# RSA ACE/Server 5.2
# Deployment Guide

### Contact Information

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


**RSA Security Inc.**
**www.rsasecurity.com**

**RSA Security Ireland Limited**
**www.rsasecurity.ie**


### Trademarks



### License agreement



### Note on encryption technologies

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

### Distribution

Limit distribution of this document to trusted personnel.

### RSA Security Notice





First printing: October 2003

# Contents

# 1 Introduction

This deployment guide is intended for customers who have purchased the RSA ACE/Server and RSA SecurID user authentication security solution. It provides guidelines for planning the deployment of RSA SecurID authentication devices and the ongoing administration of the RSA ACE/Server system. The recommendations are based on general customer requirements and capabilities.

For deployment consulting, contact your sales representative to discuss options provided by RSA Security Professional Services. For information on planning the setup and use of RSA ACE/Server 5.2 in your organization's network infrastructure, see the *RSA ACE/Server 5.2 Scalability and Performance Guide.*

Each subject covered in this guide includes a list of items to consider and a discussion of these items. Although recommendations are made towards a course of action, you should base final decisions on your specific requirements and capabilities. Successful deployment will depend on many variables, including available resources, existing processes, and infrastructure.

**Note:** Discussion and recommendations about security policies are beyond the scope of this publication.

# 2 Deployment Planning

## Planning Data Collection and Population

The RSA ACE/Server database stores information about each user who will be authenticating onto your system or network. Determining what information you need to store and where you will get that information is an important component of token deployment.

### Things to Consider

- What information do you need to know about your users?
- Does the user information already exist in another one of your company's data repositories, such as LDAP?
- Will you use groups?
- Will you use RSA RADIUS?

### Discussion

#### Adding User Information

The RSA ACE/Server database requires information about each user before you can assign tokens to them. The standard fields, some of which are optional, for the RSA ACE/Server database include

- User's first and last name
- Default login
- Default shell (when on a UNIX Agent Host other than AIX)
- If the user is a local user, the serial numbers of the user's assigned tokens
- Administration authority level
- Whether or not the user can make up his or her own PINs
- Start and end dates of the period during which the user can be authenticated
- If the user is directly activated on one or more Agent Hosts, the times when the user can be authenticated on each Agent Host

For additional information regarding the contents of a user record, see the *RSA ACE/Server 5.2 Administrator's Guide*.

### Using LDAP

By running LDAP synchronization jobs, you can import users from an LDAP directory to the RSA ACE/Server database. Supported LDAP directories include

- Microsoft Active Directory
- Sun ONE Directory Server
- Novell NDS eDirectory

When a synchronization job runs, the RSA ACE/Server connects with a specified directory and examines the contents of that directory. Synchronization jobs can be configured to

- Delete users that are no longer in LDAP
- Enable or disable users that are enabled or disabled in LDAP
- Assign LDAP users to an existing group
- Create RSA ACE/Server groups based on existing LDAP groups

You can schedule times at which synchronization jobs run and use the synchronization interface to delete jobs that are no longer needed, edit existing jobs, or copy information from an existing job and use it to configure a new job. You can also run any job on demand.

For complete information on LDAP, refer to the *RSA ACE/Server 5.2 Administrator's Guide.*

### Using Groups

The RSA ACE/Server allows for creation of groups and sites. Groups, which can include users related by geography, job level, job duration, and so on, organize users into a single, manageable entity. You can then organize groups into sites.

Groups and sites offer an easy way of administering a large number of users, especially when providing access to specific Agent Hosts. Some of the advantages of groups include

- Automatic activation of a user on all relevant Agent Hosts
- Single-step removal of access privileges for multiple users
- Single-step activation of users on a new Agent Host
- Easier management and reporting

If you can use groups and sites, you will need to plot out a strategy for their creation and their activation on Agent Hosts, described in the chapter "Registering Users for Authentication" in the *RSA ACE/Server 5.2 Administrator's Guide.*

### Using RADIUS

If your RSA ACE/Server is installed in a system that was originally set up for RADIUS authentication or you have merged a large number of RADIUS users into your realm database, you can import RADIUS user and client data directly, rather than create new records manually.

The RSA ACE/Server RADIUS feature allows you to

- Import user profiles.
- Import the client on which the users are activated. An Agent Host record is created for the client.
- Import the user profiles and activate the users on a client that has already been imported. The user data file you specify is loaded into the database and the users are activated on the RADIUS client, now an Agent Host.

User and Agent Host records created through these utilities are unlikely to be complete. Therefore, you will need to edit them to add information such as group and token assignments.

In addition, you need to create and assign profiles. The RADIUS server supports the RADIUS protocol through profiles, each of which contains a set of connection parameters (in the form of "attribute-value pairs" — that is, the name of each parameter paired with its value) that RADIUS users need to access the network protected by RSA SecurID.

**Note:** Depending on the network access server (NAS) device you are using, a user who requests access through a RADIUS server may or may not need a profile in the Server database.

To save time and work, you can define a default profile for all users. The default profile is the administrator-defined profile that the system assigns automatically to any user who has otherwise not been assigned a profile.

For details regarding the RSA RADIUS, see the *RSA ACE/Server 5.2 Administrator's Guide.*

## Planning Token Deployment

Before you can begin deploying tokens to users, you should determine which deployment method best suits your needs.

### Things to Consider

- How will you staff the rollout effort?
- In what way will you configure authenticator PINs?
- Will you test your process?
- Will you be deploying hardware tokens, software tokens, or both?

## Discussion

### Staffing the Rollout Effort

To determine how large a staff you will need for the initial rollout effort, consider the number of users to whom you must deploy tokens within your projected time frame. If your users are located at different geographic areas, you may need to set up different deployment stations or have one deployment team travel around to different locations.

In addition, you should carefully consider who you assign to the rollout effort. A dedicated team is essential, even if your longer-term plan is to have a centralized help desk or support group provide ongoing administration and troubleshooting. Dedicated team members will have focus and synergy for this type of effort.

Administrator training is available from the RSA Security Educational Services Group.

### Configuring Authenticator PINs

Authenticator PINs can have several configuration options on a per Server basis. You need to consider the options for PIN assignment, PIN length, and PIN type.

**PIN assignment.** You can specify one of the following PIN assignment modes:

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

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

However, user-designated PINs have advantages also. If a user's RSA SecurID token is registered on another RSA Security access control product used by your organization (for example, an ACM/1600), the user can elect to use the same PIN on that system. A user who has more than one token might want to use the same PIN for both.

**PIN Length.** Options include a fixed length or a range of lengths. Currently, the range for both options is four to eight digits. RSA Security recommends PINs with at least six characters. Longer PINs provide greater security, but users find shorter PINs more convenient. Six characters provide a good balance between security and convenience.

**Alphanumeric or numeric PINs (for standard cards and key fobs only).** RSA Security recommends the use of alphanumeric PINs with RSA SecurID standard cards and key fobs. PINs that include both digits and letters provide greater security because they are more difficult to guess. A potential disadvantage of using alphanumeric PINs is that long, system-generated alphanumeric PINs are usually difficult to memorize. A user who receives a PIN like **kh8n4wo** is likely to write it down, thereby compromising security.

**Tokens that do not require PINS.** RSA ACE/Server also supports authentication with tokens that do not require a PIN. To authenticate, instead of entering the PIN followed by the tokencode, the user enters just the tokencode currently displayed on his or her token. Authenticating with just a tokencode is ideal for tokens on smart cards that users have to unlock with a PIN, or for tokens on a desktop that users have to unlock with a password. In these situations, the resource is protected by two-factor authentication without the user having to enter two different PINs.

### Testing Your Process

RSA Security recommends that you test your deployment process by using a pilot group of users. Feedback from pilot users can eventually save you significant time and expense in the rollout process. Try to include IT staff, specifically those who will support end users, in the pilot group.

### Determining the Token Type

If you will be deploying hardware tokens, see "Planning Hardware Token Deployment" on page 11. If you will be deploying software tokens, see "Planning RSA SecurID Software Token Deployment" on page 13.

## Planning Hardware Token Deployment

### Things to Consider

- How will you prepare hardware tokens for delivery?
- Which method will you use to distribute hardware tokens?

### Discussion

#### Preparing Hardware Tokens for Delivery

Hardware tokens can be initially enabled or disabled. Those that are initially disabled cannot be used until they are enabled.

#### Distributing Hardware Tokens

The two methods of deploying hardware tokens are

- **Method 1: Traditional Hardware Token Deployment.** This option requires dedicated personnel to assign the hardware tokens to the users in the RSA ACE/Server database and ship the tokens to these users.
- **Method 2: RSA SecurID Web Express.** This option is a web-based application that automates hardware token deployment and supports distribution through traditional methods or through a fulfillment house.

### Method 1: Using Traditional Hardware Token Deployment

The two major alternatives for delivering hardware tokens are

- **Users pick up tokens at a central location:** This is the most secure and fastest alternative, although this may not be feasible for all users. To accommodate delivery, consider locating administrative personnel at each office site. Alternatively, have your administrative staff travel to different office locations at pre-announced times. The advantages of this distribution method are the assurance that the hardware tokens are delivered to the right users and that they work when users receive them.
- **Users receive tokens in the mail*:*** Mailing hardware tokens through interoffice mail, post, or overnight express, for example, may be more feasible for your organization. However, this usually involves more up-front work to ensure success. You will need to develop a process for generating mailing labels, mailing the hardware tokens, and verifying that users receive their tokens. The most secure recommendation is to set tokens to disabled. Any information about enabling tokens should be sent separately from the actual tokens or made accessible only from a secure location. You will also want to group users so that mailing can be accomplished in a controlled manner.

Ultimately, you may need to use a combination of these delivery methods.

### Method 2: Using RSA SecurID Web Express

RSA SecurID Web Express is a web-based workflow application that automates many of the tasks that administrators must do before and during token deployment. These tasks include

- Identifying end users
- Approving or rejecting token requests, and informing users
- Populating the RSA ACE/Server database with user records
- Associating token serial numbers with end users

In addition, Web Express decreases the workload of administrators by enabling users to perform some administrative tasks themselves. In Web Express, users can

- Request and activate their own tokens
- Replace expiring hardware tokens
- Perform a test authentication for either RSA SecurID tokens or Q & A Authentication

Users can also manage their accounts, which includes setting up Q & A Authentication and changing their PINs.

RSA SecurID tokens can be distributed to end users in a number of ways, such as mailing them or having users pick them up in person. Web Express offers a list of fulfillment houses that your organization can use to have hardware tokens delivered to end users.

For more information about RSA SecurID Web Express, contact your local RSA Security sales representative, or visit the RSA Security web site at **www.rsasecurity.com**.

# Planning RSA SecurID Software Token Deployment

An RSA SecurID software token (formerly called SoftID) is a software-based security token that resides on a user's computer, an RSA SecurID Smart Card, or other devices such as Palm Pilots, Pocket PCs, and cell phones.

## Things to Consider

- What file-naming convention should you use?
- Should you enable copy protection?
- Should you bind the software token to a specific device?
- Will you use passwords to protect Software Token 3.0 files?
- What method will you use to issue software tokens?

## Discussion

### Naming Software Token Files

Although RSA Security delivers software tokens as **.asc** (2.0) and **.xml** (3.0) files, the RSA ACE/Server issues all software tokens as .**sdtid** files. Therefore, to differentiate between 2.0 and 3.0 software tokens, you may want to integrate the version number into the name of the software token files. For example, you might name a Software Token 2.0 file **stoken_2.sdtid** and a Software Token 3.0 file **stoken_3.sdtid**.

### Enabling Copy Protection

The Enable Copy Protection option ensures that the software token cannot be copied or moved from the directory in which it is installed on a user's computer or other device. By default, the option is enabled. RSA Security strongly recommends that you use copy protection.

### Binding a Software Token to a Device

RSA Security ships software tokens with a pre-defined extension field named **DeviceSerialNumber**, which you can use to bind the issued token to a specific device. A token that is bound to a specific device cannot be installed on any other device.

When you issue the token, you include in the token file the serial number of the device. If the serial number in the token file does not match the serial number of the device, the token cannot be installed.

### Using Passwords to Protect Software Token 3.0 Files

RSA Security strongly recommends that you take advantage of the ability to use passwords to protect Software Token 3.0 files.

You may select from the following password generation methods:

- If you select **Static Password** (the default), you enter a single password of your choice that applies to all software tokens that you issue.
- If you select **Combination**, the user's default login is appended to the password you enter.
- If you select **Default Login**, the user's default login is used as the password.

### Selecting a Method for Issuing Software Tokens

You may select from the following methods for issuing software tokens:

- If you select **Multiple Tokens per File**, up to 1000 token records are written to a file in the directory specified in the Target Folder box. When over 1000 token records have been written, a subsequent file is created. The name of the file will be the serial number of the first token in the file, followed by the letters MULTI. To issue multiple tokens per file with password protection, you must use a Static Password.
- If you select **One Token per File**, one software token record is written to a file in the directory specified in the Target Folder box. The name of the file is the user's default login.

For additional information regarding software tokens, see the *RSA SecurID Software Token Administrator's Guide*, the *RSA ACE/Server 5.2 Administrator's Guide*, and the RSA ACE/Server 5.2 Help.

## Planning Communication with End Users

Informing your end users about the new processes associated with the RSA ACE/Server is an essential component of successful deployment.

### Things to Consider

- When and how will you inform end users about the impending rollout?
- How will you communicate authentication instructions to end users?
- Where will you post documentation?

## Discussion

### Deciding When and How to Inform End Users About the Impending Rollout

Give users advance notice of the impending change. By doing so, you give them a chance to ask questions and clear up any confusion before you implement the new procedures.

You may want to inform users through one of the following methods:

- e-Mail
- Company/IT/MIS newsletter
- Intranet

### Communicating Authentication Instructions to End Users

RSA Security recommends that you provide some printed documentation with each token. If you are mailing hardware tokens, you could include a small card with instructions to locate a more detailed procedure or a telephone number to call to enable the device. If you are handing hardware tokens directly to users, give them complete procedures as part of the package. A good understanding of your user base, including their work habits and technical levels, helps in this effort.

Consider the following options:

- **Using Documentation Provided by RSA Security:** RSA Security provides sample instructions for users that can be customized to reflect your company's procedures or distributed out of the box. These samples are provided as Microsoft Word (**.doc**) and Adobe Acrobat (**.pdf**) files on the RSA ACE/Server CD.
- **Writing Your Own Documentation*:*** If you choose to write your own documentation, be sure to document procedures for performing certain functions, including enabling the token, setting an initial PIN, resetting a PIN, and acquiring help with authentication problems. You may want to include screenshots of different processes, though text-only versions are more compact and therefore download quicker.
- **Using the RSA SecurID Tour**: RSA Security has developed an online Macromedia Flash tour that can be accessed on the RSA ACE/Server CD or downloaded from RSA SecurCare Online. The tour explains the concept of two-factor authentication, the different types of RSA SecurID authenticators, and the procedures associated with two-factor authentication.

### Deciding Where to Post the Documentation

Documentation should be kept in a central but secure location. When documentation is secure, even if a token is stolen, the unauthorized user is denied access to important information necessary to use the token. Your company's intranet or groupware software are good places in which to keep the documentation.

# Planning for Ongoing Administration

Ongoing administration is a topic that warrants consideration during the deployment process. Many of the activities that take place during the initial rollout will continue during the lifetime of the RSA ACE/Server product. If you expect to hand off ongoing administration to a centralized help desk or technical support group, you will need to make sure they have the tools to do their jobs properly. Get input from these groups when designing the administration process.

## Things to Consider

- What different levels of RSA ACE/Server administration will you need?
- In what way will you define administrative roles?
- Will you use remote or web-based administration?
- If you are passing control to a central administration group or help desk, when will you involve this group?
- What frequency and method will you adopt to update the user information in the RSA ACE/Server?

## Discussion

### Determining the Different Levels of Administration

Administration of the RSA ACE/Server involves at least the following actions:

- Adding new users
- Deleting terminated users
- Changing user information
- Replacing expired/defective/destroyed tokens
- Planning for emergency access
- Activating users on different Agent Hosts
- Producing reports, both for database updates and for management reporting

Depending on the size of your company and how often you will need to update the RSA ACE/Server database, you may want to set up a centralized administration area or help desk. Administration and help desk sites require many levels of administration. For example, many Tier 1 help desk administrators require access to just user and token records rather than full administration access, while Tier 2 administrators require additional access.

### Defining Administrative Roles

An administrative role is a template comprising a set of tasks an administrator can perform on a specific realm, site, or group. By assigning administrative roles, you can limit the power of administrators to specific kinds of actions and specific segments of the RSA ACE/Server database. Once you define an administrative role, you can assign it to any number of administrators.

The two components of an administrative role are

- **Administrative Scope**: Specifies which sites, Agent Hosts, groups, users, and tokens the administrative role can affect.
- **Administrative Task List**: Named set of tasks that administrators to whom the role is assigned can perform, albeit within the scope that is also defined as part of the role.

For details regarding administrative roles, see the *RSA ACE/Server 5.2 Administrator's Guide.*

### Using Remote and Web-Based Administration

To accommodate your administrative needs, RSA ACE/Server provides the following options:

- **Remote Administration**. The RSA ACE/Server Remote Administration application enables complete administration of RSA ACE/Server from any Windows-based machine that is on the same network as the RSA ACE/Server. For additional information, see the *RSA ACE/Server 5.2 Administrator's Guide.*
- **Web-based Administration**. RSA ACE/Server Quick Admin is a web-based application that is ideal for help desks. This application allows the administrator to perform the most common user and token administrative tasks, such as deleting a user, resetting a PIN, or placing a token in lost status, through a web browser. This application is ideal for the many large organizations that outsource Tier 1 token help-desk operations to a third party. For additional information, see the *RSA ACE/Server 5.2 Administrator's Guide*.

### Determining When to Involve a Central Administration Group or Help Desk

RSA Security recommends involving administration and help desk personnel early in the planning process so that they thoroughly understand the product and can provide valuable input. In addition, you will need to arrange for adequate training of administrative personnel. Training is available from the RSA Security Educational Services Group.

### Updating the Database

You have already determined what user information to include in the RSA ACE/Server database and where you will obtain this information. Now you must decide how you will update the RSA ACE/Server database. You will want to account for new employees, terminated employees, and changes that occur as part of your business.

The two methods of updating the RSA ACE/Server database are

- Automatic Entry
- Manual Entry

**Automatic Entry:** RSA Security recommends that you use automatic entry to avoid errors that can occur with manual data entry. Entering information into the database in real time — or as close as possible — improves security and reduces administrative exception handling. Types of automatic entry include:

- **Directly from another database**

  This approach will require some additional programming to directly access the source database.

- **From another database through a flat, or comma-delimited, file**

  As discussed in "Using LDAP" on page 8, you may use the LDAP utility provided with the RSA ACE/Server. In addition, RSA Professional Services offers the RSA ACE Bulk Administrator utility to load the required fields from a flat file with a specific comma-delimited format. Or, using function calls from the RSA ACE/Server Administration Toolkit, you can program your own utility for bulk loading of user information and automatic assignment of authenticators to your users. You would likely create this flat file from other in-house systems.

- **Web registration**

  With RSA SecurID Web Express, users can register online. After registering, Web Express automates the workflow process for approval of the request. When approved, the user is added to the RSA ACE/Server database, and a request is forwarded to a Distributor, who sends the token to the end user. For more information, see "Method 2: Using RSA SecurID Web Express" on page 12.

**Manual Entry**: You may decide to manually enter user information through the Add User dialog box. This option is the most labor-intensive and time-consuming and must be done very carefully to avoid errors in the data.

## Conclusion

The key to successful deployment is planning. Carefully consider the issues raised in this document, and define others that are specific to your particular business needs. By doing so, you can successfully implement the strong two-factor authentication critical for protecting your organization's valuable information assets.