# RSA ACE/Server 6.0 for Windows Installation Guide

### Contact Information

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


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


### Trademarks



### License agreement



### Note on encryption technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when exporting this product.

### Distribution

Limit distribution of this document to trusted personnel.

### RSA Security Notice





First printing: September 2004

# Contents

# Preface

This manual explains how to install RSA ACE/Server 6.0 for Windows 2000 and Windows 2003.

| Task | See |
|---|---|
| Prepare for any type of upgrade or new installation. | "RSA ACE/Server Requirements" on page 11 |
| Minimize your system for security purposes | "Minimum System Requirements (Windows 2003 Server Only)" on page 65 |
| Install a new RSA ACE/Server | "Installing the RSA ACE/Server" on page 15 |
| Upgrade an existing RSA ACE/Server | "Upgrading to RSA ACE/Server 6.0" on page 21 |
| Enable and configure a RADIUS server.** | "The RSA RADIUS Server" on page 31 |
| • Install and upgrade RSA ACE/Server Remote Administration software<br>• Add a Server to administer remotely. | "Installing and Upgrading Remote Administration Software" on page 27 |
| Install or upgrade Quick Admin. | "Installing the Quick Admin Software" on page 45 |
| Use database utilities. | "Database Utilities" on page 67 |
| Import users to the RSA ACE/Server database from a Windows SAM database. | "Creating User Records from a SAM Database" on page 81 |
| Uninstall the RSA ACE/Serversoftware | "Uninstalling the RSA ACE/Server" on page 87 |

** 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 Windows 2000 and Windows 2003 security system administrators. The person who installs RSA ACE/Server must be familiar with your server platform, operating system version, and system peripherals.

Do not make this guide available to the general user population.

## 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** |

## Documentation

The RSA ACE/Server 6.0 software for Windows 2000, Windows 2003, and UNIX is provided on a single CD, which also includes:

- Help for RSA ACE/Server 6.0 for Windows 2000 and Windows 2003
- Printable documentation files in PDF format for Windows 2000, Windows 2003, and UNIX

### Documentation Provided as PDF Files

You can access PDF files from either:

- **\aceservdoc** on the RSA ACE/Server CD.
- The local ***ACEDOC*** directory on your hard drive, provided you opted to install the documentation as part of the installation process.

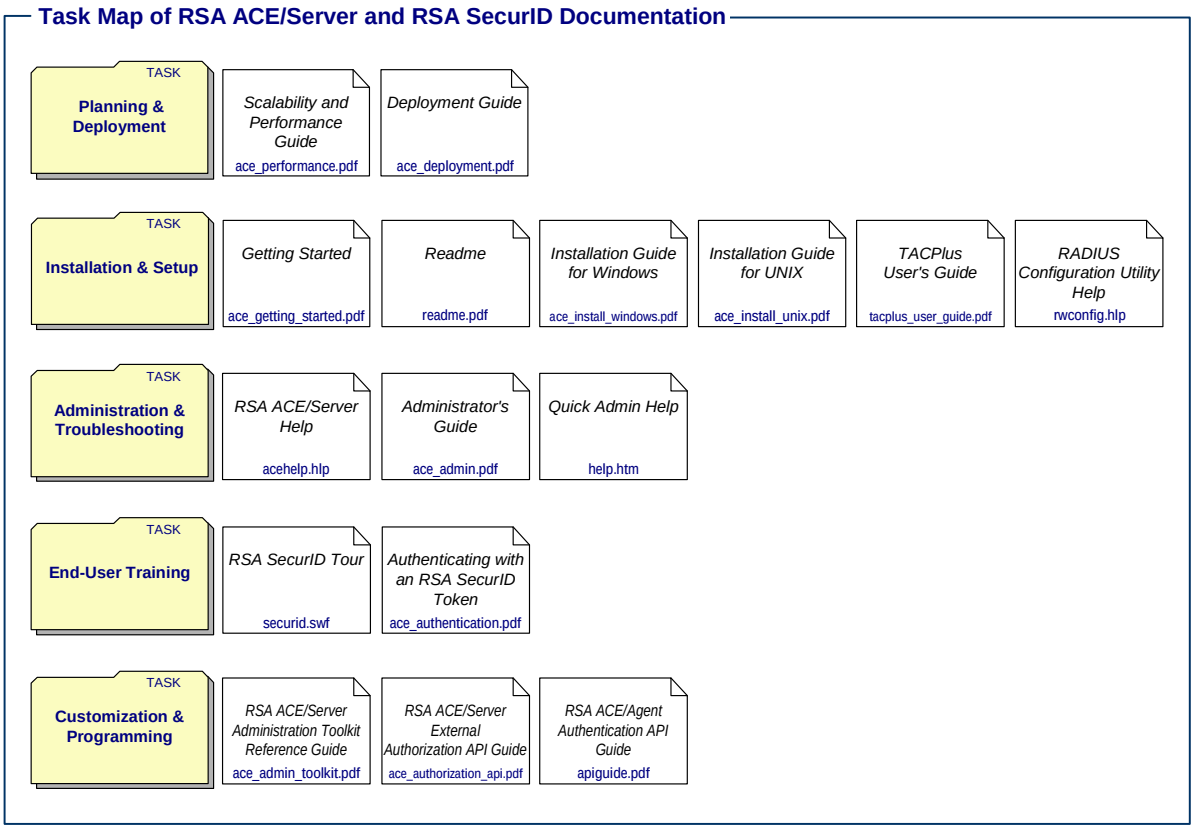
**Note:** Authentication instructions are also delivered in a Microsoft Word (.doc) file for customization purposes.

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 6.0 includes an extensive Help system that you can access 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 6.0

Some upgrade customers have the option of downloading RSA ACE/Server 6.0 as a zip file. When unzipped, the file contains the same directory layout and contents as the RSA ACE/Server 6.0 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 steps. For example, you might navigate to a directory rather than insert a CD.

The Welcome Kit and license diskettes are in 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 Customer Support

Make sure you have direct access to the computer running the RSA ACE/Server software.

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 running the Configuration Management application on the Windows 2000 or Windows 2003 platforms, or by typing ‘sdinfo’ on any UNIX platform.
- RSA ACE/Server software version number.
- The name and version of the operating system under which the problem occurs.
- Whether you are running a name resolution service (for example, DNS).

# 1 RSA ACE/Server Requirements

## 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 active users in the RSA ACE/Server database as specified by the active user tier that was purchased.
- On 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 environment:

- 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.

For detailed information about licenses and active users, see the *RSA ACE/Server 6.0 Administrator's Guide*.

## System Requirements

For information about requirements for your system, see Appendix B, "Minimum System Requirements (Windows 2003 Server Only)."

### Supported Platforms

- Microsoft Windows 2000 Server or Advanced Server (Service Pack 4) running a supported language
- Microsoft Windows 2003 Enterprise Server running a supported language
- Microsoft Windows 2003 Standard Server running a supported language

For information about supported languages, see the *RSA ACE/Server 6.0 Administrator's Guide*.

## Hardware Requirements

- Intel Pentium 266 MHz processor or better (Windows 2000 Server)
- Intel Pentium 733 MHz processor or better (Windows 2003 Server, Standard or Enterprise Edition)
- At least 256 MB of physical memory + 1 MB per 1,000 users
- Two times physical memory swap file
- Local CD drive (unless you plan to download the software)
- NTFS File System (not required for Remote Administration software)
- Monitor display set to at least 800 x 600 pixels

To achieve the highest authentication rates possible, you need:

- Dual Intel Pentium 4 (1.8 GHz or faster) processors
- 256 MB of physical memory per processor

## Disk Space Requirements

- 200 MB for RSA ACE/Server software
- Additional 1 MB per 1,000 users
- 20 MB for RSA ACE/Server Remote Administration software
- 5 MB for RSA ACE/Agent for Windows

For more information on disk space requirements, see the chapter "Database Maintenance" for your platform in the *RSA ACE/Server 6.0 Administrator's Guide*.

## Important Installation Guidelines

- Use the Primary and Replica Server machines as RSA ACE/Servers only. Do not use RSA ACE/Server machines as domain controllers, VPNs, firewalls, or for any other purpose.
- 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 or a FAT (File Allocation Table) partition.
- Make sure that the Server machines are located in a secure area so that only trusted personnel can access the Server console.

## Merging Multiple Realms

**To merge databases from multiple realms into one 6.0 realm:**

1. Upgrade one realm to RSA ACE/Server 6.0.
2. Dump the other databases and merge them into the 6.0 database using the dump and load utilities **sddump** and **sdload**.

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

## 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.

Make sure that the time on the computer on which you are installing 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:** If you employ an NTP service, enable it on the Primary Server only. The Primary Server typically maintains the Replica Server's time synchronization automatically. For more information, including exceptions to this behavior, see "Maintaining Accurate System Time Settings" in the *RSA ACE/Server 6.0 Administration Guide*.

## Changing the Language Used by the Database

To change the language used by the RSA ACE/Server database, you must change the language and locale of the Windows 2000 or Windows 2003 machine that is running the RSA ACE/Server software. Use the Regional Setting control panel to specify the language and locale that is used by your system. Once you change the language, you must reinstall the RSA ACE/Server software. If your system is running a language other than English, the installation process will prompt you to choose the appropriate language.

**CAUTION:** Once you install the RSA ACE/Server software on a non-English language system, you cannot change the language back to English. If you want to change the language from one supported ISO-Latin-1 language to another supported ISO-Latin-1 language, see your operating system documentation.

## Pre-Installation Checklist

RSA Security recommends that you read the *RSA ACE/Server 6.0 Readme* (**readme.pdf**) before installing the RSA ACE/Server software. The *RSA ACE/Server 6.0 Readme* contains important configuration and installation information for RSA ACE/Server 6.0. It also contains information about problems in the software found too late to be included in the standard documentation.

### You must have

- ❑ The RSA ACE/Server CD (or the downloaded zip file).
- ❑ 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 6.0 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 the license in the directory is lost or corrupted, you cannot regain access using the original license diskettes. The only way to regain access is with the modified license files.

- ❑ A blank diskette on which to copy the license diskette. Use this copy when you are instructed to use the license diskette.
- ❑ A token 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.

- ❑ A machine that meets all the hardware, disk space, memory, and platform requirements described earlier in this chapter.
- ❑ Local administrator privileges on the machine.

### You must know

- ❑ The language and locale used by the Windows 2003 or Windows 2000 machine and the language you want to use. For information about supported languages, see the *RSA ACE/Server 6.0 Administrator's Guide*.
- ❑ The number of Replica Servers allowed by your license.

  If you have an RSA ACE/Server Base license, you can install 1 Replica. If you have an RSA ACE/Server Advanced license, you can install up to 10 Replicas.

- ❑ The name and IP address of any Replica you plan to install.

  You specify Replicas after the Primary installation. To add Replicas, use the Replica Management utility described in Appendix C, "Database Utilities."

**You must**

- ❑ Make backup copies of the diskettes before beginning an installation. Store the original license diskettes and the token seed record diskettes in a secure place.

**If you are installing RADIUS on the Primary during the Primary installation process, you need**

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

  You are prompted for the location of these files.

# 2 Installing the RSA ACE/Server

This chapter describes how to

- Install a new Primary Server and one or more Replicas.
- Load existing RADIUS custom data files and enable the RSA RADIUS server on the Primary Server.

## Installing a New Primary

This section explains how to install a Primary as part of a new installation.

**Important:** The name of each Server machine must be a fully-qualified computer name on the network.

**To install RSA ACE/Server on a new Primary:**

1. Log in to the machine as a local administrator.
2. Insert the CD labeled “RSA ACE/Server 6.0” into the CD drive.
3. Insert the license diskette into the diskette drive.
4. In the **aceserv\windows** directory on the RSA ACE/Server CD, double-click **setup.exe**.
5. If your Windows system uses a language other than English, a question dialog box opens.
   - To install the English version of the RSA ACE/Server database, click **Yes.**
   - To install another version of the database, click **No.** The language currently used by Windows will determine the database version to install.
6. Follow the prompts until the Installation Options dialog box opens.

   This dialog box lists the components that you can install. For descriptions of the components, see Appendix E, “Installation Components.”
7. Select **New Primary ACE/Server**, **Documentation** and, optionally, **Load RADIUS data** (to enable the RSA RADIUS server and load custom RADIUS data files into the database). Click **Next**.

   If you are loading RADIUS data, go to step 8. Otherwise, go to step 10.

   **Note:** The zero K value listed next to the **Load RADIUS data** checkbox is correct.

   The RADIUS Options dialog box opens.

8. Select the box next to the custom RADIUS data files you want to load. If you do not select any boxes, the default data files are loaded.

   You can load the following custom data files:

| 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. RADIUS is shipped with a default dictionary. |
| RADIUS SecurID Map File | A mapping file that dictates which attributes in the dictionary are user-configurable and which attributes can be multiply-defined. |

9. When prompted, specify the location of each data file you are loading.
10. Follow the prompts to complete the installation, and restart the machine.

**Note:** At the end of the installation, a license status dialog box opens that gives you detailed information regarding your current license. For additional information about licenses, see the *RSA ACE/Server 6.0 Administrator's Guide*.

11. Start the RSA ACE/Server processes. For instructions, see the following section, "Starting and Stopping the RSA ACE/Server Processes."

**Important:** You must make backup copies of your license files (**sdti.cer**, **server.cer**, **server.key**, and **license.rec**) *after* you install the RSA ACE/Server software. During the installation, the license files are modified. Therefore, if the files in the directory are 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.

## Starting and Stopping the RSA ACE/Server Processes

Start and stop all RSA ACE/Server processes through the RSA ACE/Server Control Panel.

### To start all RSA ACE/Server processes on the Primary Server:

1. Open the Control Panel on the Primary Server, and double-click the RSA ACE/Server icon.
2. In the RSA ACE/Server dialog box, under **RSA ACE/Server**, click **Start**.
3. When the **RSA ACE/Server started** message appears, click **OK**.
4. In the RSA ACE/Server dialog box, click **OK**.

**To stop all RSA ACE/Server processes on the Primary Server:**

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

1. Open the Control Panel on the Primary Server, and double-click the RSA ACE/Server icon.
2. In the RSA ACE/Server dialog box, under **RSA ACE/Server**, click **Stop**.
3. When the **Broker service stopped** message appears, click **OK**.
4. If the Broker Connections dialog box appears, click **Yes**.

## Adding Token Seed Records to the Database

If you have performed a new installation of the RSA ACE/Server on the Primary, the database does not contain any token seed records, and the administrator who installed the software is the only user in the database.

If you import the token seed records at the time of a new installation, you can create user records for your administrators and assign tokens to them. Otherwise, only the user who installed the software is able to administer the database, and then only locally on the machine that contains the Primary.

For more information about importing token seed records and adding users to the database, see the Help topic “Adding Token Records to an Existing Database.”

**To add token seed records to the RSA ACE/Server database:**

1. On the Primary Server, log in as a local administrator.
2. Insert the diskette containing the token seed records into the disk drive.
3. Click **Start > Programs > RSA ACE/Server > Database Administration - Host Mode**.
4. On the Token menu, select **Import Tokens**.
   The Import Token Filename dialog box opens.
5. Enter the path and filename of the token record file, or click **Open** to browse to the location. Token files have an **.asc** or .**xml** extension.
6. Click **OK**.
   The Import Status dialog box shows how many tokens have been imported.
7. Click **OK** to close the dialog box.
   The new token records are added to the **sdserv** database.

**To verify that the tokens were imported successfully:**

1. Click **Token** > **List Tokens**.
2. In the List Tokens dialog box, select List to **Screen,** List **All Tokens**, **All Algorithms**, and click **OK**.

   The Token Report lists all tokens in the database.
3. To close the Token Report, click **Exit**.

## Pushing the Initial Database to the Replicas using Push DB

Push DB provides an automated method of distributing RSA ACE/Server database files to Replicas.

- **With Push DB**, after you generate the Replica Package, the Primary automatically pushes the full contents of the database (***ACEDATA*\replica_package\database**) to the Replica when you start the Replica for the first time after installation.

  If you run the Replica Management utility on the Replica while the database push is under way, you can view only default information about the Replica until the database push is complete.
- **Without Push DB**, you manually copy the database files directly to each Replica.

**Note:** RSA Security recommends you disable Push DB only if you have a large (5,000 + users) database.

By default, Push DB is enabled. To disable Push DB, use the following procedure.

**To disable Push DB:**

1. Start the RSA ACE/Server Database Administration application on the Primary Server.
2. Click **System** > **Edit System Parameters**.
3. Clear **Allow Push DB Assisted Recovery**.
4. Click **OK**.

By reversing step 3, you can enable Push DB at any time.

Go to the following section, "Adding and Installing a New Replica."

## Adding and Installing a New Replica

**To add and install a new Replica:**

1. Through the RSA ACE/Server Control Panel on the Primary, shut down the database brokers.

   All administrative sessions are disconnected.

2. On the Primary, start the Replica Management utility by clicking **Start > Programs** > **RSA ACE/Server > Configuration Tools > Replica Management**.

   **Note:** If you are connected to a Replica or did not shut down the database brokers, the **Details** button is the only active button, and "READ ONLY Access to database" appears above the list of Servers.

3. Add the Replica Server to the Primary Server database. For instructions, see the Help topic "Adding a Replica to the Database."

4. Create the Replica Package on the Primary Server. The Replica Package contains the license and database files that the Replica installation requires. For instructions, see the Help topic "Creating a Replica Package."

5. Do one of the following:

   - If Push DB is enabled on the Primary Server, copy the ***ACEDATA*\replica_package\license** directory to a temporary directory outside of ***ACEDATA*** on the Replica machine. After you install and start the Replica Server, the Primary pushes the database files to the Replica.
   - If Push DB is disabled on the Primary Server, copy the contents of the ***ACEDATA*\replica_package** directory to a temporary directory outside of ***ACEDATA*** on the Replica machine.

6. Install the Replica Server. For instructions, see the following procedure "To install the RSA ACE/Server software on the Replica:"

7. Start the Replica using the RSA ACE/Server Control Panel. For instructions, see "Starting and Stopping the RSA ACE/Server Processes" on page 16.

   **Important:** Make sure that the Primary Server is running so that the initial connection between the Primary and Replica occurs and the Primary verifies that the Replica has the correct database.

**To install the RSA ACE/Server software on the Replica:**

**Important:** The name of each Server machine must be a fully-qualified computer on the network, and the name must be all lowercase.

1. Log in as a local administrator.
2. Insert the CD labeled "RSA ACE/Server 6.0" into the CD drive.
3. Double-click **setup.exe** in the **aceserv\windows** directory on the RSA ACE/Server CD.
4. When prompted, browse to the **license** directory of the Replica Package you copied from the Primary.
5. Follow the prompts until the Installation Options dialog box opens.

   This dialog box lists the components you can install. For component descriptions, see Appendix E, "Installation Components."
6. Select **New Replica RSA ACE/Server**, and click **Next**.
7. Follow the prompts to complete the installation.

   The Replica is installed. Repeat this procedure for each Replica you want to install.

## Next Steps

- If you installed RADIUS and want to configure it for user authentication, see "Adding Servers as Agent Hosts to the Primary Database" on page 38.
- To install or upgrade Remote Administration, see Chapter 4, "Installing and Upgrading Remote Administration Software."
- To install or upgrade the Quick Admin browser-based administration application, see Chapter 6, "Installing the Quick Admin Software."

# 3 Upgrading to RSA ACE/Server 6.0

This chapter describes how to upgrade to RSA ACE/Server 6.0. You can upgrade from any of the following versions: RSA ACE/Server 5.1 (and patch versions) and RSA ACE/Server 5.2 (and patch versions). If you have RSA ACE/Server version 5.0 or earlier, you must first upgrade to version 5.1 or 5.2 before proceeding.

**Important:** If you plan to upgrade your operating system from Windows NT to a supported Windows 2000 or Windows 2003 platform, you must upgrade the operating system first, and then re-install RSA ACE/Server. For more information, see Chapter 2, "Installing the RSA ACE/Server."

## Pre-Upgrade Checklist

RSA Security recommends that you read the *RSA ACE/Server 6.0 Readme* (**readme.pdf**) before upgrading the RSA ACE/Server software. The *RSA ACE/Server 6.0 Readme* contains important configuration and installation information, as well as information about problems in the software found too late to be included in the standard documentation.

### You must have

- ❑ A machine that meets all the hardware, disk space, memory, and platform requirements described in Chapter 1, "RSA ACE/Server Requirements."
- ❑ 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 **sdserv** and **sdlog** database files.

  **Note:** Stop all RSA ACE/Server Services before you create backup copies of the database files.

- ❑ Local administrator privileges on the Primary and Replica Servers.
- ❑ The RSA ACE/Server 6.0 CD or online distribution file.
- ❑ The license files from your existing Primary Server or the new license files, if you have purchased a new license.

  For additional information regarding licenses, see the *RSA ACE/Server 6.0 Administrator's Guide.*

  **Important:** If you are applying a new license, you must make backup copies of the new license *after* you upgrade the RSA ACE/Server software. During the upgrade, the license file is modified. Therefore, if your license in the 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.

**You must know**

- ❑ The language and locale used by the Windows machine and the language you want to use.

  For information about supported languages, see the *RSA ACE/Server 6.0 Administrator's Guide*.
- ❑ The name and IP address of any Replica Server you want to add.
- ❑ The number of Replica Servers allowed by your license.

  If you have an RSA ACE/Server Base license, you can install 1 Replica. If you have an RSA ACE/Server Advanced license, you can install up to 10 Replicas.

## Preparing for the Primary Server Upgrade

**Important:** Before upgrading, turn off local access protection on the Primary and Replica Servers. Failure to do so may result in you being locked out of your machine(s). For instructions, see your RSA ACE/Agent documentation.

To prepare for the Primary Server upgrade, you must perform these tasks, described in detail in the sections that follow:

- **Task 1:** Stop the RSA ACE/Server Services on the 5.1 or 5.2 Primary Server and disable the automatic startup feature
- **Task 2:** Back Up the Database and License Files
- **Task 3**: Restart the machine.

### Task 1: Stop the RSA ACE/Server Services on the 5.1 or 5.2 Primary Server

You cannot upgrade the RSA ACE/Server software while RSA ACE/Server services are running on the Server you want to upgrade. You must also disable the automatic startup feature before you upgrade the software.

**To stop all RSA ACE/Server processes on the 5.1 or 5.2 Primary Server:**

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

1. While the Replica Server(s) is running, open the Control Panel on the Primary Server, and double-click the RSA ACE/Server icon.
2. In the RSA ACE/Server dialog box, under **RSA ACE/Server**, click **Stop**.
3. When the **Broker service stopped** message appears, click **OK**.

   If the Broker Connections dialog box opens, click **Yes**.
4. If **Automatic RSA ACE/Server startup** is selected, clear it.

### Task 2: Back Up the Database and License Files

After stopping all RSA ACE/Server processes, create backup copies of the database and license files by copying the entire contents of the ***ACEDATA*** directory. This directory contains the database files, license files, custom query files, the configuration file, and any RADIUS accounting files on the Server.

By default, RADIUS accounting files are stored in the ***ACEDATA*\radacct** directory. If you specified a different directory, the full path is listed in the **Accounting** tab of the RADIUS Configuration utility (**Start > Programs > RSA ACE/Server > Configuration Tools > RADIUS Configuration > Accounting)**. To back up the RADIUS accounting files, copy *all* directories in the ***ACEDATA*\radacct** or user-specified directory.

For more information on backing up RSA ACE/Server data, see Chapter 6, "Database Maintenance (Windows)," in the *RSA ACE/Server 6.0 Administrator's Guide*.

### Task 3: Restart the machine

Once you have restarted the machine, you are ready to upgrade the Primary Server.

## Upgrading the Primary Server

**To upgrade the Primary Server:**

1. On the 5.1 or 5.2 Primary Server, log in as a local administrator.
2. Insert the CD labeled "RSA ACE/Server 6.0" into the CD drive.
3. In the **aceserv\windows** directory, double-click **setup.exe**.
4. If your Windows system uses a non-English language, a Question dialog box opens.
   - To install the English version of the RSA ACE/Server database, click **Yes.**
   - To install another version of the database, click **No.** The language currently used by Windows will determine the database version to install.

   For information about supported languages, see the *RSA ACE/Server 6.0 Administrator's Guide*.
5. Follow the prompts until the New Input Files dialog box opens. You are prompted to select a directory for storing a copy of the database files. This process serves as a safeguard to preserve the original files in the event that any unwanted modifications are made to your database files.
6. If you are using a new license, specify the directory that contains the license files, and click **Next**.
7. Follow the prompts until the Installation Options dialog box opens. Select **Upgrade Primary RSA ACE/Server** and **Documentation**. If you are using a new license, select **Upgrade Existing License**. Click **Next**.

8. Follow the prompts to complete the installation.

   **Note:** During this part of the installation, a license status dialog box that gives you detailed information regarding your current license opens. For additional information about licenses, see the *RSA ACE/Server 6.0 Administrator's Guide.*

9. Restart the machine.
10. Restart the RSA ACE/Server Services from the RSA ACE/Server dialog box in the Control Panel on the Primary Server only under the following conditions:
    - You do not plan to add any additional Replica Servers.
    - You do not need to configure the Server for RADIUS support.

      If you want to load custom RADIUS data files, see "Loading Existing RADIUS Data" on page 34.
11. If ***ACEDATA*** contains custom queries, you must recompile these queries after rebooting the machine. Any queries that were configured to share must be re-shared and any queries that were configured to acquire must be re-acquired after upgrade. For more information about custom queries, see "Advanced Application Notes for Custom Queries" in Chapter 10 of the *RSA ACE/Server 6.0 Administrator's Guide*.

    **Note:** For each default query file that has been customized, the corresponding 6.0 version of the file is installed into ***ACEDATA*** in addition to migrating the customized version. To differentiate the 6.0 version of the file from the customized version, the suffix _6.0 is appended to each of the 6.0 default query file names. All customized default query files retain their names during the upgrade process.

The Primary Server upgrade is complete.

## Preparing the Replica Server

To prepare for the Replica Server upgrade, you must perform these tasks, described in detail in the sections that follow:

- **Task 1**: Copy the Replica Package from the Primary to the Replica Server
- **Task 2**: Stop all RSA ACE/Server Services on the Replica Server and disable the automatic startup feature
- **Task 3**: Back Up the Database and License Files
- **Task 4**: Restart the Replica Server

## Task 1: Copy the Replica Package from the Primary Server to the Replica Server

The Primary Server upgrade process creates a Replica record in the database and generates a Replica Package for the Replica Server in the ***ACEDATA*\replica_package** directory.

Do one of the following:

- If Push DB is enabled on the Primary Server, copy the ***ACEDATA*\replica_package\license** directory to a temporary directory outside of ***ACEDATA*** on the Replica machine. After you upgrade and start the Replica Server, the Primary pushes the database files to the Replica.
- If Push DB is disabled on the Primary Server, copy the contents of the ***ACEDATA*\replica_package** directory to a temporary directory outside of ***ACEDATA*** on the Replica machine.

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. You must also disable the automatic startup feature before you upgrade the software.

**To stop all RSA ACE/Server processes on the Replica Server:**

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

1. On the Replica Server, log in as a local administrator.
2. In the RSA ACE/Server dialog box, under **ACE/Server**, click **Stop**.
3. When the **Broker service stopped** message appears, click **OK**.
   If the Broker Connections dialog box opens, click **Yes**.
4. If **Automatic RSA ACE/Server startup** is selected, clear it.

## Task 3: Back Up the Database and License Files

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. To back up the database and license files, copy the ***ACEDATA*** directory.

By default, RADIUS accounting files are stored in the ***ACEDATA*\radacct** directory. If you specified a different directory, the full path is listed in the **Accounting** tab of the RADIUS Configuration utility (**Start > Programs > RSA ACE/Server > Configuration Tools > RADIUS Configuration > Accounting)**. To back up the RADIUS accounting files, copy *all* directories in the ***ACEDATA*\radacct** or user-specified directory.

For more information on backing up RSA ACE/Server data, see Chapter 6, “Database Maintenance (Windows),” in the *RSA ACE/Server 6.0 Administrator’s Guide*.

### Task 4: Restart the Replica Server

Once you have restarted the machine, you are ready to upgrade the Replica Server.

## Upgrading a Replica Server

**To upgrade a Replica Server:**

1. On the Replica Server, log in as a local administrator.
2. Insert the CD labeled "RSA ACE/Server 6.0" into the CD drive.
3. In the **aceserv\windows** directory, double-click **setup.exe**.
4. Follow the prompts until the Installation Options dialog box opens. Select **Upgrade Replica RSA ACE/Server** and **Documentation**, and click **Next**.
5. Follow the prompts to complete the installation.
6. Restart the RSA ACE/Server Services on the Replica.

   **Note:** When the Replica starts, if Push DB is enabled, the Primary pushes the 6.0 database to the Replica.

   The Replica reconciles the 6.0 database with the copy of the 5.1 or 5.2 Replica Server database.

The Replica Server upgrade is complete.

## Adding a Replica Server to an Existing RSA ACE/Server

To add Replicas to an existing RSA ACE/Server system, see "Adding and Installing a New Replica" on page 19.

# 4 Installing and Upgrading Remote Administration Software

Use the Remote Administration software to administer the RSA ACE/Server database from a remote location. You can run the Database Administration application from

- The Primary Server
- A Replica Server
- Other machines that run the RSA ACE/Server Remote Administration software

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

## 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 software.

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

**Note:** Make sure the machine is located in a secure area and can be accessed by trusted personnel only. Only the Database Administration application is protected by RSA SecurID authentication.

❑ 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 database until you upgrade the Remote Administration software. If you upgrade Remote administration software, you will no longer be able to administer a pre-6.0 database from the machine running the upgraded Remote Administration software.

❑ The language and locale used by the Windows machine and the language you want to use.

- ❑ Local administrator privileges on the remote machine.
- ❑ Access to the **sdconf.rec** and **server.cer** files on the Primary Server.

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

## Installing Remote Administration for the First Time

**Note:** The Remote Administration software is installed by default on your Primary or Replica Server as part of an RSA ACE/Server 6.0 installation or upgrade. However, a remote administration connection to a Replica Server database is read-only.

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

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

- Agent Host Auto Registration
- Remote Administration
- Remote RADIUS

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

- Remote RADIUS
- Remote Administration
- Agent Host Auto Registration

### To install the Remote Administration software:

1. On the remote machine, log in as an local administrator, and insert the CD labeled "RSA ACE/Server 6.0" into the CD drive.
2. In the **aceserv\windows** directory on the RSA ACE/Server CD, double-click **setup.exe**.
3. Follow the prompts until the New Input Files dialog box opens. Browse to the disk or directory containing the **sdconf.rec** and **server.cer** files, and click **Next**.
4. Follow the prompts until the Installation Options dialog box opens. Select **New Remote Administration**, and click **Next**.
5. Follow the prompts until the installation process is complete.
6. If you are not using DNS, add the name and IP address of the Server to the **hosts** file on the Remote Administration machine.

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

When the installation is complete, for instructions on configuring the Primary Server to allow Remote Administration, see "Remote Administration" in the *RSA ACE/Server 6.0 Administrator's Guide*.

## 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 an local administrator, and insert the CD labeled "RSA ACE/Server 6.0" into the CD drive.
2. In the **aceserv\windows** directory on the RSA ACE/Server CD, double-click **setup.exe**.
3. Follow the prompts until the Installation Options dialog box opens. Select **Upgrade Remote Administration**, and click **Next**.
4. Follow the prompts until the installation process is complete.

## Adding a Server to Administer Remotely

If you need to administer additional databases from a machine running the Remote Administration software, you can add a server for Remote Administration.

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

**To add a Server for Remote Administration:**

1. Click **Start** > **Settings** > **Control Panel** > **Add/Remove Programs**.
2. 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 the Primary.
   On a Windows 2000 or 2003 machine, the **hosts** file is in ***%SystemRoot%*\System32\drivers\etc**.

**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, thereby limiting the number of remote administration sessions that can run at the same time, by specifying a range of port numbers that can be used for remote administration connections.

**To specify a range of port numbers:**

1. Using the RSA ACE/Server Control Panel, stop the RSA ACE/Server and database brokers.
2. In the **ace\rdbms32** directory, make a backup copy of the **startup.pf** file. Name it **startup.old**.
3. In a text editor, open the **startup.pf** file, and add the following lines to the end of the file:

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

   The first port that TCP uses is always one greater than the minimum port number you specify, so the range must always include one more port than you need. If you have 10 remote connections, you need 20 ports and must specify a range of 21 ports.

   For example, to use ports 3001 through 3020 you would specify:

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

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

   **Note:** For Windows systems, the minimum port number cannot be less than 3000.

   If you use the Progress Development Toolkit, your system may be using a **startup.pf** other than the one that shipped with RSA ACE/Server 6.0. In this case, RSA Security recommends that you edit both **startup.pf** files according to this procedure.
4. Restart the RSA ACE/Server.

# 5 The RSA RADIUS Server

This chapter describes

- How to configure the RSA ACE/Server to support the RSA RADIUS server.
- How to install Remote RADIUS.

## Overview

The RSA RADIUS server runs on any RSA ACE/Server Primary or Replica machine or remote server. By default, the RADIUS server software is installed on the Primary and each Replica. To use the RADIUS server on the Primary, Replica, or on a remote server, you must first enable RADIUS in the **sdconf.rec** file of the Primary Server.

If you select the **Load RADIUS data** component as part of the Primary installation, the installation process

- Prompts you for the types and locations of any existing custom RADIUS data files (dictionary, user, and client files)
- Edits the **sdconf.rec** file on the Primary, so that the RADIUS server is enabled
- Configures the RADIUS server service name to **radius** and the RADIUS port number to **1645**, which are the default values

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.

The following table lists the steps you must follow to enable RADIUS, depending on whether or not you loaded RADIUS data during the Primary installation.

| Situation | Step(s) to Install RADIUS | Additional Step(s) to Install Remote RADIUS |
|---|---|---|
| Loaded RADIUS data during installation | • Configure your system to use the RSA RADIUS server.<br>• Add Primary and each NAS to the Primary database as Agent Hosts.<br>To begin, see "Configuring Your System to Use the RSA RADIUS Server" on page 33. | • Add remote machine to Primary database as Agent Host.<br>• Configure the remote system to use the RSA RADIUS server.<br>• Install Remote RADIUS.<br>For directions, go to "Adding Servers as Agent Hosts to the Primary Database" on page 38, then "Configuring Your System to Use the RSA RADIUS Server" on page 33, and finally "Installing Remote RADIUS" on page 39. |
| Did not load RADIUS data during installation | • Configure your system to use the RSA RADIUS server.<br>• Load existing RADIUS data.<br>• Enable RADIUS Server.<br>• Configure Primary for RADIUS support.<br>• Add Primary and each NAS to Primary database as Agent Hosts.<br>To begin, go to the following section, "Required RADIUS Information Checklist" and then go to "Configuring Your System to Use the RSA RADIUS Server" on page 33. | • Add remote machine to Primary database as Agent Host.<br>• Configure the remote system to use the RSA RADIUS server.<br>• Install Remote RADIUS.<br>For directions, go to "Adding Servers as Agent Hosts to the Primary Database" on page 38, then "Configuring Your System to Use the RSA RADIUS Server" on page 33, and finally "Installing Remote RADIUS" on page 39. |

## Required RADIUS Information Checklist

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

- ❑ The procedure used to add an Agent Host to the RSA ACE/Server database. For the procedure, see the Help. For more information about Agent Hosts, see the *RSA ACE/Server 6.0 Administrator's Guide*.
- ❑ 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 keys used by each NAS.

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

## Configuring Your System to Use the RSA RADIUS Server

To run the RSA RADIUS server, you must

- Verify that the RADIUS port number specified in the RSA ACE/Server Configuration Management application is the same as the RADIUS port number listed in the **services** file.

  By default, the RADIUS port number specified in the services file on a Windows 2000 or 2003 system is **1812**. The RSA RADIUS server uses port number **1645**.
- Disable the Windows Routing and Remote Access Service and the Internet Authentication Service.

  Until you disable these services, you cannot use the RSA RADIUS server.

**To disable the Routing and Remote Access Service:**

1. Click **Start** > **Settings** > **Control Panel**.
2. Double-click **Administrative Tools**.
3. Double-click **Routing and Remote Access Service**.
4. In the **Tree** tab, select the RADIUS server (the local machine).
5. On the Action menu, click **Disable Routing and Remote Access**.

**To disable the Internet Authentication Service:**

1. Click **Start** > **Settings** > **Control Panel**.
2. Double-click **Services**.
3. In the Services window, double-click **Internet Authentication Service**.
4. Select the **General** tab in the Internet Authentication Service Properties dialog box.
5. In the Startup type list, select **Disabled**.
6. If necessary, click **Stop** to stop the Internet Authentication Service.
7. Click **Apply**, and then click **OK**.
8. Restart the system.

### Next Steps

- If you loaded RADIUS data during the Primary installation, go to "Adding Servers as Agent Hosts to the Primary Database" on page 38.
- If you did not load RADIUS data during the Primary installation, go to the following section, "Loading Existing RADIUS Data."
- If you are installing Remote RADIUS, go to "Installing Remote RADIUS" on page 39.

## Loading Existing RADIUS Data

If you have existing RADIUS data files, you can load them into the RSA ACE/Server database from the Primary Server. For information about RADIUS data files, see "RADIUS Data File Formats" on page 42.

**Note:** Although loading RADIUS data during the Primary installation does enable RADIUS on the Primary, loading RADIUS data using the utilities described in this chapter does *not* enable the RADIUS server on the Primary. If you did not load RADIUS data during the Primary installation, see "Enabling and Disabling the RADIUS Server" on page 37.

**To load RADIUS data:**

1. Click **Start** > **Settings** > **Control Panel** > **Add/Remove Programs**.
   The Add/Remove Programs Properties dialog box opens.
2. 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. Highlight **Load Radius Data**, and click **Next**.
5. Select the corresponding boxes for the data files you want to load, and click **Next.**
6. Follow the prompts until the RSA ACE/Server Maintenance is completed, and click **Finish.**

When you have finished loading RADIUS data, proceed to "Enabling and Disabling the RADIUS Server" on page 37.

RSA ACE/Server also features 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. For instructions, see the following section, "Importing a Dictionary File." |
| removeattr | Removes attributes from the database, and edits the **securidmapfile**, which determines which attributes are user configurable and multiply-defined. For instructions, see "Removing Attributes" on page 36. |
| loadraduser | Imports an existing RADIUS user file. For instructions, see "Importing User and Client Files" on page 36. |
| loadradcli | Imports an existing RADIUS client file and creates an Agent Host record in the RSA ACE/Server database. For instructions, see "Importing User and Client Files" on page 36. |

## Importing a Dictionary File

The **loadraddb** program loads the dictionary file. Use **loadraddb** under one or more of the following conditions:

- You did not load RADIUS data during the installation on the Primary, and you now want to load RADIUS data.
- You receive a new dictionary file from RSA Security.
- You edit the existing dictionary file.

To load the dictionary, type

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

- **xyzzy** is the hardcoded password required to run the **loadraddb** program.
- ***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.

## Removing Attributes

The **removeattr** program is a command line utility that disables attributes in the RSA SecurID map file and removes individual attributes from any RADIUS profile that contains the attribute. A disabled attribute cannot be configured 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`

   - **xyzzy** is the hardcoded password required to run the **removeattr** program.
   - **securidmapfile** is the RSA Security RADIUS attribute map file.
   - ***attribute-number*** is the integer encoding of the attribute.

   **Note:** Chapter 7, "Additional Administrative Tasks," in the *RSA ACE/Server 6.0 Administrator's Guide* contains the integer encodings for all RFC-defined RADIUS attributes. The dictionary file contains the integer encodings and values for all supported attributes, as well as examples of vendor-specific 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 none exists 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 one profile and assigned it to many users. When you import these user data files, **loadraduser** creates multiple profiles, one for each user. To simplify administration, after you run **loadraduser**, you can unassign these profiles and create a default profile (named **Default**), which is assigned automatically to all users without assigned profiles.

You can run **loadraduser** and **loadradcli** whenever you need to load additional RADIUS user or client data files. Click **Start > Run**, type the command followed by the full pathname of the file, and click **OK**.

| To Import | Type |
|---|---|
| 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

When the RSA RADIUS server is enabled, the RADIUS service starts each time the RSA ACE/Server starts. You can easily enable and disable the RADIUS server on any one of the RSA ACE/Servers in your system.

### To enable or disable the RSA RADIUS Server:

1. Log in to the Primary Server as a Windows local administrator.
2. Click **Start > Programs > RSA ACE/Server > Configuration Tools > Configuration Management**.

   The Configuration Management dialog box opens.
3. Click **Edit**.
4. In the Reminder dialog box, click **OK**.
5. Under **Enable Features**, do one of the following:
   - To enable the RADIUS server, select the **RADIUS Server Enabled** box.
   - To disable the RADIUS server, clear the **RADIUS Server Enabled** box.
6. Click **OK**.

**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 Primary 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 Primary that does not have the RADIUS server enabled.

If you did not load RADIUS data during the Primary install, proceed to the following section, “Configuring the Primary Server for RADIUS Support.”

## Configuring the Primary Server for RADIUS Support

By default, the correct configuration values for the RSA RADIUS server are set during the RSA ACE/Server installation. Use this procedure to either:

- Verify that the default values are the same as those used by your NAS devices
- Change the default values to reflect your NAS device configurations

**To configure the RSA ACE/Server to use the RSA RADIUS server:**

1. Log in to the Primary Server as a Windows local administrator.
2. Click **Start** > **Programs** > **RSA ACE/Server** > **Configuration Tools** > **Configuration Management**.

   The Configuration Management dialog box opens.
3. Click **Edit**.
4. In the Reminder dialog box, click **OK.**
5. Under **Services**, verify that
   - The RADIUS **Port Number** is **1645.**
   - The RADIUS **Service Name** is **radius.**

   If your NAS devices use a different port number or service name for RADIUS authentication, enter the number or name in the RADIUS **Port Number** or **Service Name** box, and click **OK**.

   If a message indicates that the RADIUS port number is not defined in the **etc/services** file, open the **services** file (located in the ***%SystemRoot%*\System32\drivers\etc** directory) in a text editor, and edit the following line to reflect your RADIUS service name and port number:

   ```
   radius      1645/udp
   ```
6. Click **OK**.

If you did not load RADIUS data during the Primary install, proceed to the following section, “Adding Servers as Agent Hosts to the Primary Database.”

## Adding Servers as Agent Hosts to the Primary Database

After configuring the RSA ACE/Server to use RADIUS, you need to add the applicable server (Primary, Replica, or remote) and each NAS to the Primary database as Agent Hosts of the Primary. For more detailed instructions on adding Agent Hosts, see the Help topic “Adding an Agent Host.”

**To add an Agent Host:**

1. Click **Start** > **Programs** > **RSA ACE/Server** > **Data Administration - Host Mode**.
2. Click **Agent Host** > **Add Agent Host**.

   The Add Agent Host dialog box opens.

3. Add the appropriate server as an Agent Host:
   - For Name, type the name of the Primary, Replica, or Remote RADIUS Server, as appropriate.
   - For Agent type, select **Net OS Agent**.
   - Do not activate any RADIUS users directly on this Agent Host.
4. Add each NAS device as an Agent Host:
   - For 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.

   You do not need to activate any of these users or groups on the Primary, Replica, or remote server Agent Host.

If you want to install Remote RADIUS, first add the remote machine to the Primary database as an Agent Host using the procedure in this section, and then go to the following section, "Installing Remote RADIUS."

## Installing Remote RADIUS

If you are 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

### Installation Checklist

Before you begin, verify that you have:

- ❑ A machine with an Intel Pentium processor running Windows 2000 or Windows Server 2003. For more information on hardware, disk space, and memory requirements, see Chapter 1, "RSA ACE/Server Requirements."
- ❑ A copy of the RSA ACE/Server 6.0 CD or online distribution file.

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

  If you did not enable RADIUS during the Primary Server installation, see "Required RADIUS Information Checklist" on page 33, and then see "Loading Existing RADIUS Data" on page 34.
- ❑ Added the remote server and each NAS to the Primary database as Agent Hosts. For instructions, see "Adding Servers as Agent Hosts to the Primary Database" on page 38.
- ❑ Local administrator privileges on the Primary Server and the remote machine.
- ❑ Access to the **sdconf.rec** and **server.cer** files on the Primary Server. Copy the **sdconf.rec** and **server.cer** files from the ***ACEDATA*** directory to a diskette, and make the file accessible to the machine on which you are installing Remote RADIUS.

  RADIUS must be enabled in the **sdconf.rec** file before you copy it from the Primary.

**Important:** Remote RADIUS automatically uses the configuration record from any RSA ACE/Agent installed on the same machine. If you are installing Remote RADIUS on a machine on which an RSA ACE/Agent is installed, make sure Remote RADIUS and the RSA ACE/Agent are both pointing to the same Primary in their respective **sdconf.rec** files. In addition, Remote RADIUS may be affected if you uninstall the RSA ACE/Agent and replace it with a different version.

### To install Remote RADIUS:

1. On the Server you want to administer, log in as a local Windows administrator.
2. On the remote machine, log in as a local administrator, and insert the CD labeled "RSA ACE/Server 6.0" into the CD drive.
3. In the **rradius\windows** directory on the RSA ACE/Server CD, double-click **setup.exe.**
4. Follow the prompts. If the install does not find the **sdconf.rec** and **server.cer** files in the ***%SystemRoot%*\system32** directory, you are prompted for their location(s). Browse to the directory containing the **sdconf.rec** and **server.cer** files, and click **Next**.

   **Note:** The **sdconf.rec** and **server.cer** files can be stored in different directories, but they must be from the same Primary or Replica Server.
5. Follow the prompts until the installation is complete.

## 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 defective or duplicated packets are remedied
- 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. To display a window where you can select RADIUS server parameters and change their values, either run **rwconfig.exe**, located by default in the ***ACEPROG*** directory, or click **Start > Programs > RSA ACE Server > Configuration Tools > RADIUS Configuration**. 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 Appendix B, “Configuring the RADIUS Server,” in the *RSA ACE/Server 6.0 Administrator’s Guide*.

## Configuring a RADIUS Device

This section describes, in generic terms, 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 the following 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, and the *recommended* minimum is 12.
- An RSA ACE/Server host with the RSA RADIUS server enabled is specified on the NAS device as a RADIUS server host.
- The RADIUS port number specified on the NAS device matches the port number specified through the Configuration Management application on the Primary Server.

  The default port number for RADIUS authentication is 1645.
- The RADIUS accounting port number specified on the NAS device is one greater than the RADIUS port number specified through the Configuration Management application on the Primary Server.

  The default port for RADIUS accounting is 1646.

For information on configuring the RSA RADIUS server, see the *RSA ACE/Server 6.0 Administrator’s Guide*.

# RADIUS Data File Formats

There are four RADIUS data files. If you edit 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 the edited files to the database using the utilities described in this chapter.

## Dictionary

The dictionary file contains the attributes and values that are supported by the RSA RADIUS server. 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 are 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               1       0
User-Password           0       0
CHAP-Password           0       0
NAS-IP-Address          0       0
NAS-Port                0       0
Service-Type            1       0
Framed-Protocol         1       0
```

### User File

The user file contains the user login name and the attribute/value pairs 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 or name 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    4568267543897
192.168.10.22    6893286346533
192.168.10.24    9888228594567
```

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

**Note:** Client files with empty keys are not imported.

## Next Steps

For an overview of the RSA ACE/Server Database Administration application, see Chapter 1, "Overview," in the *RSA ACE/Server 6.0 Administrator's Guide.*

For information about configuring the RSA RADIUS Server, see Appendix B, "Configuring the RADIUS Server" in the *RSA ACE/Server 6.0 Administrator's Guide*.

For information about how to create a generic RADIUS user profile and descriptions of the standard RADIUS attributes you can include in a user profile, see Chapter 11, "Additional Administrative Tasks," in the *RSA ACE/Server 6.0 Administrator's Guide*.

# 6 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 6.0 Administrator's Guide* and the Quick Admin Help.

## Quick Admin Architecture

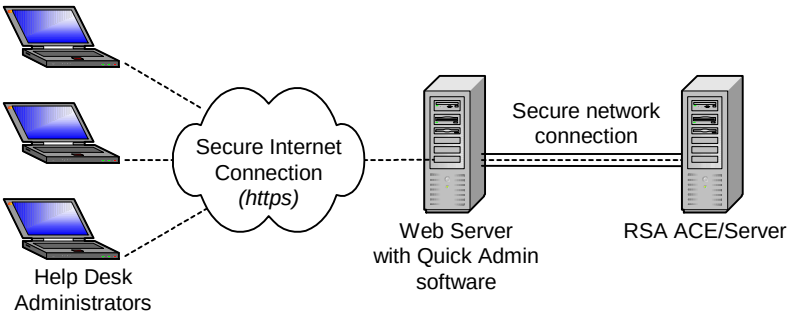
Quick Admin consists of

- 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 6.0 CD or online distribution file. | 1.3.1.03 or later. You can install this from the RSA ACE/Server 6.0 CD or online distribution file. |

RSA Security strongly recommends that you

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

The following Quick Admin installation requirements are for Solaris 8 and Solaris 9 on UltraSparc processors:

- Java System 6.x or iPlanet 5.x web servers (JavaScript-enabled).
- JavaRuntime Environment (included on the RSA ACE/Server 6.0 CD).

RSA Security strongly recommends that you

- Use a secure connection (**HTTPS**) to prevent user names and passwords from being sent in clear text.
- Secure your web server host according to the latest 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 6.0 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 by clicking **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Services**.

## 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 a 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 this message. 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 6.0 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 is completed, 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 user name 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 user name 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

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 CD into the web server host.
3. Change to the following directory on the CD

   `/cdrom/cd_name/QuickAdmin/UNIX`

   *cd_name* is the name of the RSA ACE/Server 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 user name 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 Java System 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 to Quick Admin 6.0 from a Previous Version

Use the following procedure to upgrade from Quick Admin 5.1 or 5.2 to Quick Admin 6.0.

### On a Windows Machine

**To upgrade Quick Admin on a Windows machine:**

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

1. 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 6.0 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 is completed, and then click **Finish**.

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

## On a Solaris Machine

**To upgrade Quick Admin on a Solaris machine:**

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

Follow the instructions on page 50 for installing Quick Admin 6.0 on a Solaris 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 6.0 Quick Admin with your current installation, type **y**.
- When you finish installing Quick Admin, *do not* re-configure JRun.

# Installing Quick Admin After Web Express Is Installed

The following table describes how to install Quick Admin 6.0 after Web Express 1.1 or 1.2 is already installed.

| Task | Platform | Procedure |
|---|---|---|
| Install Quick Admin 6.0 after Web Express 1.1 is installed | Windows | See the procedure "To upgrade Quick Admin on a Windows machine:" on page 51. |
| Install Quick Admin 6.0 after Web Express 1.2 is installed | Windows | See the following procedure "To install Quick Admin 6.0 on Windows when Web Express 1.2 is already installed:" |
| Install Quick Admin 6.0 after Web Express 1.1 is installed | UNIX | See the procedure "To upgrade Quick Admin on a Solaris machine:" on page 52. |
| Install Quick Admin 6.0 after Web Express 1.2 is installed | UNIX | See the procedure "To upgrade Quick Admin on a Solaris machine:" on page 52. |

**To install Quick Admin 6.0 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 6.0 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\Windows\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\properties\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 6.0 is already installed.

| Task | Platform | Procedure |
|---|---|---|
| Install Web Express 1.1 after Quick Admin 6.0 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 6.0 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.<br>The default path is **certs/**.<br>For instructions on adding certificates from more than one Primary Server, see "Administering Multiple Primary Servers" on page 60. |
| ACE_PORT | The Primary Server TCP port on which the RSA ACE/Server Quick Admin daemon is listening.<br>The default port is **5570**. |
| REPORT_PATH | The path to the directory where Quick Admin writes report files.<br>The default path is **reports/**.<br>**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.<br>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.<br>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.<br>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.<br>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.<br>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.<br>The default path is **quickadmin/**.<br>**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 58.

| Parameter | Value |
|---|---|
| USER_PWD_LIFETIME_DAYS<br>USER_PWD_LIFETIME_HOURS | Determine the number of days and hours before user passwords expire. You can set days, hours, or both.<br>For example, if USER_PWD_LIFETIME_DAYS=5<br>and USER_PWD_LIFETIME_HOURS=3, the user password expires in 123 hours.<br>Acceptable values: 0-8760 days, 0-23 hours<br>The combined number of hours and days can equal no more than 8760 days, or 24 years.<br>The default values for these parameters are<br>USER_PWD_LIFETIME_DAYS=30<br>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.<br>By default, this parameter is undefined. |
| LOST_TOKEN_PWD_LIFETIME_DAYS<br>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.<br>For example, if LOST_TOKEN_PWD_LIFETIME_DAYS=5<br>andLOST_TOKEN_PWD_LIFETIME_HOURS=3, the user password expires in 123 hours.<br>Acceptable values: 0-8760 days, 0-23 hours<br>The combined number of hours and days can equal no more than 8760 days, or 24 years.<br>The default values for these parameters are<br>LOST_TOKEN_PWD_LIFETIME_DAYS=7<br>LOST_TOKEN_PWD_LIFETIME_HOURS=0<br>For more information about temporary passwords to replace lost tokens, see the *RSA ACE/Server 6.0 Administrator's Guide*. |

| Parameter | Value |
|---|---|
| FIXED_PWD_LIFETIME_DAYS<br>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.<br>You can set days, hours, or both.<br>For example, if FIXED_PWD_LIFETIME_DAYS=5<br>and FIXED_PWD_LIFETIME_HOURS=3, the user password expires in 123 hours.<br>Acceptable values: 0-8760 days, 0-23 hours<br>The combined number of hours and days can equal no more than 8760 days, or 24 years.<br>The default values for these parameters are<br>FIXED_PWD_LIFETIME_DAYS=7<br>FIXED_PWD_LIFETIME_HOURS=0 |
| OTP_PWD_LIFETIME_DAYS<br>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.<br>For example, if OTP_PWD_LIFETIME_DAYS=5<br>and OTP_PWD_LIFETIME_HOURS=3, the user password expires in 123 hours.<br>Acceptable values: 0-8760 days, 0-23 hours<br>The combined number of hours and days can equal no more than 8760 days, or 24 years.<br>The default values for these parameters are<br>OTP_PWD_LIFETIME_DAYS=7<br>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<br>FIXED | Values defined for LOST apply to OTP | Values defined for FIXED apply to OTP |
| LOST<br>OTP | Values defined for LOST apply to FIXED | Values defined for LOST apply to FIXED and OTP |
| LOST<br>FIXED<br>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.<br>Maximum value: 2147483647<br>The value is in milliseconds (100 = 1 second.)<br>The default is 60000. |
| ACE_REPLY_RETRY | Indicates how often Quick Admin checks for a response from the RSA ACE/Server.<br>Maximum value: 2147483647<br>The value is in milliseconds (100 = 1 second.)<br>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,<br>`#Verbose=no`<br>The log file is usually in the ***JRun installdirectory/*logs** directory.<br>Note that the log file grows very quickly. If you turn on debugging, be sure to monitor it.<br>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**).<br>Note that the Verbose flag overrides all other *_Verbose flags.<br>The default value for this parameter is **no**. |
| Login_Verbose<br>SearchPage_Verbose<br>EditToken_Verbose<br>EditUser_Verbose<br>Report_Verbose<br>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**).<br>Note that the Verbose flag overrides all other *_Verbose flags.<br>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.<br>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<br>(**TCP Port** on UNIX installations) | TCP port on which the RSA ACE/Server Quick Admin daemon is running on the Primary Server.<br>The default value is **5570**. |
| Verbose | Determines whether or not detailed logging messages are written to the Windows Event Viewer or UNIX **syslog**.<br>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.<br>The inactivity parameter must be specified in minutes.<br>The default value is **15**.<br>**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 user name 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 Transferring the RSA ACE/Server from UNIX to Windows

**To transfer the RSA ACE/Server from UNIX to Windows:**

1. Perform a fresh installation of the RSA ACE/Server on a Windows machine. For instructions, see "Installing a New Primary" on page 15.

   After installation, the database on the Windows machine contains one record, which is a user record for the administrator who installed the RSA ACE/Server software.

2. On the existing UNIX Primary Server, stop the **aceserver** by typing

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

3. Create a dump file for the Server database. Type

   ```
   ./sddump -s
   ```

   A file named **sdserv.dmp** is created in the current directory.

4. Create a **\dump** directory on your Windows system.

5. Copy the **sdserv.dmp** and **license.rec** files from the UNIX system running the RSA ACE/Server to the **\dump** directory. If you use **ftp** to transfer the files, copy them in binary mode.

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

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

**To load the dump files:**

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

1. Verify that no RSA ACE/Server processes are running on the Primary:
   - On the Server, open the Control Panel and double-click the ACE/Server icon.
   - In the RSA ACE/Server dialog box, under ACE/Server, click **Stop**.
   - When the Broker service stopped message appears, click **OK**.
   - If the Broker Connections dialog box opens, click **Yes**.
2. Click **Start > Programs > RSA ACE/Server > Database Tools > Load** (or, in the ***ACEPROG*** directory, double-click **sdload.exe**).

   The Database Load dialog box opens.
3. Select the **Server Database** box to indicate that you want to load a Server dumpfile.

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

   **Important:** RSA Security strongly recommends that you back up your current database before performing a Database Load in Merge mode. For more information about the Merge option, see "Merge Logic" on page 70.

6. Click **OK**.

   The **sdload.exe** program loads the dump files into the RSA ACE/Server 6.0 database.
7. Click **Close**.

**Note:** The RSA ACE/Server UNIX machine is automatically added to the RSA ACE/Server Windows machine as a Replica. To delete it, go to **Start > Programs > RSA ACE/Server > Configuration Tools > Replication Management**.

# B Minimum System Requirements (Windows 2003 Server Only)

This appendix specifies the minimum Windows 2003 Server components required for the RSA ACE/Server to function properly. Before you minimize your system, review "Important Installation Guidelines" for RSA ACE/Server on page 12.

**Note:** For information about RSA ACE/Server services and processes, see Appendix I, "Services and Processes," in the *RSA ACE/Server 6.0 Administrator's Guide*.

To ensure that your system is properly minimized, RSA Security recommends that you perform a fresh installation of Windows 2003 Server. During the installation, when you set up the network interface card (NIC), do the following

- Use **Custom Settings**.
- Uninstall all settings except **Internet Protocol (TCP/IP)**.

When you configure DNS and WINS on the NIC, do the following:

- If DNS is not supported in your environment, disable **Register This Connection's Address in DNS**.
- Disable **Enable LMHOSTS lookup**.
- On the WINS tab, select **Disable NetBIOS Over TCP/IP**.
- Ensure that the system is part of a self-contained workgroup.

When you complete the installation, you must configure the services.

## Configuring Windows 2003 Server Services for Minimization

After you install the operating system, set the following services to **Automatic** and make sure they are started:

- DNS Client
- Event Log
- Logical Disk Manager
- Network Connections
- Plug & Play
- Protected Storage
- Remote Procedure Call
- Removable Storage
- Secondary Login Service
- Security Accounts Manager
- Windows Management Instrumentation

Set the following services to **Manual**, and make sure they are stopped:

- Uninterrupted Power Supplies
- Windows Installer
- Windows Time

Disable *all* other services.

## Windows 2003 Server Service Packs

Once you have installed and minimized Windows 2003 Server, you may install the appropriate service packs and hot fixes. Note that RSA Security may not yet have verified RSA ACE/Server 6.0 against recently released hot fixes. Therefore, you should consult RSA Security Customer Support prior to installing any recent hot fixes.

# C Database Utilities

This appendix describes the database utilities that enable you to perform installation and administration tasks. The utilities are:

| Utility | Purpose |
|---|---|
| Database dump (**sddump.exe**) | Dumps the contents of the Server database and the log database to separate dump files (**sdserv.dmp** and **sdlog.dmp**). |
| Database creation (**sdnewdb.exe**) | Creates a new, empty database, which is required before you can load the dump files. |
| Database load (**sdload.exe**) | Loads the dump files into a new database. |
| Database dump reader (**dumpreader.exe**) | Outputs the contents of a dump file to any of several industry-standard text formats (CSV, HTML, XML, TXT). |

The database dump and load utilities include interface and command line versions. The command line versions of the dump and load utilities can be run from a DOS prompt. These versions contain additional functionality that allows you to dump and load specific database tables. For more information, see "Using the Dump and Load Utilities in DOS" on page 70.

**Note:** This appendix does not cover the Replica Management (**sdrepmgmt_nt**) utility, which performs a number of important functions related to Replica Servers. This utility enables you to add and delete Replica Servers, mark Replica Servers as requiring a new database, create Replica Packages, and promote a Replica Server to the Primary. For information, see the *RSA ACE/Server 6.0 Administrator's Guide*.

## Dumping the Database

**To dump the database:**

1. Click **Start > Programs > RSA ACE/Server > Database Tools >Dump**.
   The ACE/Server Database Dump dialog box opens.
2. Under Select Databases to dump, select **Dump Log Database** and **Dump Server Database**.
3. Under Options, select **Include delta tables in dump file** to dump all associated delta information. **Allow database connections in multi-user mode** allows you to perform the dump while the database is active. If you have stopped all RSA ACE/Server Services, you can select the box to enable this option. If you have *not* stopped all RSA ACE/Server services, the option is enabled by default.

**Note:** A dump file generated from an active database usually contains temporary records resulting from other administrative activity. Multi-user mode is recommended only when you are creating dump files for examining the contents of a database for other pre-load testing purposes.

4. Under **Selective Dump**, you can use the radio buttons to specify different categories of data. Choose
   - **By Group** to dump a specific group. Enter the name of a group.
   - **By User** to dump a specific user. Enter a default user name.
   - **By Token** to dump a specific token. Enter a serial number.
5. Under **Disk Space Requirements**, verify that the amount of disk space available exceeds the amount of space required. In the **Output Directory** box, specify the path of the directory in which you want to create the dump files.

   Specify a path that is outside of the directory that contains the RSA ACE/Server software (usually **ace**). If you create the dump files in the default directory location, you must copy them to another directory before uninstalling the RSA ACE/Server software.
6. Click **OK**.

   The RSA ACE/Server Database Dump dialog box displays the status of the dump process.
7. Do one of the following:
   - Click **Close** when the dump process is done.
   - If you want to save the status report of the dump process, click **Save As**, specify a file name and a directory, click **Save**, and then click **Close**.

   The directory you specified in the **Output Directory** box now contains the dump files **sdserv.dmp** and **sdlog.dmp**. The database load process, described in "Loading Dump Files" on page 69, requires these dump files and the **license.rec** file you copied from the ***ACEDATA*** directory.

The dump process is complete.

## Creating a New Database

Creating a new database overwrites all records in the existing database. Make sure that any dump file you load into the new database contains at least one local administrator record.

**To create a new database:**

1. Make sure that no RSA ACE/Server processes are running.
2. In the ***ACEPROG*** directory, double-click **sdnewdb.exe**.
3. To create a new, empty RSA ACE/Server database, select the **Log Database** and **Server database** boxes.
4. Click **OK**.

   When the program is complete, you are asked to confirm the creation of the new database.

## Loading Dump Files

**To load the dump files:**

1. Make sure that no RSA ACE/Server processes are running.
2. Copy the dump files to the ***ACEDATA*** directory.
3. In the ***ACEPROG*** directory, double-click **sdload.exe**.
4. Select the **Server** and **Log** boxes to indicate that you want to load Server and log dump files.
5. In the **Path of server dump file**, enter the location of the Server dump file, and the **license.rec** file if you are merging a database from another realm, or click **Browse** to select the location.
6. In the **Path of log dump file,** enter the location of the log dump file or click **Browse** to select the location.
7. In the **Server Database Load Options** box, specify the criteria to use in the load operation by selecting one or a combination of the following:
   - **Server dump file has a different licence record than the current database** to load dump files from a different installation of the RSA ACE/Server, or to merge dump files from different realms into an RSA ACE/Server 6.0 database.
   - **Load delta records** to load a dump file and associated delta records.
   - **Commit loaded records only if all records are loaded successfully** to commit the records to the database only when the dump file loads successfully. If the dump file does not load successfully, no changes are committed to the database.
   - **Merge records from server dump file with records in current database** to insert data from a Server dump file into the database. For more information, see the following section, "Merge Logic."
8. To load the dump file(s) into the database, click **OK.**

### Merge Logic

When you select **Merge records from server dump file with records in current 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. Note that system records from the dump file are not loaded into the new database.

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

Selecting **Commit loaded records only if all records are loaded successfully** 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.

## Using the Dump and Load Utilities in DOS

The database dump and load utilities include DOS command line versions that allow you to dump specific tables from the Server database or load specific tables into the Server database from a dump file. This section describes the four command line dump and load utilities.

### sdloadsrv

The **sdloadsrv** utility allows you to load a Server dump file to the database using the DOS command line. There is additional functionality in this command line version that is not available using the interface version of the load utility (**sdload.exe**). This additional functionality includes the ability to selectively load tables from Server dump files.

The following table describes the option and arguments of **sdloadsrv**:

| Option | Argument | Description |
|---|---|---|
| **-d** | *database name* | Specifies database file name. If not specified, defaults to ***ACEDATA*\sdserv**. |
| **-f** | *filename* | Specifies load file name. This option is required. |
| **-a** | None | Compression mode. Loading compresses the database file. Retains all delta records. |
| **-m** | None | Merges Server dump files (from any version) into the Primary Server database. |
| **-u** | None | Loads a version 4.1 or earlier dump file in upgrade mode, which creates the Replica table in the new database and adds the current system as the Primary Server. When used with a 6.0 dump file, this option behaves like the **-r** option. |

| Option | Argument | Description |
|---|---|---|
| **-t** | *table_list* | Specifies a list of tables containing associated data for each record to be read from the dump file. |
| **-r** | None | Makes the current system the Primary Server. Use this option only when you are attempting to recover a failed database or Server. When used with a 4.1 or earlier dump file, this option behaves like the **-u** option. |
| **-l** | *licensefile* | Specifies a license file. |
| **-c** | None | Commit changes to the database only when the dump file loads successfully. If the dump file does not load successfully, no changes are committed to the database. |
| **-v** | None | Provides detailed output information. |

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

## sddumpsrv

The **sddumpsrv** utility allows you to create a dump file from the database using the DOS command line. There is additional functionality in this command line version that is not available using the interface version of the dump utility (**sddump.exe**). This additional functionality includes the ability to selectively dump tables from the Server database.

The following table describes the option and arguments of **sddumpsrv**:

| Option | Argument | Description |
|---|---|---|
| **-d** | *database name* | Specify database file name. |
| **-f** | *filename* | Specify dump file name. |
| **-t** | *table list* | Specifies a list of tables containing associated data for each record to be read from the dump file. |
| **-p** | None | Dumps required parent tables. |
| **-r** | None | Dumps replica (delta) records. |
| **-m** | None | Allows you to dump the database in multi-user mode (while the database brokers are running). |
| **-g** | None | Dumps group, group members, users, and their tokens. |
| **-u** | *login* | Dumps a user record and tokens by associated default login. |
| **-l** | *login* | Same as **-u.** |

| Option | Argument | Description |
|---|---|---|
| **-a** | *serial number* | Dumps a single token, specified by the serial number. |
| **-v** | None | Provides detailed output information. |

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

## sdloadlog

The **sdloadlog** utility allows you to load a log dump file to the database using the DOS command line.

The following table describes the option and arguments of **sdloadlog**:

| Option | Argument | Description |
|---|---|---|
| **-d** | *database name* | Specifies a database file name. |
| **-f** | *filename* | Specifies a load file name. |

## sddumplog

The **sddumplog** utility allows you to dump a log database using the DOS command line.

The following table describes the option and arguments of **sddumplog**:

| Option | Argument | Description |
|---|---|---|
| **-d** | *dbname* | Specifies a database file name. |
| **-f** | *filename* | Specifies a load file name. |
| **-m** | None | Allows you to dump the database in multi-user mode while the database brokers are running. |

# Using the Dumpreader Utility

With the Dumpreader utility, you can 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 DOS

The Dumpreader utility can be run only from a DOS command prompt.

**Note:** A version of the Dumpreader utility is also available for UNIX platforms. For information, refer to the *RSA ACE/Server 6.0 for UNIX 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:<br>• **CSV** – Comma-separated values; can be imported into Microsoft Excel or some other third-party reporting format.<br>• **HTML** – Hypertext Markup Language; can be viewed in a web browser.<br>• **XML** – Extended Markup Language; can be imported into a third-party reporting application.<br>**Note:** For CSV, HTML, and XML, one file is created for each table in the database.<br>• **XML2** – Similar to XML, except that it uses a different document type definition (DTD), and all output is collected in one file.<br>• **TXT** – Structured text format; can be viewed in a text editor. All output is collected in one file. |

| Option | Argument | Description |
|---|---|---|
| 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.<br>For XML2 and TXT, specifies the name of the file to which the output will be written. If no parameter is provided, the output is written to **stderr** (the console). If the parameter is empty but surrounded by double-quotes ("), the output is to **stdout**, which is also typically the console. |
| **-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.<br>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.

### HTML

To view dump file data in your web browser, use the **HTML** argument in the **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 contains 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 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 77.

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 a third-party program such as Microsoft Excel, use the CSV argument in the **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 folder 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), use the XML argument in the **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 folder 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 contained. 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, Notepad). With the **-c** option, the tables are consolidated and placed in alphabetical order within the text file.

For 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 use 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 6.0 Administration Toolkit Reference Guide* (**ace_admin_toolkit.pdf**).

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

## 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 |
|---|---|
| 6.0 | 20.00.00 |
| 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:** For details about the Dumpreader utility command syntax, see "Using the Dumpreader Utility" on page 73. 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.

# D Creating User Records from a SAM Database

This appendix describes two utilities you can use to move user information from an existing Security Accounts Manager (SAM) database on a Windows NT system to the RSA ACE/Server database on Windows 200 Server or Windows 2003 Server.

| Utility | Purpose |
|---|---|
| **dumpsamusers.exe** (NT only) | Reads user records from one or more SAM databases and writes them to a comma-separated text file. Each record contains the login, first name, and last name of a single user. |
| **loadsamusers.exe** (Windows 2000 and Windows 2003 only) | Reads and parses the text file. For each user in the file, creates a record in the RSA ACE/Server database containing the three pieces of data for that user. |

It is not possible to automate the transfer process completely. Windows NT 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. However, some inconsistencies are likely to occur, and you will have to edit the output file manually to eliminate these before **loadsamusers** can work properly.

## Extracting SAM User Records with dumpsamusers.exe

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

### Syntax

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

### Arguments

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

### Editing the Output File

**dumpsamusers** parses names according to these rules:

- When the order is “last, first,” whatever precedes the comma is parsed as the last name, and whatever follows the comma 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 the comma is parsed as the first name.

If middle initials are used, **dumpsamusers** 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<br>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, 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 proportion of the records need to be changed.

## Creating RSA ACE/Server User Records with loadsamusers.exe

Run the **loadsamusers** utility from a Windows 2000 or Windows 2003 command prompt. Because it employs functions that are part of the RSA ACE/Server Administration Toolkit, you must invoke this utility from a directory that also contains the **apidemon.exe** program, and the database broker must be running when the utility is invoked.

### Syntax

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

### Arguments

| | |
|---|---|
| *infile* | Specifies the input file—that is, the **dumpsamuser**s 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. Non-fatal 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, RSA ACE/Server creates it. Optional: If omitted, users are not assigned to a group.<br>**Note:** This argument is case-sensitive. |

**loadsamusers** 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 RSA ACE/Server database.

# E Installation Components

The following table describes the components displayed in the Installation Options dialog box. The components you see in the Installation Options dialog box depend on whether you are installing a new RSA ACE/Server or upgrading an existing RSA ACE/Server.

| Component | Description |
|---|---|
| New Primary RSA ACE/Server | Installs RSA ACE/Server 6.0 and Remote Administration software on a Primary Server. |
| Upgrade Primary RSA ACE/Server | Upgrades Primary Server to an RSA ACE/Server 6.0 Primary Server and installs the Remote Administration software. |
| New Replica RSA ACE/Server | Installs RSA ACE/Server 6.0, and Remote Administration software on a Replica Server machine. |
| Upgrade Replica Server | Upgrades a Replica Server to an RSA ACE/Server 6.0 Replica Server and installs the Remote Administration software. |
| New Remote Administration | Installs the Remote Administration software on a machine running a supported version of the Windows operating system. The Remote Administration software is installed by default on your Primary and Replica Servers as part of the RSA ACE/Server installation. |
| Upgrade Remote Administration | Upgrades the Remote Administration software. |
| Add Server for Remote Administration | Enables the Remote Administration machine to administer additional Servers. |
| Load RADIUS data | Imports existing, user-specified RADIUS data files and enables the RADIUS server on a 6.0 Server. |
| Documentation | Installs the RSA ACE/Server 6.0 documentation in the ***ACEDOC*** directory. |

F

# Uninstalling the RSA ACE/Server

Before uninstalling the software, back up all RSA ACE/Server files. For information on backing up RSA ACE/Server data, see Chapter 6, “Database Maintenance (Windows),” in the *RSA ACE/Server 6.0 Administrator’s Guide*.

**To uninstall the RSA ACE/Server:**

1. Shut down all RSA ACE/Server processes on the Server by opening the Control Panel on the Primary Server, and double-clicking the RSA ACE/Server icon.

   The RSA ACE/Server dialog box opens.
2. In the RSA ACE/Server dialog box, under **RSA ACE/Broker**, click **Stop**.
3. When the **Broker service stopped** message appears, click **OK**.

   If the Broker Connections dialog box opens, make sure that no administration sessions are connected to the database. Notify any remote administrators of the impending shutdown, and click **Yes**.
4. Click **Start > Settings > Control Panel > Add/Remove Programs**.

   The Add/Remove Programs Properties dialog box opens.
5. In the list of currently installed programs, select **RSA ACE/Server**, and click **Change/Remove**.

   The RSA ACE/Server Maintenance dialog box opens.
6. Select **Uninstall**, and click **Next**.
7. Follow the prompts until the uninstall is complete, and click **OK.**

The RSA ACE/Server software has been uninstalled from your computer.

# 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**).

**Administration Toolkit**

A toolkit for creating custom administration applications in C or Tcl. The Administration Toolkit, also called the API Toolkit, consists of functions and executables that can be read from or write to the RSA ACE/Server databases.

**Agent Host**

A computer or another device that is running RSA ACE/Agent software and is protected by the RSA ACE/Server to prevent unauthorized access. Agent Hosts include devices running RSA ACE/Agent software, as well as third-party devices that integrate RSA ACE/Agent software (for example, communication servers, firewalls, and routers).

**Configuration Management Application**

The application used on the Primary or a Replica Server to display and edit information in the system configuration record file (**sdconf.rec**). This application also displays license information.

**Database Administration Application**

The application used to administer the RSA ACE/Server database.

**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 type and the number of users in the license.

**Primary Server**

The RSA ACE/Server on which administration can be performed. The Primary also 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 the Primary's 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.

**Replica Server**

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

**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/Server Services**

The Control Panel application labeled "RSA ACE/Server" that starts and stops the Authentication Service and the Replication Service. This application can also be used to stop the database brokers.

**sdconf.rec**

The configuration file created by the installation program.

**sdlog Database**

The database that stores records for each authentication attempt and for actions taken through the RSA ACE/Server Database Administration application. It is also called the log database.

**sdserv Database**

The database that contains information such as system parameters, token and user records, and Agent Host information. It is also called the Server database.

**%SystemRoot%**

The root directory of the Windows operating system, for example, **\winnt**.

**Token**

Usually refers to a physical device, such as an RSA SecurID standard card, key fob, or PINPad, that displays a tokencode. User passwords, RSA SecurID smart cards, and software tokens are token types with individual characteristics. The token is one of the factors in the RSA SecurID authentication system. The other factor is the user's PIN.

# Index

## L



## M



## O



## P



## Q



## R

## S



## T



## U



## W