RSA Authentication Manager 6.1 for UNIX Installation Guide

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 Security Notice

First printing: September 2005

Contents

Preface

This manual provides instructions for installing RSA Authentication Manager 6.1 for UNIX.

Audience

This manual is intended for UNIX security system administrators. The person who installs RSA Authentication Manager must have a working knowledge of UNIX, your Authentication Manager platform, the operating system version, and system peripherals.

Directory Names

The following table shows the convention used in this guide for referring to certain directory names.

Term Used in Guide	Definition	Actual Directory Path
ACEDATA	RSA Authentication Manager data directory	**\RSA Authentication Manager\data**
ACEDOC	RSA Authentication Manager document directory	**\RSA Authentication Manager\doc**
ACEPROG	RSA Authentication Manager executables directory	**\RSA Authentication Manager\prog**

Documentation

The RSA Authentication Manager software for UNIX, for Windows 2000 and Windows 2003, is provided on a single CD, which also includes:

- Help for RSA Authentication Manager Remote Administration on Windows 2000 and Windows 2003
- Printable documentation files in PDF format for UNIX, Windows 2000, and Windows 2003

For information about all RSA Authentication Manager resources available to you, see the printed *Getting Started* book in the RSA Authentication Manager package.

Documentation Provided as PDF Files

You can access PDF files from either:

- **auth.mgrdoc** on the RSA Authentication Manager CD.
- The local **RSA Security\RSA Authentication Manager\doc** directory on your hard drive, provided you opted to install the documentation as part of the installation process.

Note: RSA Security provides an authentication instructions template in a Microsoft Word (.doc) file that you can customize and provide to your users. If you do not have access to Microsoft Word, you can distribute the PDF version of the instructions.

If you are deploying the RSA SecurID Authenticator SID800, for end-user instructions 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 security reasons, RSA Security recommends that you obtain the latest version of Adobe Reader for any platform at **www.adobe.com**.

How RSA Authentication Manager Documentation Is Organized

During installation, you have the option of copying the documentation PDF files from the CD onto your hard drive. In this case, the documentation is copied into the ***ACEDOC*** subdirectory of the RSA Authentication Manager installation directory. If you decide not to install the documentation, you can always access it from the **aceservdoc** directory at the top-level of the RSA Authentication Manager CD.

Help

RSA Authentication Manager 6.1 includes an extensive Help system that is available when you use remote administration on a Windows system in order to administer RSA Authentication Manager running on a UNIX system. You can access the Help by either:

- Clicking the **Help** buttons in individual dialog boxes
- Selecting **Help for Database Administration** on the Help menu of the Database Administration application

Online Distribution of RSA Authentication Manager 6.1

Customers have the option of downloading RSA Authentication Manager 6.1 as a zip file. When unzipped, the file contains the same directory layout and contents as the RSA Authentication Manager 6.1 software CD.

In the documentation, where appropriate, substitute the term *online distribution file* for *software CD*. In procedures, you may need to adjust the details of some of the steps.

The Welcome Kit and license media are in your original RSA Authentication Manager package.

Getting Support and Service

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

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

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

Before You Call for Customer Support

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

Please have the following information available when you call:

- Your RSA Security Customer/License ID. You can find this number on the license distribution medium or by typing ‘sdinfo’ on any UNIX platform.
- 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.
- Whether you are running a name resolution service (for example, DNS).

1 RSA Authentication Manager Requirements

Read this chapter to perform a thorough review of the system or systems onto which you will install RSA Authentication Manager 6.1 software. Your system must meet the software, hardware, and configuration requirements listed in this chapter.

If your system does not conform to each requirement, contact your RSA Security sales representative or local distributor.

Licensing Options

RSA Authentication Manager enforces the Base license and the Advanced license during installation and in the normal course of daily operation and administration. Both license types are permanent.

Base License

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

- With as many users in the RSA Authentication Manager database as specified by the user tier that was purchased.
- One Primary and one Replica Authentication Manager in one realm.

Advanced License

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

- 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.

For detailed information about licenses and active users, see the *Administrator's Guide*.

Installation Requirements

This section lists the requirements for new and upgrade installations. Check each item in this section only if your system meets the *minimum* requirement stated. If you are unable to mark off each item, do not proceed with installing the RSA Authentication Manager software.

Supported Platforms and Hardware

The RSA ACE/Server must be running one of the UNIX operating system versions listed below. If you install RSA Authentication Manager 6.1 software on a platform that is not listed here, RSA Security cannot provide support for it.

- ❑ HP-UX 11i running on PA-RISC 2.x processors
- ❑ IBM AIX 5L v 5.2 on PowerPC and RISC/6000 processors
- ❑ Solaris 9 on UltraSparc processors
- ❑ Red Hat Enterprise Linux 3.0

Use the **uname -a** command to view platform information.

System Patches

You must install the following system patches:

- ❑ HP-UX 11i: **BUNDLE 11i** (B.11.11.0306.1) and **GOLDBASE11i** (B.11.11.0412.5)
- ❑ IBM AIX 5L v 5.2: APAR IY 44173
- ❑ Red Hat Enterprise Linux 3.0: Legacy Software Development—available through Red Hat Package Manager on the Red Hat Enterprise Linux 3.0 CD

High Availability

RSA Authentication Manager 6.1 is certified for High Availability on Solaris 9 Veritas Cluster Server.

Disk Space

Reserve the following required space before beginning the installation process. If you do not have enough disk space on your system, the installation process exits. Do not attempt to circumvent the disk space requirements by mounting the **/ace** directory or the **/ace_tmp** directory as a separate file system.

- ❑ 400 MB of disk space is required for installation of RSA Authentication Manager files.
- ❑ 128 MB of physical memory per processor plus 1 MB per 1,000 users
- ❑ 1 MB of free disk space per 1,000 users must be reserved for RSA Authentication Manager database growth.
- ❑ 1 GB reserved for log database growth.
- ❑ A swap file that is two times the size of the amount of physical memory is required.

Drives

- You must have a CD drive on which you can mount the RSA Authentication Manager software CD and license CD. An acceptable alternative is a local CD drive on a workstation that can be accessed using NFS facilities.

  Note: If you downloaded the application, you do not need a CD drive. When unzipped, the downloaded file contains the same directory layout and contents as the RSA Authentication Manager 6.1 software CD.

  The CD drive on which the RSA Authentication Manager software distribution media is mounted must be compatible with the workstation that reads from it, and the default permissions of the drive must be intact.

Hostnames

- If you are using a name server, such as NIS or DNS, the primary hostname (also known as its "boot name") of the Primary and Replicas must meet the following requirements:
  - The name must be the first name in any list of aliases for the machine, and the entry for the machine must include the IP address followed by the fully-qualified name.
  - On a multi-homed machine, the name must resolve to the Primary Network Interface card.

Kernel Configuration

- Verify that your system kernel configuration values are set at or above the minimum values listed in Appendix B, "Modifying Kernel Parameters." Before modifying any kernel setting, make sure that you have accounted for all applications running on the system. If any setting is too low, modify the kernel configuration. Parameter names are case sensitive, so be sure you specify or search for them *exactly* as they appear in the tables.

Important Installation Guidelines

- RSA Security recommends that the Primary and Replica machines be used as RSA Authentication Managers only.
- Make sure that the Authentication Manager machines are located in a secure area and can be accessed by trusted personnel only.
- The name of each Authentication Manager machine must be a fully-qualified computer name on the network.
- Do not run multiple RSA Authentication Managers on the same machine.
- Do not install RSA Authentication Manager software on a network drive.
- Do not install RSA Authentication Manager software into a directory with a pathname that includes blank spaces. Blank spaces cause the installation to fail.
- Make backup copies of the files before beginning an installation. Store the original license files, the token seed record files, the RSA Authentication Manager 6.1 CD, and any copies you make in a secure place.

Merging Multiple Realms

To merge databases from multiple realms into one 6.1 realm, you need to:

1. Upgrade one realm to RSA Authentication Manager 6.1.
2. Dump the other databases and merge them into the 6.1 database using the dump and load utilities **sddump** and **sdload**.

For more information, see Appendix D, "Database Utilities."

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 must always be correct in relation to UTC. If the time settings drift by more than a minute, authentication will fail.

Make sure that the time on the Primary 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: To ensure that time synchronization works correctly, the RSA Authentication Manager processes on the Primary and the Replicas must be running with root privileges, so that time can be reset if required.

Pre-Installation Checklist

RSA Security recommends that you review the *Readme* (**authmgr_readme.pdf**) before installing the RSA Authentication Manager software. The *Readme* contains important configuration and installation information for RSA Authentication Manager 6.1. It also contains information about problems in the software found too late to be included in the standard documentation.

Before you begin, use the following checklists to verify that you have all the hardware, software, and information you need to install RSA Authentication Manager software.

You must have the following materials:

- ❑ The RSA Authentication Manager CD or download.
- ❑ The license CD.

  Important: Make a backup copy of the license file before beginning any installation procedures and store the original file, the token seed record file, the RSA Authentication Manager 6.1 CD, and any copies you make in a secure place. In addition, you must make backup copies of your license *after* you install the RSA Authentication Manager software. During the installation, the license file is modified. Therefore, if your license in the ***ACEDATA*** directory is ever lost or corrupted, you cannot regain access using the original license files. The only way to regain access is with the modified license files.

- ❑ A token record file, if you received a shipment of tokens.

  Note: Each shipment of RSA SecurID tokens contains a DOS file containing token seed records in one or more ASCII or XML files. The token record file is not shipped in the RSA Authentication Manager package.

You must have the following:

- ❑ A machine that meets all the hardware, disk space, memory, and platform requirements described in this chapter.
- ❑ Administrator (root) privileges on the machine.

  The installation and configuration tasks that are performed using the **sdsetup** utility require root privileges.
- ❑ The names and IP addresses of the Replicas you plan to install.
- ❑ You need to specify the Replicas after Primary installation. You can add Replicas (up to 10 total, depending on the type of license you have) using the Replica Management utility (**sdsetup -repmgmt**). The exact commands you need to use are described in the corresponding chapters of this book. For a full description of the Replica Management utility, see the *Administrator's Guide*.
- ❑ Methods of delivering the Replica Package to the Replica.

  There are two methods to deliver the Replica Package to the Replicas:

  – Configure your Primary to allow Push DB assisted Recovery, which sends the Replica Package to the Replica after you install and start the Replica.

  – Disable Push DB, create the Replica Package, manually copy it to the Replica, and install the Replica.

    For more information on disabling Push DB, see "Disabling Database Push" on page 91.

Pre-Installation Tasks

Unless instructed otherwise, complete each task on the machine or machines that will run RSA Authentication Manager software. If you do not understand or are unable to comply with an instruction, contact RSA Security Customer Support before proceeding.

Before you install RSA Authentication Manager, perform the following tasks:

1. Create a full system backup of the target machine. A current and complete system backup will ensure protection against the usual risk of data loss. If you are upgrading, stop all RSA Authentication Manager processes before creating the backup. To stop the Report Creation utility, type:

   ```
   ACEUTILS/rptconnect stop
   ```

   Stop the RSA Authentication Manager services and database brokers. Type:

   ```
   ACEPROG/aceserver stop
   ACEPROG/sdconnect stop
   ```

2. Set the Authentication Manager system time. Reliable system time is critical to proper RSA Authentication Manager operation.

   - *If this is a first-time installation*, set the Authentication Manager system time according to Coordinated Universal Time with an offset for your time zone. To get UTC, call a reliable time service.
   - *If you are upgrading and the target machine is not the existing* Authentication Manager *machine,* set the target machine time to match that of the existing Authentication Manager. If the time is not set to match the existing Authentication Manager time, some or all tokenholders may be denied access.

3. Create a permanent RSA Authentication Manager top-level directory into which all RSA Authentication Manager subdirectories, databases, and program files will be installed. If you are upgrading, use the existing top-level directory.

   The RSA Authentication Manager top-level directory

   - Must have enough disk space to hold all RSA Authentication Manager files and allow for the growth of the data files.
   - Must not be on a partition available to the network through, for example, NFS.

4. Add the RSA Authentication Manager service names and port numbers to **/etc/services**. Add the following lines to **/etc/services** if you do not have these entries already. Even if you will not be using all of the services immediately, you may want to add entries for them.

```
securid         5500/udp
securidprop_00 5505/tcp
securidprop_01 5506/tcp
securidprop_02 5507/tcp
securidprop_03 5508/tcp
securidprop_04 5509/tcp
securidprop_05 5510/tcp
securidprop_06 5511/tcp
securidprop_07 5512/tcp
securidprop_08 5513/tcp
securidprop_09 5514/tcp
securidprop_10 5515/tcp
sdlog           5520/tcp
sdserv          5530/tcp
sdreport        5540/tcp
sdadmind        5550/tcp
sdlockmgr       5560/tcp
sdcommd         5570/tcp
sdoad           5580/tcp
tacacs          49/tcp       #TACACS+
```

The preceding values are the version 6.1 defaults, not requirements. Following are the requirements:

- The service name for the replication service must be the authentication service name with "prop" appended to it, as with **securid** and **securidprop**, or **auth** and **authprop**.

  By default, a Replica is assigned a replication service name and port number when you add the Replica to your system using the **sdsetup -repmgmt** utility. Default port numbers begin at 5506, with 5505 assigned to the Primary. Default port names have a two-digit number appended to them, so the Primary is **securidprop_00**, and the first Replica added to the system is **securidprop_01**. You need to add the same names and port numbers to the **services** file on the Primary and all Replicas.

- The UNIX Server and the Windows machine from which it is administered must have identical service name and port number entries for **sdlog**, **sdserv**, and **sdadmind**.

If you are not using the default service names and port numbers, you must change these parameters as described in Appendix F, "Configuring the RSA Authentication Manager (UNIX)," in the *Administrator's Guide* and make the appropriate entries in the **/etc/services** file of the Authentication Manager.

5. Add the Authentication Manager hostname to the hosts file. Check for Primary and Replica entries in **/etc/hosts**. Add them if they are not there already. If you will not be adding a Replica until later, its hostname does not have to be in the **hosts** file until that time. For requirements for entries in the **hosts** file, see "Hostnames" on page 13.

   If you have DNS, you do not need to include the Authentication Manager names in the **hosts** file, but you must allow reverse lookup. At the command prompt, type **nslookup** ***machine name***. If the command returns the IP address of the machine, you do not need to add the Authentication Manager names to the **hosts** file.

6. Designate the RSA Authentication Manager administrators. Create a UNIX group of RSA Authentication Manager administrators. If you do not already have such a UNIX group, edit the **/etc/group** file to create a group whose members are all those who will be registered in the Authentication Manager database as RSA Authentication Manager administrators. You must create this UNIX group for RSA Authentication Manager file privileges to be set appropriately.

7. Designate an RSA Authentication Manager file owner.

   During installation, the designated file owner is added to the database as the only RSA Authentication Manager administrator. Select a member of the UNIX group of Authentication Manager administrators to be named as the owner of all RSA Authentication Manager files. Verify that this primary UNIX group ID (GID) on this account is that of the UNIX group of administrators you created in the previous step.

   If you are performing a rolling upgrade, you already have a file owner selected. There is no need to select a different file owner now. To see who is the current Authentication Manager file owner, run **sdinfo** on the Authentication Manager. If you want to select a different file owner, you must select a member of the UNIX group of administrators who is already registered in the RSA Authentication Manager database as a realm administrator.

8. Verify that the RSA Authentication Manager file owner has an entry in the Authentication Manager **/etc/passwd** file. If there is no entry for that account, add it.

9. Verify that the kernel parameter settings are configured to meet the requirements described in Appendix B, "Modifying Kernel Parameters."

Next Steps

Do one of the following:

- If your system has failed to meet any requirement listed in this chapter, **STOP**. Do not go to Chapter 2, "Installing RSA Authentication Manager." Contact RSA Security Customer Support for assistance.
- If you have successfully completed the pre-installation tasks, and you are installing the RSA Authentication Manager for the first time, see Chapter 2, "Installing RSA Authentication Manager," for complete instructions.
- If you have successfully completed the pre-installation tasks, and you are performing an upgrade from RSA ACE/Server 5.1 or 5.2, see Chapter 3, "Upgrading to RSA Authentication Manager."

2 Installing RSA Authentication Manager

Follow the instructions in this chapter to install the RSA Authentication Manager software on your Primary and Replica Authentication Managers, and perform post-installation tasks.

Installing the Primary Software

The installation procedure in this section assumes that the RSA Authentication Manager 6.1 distribution medium (RSA Authentication Manager software and license) can be mounted on your Authentication Manager workstation. If the target Authentication Manager workstation does not have a local CD drive, you can use NFS facilities to export the CD drive mount point to the target Authentication Manager workstation, mount the drive, and install from the CD. You can also copy the appropriate directory from the CD to a directory on the workstation and install from the workstation directory.

To install the Primary software:

1. Log on to the designated Primary as **root**.
2. If you are performing an upgrade, go to step 3. If you are installing a Primary as part of a new installation, copy the following files from the license CD to the installation directory on your workstation.

   license.rec

   server.cer

   server.key

   sdti.cer

   The filenames *must* be in all lowercase letters.

   Omit step 3, and go directly to step 4.
3. Do one of the following:
   - If you are upgrading the Primary on the same system, **do not** copy the files mentioned in step 2 to the current directory. The upgrade completes this task automatically.
   - If you are upgrading the Primary on a new system, you need to copy the files mentioned in step 2 from your existing ***ACEDATA*** directory to the current directory.
4. Create a mount-point directory for the CD drive that is outside your top-level Server directory:

   ```
   mkdir /cdrom
   ```

Note: Make sure your current directory is writable. Do not attempt to install the RSA Authentication Manager 6.1 software by changing to a directory on the CD.

5. Mount the CD drive. Use the following table to find the **mount** command for your operating system.

OS	Command
Solaris and Linux	Not necessary because the volume manager mounts the CD automatically.
HP-UX	As **root** with **/usr/sbin** in your execution path, type `mount -F cdfs /dev/dsk/c3t2d0 /cdrom`
AIX	`mount -o ro -v cdrfs /dev/cd0 /cdrom`

Note: CD device names vary from host to host. On HP-UX systems, the device name depends on the CD driver used by your system. If your machine returns an "unknown command" error message, consult the documentation that came with your operating system.

6. Determine the **/cdrom/*platform*** directory, where ***platform*** is the abbreviation for your operating system.

OS	Platform Abbreviation	Directory
Solaris	sol	**/cdrom/*cd_name*/sol**
HP-UX	hp	**/cdrom/hp**
AIX	aix	**/cdrom/aix**
Linux	linux	**/cdrom/linux**

On Solaris, you must include the name of the CD in the directory path.

7. The command to start the Primary Authentication Manager installation is:

```
/cdrom/platform/sdsetup -primary[-f fileowner]
[-o yes] [-p path][-r {yes|no}]
```

If you are performing an automatic migration, run this command from the top-level directory that contains the existing RSA Authentication Manager installation.

The arguments in brackets are optional. If you do not supply them, you will be prompted for them during the installation. The *italicized* words represent values you supply.

If you supply values for all the parameters in the command line, the installation program runs to completion on its own once you select a country of origin and accept the terms of the license agreement.

If you omit any one of the arguments and the installation program requires a value for it, you will be prompted for the value after you have selected a country and accepted the terms of the displayed license agreement. You must respond to each prompt before the installation procedure continues.

If you issue the sdsetup primary command with no additional arguments, the first part of the installation program runs interactively, prompting you to select a country, accept the terms of the license agreement, and to enter those configuration values that you must set. After you have answered all of the questions presented, the program runs to completion on its own.

Command Line Arguments

-f *fileowner*	Supply the name of the file owner you selected during Authentication Manager preparation.
-o yes | no	Reinstall without first removing existing files from the **ace/prog** subdirectory. When you specify **-o yes**, the installation program moves the contents of **ace** to **ace_tmp**. When you specify **-o no**, the installation terminates.
-p *path*	Supply the pathname of the top-level RSA Authentication Manager directory you selected or created during Authentication Manager preparation.

Example with Command Line Arguments

The following example command, issued on an HP system that has been properly prepared for RSA Authentication Manager installation, produces the following results:

```
/cdrom/aceserv/hp/sdsetup -primary -f smith -o yes -p /top -r yes
```

- Values for all configuration parameters that require user input are provided in this example command. Because the installation program requires additional configuration information, you must perform the following tasks:
  - Select a country of origin.
  - Accept the terms of the license agreement.
- RSA Authentication Manager files are owned by user **smith**, so all members of the smith primary UNIX group will have the permissions required to run RSA Authentication Manager programs.
- All Authentication Manager files are stored in subdirectories of **/top**.
- If the installation program finds files in **/top/ace**, the files will be moved to **/top/ace_tmp** without notification, and files already in **/top/ace_tmp** will be deleted without notification.
- For an upgrade, if database dump files exist in **/top/ace/data**, you will be asked if you want to migrate them to your 6.1 database. Type "**y**" (for Yes) or "**n**" (for No), and press ENTER.

Installation Prompts

The installation program prompts for any required information not supplied in the command line. The prompts, which appear after a few startup screens, are described in the order they appear.

Country of Origin

You can select the country from which you ordered the RSA Authentication Manager software. Once you choose yes (**y**) or no (**n**), the correct license displays.

License Agreement

The terms and conditions under which the RSA Authentication Manager software may be used are displayed after you select the country of origin. Accept the terms of the license by entering **A**. If you choose not to accept those terms and conditions, the installation program terminates.

Fileowner

When you are prompted for a file owner, enter the logon name or user name you designated in step 7 on page 18. Confirm the name you entered when prompted.

Path

Supply the pathname of the top-level RSA Authentication Manager directory you selected or created during Authentication Manager preparation. The path you specify contains all Authentication Manager subdirectories, databases, and program files.

Overwrite

This prompt appears if the installation program detects that an installation of RSA Authentication Manager software exists on the machine. Enter **y** to overwrite, **r** to respecify, or **q** to quit.

If any RSA Authentication Manager database dump files exist in the **ace/data** subdirectory, the installation program prompts you to specify whether you want to use the existing dump files to perform the database migration, or if you want the installation process to create and use dump files from the current database to migrate the database to 6.1. If you answer **yes**, the installation program uses the existing dump files to create the database. If you answer **no**, the installation program creates dump files from the existing database and uses them to create the new database. The installation program moves the existing RSA Authentication Manager files to **ace_tmp**, overwriting the current contents of **ace_tmp**.

Important: Once files are moved to **ace_tmp**, you can delete them or move them to another location. If you do not move or back up the files in **ace_tmp** and then reinstall or upgrade the Authentication Manager software, the contents of **ace_tmp** will be lost permanently when overwritten by this installation.

Upgrade Warnings

This prompt appears if you are performing an upgrade of the Primary. It is a reminder to back up any existing files. Answer **o** to continue with the installation.

Replicas

If this is a new installation, you are asked if you want to add Replicas and create Replica packages for them. If you are upgrading, you are asked if you want to create Replica packages for any preexisting Replicas in the database. For information, see "Preparing the System for Replica Support" on page 27 and "Adding Replicas to the Database" on page 28.

You can also add Replicas to your database if you have upgraded from a previous version. Your license controls the number of Replicas that you can have in your RSA Authentication Manager installation. For more information about licenses, see the section "Licensing Options" on page 11.

Primary Installation Is Complete

The program notifies you and displays the Authentication Manager configuration and license information when installation has completed successfully. If the number of users or Replicas in your database exceeds the license limit, the installation program displays upgrade violation information. For more information about licenses, see Chapter 1, "Overview," in the *Administrator's Guide*.

If you also receive a message about service names being unresolvable, it is possible that the service names were incorrectly entered in **/etc/services** (see page 17), or that you chose to use service names other than the defaults. If the latter is true, for instructions on modifying the Authentication Manager configuration file, see the chapter "Configuring the RSA Authentication Manager (UNIX)," in the *Administrator's Guide*.

Post-Installation Setup

This section contains information about the Primary after installation and the tasks that you must perform on the Primary before installing the RSA Authentication Manager software on a Replica.

Although most administration of the RSA Authentication Manager for UNIX database is performed remotely on a Windows machine, UNIX Server configuration and some setup tasks must be performed directly on the UNIX Server itself. These setup tasks are described in this section.

The interface for reconfiguration and administration on the UNIX Server is limited to command lines and the Server administration program in TTY mode (character-based). If you have never used **sdadmin** in character mode, see "Extracting and Importing Token Records" on page 25.

Security Requirements

The following list contains security requirements and issues. Verify that the RSA Authentication Manager machine meets these requirements:

- ❑ RSA Authentication Manager computers must be secure. Only trusted personnel should have physical access to the Primary and Replicas, and the Authentication Managers must be protected by RSA SecurID.
- ❑ Only UNIX administrators must have accounts on the Primary and Replicas.
- ❑ Disable the **rsh** and **rcp** commands. They are unable to provide RSA SecurID protection.
- ❑ Do not use **rexec** or any other routines that bypass UNIX security. Disable the **rexec** daemon and other daemons if necessary. Also, avoid using **hosts.equiv** and **.rhosts** files. This is especially important on AIX platforms because passcode prompting does not occur if there are **hosts.equiv** or **.rhosts** files.
- ❑ If RSA SecurID authentication is invoked through the **/etc/passwd** file, avoid all sign-on situations that do not invoke a user's shell and therefore do not invoke **sdshell** and passcode processing.
- ❑ The **chsh** and **passwd** commands must be used only by administrators. If a user can modify the **/etc/passwd** file and change his or her logon shell from **sdshell**, the user will no longer be required to provide an RSA SecurID passcode to gain system access. Where **chsh** is supported, the **/etc/shells** file must contain **sdshell** *only*. This disables **chsh** and **passwd** equivalents (**passwd -s**). On an HP-UX system, you must disable **chsh** manually.

Telnet

If you use **telnet**, use encrypted telnet or use telnet in line mode. If neither of these is available, you may want to make either of the following changes to the configuration record:

- Change the settings for **Bad PASSCODEs before Next Tokencode** and **Bad PASSCODEs before Disabling Token** to lower values because the passcode is sent one character at a time in clear text.
- Increase the value of the **Response Delay** so that the Authentication Manager waits longer to detect the last character of the passcode.

For information on changing the configuration record, see the chapter "Configuring the RSA Authentication Manager (UNIX)," in the *Administrator's Guide*.

Logging Replication Messages to the syslog

If you want to log RSA Authentication Manager replication status messages to the syslog, edit the **syslog.conf** file on each Authentication Manager to include messages that use the ***.info** suffix. These status messages are logged when database changes are replicated.

Using a text editor, open the **/etc/syslog.conf** file and add ***.info** to the line that specifies your system log file.

CAUTION: Logging replication status messages can cause the syslog to grow rapidly. RSA Security recommends that you log these messages to the syslog only when you need to see that the replication process is occurring. If you need to log these status messages, clean the syslog frequently.

Testing Authentication

Follow the procedures in this section to verify that your Primary and Replicas are installed properly and that you can implement protection for them as Agent Hosts.

Extracting and Importing Token Records

If you received a CD containing token records (.asc or .xml files), you must extract the token records from the diskette using the method you normally use and transfer them to the Primary so that you can import the tokens into the database and assign tokens to your users.

Note: If you are upgrading, preexisting token records are automatically migrated into your 6.1 database.

Important: After you extract and import the token records, delete any copies of the token record file from your system and store the diskette in a secure place. Token records contain important and sensitive information and must be handled by trusted personnel only.

You can import the token records into the database using the character-based Database Administration application **sdadmin** or the Remote Administration software on a Windows-based machine. The following procedure describes how to import tokens using **sdadmin**. For more information about **sdadmin**, see "Using sdadmin" in Appendix D, "Database Utilities."

To import tokens:

1. Log on to the Primary as the RSA Authentication Manager file owner.
2. Start the database brokers:

```
ACEPROG/sdconnect start
```

3. Run the RSA Authentication Manager administration program:

   ```
   ACEPROG/sdadmin
   ```

   For instructions on how to use the Authentication Manager administration program, see "Interface Conventions" on page 86.

4. From the Token menu, select **Import Tokens**.

5. Enter the path and filename of the token record file you extracted from the diskette that was included in your initial RSA Authentication Manager software package.

Implementing RSA SecurID Authentication for a User

The following procedure describes how to add a user to the RSA Authentication Manager database, assign a token to the user, and activate the user on an Agent Host. When you have completed the procedure, you can use the test user to test local authentication from the Agent Host to the RSA Authentication Manager. With local authentication, the RSA Authentication Manager is also acting as the Agent Host (both the RSA Authentication Manager and the RSA Authentication Agent reside on the same machine). When the test user logs on to the Authentication Manager, he or she is prompted for RSA SecurID authentication.

Important: Do not use the RSA Authentication Manager administrator as the test user. If the test authentication fails, you may be locked out of the system.

To implement RSA SecurID authentication:

1. In the RSA Authentication Manager administration program, create a local user record for a test user. Click **User > Add User**. Enter the appropriate information. Click **OK** to close the Add User dialog box.

2. Assign a token to the test user. Click **Assign Token**.

   Select a token record by serial number. Locate the token itself by matching the serial number that appears on the back of the token.

3. Click **Agent Host** > **List Agent Hosts** to see if the Primary and Replicas are registered as Agent Hosts.

4. If the Primary or Replica is not registered as an Agent Host, click **Agent Host > Add Agent Host**, enter the hostname of the machine, select **Agent type: UNIX Agent**, and then select **User Activations** to specify that the test user can be granted access to the machine after being authenticated by RSA SecurID.

5. Exit **sdadmin** by selecting **Exit** on the File menu.

Performing a Test Authentication

Performing a test authentication ensures that you have installed and configured the RSA Authentication Manager correctly.

To test RSA SecurID authentication:

1. If the **aceserver** is not already running, start it on the Authentication Manager by typing:

   ```
   ACEPROG/sdconnect start
   ACEPROG/aceserver start
   ```

2. Run the test authentication utility. Type:

   ```
   ACEPROG/sdtestauth
   ```

   You are prompted for a User ID and RSA SecurID passcode.

3. At the **Enter PASSCODE** prompt, type the code that appears on the RSA SecurID token you assigned in step 2 of the previous procedure. Press ENTER. Follow the directions that appear on the screen to obtain a personal identification number (PIN).

4. When you have received or chosen your PIN, you are prompted again for a passcode. Wait for a new tokencode, then enter a combination of the PIN and the current RSA SecurID tokencode. Specifically, *if you have an RSA SecurID standard card or key fob*, you enter the PIN followed by the code that appears on the card. *If you have an RSA SecurID PINPad*, enter the PIN into the card itself and press the diamond that appears near the bottom of the card. Answer the **Enter PASSCODE** prompt by typing the code that now appears on the PINPad.

   If you are consistently denied access, after having performed all installation and setup procedures as directed and having entered valid passcodes, see the appendix "Troubleshooting," in the *Administrator's Guide*. If you are unable to resolve the problem, call RSA Security Customer Support.

Preparing the System for Replica Support

1. If you have not done so already, verify that the Replica workstation meets all system requirements listed in Chapter 1, "RSA Authentication Manager Requirements."
2. Prepare the workstation as described in "Pre-Installation Checklist" on page 14.
3. Be sure that the replication service communications service name and port number are in the **/etc/services** file of each Authentication Manager. For a list of the default service names and port numbers, see page 17.
4. If necessary, every 24 hours the Primary/Replica communications program **acesyncd** will adjust the Replica system clock to match the Primary system clock. If this is a first-time installation, and the Primary and Replica system clocks are not in sync, this change could upset scheduled tasks and other time-based applications. Avoid problems by changing the Replica clock manually and making all the adjustments this may require. If you are upgrading existing Authentication Managers, you do not need to change the Replica clock manually.

Note: You must have root privileges to make changes to the Replica clock. In addition, if you are using NTP, it should be enabled on the Primary and on each Replica. For more information, see "Maintaining Accurate System Time Settings" on page 14.

5. If you are upgrading, when configuration is complete, update all Agent Hosts that are registered on the Primary. For UNIX Agent Hosts and certain other RSA Authentication Agents, this means installing the modified **sdconf.rec** file into each Agent Host data directory. Legacy Agent Hosts may require **sdconf.rec** files that are configured to use different Acting Master/Slave pairs.
6. Other Agent types, such as third-party devices, may require changes to their configuration files. For information on updating each Agent type's configuration, refer to the documentation on each Agent type.
7. Follow the instructions in the next section to add a Replica to the database.

   If you are performing an automatic migration of the database as part of an upgrade, go directly to "Installing the Replica Software" on page 30.

Adding Replicas to the Database

Before you can install the RSA Authentication Manager software on a Replica, you must add each Replica to the database and create the Replica Package on the Primary. The Replica Package contains the license and database files that the Replica installation requires.

To add the Replicas to the Database:

1. Log on as **root** on the Primary.
2. Stop the Report Creation utility. Type:

   ```
   ACEUTILS/rptconnect stop
   ```

3. Stop the RSA Authentication Manager services and database brokers. Type:

   ```
   ACEPROG/aceserver stop
   ACEPROG/sdconnect stop
   ```

4. Type:

   ```
   ACEPROG/sdsetup -repmgmt add
   ```

5. Enter the following information about the Replica when prompted:
   - The hostname of the Replica machine. The IP address is resolved automatically.
   - The alias IP addresses used by the Replica, which can be used to configure Agent Hosts that need to authenticate through a firewall.
   - The service name and port number of the replication service used for communication between the Primary and the Replica.

- By default, the service name is **securidprop** with a number appended. For example, the first Replica added uses the service name **securidprop_01**, and the service name for any additional Replicas is incremented by one.
- By default, the port numbers used by the Replicas to communicate with the Primary begin at 5506, and are incremented by 1 for each additional Replica.
- The number of seconds after the Primary starts up that the first replication attempt is made (the startup delay interval).
- How often the Primary performs a replication pass (the Replication Interval).

6. Repeat step 5 for each Replica you want to add.
7. To view a list of all the Replicas in the database, type:

   ```
   ACEPROG/sdsetup -repmgmt list
   ```

   For a full description of the **sdsetup -repmgmt** utility, see the *Administrator's Guide*.
8. Follow the instructions in the next section "Creating a Replica Package."

Creating a Replica Package

The Replica Package contains the database and license files needed to install the Replica software. The procedure in this section assumes that you have already added the Replicas, as described in the preceding section "Adding Replicas to the Database."

To create the Replica Package:

1. Log on as **root** on the Primary.
2. Stop the Report Creation utility. Type:

   ```
   ACEUTILS/rptconnect stop
   ```
3. Stop the RSA Authentication Manager database brokers and processes. Type:

   ```
   ACEPROG/aceserver stop
   ACEPROG/sdconnect stop
   ```
4. Create a Replica Package. Type:

   ```
   ACEPROG/sdsetup -package
   ```

   Information is displayed about the number of Replicas currently in your database, and the number that your license allows.

   You are asked if you want to add a new Replica before you generate a Replica Package.

5. Type **y** to add a new Replica. If you do not want to add a new Replica, type **n**, and then press ENTER.

   The **replica_package** directory is created in the ***ACEDATA*** directory and contains two directories: the **database** directory, which contains the database files (**sdserv.db**, **sdserv.bi**, **sdserv.lg** and **sdserv.vrs**), and the **license** directory, which contains the license files (**license.rec**, **sdconf.rec**, **sdrepnodes.txt**, **server.cer**, **server.key**, and **sdti.cer**). If you are performing a rolling upgrade, the **license** directory contains an additional file: **uidxlate.map**.

6. Copy only the **license** directory to each Replica. The Primary pushes the database files after you install and start the Replica.

   If you have disabled Push DB on the Primary, copy the contents of the **replica_package** directory to each of the Replica machines.

   In either case, the directory must be outside of the top-level RSA Authentication Manager directory.

   RSA Security recommends that when you create a Replica Package, you deliver it to the Replica as soon as possible. Once you create the Replica Package, the Primary begins saving subsequent database changes that it sends to the Replica on the first replication pass. The longer you wait to create and install the Replica Package, the more changes the Primary may have to send to the Replica.

7. Start the Primary.

   ```
   ACEPROG/sdconnect start
   ACEPROG/aceserver start
   ```

8. Follow the instructions in the next section to install the Replica software.

Installing the Replica Software

The installation procedure in this section assumes that the RSA Authentication Manager 6.1 CD can be mounted on your Authentication Manager workstation. If the target Authentication Manager workstation does not have a local CD drive, you can use NFS facilities to export the CD drive mount point to the target Authentication Manager workstation, mount the drive, and install from the CD. You can also copy the appropriate directory structure from the CD to a directory on the workstation and install from the workstation directory.

To install the Replica software:

1. Log on to the Replica as **root**.
2. Create a mount-point directory for the CD drive:

   ```
   mkdir /cdrom
   ```

3. Mount the CD drive. Consult the following table to find the **mount** command for your platform.

OS	Command
Solaris and Linux	Not necessary as the volume manager mounts the CD automatically.
HP-UX	As **root** with **/usr/sbin** in your execution path, type `mount -F cdfs /dev/dsk/c3t2d0 /cdrom`
AIX	`mount -o ro -v cdrfs /dev/cd0 /cdrom`

Note: CD device names vary from host to host. On HP-UX systems, the device name depends on the CD driver used by your system. If your machine returns an unknown command error message, consult the documentation that came with your operating system.

4. Determine the **/cdrom/*platform*** directory from which you want to install, where ***platform*** is the abbreviation for your operating system.

OS	Platform Abbreviation	Directory
Solaris	sol	**/cdrom/*cd_name*/sol**
HP-UX	hp	**/cdrom/hp**
AIX	aix	**/cdrom/aix**
Linux	linux	**/cdrom/linux**

On Solaris, you must include the name of the CD in the directory path.

5. The command to start Replica installation is

   `/cdrom/`*platform*`/sdsetup -replica [-o yes]`
   `[-p` *path*`] [-R` *path*`]`

   The arguments in the brackets are optional. If you do not supply them, you will be prompted for them during the installation. The *italicized* words represent values you supply.

   If you supply values for all the parameters in the command line, the installation program runs to completion on its own once you select a country of origin and accept the terms of the license agreement.

   If you omit any one of the arguments and the installation program requires a value for it, you will be prompted for the value in the first five to ten minutes of the program's execution. You must respond to any prompts before the installation procedure continues.

   If you issue the sdsetup -replica command with no additional arguments, the first part of the installation program runs interactively, prompting you to enter those configuration values that you must set. After you have answered all of the questions presented, the program runs to completion on its own.

Command Line Arguments

-o yes | no	If you are upgrading, with this argument you can reinstall without first removing existing files from the **ace/prog** subdirectory. When you specify **-o yes**, the installation program moves the contents of **ace** to **ace_tmp**. When you specify **-o no**, the installation terminates.
-p *path*	Supply the pathname of the top-level RSA Authentication Manager directory you selected or created during Authentication Manager preparation. Use the same pathname on the Replicas and the Primary.
-R *path*	Specify the pathname of the directory that contains the Replica Package files you copied from the Primary to the Replica.

Installation Prompts

The installation program prompts you for any required information not supplied in the command line. The prompts, which appear after a few startup screens, are described in the order in which they appear.

Top-Level RSA Authentication Manager Directory

Supply the pathname of the directory you selected or created during Authentication Manager preparation. The path you specify contains all RSA Authentication Manager subdirectories, databases, and program files. Use the same pathname on the Replicas and the Primary.

Replica Package

Specify the pathname of the directory that contains the Replica Package files. If your System Parameters are configured to allow Push DB Assisted Recovery, the specified path needs to contain only the license files. If your System Parameters are *not* configured to allow Push DB Assisted Recovery, the path must contain the license and database files.

Important: Once files are moved to **ace_tmp**, you can delete them or move them to another location. If you do not move or back up the files in **ace_tmp** and then reinstall or upgrade RSA Authentication Manager software, the contents of **ace_tmp** will be lost permanently when overwritten by this installation.

Completing the Replica Installation

The installation program notifies you and displays the Authentication Manager configuration and license information when installation has been successfully completed. If the number of users or Replicas in your database exceeds the license limit, the installation program displays upgrade violation information. For more information about licenses, see the chapter "Overview," in the *Administrator's Guide*.

Troubleshooting Service Name and Port Numbers

If you also receive a message about service names being unresolvable, it is possible that the service names were incorrectly entered in **/etc/services** (see page 17), or that you chose to use service names other than the defaults. For instructions on modifying the Authentication Manager configuration file, see the *Administrator's Guide*.

Monitoring Startup Processes

Before you start the Replica, you can start the log monitor on the Primary by running the following command:

```
ACEPROG/sdlogmon -t
```

This command displays the Log Monitor, and you can see that communication has been established between the Primary and the Replica. If PushDB (the process that sends the latest database to a Replica) is enabled, you see messages that this process is starting. The Primary shuts down the database brokers and authentication process on the Replica, pushes the database, and then restarts the database brokers and the authentication process on the Replica. For more information about PushDB, see the chapter "Overview," in the *Administrator's Guide*.

Starting the Replica

To start the Replica:

1. Log on to the Authentication Manager as the RSA Authentication Manager file owner.
2. Start the database brokers:

   ```
   ACEPROG/sdconnect start
   ```

   A series of messages follows, indicating that the database brokers are starting. When startup is complete, a message informs you that:

   ```
   Database broker start operation completed
   ```

   If Push DB is enabled, omit step 3. The Primary immediately stops the brokers on the Replica and pushes the database to the Replica. When the push is complete, the Primary restarts the brokers and the authentication service on the Replica, so there is no need to issue the **aceserver start** command.

3. Start the authentication service:

   ```
   ACEPROG/aceserver start
   ```

   A series of messages follows, indicating that RSA Authentication Manager is starting. When startup is complete, a message informs you that:

   ```
   RSA ACE/Server start operation completed
   ```

   The Replica is now ready to authenticate users.

Next Steps

Important: You must make backup copies of your license after you install the RSA Authentication Manager software. During installation, the license file is modified. Therefore, if your license in the ***ACEDATA*** directory is lost or corrupted, you cannot regain access using the original license diskettes. The only way to regain access is with the modified license files.

To install a TACACS+ device and to turn on RSA Authentication Manager support for the TACACS+ protocol, see Chapter 5, "RSA Authentication Manager TACACS+ Support."

3 Upgrading to RSA Authentication Manager

You can upgrade to RSA Authentication Manager 6.1 if you are running RSA ACE/Server 5.1 or later, or RSA Authentication Manager 6.0 or later.

You can perform an automatic migration (if you have just a Primary) or a rolling upgrade (if you have one or more Replicas) when:

- You are installing RSA Authentication Manager 6.1 over an existing installation in the same directory as your previous version.
- You are running on an operating system version that is supported for RSA Authentication Manager 6.1.

When the RSA Authentication Manager installation program finds a version 5.1 or later database in the **ace/data** subdirectory and the appropriate migration tools in the **ace/prog** subdirectory, the program automatically migrates the data into the version 6.1 database.

Important: If database dump files (files with the .dmp extension) exist in the **ace/data** directory, the installation prompts you to specify whether you want to use those files, or if you want the installation process to dump and load the existing database.

Pre-Upgrade Checklist

RSA Security recommends that you review the *Readme* (**authmgr_readme.pdf**) before upgrading the RSA Authentication Manager 6.1 software. The *Readme* contains important configuration and installation information, as well as information about software issues found too late to be included in the standard documentation.

Important: If you use the RSA RADIUS Server in your current installation and want to migrate to the RSA RADIUS Server 6.1, see Appendix A, "Migrating Your RSA RADIUS Server" *before* you upgrade your Primary and Replica Servers.

You must have

- ❑ A machine that meets all the hardware, diskspace, memory, and platform requirements described in Chapter 1, "RSA Authentication Manager Requirements."
- ❑ A supported version of the RSA Authentication Manager software installed on an Authentication Manager.
- ❑ Sufficient disk space (preferably on another system) to create backup copies of the existing Primary Authentication Manager **sdserv** and **sdlog** database files and the existing Replica Authentication Manager **sdserv** database files.

  Note: Stop all RSA Authentication Manager processes before you create backup copies of the database files.

- ❑ Root and administrator privileges on the Primary and Replicas.
- ❑ The RSA Authentication Manager 6.1 CD or online distribution file.
- ❑ The license files from your existing Primary or the new license files. If you have received new license files, RSA Security recommends that you apply them after you perform the upgrade.

You must know

- ❑ The name and IP address of any Replicas you want to add.
- ❑ The number of Replicas allowed by your license.
- ❑ If you have an RSA Authentication Manager Base license, you can install one Replica. If you have an RSA Authentication Manager Advanced license, you can install up to 10 Replicas.

Preparing for the Primary Upgrade

Important: Before upgrading, turn off local access protection on the Primary and Replicas, if they are protected by RSA Authentication Agent software. Failure to do so may result in being locked out of your machines. For instructions on turning on local access protection, see your RSA Authentication Agent documentation.

Before you upgrade the RSA Authentication Manager software, log on to the Primary as an administrator, and perform these tasks:

Task 1: Stop the RSA Authentication Manager Services on the Primary

You cannot upgrade the RSA Authentication Manager software while RSA Authentication Manager services are running on the Authentication Manager you want to upgrade. You must also disable any automatic startup of the RSA Authentication Manager you may have configured on the system.

Stop all RSA Authentication Manager programs and database brokers running on the Primary. When you stop **aceserver** on the Primary, the Replicas continue to authenticate users and log activity, but you cannot administer the database.

Stopping RSA Authentication Manager

Make sure all administrators have exited **sdadmin**, **sdlogmon**, and **sdreport**. To stop the Report Creation utility, type:

```
ACEUTILS/rptconnect stop
```

then, to stop the services and database brokers, type:

```
ACEPROG/aceserver stop
ACEPROG/sdconnect stop
```

Task 2: Back Up the Database and License Files on the Primary

After stopping all RSA Authentication Manager processes, create backup copies of the database files, license files, the configuration file, and any RADIUS accounting files on the Authentication Manager.

The database and license files are stored in the ***ACEDATA*** directory (for example, **ace**/**data**). To back up the database and license files, copy the ***ACEDATA*** directory.

By default, RADIUS accounting files are stored in the ***ACEDATA*****\radacct** directory. If you specified a different directory, the full path is listed in the Accounting menu of the RADIUS Configuration utility (***ACEPROG*****/rtconfig**). To back up the RADIUS accounting files, copy *all* directories in the ***ACEDATA*****\radacct** or user-specified directory.

You are ready to upgrade the Primary. See the following section, "Upgrading a Primary".

Upgrading a Primary

The procedures for upgrading a Primary are described in Chapter 2, "Installing RSA Authentication Manager," in the following sections:

- "Installing the Primary Software"
- "Post-Installation Setup"
- "Testing Authentication"

Follow the instructions in each of these sections and then start the Primary. Type:

```
ACEPROG/sdconnect start
ACEPROG/aceserver start
```

Preparing for a Replica Upgrade

Before you upgrade a Replica, perform these tasks:

Task 1: Copy the Replica Package from the Primary

The Primary upgrade process generates a Replica Package for the Replicas in the ***ACEDATA*\replica_package** directory (or in the directory specified by the REP_ACE environment variable).

Do one of the following:

- If Push DB Assisted Recovery is enabled on the Primary, copy the ***ACEDATA*\replica_package\license** directory from this location to a temporary directory that is outside of the RSA Authentication Manager directory on the Replica machine. After you upgrade and start the Replica, the Primary pushes the database files to the Replica.
- If Push DB Assisted Recovery is disabled on the Primary, copy the contents of the ***ACEDATA*\replica_package** directory to a temporary directory that is outside of the RSA Authentication Manager directory on the Replica machine.

During the Replica upgrade, you must specify the location of the license files.

Task 2: Stop All RSA Authentication Manager Services on the Replica

You cannot upgrade the RSA Authentication Manager software while RSA Authentication Manager services are running on the Authentication Manager you want to upgrade. See "Stopping RSA Authentication Manager" on page 36.

You are ready to upgrade the Replica. For instructions, see the following section "Upgrading a Replica".

Upgrading a Replica

The procedures for upgrading a Replica are described in Chapter 2, "Installing RSA Authentication Manager," in the following sections:

- "Installing the Replica Software"
- "Completing the Replica Installation"

Follow the instructions in these two sections and then return to this section.

Next Steps

To install a TACACS+ device and to turn on RSA Authentication Manager support for the TACACS+ protocol, see Chapter 5, "RSA Authentication Manager TACACS+ Support."

4 Installing Remote Administration Software

Remote administration provides a graphical user interface for administering an RSA Authentication Manager database, and provides the only supported method of accessing all administrative features that are available in the Database Administration application. Remote administration of an RSA Authentication Manager database on a UNIX platform can be performed from machines running

- Windows 2003 Server
- Windows 2000 Professional, Windows 2000 Server, and Windows 2000 Advanced Server
- Windows XP Professional

You can also use the browser-based RSA Authentication Manager Quick Admin software to perform some common tasks, but Quick Admin does not allow full administration of the database. For more information, see Chapter 6, "Installing the Quick Admin Software."

Note: With the Remote Administration application, you can change the database on the Primary Server only. When you connect to the database on a Replica Server, the connection is read-only. You can run reports, run the log monitor, and view database information, but you cannot make administrative changes to the Replica database.

Configuring Remote Administration Authentication Methods

By default, RSA Authentication Manager is configured to allow remote administration. However, you must select the types of tokens (or authentication *methods*) that remote administrators use when logging on by way of Remote Administration. The administrator authentication methods include RSA SecurID cards and key fobs, Lost Token Passwords, software tokens, and User Passwords.

To configure administrator authentication methods:

1. On the Primary Server, change to the ***ACEPROG*** directory, and run **sdadmin**.
2. From the System menu, select **System Configuration**, then select **Edit System Parameters**.
3. Under **Administrator Authentication Methods**, select the methods to be used to authenticate remote administrators.

Installation and Upgrade Checklist

Before you begin, use this checklist to verify that you have all the hardware, software, and information you need to upgrade the RSA Authentication Manager Remote Administration software.

- ❑ A machine with an Intel Pentium processor running Windows 2000 Professional, Windows 2000 Server, or Windows 2000 Advanced Server (Service Pack 4), Windows XP Professional, or Windows 2003 Server. For more information on hardware, disk space, and memory requirements, see Chapter 1, "RSA Authentication Manager Requirements."

  Note: Make sure the machine is located in a secure area and can be accessed by trusted personnel only. Only the Database Administration application is protected by RSA SecurID authentication. If you want RSA SecurID protection for the machine itself, you must install the RSA Authentication Agent for Windows software.

- ❑ A supported version of the RSA Authentication Manager software installed on a Primary.

  The version of the RSA Authentication Manager software must match the version of the Remote Administration software you are installing. If you installed the Remote Administration software with previous versions of RSA Authentication Manager, you cannot remotely administer an RSA Authentication Manager 6.1 database until you upgrade the Remote Administration software. If you upgrade Remote administration software, you will no longer be able to administer a pre-6.1 database from the machine running the upgraded Remote Administration software.

- ❑ Local administrator privileges on the Primary and the remote machine.

- ❑ Access to the **sdconf.rec** and **server.cer** files on the Primary.

  Copy the **sdconf.rec** and **server.cer** files from the ***ACEDATA*** directory to a diskette, or make the files accessible to the remote administration machine.

Installing Remote Administration for the First Time

RSA Security recommends using dedicated machines to run each component, but if you decide to run several components on the same machine you must follow certain guidelines.

When installing Remote RADIUS, Remote Administration, and Agent Host Auto Registration on the same machine, you must install the components in the following order:

- Agent Host Auto-Registration
- Remote Administration
- Remote RADIUS

When uninstalling Remote RADIUS, Remote Administration, and Agent Host Auto-Registration from the same machine, you must uninstall the components in the following order:

- Remote RADIUS
- Remote Administration
- Agent Host Auto-Registration

To install the Remote Administration software:

1. On the remote machine, log on as a local administrator, and insert the CD labeled "RSA Authentication Manager 6.1" into the CD drive.
2. In the **aceserv\windows** directory on the RSA Authentication Manager CD, double-click **setup.exe**.
3. Follow the prompts until the New Input Files dialog box opens. Browse to the disk or directory containing the **sdconf.rec** and **server.cer** files, and click **Next**.
4. Follow the prompts until the Installation Options dialog box opens. Select **New Remote Administration**, and click **Next**.
5. Follow the prompts until the installation process is complete.
6. If you are not using DNS, add the name and IP address of the Server to the **hosts** file on the Remote Administration machine.

   On a Windows 2000 or Windows 2003 machine, the **hosts** file is in ***%SystemRoot%*\System32\drivers\etc**.

Upgrading Remote Administration

Important: If you are upgrading Remote Administration on a machine on which Remote RADIUS is also installed, you must first uninstall Remote RADIUS, perform the Remote Administration upgrade, then reinstall Remote RADIUS.

To upgrade the Remote Administration software:

1. On the remote machine, log on as a local administrator, and insert the CD labeled "RSA Authentication Manager 6.1" into the CD drive.
2. In the **aceserv\windows** directory on the RSA Authentication Manager CD, double-click **setup.exe**.
3. Follow the prompts until the Installation Options dialog box opens. Select **Upgrade Remote Administration**, and click **Next**.
4. Follow the prompts until the installation process is complete.

Adding an RSA Authentication Manager to Administer Remotely

If you need to administer additional databases from a machine running the Remote Administration software, follow the instructions in this section. You must have already installed the Remote Administration software as described on page 40.

During the procedure, you are prompted for the location of the **server.cer** and **sdconf.rec** files from the Primary.

To add a server for Remote Administration:

1. Click **Start > Settings > Control Panel > Add/Remove Programs**.
   The Add/Remove Programs Properties dialog box opens.
2. Select RSA Authentication Manager **for Windows**, and click **Add/Remove.**
   The RSA Authentication Manager Maintenance dialog box opens.
3. Select **Modify**, and click **Next**.
4. Select **Add/Remove Remote Administration,** and click **Next**.
5. Click **Add.**
6. Follow the prompts until RSA Authentication Manager Maintenance is complete, and click **Finish.**
7. If you are not using DNS, add the name and IP address of the Server to the **hosts** file on the Remote Administration machine and the Primary, and verify that you can resolve the Remote Administration machine from the Server you want to administer. For the requirements for entries in the **hosts** file, see "Hostnames" on page 13.
   On a Windows 2000 or Windows 2003 machine, the **hosts** file is in ***%SystemRoot%*\System32\drivers\etc**.
   If you have DNS, you do not need to include the Server names in the **hosts** file, but you must allow reverse lookup. At the command prompt, type **nslookup *machine name***. If the command returns the IP address of the machine, you do not need to add the Server names to the **hosts** file.

Note: The same procedure can be used to remove Remote Administration servers. At step 5, highlight the Remote Administration server you want to remove, and click **Remove**.

Configuring Remote Administration Ports

Remote administration uses TCP, which opens two ports for each remote administration session running on your RSA Authentication Manager. You can limit the number of ports that can be opened at the same time, thereby limiting the number of remote administration sessions that can run at the same time, by specifying a range of port numbers that can be used for remote administration connections. You must specify the range on each RSA Authentication Manager.

To specify a range of port numbers:

1. Stop the Report Creation utility. Type:

   ```
   ACEUTILS/rptconnect stop
   ```

2. Stop the RSA Authentication Manager services and database brokers. Type:

   ```
   ACEPROG/aceserver stop
   ACEPROG/sdconnect stop
   ```

3. In the **ace/rdbms** directory (UNIX), make a backup copy of the **startup.pf** file. Name it **startup.old**.

4. Open the **startup.pf** file in a text editor, and add the following lines to the end of the file:

   ```
   -minport minimum port number
   -maxport maximum port number
   ```

   TCP does not use the port you specify as the minimum port number. The first port that TCP uses is always one greater than the minimum port number that you specify, so the range must always include one more port than you need. If you have 10 remote connections, you need 20 ports and must specify a range of 21 ports.

   For example, to use ports 3001 through 3020, add these lines to the file:

   ```
   -minport 3000
   -maxport 3020
   ```

   Make sure the range does not include port numbers used by other services.

   If you use the Progress Software Development Toolkit, your system may be using a **startup.pf** other than the one that shipped with RSA Authentication Manager 6.1. In this case, RSA Security recommends that you edit both **startup.pf** files according to this procedure.

5. Restart RSA Authentication Manager. Type:

   ```
   ACEPROG/sdconnect start
   ACEPROG/aceserver start
   ```

5 RSA Authentication Manager TACACS+ Support

This chapter is for network administrators who have experience with communications servers or routers.

RSA Authentication Manager supports RSA SecurID access control for routers and communication servers running TACACS+ 2.1, also referred to as TACACS (Terminal Access Controller Access Control System) Plus.

TACACS+ provides more detailed accounting information and greater administrative control of authentication and authorization processes. TACACS+ also supports the RSA Authentication Manager Next Tokencode and New PIN modes.

TACACS support is provided through Cisco Systems security software made up of client and server code. The client code is shipped as part of the standard software distribution with Cisco systems and other routers and communication servers. The server code has been integrated with the RSA Authentication Manager.

This chapter provides information on:

- Configuring the RSA Authentication Manager to support a TACACS+ client device and configuring a TACACS+ client device.
- Protecting Enable mode with TACACS+.

Configuration of your TACACS+ device is managed through a startup file and a configuration file to which the startup file points.

```
ACEDATA/sdtacplus.arg.
```

The startup file provides command line arguments needed for the Cisco Systems TACACS+ software. The startup file also points to a protocol-specific configuration file named **sdtacplus.cfg**, which contains

- Information on which users are to be authenticated by RSA SecurID
- Settings for various TACACS+ configuration parameters

When the RSA Authentication Manager system is started with TACACS+ support enabled, it searches for the configuration file specified in the startup file.

Authenticating on a TACACS+ Device

Authentication of TACACS+ Users

1. When a user initiates a logon session through a protected port, that user is prompted for a user name.
2. After the user name is entered, if the user is designated in the configuration file as an RSA SecurID user, the following prompt displays:

   ```
   Enter PASSCODE:
   ```

   The user's response is transmitted to **_sdtacplusd** running on the Authentication Manager. For information on encryption, see "Sample TACACS+ Configuration File" on page 49.
3. When the request is received by **_sdtacplusd**, it invokes RSA Authentication Agent code, which communicates with the **aceserver**. If authentication services are not available because of a network failure, or because no **aceserver** is running, a secondary authentication method is invoked. If there is no secondary method enabled, the TACACS+ client displays:

   ```
   No response from authentication TACACS server.
   ```

   When the **aceserver** receives an authentication request from the client, it performs passcode checking to authenticate the user's identity. The Authentication Manager sends the result to the client device, which displays **PASSCODE Accepted** or **Access Denied**, or performs the New PIN or Next Tokencode procedure, if necessary.

   After a specified number of unsuccessful retries, the client reports **Authentication failed**, the connection is broken, and the logon session must be reinitiated.

Enabling and Configuring TACACS+ Support

To enable and configure TACACS+ Support:

1. Run the Database Administration application and select **Add Agent Host** to register the TACACS+ device as an Agent Host in the RSA Authentication Manager database. Choose **Communication Server** as the Agent type. Activate users or groups of users on the TACACS+ device. For instructions, see the Help topic "Add Agent Host."
2. Exit the Database Administration application.
3. Verify that the following line appears in **/etc/services**:

   ```
   tacacs 49/tcp
   ```
4. If your system is not already configured for TACACS+ support, run **sdsetup -config** to activate it. For more information on running **sdsetup -config**, see the appendix "Configuring the RSA Authentication Manager (UNIX)," in the *Administrator's Guide*.

5. If you had an existing, customized **sdtacplus** argument and configuration files before you installed RSA Authentication Manager 6.1, copy them from **ace_tmp** to the **ace/data** subdirectory to overwrite the default files put there by the installation program.

   If this is a new installation, modify the default **sdtacplus.arg**, which is stored in the **ace/data** subdirectory, to specify command line arguments for the TACACS+ software. All arguments in this file are case sensitive.

6. Modify the default configuration file to

   - Specify which users must be authenticated by RSA SecurID.
   - Set TACACS+ configuration options.
   - Supply an encryption key to protect client/server communications.

   See the sample **sdtacplus** configuration file to learn how RSA SecurID user designations and TACACS+ configuration options are set in the configuration file.

7. For client/server communications to be encrypted, the configuration file must contain a line similar to the following:

   ```
   key = old+gnu$8a1u
   ```

   where **old+gnu$8a1u** is an example of a user-specified key. If you include spaces in the key, enclose the key in double quotation marks.

   Note: You must enter the user-specified key into the configuration file on each TACACS+ client device. In addition, you must set the client/server communication encryption type to DES.

8. Copy the modified **sdtacplus.arg** and **sdtacplus.cfg** files to the ***ACEDATA*** directory on the Replica.

9. To reread the TACACS+ configuration file without stopping the **aceserver** process, issue the following command:

   ```
   kill -USR1 (pid)
   ```

   where **(pid)** is the process id of **_sdtacplusd**. This capability is especially useful when modifying the TACACS+ ‘cfg’ table.

Sample TACACS+ Argument File

```
#################################################################
#                   ACE/Server TACACS+ command line argument file
#
#################################################################
# This file or one patterned after it should be kept as sdtacplus.arg
# Customize your TACACS+ application by choosing the desired options
# Specify the name of the optional TACACS+ configuration file. See your
Cisco
# manual for complete details.
-Csdtacplus.cfg
# To make sure that this TACACS+ configuration file has no errors, uncomment
# the following line.  When you run _sdtacplusd, this file will be read and
# processed, but the server will terminate itself afterwards.
# -P
# Disallow TACACS+ forking, thus only runs single threaded
# -g
# Allows the user to specify an alternate prompt string to Enter PASSCODE:
# for password logins. If nothing is specified, displays Enter PASSCODE:
# under current schema
# -mEnter Password:
# Display the version number and exit
# -v
# ======================================================
# Normally, only messages at error level or above are written to syslog.
# To write TACACS+ info messages to the syslog, this option takes a
parameter
# based on a sum of the following options:
#number information about
# 1     general
# 2     parsing
# 4     forking
# 8     authorization
# 16    authentication
# 32    passwords
# 64    accounting
# 128   configuration
# 256   packet
# 512   hex
# 1024  md5 hash
# 2048  xor
# 4096  clean
# 8192  subst
#
# For more information on the various debug flags, see your Cisco manual.
# -d16383
# Write TACACS+ info/debug messages to the console (only when -d set).
# -t
# ================================================
#################################################################
```

Sample TACACS+ Configuration File

The default location and name of the configuration file for TACACS+ is ***ACEDATA*/sdtacplus.cfg**. This file is pointed to by a line in the TACACS+ startup file (***ACEDATA*/sdtacplus.arg)**.

Enter configuration values in the following format (paying special attention to spaces and letter case):

```
#################################################################
#                     ACE/Server TACACS+ configuration file
#
#################################################################
# This file or one patterned after it should be kept as sdtacplus.cfg
# Customize your TACACS+ application by uncommenting the desired lines in
# this file
# Refer to Cisco manual for additional configuration of TACACS+
# The following are examples of different TACACS+ configurations
#
# Encryption key is used to secure communication between sdtacplus daemon
# and NAS and is recommended to be used
# If the following encryption key is used, issue command
# "tacacs-server key your_encryption_key" on the NAS
# key = "your_encryption_key"
#To write all accounting data sent from the access server into file
# /var/tmp/accounting.log on the TACACS+ server uncomment the
# following line
# accounting file = /var/tmp/accounting.log
# default authorization = permit
# Add users: testuser1 - testuser3 to the ACE/Server Database
# to enable SecurID authentication. Also add both the name of your
# router/comm server and the UNIX client to the client table;
# user = testuser1
# {
# member of group secure
# member = secure
# individual user declaration can be used to override the group settings
# for instance the following login selection will override group
# "secure" login
# and will use regular password "whatever" instead of SecurID PASSCODE
# login = cleartext whatever
# following restricted telnet command will allow access only to the range
# of ip addresses from 111.1.1.1 to 111.1.1.9;
# Note: This will deny telnet access to other ip addresses
# Issue command "aaa authorization commands 1 tacacs+ if-authenticated"
# or "aaa authorization commands 15 tacacs+ if-authenticated" on the NAS
#        cmd = telnet
#       {
#       permit "111\.1\.1\.[1-9] "
#       }
# }
# user = testuser2
# {
```

```
# Use DES encrypted password "securid" to login to NAS
# login = des xAWcPaFGcWp8g
# When using PPP to connect to NAS issue following commands first:
# For selected line (ex. line 1) on NAS:
# "autoselect ppp"
# "transport input all"
# "rxspeed 19200"
# "txspeed 19200"
# "modem InOut"
# For selected asynchronous line (ex. interface async 1) on NAS:
# "encapsulation ppp"
# "async default ip address 111.1.1.116"
# "async mode interactive"
# "ppp authentication chap" or "ppp authentication pap"
# If CHAP authentication is used with PPP uncomment the following line;
# chap = cleartext chap_passwd
# When using PPP to connect to NAS issue following commands first :
# For selected line (ex. line 1) on NAS:
# "autoselect ppp"
# "transport input all"
# "rxspeed 19200"
# "txspeed 19200"
# "modem InOut"
#        service = ppp protocol = ip {
# Assign local host the following ip address for PPP negotiations
# addr=111.1.1.116
# }
# }
# user = testuser3
# {
# member = secure
# }
# group = secure
# {
# login = securid
#        cmd = telnet
# {
#
# Deny telnet access to 222.2.(any extension).1
# deny "222\.2\.[0-9]+\.1 "
# Allow telnet to the rest of ip addresses
# permit .*
# }
# }
```

Configuring a Cisco Systems TACACS+ Client Device

Note: If during the configuration you need additional help with TACACS+ commands, type:

```
tacacs ?
```

To configure a Cisco Systems device for TACACS+:

1. Log on to the client device, and enter privileged mode by typing **enable** (and the password, if necessary).

   When the client is protected by RSA SecurID, to enter privileged mode a user must be designated in the RSA Authentication Manager database as a Site Administrator whose Task List includes the ability to edit the client.

2. To review your current configuration, type:

   ```
   show config
   ```

3. Enter Configuration mode from the terminal by typing:

   ```
   config t
   ```

4. Associate the IP address and hostname of the TACACS+ server by typing:

   ```
   ip host hostname ip-address
   ```

   where *hostname* is the name of a host machine with an address of *ip-address*. This step is optional, but if you omit it you must refer to the host by its IP address in all subsequent steps. Subsequent instructions assume that you have made this association. Example:

   ```
   ip host cassatt 192.168.10.23
   ```

   For a Replica Authentication Manager, make the same association for it.

5. Specify that this host is to be used as the TACACS+ server hostname by typing:

   ```
   tacacs-server host hostname
   ```

   If at any time you want to remove TACACS+ and RSA Authentication Manager authentication from the client device, type:

   ```
   no tacacs-server host hostname
   ```

   If you later want to change the host running the server, first remove the hostname, as in the preceding line, then define the new hostname by typing:

   ```
   tacacs-server host newhostname
   ```

6. For a Replica, specify the Replica Authentication Manager hostname using another **tacacs-server host** command.

   The order in which you specify the Authentication Manager hostnames determines the order in which the client device searches for a valid RSA Authentication Manager.

7. Set the number of logon attempts that can be made on a TACACS-protected line. The RSA Authentication Manager default is to allow three attempts before the connection is dropped. The client device has its own retry limit. *The lower of the two limits prevails.*

   Allowing three attempts before disconnection offers a good balance between user convenience and security. Decrease the number for tighter security. However, this makes logging on less convenient for users who mistype their passcode and have to reinitiate a logon session.

   Try increasing the number of retries allowed if you suspect that line noise or heavy network traffic is interfering with the ability of the system to respond appropriately to valid logon attempts. Realize that this value is capped by the RSA Authentication Manager Agent Retry count stored in ***ACEDATA*/sdconf.rec**.

   To set a new value for the number of attempts allowed, type:

   ```
   tacacs-server attempts count
   ```

   where *count* is the number of attempts. To restore the default (3), type:

   ```
   no tacacs-server attempts
   ```

8. Set the retry-control value, which is the number of times the client device searches through the RSA Authentication Manager host list to find an Authentication Manager that is running.

   The default is two tries, which is a good balance between user convenience and security. Decrease the number of allowed attempts for tighter security. However, doing so makes logging on less convenient for users who have to reinitiate a session if no Authentication Manager is found on the first try.

   Increase the number of retries allowed if you suspect that line noise or congestion is interfering with the ability of the system to recognize the existence of an Authentication Manager.

   To set a new value for the number of retries, type:

   ```
   tacacs-server retransmit retries
   ```

   where *retries* is the retransmit count. To restore the default (2), type:

   ```
   no tacacs-server retransmit
   ```

9. Specify the number of seconds the client waits for a response from the RSA Authentication Manager. The default value for a Cisco Systems device is five seconds. However, RSA Security recommends increasing the value to a minimum of 10 seconds to avoid timeouts due to congested or noisy lines, and to ensure better performance during Next Tokencode procedures. Set the value higher than 10 seconds if users experience long delays after entering their passcodes, receive the message **Access Denied**, and are then reprompted for their user name.

   To increase the number of seconds, type:

   ```
   tacacs-server timeout seconds
   ```

   where *seconds* is the time interval.

10. To activate TACACS+ on the device, add

    ```
    aaa new-model
    ```

    List the authentication methods, including RSA SecurID authentication, to be used on each of the lines you want to protect. The syntax is

    ```
    aaa authentication login default [or list_name] method 1
    ... method 4
    ```

    where you can specify any of four methods. Possible values are:

    ```
    tacacs+  use TACACS+
    line     use the line password
    enable   use the enable password
    none     use no authentication
    ```

    RSA Security strongly recommends you avoid using the “none” value.

    Each method is attempted in the order specified, with the next one attempted only if the previous one fails due to a device or network failure, not if the authentication information is invalid. The most secure order is TACACS+ first and the line password second. RSA Security recommends:

    ```
    aaa authentication login securid tacacs+
    aaa authentication login securid2 tacacs+ line
    ```

    The list_name **securid** specifies TACACS+ as the only authentication method. With **securid** specified, users logging on are asked for an RSA SecurID passcode. If this fails, they are denied access.

    The list_name **securid2** specifies TACACS+ as the first authentication method. If there is a failure—for example, if the network connection to the TACACS+ server is not working or the TACACS+ server is not running—the second authentication method in the list_name **securid2** is used. With **securid2** specified, users logging on are asked for an RSA SecurID passcode. If this method fails, they are asked for a password. The valid password is the one specified for the line protected by list_name **securid2**. The use of **securid2** is discussed in the following steps.

    Note: Typing an incorrect passcode during the TACACS+ authentication is called an “error,” not a “failure.” When there is an error in the RSA SecurID authentication information supplied by the user, the subsequent alternate methods of authentication are never invoked.

11. Enable RSA SecurID authentication on the client device lines you want to protect. For the terminal attached to the console port, type:

    ```
    line con 0 password <password>
    login authentication securid2
    ```

    Use the list_name **securid2** only for configuring the console port. When you use **securid2**, access is determined by a password if RSA SecurID authentication fails. If the **aceserver** is not running or the connection is lost to the Authentication Managers, then you as administrator can still log on to the client device through the console port, using the password defined for it.

For the terminal attached to the auxiliary port, type:

```
line aux 0
login authentication securid
```

For the terminals attached to virtual line numbers 0 to ***max***, type:

```
line vty 0 max
login authentication securid
```

The value for ***max*** is determined by the configuration of the client device.

12. To leave a particular virtual line unprotected, configure each line separately. For example, the configuration

```
line vty 0 2
login authentication securid

line vty 3
password xyzzy
login authentication line

line vty 4 max
login authentication securid
```

sets virtual line 3 to use password xyzzy for access. Access to line 3 is not controlled by the RSA Authentication Manager. All other virtual lines in the device require RSA SecurID authentication.

You may want to implement such a configuration in case communication between the device and the RSA Authentication Manager is lost. This is especially important if you have a single Primary with no Replica. If the single Authentication Manager has a serious and long-term hardware failure and all lines are set for RSA SecurID authentication, no one will be able to access the protected device.

If you do choose to leave a line unprotected by RSA Authentication Manager authentication, RSA Security strongly recommends that you protect the line in another way. At a minimum, the terminal attached to the line must be kept in a physically secure area.

13. If you are using a communication server (rather than a router, which has virtual, console, and auxiliary lines), use the following command to provide RSA SecurID authentication for line numbers 0 to ***max***. The value for ***max*** is determined by the configuration of your communication server. Type:

```
line 0 max
login authentication securid
```

You can configure each line separately:

```
line 0
login authentication securid

line 1
login authentication securid2

line 2 max
login authentication securid
```

In the preceding configuration, line 1 is set for TACACS+ RSA SecurID authentication as the primary method and for the line password defined in the list_name **securid2** as the secondary method. Being prompted for a password is useful to you as an administrator if RSA SecurID authentication were to fail because the Authentication Manager was not working or the network connection was broken.

Use the list_name **securid2** only for configuration of the line used by administrators. When you use **securid2**, access is determined by a password if RSA SecurID authentication fails. If the Authentication Manager is not running or the connection to the Authentication Managers is lost, you as administrator can still log on to the client device through this line, using the password defined for it.

14. With TACACS+, messages sent between the client and Authentication Manager can be encrypted so that the messages are not passed as clear text. For communications to be encrypted, add a line similar to the following to the client configuration file:

    ```
    tacacs-server key 1234abcd
    ```

    The **1234abcd** is an example encryption key. Enter the same key that is in the Authentication Manager configuration file and the other TACACS+ clients' configuration files.

    At this point all the new configuration parameters are set and the values are in effect but not saved. You will save the values in step 16. Press CTRL+Z to exit configuration mode.

15. Before saving the configuration, test the options you selected to verify that they are as you intended. For example, perform a series of logons to verify that time-out and retry values are optimal for convenience plus security in your environment.

16. Save the settings by typing:

    ```
    write memory
    ```

    Important: If you do not do this, the settings will be lost if you turn off or unplug the client device.

    To save the configuration values to a remote file, refer to Cisco Systems documentation on the **write network** command.

    Configuration of the TACACS+ client device is now complete. To use the Cisco Systems Accounting or Authorization features, refer to your Cisco Systems configuration manuals.

Protecting Enable Mode

Follow the instructions in this section to protect Enable mode with RSA SecurID. When configuration is complete, a user designated in the RSA Authentication Manager database as a site administrator whose Task List includes the ability to edit the TACACS+ client's Agent Host record may enter Enable mode after being authenticated by RSA SecurID. Non-administrators who attempt to enter Enable mode see an **Enter PASSCODE** prompt but do not gain access. There are two methods of protecting Enable mode:

- Authenticate all users and allow only designated RSA Authentication Manager administrators to enter Enable mode.
- Allow all users to enter Enable mode, but require authentication by RSA SecurID when a user attempts to run a level-15 command.

RSA Security recommends the first method of protection.

Authenticate All Users

In Configuration mode, type:

```
enable password password
aaa authentication enable default tacacs+ enable
```

Now, only site administrators whose Task List includes the ability to edit the client's Agent Host record may enter Enable Mode. Unauthorized users cannot enter Enable mode, even though they see an **Enter PASSCODE** prompt.

If there is a failure in the TACACS+ authentication, such as the RSA Authentication Manager is not running or the connection to the Authentication Managers is lost, the prompt for the Enable password is issued instead.

Authenticate Users Running Level-15 Commands

Type:

```
enable password password
aaa authorization commands 1 tacacs+
```

This way, when a user types **enable**, the user is prompted for the Enable password and is not authenticated by RSA SecurID. However, when a user attempts to run a level-15 command, that user is checked by the TACACS+ authorization protocol only.

To give a user privilege for all commands, enter the following into the TACACS+ configuration file:

```
user username {
default service = permit
}
```

You can place other user-level commands within the braces, but these commands must follow the **default service = permit** line.

6 Installing the Quick Admin Software

This chapter describes how to install the RSA Authentication Manager Quick Admin software. This software enables a system or Help Desk administrator to use a web browser to view and modify user, token, and extension record data in the RSA Authentication Manager Primary database.

For more information about Quick Admin, see the *Administrator's Guide* and the Quick Admin Help.

Quick Admin Architecture

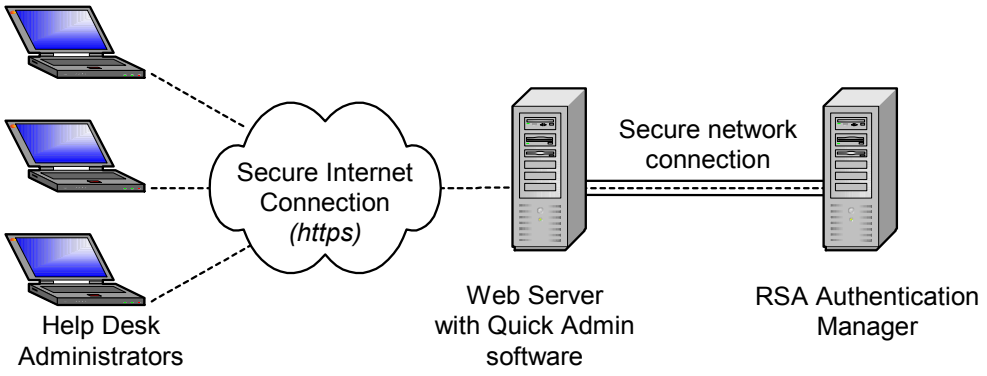
Quick Admin consists of:

- Java servlets accessible through a web server. These are powered by the Apache Jakarta Tomcat 5.5.7 servlet engine.
- A back-end daemon that runs on the RSA Authentication Manager Primary Server. The 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.

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.



System Requirements

Quick Admin users must have Internet Explorer 5.5 (Service Pack 1) or later or Netscape Communicator 6.22 or 7.1 installed on their systems, and the screen resolution must be set to 800 x 600 or higher. In addition, RSA Security recommends that you turn off page caching in the browser.

Windows 2000 and Windows 2003

The following table lists the requirements for installing Quick Admin on Windows 2000 and Windows 2003 machines.

	Windows 2000	Windows 2003
Web Server (Must be JavaScript-enabled)	Internet Information Server (IIS) 5.0	Internet Information Server (IIS) 6.0
Service Pack	Service Pack 4	N/A

RSA Security strongly recommends that you

- Use a secure connection (**HTTPS**) to prevent user names and passwords from being sent in clear text.
- Secure the web server host according to the latest Microsoft guidelines and best practices. For more information about securing IIS, go to Microsoft TechNet at **www.microsoft.com/technet/**.

Solaris

Install Quick Admin only on an UltraSparc system running Solaris 9 with the Java System 6.1 web server (JavaScript-enabled).

RSA Security also strongly recommends that you:

- Use a secure connection (**HTTPS**) to prevent user names and passwords from being sent in clear text.
- Secure your web server host according to the latest Sun Microsystems guidelines and best practices. For more information, go to **http://docs.sun.com/db/prod/s1websrv**.

Pre-Installation Checklist and Tasks

Checklist

Before you begin installing the RSA Authentication Manager Quick Admin software, make sure you have the following files and information:

- ❑ A copy of the **server.cer** file from the **RSA Authentication Manager\data** directory of your RSA Authentication Manager Primary.
- ❑ A copy of the **sdti.cer** file from the **RSA Authentication Manager\data** directory of your Primary.
- ❑ The fully qualified DNS name of your Primary.
- ❑ The IP address of your Primary.
- ❑ The port number on which your Quick Admin daemon (**sdcommd**) is running. The default port is **5570**.

  To change the port assignment, edit the **sdcommdconfig.txt** file (**sdcommd.conf** on Solaris) in the **RSA Authentication Manager\prog** directory.

Tasks

Complete the following tasks on the RSA Authentication Manager Primary host. For more information about these tasks, see the *Administrator's Guide*.

- ❑ Add the following entries to the **hosts.conf** file in the **RSA Authentication Manager\prog** directory: the Quick Admin web server's fully-qualified (DNS) name and IP address, and the host name and IP address. For example,

```
test.rsasecurity.com, 10.1.2.3
test, 10.1.2.3
```

  Note: You must restart the RSA Authentication Manager for the changes to take effect.

- ❑ Set the Administrative Role of each Quick Admin user to **Administrator** and assign the necessary task list.
- ❑ Set the RSA Authentication Manager System Parameters to allow Remote Administration.
- ❑ Verify that the RSA Authentication Manager Quick Admin Daemon is running on the Primary by clicking **Start > Settings > Control Panel > Administrative Tools > Services**.

Installing and Configuring Quick Admin on Windows

To run Quick Admin on a Windows 2000 or Windows 2003 system, you must install the Quick Admin software and configure your Microsoft Internet Information Services (IIS) as described in this section.

Before you begin, make sure that you have installed a supported Microsoft IIS version on your web server host system. Also, verify that no other products using Tomcat are currently installed on the web server host system.

Note: If your web server host has an older version of Quick Admin, you must uninstall the older version before installing the new version. For more information, see "Upgrading to Quick Admin 6.1 from a Previous Version" on page 65. If you want to install both RSA Quick Admin 6.1 and RSA SecurID WebExpress 1.3 on the same web server host, see "Installing Quick Admin and Web Express On the Same System" on page 65. In this case, both products share the same Tomcat servlet engine.

To install the Quick Admin software on Windows 2000 or Windows 2003:

1. Stop the World Wide Web Publishing Service on the web server host.
   For instructions, see your Internet Information Server (IIS) documentation.
2. Insert the CD that contains the Quick Admin software into the CD drive of the web server host, and browse to the **QuickAdmin\Windows** directory on the CD.
3. Double-click the **quickadmin.exe** icon.
   The Quick Admin Setup Wizard opens.
4. Follow the prompts through the Setup Wizard, and then click **Finish**.
   During setup, note that a Windows service named "RSA Web Service" is installed.
5. Depending on your Microsoft IIS version (5 or 6), complete the appropriate IIS configuration procedure in this section.

To configure Microsoft IIS 5 with the Tomcat servlet engine:

1. From the Windows Control Panel, click **Administrative Tools > Internet Information Services (IIS) Manager**.
2. In the IIS window, in the left navigation pane, expand the local computer entry to display the default web site.
3. For the default web site, specify a virtual directory to the Quick Admin application.
   - In the IIS Manager window, in the left navigation pane, right-click the default web site. From the context menu, select **New > Virtual Directory**. This opens the Virtual Directory Creation Wizard.
   - Click **Next**.
   - In the Alias text box, enter "tomcat" as the value, and click **Next**.

- Browse to the ***Quick Admin installation directory*\Tomcat\conf** directory, and click **Next**.
- Select the **Read**, **Run scripts**, and **Execute** options, and click **Next**.
- Click **Finish**.

4. Add the Quick Admin ISAPI Redirector to the default web site.
   - Right-click the default web site and select **Properties** from the context menu.
   - Select the **ISAPI Filters** tab, and click **Add**.
   - Enter "tomcat" as the filter name.
   - Browse to the ***Quick Admin installation directory*\Tomcat\conf** directory, select the **isapi_redirector.dll** file, and click **Open**.
   - Click **OK** to close the Properties dialog box.
5. Start the necessary services on the web server host.
   - From the Windows Control Panel, click **Administrative Tools > Services**.
   - In the Services window, make sure that these three services are started:
     - IIS Admin Service
     - World Wide Web Publishing Service
     - RSA Web Service
   - If any of the three services are stopped, start them.

To configure Microsoft IIS 6 with the Tomcat servlet engine:

1. From the Windows Control Panel, click **Administrative Tools > Internet Information Services (IIS) Manager**.
2. In the IIS window, in the left navigation pane, expand the local computer entry to display the default web site.
3. For the default web site, specify a virtual directory to the Quick Admin application.
   - In the IIS Manager window, in the left navigation pane, right-click the default web site. From the context menu, select **New > Virtual Directory**.
   - Click **Next** in the Virtual Directory Creation Wizard.
   - In the Alias text box, enter "tomcat" as the value, and click **Next**.
   - Browse to the ***Quick Admin installation directory*\Tomcat\conf** directory, and click **Next**.
   - Select the **Read**, **Run scripts**, and **Execute** permissions, and click **Next**.
   - Click **Finish**.
4. Add the Quick Admin ISAPI Redirector to the default web site.
   - Right-click the default web site and select **Properties** from the context menu.
   - Select the **ISAPI Filters** tab, and click **Add**.

- Enter “tomcat” as the filter name.
- Browse to the ***Quick Admin installation directory*****\Tomcat\conf** directory, select the **isapi_redirector.dll** file, and click **Open**.
- Select the **Home Directory** tab, and click **Configuration**.
- In the Application Configuration dialog box, click **Add**.
- Browse to the ***Quick Admin installation directory*****\Tomcat\conf** directory, select the **isapi_redirector.dll** file, and click **Open**.
- In the Extension text box, type:

  ```
  jsp
  ```

  and click **OK**.
- Click **OK** to close the Configuration dialog box.
- Click **OK** again to close the Properties dialog box.

5. Add Tomcat as a web server extension.
   - In the IIS Manager window, in the left navigation pane, right-click Web Service Extensions, and select **Add a new Web service extension** from the context menu.
   - In the Extension name text box, enter “tomcat” as the value, and click **Add**.
   - Browse to the ***Quick Admin installation directory*****\Tomcat\conf** directory, select the **isapi_redirector.dll** file, and click **Open**.
   - Click **OK** in the Add File dialog box.
   - Select the **Set extension status to Allowed** option.
   - Click **OK**.
6. Start the necessary services on the web server host.
   - From the Windows Control Panel, click **Administrative Tools > Services**.
   - In the Services window, locate these three services:
     - IIS Admin Service
     - World Wide Web Publishing Service
     - RSA Web Service
   - If any of the three services are not running, start them.

After you finish configuring Microsoft IIS, the RSA Authentication Manager Quick Admin application is ready to use.

To log on to Quick Admin, point your web browser to **https://*servername*/quickadmin/**, where *servername* is the name of the web server host.

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**.

Installing and Configuring Quick Admin on Solaris

To run Quick Admin on a Solaris 9 system, you must install the Quick Admin software and configure your Sun Java Systems web server as described in this section.

Before you begin, make sure that you have installed a supported Sun Java Systems web server on your web server host system. Also, verify that no other products using the Tomcat servlet engine are currently installed on the web server host system.

Note: If your web server host has an older version of Quick Admin, you must uninstall the older version before installing the new version. For more information, see "Upgrading to Quick Admin 6.1 from a Previous Version" on page 65. If you want to install both RSA Quick Admin 6.1 and RSA SecurID WebExpress 1.3 on the same web server host, see "Installing Quick Admin and Web Express On the Same System" on page 65. In this case, both products share the same Tomcat servlet engine.

To install Quick Admin on Solaris:

1. Stop all web services on the web server.
2. Insert the CD that contains the Quick Admin software into the CD drive of the web server host.
3. Change to the following directory on the CD.

   `/cdrom/cd_name/QuickAdmin/UNIX`
4. Type:

   `./quickadmin.sh`

   The Quick Admin setup script starts.
5. Follow the instructions on your screen.
6. After the installation script finishes, you must configure your web server with Tomcat as described in the following procedure.

To configure the Java System (SunOne) 6.1 web server for Quick Admin:

1. Change to the ***web server installation directory*/https-*hostname*/config** directory.
2. Using a text editor, open the **magnus.conf** file, and enter the following lines of data at the end of the file:

   ```
   Init fn="load-modules" funcs="jk_init,jk_service"
   shlib="Quick Admin Install Dir/Tomcat/conf/nsapi_redirector.so"

   Init fn="jk_init" worker_file="Quick Admin Install Dir/
   Tomcat/conf/workers.properties" log_level="error"
   log_file="Quick Admin Install Dir/Tomcat/logs/nsapi.log"
   ```
3. Save the changes and close the **magnus.conf** file.

4. Open the **obj.conf** file, and enter the following lines of data immediately after the tag <**Object name="default"**>:

```
NameTrans fn="assign-name" from="/quickadmin"
name="rsaweb"

NameTrans fn="assign-name" from="/quickadmin/*"
name="rsaweb"

NameTrans fn="assign-name" from="/jsp-examples"
name="rsaweb"

NameTrans fn="assign-name" from="/jsp-examples/*"
name="rsaweb"

NameTrans fn="assign-name" from="/servlets-examples"
name="rsaweb"

NameTrans fn="assign-name" from="/servlets-examples/*"
name="rsaweb"
```

5. At the end of **obj.conf** file, add the following lines:

```
<Object name="rsaweb">

ObjectType fn=force-type type=text/plain

Service fn="jk_service" worker="RSAWorker"

</Object>
```

6. Save the changes and close the **obj.conf** file.
7. Change to the ***Quick Admin installation directory*/Tomcat/bin** directory, and start Tomcat with following command:

```
./startup.sh
```

8. Start your Java Systems (SunOne) web server.

The RSA Authentication Manager Quick Admin is now installed and configured on your Solaris web server host.

To log on to Quick Admin, browse to **https://*servername*/quickadmin/**, where *servername* is the name of the web server host.

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**. Also, RSA Security strongly recommends that, if you need to stop and restart Tomcat, you also stop and restart the Java Systems (SunOne) web server.

Upgrading to Quick Admin 6.1 from a Previous Version

Depending on your platform, use one of the following procedures to upgrade from Quick Admin 5.2 or 6.0 to Quick Admin 6.1.

On a Windows Machine

To upgrade Quick Admin on a Windows machine:

Note: Make sure no administrators are using the Quick Admin directories while you perform the upgrade.

1. Uninstall Quick Admin 5.2 or 6.0 completely from your web server host.

   RSA Security recommends that you stop all services related to Quick Admin before uninstalling. For complete instructions, see the *RSA ACE/Server 5.2 for Windows Installation Guide* or *RSA Authentication Manager 6.0 for Windows Installation Guide*.

2. Install Quick Admin 6.1 as described in "Installing and Configuring Quick Admin on Windows" on page 60.

On a Solaris Machine

To upgrade Quick Admin on a Solaris machine:

Note: Make sure no administrators are using the Quick Admin directories while you perform the upgrade.

1. Uninstall Quick Admin 5.2 or 6.0 from your web server host.

   RSA Security recommends that you stop all services related to Quick Admin before uninstalling. For complete instructions, see the *RSA ACE/Server 5.2 for UNIX Installation Guide* or *RSA Authentication Manager 6.0 for UNIX Installation Guide*.

2. Install Quick Admin 6.1 as described in "Installing and Configuring Quick Admin on Solaris" on page 63.

Installing Quick Admin and Web Express On the Same System

Both Quick Admin 6.1 and Web Express 1.3 use the Apache Software Foundation Tomcat 5.5.7 servlet engine, and can run on the same web server host. When running on the same host, these applications share the same version of Tomcat.

For information about installing and configuring Web Express 1.3, see the *RSA Web Express 1.3 Installation and Configuration Guide* for your platform.

Important: Earlier versions of Quick Admin and Web Express use the Macromedia Inc. JRun servlet engine and are incompatible with the new Tomcat-based versions. Make sure to uninstall older versions of Quick Admin and Web Express from the web server host before you install the new versions. For information about uninstalling older versions of Quick Admin, see the *RSA ACE/Server 5.2 Installation Guide* or *RSA Authentication Manager 6.0 Installation Guide* for your platform. For information about uninstalling older versions of Web Express, see the *RSA Web Express Installation and Configuration Guide* for your platform and version.

Depending on your platform, use one of the following procedures to install Quick Admin 6.1.

On a Windows Machine

To install Quick Admin 6.1 on Windows when Web Express 1.3 is already installed:

1. From the Windows Control Panel, click **Administrative Tools > Services**, and stop the following services on the web server host:
   - World Wide Web Publishing Service
   - RSA Web Service
2. Insert the CD that contains the Quick Admin software into the CD drive of the web server host, and browse to the **QuickAdmin\Windows** directory on the CD.
3. Double-click the **quickadmin.exe** icon.
   The Quick Admin Setup Wizard opens.
4. Follow the prompts through the Setup Wizard, and then click **Finish**.
5. From the Windows Control Panel, click **Administrative Tools > Services**, and restart the following services on the web server host:
   - World Wide Web Publishing Service
   - RSA Web Service

On a Solaris Machine

To install Quick Admin 6.1 on Solaris when Web Express 1.3 is already installed:

1. Stop all web services on the web server.
2. Insert the CD that contains the Quick Admin software into the CD drive of the web server host.
3. Change to the following directory on the CD.

   ```
   /cdrom/cd_name/QuickAdmin/UNIX
   ```

4. Type:

   ```
   ./quickadmin.sh
   ```

   The Quick Admin setup script starts.

5. Follow the instructions on your screen.
6. Restart all web services on the web server.

Changing Quick Admin Configuration Settings

If you need to make changes to your Quick Admin environment, you must edit the **quickadminconfig.properties** file. By default, this file resides in the ***Quick Admin installation directory*\Tomcat\webapps\quickadmin\WEB-INF\properties** directory.

The following tables summarize the parameters that you can modify. Many of these values were set during installation and should be modified with caution. In addition, RSA Security strongly recommends against modifying parameters in the **##DO NOT MODIFY##** section of the properties file.

Directory paths in the tables are relative to the ***Quick Admin installation directory*\Tomcat\webapps\quickadmin** directory.

Note: If you make changes to the **quickadminconfig.properties** file, you must stop and restart RSA Web Services (Tomcat) for the changes to take effect.

Quick Admin Configuration Settings

Parameter	Value
ACE_SERVER	The fully qualified name of the RSA Authentication Manager Primary.
ACE_IP	The IP address of the RSA Authentication Manager Primary.
CERT_PATH	The directory path that contains copies of the **sdti.cer** and **server.cer** files from your RSA Authentication Manager Primary. The default path is **certs/**. For instructions on adding certificates from more than one Primary, see "Administering Multiple Primary Servers" on page 73.
ACE_PORT	The Primary TCP port on which the RSA Authentication Manager Quick Admin daemon is listening. The default port is **5570**.
REPORT_PATH	The directory path where Quick Admin writes report files. The default path is **reports/**. **Important:** Because each report generates a new text file, RSA Security recommends that you clean out the **reports** directory periodically to conserve disk space.
PROP_PATH	The directory path that contains the **quickadminconfig.properties** file. The default path is **properties/**.

Parameter	Value
MAX_SEARCH	The maximum number of objects (user records, token records, and so on) that are returned when a user searches the RSA Authentication Manager database. This value greatly affects the performance of the Quick Admin application while users are searching. If the value is set very high, the application performs poorly. The default value for this parameter is **150**.
MAX_REPORT	The maximum number of objects (user records, token records, and so on) that are returned when a user generates a report. This value greatly affects the performance of the Quick Admin application while users are generating reports. If the value is set very high, the application performs poorly. The default value for this parameter is **300**.
HTML_SRC	The directory path that contains the HTML templates that the Quick Admin application uses to create the forms that users see. The default path is **quickadmin/**. **Note: quickadmin/** *is not* relative to the ***Quick Admin installation directory*\Tomcat\webapps\quickadmin** directory.

Password Token Lifetimes Settings

Note: The value you set for each password parameter can change the meaning of the values you set for other password parameters. For more information, see "How Password Token Lifetime Settings Affect Each Other" on page 70.

Parameter	Value
USER_PWD_LIFETIME_DAYS USER_PWD_LIFETIME_HOURS	Determine the number of days and hours before user passwords expire. You can set days, hours, or both. For example, if USER_PWD_LIFETIME_DAYS=5 and USER_PWD_LIFETIME_HOURS=3, the user password expires in 123 hours. Acceptable values: 0-8760 days, 0-23 hours The combined number of hours and days can equal no more than 8760 days, or 24 years. The default values for these parameters are USER_PWD_LIFETIME_DAYS=30 USER_PWD_LIFETIME_HOURS=0

Parameter	Value
LOST_TOKEN_CONTROL_FLAG	Determines whether the days and hours set for lost token user passwords can be changed in the Quick Admin interface. If set to **fixed**, the days and hours cannot be changed in the interface. If undefined or commented out, the days and hours can be changed in the interface. By default, this parameter is undefined.
LOST_TOKEN_PWD_LIFETIME_DAYS LOST_TOKEN_PWD_LIFETIME_HOURS	Determine the number of days and hours before user passwords issued to replace lost tokens expire. You can set days, hours, or both. This setting applies to both fixed and one-time passwords. For example, if LOST_TOKEN_PWD_LIFETIME_DAYS=5 and LOST_TOKEN_PWD_LIFETIME_HOURS=3, the user password expires in 123 hours. Acceptable values: 0-8760 days, 0-23 hours The combined number of hours and days can equal no more than 8760 days, or 24 years. The default values for these parameters are LOST_TOKEN_PWD_LIFETIME_DAYS=7 LOST_TOKEN_PWD_LIFETIME_HOURS=0 For more information about temporary passwords to replace lost tokens, see the *Administrator's Guide*.
FIXED_PWD_LIFETIME_DAYS FIXED_PWD_LIFETIME_HOURS	Determine the number of days and hours before fixed passwords issued to replace lost tokens expire. Fixed passwords can be used repeatedly until they expire. This parameter set gives you the option to override the LOST_TOKEN_PWD_LIFETIME_DAYS and LOST_TOKEN_PWD_LIFETIME_HOURS parameters as they apply to fixed passwords. You can set days, hours, or both. For example, if FIXED_PWD_LIFETIME_DAYS=5 and FIXED_PWD_LIFETIME_HOURS=3, the user password expires in 123 hours. Acceptable values: 0-8760 days, 0-23 hours The combined number of hours and days can equal no more than 8760 days, or 24 years. The default values for these parameters are FIXED_PWD_LIFETIME_DAYS=7 FIXED_PWD_LIFETIME_HOURS=0

Parameter	Value
OTP_PWD_LIFETIME_DAYS OTP_PWD_LIFETIME_HOURS	Determine the number of days and hours before one-time password (OTP) sets issued to replace lost tokens expire. One-time passwords can be used only one time each and expire on a specified date. You can set days, hours, or both. This parameter set gives you the option to override the LOST_TOKEN_PWD_LIFETIME_DAYS and LOST_TOKEN_PWD_LIFETIME_HOURS parameters as they apply to OTP. For example, if OTP_PWD_LIFETIME_DAYS=5 and OTP_PWD_LIFETIME_HOURS=3, the user password expires in 123 hours. Acceptable values: 0-8760 days, 0-23 hours The combined number of hours and days can equal no more than 8760 days, or 24 years. The default values for these parameters are OTP_PWD_LIFETIME_DAYS=7 OTP_PWD_LIFETIME_HOURS=0

How Password Token Lifetime Settings Affect Each Other

The value you set for each password parameter can change the meaning of the values you set for other password parameters. The following table describes how the settings for each password parameter affect each other.

Which parameters are defined	LOST_TOKEN_CONTROL_FLAG set to FIXED	LOST_TOKEN_CONTROL_FLAG undefined
None	Default values apply	Default values apply
LOST	Values defined for LOST apply to FIXED and OTP	Values defined for LOST apply to FIXED and OTP
LOST FIXED	Values defined for LOST apply to OTP	Values defined for FIXED apply to OTP
LOST OTP	Values defined for LOST apply to FIXED	Values defined for LOST apply to FIXED and OTP
LOST FIXED OTP	Values defined for FIXED and OTP override values defined for LOST	Values defined for FIXED apply to OTP
FIXED	Default values apply to OTP	Values defined for FIXED apply to OTP
OTP	Default values apply to FIXED	Default values for LOST apply to FIXED and OTP

Quick Admin Timeout Settings

Parameter	Value
ACE_REPLY_TIMEOUT	Indicates how long Quick Admin waits for a response from the RSA Authentication Manager before returning an error message. Maximum value: 2147483647 The value is in milliseconds (100 = 1 second.) The default is 60000.
ACE_REPLY_RETRY	Indicates how often Quick Admin checks for a response from the RSA Authentication Manager. Maximum value: 2147483647 The value is in milliseconds (100 = 1 second.) The default is 500.

Debugging On/Off Settings

Parameter	Value
Verbose	Determines whether or not debugging information about Quick Admin and its communications with the RSA Authentication Manager are written to the log file (**catalina.out** on Solaris and **stdout**_*date*.**log** on Windows). The Verbose flag overrides all other *_Verbose flags. To prevent the Verbose flag from overriding the *_Verbose flags, insert a pound sign (#) at the beginning of the line. For example, `#Verbose=no` The log file is usually in the ***Quick Admin installation directory*****Tomcat\logs** directory. Note that the log file grows very quickly. If you turn on debugging, be sure to monitor it. The default value for this parameter is **no**.
Init_Verbose	Determines whether or not debugging information from the Quick Admin startup routines are written to the log file (**catalina.out** on Solaris and **stdout**_*date*.**log** on Windows). Note that the Verbose flag overrides all other *_Verbose flags. The default value for this parameter is **no**.
Login_Verbose SearchPage_Verbose EditToken_Verbose EditUser_Verbose Report_Verbose EditExtension_Verbose	These parameters determine whether or not debugging information from activities related to the corresponding Quick Admin forms are written to the log file (**catalina.out** on Solaris and **stdout**_*date*.**log** on Windows). Note that the Verbose flag overrides all other *_Verbose flags. For example, entering **yes** for the **EditUser_Verbose** parameter results in information about actions a user performs on the Edit User form being written to the file. The default value for these parameters is **no**.

Changing RSA Authentication Manager Communication Settings

Communication between the RSA Authentication Manager Primary and the Quick Admin server is controlled by settings in a configuration file on the Primary.

- If your RSA Authentication Manager Primary is running on Windows, the settings are in the **RSA Authentication Manager\prog\sdcommdconfig.txt** file**.**
- If your RSA Authentication Manager Primary is running on UNIX, the settings are in the **RSA Authentication Manager/prog/sdcommd.conf** file.

The following table explains the settings in the configuration file.

Parameter	Value
Windows port (TCP Port on UNIX installations)	TCP port on which the RSA Authentication Manager Quick Admin Daemon is running on the Primary. The default value is **5570**.
Verbose	Determines whether or not detailed logging messages are written to the Windows Event Viewer or UNIX **syslog**. The default value is **no**.
Inactivity TimeOut	Controls the time-out for Quick Admin sessions. If a user leaves a Quick Admin session open for the specified duration, the session is closed automatically. The inactivity parameter must be specified in minutes. The default value is **15**. **Important:** The **Inactivity TimeOut** value **must** be larger than the Tomcat session time-out value. You set the session time-out value in the ***Quick Admin installation directory*\Tomcat\conf\web.xml** file or in the ***Quick Admin installation directory*\Tomcat\webapps\quickadmin\WEB-INF\web.xml** file. (If you insert a session time-out value in both files, and they are different, preference is given to the setting in the second file.) Setting a session time-out value ensures that the session times out before the RSA Authentication Manager Quick Admin daemon on the Primary Server. Without a session time-out, Quick Admin users can experience terminated sessions.

Administering Multiple Primary Servers

Quick Admin supports administering more than one RSA Authentication Manager Primary through a single Quick Admin server.

To use Quick Admin with multiple Primary Servers:

1. Create a new subdirectory for each Server under the ***Quick Admin installation directory*\Tomcat\webapps\quickadmin\WEB-INF\certs** directory. You must create a subdirectory for each Primary you want to administer.

   The subdirectories must have the same name as the Primary host name. For example, to enable Quick Admin for Servers **cassatt** and **vermeer**, create subdirectories named **cassatt** and **vermeer**.

2. Obtain copies of the **sdti.cer** and **server.cer** certificate files from the **RSA Authentication Manager\data** directory of each Server, and place them in the appropriate subdirectories under **certs**. For example, certificate files from Server **cassatt** must be copied into the **cassatt** subdirectory.

3. When you log on to Quick Admin, enter the Server name in the **Realm** box of the logon page.

   Quick Admin connects to the Primary you specified. If you do not specify a Primary, Quick Admin connects to the Primary that you specified during the Quick Admin installation.

Uninstalling Quick Admin

Depending on your platform, to uninstall Quick Admin, refer to one of the following sections.

From a Windows Machine

To remove the Quick Admin software from a Windows machine:

1. From the Windows Control Panel, double-click **Add/Remove Programs**.
2. Select **RSA Quick Admin 6.1**, and click **Remove**.

   The Quick Admin Setup Wizard opens.
3. Select **Complete Uninstall**, and click **Next**.

   Important: If Web Express 1.3 is installed, and you do not want it uninstalled during this process, select **Undeploy RSA Quick Admin 6.1** instead of **Complete Uninstall**.

4. Follow the prompts through the Setup Wizard, then click **Finish**.
5. Restart the system.

To remove Quick Admin entries from IIS:

Important: If you want Web Express 1.3 to remain installed on this web server, do not perform this procedure.

1. From the Windows Control Panel, click **Administrative Tools > Internet Information Services (IIS) Manager**.
2. In the IIS window, in the left navigation pane, expand the local computer entry to display the default web site, and click the default web site to expand it.
3. Under the default web site, right-click the **tomcat** item, and select **Delete** from the context menu.
4. In the IIS window, in the left navigation pane, right-click the default web site, and select **Properties** from the context menu.
5. Select the **ISAPI Filters** tab.
6. Select the **tomcat** filter in the list, and click **Remove**.
7. Click **OK**.
8. Close the Internet Information Services Manager.

From a Solaris Machine

To remove the Quick Admin software from a Solaris machine:

1. Stop the Tomcat servlet engine.
   - Change to the directory ***Quick Admin installation directory*/Tomcat/bin**.
   - Type:

     ```
     ./shutdown.sh
     ```
2. Remove Quick Admin.
   - Change to the parent directory above the Quick Admin installation directory.
   - Type:

     ```
     rm -rf Quick Admin installation directory
     ```

A Migrating Your RSA RADIUS Server

This appendix describes how to

- Migrate from previous versions of RSA RADIUS Server to RSA RADIUS Server 6.1 as part of the upgrade to RSA Authentication Manager 6.1
- Convert existing RSA RADIUS user extension data to the format that RSA RADIUS Server 6.1 requires

Migrating to RSA RADIUS Server 6.1

This section lists the tasks you need to perform to migrate your pre-6.1 RSA RADIUS Server to RSA RADIUS Server 6.1 as part of an upgrade to RSA Authentication Manager 6.1.

To migrate to RSA RADIUS 6.1:

1. If you have user extension data associated with your RSA RADIUS users, run a test conversion. For instructions, see "Running a Test Conversion" on page 76.
2. If you have configured prompts for the RSA RADIUS Server, back up the appropriate ***ACEDATA*\radius.cfg** file.
3. Upgrade the Primary Authentication Manager. For instructions, see "Preparing for the Primary Upgrade" on page 36 and then "Upgrading a Primary" on page 37.
4. Copy the **radius.cfg** file into the ***ACEDATA*** directory on the Primary.
5. If you have user extension data associated with your RSA RADIUS users, run a full conversion. For instructions, see "Running a Full Conversion" on page 77.
6. Upgrade the Replica Authentication Manager. For instructions, see "Preparing for a Replica Upgrade" on page 38 and then "Upgrading a Replica" on page 38.
7. Install RSA RADIUS Server 6.1. For instructions, see the *RSA RADIUS Server 6.1 Administrator's Guide*.

Converting Your RSA RADIUS User Extension Data

Extension records enable you to define and manage additional database information that is useful to your organization but is not required to run Authentication Manager programs. This customer-defined information is called extension data.

RSA RADIUS Server 6.1 requires a format for user extension data that differs from previous versions of the RSA RADIUS Server. Previously, the key portion of the user extension data could be any string. In 6.1, the key must be in the following format:

ATTR<*valid attribute number*>_<*unique identifier*>

For more information about the new format, see the Help.

If you have RADIUS-specific user extension data that you want to migrate to RSA RADIUS 6.1, you must convert the data format using the **rsaextconv** program. The **rsaextconv** program is a command-line utility that

- Creates new extension keys based on the keys in your current installation
- Points the profile links to the new extension keys
- Removes the old extension keys

Running a Test Conversion

The test conversion shows you the changes that will be made to the user extension information in your database without actually making the changes. This enables you to manually resolve any existing issues.

Important: RSA Security strongly recommends that you perform a test conversion on your existing user extension data *before* you upgrade to RSA Authentication Manager 6.1. Once you upgrade to RSA Authentication Manager 6.1, you do not have the ability to edit attribute-value pairs in RADIUS Server profiles.

In addition, running the test version gives you an idea of how much downtime to plan for your RADIUS users after you upgrade to RSA Authentication Manager 6.1.

To run a test conversion through Remote Administration:

1. Open a Remote Administration session for the appropriate server, and insert the RSA Authentication Manager 6.1 CD into the CD drive.
2. Click **File > Run Custom 4GL**.
3. Browse to **<*CD drive*>:\aceserv\windows\rsaextconv.p**, and click **OK**.

The sample results of the test conversion are logged in ***ACEPROG*\progui\rsaextconv.log**. When you are satisfied with the results, upgrade to RSA Authentication Manager 6.1, after which you can perform a full conversion.

Running a Full Conversion

After you have upgraded to RSA Authentication Manager 6.1, but before you install RSA RADIUS Server 6.1, perform a full conversion by running the **rsaextconv** program.

Note: If you did not perform a test conversion before upgrading to RSA Authentication Manager 6.1, you can perform one using the following command:

```
ACEPROG/rsaextconv -f -d
```

The sample results are logged in ***ACEPROG*\rsaextconv.log**. Note that once you upgrade to RSA Authentication Manager 6.1, you no longer have the ability to edit attribute-value pairs in RADIUS Server profiles.

To run a full conversion on RSA Authentication Manager 6.1:

The command to run a full conversion is

```
ACEPROG/rsaextconv -f -e
```

The sample results are logged in ***ACEPROG*\rsaextconv.log**.

Troubleshooting

The following table provides possible solutions for the four categories of error messages you might encounter when running the **rsaextconv** program.

Error Message Topic	Possible Solutions
Database-related	• 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**. • Check your network connection. If neither solution helps, you may be experiencing database corruption. Contact RSA Security Customer Support.
Parameter-related	Review the instructions in "Running a Full Conversion" on page 77, and try the procedure again.
Server Identity-related	Verify that the Server information matches in the following areas: • Network identity • Replica Table • Configuration Record
Log File-related	• Make sure the disk is not full • Make sure you have the correct permissions

B Modifying Kernel Parameters

The RSA Authentication Manager requires shared memory resources from the UNIX operating system. If your system does not meet the minimum requirements listed in the parameter tables found in this appendix, you must modify the UNIX kernel configuration values.

Use the directions in this appendix or in the documentation for your operating system to bring the UNIX resource settings up to the minimum values required for RSA Authentication Manager installation and operation. You may need to increase the values to allow additional administration connections to the RSA Authentication Manager database. Additional connections to the database allow you to run more Remote Administration and RSA Quick Admin sessions.

The minimum values listed in this appendix are based on the assumption that the Authentication Manager is dedicated to running RSA Authentication Manager software.

Once the system is installed and running, it should not report system resource errors. If it does, however, perform these steps again and increase by 50 percent any setting that is identified as too low in the error message. Repeat this procedure again if necessary. Parameter names are case sensitive, so be sure you specify or search for them exactly as they appear in the tables.

Perform all instructions in this section when you are logged on as the **root** user on the console.

Note: No kernel modifications are required on Red Hat Enterprise LINUX 3.0.

Modifying Kernel Parameters for HP-UX

To modify kernel parameters for HP-UX:

1. Make a backup copy of your current kernel configuration.
2. Put the system into single user mode, using the following command:

   ```
   shutdown
   ```

   Users must not be on the system while you are reconfiguring the kernel.
3. Run the HP-UX system administration utility. Choose the specified menu picks:

   ```
   sam
   Kernel Configuration ->
   Configurable Parameters ->
   ```

4. Once you are in the Configurable Parameters list, modify the kernel parameters, checking the value for each of the parameters. Make modifications as required to specify the minimum required values for each parameter, or the values for allowing more administration connections to the database.

   Note: RSA Security recommends 16 as the value for the semmni parameter. The RSA Authentication Manager requires three sets of semaphores, so you may need to set the value of this parameter higher depending upon your operating system configuration.

Parameter	Minimum Value
nproc	640
shmmni	64
shmseg	16
shmmax	16777216
semmni	16
semmns	500
semmnu	500
max_threads_proc	300

   Highlight the parameter you want to change, and select **Modify Configurable Parameter** from the Actions menu. A dialog box opens, prompting you to enter the new value for the parameter.

   ```
   highlight parameter
   Actions -> Modify Configurable Parameter
   ```

5. Compile the new kernel by selecting **Create a New Kernel** from the Actions menu. You are prompted to build the kernel and start the computer. Answer **Yes**. The old kernel is automatically backed up as **/SYSBCKUP**.

   ```
   Actions -> Create a New Kernel
   Should the system be rebooted?   Yes
   ```

Modifying Kernel Parameters for IBM AIX

To modify kernel parameters for IBM AIX:

1. Set the **fsize** value to **4194303** by editing the **/etc/security/limits** with a text editor. The following example uses the "vi" editor:

   ```
   vi    /etc/security/limits
   ```

2. Log off the system and log back on for the modification to take effect. There is no need to start the system.

   You may want to edit the **fsize** for the RSA Authentication Manager file owner only.

Modifying Kernel Parameters for Solaris

Although you do not have to set the system into single-user mode, there must be no other users on the system during the kernel reconfiguration.

To modify kernel parameters for Solaris:

1. Copy the current version of the configuration file to preserve your current kernel configuration parameters.

   ```
   cp    /etc/system    /etc/system.old
   ```

   If you need to return to your current kernel configuration, you must restore this saved file and start your system as shown in step 5.

2. The Solaris kernel is dynamically configured. Editing the configuration file changes the kernel configuration. Modify the kernel configuration file using a text editor of your choosing. The following example uses the "vi" editor:

   ```
   vi    /etc/system
   ```

3. Check that all parameters listed in the following table are set to at least the minimum values.

Note: RSA Security recommends 16 as the value for the semmni parameter. The RSA Authentication Manager requires three sets of semaphores, so you may need to set the value of this parameter higher depending upon your operating system configuration

Parameter	Minimum Value
shmsys:shminfo_shmmni	64
shmsys:shminfo_shmseg	16
shmsys:shminfo_shmmax	16777216
semsys:seminfo_semmni	16
semsys:seminfo_semmsl	200
semsys:seminfo_semmns	500
semsys:seminfo_semmnu	500

For example, for the **shmsys:shminfo_shmmni** parameter, you could find a line such as

```
set shmsys:shminfo_shmmni=64
```

4. Make sure there are no other users on the system.
5. Shut down the computer, and start it at the **OK** prompt. Type:

```
reboot
```

C Transferring the RSA Authentication Manager from UNIX to Windows

To transfer the RSA Authentication Manager from Windows to UNIX:

1. Perform a new installation of the RSA Authentication Manager 6.1 on a UNIX machine. For instructions, see Chapter 1, "RSA Authentication Manager Requirements."

   After installation, the database on the UNIX machine contains one record, which is a user record for the administrator who installed the RSA Authentication Manager 6.1 software.

2. On the existing Windows Primary Authentication Manager, stop the RSA Authentication Manager services.
   - Click **Start** > **Programs** > **RSA Security> RSA Authentication Manager Control Panel**.
   - In the RSA Authentication Manager dialog box, under RSA Authentication Manager, click **Stop**.
   - When the RSA Authentication Manager stopped message appears, click **OK**.
   - When the Database Broker stopped message appears, click **OK**.

     If the Broker Connections dialog box opens, click **Yes**.
   - To close the Control Panel, click **OK**.
3. Create a dump file of the Authentication Manager database.
   - Click **Start > Programs > RSA Security >** RSA Authentication Manager **Database Tools > Dump** (or, in the ***ACEPROG*** directory, double-click **sddump.exe**).

     The Database Dump dialog box opens.
   - Select **Dump Server Database** to indicate that you want to create a Authentication Manager dumpfile.
   - Click **OK**.

   A file named **sdserv.dmp** is created in the ***ACEDATA*** directory.
4. Click **Close** when the dump completes.
5. Create a **/dump** directory on your UNIX system.
6. Copy the **sdserv.dmp** and **license.rec** files from the Windows system running the RSA Authentication Manager to the **/dump** directory. If you use **ftp** to transfer the files, copy them in binary mode.

   Note: Do not copy these files to the ***ACEDATA*** directory on the Primary.

Your UNIX system now contains the dump files. You are ready to load the dump files.

To load the dump files:

Important: Make sure no administration sessions are connected to the database, and notify any remote administrators of the impending shutdown.

1. Verify that no RSA Authentication Manager processes are running on the Primary. Type:

   ```
   ./aceserver stop
   ./sdconnect stop
   ```

2. Load the Authentication Manager database dump file on the UNIX Server. Type:

   ```
   ./sdload -s -m -k /dump/license.rec
   ```

3. In the **Path of server dump file** field, either specify the path for the dump file and **license.rec** file, or browse to their directory.
4. Under server Database Load Options, select **Server dump file has a different license record than the current database** and **Merge records from server dump file with records in current database**.

   Important: RSA Security strongly recommends that you back up your current database before performing a Database Load in Merge mode. For more information about the Merge option, see "Merge Logic" on page 91.

5. Click **OK**.

   The **sdload.exe** program loads the dump files into the RSA Authentication Manager 6.1 database.
6. Click **Close**.

Note: The RSA Authentication Manager 6.1 UNIX machine is automatically added to the RSA Authentication Manager 6.1 Windows machine as a Replica. To delete it, click **Start > Programs > RSA Security > RSA Authentication Manager Configuration Tools > RSA Authentication Manager Replication Management**.

D Database Utilities

This appendix describes the utilities that you use to perform installation and administration tasks on the Primary Authentication Manager. The utilities are:

- The database administration application **sdadmin**.
- The database utilities (**sddump, sdload**, **sdnewdb** and **dumpreader**). Respectively, these utilities enable you to dump an existing database, load a dumped database, create a new empty database, and convert a dump file to one of several readable formats.

There are additional utilities described in other parts of the documentation:

sdsetup -config. You can edit the configuration record on the Primary. For more information, see the appendix "Configuring the RSA Authentication Manager (UNIX)," in the *Administrator's Guide.*

sdsetup -repmgmt. You can perform the following tasks:

- Add or delete a Replica.
- Display information about the Authentication Managers in your realm.
- Mark a Replica that requires a new database.
- Create a Replica Package.
- Nominate a Replica to replace the Primary. See the *Administrator's Guide*.

loadsamusers. You can move user information from an existing SAM (Security Account Manager) database on a Windows system to the RSA Authentication Manager database. For more information on this utility, see Appendix F, "Creating User Records from a SAM Database."

sdaceldap. You can create and update RSA Authentication Manager user records with information from an LDAP directory. For more information on this utility, see the *Administrator's Guide*.

Using sdadmin

The **sdadmin** program can be run on a UNIX Primary by one or more authorized administrators. A passcode is not required to run **sdadmin**. Instead, the program checks the user record for RSA Authentication Manager administrator privilege. If a non-administrator tries to run **sdadmin**, the program will not start and a message that includes the user's name is logged.

Whoever runs **sdadmin** for the first time must log on as the RSA Authentication Manager fileowner specified during installation. If you do not know which account was specified, run **sdinfo** and look at the File Ownership line.

If you already have an RSA Authentication Manager database set up with administrators registered, you can run **sdadmin** from the account of one of these administrators if the account has the same UNIX group ID (GID) as the RSA Authentication Manager file owner.

Note: While the **sdadmin** program allows you to 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.

Before you begin, read the following section "Interface Conventions" to learn how to run the program and to become familiar with its interface conventions.

Interface Conventions

- Enter the menu bar by pressing the F3 or PF3 key.
- 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 pressing ENTER.
- Actions in an option box can be initiated with a keystroke only in the currently active area of the box. A rectangle highlights this area of focus.
- To move forward from one area of an option box to another, press the TAB key. To move backwards, press CTRL+U.
- To move from item to item within an area, use the arrow keys.
- When the focus is on a list item, a radio button, or a checkbox, select it by pressing the spacebar. In a list, the arrow keys also can be used to highlight an item (except for the first item, which is highlighted when you first enter the list, you must use the spacebar to select it).
- Pressing ENTER initiates the action of whichever button is highlighted. If focus has not been taken off the default action button (frequently the **OK** button, which may close the dialog box), that action will be carried out when you press ENTER.
- Pressing ENTER in a fill-in field is equivalent to pressing TAB.
- If the focus is on a checkbox or radio button, pressing ENTER turns it on or off.
- When you click a **Cancel** button or press the F4 or PF4 keys, you are canceling any modification made in the dialog box that has not been saved already. These actions also close the 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.
- When buttons are not available, they look the same but cannot be selected (the cursor will not move to the button).
- To exit **sdadmin**, select **Exit** from the File menu. While on some systems pressing CTRL+C will terminate **sdadmin**, you should quit the program properly by using the **Exit** option from the File menu instead.

Running sadmin

To run sadmin:

1. Start the database brokers. Type:

   ```
   ACEPROG/sdconnect start
   ```

   If you see the following message, you may need to increase some of the system kernel configuration values:

   ```
   Warning: only 25 wait semaphores are available
   Maximum number of shared-memory segments per process
   exceeded.
   ```

   For procedures on changing UNIX configuration values, see Appendix B, "Modifying Kernel Parameters."

2. Run the RSA Authentication Manager administrative program:

   ```
   ACEPROG/sdadmin
   ```

Important: Do not run **sdadmin** as a background process or leave the Authentication Manager unattended while **sdadmin** is running. If you do, anyone with access to the machine can make changes to RSA Authentication Manager data under your identity. Be sure to exit **sdadmin** and log off before leaving the Authentication Manager.

Dumping the Database Using sddump

The **sddump** program creates dump files of your Authentication Manager and log databases.

The following table describes the options of the **sddump** program.

Option	Argument	Description
-s	None	Dumps the Authentication Manager database.
-l	None	Dumps the log database.
-d	*database name*	The name of the Authentication Manager (or Log) database you want to dump.
-f	*dump file name*	The name of the dump file, if you want to use a location and name that differs from the default location and name (**/ace/data/sdserv.dmp** for the Authentication Manager database dump file and **/ace/data/sdlog.dmp** for the log database dump file).

Option	Argument	Description
-t	*table list*	Specifies one or more database tables to dump. The names of the tables must be separated by commas. The table list argument contains acronyms for the actual table names. These acronyms are described in the following section, "Required Tables."
-p	None	Dumps any required tables for each table in the table list specified with the **-t** option.
-r	None	Includes delta records in the dump file.
-m	None	Allows the dump to be performed while the database is active.
-g	None	Dumps a specified group, its members, and their tokens.
-u	*login*	Dumps a user record (and tokens belonging to the user) by a specified default login.
-k	*login*	Same as **-u**.
-a	*serial number*	Dumps a single token, specified by serial number.
-v	None	Provides detailed output information.

The **-p** option is only valid if selective dump mode (**-t**) is used.
Options **-t**, **-g**, **-u** and **-a** are mutually exclusive.

Required Tables

If you choose to perform a partial dump of the database, be aware that some tables require the presence of other tables in the dump file. If you do not specify all the required tables, you may not be able to load the dump file. To ensure that all required tables are dumped along with the tables you specify, use the **-p** option.

The following table lists the abbreviated table name identifiers used as arguments of the **-t** parameter, the corresponding table names as described in the *Administration Toolkit Reference Guide*, and the required tables for each table in the database.

Identifier	Database Table Name	Required Tables
administrator	SDAdministrator	SDUser
admrole	SDAdministrativeRole	SDAdministrator, SDTaskList, SDRealm, SDSite, SDGroup
attribute	SDAttribute	None
attrvalue	SDAttributeValue	SDProfile, SDAttribute
aalm	SDAALM	None

Identifier	Database Table Name	Required Tables
client	SDClient	SDSystem
clientext	CustClientExt	SDClient
enabledgroup	SDEnabledGroup	SDClient, SDGroup
enableduser	SDEnabledUser	SDClient, SDUser
groupext	CustGroupExtension	SDGroup
groupmem	SDGroupMember	SDGroup, SDUser
logext	CustLogExtension	SDLog
msg	SDLogMessage	None
node	SDSecondaryNode	SDClient
onetimepassword	SDOneTimePassword	SDSystem, SDUser, SDToken
profile	SDProfile	None
realmext	CustRealmExtension	SDRealm
realmenableduser	SDRealmEnabledUser	SDRealm, SDUser
realmenabledgroup	SDRealmEnabledGroup	SDRealm, SDGroup
site	SDSite	None
siteext	CustSiteExtension	SDSite
sys	SDSystem	None
sysext	CustSystemExtension	SDSystem
syslogcr	SDSysLogCriteria	None
tasklist	SDTaskList	None
tasklistitem	SDTaskListItem	SDTasklist
token	SDToken	SDSystem
tokenext	CustTokenExtension	SDToken
user	SDUser	None
userext	CustUserExtension	SDUser
value	SDValue	SDAttribute

Creating a New Database Using sdnewdb

The **sdnewdb** program overwrites the existing Authentication Manager or log database and creates a new, empty Authentication Manager or log database. Make sure that you have backed up your database files or created dump files before using the **sdnewdb** program.

Note: Creating a new database generates a new encryption key that is used to encrypt certain fields in the database. Existing Replicas do not have access to the new key during a database push, and therefore cannot decrypt the new database. For this reason, you must manually copy the Replica Package to the Replica and apply the Replica Package.

The **sdnewdb** program has the following syntax:

```
sdnewdb [server|log|all]
```

where

server	specifies that you want to create a new Authentication Manager database
log	specifies that you want to create a new log database
all	specifies that you want to create new Authentication Manager and log databases

Loading a Dump File Using sdload

The **sdload** program loads the database dump file into the new database.

The following table describes the arguments of the **sdload** program.

Option	Argument	Description
-s	None	Loads an Authentication Manager dump file.
-l	None	Loads a log database dump file.
-d	*database name*	Specifies database filename. If not specified, defaults to ***ACEDATA*/sdserv** or **sdlog**.
-f	*load file name*	Specifies the name of the dump file to load.
-a	None	Compression mode. Loading compresses the database file. Retains all delta records. Resulting database uses less space than database used before dump.
-m	None	Merges the dump file into the database specified by the **-d** argument. See the following section, "Merge Logic," for more information.

Option	Argument	Description
-c	None	When used with **-m**, permits the merge of a dump file only when there are no conflicts between the database and the dump file.
-u	None	Loads a version 5.1 dump file in upgrade mode and adds the current system as the Primary.
-t	*table list*	Specifies one or more tables to dump. The names of the tables must be separated by commas.
-r	None	Makes the current system the Primary. Use this option only when you are attempting to recover a failed database or Authentication Manager.
-k	*license file*	Specifies a license to be loaded with the dump file. Use this argument when loading the dump file into a new database (specified by the **-d** argument) or merging a dump file into a database on the Primary.

Option **-t** is only valid if merge mode (**-m**) is enabled.
Options **-a**, **-m**, **-u** and **-r** are mutually exclusive.

Merge Logic

When you use the **-m** option to merge a dump file into a database, information in the database is preserved. If the dump file contains information that conflicts with information in the database (such as a duplicate user or group name), the conflicting information is rejected in favor of the existing information in the database. All conflicts are reported to standard output, but you can pipe the output to a file for viewing later. The **-c** option merges information only when there are no conflicts. Use this option to see the conflicts between the dump file and the database before you commit any changes to the database.

Important: RSA Security strongly recommends that you back up your current database before performing a Database Load in Merge mode.

Disabling Database Push

Database push (also known as Push DB) updates the database on a Replica automatically by sending the Replica Package database files to the Replica. If the System Parameters on the Primary are set to **Allow Push DB Assisted Recovery**, when you create a Replica Package, the Primary sends the database in the ***ACEDATA*\replica_package** directory to the Replica you specify.

There are two situations in which you would want to push the database to a Replica: as part of a database or hardware recovery, or as part of the initial installation of a Replica, in which case database push saves you the time and effort of copying the database files from the Replica Package to the Replica.

Push DB is allowed by default. If you do not want to push the database files to the Replica, use the following procedure to disable Push DB.

To disable Push DB:

1. On a remote administration machine, start the RSA Authentication Manager Database Administration application and connect to the Primary.
2. Click **System > Edit System Parameters**.
3. Clear **Allow Push DB Assisted Recovery**.
4. Click **OK**.

Once you have disabled Push DB, any Replica Packages you generate must be manually copied to the Replica. If you have already installed the Replica, you must also apply the Replica Package. For more information about **sdsetup -apply_package**, see the chapter "Replica Management Utility (UNIX)," in the *Administrator's Guide*.

If you have not yet installed the Replica, the installation process uses the Replica Package. You do not need to apply the Replica Package during a Replica installation.

Note: If you run the Replica Management utility on the Replica and attempt to view the information about that Replica, default values are displayed until the database push is complete.

Using the Dumpreader Utility

The Dumpreader utility enables you to view the RSA Authentication Manager data in a dump file. This is useful, for example, when you:

- Have multiple dump files and want to check their contents before importing them into your current RSA Authentication Manager database.
- Want to create a report from the data contained in the dump file, using a third-party tool. The Dumpreader utility supports output to files in CSV, HTML, XML, and TXT formats.

Running Dumpreader from a UNIX Shell

The Dumpreader utility can only be run from a UNIX shell prompt.

Note: A version of the Dumpreader utility is also available for Windows platforms. For information, refer to the *Windows Installation Guide*.

To list the **dumpreader** command syntax and options on your screen, type:

```
dumpreader
```

The syntax of the **dumpreader** command is as follows:

```
dumpreader dumpfile format [parameter] [-c]
```

The following table describes the options and arguments of **dumpreader**:

Option	Argument	Description
None	*dumpfile*	Required. Specifies the name of the dump file, typically either **sdserv.dmp** or **sdlog.dmp.**
None	*format*	Required. Specifies the file format to which the dump file data will be written: • **CSV** – Comma-separated values; can be imported into Microsoft Excel or some other third-party reporting format. • **HTML** – Hypertext Markup Language; can be viewed in a web browser. • **XML** – Extended Markup Language; can be imported into a third-party reporting application. **Note:** For CSV, HTML, and XML, one file is created for each table in the database. • **XML2** – Similar to XML, except that it uses a different document type definition (DTD), and all output is collected in one file. • **TXT** – Structured text format; can be viewed in a text editor. All output is collected in one file.
None	*parameter*	Optional. For CSV, HTML, and XML, specifies the directory name to which multiple files, each containing a table of the database, is written. If you do not specify this parameter, the output files are written to the current directory. For XML2 and TXT, this parameter is the name of the file to which the output is written. If no parameter is provided, the output is written to **stderr**, typically the terminal. If the parameter is empty but surrounded by double-quotes ("), the output is to **stdout**, which is also typically the terminal.
-c	None	C*onsolidate* option for dump files that you create by running the **Export Tokens by User** and **Export Tokens** commands from the Administration program. These dump files have a different internal structure from dump files that you create with the Dump utilities described in this appendix. Different parts of one table can be mixed with parts of another table. Each time a part of a different table is found, the Dumpreader creates a new output file. Using the **-c** option reduces the number of files that are output by consolidating all parts of the same table, and then sending the consolidated table to one file. Tables generated by the **-c** option are listed in alphabetical order instead of their order in the dump file.

Dumpreader Output Formats

The Dumpreader utility offers five output options: CSV, HTML, TXT, XML, and XML2. These are described in more detail in the following subsections.

HTML

To view dump file data in your web browser, use the **HTML** argument in your dumpreader command. For example:

```
dumpreader sdserv.dmp HTML dumpoutput
```

In the example, a dump file, **sdserv.dmp**, is output in HTML format to a subdirectory named **dumpoutput** located in the current directory (the one from which the command was run).

The **output** folder will contain multiple HTML files, including a summary file and one file for each database table in the dump file. If you list the directory contents, the summary filename will be similar to:

```
dump_summary_04.01.03_11.40.37.html
```

This means that the output was created on April 1, 2003 at 11:40:37 a.m.

The other files are identified by the table name in the RSA Authentication Manager database schema followed by the same date, time, and extension. For example:

```
SDUser_04.01.03_11.40.37.html
```

The summary file contains links to all the database tables in the dump file. You can view these files in your browser by clicking their related links in the summary file. Alternatively, you can open any of these files directly in your browser (or other HTML-capable application).

Note: In HTML output, the schema version of the data in the dump file is also shown, indicating the release of RSA Authentication Manager from which the file was created. For more information, see "Schema Versions in RSA Authentication Manager Releases" on page 97.

With HTML output, the Dumpreader utility parses special characters in the field names and data and performs these substitutions:

Character	Replaced by
>	&gt
<	&lt
&	&amp
"	&quot
[space]	

CSV

To format dump file data for third-party spreadsheet or other programs, you can use the CSV argument in your dumpreader command. For example:

```
dumpreader sdserv.dmp CSV dumpoutput
```

In the example, a dump file, **sdserv.dmp** is output in CSV format to a subdirectory named **dumpoutput** located in the current directory (the one from which the command was run).

The output directory contains a summary file and one file for each database table in the dump file. For example:

```
dump_summary_04.01.03_11.40.37.csv
SDAdministrativeRole_04.01.03_11.40.37.csv
SDAdministrator_04.01.03_11.40.37.csv
.
.
.
```

With CSV output, the Dumpreader utility parses special characters in the data and substitutes a space for any comma or symbol with an ASCII code below that of the space character (decimal 32).

XML

To format dump file data for third-party reporting programs (for example, Crystal Reports from Crystal Decisions), you can use the XML argument in your dumpreader command. For example:

```
dumpreader sdserv.dmp XML dumpoutput -c
```

In the example, a dump file, **sdserv.dmp** is output to multiple text files with embedded XML codes. These files are saved in a subdirectory named **dumpoutput** located in the current directory (the one from which the command was run).

The output directory contains a summary file and one file for each database table in the dump file. For example:

```
dump_summary_04.01.03_11.40.37.xml
SDAdministrativeRole_04.01.03_11.40.37.xml
SDAdministrator_04.01.03_11.40.37.xml
.
.
.
```

Filenames include a base name and a timestamp that indicates the exact date and time the files were created. This prevents files from being overwritten if you run the Dumpreader utility again.

With XML output, the Dumpreader utility parses special characters in the field names and data and performs these substitutions:

Character	Replaced by
>	&gt
<	&lt
&	&amp

XML2

Use the XML2 option to place the contents of the dump file in one XML-encoded output file. For example:

```
dumpreader sdserv.dmp XML2 sdserv.xml -c
```

In the example, the output file, **sdserv.xml**, contains XML-encoded database tables and the records they contain. Because the **-c** option was used, the tables are consolidated and placed in alphabetical order within the XML file.

For XML2 output, the Dumpreader performs no parsing of special characters. They are output as found in the dump file data.

TXT

Use the TXT option to place the contents of the dump file in a structured text file. For example:

```
dumpreader sdserv.dmp TXT sdserv.txt -c
```

In the example, the data in the output file, **sdserv.txt**, is straight text, formatted for viewing in a text editor (for example, **emacs**). With the **-c** option, the tables are consolidated and placed in alphabetical order within the text file.

With TXT output, the Dumpreader performs no parsing of special characters. They are output as found in the dump file data.

Schema Field Name Differences

To make use of output from the Dumpreader utility, you need to understand the RSA Authentication Manager database schema (the database tables and the records they contain).

You can find complete information about the database schema, including dump file differences, in the Help and in the *Administration Toolkit Reference Guide* (**authmgr_admin_toolkit.pdf**), which is available in the ***ACEDOC*** directory.

Note: Some database field names in dump files are different from their counterparts in the actual database schema.This is necessary to maintain backward compatibility with earlier versions of the dump files. For more information, see the following section, "Schema Versions in RSA Authentication Manager Releases."

Schema Versions in RSA Authentication Manager Releases

RSA Authentication Manager database schema has changed over the product's life cycle. The possible versions of the schema that a dump file could contain are listed in the following table.

Server Version	Schema Version
5.2	19.00.00
5.1	18.00.00
5.0	17.00.00
4.1	16.00.00
4.0	14.00.00
3.31	12.00.00
3.2	12.00.00
3.1	11.00.00
3.0.1	10.00.00

Troubleshooting the Dumpreader Utility

The Dumpreader utility detects dump file, user input, and other problems, and can generate a variety of error messages. This section lists and describes Dumpreader error messages in alphabetical order. For more information on the Dumpreader utility command syntax, see "Using the Dumpreader Utility" on page 92.

Note: To view a complete usage summary on your screen, run the **dumpreader** command without arguments.

Invalid number of parameters. See the usage summary.

The command line has less than two or more than four arguments.

Invalid command line parameter. See the usage summary.

There are three or four arguments but the third or fourth argument is not **-c**.

Invalid format. See the usage summary.

The format parameter is not one of the following:

```
CSV
HTML
XML
XML2
TXT
```

Could not open dump file.

The specified dump file could not be opened. You may have misspelled the dump file name, the dump file could be corrupted, or you may not have appropriate permissions to open the file.

Could not read schema version from the dump file.

The version information could not be read from the dump file. The dump file may be corrupted.

Could not consolidate table information.

The Dumpreader has run out of memory while attempting to consolidate the output of a large dump file. Use a machine with more memory or more swap space, or run the **dumpreader** command without the **-c** option.

Invalid file format.

The dump file could not be read. It may be corrupted, or another file type may erroneously have a .dmp file extension.

Could not open output file.

The specified output format is XML2 or TXT, and the output file or pathname is write-protected, or the disk may be full.

Could not write tag into the output file.

The specified output format is XML2 or TXT, and the output file could not be generated because the disk is full, was removed, or is damaged.

Could not read field from dump file.

The Dumpreader could not read information from the dump file. The file may be corrupted, or the media on which it is stored could be faulty.

Could not create output file for the table <*table name*>.

The CSV, HTML, or XML output file could not be written. The output directory does not exist or is write-protected, or the disk was removed or is full.

Could not write table name into the output file.

In the case of XML2 or TXT formats, the Dumpreader could not write a table name to the output file. The disk may be full or faulty, or was removed.

Could not write the close record tag into the output file.

The Dumpreader could not write to the XML2 or TXT output file. The disk may be full or faulty, or was removed.

Internal error. Dump file might be corrupt.

The Dumpreader utility has encountered unexpected data in the dump file. The dump file may be corrupted.

Could not add field to the table.

The Dumpreader failed to define a new field in a table in the XML, HTML, or CSV output file. This is typically a memory issue. Free up memory or swap space, and try again.

Could not write the open record tag into the output file.

The Dumpreader failed to write information to an XML2 or TXT output file. The disk may be full or faulty, or was removed.

Could not write field data into the output file.

The Dumpreader failed to write information to the output file (any format). The disk may be full or faulty, or was removed.

E Troubleshooting

If you experience problems with the RSA Authentication Manager distribution media or the installation software, go to the section heading in this appendix that describes the symptom or quotes the error message you received. If the explanations and troubleshooting tips do not resolve the problem, contact RSA Security Customer Support. For contact information, see "Getting Support and Service" on page 9.

Distribution Media

CD mount command produces an unknown command error message

CD device names vary from host to host. If your machine returns an unknown command error when you attempt to mount the CD drive, consult your operating system documentation.

"Cannot create administrator. Use an empty database."

This error message appears if you are not **root** and you try to install the RSA Authentication Manager on an AIX system with the ulimit set too low. The ulimit fsize must be at least 4194303. For more information on required minimum values and instructions on modifying system values, see Appendix B, "Modifying Kernel Parameters."

sdsetup Will Not Run or Terminates

Errors associated with insufficient disk space

If you experience disk space problems during an upgrade, purge your log database before migrating to the new installation. This creates disk space for the new installation. For more information, see the chapter "Database Maintenance (UNIX)," in the *Administrator's Guide*.

"You must be root in order to run sdsetup... ."

The following message appears if the administrator running **sdsetup** does not have a UID of 0.

```
You must be root in order to run 'sdsetup.' Please 'su' to
root or log out and log in as root.
```

You do not receive this message if you are logged on as **root**. On some platforms this error will occur if you have become **root** by using the **su** command without the minus argument.

Halt the installation and log on as **root**, or **su** to **root** with the following command:

```
su - root
```

Try again to run **sdsetup**.

"Error - The sdserv [*log*] database is currently busy - exiting."

If the installation program aborts and this message appears, an RSA Authentication Manager database broker is running or was not shut down properly.

To proceed with the installation, make sure that no Authentication Manager programs are running. Then, from the directory that contains the Authentication Manager program files, stop the Report Creation utility. Type:

```
ACEUTILS/rptconnect stop
```

To stop the database brokers and services, type:

```
ACEPROG/aceserver stop
ACEPROG/sdconnect stop
```

If you get an error message saying that the database broker is already stopped, see if there are database lock files (**sdserv.lk** or **sdlog.lk**) in the ***ACEDATA*** directory. If so, running **sdconnect clean** from the system startup file might solve the problem.

In the startup file, enter the command:

```
ACEPROG/sdconnect clean
```

Reboot the Authentication Manager, and try to run **sdsetup** again.

Call RSA Security Customer Support if you need further assistance.

"sdsetup is running already"

When you invoke **sdsetup**, you may receive the following message:

```
A copy of sdsetup is currently running or was abnormally
terminated. Please conclude the running copy before starting
another. If you shelled from sdsetup, you may return by
typing 'exit.'
```

If you are entirely sure another copy of **sdsetup** is not running, yet you receive this message, you may remove the file **sdsetup.running**.

This message appears if the file **sdsetup.running** exists in the current working directory. Either someone else is running **sdsetup**, or the file is from a previously aborted installation. Delete the **sdsetup.running** file from your current working directory only if you are sure no one else is running **sdsetup**.

Post-Installation Errors

"Hostname cannot be resolved"

If you are using a name server and your RSA Authentication Manager Primary or Replica hostname cannot be resolved properly, make sure that the primary hostname of the Authentication Manager (also known as its "boot name") is the first name in any list of aliases for that machine.

"Unable to set ulimit to 4194303, errno=1..."

You see this error message if you are not **root** and you try to run a Server program on an AIX system with the ulimit set too low. The ulimit fsize must be at least 4194303. For instructions on modifying this value on your system, see Appendix B, "Modifying Kernel Parameters."

"BROKER 0: Unable to find server... in file SERVICES..."

This message may appear when you attempt to run **sdconnect**. Check that you have added the service names and port numbers in **/etc/services** as shown in "Pre-Installation Tasks" on page 16.

"This account does not have permission to access the server database"

This message may appear when you attempt to run **sdconnect.** Check that file permissions are set correctly. You must be logged on as root or the RSA Authentication Manager file owner to run **sdconnect**.

If the correct permissions are set, check that you have configured the UNIX kernel parameters as described in Appendix B, "Modifying Kernel Parameters." You may need to increase some of the kernel parameters.

TACACS+ Troubleshooting

If you cannot authenticate on the TACACS+ device, perform the following steps.

To troubleshoot authentication problems on a TACACS+ device:

1. Run **sdadmin**, and look at an RSA Authentication Manager audit trail report for information about the authentication failures.
2. Verify that the physical connection of the Agent Host to the Authentication Manager is not broken.
3. Verify that the **aceserver** is running.
4. Verify that the TACACS+ daemon (**sdtacplusd**) is running and that the daemon is owned by **root**.
5. View **sdconf.rec** on the Authentication Manager by running **sdinfo**. Verify that TACACS Plus is enabled. If it is not, there can be no TACACS support. To enable TACACS+, run **sdsetup -config** as described in Chapter 5, "RSA Authentication Manager TACACS+ Support."

6. Verify that the argument file (**sdtacplus.arg**) is present in the **ace/data** subdirectory of your Authentication Manager.
7. Make sure that the configuration file, as specified in the **.arg** file, is present.
8. Use the **sdadmin** List Agent Hosts option to verify that the Primary and Replicas are registered in the Authentication Manager database as Agent Hosts. If they are not, no authentications from a TACACS Agent Host will succeed and "Agent Host Not Found" will be logged on the Authentication Manager audit trail.
9. If you need more information to help troubleshoot a problem, turn on the **syslog** daemon to view the messages logged by the TACACS server. On the Authentication Manager machine, go to the daemon directory (usually **/usr/etc** or **/usr/sbin**) and type **syslogd**. Read the *UNIX man page* on **syslogd** to learn how to set up the **syslog** configuration file. Information on **syslog** messages, including those that start with the **ACE/Server** prefix, can be found in the Cisco Systems documentation.
10. Run the TACACS debug option on the Network Access Server (NAS). To do this, make sure you are in the **enable** mode. To see what commands are available for debugging, type:

    ```
    debug ?
    ```

    Choose the available *command_name* to debug, and type:

    ```
    debug command_name
    ```

    For example:

    ```
    debug tacacs
    ```

    You receive a TACACS "Access control debugging is on" acknowledgment from the NAS.

    Note: If you are using an X terminal, you must type **terminal monitor** in order to see the debugging log.

    Also, there is additional TACACS+ daemon debugging available in the **sdtacplus.arg** file. Uncomment the **-d** option in the .arg file and restart RSA Authentication Manager. The TACACS+ debugging log is in **var/tmp/tacplus.log**.

Authentication Session Timeouts

A 30-second inactivity time-out is hardcoded in Cisco Systems TACACS+ firmware. This time-out can interfere with the Next Tokencode operation. Advise the user that, to avoid another time-out while waiting for the next tokencode to display, he or she must press character keys on the keyboard, then remove the characters with the backspace key before pressing ENTER.

RSA Authentication Manager Log Messages

Agent Host Not Found *Agent Host = server's IP address*

The defaults **utmp** and **wtmp** are stored in the **var/adm/tacacs** directory. When **-h** is set in the configuration file, the Authentication Manager creates a **wtmp** file for each and every TACACS Agent Host. The filenames for these are the **wtmp** file **sdtac_wtmp** concatenated with the hostname. For example, if a logon were made from Agent Host *panama*, a **wtmp** entry would be made in **sdtac_wtmp** and **sdtac_wtmp.panama**.

TACACS Enable Not Authorized

This message appears if anyone other than a global administrator or an administrator of the specified Agent Host tries to enter Enable mode on the NAS.

TACACS Enable Succeeded

An Agent Host administrator entered the Enable mode.

TACACS Fail with TACACS passwd

A user logging on failed to enter a valid UNIX-style password.

TACACS Login with TACACS passwd

A non-tokenholder has been authenticated against a local UNIX password file.

F

Creating User Records from a SAM Database

As an aid in setting up your RSA Authentication Manager database, RSA Security provides a pair of utilities you can use to move user information from an existing SAM (Security Account Manager) database on a Windows system to the RSA Authentication Manager database.

- **dumpsamusers.exe**, which runs only on Windows, reads user records from one or more SAM databases and writes them to a comma-separated flat file. Each of these records contains the logon, first name, and last name of a single user.
- **loadsamusers**, which runs on UNIX, reads and parses the flat file and, for each user in the file, creates a record in the Authentication Manager database containing the three items of information found in the file.

Because **dumpsamusers** runs only on Windows, only **loadsamusers** is installed with RSA Authentication Manager for UNIX. If your network includes Windows systems and you want to dump user information from their SAM files to load with **loadsamusers**, you can obtain a copy of **dumpsamusers.exe** directly from the RSA Authentication Manager installation CD without going through the entire Windows installation process. The **dumpsamusers.exe** file is located in the **aceserv\nt_i386** directory on the CD. The instructions in this appendix assume that you are running **dumpsamusers** on a Windows system.

It is not possible to automate the transfer process completely. Windows does not provide separate first name and last name fields in the SAM database. Instead, it provides a single full name field and imposes no restrictions on how this field is used. You can use an argument to tell **dumpsamusers** whether to expect the first or the last name to come first, but some inconsistencies are almost certain to occur. You will have to edit the output file manually to eliminate these inconsistencies before **loadsamusers** can do its work properly.

Note: RSA Security provides a utility for creating user records from LDAP directories. For more information, see the chapter "Registering Users for Authentication," in the *Administrator's Guide* and the Help topic "Manage LDAP Users."

Extracting SAM User Records with dumpsamusers.exe

Run the **dumpsamusers** utility from a Windows command prompt.

Syntax

```
dumpsamusers [server(s)...] -lf | -fl outfile
```

Arguments

[*server(s)*...]	Names one or more networked servers, separated by spaces and each preceded by two backslashes (for example, **\\system1 \\system2**). Optional: if omitted, the command affects only the system where the utility is run.
-lf *or* **-fl**	Specifies the order in which user names are found in the SAM database: "last, first" (assumes that a comma separates the two names) or "first last" (assumes no comma).
outfile	Specifies the output file to which the user records should be written.

Editing the Output File

dumpsamusers parses names according to these rules:

- When the order is "last, first," whatever precedes the comma is parsed as the last name, and whatever follows it is parsed as the first name.
- When the order is "first last," whatever follows the last space is parsed as the last name, and everything before it is parsed as the first name.

If middle initials are used, **dumpsamusers**, following these rules, classifies them as part of the first name. Anomalies can occur with two-part surnames, with qualifiers that follow a surname, and with entries consisting of descriptions rather than names. The following examples are based on "first last" order.

Name as found in record	Name as parsed First	Last
Anne Van Ostkamp	Anne Van	Ostkamp
Robert F. Martin III	Robert F. Martin	III
John Daly Jr.	John Daly	Jr.
Development Group	Development	Group

Problems may be less frequent with "last, first" order, but they can occur. For example, problems occur when a comma is used before a qualifier, so that "Brown, Thomas G., Sr." is parsed as "First name: Brown, Thomas G.; last name: Sr." Descriptions such as "Development Group" are equally anomalous regardless of which order is being used.

Because the utility cannot distinguish and accommodate all possible deviations from the simple “last, first” and “first last” patterns, you must review and edit the **dumpsamusers** output file before running **loadsamusers**. The file is in ASCII format, and all fields are labeled. Under most circumstances, only a small portion of the records need to be changed.

Creating RSA Authentication Manager User Records with loadsamusers.exe

Run the **loadsamusers** utility from a UNIX command prompt.

Because it employs functions that are part of the RSA Authentication Manager Administration Toolkit, the **loadsamusers** utility has the following requirements:

- You must set the RSA Authentication Manager environment variables.

  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.
- The database broker must be running when you run **loadsamusers**.
- You must run **loadsamusers** from a directory that also contains the **apidemon** program. The default directory containing these two programs is ***ACEUTILS*/toolkit**.

Syntax

```
loadsamusers infile [-i | -b] [outfile] [-g group]
```

Arguments

infile	Specifies the input file (**dumpsamuser**).
-i *or* **-b**	Indicates whether the utility is invoked as an interactive or batch process. Optional: the default is interactive mode, in which the user is prompted for a replacement string when any record contains invalid characters. In batch mode, these records are not imported, but a list is displayed. Nonfatal errors such as duplicate logons are also displayed or, if an output file is specified (see the next argument), written to that file.
outfile	Specifies an output file to which the list of records with nonfatal errors (see the previous argument) is to be written. Optional: if omitted, the list of records is displayed on the screen.
-g *group*	Specifies an RSA Authentication Manager group to which all users added through this command are to be assigned. If no such group exists, the Authentication Manager creates it. Optional: if omitted, users are not assigned to a group.

The **loadsamusers** program is designed to exit when it encounters a record that it cannot load. Users loaded up to that point remain in the Authentication Manager database.

G Minimum System Requirements (Solaris 9)

This appendix specifies the minimum operating system components required for the RSA Authentication Manager to function properly on Solaris 9. Before you minimize your system, review "Important Installation Guidelines" on page 13.

To ensure that your system is properly minimized, RSA Security recommends that you perform a new installation of Solaris 9. Choose the core components cluster, then add the following packages:

- SUNWlibC
- SUNWlibCx

Configuring Solaris Services for Minimization

After you install the operating system, you may want to remove certain packages depending upon your system configuration and the environment in which you plan to use the machine. Use the **pkginfo** command to display the packages currently included as part of the installation. Use the **pkgrm** command to remove packages.

The following minimum configuration requirements are for Solaris 9 running on a Sun SPARC SunFire processor.

Hardware:

- SUNWced
- SUNWcedx
- SUNWdmfex
- SUNWeridx
- SUNWged
- SUNWgedx
- SUNWhmd
- SUNWhmdx
- SUNWqfed
- SUNWqfedx
- SUNWpd
- SUNWpdx

Base Components:

- SUNWbip
- SUNWbzip
- SUNWcar
- SUNWcarx
- SUNWcs
- SUNWcsl
- SUNWcslx
- SUNWcsr
- SUNWcsu
- SUNWcsxu
- SUNWesu
- SUNWkvm
- SUNWkvmx
- SUNWlibC
- SUNWlibCx
- SUNWlibms
- SUNWlmsx
- SUNWnamos
- SUNWnamo
- SUNWswmt

Glossary

***ACEDATA* directory**

The RSA Authentication Manager data directory. This term appears in bold italics (***ACEDATA***) and stands in place of the actual directory name (for example, **/ace/data**).

***ACEDOC* directory**

The RSA Authentication Manager document directory. This name appears in bold italics (***ACEDOC***) and stands in place of the actual directory name (for example, **/ace/doc**).

***ACEPROG* directory**

The RSA Authentication Manager executables directory. This name appears in bold italics (***ACEPROG***) and stands in place of the actual directory name (for example, **/ace/prog**).

ACEUTILS directory

The RSA Authentication Manager utilities directory. This name appears in bold italics (***ACEUTILS***) and stands in place of the actual directory name (for example, **/ace/utils**).

ace/data, ace/prog, ace/rdbms, ace/utils, and ace/doc subdirectories

The subdirectories created by the installation program to hold RSA Authentication Manager data, RSA Authentication Manager program files, the Progress Software relational database management system software, utilities such as the Report Creation Utility, and documentation files respectively. All five subdirectories are in the top-level RSA Authentication Manager directory specified during installation.

aceserver

The background Authentication Manager process that performs authentication for the RSA Authentication Manager product.

acesyncd

The background process that provides Primary/Replica communications and allows the Authentication Manager databases to replicate to and from the Primary.

***ACEUTILS* directory**

The RSA Authentication Manager utilities directory. The name appears in bold italics (***ACEUTILS***) and stands in place of the actual directory name (for example, **/top/ace/utils**).

Acting Master

An Acting Master that is configured to respond to legacy Agent authentication requests. An Acting Master is a fully functional version 5.2 RSA ACE/Server.

Acting Slave

An Acting Slave responds to a legacy Agent authentication request when an Acting Master is unable to respond.

Agent Host

A computer or another device that is protected by the RSA Authentication Manager to prevent unauthorized access.

automatic migration

A method of upgrading an existing Master Authentication Manager to the Primary, in which the Master Authentication Manager database is migrated automatically to a 5.2 database. When performed with a Slave configured in your system, you have the option of performing a rolling upgrade.

Coordinated Universal Time or UTC

The standard for time throughout the world. Also known as Greenwich Mean Time. To get Coordinated Universal Time, call a reliable time service.

database broker

A process that provides a connection between one of the RSA Authentication Manager databases and the RSA Authentication Manager programs that access the databases.

license.rec

The file that contains site-specific information, such as the license and customer ID number, the number of users and Replicas allowed in the database, and whether this is a trial license.

New PIN mode

When the Authentication Manager puts a token in this mode, the user must receive or create a new PIN in order to gain access to a system protected by RSA SecurID.

Next Tokencode mode

When a user attempts authentication with a series of incorrect passcodes, the Authentication Manager puts the token in this mode so that the user, after finally entering a correct code, is prompted for another tokencode before being allowed access.

node secret

A string of pseudorandom data known only to the Agent Host and the Authentication Manager. The node secret is combined with other data to encrypt Agent Host/Authentication Manager communications.

passcode

The user's PIN plus the tokencode displayed by the user's token.

PIN

The user's Personal Identification Number. The PIN is one factor in the RSA SecurID authentication system. The other factor is the tokencode.

Primary Authentication Manager

The RSA Authentication Manager on which administration can be performed and which replicates database changes to the Replicas.

RADIUS profile

A list of requirements that must be met before the RSA Authentication Manager software challenges a RADIUS user for a passcode. Users who authenticate through a RADIUS server must have a profile in the RSA Authentication Manager database.

realm

An RSA Authentication Manager Primary (and one or more Replicas) along with its databases, Agent Hosts, users, and tokens.

Remote Administration application

The application that makes it possible to administer an RSA Authentication Manager database through a remote connection. Remote administration of an RSA Authentication Manager for UNIX database can be performed from machines running Windows NT, Windows 2000, Windows XP, or Windows 98. Remote administration provides a graphical user interface for administering an RSA Authentication Manager database and provides the only supported method of accessing administrative features added with version 3.0 and later.

REP_ACE

The environment variable that specifies the directory that contains the Replica Package. If you do not set REP_ACE, by default the Replica Package is created in the ACEDATA directory.

Replica Package

The database and license files required to install a Replica. You create the Replica Package on a Primary using the Replica Management utility, and the files are created in **replica_package/database** and **replica_package/license** directories in the ***ACEDATA*** directory, or in the directory specified by REP_ACE.

Replica Authentication Manager

The RSA Authentication Manager whose main function is to perform RSA SecurID authentication.

rolling upgrade

A method of upgrading an existing Master and Slave to the Primary and a Replica. In a rolling upgrade, the existing databases are migrated to 6.0 databases with no loss of data and no downtime of authentication services.

RSA Authentication Agent

A product developed by RSA Security that is installed on a computer or another device and that works with the RSA Authentication Manager to prevent unauthorized access. Designated users of this computer or device must provide a valid RSA SecurID passcode in order to gain access.

RSA Authentication Agent software

The programs that perform the authentication dialog on RSA Authentication Agents and third-party Agent Hosts.

RSA SecurID Software Token

A software-based, one-time password authentication method for network protection.

sdadmin

This program can be used to perform a limited number of administrative tasks directly on the Primary RSA Authentication Manager for UNIX only in TTY mode (character-based interface). RSA Authentication Manager administrative features added with versions 3.0 and later are available only through the Database Administration application run remotely under Windows NT, Windows 2000, Windows XP, or Windows 98.

sdconf.rec

The configuration file created by the installation program. When an Agent Host is installed, this configuration file must be copied to the Agent Host (unless it is a third-party device that integrates RSA Authentication Agent code and has its own configuration record).

sdinfo

Run on a UNIX Agent Host, this utility displays the information in the Agent Host copy of the system configuration record (**sdconf.rec**). Run on a UNIX Authentication Manager, it displays both configuration and license information (the contents of **sdconf.rec** and **license.rec**).

sdlogmon

A utility that displays log entries on the screen as they are written to the log record database.

sdsetup

The RSA Authentication Manager program that installs and configures the Authentication Manager system.

sdshell

The shell that requires RSA SecurID authentication of users on UNIX Agent Hosts, including AIX Agent Hosts using name servers such as NIS or DNS, but *excluding* AIX Agent Hosts using an authentication method defined in **/etc/security/login.cfg**.

sdshell_adm

For system administrators who prefer the convenience of using the **su** command without having to provide an RSA SecurID passcode, a third authentication shell, **sdshell_adm**, is provided. Although it is not recommended, you may substitute **sdshell_adm** for **sdshell**.

sdshell_auth

The shell used to authenticate RSA SecurID users on AIX Agent Hosts that do not use name servers. A user's primary authentication method on these Agent Hosts must be "SecurID," and RSA SecurID must be defined in **/etc/security/login.cfg** to run **sdshell_auth**.

token

Usually refers to a handheld 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 the token. The tokencode along with the PIN make up the RSA SecurID passcode.

two-factor authentication

The authentication method used by the RSA Authentication Manager system in which the user must enter a secret, memorized personal identification number (PIN) and the current code generated by the user's assigned RSA SecurID token. The PIN and tokencode make up the passcode.

user password

A special token type, provided for administrator convenience, that allows a user to enter a password at the passcode prompt during authentication.

Index

S

T

U

W