RSA Authentication Manager 6.1
Deployment Guide

RSA

SECURITY™

Contact Information

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

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

Trademarks

License agreement

Note on encryption technologies

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

Distribution

Limit distribution of this document to trusted personnel.

RSA notice

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

First printing: September 2005

Contents

Preface 5
Audience 5
Documentation 5
Getting Support and Service 6

Chapter 1: Introduction 7

Chapter 2: Deployment Planning 9
Planning Data Collection and Population 9
Planning Token Deployment 12
Planning Hardware Token Deployment 14
Planning RSA SecurID Software Token Deployment 16
Planning Communication with End Users 17
Planning for Ongoing Administration 19
Conclusion 22

Appendix A: Preparing Users for First-Time Token Use 23

Preface

This book provides information for deploying the tokens that you distribute to your users as part of your RSA Authentication Manager implementation. For information about deploying RSA Authentication Manager and the RSA Authentication Agents, see the *RSA SecurID for Microsoft Windows Planning Guide*.

Audience

This book is intended for system administrators and other trusted personnel only. The person who installs RSA Authentication Manager must be familiar with your server platform, operating system version, and system peripherals.

Do not make this book available to your general user population.

Documentation

The RSA Authentication Manager 6.1 software is provided on a single CD, which also includes:

- A Windows-based Help system.
- Printable documentation files in PDF format.

Documentation Provided in PDF Files

You can access PDF files from either:

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

Note: RSA Security provides an authentication instructions template in a Microsoft Word (.doc) file that you can customize and provide to your users.

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

RSA Security recommends that you obtain the latest version of Adobe Acrobat Reader for your platform at **www.adobe.com**.

RSA Authentication Manager 6.1 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

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 Authentication Manager 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 Authentication Manager 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 Introduction

This deployment guide is intended for customers who have purchased the RSA Authentication Manager and RSA SecurID user authentication security solution. It provides guidelines for planning the deployment of RSA SecurID authentication devices and their ongoing administration in the RSA Authentication Manager 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 Authentication Manager 6.1 in your organization's network infrastructure, see the *RSA Authentication Manager 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, base your final decisions on the specific requirements and capabilities of your environment. Successful deployment depends on many variables, including available resources, existing processes, and infrastructure.

Note: Discussion and recommendations about security policies are not covered in this document.

2 Deployment Planning

Planning Data Collection and Population

The RSA Authentication Manager database stores information about each RSA SecurID user in your system or network. Determining what information you need to store and where to 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 data repository, such as LDAP?
- Will you use groups?
- Will you use RSA RADIUS?
- Will you require offline users to authenticate with RSA SecurID?
- Will you enable the Windows password integration feature for RSA SecurID users?
- Will you provide emergency codes for offline user access?

Discussion

Adding User Information

The RSA Authentication Manager database requires information about each user before you can assign tokens. The standard information fields, some of which are optional, include:

- User’s first and last name
- Default login
- Default shell
- If the user is within the local realm, the serial numbers of the user’s assigned tokens
- Administration authority level
- Whether users can define their 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 more information about registering Agent Hosts in the RSA Authentication Manager database, see the *RSA Authentication Agent 6.1 for Windows Installation and Administration Guide*.

For additional information regarding the contents of a user record, see the *RSA Authentication Manager 6.1 Administrator's Guide*.

Using LDAP

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

- Microsoft Active Directory
- Sun Java System Directory Server
- Novell NDS eDirectory

When a synchronization job runs, the RSA Authentication Manager connects with a specified directory and examines the contents of that directory. You can configure synchronization jobs 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 Authentication Manager 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 Authentication Manager 6.1 Administrator's Guide.*

Using Groups

The RSA Authentication Manager allows you to create groups and sites. Using groups helps you to organize users into a single, manageable entity. For example, a group may contain users related by geography, job level, or job duration.

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 are:

- 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 need to plot a strategy for creating and activating them on Agent Hosts. For information, see the chapter "Registering Users for Authentication" in the *RSA Authentication Manager 6.1 Administrator's Guide.*

Planning for RADIUS

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

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

As you plan your RADIUS environment, consider how you want to track RADIUS authentications in the RSA Authentication Manager database log. If you want the log to include the name of a RADIUS client on which an authentication occurs, you need to add the client as an Agent Host in the RSA Authentication Manager database. RSA Security recommends this method of logging to enhance security.

Note: If you do not use this method of logging, you must change the `CheckUserAllowedByClient` default setting in the **securid.ini** file on the RSA RADIUS server. For more information, see the *RSA RADIUS Server 6.1 Reference Guide*.

To control access, you can add RADIUS users to groups and activate the groups on the Agent Hosts of your RADIUS clients. For more information about adding and activating groups, see the RSA Authentication Manager Help.

Using RADIUS

You perform most of the administration of the RSA RADIUS Server 6.1 through its own administration application, which you can launch from the RSA Authentication Manager Database Administration application by clicking **RADIUS > Manage RADIUS Server**. You assign profiles to users and groups through the RSA Authentication Manager.

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

For more information about profiles, see the RSA Authentication Manager Help.

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

Requiring Offline Users to Authenticate with RSA SecurID

You may decide to implement offline authentication, which will prompt your users to authenticate to their computers when disconnected from the network. For more information, see the *RSA SecurID for Microsoft Windows Planning Guide*.

Providing Windows Password Integration

You can provide login password integration, so that users who have previously authenticated with Microsoft passwords can continue to authenticate in the Windows environment using their RSA SecurID passcode. For more information, see the *RSA Authentication Manager 6.1 Administrator's Guide*.

Providing Emergency Codes for Offline User Access

In the event that you have enabled offline authentication and your users are locked out of their computer for any reason, you can provide them with an emergency code. For more information, see the *RSA SecurID for Microsoft Windows Planning Guide*.

Planning Token Deployment

Before you can begin deploying tokens to users, 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 deploy hardware tokens, software tokens, or both?
- Will you deploy the RSA SecurID Authenticator SID800 and the RSA Authenticator Utility 1.0?
- If you are planning to provide support for offline authentication, what types of tokens will support this feature?

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, 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 have focus and synergy for this type of effort.

You can get administrator training from the RSA Security Educational Services Group.

Configuring Authenticator PINs

Authenticator PINs can have several configuration options on a per Authentication Manager 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 create their own PINs.
- Designated users are permitted to create 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. Using system-generated PINs can also prevent against compromises in security that sometimes result from allowing users to re-use their self-generated PINs when their token is put into New PIN mode.

However, user-designated PINs have advantages also. If a user's RSA SecurID token is registered on more than one RSA Security access control product (for example, an ACM/1600), the user can create a specific PIN for each product that might make it easier to remember the PINs.

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.

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. However, it is important to provide your users with the rules they must follow to help keep your system secure. For example, a user who receives a PIN like **kh8n4wo** might be inclined to write it down, since a system-generated password is more difficult to remember than a user-defined password. You must educate your users about security compromises that can result from keeping a written record of password data.

Tokens that do not require PINs. RSA Authentication Manager also supports authentication with tokens that do not require PINs. To authenticate, instead of entering the PIN followed by the tokencode, users enter just the tokencode currently displayed on their 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 14. If you will be deploying software tokens, see "Planning RSA SecurID Software Token Deployment" on page 16.

If you plan to deploy the RSA SecurID Authenticator SID800 and the RSA Authenticator Utility 1.0, see the RSA Authenticator Utility 1.0 documentation for detailed information.

Choosing Token Types that Support Offline Authentication

If you decide to enable offline authentication for your users, you must specify the types of tokens that support this feature. By default, passcode tokens support this feature only. You can allow offline authentication with other types of tokens, but the security of your system might be compromised. For more information, see the *RSA Authentication Manager 6.1 Administrator's Guide*.

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 Authentication Manager 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.

Each of these methods is described in detail below.

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 Authentication Manager 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 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 Authentication Manager 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**. You can use this field 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 use passwords to protect Software Token 3.0 files.

You may select from the following password generation methods:

- **Static Password**—Enter a single password of your choice that applies to all software tokens that you issue.
- **Combination**—The user's default login is appended to the password you enter.
- **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:

- **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.
- **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, see the *RSA Authentication Manager 6.1 Administrator's Guide* and the RSA Authentication Manager 6.1 Help.

Planning Communication with End Users

Informing your end users about the new processes associated with the RSA Authentication Manager is essential for a successful deployment.

Things to Consider

- When and how will you inform end users about the planned 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 Planned Rollout

Give users advance notice of the scheduled changeover. 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 documentation with each token. If you plan on mailing hardware tokens to your users, consider including a small card with instructions for locating a more detailed procedure or a telephone number to call to enable the device. If you plan to distribute hardware tokens directly to users, consider giving them complete procedures as part of the package. A good understanding of your user base, including your users' work habits and technical levels, helps in this effort.

Consider the following options:

- **Using Documentation Provided by RSA Security:** RSA Security provides sample instructions that you customize to reflect your company's procedures.

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

- **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 provides an online Macromedia Flash tour that you can get from the RSA Authentication Manager CD or download 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

Keep the documentation 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 to store the documentation.

Planning for Ongoing Administration

Ongoing administration 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 Authentication Manager 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 Authentication Manager 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 Authentication Manager?
- Will you provide administrators with the ability to distribute Emergency Access Codes to users, in the event that an interruption in communication occurs between an Agent Host and the RSA Authentication Manager?

Discussion

Determining the Different Levels of Administration

Administration of the RSA Authentication Manager involves the following tasks:

- 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 Authentication Manager 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 comprised of 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 Authentication Manager 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, within the scope that is also defined as part of the role.

For details regarding administrative roles, see the *RSA Authentication Manager 6.1 Administrator's Guide.*

Using Remote and Web-Based Administration

To accommodate your administrative needs, RSA Authentication Manager provides the following options:

- **Remote Administration**. The RSA Authentication Manager Remote Administration application enables complete administration of RSA Authentication Manager from any Windows-based machine that is on the same network as the RSA Authentication Manager. For additional information, see the *RSA Authentication Manager 6.1 Administrator's Guide.*
- **Web-based Administration**. RSA Authentication Manager 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 Authentication Manager 6.1 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 Authentication Manager database and where you will obtain this information. Now you must decide how you will update the RSA Authentication Manager database. You must account for new employees, terminated employees, and changes that occur as part of your business.

The two methods of updating the RSA Authentication Manager 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. Using automatic entry improves security and reduces administrative exception handling. Types of automatic entry include:

- **Directly from another database**

  This approach requires 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 10, you may use the LDAP utility provided with the RSA Authentication Manager. In addition, RSA Professional Services offers the RSA Authentication Manager 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 Authentication Manager 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 Authentication Manager 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 15.

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.

Providing Reserve Access for Administrators

Occasionally, the connection between an administrator's computer and the RSA Authentication Manager may be interrupted, preventing administrators from accessing their computers. For such cases, you can choose reserve access methods for administrators.

For more information about reserve access methods, see the *RSA SecurID for Microsoft Windows Planning Guide*.

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.

A Preparing Users for First-Time Token Use

The following is a sample memo that you can distribute when you issue RSA SecurID tokens to your employees. You can modify the memo as needed to suit your particular deployment scenario.

TO:	All Employees
FROM:	IT Department
DATE:	October 1, 2004
SUBJECT:	New Log On Procedures

The IT Department has issued you an RSA SecurID token. Beginning today, you must use this token to log on to your local desktop and to the network.

When you attempt to log on today, you will notice that your logon screen has changed. Instead of your password, you are prompted for your RSA SecurID passcode. A passcode is a personal identification number (PIN) followed by the tokencode displayed on your token.

The first time you use your token you must create a PIN and store your password. Follow the steps below to log on for the first time.

1. Press **CTRL+ALT+DELETE** to start the logon process.
2. Enter your user name as you typically do.
3. In the Passcode field, enter your tokencode (the number currently displayed on the screen of your token) and click **OK**.
4. Follow the on-screen instructions to create your PIN. Choose a PIN that you can easily remember. Do not write it down.
5. After you create your PIN, log on to your computer a second time, using your passcode. To enter your passcode, type your newly-created PIN followed by the *next* tokencode that is displayed on your token.

   Note: If the tokencode you entered in step 3 is still displayed on your token, do not enter it. Wait for the tokencode to change before entering it or else you will be denied access.

Note: If you have enabled Windows password integration, add step 6 as well.

6. Enter your Windows password so that RSA SecurID can store it for you.

Proper use of your token involves following a few simple rules:

- **Do not forget your PIN.** Choose a PIN that you can easily remember. Do not write it down.
- **Enter your passcode carefully.** You are allowed to enter your passcode only a limited number of times before you are locked out of your computer.
- **Keep your token with you at all times.** By carrying your token on a key chain or wearing it as a necklace, you will reduce your chances of forgetting or losing it.

If you get locked out of your computer, you must contact your administrator, who can provide you with an emergency code to access your computer.

If you lose your token, contact your administrator immediately.