RSA ACE/Server 5.2 for UNIX
Installation Guide

Contact Information

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

RSA Security Inc.
www.rsasecurity.com

RSA Security Ireland Limited
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: October 2003

P/N 1307/A4

Contents

Preface 7
Audience 8
Directory Names 8
Documentation 8
How RSA ACE/Server Documentation Is Organized 9
Help 9
Online Distribution of RSA ACE/Server 5.2 10
Getting Support and Service 10
Before You Call for Customer Support 10

Chapter 1: RSA ACE/Server Requirements 11
Licensing Options 11
Base License 11
Advanced License 11
System Requirements 12
Supported Platforms and Hardware 12
Disk Space Requirements 12
Drives 13
Hostnames 13
Kernel Configuration 13
Important Installation Guidelines 13
Merging Multiple Realms 14
Maintaining Accurate System Time Settings 14
Pre-Installation Checklist 14
Pre-Installation Tasks 16
Next Steps 18

Chapter 2: Installing the RSA ACE/Server 21
Installing the Primary Server Software 21
Command Line Arguments 23
Installation Prompts 24
Primary Server Installation Is Complete 27
Post-Installation Setup 27
Security Requirements 27
Telnet 28
Logging Replication Messages to the syslog 28
Testing Authentication 29
Extracting and Importing Token Records 29
Implementing RSA SecurID Authentication for a User 30
Performing a Test Authentication 30
Preparing the System for Replica Server Support 31
Adding Replica Servers to the Database 32
Creating a Replica Package 33

Installing the Replica Server Software 34
Command Line Arguments 35
Installation Prompts 36
Completing the Replica Server Installation 36
Troubleshooting Service Name and Port Numbers 36
Monitoring Startup Processes 37
Starting the Replica 37
Next Steps 38

Chapter 3: Upgrading to RSA ACE/Server 5.2 39
Pre-Upgrade Checklist 39
Preparing for the Primary Server Upgrade 40
Task 1: Stop the RSA ACE/Server Services on the Primary Server 40
Task 2: Back Up the Database and License Files on the Primary Server 41
Upgrading a Primary Server 41
Preparing for a Replica Server Upgrade 41
Task 1: Copy the License Files from the Primary Server 41
Task 2: Stop All RSA ACE/Server Services on the Replica Server 42
Upgrading a Replica 42
Next Steps 42

Chapter 4: Installing Remote Administration Software 43
Configuring Remote Administration Authentication Methods 43
Installation/Upgrade Checklist 44
Installing Remote Administration for the First Time 44
Upgrading Remote Administration 45
Adding an RSA ACE/Server to Administer Remotely 46
Configuring Remote Administration Ports 47

Chapter 5: The RSA RADIUS Server 49
Overview 49
Pre-Configuration Checklist 50
Loading Existing RADIUS Data 51
RADIUS Utilities 52
Importing a Dictionary File 53
Removing Attributes 53
Importing User and Client Files 54
Enabling and Disabling the RADIUS Server 55
Configuring RADIUS Services on the RSA ACE/Server 56
Adding Servers as Agent Hosts to the Primary Database 57
Configuring the RADIUS Server 57
Configuring a RADIUS Device 58

RADIUS Data File Formats 58
Dictionary 58
Map File 59
User File 59
Client File 60
Next Steps 60

Chapter 6: RSA ACE/Server TACACS+ Support 61
Authenticating on a TACACS+ Device 62
Authentication of TACACS+ Users 62
Enabling and Configuring TACACS+ Support 62
Sample TACACS+ Argument File 64
Sample TACACS+ Configuration File 65
Configuring a Cisco Systems TACACS+ Client Device 67
Protecting Enable Mode 71
Authenticate All Users 72
Authenticate Users Running Level-15 Commands 72

Chapter 7: Installing the Quick Admin Software 73
Quick Admin Architecture 73
System Requirements 74
Windows 2000 and Windows 2003 74
Solaris and HP-UX 11i 75
Pre-Installation Checklist and Tasks 75
Installing Quick Admin on Windows 2000 and Windows 2003 76
Installing Quick Admin on Solaris or HP-UX 11i 78
Upgrading from Quick Admin 5.1 to Quick Admin 5.2 79
On a Windows Machine 79
On a UNIX Machine 80
Installing Quick Admin After Web Express Is Installed 80
Installing Web Express After Quick Admin Is Installed 82
Changing Quick Admin Settings 82
ACE Web Admin for ACE/Server Configuration Settings 83
Password Token Lifetimes Settings 84
Quick Admin Timeout Settings 86
Debugging On/Off Settings 87
Changing RSA ACE/Server Communication Settings 88
Administering Multiple Primary Servers 88
Uninstalling Quick Admin 89

Appendix A: Modifying Kernel Parameters 91
Modifying Kernel Parameters for HP-UX 91
Modifying Kernel Parameters for IBM AIX 92
Modifying Kernel Parameters for Solaris 93

Appendix B: Database Utilities 95
Using sdadmin 95
Interface Conventions 96
Running sdadmin 97
Dumping the Database Using sddump 97
Required Tables 98
Creating a New Database Using sdnewdb 100
Loading a Dump File Using sdload 100
Merge Logic 101
Disabling Database Push 102
Using the Dumpreader Utility 102
Running Dumpreader from a UNIX Shell 103
Dumpreader Output Formats 104
Schema Field Name Differences 107
Schema Versions in RSA ACE/Server Releases 107
Troubleshooting the Dumpreader Utility 107

Appendix C: Troubleshooting 111
Distribution Media 111
sdsetup Will Not Run or Terminates 111
Post-Installation Errors 113
TACACS+ Troubleshooting 113
RSA ACE/Server Log Messages 115

Appendix D: Creating User Records from a SAM Database 117
Extracting SAM User Records with dumpsamusers.exe 118
Syntax 118
Arguments 118
Editing the Output File 118
Creating RSA ACE/Server User Records with loadsamusers.exe 119

Appendix E: Minimum System Requirements (Solaris 9) 121
Configuring Solaris Services for Minimization 121

Glossary 123

Index 127

Preface

This manual provides instructions for installing RSA ACE/Server 5.2 for UNIX.

Task	See
Prepare for any type of upgrade or new installation.	"RSA ACE/Server Requirements" on page 11
Install and configure a new Primary or Replica.	"Installing the RSA ACE/Server" on page 21
Perform a rolling upgrade from RSA ACE/Server 5.0 or 5.1.	"Upgrading to RSA ACE/Server 5.2" on page 39
Install the RSA ACE/Server Remote Administration software on a Windows machine.	"Installing Remote Administration Software" on page 43
Enable and configure a RADIUS server.	"The RSA RADIUS Server" on page 49*
Configure RSA ACE/Server for TACACS+ support.	"RSA ACE/Server TACACS+ Support" on page 61
Install or upgrade Quick Admin.	"Installing the Quick Admin Software"on page 73
Modify kernel parameters.	"Modifying Kernel Parameters" on page 91
Use the RSA ACE/Server database utilities to dump and load the database.	"Database Utilities" on page 95
Troubleshoot installation issues.	"Troubleshooting" on page 111
Import users to the RSA ACE/Server database from a Windows SAM (Security Accounts Manager) database.	"Creating User Records from a SAM Database" on page 117

* If you want to use a third-party RADIUS server for RADIUS authentications, refer to the third-party documentation for instructions.

Audience

This manual is intended for UNIX security system administrators. The person who installs the RSA ACE/Server must have a working knowledge of UNIX, your Server 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 ACE/Server data directory	**/ace/data**
ACEDOC	RSA ACE/Server document directory	**/ace/doc**
ACEPROG	RSA ACE/Server executables directory	**/ace/prog**
ACEUTILS	RSA ACE/Server utilities directory	**/ace/utils**

Documentation

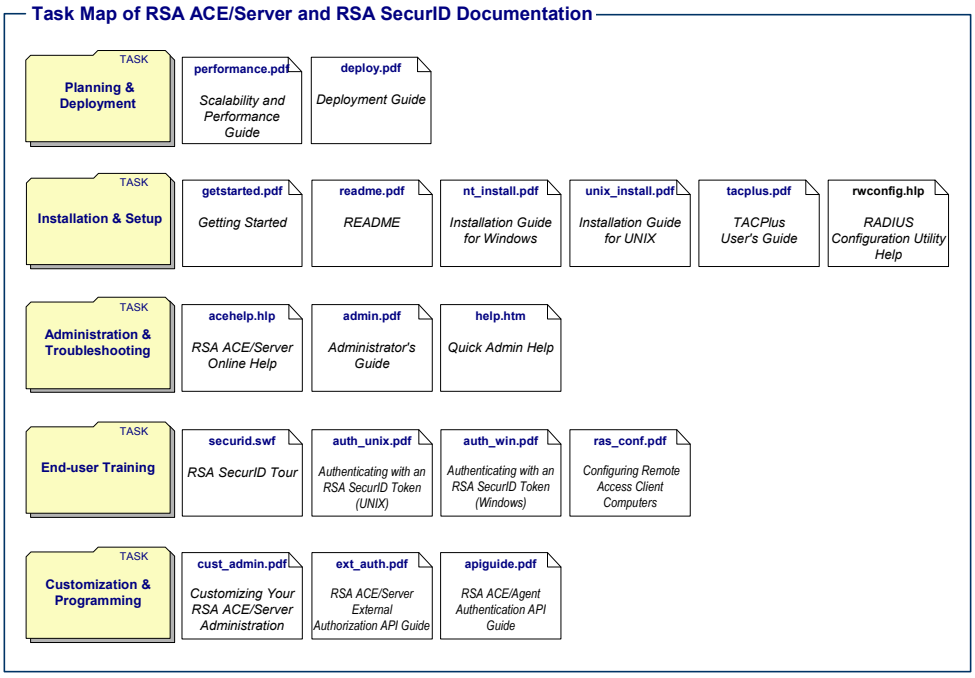
The RSA ACE/Server 5.2 package provides the software on a single CD for both Windows and UNIX installations. In addition, the CD contains all RSA ACE/Server documentation and Help, which together provide complete instructions for RSA ACE/Server installation, configuration, administration, and troubleshooting. For information about all RSA ACE/Server 5.2 resources available to you, see the printed *RSA ACE/Server 5.2 Getting Started* booklet in the RSA ACE/Server package.

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

How RSA ACE/Server Documentation Is Organized

During RSA ACE/Server 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 ACE/Server 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 ACE/Server CD.

The following diagram provides a task-oriented map of the RSA ACE/Server documentation so that you can find the information you need.



Help

RSA ACE/Server 5.2 includes an extensive Help system that is available when you use remote administration on a Windows system in order to administer an RSA ACE/Server 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 ACE/Server 5.2

Some upgrade customers have the option of downloading RSA ACE/Server 5.2 as a zip file. When unzipped, the file contains the same directory layout and contents as the RSA ACE/Server 5.2 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.

You should have already received the Welcome Kit and license diskettes with your original RSA ACE/Server package.

Getting Support and Service

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

Before You Call for Customer Support

Make sure you have direct access to the computer running the RSA ACE/Server 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 ACE/Server software version number.
- ❑ The make and model of the machine on which the problem occurs.
- ❑ The name and version of the operating system under which the problem occurs.

1 RSA ACE/Server Requirements

Follow this chapter to perform a thorough review of the system or systems onto which you will install RSA ACE/Server 5.2 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 ACE/Server 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 ACE/Server Base license provides the rights to use the RSA ACE/Server software in the following environment:

- With as many users in the RSA ACE/Server database as specified by the user tier that was purchased.
- 1 Primary and 1 Replica Server in 1 Realm.

Advanced License

The RSA ACE/Server Advanced license provides the rights to use the RSA ACE/Server software in the following environments:

- With as many active users in the RSA ACE/Server database as specified by the active user tier that was purchased.
- On 1 Primary and up to 10 Replica Servers in up to 6 Realms.

  Multiple Advanced licenses may be purchased for customers who want to install the software in more than six Realms.
- Installed on a qualified High Availability hardware system.

For detailed information about licenses and active users, see the *RSA ACE/Server 5.2 Administrator's Guide.*

System 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 ACE/Server 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 ACE/Server 5.2 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 5.1 or 5.2 on PowerPC and RISC/6000 processors
- ❑ Solaris 8 or Solaris 9 on UltraSPARC processors

Use the **uname -a** command to view platform information. On AIX systems, the command is **oslevel**

In addition, you must install the following operating system patches on AIX 5L v 5.1 and 5.2 *before* you install RSA ACE/Server 5.2:

- AIX 5L v 5.1: APAR IY 43694
- AIX 5L v 5.2: APAR IY 44173

You can download the appropriate patch from the IBM web site at **https://techsupport.services.ibm.com/server/aix.fdc**

High Availability

RSA ACE/Server 5.2 is certified for High Availability on Solaris 9 Veritas Cluster Server.

Recommended Performance Configuration for Supported Platforms

To achieve higher authentication rates with RSA ACE/Server 5.2 running on UNIX, the following more advanced hardware platforms are recommended:

- ❑ For HP-UX: HP J2240 with dual 236 MHz PA-8200 processors
- ❑ For AIX: RS/6000 with dual 233MHz processors
- ❑ For Solaris: Ultra SPARC II with dual 300MHz processors

Disk Space Requirements

Reserve the required space listed below 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 ACE/Server 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 ACE/Server 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 ACE/Server software distribution medium. An acceptable alternative is having a local CD drive on a workstation that can be accessed using NFS facilities.

  The CD drive on which the RSA ACE/Server software distribution media will be mounted must be compatible with the workstation that will read from it, and the default permissions of the drive must be intact.

- ❑ Your license record files were shipped to you on a DOS diskette. You must have a 3.5-inch, 1.44-MB drive on the Server or another workstation. If you use **ftp** to transfer the files, perform the transfer in binary mode.

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 Replica Servers 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 the appendix "Modifying Kernel Parameters" in this book. 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 Server machines be used as RSA ACE/Servers only.
- Make sure that the Server machines are located in a secure area and can be accessed by trusted personnel only.
- The name of each Server machine must be a fully-qualified computer name on the network.
- Do not run multiple RSA ACE/Servers on the same physical platform.
- Do not install RSA ACE/Server software on a network drive.
- Do not install RSA ACE/Server software into a directory with a pathname that includes blank spaces. Blank spaces will cause the installation to fail.
- Make backup copies of the diskettes before beginning an installation. Store the original license diskettes, the token seed record diskettes, the RSA ACE/Server 5.2 CD, and any copies you make in a secure place.

Merging Multiple Realms

To merge databases from multiple realms into one 5.2 realm, you need to:

1. Upgrade one realm to RSA ACE/Server 5.2.
2. Dump the other databases and merge them into the 5.2 database using the dump and load utilities **sddump** and **sdload**.

For more information, see the appendix "Database Utilities" in this book.

Maintaining Accurate System Time Settings

RSA ACE/Server relies on standard time settings known as Coordinated Universal Time (UTC). The time, date, and time zone settings on computers running RSA ACE/Server must always be correct in relation to UTC. If the time settings happen to drift by more than a minute, authentication will fail.

Make sure that the time on the Primary RSA ACE/Server 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 ACE/Server 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 ACE/Server 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 read the *RSA ACE/Server 5.2 Readme* (**readme.pdf**) before installing the RSA ACE/Server software. The *RSA ACE/Server 5.2 Readme* contains important configuration and installation information for RSA ACE/Server 5.2. 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 ACE/Server software.

You must have the following materials:

- ❑ The RSA ACE/Server CD.
- ❑ The license diskette.
- ❑ A blank diskette on which to copy the license diskette.

Important: Make a backup copy of the license diskette before beginning any installation procedures and store the original diskette, the token seed record diskette, the RSA ACE/Server 5.2 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 ACE/Server 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 diskettes. The only way to regain access is with the modified license files.

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

Note: Each shipment of RSA SecurID tokens contains a DOS diskette containing token seed records in one or more ASCII or XML files. The token seed record diskette is not shipped in the RSA ACE/Server 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 will 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 procedures in the appropriate chapters of this book. For a full description of the Replica Management utility, see the *RSA ACE/Server 5.2 Administrator's Guide*.

- ❑ The method of delivering the Replica Package to the Replica.

  There are two methods of delivering 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 Server.

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

    For more information on disabling Push DB, see "Disabling Database Push" on page 102.

If you are installing RADIUS on the Primary, you will also need

- ❑ Access to any existing RADIUS user file, client file, or dictionary file.

  The installation process prompts you for the location of these files. If you have no RADIUS data files, the RSA RADIUS default dictionary file is loaded.

- ❑ The port numbers for RADIUS authentications (**1645**) and RADIUS accounting (**1646**), if you are installing RADIUS but not using the specified default ports

Pre-Installation Tasks

Unless instructed otherwise, complete each task on the machine or machines that will run RSA ACE/Server 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 ACE/Server, 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 ACE/Server processes before creating the backup. To stop the Report Creation utility, type

   ```
   ACEUTILS/rptconnect stop
   ```

   Stop the RSA ACE/Server services and database brokers. Type

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

2. Set the Server system time. Reliable system time is critical to proper RSA ACE/Server operation.

   - *If this is a first-time installation*, set the Server 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 Server machine,* set the target machine time to match that of the existing Server. If the time is not set to match the existing Server time, some or all tokenholders may be denied access.

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

   The RSA ACE/Server top-level directory

   - Must have enough disk space to hold all RSA ACE/Server 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 ACE/Server 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 now.

```
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
tacacs          49/tcp       #TACACS+
radius          1645/udp
```

   The preceding values are the version 5.2 defaults, not requirements. These 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 Server. Default port names have a two-digit number appended to them, so the Primary Server is **securidprop_00**, and the first Replica added to the system is **securidprop_01**. You will 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 will not be using the default service names and port numbers, you must change these parameters as described in the appendix "Configuring the RSA ACE/Server (UNIX)" in the *RSA ACE/Server 5.2 Administrator's Guide* and make the appropriate entries in the **/etc/services** file of the Server.

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

   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.

6. Designate the RSA ACE/Server administrators. Create a UNIX group of RSA ACE/Server 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 Server database as RSA ACE/Server administrators. You must create this UNIX group for RSA ACE/Server file privileges to be set appropriately.

7. Designate an RSA ACE/Server fileowner.

   During installation, the designated fileowner is added to the database as the only RSA ACE/Server administrator. Select a member of the UNIX group of Server administrators to be named as the owner of all RSA ACE/Server files. Verify that this primary UNIX group ID (GID) of this account is that of the UNIX group of administrators you created in the previous step. Record that account login below.

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

8. Verify that the RSA ACE/Server fileowner has an entry in the Server **/etc/passwd** file. If there is no entry for that account, add it now.

9. Verify that the kernel parameter settings are configured to meet the requirements described in the appendix "Modifying Kernel Parameters" in this book.

Next Steps

Do one of the following:

- If your system has failed to meet any requirement listed in this chapter, **STOP**. Do not go on to "Installing the RSA ACE/Server." Contact RSA Security Customer Support for assistance.
- If you have successfully completed the pre-installation tasks, and you are Installing the RSA ACE/Server for the first time, see the chapter "Installing the RSA ACE/Server" in this book for complete instructions.
- If you have successfully completed the pre-installation tasks, and you are performing an upgrade from RSA ACE/Server 5.0 or 5.1, see the chapter "Upgrading to RSA ACE/Server 5.2" in this book.

2 Installing the RSA ACE/Server

Follow the instructions in this chapter to install the RSA ACE/Server software on your Primary and Replica Servers, and perform post-installation tasks.

Installing the Primary Server Software

The installation procedure in this section assumes that the RSA ACE/Server 5.2 CD can be mounted on your Server workstation. If the target Server workstation does not have a local CD drive, you can use NFS facilities to export the CD drive mount point to the target Server 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 Server software:

1. Log in to the designated Primary Server 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, insert the RSA ACE/Server license diskette into the 3.5-inch, 1.44-MB drive on the Server or another workstation. Following your usual procedure for transferring files in binary mode from a DOS-formatted diskette, copy the following files to the current directory:

   ```
   license.rec
   server.cer
   server.key
   sdti.cer
   ```

   The filenames *must* be in all lowercase letters.

   Skip step 3, and go 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
   ```

   Troubleshooting tip: Make sure your current directory is writable. Do not attempt to install the RSA ACE/Server 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	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/aceserv/*platform*** directory, where ***platform*** is the abbreviation for your operating system.

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

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

7. The command to start the Primary Server installation is

```
/cdrom/aceserv/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 ACE/Server 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 fileowner you selected during Server preparation.
-o yes | no	This argument allows you to re-install 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 ACE/Server directory you selected or created during Server preparation.
-r yes | no	This argument allows you to enable RADIUS. If you specify **-r no**, RADIUS will not be enabled. You can enable RADIUS at any time after the Primary Server installation is complete (see "Enabling and Disabling the RADIUS Server" on page 55). If you specify **-r yes**, the installation accepts the default RADIUS port number (1645) and the default values to the RADIUS configuration prompts listed in step 2 through step 5 on page 26. When the Primary Server installation is complete, you can import existing RADIUS user and client data files (see "Loading Existing RADIUS Data" on page 51).

Example with Command Line Arguments

The following example command, issued on an HP system that has been properly prepared for RSA ACE/Server installation, produces the results listed:

```
/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 ACE/Server files will be owned by user **smith**, so all members of the smith primary UNIX group will have the permissions required to run RSA ACE/Server programs.
- All Server files will be 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 5.2 database. Type "**y**" (for Yes) or "**n**" (for No), and press ENTER.
- RADIUS will be enabled using the default values for the RADIUS prompts. See "Enabling RADIUS" on page 25.

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 here in the order they appear.

Country of Origin

Allows you to select the country from which you ordered the RSA ACE/Server software. Once you choose yes (**y**) or no (**n**), the correct license displays.

License Agreement

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

Fileowner

When you are prompted for a fileowner, enter the login name or username you designated in step 7 on page 18. Confirm the name you entered when prompted.

Path

Supply the pathname of the top-level RSA ACE/Server directory you selected or created during Server preparation. The path you specify will contain all Server subdirectories, databases, and program files.

Overwrite

This prompt appears if the installation program detects that an installation of RSA ACE/Server software exists on the machine. Enter **y** to overwrite, **r** to re-specify, or **q** to quit.

If any RSA ACE/Server 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 5.2. 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 ACE/Server 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 re-install or upgrade the Server 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 Server. 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 pre-existing Replicas in the database. For information, see "Preparing the System for Replica Server Support" on page 31 and "Adding Replica Servers to the Database" on page 32.

You can also add Replicas to your database if you have upgraded from a previous version. Your license will control the number of Replicas that you can have in your RSA ACE/Server installation. See the section "Licensing Options" on page 11 for more information about licenses.

Enabling RADIUS

RSA ACE/Server software supports the RADIUS protocol for cross-realm authentication services. The Primary Server installation program will prompt you to configure the system for RADIUS.

If you do not want to enable RADIUS at this time, answer **n**.

Note: You can enable RADIUS and import existing RADIUS data files any time after installing the RSA ACE/Server software. See "Loading Existing RADIUS Data" on page 51 for instructions.

Enable RADIUS support by answering the following RADIUS configuration prompts:

1. Answer **y** at the following prompt:

```
Do you want to configure radius now? (y/n) [n]:
```

The program prompts for any existing RADIUS data files that you want to import. The following table describes the RADIUS data files you can import.

File Type	Description
RADIUS Users File	Contains RADIUS account information about users.
RADIUS Clients File	Contains information about devices that support RADIUS logins.
Dictionary File	Contains definitions of Attributes and Values. The RADIUS option includes a default dictionary.
SecurID Map File	A mapping file that dictates which attributes in the dictionary can be configured and which ones can be multiply-defined.

2. To import an existing dictionary, answer **y** at the following prompt:

   ```
   Do you have your own dictionary file? (y/n) [n]:
   ```

   When prompted for the pathname, specify the location of your dictionary file. If you have no dictionary file, the default RSA RADIUS dictionary file is used.

3. To import an existing map file, answer **y** at the following prompt:

   ```
   Do you have your own securid map file? (y/n) [n]:
   ```

   When prompted for the pathname, specify the location of your map file. If you have ever edited the **securid** map file, specify the location of the edited file. If you answer **n**, the default map file is used.

4. To import an existing RADIUS clients file, answer **y** at the following prompt:

   ```
   Do you wish to migrate RADIUS clients? (y/n) [n]:
   ```

   When prompted for the pathname, specify the location of your clients file.

5. To import an existing RADIUS users file, answer **y** at the following prompt:

   ```
   Do you wish to migrate RADIUS users? (y/n) [n]:
   ```

   When prompted for the pathname, specify the location of your users file.

After you respond to the prompts and specify the location of the data files you want to import, RADIUS is enabled.

When you enable RADIUS on a Primary Server, and load existing RADIUS data files, the installation process:

- Creates a profile (***loginname*Profile**) for each user in the RADIUS user data file
- Creates a user record if there is no existing user record for the login name in the RSA ACE/Server database
- Assigns the profile to the user record that contains the login name

Although each profile name is unique, the profiles may contain the same attributes and values. For example, you may have created 1 profile and assigned it to 50 users. When you import these user data files, 50 user profiles are created in the database, 1 for each user in the file. To ease administration, create a default profile and assign it to the 50 users.

See the chapter "The RSA RADIUS Server" in this book for more information.

Primary Server Installation Is Complete

The program notifies you and displays the Server 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. See the chapter "Overview" in the *RSA ACE/Server 5.2 Administrator's Guide* for more information about licenses.

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, see the appendix "Configuring the RSA ACE/Server (UNIX)" in the *RSA ACE/Server 5.2 Administrator's Guide* for instructions on modifying the Server configuration file so that it contains the service names and port numbers you want to use.

Post-Installation Setup

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

Although most administration of the RSA ACE/Server for UNIX database will be 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 29.

Security Requirements

The following list contains security requirements and issues. Verify that the RSA ACE/Server machine adheres to these requirements:

- ❑ RSA ACE/Server computers must be secure. Only trusted personnel should have physical access to the Primary and Replica Servers, and the Servers should be protected by RSA SecurID.
- ❑ Only UNIX administrators should have accounts on the Primary and Replica Servers.
- ❑ Disable the **rsh** and **rcp** commands. They are non-interactive remote commands that are unable to provide RSA SecurID protection by prompting for a passcode.
- ❑ No machine should allow **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 will 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 thus do not invoke **sdshell** and passcode processing.
- ❑ Only trusted personnel should have access to the **chsh** and **passwd** commands. If a user can modify the **/etc/passwd** file and change his or her login 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 Server waits longer to detect the last character of the passcode.

See "Changing the Configuration" in the appendix "Configuring the RSA ACE/Server (UNIX)" in the *RSA ACE/Server 5.2 Administrator's Guide* for information on changing the configuration record.

Logging Replication Messages to the syslog

If you want to log RSA ACE/Server replication status messages to the syslog, edit the **syslog.conf** file on each Server 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 Replica Servers were installed properly and that you can implement protection for them as Agent Hosts.

Extracting and Importing Token Records

If you received a DOS-formatted diskette 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 Server so that you can import the tokens into the database and assign tokens to your users.

Note: If you are upgrading, pre-existing token records are automatically migrated into your 5.2 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 should 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 the appendix "Database Utilities" in this book.

To import tokens:

1. Log in to the Primary Server as the RSA ACE/Server fileowner.
2. Start the database brokers:

   ```
   ACEPROG/sdconnect start
   ```

3. Run the RSA ACE/Server administration program:

   ```
   ACEPROG/sdadmin
   ```

   See "Interface Conventions" on page 96 for instructions on how to use the Server administration program.

4. Select **Import Tokens** from the Token menu.
5. Enter the path and filename of the token record file you extracted from the diskette that was included in your initial RSA ACE/Server software package.

Implementing RSA SecurID Authentication for a User

The following procedure describes how to add a user to the RSA ACE/Server 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 ACE/Server. With local authentication, the RSA ACE/Server is also acting as the Agent Host (both the RSA ACE/Server and the RSA ACE/Agent reside on the same machine). So, when the test user logs in to the Server, he or she is prompted for RSA SecurID authentication.

Important: Do not use the RSA ACE/Server 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 ACE/Server administration program, create a local user record for a test user. Select **User > Add User**. Enter the appropriate information. Select **OK** to close the Add User dialog box.
2. Assign a token to the test user. Select **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. Select **List Agent Hosts** on the Agent Host menu to see if the Primary and Replica Servers are registered as Agent Hosts.
4. If the Primary or Replica Server is not registered as an Agent Host, select **Add Agent Host**, enter the hostname of the machine, select **Agent type: UNIX**, 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 ACE/Server correctly.

To test RSA SecurID authentication:

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

   ```
   ACEPROG/sdconnect start
   ACEPROG/aceserver start
   ```
2. Run the test authentication utility. Type

   ```
   ACEPROG/sdtestauth
   ```

   You should be 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 get a personal identification number (PIN).

4. When you have received or chosen your PIN, you will be prompted again for a passcode. Wait for a new tokencode, then respond by entering 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 denied access consistently, in spite of having performed all installation and setup procedures as directed and having entered valid passcodes, refer to the appendix "Troubleshooting (UNIX)" in the *RSA ACE/Server 5.2 Administrator's Guide*. If you are unable to resolve the problem, call RSA Security Customer Support.

Preparing the System for Replica Server Support

1. If you have not done so already, verify that the Replica Server workstation meets all system requirements listed in the chapter "RSA ACE/Server Requirements" in this book.
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 Server. See page 17 for a list of the default service names and port numbers.
4. If necessary, every 24 hours the Primary Server/Replica Server communications program **acesyncd** will adjust the Replica Server system clock to match the Primary Server system clock. If this is a first-time installation and the Primary Server and Replica Server system clocks are not in sync, this change could upset scheduled tasks and other time-based applications. Avoid problems by changing the Replica Server clock yourself and making all the adjustments this may require. If you are upgrading existing Servers, this step should be unnecessary.

   Note: You must have root privileges to make changes to the Replica Server 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 Server. For UNIX Agent Hosts and certain other RSA ACE/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 Server pairs.
6. Other Agent types, such as third-party devices, may require changes to their configuration files. Refer to the documentation on each Agent type for information on updating its configuration.

7. Follow the instructions in the next section to add a Replica Server to the database.

   If you are performing an automatic migration of the database as part of an upgrade, skip the next two sections and go to "Installing the Replica Server Software" on page 34.

Adding Replica Servers to the Database

Before you can install the RSA ACE/Server software on a Replica, you must add each Replica Server 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 Replica Servers to the Database:

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

   ```
   ACEUTILS/rptconnect stop
   ```

3. Stop the RSA ACE/Server 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 will be resolved automatically.
   - 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 1.
   - 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).
   - The alias IP addresses used by the Replica, which can be used to configure Agent Hosts that need to authenticate through a firewall.
6. Repeat step 5 for each Replica Server 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 *RSA ACE/Server 5.2 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 Replica Servers to the Database."

To create the Replica Package:

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

   ```
   ACEUTILS/rptconnect stop
   ```

3. Stop the RSA ACE/Server 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 the **license** directory only to each Replica. The Primary will push the database files after you install and start the Replica Server.

   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 ACE/Server 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 will send to the Replica on the first replication pass. The longer you wait to create and install the Replica Package, the more changes the Primary will 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 Server software.

Installing the Replica Server Software

The installation procedure in this section assumes that the RSA ACE/Server 5.2 CD can be mounted on your Server workstation. If the target Server workstation does not have a local CD drive, you can use NFS facilities to export the CD drive mount point to the target Server 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 Server software:

1. Log in to the Replica Server 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	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/aceserv/*platform*** directory from which you will install, where ***platform*** is the abbreviation for your operating system.

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

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

5. The command to start Replica Server installation is

```
/cdrom/aceserv/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, this argument allows you to re-install 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 ACE/Server directory you selected or created during Server preparation. Use the same pathname on the Replica Servers and the Primary Server.
-R *path*	Specify the pathname of the directory that contains the Replica Package files you copied from the Primary Server to the Replica Server.

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 ACE/Server Directory

Supply the pathname of the directory you selected or created during Server preparation. The path you specify will contain all RSA ACE/Server subdirectories, databases, and program files. Use the same pathname on the Replica Servers and the Primary Server.

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 re-install or upgrade RSA ACE/Server software, the contents of **ace_tmp** will be lost permanently when overwritten by this installation.

Completing the Replica Server Installation

The installation program notifies you and displays the Server 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. See the chapter “Overview” in the *RSA ACE/Server 5.2 Administrator’s Guide* for more information about licenses.

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. If the latter is true, see the appendix “Configuring the RSA ACE/Server (UNIX)” in the *RSA ACE/Server 5.2 Administrator’s Guide* for instructions on modifying the Server configuration file so that it contains the service names and port numbers you want to use.

Monitoring Startup Processes

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

```
ACEPROG/sdlogmon -t
```

This will display the Log Monitor, and you will be able to see that communication has been established between the Primary and the Replica. If PushDB is enabled, you will see messages that this process (copying the database to the Replica) 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.

Starting the Replica

To start the Replica:

1. Log in to the Server as the RSA ACE/Server fileowner.
2. Start the database brokers:

   ```
   ACEPROG/sdconnect start
   ```

   A series of messages will follow, 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, skip 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 will follow, indicating that RSA ACE/Server is starting. When startup is complete, a message informs you that:

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

   The Replica Server is now ready to authenticate users.

Next Steps

Important: You must make backup copies of your license after you install the RSA ACE/Server 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 diskettes. The only way to regain access is with the modified license files.

If you loaded RADIUS data during the Primary installation, see the chapter "The RSA RADIUS Server" in this book for more information on configuring your RSA ACE/Server to run the RSA RADIUS server software.

To install a TACACS+ device and to turn on RSA ACE/Server support for the TACACS+ protocol, go to the chapter "RSA ACE/Server TACACS+ Support" in this book.

3 Upgrading to RSA ACE/Server 5.2

You can upgrade to RSA ACE/Server 5.2 if you are running RSA ACE/Server 5.0 or 5.1, including any allowable patch.

Note: Throughout this chapter, the term *5.x* is used to indicate either RSA ACE/Server 5.0 or 5.1, or any allowable patch.

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 ACE/Server 5.2 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 ACE/Server 5.2.

When the RSA ACE/Server installation program finds a version 5.*x* 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 5.2 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

Before you upgrade, use this checklist to verify that you have all the necessary hardware, software, and information.

- ❑ A machine that meets all the hardware, diskspace, memory and platform requirements described in the chapter "RSA ACE/Server Requirements" in this book.
- ❑ Root and administrator privileges on the Primary and Replica Servers.
- ❑ A supported version of the RSA ACE/Server software installed on a Server.
- ❑ Sufficient disk space (preferably on another system) to create backup copies of the existing Primary Server **sdserv** and **sdlog** database files and the existing Replica Server **sdserv** database files.

  Note: Stop all RSA ACE/Server processes before creating the backup.

- ❑ The name and IP address of any Replica Servers you want to add.

- If you are performing an upgrade in which you install the Primary on a new machine, the license files from your existing Primary Server. If you have received new license files, RSA Security recommends that you apply them after you perform the upgrade.

  Important: If you are upgrading from an RSA ACE/Server 5.1 Advanced license to an RSA ACE/Server 5.2 Advanced license, you must obtain new license files from RSA Security and apply them after you perform the upgrade. Be aware that your RSA ACE/Server will be in *upgrade violation* mode until you apply the new license. Upgrade violation mode effectively turns your license into a 90-day temporary license. When your license expires, it goes into *violation* mode, meaning you are prevented from activating additional users and/or adding new Replicas. For additional information regarding licenses, including how to upgrade your license, see the *RSA ACE/Server 5.2 Administrator's Guide*.

- Access to any existing RADIUS user file, client file, or dictionary file, if you have never loaded RADIUS data or used the RSA RADIUS server, but plan to use it now.

  If you choose to load RADIUS data, you will be prompted for the location of the RADIUS data files.

- The port number for RADIUS authentications, if you are enabling the RSA RADIUS server. The default port number is **1645**.

- The RSA ACE/Server 5.2 CD.

Preparing for the Primary Server Upgrade

Before you upgrade the RSA ACE/Server software, log in to the Primary Server as an administrator, and perform these tasks:

Task 1: Stop the RSA ACE/Server Services on the Primary Server

You cannot upgrade the RSA ACE/Server software while RSA ACE/Server services are running on the Server you want to upgrade.

Stop all RSA ACE/Server programs and database brokers running on the Primary Server. When you stop **aceserver** on the Primary Server, the Replica Servers continue to authenticate users and log activity, but you will not be able to administer the database.

Stopping the RSA ACE/Server

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 Server

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

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.

You are ready to upgrade the Primary Server. Go to the following section "Upgrading a Primary Server".

Upgrading a Primary Server

The procedures for upgrading a Primary are described in the chapter "Installing the RSA ACE/Server" in this book, in the sections listed below:

- "Installing the Primary Server 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
```

If the RSA RADIUS server is enabled, it starts when you start the RSA ACE/Server.

Preparing for a Replica Server Upgrade

Before you upgrade a Replica, perform these tasks:

Task 1: Copy the License Files from the Primary Server

The Primary Server 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). Copy the **license** directory from this location to a directory that is outside of the RSA ACE/Server directory on the Replica Server.

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

Task 2: Stop All RSA ACE/Server Services on the Replica Server

You cannot upgrade the RSA ACE/Server software while RSA ACE/Server services are running on the Server you want to upgrade. See "Stopping the RSA ACE/Server" on page 41.

You are ready to upgrade the Replica Server. Go to the following section "Upgrading a Replica" for instructions.

Upgrading a Replica

The procedures for upgrading a Replica are described in the chapter "Installing the RSA ACE/Server" in this book, in the sections listed below:

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

Follow the instructions in these two sections and then return here.

Next Steps

If you loaded RADIUS data during the Primary installation, see the chapter "The RSA RADIUS Server" in this book for more information on configuring your RSA ACE/Server to run the RSA RADIUS server software.

To install a TACACS+ device and to turn on RSA ACE/Server support for the TACACS+ protocol, go to the chapter "RSA ACE/Server TACACS+ Support" in this book.

4 Installing Remote Administration Software

Remote administration provides a graphical user interface for administering an RSA ACE/Server 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 ACE/Server database on a UNIX platform can be performed from machines running

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

You can also use the browser-based RSA ACE/Server Quick Admin software to perform some common tasks, but Quick Admin does not allow full administration of the database. See the chapter "Installing the Quick Admin Software" in this book for more information.

Note: You can remotely administer the database on the Primary Server or a Replica Server, but the connection to a Replica Server is read-only. When connected to a Replica Server, you can run reports, run the log monitor, and view database information, but you cannot make administrative changes to the database.

Configuring Remote Administration Authentication Methods

By default, the RSA ACE/Server is configured to allow remote administration. However, you must select the types of tokens (or authentication *methods*) that remote administrators will use when logging in by way of Remote Administration. The administrator authentication methods include **SecurID Cards and Fobs**, **Lost Token Passwords**, **SecurID Software Tokens**, and **User Passwords**.

To configure administrator authentication methods:

1. On the Primary Server, change to the ***ACEPROG*** directory, and run **sdadmin**.
2. On the **System** menu, select **Systems Parameters**.
3. Under **Administrator authentication methods**, select the methods that will be used to authenticate remote administrators.

Installation/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 ACE/Server Remote Administration software.

- ❑ A machine with an Intel Pentium processor running Windows NT, Windows 2000 Professional, Windows XP Professional, or Windows 98. For more information on hardware, disk space, and memory requirements, see the chapter "RSA ACE/Server Requirements" in this book.

  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, it must be running Windows NT, Windows 2000 Professional or Windows XP Professional, and have the RSA ACE/Agent for Windows software installed.

- ❑ A supported version of the RSA ACE/Server software installed on a Primary Server.

  The version of the RSA ACE/Server 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 ACE/Server, you cannot remotely administer an RSA ACE/Server 5.2 database until you upgrade the Remote Administration software. If you upgrade Remote administration software, you will no longer be able to administer a pre-5.1 database from the machine running the upgraded Remote Administration software.

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

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

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. Copy only the **sdconf.rec** and **server.cer** files on the Primary Server to a diskette.
2. Log in on the Windows remote machine, and insert the RSA ACE/Server 5.2 CD.
3. Insert the diskette containing the **sdconf.rec** and **server.cer** files into the diskette drive.
4. In the **aceserv\nt_i386** directory on the RSA ACE/Server CD, double-click **setup.exe**.
5. 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**.
6. Follow the prompts until the Installation Options dialog box opens. Check **New Remote Administration**, and click **Next**.
7. Follow the prompts until the installation process is complete.
8. 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 NT, Windows 2000 or Windows XP Professional machine, the **hosts** file is in ***%SystemRoot%*\System32\drivers\etc**. On a Windows 98 machine, the **hosts** file is in the **Windows** directory.

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 re-install Remote RADIUS.

To upgrade the Remote Administration software:

1. On the remote machine, log in as a local administrator, and insert the RSA ACE/Server 5.2 CD into the CD drive.
2. In the **aceserv\nt_i386** directory on the RSA ACE/Server CD, double-click **setup.exe**.
3. Follow the prompts until the Installation Options dialog box opens. Check **Upgrade Remote Administration**, and click **Next**.
4. Follow the prompts until the installation process is complete.

Adding an RSA ACE/Server to Administer Remotely

If you need to administer additional RSA ACE/Servers from a machine running the Remote Administration software, follow the instructions in this section. This section assumes that you have already installed the Remote Administration software as described on page 44.

During the procedure, you will be 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. Scroll down to and select **RSA ACE/Server for Windows**, and click **Add/Remove.**
   The RSA ACE/Server 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 ACE/Server 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 verify that you can resolve the Remote Administration machine from the Server you want to administer. See "Hostnames" on page 13 for the requirements for entries in the **hosts** file.
   On a Windows NT, Windows 2000 or Windows XP Professional machine, the **hosts** file is in ***%SystemRoot%*\System32\drivers\etc**. On a Windows 98 machine, the **hosts** file is in the **Windows** directory.
   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 ACE/Server. You can limit the number of ports that can be opened at the same time (and thereby limit 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 ACE/Server.

To specify a range of port numbers:

1. Stop the Report Creation utility. Type

   ```
   ACEUTILS/rptconnect stop
   ```

2. Stop the RSA ACE/Server 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 it uses is always one greater than the specified minimum port number, so the range of ports you specify 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, you would add these lines to the file:

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

   Note: Make sure that the range of port numbers you specify does not include port numbers used by other services.

5. Restart the RSA ACE/Server. Type

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

5 The RSA RADIUS Server

This chapter describes how to configure the RSA ACE/Server for UNIX to support the RSA RADIUS server. Use the procedures in this section when you want to configure and enable RADIUS *after* the installation of the RSA ACE/Server software.

Note: On UNIX platforms, the RSA RADIUS server must be installed on the same machine as the RSA ACE/Server. If you want to run an RSA RADIUS server on a separate machine, you must install the RADIUS software on a Windows-based machine. For more information on installing a remote RADIUS server, see the chapter "The RADIUS Server" in the *RSA ACE/Server 5.2 for Windows Installation Guide*.

Overview

The RSA RADIUS server runs on any RSA ACE/Server Primary or Replica machine.The RADIUS software is installed on each RSA ACE/Server by default. However, to use the RADIUS server, you must perform the following tasks:

- Configure the service name and port number that is used for RADIUS.
- Load RADIUS data into the database on the Primary.

  Loading RADIUS data allows you to specify existing RADIUS data files that you may want to use and loads the dictionary file, which contains the attributes and values you will need to create and assign RADIUS profiles to users.
- Enable RADIUS in the configuration file (**sdconf.rec**) of each RSA ACE/Server that you want to use as a RADIUS server.

  Enabling RADIUS in the configuration file causes the RADIUS daemon on the Server to start when the RSA ACE/Server starts.

You can perform these tasks during the Primary Server installation by responding **Yes** to the "Would you like to configure radius now?" prompt. If you respond **Yes**, the installation process

- Prompts you for the RADIUS server service name (default name **radius**) and the RADIUS port number (default value **1645**).
- Prompts you for the types and locations of any existing RADIUS data files (dictionary, user and client files).

  If you have no dictionary file, the default dictionary is used.
- Edits the **sdconf.rec** file on the Primary, so that the RADIUS server is enabled.

The RADIUS data you specify and the edited **sdconf.rec** file are propagated to your Replicas when you create a Replica Package and install the RSA ACE/Server software on the Replicas. If you prefer to limit the number of enabled RADIUS servers, you can disable the RADIUS server on any RSA ACE/Server by editing the Server's **sdconf.rec** file. See "Enabling and Disabling the RADIUS Server" on page 55.

If you want to use a different service name or port number, see "Loading Existing RADIUS Data" on page 51.

If you did not configure RADIUS during the Primary installation, use the information in this chapter to perform the configuration tasks.

Pre-Configuration Checklist

Before you attempt to configure your system to use the RSA RADIUS server, obtain the following information:

- ❑ The RADIUS port number used by any existing RADIUS Network Access Servers (NAS). By default, the RSA RADIUS server uses port 1645 for authentication.
- ❑ The names of any existing NAS devices.

  You must add these devices to the RSA ACE/Server database as Agent Hosts.
- ❑ The NAS Agent type.

  When you add the NAS to the database as an Agent Host, you must specify the Agent type. The NAS is either a **Communication Server** or a **Single-Transaction Comm Server**.
- ❑ The encryption key (or shared secret) used by each NAS.

  You must assign the same encryption key to the NAS Agent Host record in the Server database. RSA Security recommends that each NAS has its own individual encryption key.
- ❑ The names of users and groups who will access the network through each NAS.
- ❑ The IP addresses of any RSA ACE/Server machine functioning as an RSA RADIUS server.

Loading Existing RADIUS Data

Configuring the RSA ACE/Server to act as a RADIUS server requires importing RADIUS data into the RSA ACE/Server database and enabling RADIUS in the configuration file of the Server. You must use the **sdsetup -radius** command to perform these two tasks.

When run on the Primary, **sdsetup -radius** prompts you to import existing RADIUS data files (RADIUS user, client, dictionary and map files) and enables RADIUS in the configuration file on the Primary. When run on a Replica, **sdsetup -radius** enables or disables the RADIUS server on the Replica only. RADIUS data cannot be imported into the database on a Replica because database administrative tasks require a connection to the Primary database.

If you have no existing RADIUS data files, you must run **sdsetup -radius** to import the default RSA RADIUS dictionary and map files.

You can also use the RSA RADIUS utilities described in "RADIUS Utilities" on page 52 to import RADIUS data files. Use the **sdsetup -radius** command when you import files for the first time.

RADIUS accounting provides you with the ability to gather connection information about your users. You can configure the location of the RADIUS accounting directory by using the RADIUS Configuration Utility described in the appendix "Configuring the RADIUS Server" in the *RSA ACE/Server 5.2 Administrator's Guide*.

To load RADIUS data:

1. Log in to the Primary Server as **root** or as an RSA ACE/Server administrator, and change to the ***ACEPROG*** directory.
2. Type **sdsetup -radius**.
3. Answer **y** at the following prompt:

   ```
   Do you want to configure radius now? (y/n) [n]:
   ```

   Answering **y** prompts you for any existing RADIUS data files that you want to import. The following table describes the RADIUS data files you can import.

File Type	Description
RADIUS Users File	RADIUS account information about users.
RADIUS Clients File	Devices that support RADIUS logins.
RADIUS Dictionary File	Definitions of Attributes and Values. RSA Security's RADIUS product ships with a default dictionary.
RADIUS SecurID Map File	A mapping file that dictates which attributes in the dictionary can be configured and which attributes can be multiply defined.

4. To import an existing dictionary, answer **y** at the following prompt:

   ```
   Do you have your own dictionary file? (y/n) [n]:
   ```

   When prompted for the pathname, specify the location of your dictionary file. If you have no dictionary file, the default RSA RADIUS dictionary file is used.

5. To import an existing map file, answer **y** at the following prompt:

   ```
   Do you have your own securid map file? (y/n) [n]:
   ```

   When prompted for the pathname, specify the location of your map file. If you have ever edited the **securid** map file, specify the location of the edited file. If you answer **n**, the default map file is used, and any changes you have made are lost.

6. To import an existing RADIUS clients file, answer **y** at the following prompt:

   ```
   Do you wish to migrate RADIUS clients? (y/n) [n]:
   ```

   When prompted for the pathname, specify the location of your clients file.

7. To import an existing RADIUS users file, answer **y** at the following prompt:

   ```
   Do you wish to migrate RADIUS users? (y/n) [n]:
   ```

   When prompted for the pathname, specify the location of your users file.

   After you respond to these prompts, the program that configures RADIUS begins.

   If you want to use the RADIUS server on a Replica, you must enable RADIUS on the Replica. You cannot import RADIUS files to the Replica.

RADIUS Utilities

When you enable RADIUS after the Primary Server installation is completed, you can use data, including a dictionary file, user profiles, and client files, from an existing RADIUS installation. The RSA ACE/Server also includes four programs that you can use to load and edit RADIUS data files:

Program	Purpose
loadraddb	Loads the default dictionary or an existing dictionary that you specify.
removeattr	Edits the **securid** map file, which determines which attributes are user-configurable and multiply-defined.
loadraduser	Imports an existing RADIUS user file.
loadradcli	Imports an existing RADIUS client file and creates an Agent Host record in the RSA ACE/Server database.

The following sections describe how to run these programs after installing or upgrading RSA ACE/Server.

Importing a Dictionary File

The **loadraddb** program loads the dictionary file. Use **loadraddb** under the following conditions:

- You did not load RADIUS data during the installation on the Primary and you now want to load RADIUS data.
- You edit the existing dictionary file to add or delete an attribute.

If you add a non-compliant attribute to the dictionary file, by default the attribute will display in the Database Administration application. Certain attributes can be added to the **dictionary** and the Database Administration application will not display them.

Note: If you remove an RFC-compliant attribute, then add it back into the dictionary and load the dictionary, the attribute will not display in the Database Administration application until you edit the map file (**securidmapfile**) to display the attribute. Open the map file in a text editor, change the **User Config** value for the attribute from **0** to **1** and save the file.

To load the dictionary, type:

```
loadraddb xyzzy ACEDATA/dictionary ACEDATA/securidmapfile
[-p]
```

where

- **xyzzy** is the password required to run loadraddb. In all cases, the password is **xyzzy**.
- ***dictionary*** is the name of the dictionary file.
- **-p** is an optional parameter that deletes all values from any profiles in the RSA ACE/Server database before the dictionary is reloaded.

Note: Running **loadraddb** requires a password, which is **xyzzy**. You must type **loadraddb xyzzy** to load the dictionary.

Removing Attributes

The **removeattr** program is a command line utility that removes attributes from the RSA ACE/Server database, removes individual attributes from any RADIUS profile that contains the attribute and disables RFC-compliant attributes in the RSA SecurID map file. Disabling an attribute in the map file makes the attribute unavailable for inclusion in RADIUS profiles.

To remove a RADIUS attribute:

1. From the command line, change to the ***ACEPROG*** directory.
2. Type

   ```
   removeattr xyzzy ACEDATA/securidmapfile
   -rattribute_number
   ```

   where

   - **xyzzy** is the hardcoded password required to run the **removeattr** program.
   - **securidmapfile** is the RSA RADIUS attribute mapfile.
   - ***attribute_number*** is the integer encoding of the attribute.

   Note: The "Additional Administrative Tasks" chapter of the *RSA ACE/Server 5.2 Administrator's Guide* contains the integer encodings for the supported, standard RADIUS attributes.

3. Repeat this procedure for each attribute you want to remove.

Importing User and Client Files

The **loadraduser** program

- Creates a profile (***loginname*Profile**) for each user in the RADIUS user data file
- Creates a user record if there is no existing user record for the login name in the Server database
- Assigns the profile to the user record that contains the login name

Although each profile name is unique, the profiles may contain the same attributes and values. For example, you may have created one profile and assigned it to many users. When you import these user data files, **loadraduser** creates multiple profiles, one for each user. To ease administration, after you run **loadraduser**, you can unassign these profiles and create a default profile (named **Default**) that is assigned to all users without assigned profiles.

You can run **loadraduser** and **loadradcli** at any time that you need to load additional RADIUS user or client data files. At the command prompt, type the command followed by the full pathname of the file, and press ENTER.

Data	Command
User profiles	**loadraduser *userfile***
The client on which users are activated*	**loadradcli *clientfile***
User profiles and activate the users on a client that has already been imported**	**loadraduser *userfile clientfile***

*An Agent Host record for each client in the client file is created in the RSA ACE/Server database.

**The user data file you specify is loaded into the database, Agent Host records are created for each client in the client file, and the users are activated on the Agent Hosts.

Enabling and Disabling the RADIUS Server

The RADIUS server is enabled on the Primary by default when you import RADIUS data into the RSA ACE/Server database. When the **sdconf.rec** file is distributed to the Replicas for any reason, the setting in the new configuration file overwrites the existing settings. Depending upon how you have configured the Primary and the Replicas, you may need to re-enable or disable the RADIUS server on a Replica after copying the **sdconf.rec** file.

To enable RADIUS on a Primary Server:

1. Log in to the Primary Server as **root** or as an RSA ACE/Server administrator, and change to the ***ACEPROG*** directory.
2. Type **sdsetup -radius**.
3. Answer **y** at the following prompt:

   ```
   Do you want to configure radius now? (y/n) [n]:
   ```

4. Answer **n** at each of the four prompts for importing RADIUS data.
   After the last prompt displays, RADIUS is enabled.

To enable RADIUS on a Replica Server:

1. Log in to the Replica Server as **root** or as an RSA ACE/Server administrator, and change to the ***ACEPROG*** directory.
2. Type **sdsetup -radius**.
3. Answer **y** at the following prompt:

   ```
   Do you want to configure radius now? (y/n) [n]:
   ```

   RADIUS is enabled.

To disable RADIUS on a Server:

1. Log in to the Server as **root** or as an RSA ACE/Server administrator, and change to the ***ACEPROG*** directory.
2. Type **sdsetup -radius**.
3. Answer **n** at the following prompt:

   ```
   Do you want to configure radius now? (y/n) [n]:
   ```

   RADIUS is disabled.

Configuring RADIUS Services on the RSA ACE/Server

The RSA ACE/Server configuration file **sdconf.rec** must indicate that RADIUS is enabled and must contain the RADIUS service name and port number. This information is read during RSA ACE/Server startup and indicates that the RADIUS daemon must be started also. Run **sdsetup -config** according to the following procedure to ensure that the correct RADIUS information is included in the **sdconf.rec** file.

To configure RADIUS services on the RSA ACE/Server

1. Log in as **root** or as an RSA ACE/Server administrator on the Primary Server.
2. Change to the ***ACEPROG*** directory, and run **sdsetup -config**.
3. You will be asked a series of RSA ACE/Server configuration questions. Press ENTER through the first several prompts, as the questions are not related to RADIUS support.
4. Enable RADIUS by answering **y** at the following prompt:

   ```
   Do you want to enable RADIUS? [y]:
   ```

5. At the following prompt, accept the default or specify the port number that will be used for RADIUS authentication:

   ```
   Which port number should RADIUS use? [1645]:
   ```

   If you enter a different port number, it must match the port number specified in the **/etc/services** file on the Server. The default port number is **1645**.
6. At the following prompt, accept the default or specify the service name for RADIUS:

   ```
   What is the service name you will use? [radius]:
   ```

   If you enter a different service name, it must match the service name specified in the Server **/etc/services** file. The default service name is **radius**.
7. Accept the default values for the remaining prompts.

Note: When you make changes to the configuration record, you are sometimes required to copy the updated **sdconf.rec** file to a Replica. If you copy a configuration file from a Server that does not have the RADIUS server enabled to a Replica that does have the RADIUS server enabled, you disable the RADIUS server. Either make the same changes to the configuration record on the Replica with RADIUS enabled, or enable the RADIUS server each time you copy an updated **sdconf.rec** file from a Server that does not have the RADIUS server enabled.

Adding Servers as Agent Hosts to the Primary Database

After configuring the RSA ACE/Server to use RADIUS, you need to add the RSA ACE/Server and each NAS to the Server database as Agent Hosts. See the Help topic "Add Agent Host" for instructions. The following procedure contains only the specific information you need to add the RSA ACE/Server and the NAS devices to the database using the Remote Administration software.

To add an Agent Host:

1. On the Remote Administration machine, click **Start** > **Programs** > **RSA ACE/Server** > **Data Administration - Remote Mode**.
2. If necessary, add the Server as an Agent Host. Click **Agent Host** > **Add Agent Host**, and type the name of Server in the **Name** box.
   - As the Agent type, select **UNIX Agent**.
   - Do not activate any RADIUS users directly on this Agent Host.
3. Add each NAS device as an Agent Host.
   - As the Agent type, select **Communication Server** or **Single Transaction Server**, as appropriate.
   - Click **Assign/Change Encryption Key**, and enter the same encryption key assigned on the NAS you are adding.
   - Activate all users and groups who are authorized to access the system through this Agent Host, or click **Open to All Locally Known Users** to allow all users in the Server database to authenticate through this Agent Host.
   - None of these users or groups need to be activated on the RSA ACE/Server system Agent Host.

Configuring the RADIUS Server

To optimize the performance of the RADIUS server in your network, you can set parameters that control the operation of the server in several ways, including the following:

- How to deal with defective or duplicated packets
- Whether accounting packets are processed, and if so, where accounting data is stored and how it is reported
- The number of invalid responses users are allowed before they are denied access
- Whether and how data is cached to improve performance
- How prompts for users are phrased
- How user profile data is handled in response packets

You can use the RSA RADIUS Server Configuration Utility to set these parameters. Run **rtconfig** (located by default in the ***ACEPROG*** directory) to display a window where you can select RADIUS server parameters and change their values. Parameters are displayed on seven tabs, grouped according to function, with Help for each tab and each parameter. When you save changes made through this utility, they are written to the **radius.cfg** file in the ***ACEDATA*** directory. (For more information, see the appendix "Configuring the RADIUS Server" in the *RSA ACE/Server 5.2 Administrator's Guide*.

Configuring a RADIUS Device

This section describes how to configure a RADIUS network access server. This server acts as a RADIUS client and passes user information to the RADIUS server. See the NAS device manual for specific configuration instructions.

Make sure that your RADIUS device is configured to meet these requirements:

- An encryption key is specified on the NAS device and provided to the RSA ACE/Server when the device is added as an Agent Host. The maximum key length is 48 characters.
- The Primary and Replica Servers must be specified as RADIUS server hosts on the NAS device.
- The RADIUS port number specified on the NAS device must match the port number on the Primary Server specified through **sdsetup**.
- The default port number for RADIUS authentication is 1645.
- The RADIUS accounting port number specified on the NAS device must be one greater than the RADIUS port number specified during Server configuration.

  The default port for RADIUS accounting is 1646.

RADIUS Data File Formats

There are four RADIUS data files. If you edit the any of the files, you must adhere to the file formats described in this section. If you edit the dictionary, or create or edit user or client files, you must import edited files to the database using the utilities described in "RADIUS Utilities" on page 52.

Dictionary

The dictionary file contains the RFC-compliant RADIUS attributes and values. The RSA RADIUS server supports the attributes and values described in RFC-2865 and RFC-2866. The file contains two types of entries:

- ATTRIBUTE, which contains the name of the attribute, the integer encoding of the attribute, and the attribute type (string, integer, date, or ipaddr)
- VALUE, which lists the possible values for the attribute

If you add attributes to the dictionary, they will be available for inclusion in user profiles unless you specifically restrict them as not user-configurable in the RSA SecurID map file described in the following section "Map File."

Map File

The RSA SecurID map file determines which attributes are user-configurable and which attributes can be multiply-defined. You can add user-configurable attributes to RADIUS profiles that you assign to users. If an attribute is not user-configurable, you cannot add it to a profile. If an attribute is multiply-defined, you can include more than one instance of the attribute in a RADIUS profile.

The RSA SecurID map file contains a line for each attribute, and each line must include the attribute name and two integers. The first integer indicates that the attribute is user configurable (1) or not user-configurable (0). The second integer indicates that the attribute can be multiply-defined (1) or that it cannot be multiply-defined (0).

For example,

```
User-Name        10
User-Password    00
CHAP-Password    00
NAS-IP-Address   00
NAS-Port         00
Service-Type     10
Framed-Protocol  10
```

User File

The user file contains the user login name, and the attributes (and their values) in the user's profile. The following text is a sample user file:

```
User1 Service-Type=Login,
      Login-Service=Telnet,
      Login-IP-Host=10.100.104.65

User2 Service-Type=framed,
      Framed-Protocol=PPP,
      Framed-IP-Address=192.168.40.214,
      Framed-IP-Netmask=255.255.0.0,
      Framed-Routing=broadcast-listen,
      Framed-MTU=1500,
      Framed-Compression=Van-Jacobsen-tcp-ip

User3 Service-Type=Login,
      Login-Service=Telnet,
      Login-IP-Host=10.100.104.67
```

The login name and the first attribute must be on the first line, and the remaining attributes on separate lines. The information for each user must be separated by a blank line.

Client File

The client file contains the IP address of the client, and the secret key shared between the RADIUS server and the client. The following text is a sample client file:

```
# Client Name Key

shiva_sqa 1111
ce_cisco 5678
192.168.10.23 123abc
192.168.10.22 68932
192.168.10.24 98882
```

Each IP address and secret must be on a separate line.

Next Steps

See the appendix "Configuring the RADIUS Server" in the *RSA ACE/Server 5.2 Administrator's Guide* for information about configuring the RSA RADIUS Server.

See "Creating and Modifying Profiles for RADIUS Users" in the chapter "Additional Administrative Tasks" in the *RSA ACE/Server 5.2 Administrator's Guide* for information about how to create a generic RADIUS user profile.

Note: You must install the Remote Administration software on a Windows machine before you can use the Database Administration application to create or edit RADIUS user profiles.

6 RSA ACE/Server TACACS+ Support

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

RSA ACE/Server supports RSA SecurID access control for routers and communication servers running TACACS+ v 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 ACE/Server Next Tokencode and New PIN modes.

TACACS support is provided through Cisco-developed security software made up of client and server code. The client code is shipped as part of the standard software distribution with Cisco and other routers and communication servers. The server code has been integrated with the RSA ACE/Server.

This chapter provides information that will enable you to

- Configure the RSA ACE/Server to support a TACACS+ client device and to configure a TACACS+ client device.
- Protect 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.

The startup file is

ACEDATA/sdtacplus.arg

The startup file provides command line arguments needed for the Cisco 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 ACE/Server system is started with TACACS+ support enabled, it looks for the configuration file specified in the startup file.

Authenticating on a TACACS+ Device

Authentication of TACACS+ Users

1. When a user initiates a login session via a protected port, that user is prompted for a username.
2. After the username 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 Server. For information on encryption, see "Sample TACACS+ Configuration File" on page 65.
3. When the request is received by **_sdtacplusd**, it invokes RSA ACE/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 Server sends the result to the client device, which displays the message **PASSCODE Accepted** or **Access Denied**, or performs the New PIN or Next Tokencode operation, if necessary.

   After a specified number of unsuccessful retries, the client reports **Authentication failed**, the connection is broken, and the login 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 ACE/Server database. Choose **Communication Server** as the Agent type. Activate users or groups of users on the TACACS+ device. See the Help topic "Add Agent Host" for instructions.
2. Exit the Database Administration application.
3. Verify that the following line appears in **/etc/services**:

   ```
   tacacs49/tcp
   ```
4. If your system is not already configured for TACACS+ support, run **sdsetup -config** to turn it on. See "Changing the Configuration" in the appendix "Configuring the RSA ACE/Server (UNIX)" in the *RSA ACE/Server 5.2 Administrator's Guide* for information on running **sdsetup -config**.

5. If you had an existing, customized **sdtacplus** argument and configuration files before you installed RSA ACE/Server 5.2, 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 should 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.

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

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 in 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 ACE/Server 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 skip it you must refer to the host by its IP address in all subsequent steps. Subsequent instructions assume that you made this association. Example:

   ```
   ip host cassatt 192.168.10.23
   ```

   For a Replica Server, make the same association for it.

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

   ```
   tacacs-server host hostname
   ```

   If at any time you want to remove TACACS+ and RSA ACE/Server 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 Server hostname using another **tacacs-server host** command.

   The order in which you specify the Server hostnames will determine the order in which the client device searches for a valid RSA ACE/Server.

7. Set the number of login attempts that can be made on a TACACS-protected line. The RSA ACE/Server 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 will prevail.*

   Allowing three attempts before disconnection offers a good balance between user convenience and security. Decrease the number for even tighter security. However, this will make logging in less convenient for users who mistype their passcode and have to reinitiate a login 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 login attempts. Realize that this value is capped by the RSA ACE/Server 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 will search through the RSA ACE/Server host list to find a Server 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 even tighter security. However, doing so will make logging in less convenient for users who have to reinitiate a session if no Server 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 a Server.

   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 will wait for a response from the RSA ACE/Server. The default value for a Cisco 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 even higher than 10 seconds if users experience long delays after entering their passcode, get the message **Access Denied**, and are then reprompted for their username.

   To increase the number of seconds, type

   ```
   tacacs-server timeout seconds
   ```

   where ***seconds*** is the time interval.

10. To turn on TACACS+ on the device, be sure to add

    ```
    aaa new-model
    ```

    List the authentication methods, including RSA SecurID authentication, to be used on each of the lines that are to be protected. 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 in will be asked for an RSA SecurID passcode. If this fails, they will be 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 down or the TACACS+ server is not running—the second authentication method in the list_name **securid2** will be used. With **securid2** specified, users logging in will be asked for an RSA SecurID passcode. If this method fails, they will be 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 that are to be protected. 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 Servers, then you as administrator can still log in 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 will not be controlled by the RSA ACE/Server. All other virtual lines in the device will require RSA SecurID authentication.

You may want to implement such a configuration in case communication between the device and the RSA ACE/Server is ever lost. This is especially important if you have a single Primary Server with no Replica Server. If the single Server 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 ACE/Server 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 would be useful to you as an administrator if RSA SecurID authentication were to fail because the Server was down 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 Server is not running or the connection to the Servers is lost, you as administrator can still log in to the client device through this line, using the password defined for it.

14. With TACACS+, messages sent between the client and Server 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 Server 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 logins to check 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 power off or unplug the client device.

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

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

Protecting Enable Mode

Follow the directions in this section to protect Enable mode with RSA SecurID. When configuration is complete, a user designated in the RSA ACE/Server 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 will see an **Enter PASSCODE** prompt but will not gain access. There are two methods of protecting Enable mode:

- Authenticate all users and allow only designated RSA ACE/Server 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. Non-administrators and unauthorized users will not be able to enter Enable mode, even though they will see an **Enter PASSCODE** prompt.

If there is a failure in the TACACS+ authentication, such as if the RSA ACE/Server is down or the connection to the Servers 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
}
```

This will give *username* permission to be authorized always. You can place other user-level commands within the braces, but these commands must follow the **default service = permit** line.

7 Installing the Quick Admin Software

This chapter describes how to install the RSA ACE/Server 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 Primary RSA ACE/Server database.

For more information about Quick Admin, see the *RSA ACE/Server 5.2 Administrator's Guide* and the Quick Admin Help.

Quick Admin Architecture

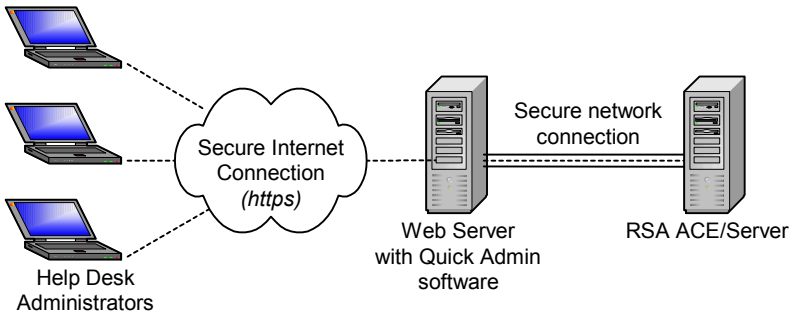
Quick Admin is made up of

- Java servlets, powered by Macromedia Corporation's JRun servlet engine, that are accessible through a web server.
- A back-end daemon that runs on the RSA ACE/Server Primary Server. The daemon manages the encrypted communication between the servlets and the Primary Server database.

Do not install the web server on the same machine as the RSA ACE/Server.

Important: For security purposes, RSA Security strongly recommends that you follow the latest Macromedia Corporation guidelines and best practices. For more information, go to **http://www.macromedia.com/**.

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
Java Runtime Environment (JRE)	1.3.1.03 or later. You can install this from the RSA ACE/Server 5.2 CD.	1.3.1.03 or later. You can install this from the RSA ACE/Server 5.2 CD.

RSA Security strongly recommends that you

- Use a secure connection (**HTTPS**) to prevent usernames 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, visit Microsoft TechNet at **www.microsoft.com/technet/**.
- Be aware that the Microsoft IIS Lockdown Tool removes the web server scripts directory (usually **c:\inetpub\scripts)**, which is necessary for creating the JRun Connector. If you secure your web server using the Microsoft IIS Lockdown Tool, you must create a new directory on the web server that has execute and script permissions. In step 3 of the JRun Connector Wizard, instead of entering **c:\inetpub\scripts** as the path to your web server scripts directory, enter the new directory path.

Solaris and HP-UX 11i

The following Quick Admin installation requirements are for Solaris 9 on UltraSparc processors and HP-UX11i machines:

- Sun ONE 6.x or iPlanet 5.x web servers (JavaScript-enabled).
- JavaRuntime Environment (included on the RSA ACE/Server 5.2 CD).

RSA Security strongly recommends that you

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

Pre-Installation Checklist and Tasks

Checklist

Before you begin installing the RSA ACE/Server Quick Admin software, make sure you have the following files and information:

- ❑ A copy of the **server.cer** file from the ***ACEDATA*** directory of your Primary RSA ACE/Server.
- ❑ A copy of the **sdti.cer** file from the ***ACEDATA*** directory of your Primary RSA ACE/Server.
- ❑ The fully qualified DNS name of your Primary Server.
- ❑ The IP address of your Primary Server.
- ❑ 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 ***ACEPROG*** directory.

Tasks

Complete the following tasks on the Primary RSA ACE/Server host. For more information about these tasks, see the *RSA ACE/Server 5.2 Administrator's Guide*.

- ❑ Add the host name and IP address of the Quick Admin web server to the **hosts.conf** file in the ***ACEPROG*** directory.

  Note: You must restart the RSA ACE/Server 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 ACE/Server System Parameters to allow Remote Administration.

- ❑ Verify that the RSA ACE/Server Quick Admin daemon is running on the Primary Server.
  - – On Windows hosts, verify this in **Start > Settings > Control Panel > Administrative Tools > Services**.
  - – On UNIX hosts, type

```
ps -ef | grep sdcommd
```

Installing Quick Admin on Windows 2000 and Windows 2003

Before you begin, make sure you have installed the supported IIS web server and the Java Runtime Environment on the web server host. Note the following issues when you install Java Runtime:

- If you are prompted to overwrite any existing **.dll** files on your system, do not do so.
- You may see an erroneous message that begins: **Evaluating your Java Virtual Machine... JRun Java Virtual Machine Advisor**

  The message then says: **No information is available for this JVM. Please refer to your JVM vendor for any further information.**

  You can disregard it. Java Runtime installs successfully even though this message is displayed.

When the installation Wizard completes, you are prompted to perform some minor JRun configuration.

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 RSA ACE/Server 5.2 CD into the CD drive of the web server host, and browse to the ***drive*:\QuickAdmin\Windows** directory, where *drive* is the letter assigned to your CD drive.
3. Double-click the **quickadmin.exe** icon.

   The Quick Admin Setup Wizard opens.
4. Follow the prompts until the Setup Wizard completes, and then click **Finish**.

   JRun opens in your default web browser.
5. If you are running IIS 5.0 web server on Windows 2000, enter the JRun administrator username and password that you specified during installation and go to the following section "To configure JRun:". Otherwise, proceed to step 6.
6. If you are running IIS 6.0 web server on Windows 2003, you must upgrade your JRun Application Server. The upgrade is available from RSA Security at **ftp://ftp.rsasecurity.com/support/Patches/Ace/JRun/31/jrun-31-win-upgrade-us.exe**.

7. Configure the JRun upgrade by following the instructions from RSA Security Customer Support at **ftp://ftp.rsasecurity.com/support/Patches/Ace/JRun/31/31iis6.htm**.
8. Launch JRun, and enter the JRun administrator username and password that you specified during installation.

To configure JRun:

1. In Step 1 of the Wizard:
   - In the **JRun Server Name** box, click **JRun Default Server**.
   - In the **Web Server Type** list, click **Internet Information Server**.
   - In the **Web Server Version** list, for Windows 2000 click **5.0**., and for Windows 2003 click **6.0**.
   - In the **Web Server Platform** list, click **Intel-win**.
   - Click **Next**.
2. In Step 2 of the Wizard:
   - In the **JRun Server IP Address** box, enter **127.0.0.1**, the localhost IP address.
   - In the **JRun Server Connector Port** box, enter the port number the JRun server uses to connect to the web server. The default port is **51000**.
   - Click **Next**.
3. In Step 3 of the Wizard, erase the default path. Then, enter the path to your web server scripts directory (usually **c:\inetpub\scripts**), and click **Next**.

   Note: If you secured your web server using the Microsoft IIS Lockdown Tool, you must create a new directory on the web server that has execute and script permissions. In step 3 of the JRun Connector Wizard, instead of entering **c:\inetpub\scripts** as the path to your web server scripts directory, enter the new directory path.

4. In Step 4 of the Wizard, click **Done**.
5. Close the JRun Management Console.
6. Stop and restart the JRun Default server and restart the World Wide Web Publishing Service in **Start > Settings > Control Panel > Administrative Tools > Services**.

   Note: If you installed JRun as an application instead of a service, use the JRun icons in the system tray to stop and restart.

The RSA ACE/Server Quick Admin is now installed and configured.

To log in 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 Macromedia Corporation guidelines and best practices. For more information, go to **http://www.macromedia.com/**.

Installing Quick Admin on Solaris or HP-UX 11i

Before you begin, make sure you have installed the Java Runtime Environment on the web server host. When the installation is complete, you must perform some minor JRun configurations.

To install the Quick Admin software on UNIX:

1. Stop all web services on the web server.
2. Insert the RSA ACE/Server 5.1 CD into the web server host.
3. Change to the following directory on the CD

   `/cdrom/cd_name/QuickAdmin/UNIX`

   where *cd_name* is the name of the RSA ACE/Server 5.1 CD.
4. Type

   `./jrun-31-unix-us.sh`

   The Quick Admin setup script starts.
5. Follow the instructions on your screen.
6. When the script finishes, point your web browser to the JRun administration URL (the default URL is **http://localhost:8000**).

   The JRun Application Management Console opens.If you are prompted to authenticate, enter the JRun administrator username and password that you specified during installation.

To configure JRun:

1. Click **Connector Wizard**.
2. In Step 1 of the Wizard:
   - In the **JRun Server Name** box, click **JRun Default Server.**
   - In the **Web Server Type** list, click **Netscape Enterprise Server**.
   - In the **Web Server Version** list, if you are using the iPlanet web server, click **4.0/4.1 (iPlanet)**. If you are using the Sun ONE web server, click **6x (iPlanet)**.
   - In the **Web Server Platform** list, click the platform that corresponds to the server you are using.
   - Click **Next**.
3. In Step 2 of the Wizard:
   - In the **JRun Server IP Address** box, enter **127.0.0.1**, the localhost IP address.
   - In the **JRun Server Connector Port** box, enter the port number the JRun server uses to connect to the web server. The default port is **51000**.
   - Click **Next**.

4. In Step 3 of the Wizard, erase the default path. Then, enter the path to your web server scripts directory, and click **Next**.
5. In Step 4 of the Wizard, click **Done**.
6. Stop and restart the JRun Default server.
   From the **.../JRun/bin** directory, type

   ```
   ./jrun restart
   ```
7. Restart your web server.

The RSA ACE/Server Quick Admin is now installed and configured.

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

Important: RSA Security strongly recommends that you stop the JRun Admin server after you finish configuring the Default server. Leaving the Admin server running is a possible security hole. To stop the Admin server, change to the **.../JRun/bin** directory and enter the command **./jrun stop admin**.

Upgrading from Quick Admin 5.1 to Quick Admin 5.2

On a Windows Machine

To upgrade Quick Admin on a Windows machine:

Note: Make sure no admininstrators are in the Quick Admin directories while you perform the upgrade.

1. From the **Start > Settings > Control Panel > Administrative Tools > Services** window, stop the World Wide Web Publishing Service.
2. Stop the JRun Default Server and the JRun Admin Server.
3. Insert the RSA ACE/Server 5.2 CD into the CD drive of the web server host, and browse to the ***drive*:\QuickAdmin\Windows** directory, where *drive* is the letter assigned to your CD drive.
4. Double-click the **quickadmin.exe** icon.
   The Quick Admin Setup Wizard opens.
5. Follow the prompts until the Setup Type dialog box opens. Select **Deploy RSA ACE/Server Quick Admin**.
6. Follow the prompts until you are asked if you would like to re-deploy Quick Admin. Click **Yes**.
7. Follow the prompts until the Setup Wizard completes, and then click **Finish**.

Note: When you finish installing Quick Admin, *do not* configure JRun.

On a UNIX Machine

To upgrade Quick Admin on a UNIX machine:

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

Follow the instructions on page 78 for installing Quick Admin 5.2 on a UNIX machine, with the following exceptions:

- When the installation script asks "Do you already have an installation of JRun 3.1?(y/n) [y]," type **y**.
- When you are asked if you would like to deploy RSA ACE/Server 5.2 Quick Admin with your current installation, type **y**.
- When you finish installing Quick Admin, *do not* configure JRun.

Installing Quick Admin After Web Express Is Installed

The following table describes how to install Quick Admin 5.2 after Web Express 1.1 or 1.2 is already installed.

Task	Platform	Procedure
Install Quick Admin 5.2 after Web Express 1.1 is installed	Windows	See the procedure "To upgrade Quick Admin on a Windows machine:" on page 79.
Install Quick Admin 5.2 after Web Express 1.2 is installed	Windows	See the following procedure "To install Quick Admin 5.2 on Windows when Web Express 1.2 is already installed:"
Install Quick Admin 5.2 after Web Express 1.1 is installed	UNIX	See the procedure "To upgrade Quick Admin on a UNIX machine:" on page 80.
Install Quick Admin 5.2 after Web Express 1.2 is installed	UNIX	See the procedure "To upgrade Quick Admin on a UNIX machine:" on page 80.

To install Quick Admin 5.2 on Windows when Web Express 1.2 is already installed:

1. Shut down the Web Express service on the web server.
2. Insert the RSA ACE/Server 5.2 CD into the CD drive.
3. Start the JRun Admin server. On the web server, click **Start > Programs > RSA SecurID Web Express > JRun Admin Server Start**.
4. Start the JRun Application Management Console by browsing to **http://localhost:8000**.
5. Log in to the JRun Application Management Console.

6. Under the name of the web server, click **RSA WebExpress Server > Web Applications**.
7. In the Edit/Create/Deploy and Remove Applications page, click **Deploy an Application**.
8. In the Servlet War File or Directory field, enter ***drive*\QuickAdmin\UNIX\quickadmin.war**, or browse to the same location.
9. Enter the following Web Application Information, and then click **deploy**:
   - Application Name: **quickadmin**
   - Application URL: **/quickadmin**
10. Under the name of the web server, click **RSA WebExpress Server > Web Applications > quickadmin > Application Variables**, and then click **Edit**.
11. For the AppPath variable, enter the path to the **quickadmin** directory you just created. For example, ***Web_Express_installation_directory*\JRun\servers\default\quickadmin**.

    Important: The AppPath variable must end with a trailing slash.

12. Enter the new variable name **ConfigPath**, specify **WEB-INF/config** as the value, and click **Update**.
13. In the **RSAWebExpress\servers\default\quickadmin\WEB-INF\certs** directory, create a new directory, and name it after the fully-qualified name of the RSA ACE/Server Primary.
14. Copy the **server.cer** and **sdti.cer** files from the ***ACEDATA*** directory on the Primary to the directory that you created in step 13.
15. In the **RSAWebExpress\servers\default\quickadmin\WEB-INF\quickadminconfig.properties** file, edit the following entries to specify the fully-qualified name and IP address of the RSA ACE/Server Primary and save the file.

    ```
    ACE_SERVER=<fully-qualified name of the Primary>
    ACE_IP=<IP address of the Primary>
    ```

16. Start the RSA Web Express service on the Web Express host.

Installing Web Express After Quick Admin Is Installed

The following table describes how to install Web Express 1.1 or 1.2 after Quick Admin 5.2 is already installed.

Task	Platform	Procedure
Install Web Express 1.1 after Quick Admin 5.2 is installed	Windows and UNIX	Follow the Web Express installation instructions in the Web Express installation guide, but *do not* install JRun. Web Express can use the JRun Default Server from your Quick Admin installation.
Install Web Express 1.2 after Quick Admin 5.2 is installed	Windows and UNIX	First uninstall Quick Admin, install Web Express 1.2 according to the Web Express instructions, and then re-install Quick Admin.

Changing Quick Admin 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 ***JRun install directory*\servers\default\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 great care. 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 ***JRun install directory*\servers\default\quickadmin** directory.

Note: If you make changes to the **quickadminconfig.properties** file, you must stop and restart the JRun Default Server for the changes to take effect

ACE Web Admin for ACE/Server Configuration Settings

Parameter	Value
ACE_SERVER	The fully qualified name of the RSA ACE/Server Primary Server.
ACE_IP	The IP address of the RSA ACE/Server Primary Server.
CERT_PATH	The path to the directory that contains copies of the **sdti.cer** and **server.cer** files from your Primary RSA ACE/Server. The default path is **certs/**. For instructions on adding certificates from more than one Primary Server, see "Administering Multiple Primary Servers" on page 88.
ACE_PORT	The Primary Server TCP port on which the RSA ACE/Server Quick Admin daemon is listening. The default port is **5570**.
REPORT_PATH	The path to the directory where Quick Admin writes report files. The default path is **reports/**. **Important**: Because each report generates a new text file, it is recommended that you clean out the **reports** directory periodically to conserve disk space.
PROP_PATH	The path to the directory that contains the **quickadminconfig.properties** file. The default path is **properties/**.
MAX_SEARCH	The maximum number of objects (user records, token records, and so on) that are returned when a user searches the RSA ACE Server 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 path to the directory 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 ***JRun install directory*\servers\default\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 User Password Settings Affect Each Other" on page 86.

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
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. For example, if LOST_TOKEN_PWD_LIFETIME_DAYS=5 andLOST_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 *RSA ACE/Server 5.2 Administrator's Guide*.

Parameter	Value
FIXED_PWD_LIFETIME_DAYS FIXED_PWD_LIFETIME_HOURS	Determine the number of days and hours before user passwords issued to replace lost tokens expire. Fixed passwords can be used repeatedly until they expire. 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
OTP_PWD_LIFETIME_DAYS OTP_PWD_LIFETIME_HOURS	Determine the number of days and hours before user passwords issued to replace lost tokens expire. OTP, or one-time passwords, can be used only one time each and expire on a specified date. You can set days, hours, or both. 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 User Password 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 <*type*>_PWD_LIFETIME_DAYS and <*type*>_Pwd_LIFETIME_HOURS parameters are defined	If LOST_TOKEN_CONTROL_FLAG is set to FIXED	If LOST_TOKEN_CONTROL_FLAG is 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 cancel out 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 ACE/Server 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 ACE/Server. 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 ACE/Server are written to the log file (**default-out.log**). 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 ***JRun installdirectory/*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 (**default-out.log**). 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 (**default-out.log**). 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 ACE/Server Communication Settings

Communication between the Primary RSA ACE/Server and the Quick Admin server is controlled by settings in a configuration file on the Primary Server.

- If your Primary RSA ACE/Server is running on Windows, the settings are in the ***ACEPROG*\sdcommdconfig.txt** file**.**
- If your Primary RSA ACE/Server is running on UNIX, the settings are in the ***ACEPROG*\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 ACE/Server Quick Admin daemon is running on the Primary Server. 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 JRun session time-out value that you set in the JRun Management Console. Doing so ensures that the session times out before the RSA ACE/Server Quick Admin daemon does on the Primary Server. Otherwise, Quick Admin users might experience the hanging of terminated sessions.

Administering Multiple Primary Servers

Quick Admin supports administering more than one Primary RSA ACE/Server through a single Quick Admin server.

To use Quick Admin with multiple Primary Servers:

1. Create a new subdirectory for each Server under the ***JRun install directory*\servers\default\quickadmin\WEB-INF\certs** directory. You must create a subdirectory for each Primary Server you want to administer.

   The subdirectories must have the same name as the Primary Server 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 ***ACEDATA*** 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 in to Quick Admin, enter the Server name in the **Realm** box of the login page.

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

Uninstalling Quick Admin

To remove the Quick Admin software from a Windows or UNIX machine:

1. Point your web browser to the JRun administration URL (the default URL is **http://localhost:8000**), and log in using the JRun administrator username and password that you specified during installation.
2. Close the JRun Quick Start Product Tour - Microsoft Internet Explorer window.
3. In the JRun Application Management Console, in the left frame, click **JRun Default Server**.
4. In the left frame under **JRun Default Server**, click **Web Applications**.
5. In the right frame, click **Remove an Application**.
6. In the Application Removal Information window, select **quickadmin**, and click **Remove**.
7. Log out of the JRun Management Console.
8. Stop and restart the **JRun Default Server**.

   On Windows machines, stop and restart the **JRun Default Server** by clicking **Start > Settings > Control Panel > Services**.

   On UNIX machines, from the **/opt/JRun/bin** directory, type

   ```
   ./jrun stop default
   ./jrun -nohup default
   ```
9. Delete the **quickadmin** directory from ***JRun install directory*/servers/default/**.

A Modifying Kernel Parameters

The RSA ACE/Server 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 will have to 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 ACE/Server installation and operation. You may need to increase the values to allow additional administration connections to the RSA ACE/Server database. Additional connections to the database allow you to run more Remote Administration and RSA Quick Admin sessions.

The minimum values listed in this chapter are based on the assumption that the Server is dedicated to running RSA ACE/Server 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 in as the **root** user on the console.

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
   ```

   No other users should 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: 16 is the value currently recommended by RSA Security for the **semmni** parameter. The RSA ACE/Server requires 3 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

Highlight the parameter you want to change, and select **Modify Configurable Parameter** on 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** on the Actions menu. You are prompted to build the kernel and reboot 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 of your choosing. The following example uses the "vi" editor:

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

2. Log out of the system and log back in for the modification to take effect. There is no need to reboot the system.

   You may want to edit the **fsize** for the RSA ACE/Server fileowner only.

Modifying Kernel Parameters for Solaris

Although you do not have to set the system into single-user mode, there should 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 reboot your system as shown in step 5.

2. The Solaris kernel is dynamically configured. Editing the configuration file will change 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: 16 is the value currently recommended by RSA Security for the **semsys:seminfo_semmni** parameter. The RSA ACE/Server requires 3 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 reboot it at the **OK** prompt. Type

   ```
   reboot
   ```

B Database Utilities

This chapter describes the utilities that you will use to perform installation and administration tasks on the Primary Server. 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:

- The **sdsetup -config** utility, which allows you to edit the configuration record on the Primary Server. See "Changing the Configuration" in the appendix "Configuring the RSA ACE/Server (UNIX)" in the *RSA ACE/Server 5.2 Administrator's Guide* for information on changing the configuration record.
- The Replica Management utility (**sdsetup -repmgmt**), which adds and deletes Replica Servers, displays information about the Servers in your realm, marks Replica Servers as requiring a new database, and creates Replica Packages and, in recovery situations, allows you to nominate a Replica to replace the Primary. See the *RSA ACE/Server 5.2 Administrator's Guide*.
- The **loadsamusers** utility, which allows you to move user information from an existing SAM (Security Account Manager) database on a Windows system to the RSA ACE/Server database, is described in the appendix "Creating User Records from a SAM Database" in this book.
- The **sdaceldap** utility, which allows you to create and update RSA ACE/Server user records with information from an LDAP directory, is described in the section "Importing LDAP User Data" in the chapter "Registering Users for Authentication" in the *RSA ACE/Server 5.2 Administrator's Guide*.

Using sdadmin

The **sdadmin** program can be run on a UNIX Primary Server by one or more authorized administrators. A passcode is not required to run **sdadmin**. Instead, the program checks the user record for RSA ACE/Server 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 in as the RSA ACE/Server 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 ACE/Server 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 ACE/Server fileowner.

Note: While the **sdadmin** program allows you to access most of the features of the RSA ACE/Server software, Remote Administration provides a graphical user interface for administering an RSA ACE/Server 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, use 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 select 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** on the File menu. While on some systems pressing CTRL+C will terminate **sdadmin**, you should quit the program properly by using the **Exit** option on the File menu instead.

Running sadmin

To run sadmin:

1. Start the database brokers. Type

   ```
   ACEPROG/sdconnect start
   ```

   If a broker is already running, a message to this effect displays.

   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.
   ```

   See the appendix "Modifying Kernel Parameters" in this book for procedures on changing UNIX configuration values.

2. Run the RSA ACE/Server administrative program:

   ```
   ACEPROG/sdadmin
   ```

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

Dumping the Database Using sddump

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

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

Option	Argument	Description
-s	None	Dumps the Server database.
-l	None	Dumps the log database.
-d	*database name*	The name of the Server (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 Server database dump file and **/ace/data/sdlog.dmp** for the log database dump file).
-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."

Option	Argument	Description
-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 *RSA ACE/Server 5.2 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
client	SDClient	SDSystem
clientext	CustClientExt	SDClient

Identifier	Database Table Name	Required Tables
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 Server or log database and creates a new, empty Server 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 Server database
log	specifies that you want to create a new log database
all	specifies that you want to create new Server 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 a Server dump file.
-l	None	Loads a log database dump file.
-d	*database name*	Specifies database file name. 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 Server.
-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 Server. Use this option only when you are attempting to recover a failed database or Server.
-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 Server.

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 ACE/Server Database Administration application and connect to the Primary Server.
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 appendix "Replica Management Utility" in the *RSA ACE/Server 5.2 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 ACE/Server 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 ACE/Server 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 *RSA ACE/Server 5.2 for 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, will be written. If you do not specify this parameter, the output files will be written to the current directory. For XML2 and TXT, this parameter is the name of the file to which the output will be 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.

Option	Argument	Description
-c	None	*Consolidate* 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 chapter. 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 file name 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 RSA ACE/Server's 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 on their related link 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 ACE/Server from which the file was created. For more information, see "Schema Versions in RSA ACE/Server Releases" on page 107.

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
.
.
.
```

File names include a base name and a timestamp that indicates the exact date and time the files were created. This prevents files from being overwritten should 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 ACE/Server 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 *RSA ACE/Server 5.2 Administration Toolkit Reference Guide (**ace_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. See the following section, "Schema Versions in RSA ACE/Server Releases," for more information.

Schema Versions in RSA ACE/Server Releases

RSA ACE/Server 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.

Note: See page 103 for details about the Dumpreader utility command syntax. Also, 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 written 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.

C Troubleshooting

If you experience problems with the RSA ACE/Server 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 here do not resolve the problem, contact RSA Security Customer Support. See "Getting Support and Service" on page 10 for contact information.

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 the documentation that came with your operating system.

"Cannot create administrator. Use an empty database."

This error message appears if you are not **root** and you try to install the RSA ACE/Server on an AIX system with the ulimit set too low. The ulimit fsize must be at least 4194303. See the appendix "Modifying Kernel Parameters" in this book for the minimum values required and for instructions on modifying the values on your system.

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 will free up disk space for the *new* installation. See the chapter "Database Maintenance (UNIX)" in the *RSA ACE/Server 5.2 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 will not get this message if you are logged in 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 in 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 with the above error message, an RSA ACE/Server database broker is running or was not shut down properly.

To proceed with the installation, make sure that no Server programs are running. Then, from the directory that contains the Server program files. To 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 will probably solve the problem.

In the startup file, enter the command:

```
ACEPROG/sdconnect clean
```

Reboot the Server, 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 left over 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 ACE/Server Primary or Replica Server hostname cannot be resolved properly, make sure that the primary hostname of the Server (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 will get 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. See the appendix "Modifying Kernel Parameters" in this book for instructions on modifying this value on your system.

"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 in as root or the RSA ACE/Server fileowner to run **sdconnect**.

If the correct permissions are set, check that you have configured the UNIX kernel parameters as described in the appendix "Modifying Kernel Parameters" in this book. 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 ACE/Server audit trail report for information about the authentication failures.
2. Verify that the physical connection of the Agent Host to the Server 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 Server 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 the chapter "RSA ACE/Server TACACS+ Support" in this book.

6. Verify that the argument file (**sdtacplus.arg**) is present in the **ace/data** subdirectory of your Server.
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 Replica Servers are registered in the Server 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 in the Server 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. At the Server 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 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 will 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 ACE/Server. The TACACS+ debugging log will be in **var/tmp/tacplus.log**.

Authentication Session Timeouts

A 30-second inactivity time-out is hardcoded in Cisco 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 should press character keys on the keyboard, then remove the characters with the backspace key before pressing ENTER.

RSA ACE/Server 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 Server creates a **wtmp** file for each and every TACACS Agent Host. The filenames for these will be the **wtmp** file **sdtac_wtmp** concatenated with the hostname. For example, if a login 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 in 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.

D Creating User Records from a SAM Database

As an aid in setting up your RSA ACE/Server 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 ACE/Server 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 login, 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 Server database containing the three items of information found in the file.

Because **dumpsamusers** runs only on Windows, only **loadsamusers** is installed with RSA ACE/Server 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 ACE/Server 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. See “Importing LDAP User Data” in the chapter “Registering Users for Authentication” in the *RSA ACE/Server 5.2 Administrator’s Guide* and “Manage LDAP Users” in the Help.

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 usernames 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 will need to be changed.

Creating RSA ACE/Server User Records with loadsamusers.exe

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

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

- You must set the RSA ACE/Server 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.

Syntax

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

Arguments

infile	Specifies the input file — that is, the **dumpsamuser** output file.
-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 logins 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 ACE/Server group to which all users added through this command are to be assigned. If no such group exists, the Server creates it. Optional: if omitted, users are not assigned to a group.

The **loadsamusers** program is designed to exit when it encounters a fatal error — that is, a record that it cannot load. Users loaded up to that point remain in the Server database.

E Minimum System Requirements (Solaris 9)

This appendix specifies the minimum operating system components required for the RSA ACE/Server 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 fresh 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 ACE/Server 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 ACE/Server 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 ACE/Server 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 ACE/Server 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 ACE/Server data, RSA ACE/Server program files, the Progress 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 ACE/Server directory specified during installation.

aceserver

The background Server process that performs authentication for the RSA ACE/Server product.

acesyncd

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

***ACEUTILS* directory**

The RSA ACE/Server 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 Server

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

Acting Slave Server

The Server that responds to a legacy Agent authentication request when the Acting Master Server is unable to respond.

Agent Host

A computer or another device that is protected by the RSA ACE/Server to prevent unauthorized access.

automatic migration

A method of upgrading an existing Master Server to the Primary, in which the Master Server database is migrated automatically to a 5.2 database. When performed with a Slave Server 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 ACE/Server databases and the RSA ACE/Server programs that access the databases.

license.rec

The file that contains site-specific information, such as the license/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 Server puts a token in this mode, the user is required to receive or create a new PIN in order to gain access to an RSA SecurID-protected system.

Next Tokencode mode

When a user attempts authentication with a series of incorrect passcodes, the Server 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 Server. The node secret is combined with other data to encrypt Agent Host/Server 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 Server

The RSA ACE/Server on which administration can be performed and which replicates database changes to the Replica Servers.

RADIUS profile

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

realm

An RSA ACE/Server 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 ACE/Server database through a remote connection. Remote administration of an RSA ACE/Server 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 ACE/Server 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 Server 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 Server

The RSA ACE/Server whose main function is to perform RSA SecurID authentication.

rolling upgrade

A method of upgrading an existing Master and Slave Server to the Primary and a Replica. In a rolling upgrade, the existing databases are migrated to 5.2 databases with no loss of data and no downtime of authentication services.

RSA ACE/Agent

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

RSA ACE/Agent software

The programs that perform the authentication dialog on RSA ACE/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 ACE/Server for UNIX only in TTY mode (character-based interface). RSA ACE/Server 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 ACE/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 Server, 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 ACE/Server program that installs and configures the Server 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 RSA SecurID-authenticate 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 ACE/Server 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

A

aceserver, 123
  stopping to perform upgrade, 41
acesyncd, 123
Acting Master Server, 123
Acting Slave Server, 123
Adding Replica Servers
  to database, 32
Adding Servers to administer remotely, 46
Advanced license, 11
Agent Hosts, 123
  adding RADIUS servers as Agent Hosts to the Primary, 57
architecture
  Quick Admin, 73
Authentication
  RSA SecurID, implementing, 30
  TACACS+ users, 62
  testing, 29
Authentication methods
  configuring for remote administration, 43
Automatic migration
  for upgrades, 39

B

Base license, 11
Broker. *See* database broker, 124

C

Configuring
  RADIUS, 57, 58
  remote administration ports, 47
Controls, 88
Coordinated Universal Time, 14, 16, 124
Creating Replica Package, 33

D

Database broker, 124
Database utilities, 97
  create new database, 100
  dump database, 97
  load dump files, 100
  manage Replicas, 95
Dictionary file
  RADIUS, 58
Disabling
  Push DB (Push Database), 102
  RADIUS server, 55
Documentation installed with RSA ACE/Server, 8
dump file, viewing, 102
Dumping databases
  required tables, 98
Dumpreader utility, 102
dumpreader.exe, 102
dumpsamusers.exe, 117
  extracting SAM user records with, 118

E

Enable Mode
  protecting, 71
    with TACACS+, 71
Enabling RADIUS server, 55
Enterprise authentication client. *See* RSA ACE/Agent, 125
/etc/hosts
  adding server host name to, 18
/etc/passwd
  listing RSA ACE/Server fileowner in, 18
/etc/services
  adding port numbers and service names to, 17

F

File formats for RADIUS data files, 58
Fileowner of RSA ACE/Server files, 18
  listing in /etc/passwd, 18

G

Greenwich Mean Time. *See* Coordinated Universal Time, 124

H

Help, 9
  accessing, 9
High availability platforms
  supported by RSA ACE/Server, 12
hosts file
  adding server host name to, 18

I

Installation
- guidelines, 13
- prompts, 24
- requirements, 12, 14
- tasks to perform after, 27
- upgrading Remote Administration software, 45

Installing
- pre-installation checklist, 14
- Primary Server, 21
- Replica Servers, 34
- without local CD drive, 21
- without local CD-ROM drive, 34

interface conventions
- sdadmin, 96

J

JRun
- configuring, 77, 78

K

Kernel configuration, 13
- HP-UX systems, 91
- IBM AIX systems, 92
- modifying, 91
- Solaris systems, 93

L

license types, 11
license.rec, 124
Loading database dump files, 100
- merge logic, 101

Loading existing RADIUS data, 51
loadraduser, 54
loadsamusers.exe, 117
- creating user records with, 119

Log messages, 115
Logging replication messages to syslog, 28

M

Map file in RADIUS, 59
Master Server, 123
Merge logic
- for dumping databases, 101

multiple realms
- merging, 14

N

New PIN, 124
Next Tokencode, 124
Node secret, 124

O

Online distribution, 10

P

PASSCODE, 124
PINs, 124
Platforms supported by RSA ACE/Server, 12
Port numbers
- RSA ACE/Server, 17
- specifying for remote administration, 47

Pre-installation checklist, 14
Primary Server, 124
- administering multiple with Quick Admin, 88
- after you install, 27
- installing, 21
- preparing to upgrade, 40
- security requirements, 27
- upgrading, 41
- verifying correct installation, 29

Push database, 102
- disabling, 102

Q

Quick Admin
- administering multiple Primary Servers, 88
- and Web Express, 80, 82
- Architecture, 73
- changing settings, 82, 88
- installing after Web Express, 80
- installing on UNIX, 78
- installing on Windows, 76
- logging, 88
- overview, 73
- pre-installation checklist, 75
- pre-installation tasks, 75
- properties file, 82
- session timeout settings, 88
- system requirements, 74
- system requirements (UNIX), 75
- system requirements (Windows), 74
- uninstalling, 89
- upgrading, 79

R

RADIUS
- attributes, removing, 54
- changing service names, 56
- configuring network access server, 58
- configuring RSA ACE/Server, 56
- data files, 58
- disabling, 55
- enabling, 55
- formats for data files, 58
- importing data files, 51
- importing user and client files, 54
- loading data, 51
- utilities, 52

Realm, 124
Remote Administration, 125
- adding machines for, 46
- configuring, 43, 47
- installing, 45
- platform support, 44
- upgrading, 45

removeattr program, 54
Replica management
- database push, 102
- marking Replicas for database push, 102

Replica Package
- creating, 33

Replica Servers, 125
- adding to database, 32
- installing, 34
- preparing system for, 31
- security requirements, 27
- upgrading 5.0.1 to 5.1, 42
- verifying correct installation, 29

Requirements for installing RSA ACE/Server, 12
Rolling upgrade. *See* Automatic migration, 39
RSA ACE/Server
- installation requirements, 12
- installing Primary Servers, 21
- installing Replica Servers, 34
- licensing options, 11
- online distribution, 10
- preparing system for Replica Servers, 31
- preparing to install, 14
- registering Servers as Agent Hosts, 29
- remote administration, 46
- security requirements, 27
- supported platforms, 12
- system requirements for installing, 12
- TACACS support, 61
- testing authentication, 29
- token records, managing in new installations, 29
- troubleshooting
  - distribution media problems, 111
  - log messages, 115
  - post-installation errors, 113
  - sdsetup problems, 111
  - TACACS, 113

RSA SecurID authentication
- implementing, 30

RSA SecurID Software Token, 125
RSA ACE/Agent, 125

S

sdadmin, 125
- interface conventions, 96
- using, 95

sdconf.rec, 125
sddump, 97
sdinfo, 126
sdload, 100
sdlogmon, 126
sdnewdb, 100
sdsetup, 126
- command line arguments, 22
- replica, 35
- troubleshooting problems with, 111

sdsetup -master, 22
sdsetup -package, 33
sdshell, 126
Security Accounts Manager (SAM) database
- creating user records from, 117

Security requirements
- for RSA ACE/Server, 27

semaphores, 97
Service names
- error messages about, 36
- RSA ACE/Server, 17

Slave Server, 123
Supported platforms for RSA ACE/Server, 12
syslog
- logging replication messages to, 28

System time
- importance of, 16

T

TACACS+, 61
authenticating users of, 62
configuring a Cisco system device for, 67
description of, 61
enabling and configuring support for, 62
help for using TACACS+ commands, 67
protecting enable mode with, 71
protocols, 61
sample argument file, 64
sample configuration file, 65
troubleshooting, 113
Telnet
using with RSA ACE/Server, 28
Time
maintaining accurate settings, 14, 16
Tokens, 126
importing in new installations, 29
managing in new installations, 29
Troubleshooting
RSA ACE/Server
distribution media problems, 111
log messages, 115
post-installation errors, 113
sdsetup problems, 111
TACACS, 113

U

UNIX
installing Quick Admin, 78
UNIX kernel configuration, 13
HP-UX systems, 91
Solaris systems, 93
Upgrading
preparing for, 39
Primary Server, 41
Quick Admin, 79
Remote Administration software, 45
Replica Server from 5.0.1 to 5.1, 42
User file in RADIUS, 59
User password, 126
User records
creating from a Windows NT SAM database, 117
UTC. *See* Coordinated Universal Time, 14

W

Web Express
and Quick Admin, 80
installing after Quick Admin, 82
Windows
installing Quick Admin, 76