Error transferring job record
2100	Error transferring log message
2101	Error transferring log rpt format
2102	Error transferring node
2243	Error transferring PROF
2214	Error transferring REG
2276	Error transferring replica
2105	Error transferring replica agents
2107	Error transferring replica logs
2106	Error transferring replica logs 2
2190	Error transferring replica OTPs
2108	Error transferring replica system
2277	Error transferring replica users
2209	Error transferring REU
2104	Error transferring site
2103	Error transferring site extnsn
2193	Error transferring syslog CR
2110	Error transferring system extnsn
2111	Error transferring system record
2265	Error transferring task item
2253	Error transferring tasklist

Number	Message
2113	Error transferring token
2112	Error transferring token extnsn
2115	Error transferring user
2114	Error transferring user extnsn
2245	Error transferring VAL

Failed to Lock *recordtype* Record

Number	Message
2068	Failed to lock agent host record
2069	Failed to lock system record
2070	Failed to lock token record

NAME Already Exists On Replica

Number	Message
16139	AdministrativeRole Already Exists On Replica
15612	Administrator Already Exists On Replica
15609	Agent Already Exists On Replica
15616	Agent Host Extension Already Exists On Replica
15607	AgentType Already Exists On Replica
16038	Attribute Already Exists On Replica
16085	AttributeValue Already Exists On Replica
15613	EnabledGroup Already Exists On Replica
15614	EnabledUser Already Exists On Replica
15611	Group Already Exists On Replica
15617	GroupExtension Already Exists On Replica
15615	GroupMember Already Exists On Replica
15622	LogMessage Already Exists On Replica
15624	LogReportFormat Already Exists On Replica

Number	Message
15625	LogReportFormat Already Exists On Replica
15623	OneTimePassword Already Exists On Replica
16013	Profile Already Exists On Replica
15840	Realm Already Exists On Replica
15951	RealmEnabledGroup Already Exists On Replica
15929	RealmEnabledUser Already Exists On Replica
15973	RealmExtension Already Exists On Replica
15862	Replica Already Exists On Replica
15884	SchedJob Already Exists On Replica
15610	SecondaryNode Already Exists On Replica
15608	Site Already Exists On Replica
15621	SiteExtension Already Exists On Replica
15907	SysLogCriteria Already Exists On Replica
15604	System Already Exists On Replica
15620	SystemExtension Already Exists On Replica
16115	TaskList Already Exists On Replica
16164	TaskListItem Already Exists On Replica
15606	Token Already Exists On Replica
15618	TokenExtension Already Exists On Replica
15605	User Already Exists On Replica
15619	UserExtension Already Exists On Replica
16061	Value Already Exists On Replica

Replica Rejecting *NAME* Delta

Number	Message
2126	Replica rejecting admin create
2127	Replica rejecting admin delete
2128	Replica rejecting admin modify
2248	Replica rejecting ALM create
2249	Replica rejecting ALM delete
2250	Replica rejecting ALM modify
2232	Replica rejecting AV create
2233	Replica rejecting AV delete
2234	Replica rejecting AV modify
2129	Replica rejecting CCX create
2130	Replica rejecting CCX delete
2131	Replica rejecting CCX modify
2132	Replica rejecting CGX create
2133	Replica rejecting CGX delete
2134	Replica rejecting CGX modify
2205	Replica rejecting CRX create
2206	Replica rejecting CRX delete
2207	Replica rejecting CRX modify
2135	Replica rejecting CSiteX create
2136	Replica rejecting CSiteX delete
2137	Replica rejecting CSiteX modify
2138	Replica rejecting CSysX create
2139	Replica rejecting CSysX delete
2140	Replica rejecting CSysX modify
2141	Replica rejecting CTX create
2142	Replica rejecting CTX delete

Number	Message
2143	Replica rejecting CTX modify
2144	Replica rejecting CType create
2145	Replica rejecting CType delete
2146	Replica rejecting CType modify
2147	Replica rejecting CUX create
2148	Replica rejecting CUX delete
2149	Replica rejecting CUX modify
2153	Replica rejecting E group create
2154	Replica rejecting E group delete
2155	Replica rejecting E group modify
2156	Replica rejecting E user create
2157	Replica rejecting E user delete
2158	Replica rejecting E user modify
2159	Replica rejecting group create
2160	Replica rejecting group delete
2161	Replica rejecting group modify
2162	Replica rejecting grp mem create
2163	Replica rejecting grp mem delete
2164	Replica rejecting grp mem modify
2168	Replica rejecting log msg create
2169	Replica rejecting log msg delete
2170	Replica rejecting log msg modify
2165	Replica rejecting LRF create
2166	Replica rejecting LRF delete
2167	Replica rejecting LRF modify
2171	Replica rejecting node create
2172	Replica rejecting node delete

Number	Message
2173	Replica rejecting node modify
2187	Replica rejecting OTP create
2188	Replica rejecting OTP delete
2189	Replica rejecting OTP modify
2223	Replica rejecting profile create
2224	Replica rejecting profile delete
2225	Replica rejecting profile modify
2200	Replica rejecting realm create
2201	Replica rejecting realm delete
2202	Replica rejecting realm modify
2215	Replica rejecting REG create
2216	Replica rejecting REG delete
2217	Replica rejecting REG modify
2271	Replica rejecting replica create
2272	Replica rejecting replica delete
2273	Replica rejecting replica modify
2210	Replica rejecting REU create
2211	Replica rejecting REU delete
2212	Replica rejecting REU modify
2323	Replica rejecting schedjob create
2324	Replica rejecting schedjob delete
2325	Replica rejecting schedjob modify
2174	Replica rejecting site create
2175	Replica rejecting site delete
2176	Replica rejecting site modify
2177	Replica rejecting system create
2178	Replica rejecting system delete

Number	Message
2179	Replica rejecting system modify
2254	Replica rejecting tasklist create
2255	Replica rejecting tasklist delete
2256	Replica rejecting tasklist modify
2180	Replica rejecting token create
2181	Replica rejecting token delete
2182	Replica rejecting token modify
2183	Replica rejecting user create
2184	Replica rejecting user delete
2185	Replica rejecting user modify
2229	Replica rejecting value create
2230	Replica rejecting value delete
2231	Replica rejecting value modify

Unexpected Packet. *NAME* Commit Response Expected

Number	Message
16138	Unexpected Packet. AdministrativeRole Commit Response Expected
15590	Unexpected Packet. Administrator Commit Response Expected
15587	Unexpected Packet. Agent Commit Response Expected
15594	Unexpected Packet. Agent Host Extension Commit Response Expected
15585	Unexpected Packet. AgentType Commit Response Expected
16037	Unexpected Packet. Attribute Commit Response Expected
16084	Unexpected Packet. AttributeValue Commit Response Expected
15591	Unexpected Packet. EnabledGroup Commit Response Expected
15592	Unexpected Packet. EnabledUser Commit Response Expected
15589	Unexpected Packet. Group Commit Response Expected
15595	Unexpected Packet. GroupExtension Commit Response Expected

Number	Message
15593	Unexpected Packet. GroupMember Commit Response Expected
15600	Unexpected Packet. LogMessage Commit Response Expected
15603	Unexpected Packet. LogMessage Commit Response Expected
15602	Unexpected Packet. LogReportFormat Commit Response Expected
15601	Unexpected Packet. OneTimePassword Commit Response Expected
16012	Unexpected Packet. Profile Commit Response Expected
15839	Unexpected Packet. Realm Commit Response Expected
15950	Unexpected Packet. RealmEnabledGroup Commit Response Expected
15928	Unexpected Packet. RealmEnabledUser Commit Response Expected
15972	Unexpected Packet. RealmExtension Commit Response Expected
15861	Unexpected Packet. Replica Commit Response Expected
15883	Unexpected Packet. SchedJob Commit Response Expected
15588	Unexpected Packet. SecondaryNode Commit Response Expected
15586	Unexpected Packet. Site Commit Response Expected
15599	Unexpected Packet. SiteExtension Commit Response Expected
15906	Unexpected Packet. SysLogCriteria Commit Response Expected
15582	Unexpected Packet. System Commit Response Expected
15598	Unexpected Packet. SystemExtension Commit Response Expected
16114	Unexpected Packet. TaskList Commit Response Expected
16163	Unexpected Packet. TaskListItem Commit Response Expected
15584	Unexpected Packet. Token Commit Response Expected
15596	Unexpected Packet. TokenExtension Commit Response Expected
15583	Unexpected Packet. User Commit Response Expected
15597	Unexpected Packet. UserExtension Commit Response Expected
16060	Unexpected Packet. Value Commit Response Expected

Glossary

activated

An activated user on a particular Agent Host (either directly or through membership in a group) can be authenticated on the Agent Host if the user's token is assigned and enabled. This term does not apply to open Agent Hosts.

added

A token record is added to the database during the initial installation procedures or, later, with the Import Token option on the Token menu. After the record is added, the token must be assigned to a user before the user can use the token for authentication.

assigned

An assigned token record is linked to the record of a particular user on the system. To be used for authentication on an Agent Host, a token must be assigned and enabled, and, unless the Agent Host is an open Agent Host, the assigned user must be activated on the Agent Host.

Change Required mode

The first time a user authenticates with a user password, the password is put in Change Required mode, which is similar to New PIN mode. The user must create a new password before being authenticated.

deactivated

A deactivated group or user can no longer be authenticated on a particular (restricted) Agent Host. This term does not apply to open Agent Hosts.

deleted

A deleted record has been removed permanently from the RSA Authentication Manager database.

deployed

(When used to describe an RSA SecurID Software Token.) The software token has been issued to one user or to a selected category of users. When a software token is deployed, a token record file is created.

disabled

A disabled token can be assigned to a user, but it cannot be used for authentication. A token can become disabled by administrator action (by clearing the **Enabled** checkbox in the Edit Token dialog box) or automatically, after a set number of guessed PINs or tokencodes have been tried.

enabled

An assigned token is enabled unless an administrator or the system has disabled it. An unassigned token does not have an enabled/disabled status. To be used for authentication on an Agent Host, a token must be assigned and enabled, and, unless the Agent Host is an open Agent Host, its assigned user must be activated on the Agent Host.

expired

An expired token has reached the end of its preprogrammed life span and no longer displays codes. A token's unmodifiable shutdown date is stored in the token record **Click Token > Edit Token** to display it.

issued

(When used to describe an RSA SecurID Software Token.) The software token has been enabled and assigned to one user or a selected category of users.

New PIN mode

An administrator puts a token into New PIN mode when its PIN has been compromised (that is, learned by someone other than the authorized user) or when the authorized user has forgotten the PIN. If the administrator clears the PIN, the old PIN can no longer be used for authentication, and the next authentication attempt with the token initiates the New PIN procedure. If the administrator does not clear the PIN, the old PIN can be used one more time after which the New PIN dialog begins.

Next Tokencode mode

The RSA Authentication Manager puts a token into Next Tokencode mode if the token has drifted out of synch with the Authentication Manager's system clock or if there has been a series of unsuccessful authentication attempts. Requiring two consecutive tokencodes ensures that the user actually has possession of the token.

offline authentication

An option that requires users to enter a valid RSA SecurID passcode to gain access to their computers, even when those computers are disconnected from the domain, or a connection to the RSA Authentication Manager is temporarily unavailable.

open Agent Host

An Agent Host is "open" if users are not required to be directly activated on the Agent Host or to be members of a group activated on the Agent Host. Any user registered in your RSA Authentication Manager database can be authenticated on an open Agent Host.

PIN

A user's secret, memorized personal identification number. A PIN is one of the factors in the RSA SecurID authentication system.

replaced tokens

Replaced tokens are assigned tokens that are being replaced by replacement tokens. After the replacement tokens have been used in successful authentications, the replaced tokens are automatically unassigned and disabled.

replacement tokens

Replacement tokens are unassigned tokens issued to replace assigned tokens (for example, assigned tokens that are about to expire).

restricted Agent Host

A restricted Agent Host is not open to all locally known users. Users must be activated on a restricted Agent Host before they can authenticate on the Agent Host.

revoked

A revoked software token is a previously issued software token that is unassigned from a user or a selected category of users, and is automatically disabled in the RSA Authentication Manager database.

software token

A software token is a software-based, one-time password authentication method of protecting network resources, typically used for remote access.

temporary password

A password that you can assign to temporarily replace a Lost token.

token

Usually refers to a physical device, such as an RSA SecurID standard card, key fob, or PINPad, that displays a tokencode. User passwords, RSA SecurID smart cards, and software tokens are token types with individual characteristics. The token is one of the factors in the RSA SecurID authentication system. The other factor is the user's PIN.

tokencode

The code displayed by an RSA SecurID token. The tokencode and the PIN make up the RSA SecurID authentication system.

token record

Each token on the system has a corresponding record in the RSA Authentication Manager database that contains information about the token.

unassigned

An unassigned token has no associated user. Unassigning a token breaks the link between the token record and the user record. When an administrator unassigns a token, the PIN is cleared, and the **Last Login Date** field displays the last date the token was used for authentication. The **Last Login Date**, which is meaningless for a token that has never been used for authentication, is set to 1/1/1986.

user password

A user password is an administrative token that allows a user to enter a password at the passcode prompt during authentication.

Index