RSA ACE/Agent 5.5 for Windows Installation and Administration 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: December 2002

Contents

Preface

This book explains how to install and administer RSA ACE/Agent 5.5 for Windows. RSA ACE/Agent 5.5 for Windows enhances native Windows 2000 and Windows XP security by integrating strong, two-factor authentication.

Audience

This book is intended for network and security administrators, systems integrators, and information technology managers. It is intended only for advanced security administrators and other trusted personnel. Do not make this guide available to the general user population.

Documentation and Product Support

For documentation and product support information, as well as last-minute technical information that could not be included in the documentation, see the *RSA ACE/Agent 5.5 for Windows Readme*. This file is named **readme.pdf** and is located in the **Aceclnt\nt_i386** directory of the RSA ACE/Agent 5.5 for Windows zip file.

1 Overview

Protecting Windows Resources

An Agent Host runs the RSA ACE/Agent 5.5 for Windows software and connects over a TCP/IP network to a computer running the RSA ACE/Server software. The RSA ACE/Server software provides Agent Hosts with authentication services. The RSA ACE/Agent 5.5 for Windows, when used with the RSA ACE/Server authentication management software and time-based RSA SecurID tokens, provides two-factor authentication to protect Windows computers and services.

The RSA ACE/Agent 5.5 for Windows software sets RSA SecurID protection for the following resources:

- Remote login to the machine through the Remote Access Service (RAS). This feature set is called **Remote Access Authentication**.
- Local login to the desktop. This feature set is called **Local Access Authentication**.

Note: The RSA ACE/Agent 5.5 for Windows does NOT install or support Web Access authentication for Internet Information Server (IIS), or Network Access authentication to Windows domain controllers or Windows 2000 Active Directory servers.

For more information, see the following section, "Local Access and Remote Access Authentication Overview."

Local Access and Remote Access Authentication Overview

The Local access authentication component of RSA ACE/Agent 5.5 for Windows authenticates RSA SecurID users at the local login prompt. The Local access authentication feature also supports authentications to any machine running the Windows XP Remote Desktop service. In this environment, users can be RSA SecurID challenged when accessing a remote machine running the Desktop service.

The Remote access authentication component of RSA ACE/Agent 5.5 for Windows authenticates RSA SecurID users who access resources through Remote Access Service (RAS). After the user enters either Windows login information or dial-up account credentials at the dial-up terminal window, the user is prompted to enter a valid RSA SecurID PASSCODE.

ISDN Connections

RSA ACE/Agent 5.5 for Windows does not directly support ISDN connections. There are vendor-specific solutions, however, that might apply to your ISDN environment. These solutions are described in an RSA Security white paper entitled *ISDN Solutions for RSA ACE/Agent RAS Authentication*. You can download the paper from the RSA Security SecurCare Online Web site at **www.rsasecurity.com/support/securcare/index.html**.

EAP Authentications

The RSA ACE/Agent for Windows software can use EAP (the Extensible Authentication Protocol) to authenticate users dialing in from remote Windows computers.

EAP allows third-party authentication modules to interact with the Windows RRAS (Routing and Remote Access Service) Point to Point Protocol (PPP) implementation. EAP is an extension to PPP, providing a standard support mechanism for RSA SecurID authentication. Support of EAP enables you to use a number of additional communication mediums, including PPTP, ISDN, PPP, L2TP, and X.25.

To use EAP authentication, you must install the RSA Security EAP component on the remote client computers that are running Windows 2000 or Windows XP. For more information, see "Installing RSA Security EAP on Client Computers" on page 31.

EAP is supported **only** on Windows 2000 and Windows XP RRAS client machines. Windows 98 clients must use post-dial, terminal-based authentication.

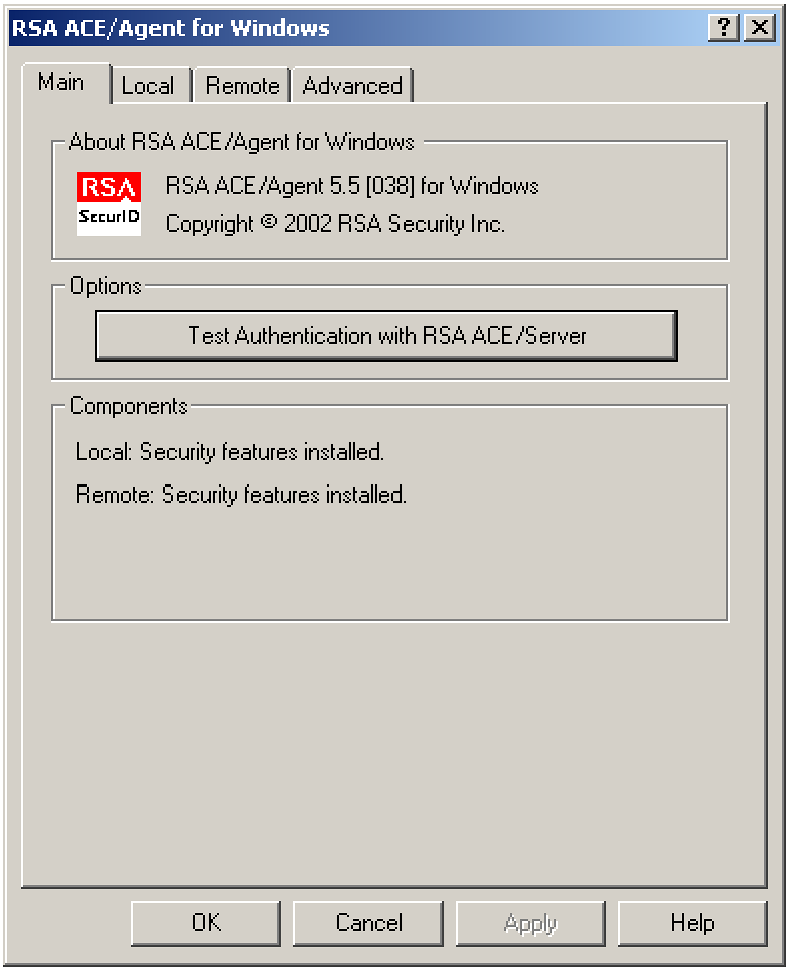
The RSA ACE/Agent Control Panel

The RSA ACE/Agent control panel contains all the tools you need to configure Local and Remote Access Authentication options, and Advanced Settings options. Click the labeled tabs in the RSA ACE/Agent control panel to view the properties sheet for each available feature set. When you modify any of the security settings, you need to re-start the Windows computer for the new settings to take effect.

To use the RSA ACE/Agent control panel:

1. Log in to the computer as an administrator.
2. Click **Start** > **Settings > Control Panel**.
3. Double-click the **RSA ACE/Agent** icon.
   The RSA ACE/Agent control panel opens.
4. Click the Main tab.

The Component Status dialog box displays the available feature sets.


RSA ACE/Agent for Windows
Main
Local
Remote
Advanced
About RSA ACE/Agent for Windows
Options
Test Authentication with RSA ACE/Server
Components
OK
Cancel
Apply
Help

RSA ACE/Agent 5.5 [038] for Windows

Copyright © 2002 RSA Security Inc.

Local: Security features installed.

Remote: Security features installed.

If you expect either the Local access or Remote access authentication features to be available but the corresponding tab is missing, make sure you have the correct services installed and enabled on the computer.

5. Click the appropriate tab to view settings for
   - Local access authentication
   - Remote access authentication
   - Advanced settings
6. Specify which users must be challenged. For more information, see "Selecting Which Users and Groups Will Be Challenged by RSA SecurID" on page 10.
7. Configure the other options for each feature set.
8. To test that RSA ACE/Agent authentication has been correctly implemented without restarting your Windows computer, see "Test Authentication Overview" on page 11.

Selecting Which Users and Groups Will Be Challenged by RSA SecurID

The RSA ACE/Agent software can use Windows 2000 or Windows XP groups to control access to a computer or to resources on the computer. These groups can be the default groups (for example, Domain Users or Dial-in Users), or groups that you create yourself using the Windows Computer Management interface.

For maximum security, the product can be configured to challenge all users who access resources that are protected by the RSA ACE/Agent software. If you want maximum local login security, open the Local properties sheet of the RSA ACE/Agent control panel and select **All users** from the **Challenge** list. If you want to challenge all users *except* local administrators, select **All users except** from the **Challenge** list, and then select the **Administrators** group.

Note: RSA Security recommends the use of a reserve password with local authentication. See "Using the Reserve Password" on page 24.

The following table explains how to enable the RSA ACE/Agent authentication using groups:

To challenge	Complete these steps
All users who log on locally	Open the Local properties sheet, and click **All users** from the **Challenge** list.
A group of users who log on locally	Open the Local properties sheet, click **Users in** from the **Challenge** list, and then select the local or domain group that you want to be RSA SecurID-challenged.
All users who log on locally, except users in a certain group	Open the Local properties sheet, click **All users except** from the **Challenge** list, and then select the local or domain group that you do not want to be RSA SecurID-challenged.
All users who dial in to the computer	Open the Remote properties sheet, and click **All users** from the **Challenge** list.
A group of users who dial in to the computer	Open the Remote properties sheet, click **Users in** from the **Challenge** list, and then select the local or domain group that you want to be RSA SecurID-challenged.
All users who dial in to the computer, except users in a certain group	Open the Remote properties sheet, click **All users except** from the **Challenge** list, and then select the local or domain group that you do not want to be RSA SecurID-challenged.

.

Test Authentication Overview

You can test that RSA ACE/Agent authentication has been correctly implemented before you deploy tokens to users. The test described in this section will help you to verify that the **sdconf.rec** file you installed on the Agent Host points to the appropriate RSA ACE/Server database, that the host has a valid node secret file, and that your system is configured properly for authentication.

Viewing RSA ACE/Server Information

Before performing a test authentication, make sure that the RSA ACE/Agent 5.5 for Windows has been properly registered as an Agent Host in the RSA ACE/Server database, and that a network connection between the Server and the Agent has been established. You can use the RSA SecurID Authentication Information window to view information about the Server that is processing authentication requests.

To view RSA ACE/Server authentication and status information

1. In the RSA ACE/Agent control panel, click the **Main** tab, then click **Test Authentication with RSA ACE/Server**.

   The RSA SecurID Authentication Information dialog box opens, and the following information is displayed:

   - **Configuration Version**: The version of the **sdconf.rec** file that is in use. For RSA ACE/Server 5.0 or later, this number is 12.
   - **DES Enabled**: If your configuration environment supports legacy protocols, “YES” is displayed.
   - **Client Retries**: The number of times the Agent sends authentication data to the Server before a time out occurs.
   - **Client Timeout**: The amount of time (in seconds) that the Agent waits before re-sending authentication data to the Server.
   - **Server Release**: The version number of the Server.
   - **Communication**: The version of protocol being used for communication between the Server and the Agent.

   If you have questions about any of the information that is displayed, consult your RSA ACE/Server administrator.

2. Click **RSA ACE/Server Status**.

   The Server Status window opens.

   The Select Server panel displays information about each RSA ACE/Server that is known to the Agent. If an alias IP address has been assigned to the Server you select, it is shown in the Server Alias Addresses panel.

   The Server information panel indicates the type of Server that you have selected from the list in the Select Server panel. The active IP address shown is the IP address that the Agent will use to communicate with the Server. This address could be the actual IP address of the Server you have selected, or it could also be an alias IP address assigned to the Server. A “00.000.00.00” indicates that the Agent has not yet received communication from the Server.

The Server Usage panel indicates any of the following conditions.

- Available for Authentications: the selected Server will be used for authentications.
- Unused: the selected Server will not be used for authentications.
- For Failover only: the selected Server has been reserved for failover use only.
- Default Server During initial requests: the selected server will be used, since no other server is available.

Testing Authentication

Testing will go more smoothly if you use a token with a PIN that is already registered in the RSA ACE/Server database. If you test authentication with a token in New PIN mode, however, you will go through the actual New PIN procedure, and the PIN will be registered in the RSA ACE/Server database. There are specific instructions for each token type that are provided in both Microsoft Word and PDF format (**auth.doc** and **auth.pdf**) in the **aceservdoc** directory on the RSA ACE/Server CD. Contact your RSA ACE/Server administrator to obtain a copy of the appropriate instructions for each of your token types, and be sure to read them before performing any authentication test. If you are using RSA SecurID Software Token 2.0, refer to the authentication instructions in the *RSA SecurID Software Token 2.0 User's Guide*. If the token you are testing has a PIN, you must know the PIN to continue testing.

Note: Because authentication is being tested, not confirmed, it is not necessary for the owner of the token to be a member of an RSA SecurID local group.

To test authentication on a token that has a PIN:

1. In the RSA ACE/Agent control panel, click the **Main** tab, then click **Test Authentication with RSA ACE/Server**.

   The RSA SecurID Authentication Information dialog box opens.

2. Click **RSA ACE/Server Status**.

   If you have questions about any of the information that is displayed, confer with your RSA ACE/Server administrator.

3. Click **RSA ACE/Server Test Directly**.

   The RSA SecurID Authentication dialog box opens.

4. On the **Choose Token** list, select **SecurID Card**.
5. In the Enter Username dialog box, enter the username of the registered RSA SecurID user who is assigned to the RSA SecurID token you are using.

6. In the Enter PASSCODE dialog box, enter the current PASSCODE that is generated by the RSA SecurID token.
   - If you have an RSA SecurID standard card or an RSA SecurID key fob, enter the PIN followed by the tokencode that is displayed on the token.
   - If you have an RSA SecurID PINPad, enter the PIN into the card, press the diamond (♦) near the bottom of the card, and then enter the PASSCODE that displays on the token.
7. Click **OK**.

   If everything is properly implemented and configured, the system displays a message that the user was authenticated successfully.

   If the system displays an Access denied message, repeat this procedure.

   If you repeat the process and are still denied access, follow the instructions for testing authentication using an RSA SecurID token that does not have a PIN. If the system displays an **ACE/Server not responding** message or you are still unable to authenticate, confer with your RSA ACE/Server administrator.

To test authentication on a token that does not have a PIN:

1. Click **Start** > **Run**.

   The Run dialog box opens.
2. Enter **sdtest** and then click **OK**.

   The RSA SecurID Authentication Information dialog box opens.
3. Click **RSA ACE/Server Test Directly**.

   The RSA SecurID Authentication dialog box opens.
4. On the **Choose Token** list, click **SecurID Card**.
5. In the **Enter Username** dialog box, enter the username of the registered RSA SecurID user who is assigned to the RSA SecurID token you are using to test authentication.
6. In the Enter PASSCODE dialog box, enter the current PASSCODE that is generated by your RSA SecurID token, then click **OK**.

   The New PIN dialog box opens.
7. In the New PIN dialog box, select the option to create your own PIN. Enter and confirm your new PIN in the provided fields, and click **OK**.

   The RSA SecurID Authentication dialog box opens.
8. In the Enter Username field, enter the username of the registered RSA SecurID user who is assigned to the RSA SecurID token you are using.

9. In the Enter PASSCODE field, enter the current PASSCODE that is generated by your RSA SecurID token:
   - If you have an RSA SecurID standard card or an RSA SecurID key fob, enter your PIN, immediately followed by the tokencode that currently displays on the token.
   - If you have an RSA SecurID PINPad, enter the PIN into the card, press the diamond (♦) near the bottom of the card, and then enter the PASSCODE that displays on the token.
10. Click **OK**.
    - If everything is properly implemented and configured, the system displays a message that the user must create or be assigned a new PIN.
    - If the system displays an **Access denied** message, repeat the process. If you see other messages, refer to the RSA ACE/Server documentation for more information. If you are still unable to authenticate, confer with your RSA ACE/Server administrator.

2 Installing RSA ACE/Agent 5.5 for Windows

The RSA ACE/Agent 5.5 for Windows is qualified to run on the following platforms and RSA Security software:

- Windows 2000 (Professional, Server)
- Windows XP (Professional)
- RSA ACE/Server 4.1 and later

The requirements needed to install and run RSA ACE/Agent 5.5 for Windows depend on which authentication component you intend to use (Local access or Remote access) and are in addition to the minimum requirements needed for the operating system.

Local Access Authentication Requirements

For RSA ACE/Agent Local access authentication features to be available on the RSA ACE/Agent Host, your system must meet the following minimum requirements:

- Windows 2000 (Server or Professional) with Service Pack 1, or Windows XP (Professional)
- 32 MB of RAM
- 5 MB of free disk space
- TCP/IP networking

Remote Access Authentication Requirements

For RSA ACE/Agent Remote access authentication features to be available on the RSA ACE/Agent Host, the RAS hosts to which users will dial in must be installed on a Windows 2000 Server, meeting the following requirements:

- 32 MB of RAM.
- 4 MB of free disk space.
- TCP/IP networking.
- Dial-in access enabled.
- Dial-in client stations must be running Windows 2000 (Server or Professional), Windows XP (Professional), or Windows 98.
- The Windows 2000 RAS Server should be physically inaccessible to all unauthorized persons. If it is not secure in this way, someone could unload the RSA ACE/Agent **.dll** files and eliminate RSA SecurID authentication.

- The device that handles incoming RAS connections (for example, your modem) must be connected to a port that the Windows 2000 RAS server recognizes as a true COM port (for example, COM1). Connecting the device through a virtual COM port or VPN port is not supported. In addition, the device must be able to accept input from a post-dial terminal (TTY) window. This is needed so that users (or a SoftID automated logon script) can respond to the **Username** and **PASSCODE** authentication prompts.

  Some multi-port modem cards and packet driver boards offer COM port emulation. RSA ACE/Agent 5.5 for Windows may work with such products in COM port emulation mode, but RSA Security does not warranty that such configurations will function properly.

Before you enable RSA SecurID authentication, you must understand the RSA ACE/Server system and its features. Some of these features include New PIN mode, client activation, and group memberships. If you have concerns or questions about these or any other RSA ACE/Server administration tasks, refer to the RSA ACE/Server documentation, or contact your RSA ACE/Server administrator.

If you intend to use the RSA ACE/Agent software to protect the files of multi-homed servers, you must account for the extra IP addresses in the RSA ACE/Server database. The RSA ACE/Server administrator has to define a secondary node for each additional IP address used on the Agent Host. In addition, you should specify an IP address override on the **Advanced** tab of the RSA ACE/Agent control panel; the override address should exactly match the network address specified for the Agent Host in the Server database. Ask your RSA ACE/Server administrator or consult the RSA ACE/Server documentation for instructions on how to define secondary nodes.

Setup Tasks for the RSA ACE/Server Administrator

You or your RSA ACE/Server administrator must complete the following tasks before you attempt to use the RSA ACE/Agent software:

- The RSA ACE/Server administrator has made the configuration file **sdconf.rec** available to you, and you have copied it to the ***%SYSTEMROOT%*****\system32** directory of the Agent Host.
- Verify that the RSA ACE/Server is available.
- The RSA ACE/Agent Host has been registered as an Agent of the RSA ACE/Server. See "Automated Registration of Agent Hosts in the RSA ACE/Server Database" on page 41.

  Note: You can provide an IP address override for the Agent if you install it on a multi-homed server. See "Setting an Overriding IP Address for an Agent Host" on page 39.

- Register the RSA SecurID users in the RSA ACE/Server database and distribute RSA SecurID tokens to those users.

- Ask your RSA ACE/Server administrator if the usernames in the RSA ACE/Server database records have the user's Windows domain name attached (for example, **DOMAIN\username**). If so, you must select the **Send domain and username to RSA ACE/Server** option when you enable RSA ACE/Agent authentication.

Setup Tasks for RSA SecurID Users

Before you begin using the RSA ACE/Agent for Windows software, the following setup tasks must be completed for your RSA SecurID users:

- Users who will be challenged for PASSCODEs have been registered as RSA SecurID users in the RSA ACE/Server database, and their tokens have been activated. These processes are described in the RSA ACE/Server documentation.

  Important: Each RSA SecurID user's Windows username must be registered in the RSA ACE/Server database. These usernames **cannot** contain spaces and **must not** exceed forty characters. For Windows 2000 or XP username parameters, run the Computer Management application in the Administrative Tools.

- Users who will be challenged for PASSCODEs have been given their assigned and activated tokens.
- Users who will be challenged remotely have been instructed on configuring their remote computers.

Installing the RSA ACE/Agent 5.5 for Windows Software

The RSA ACE/Agent 5.5 for Windows is available as a zip file that you can download from the RSA Security web site. The following procedure assumes that you have successfully downloaded the zip file, and that you have placed it in a directory on your network that is accessible to all machines on which you will be installing the RSA ACE/Agent 5.5 for Windows.

To install RSA ACE/Agent 5.5 for Windows:

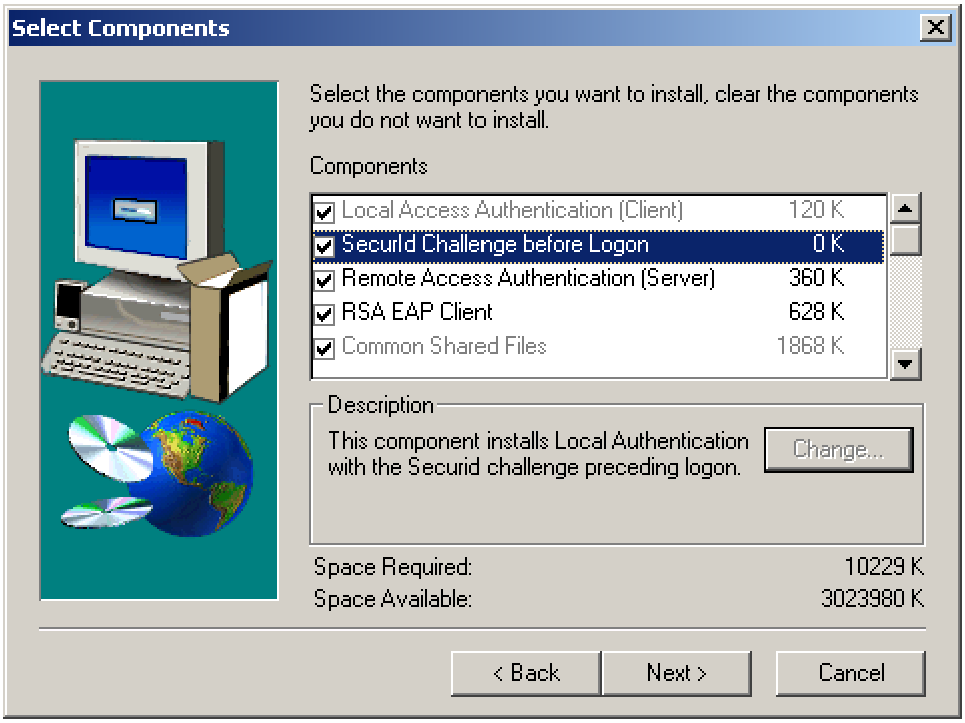
1. Log in to your system using the administrator's account or an account that is part of the Administrator group.
2. If you are running the Windows RAS service, stop the service.
3. In the **Aceclnt\nt_i386\** directory, double-click **Agent.exe**.

   The RSA ACE/Agent 5.5 for Windows Setup screen displays, and the installation wizard program starts.

Warning: Installation of the RSA ACE/Agent 5.5 for Windows removes both the Network and Web access authentication components from previous versions of Windows Agent software. If you are currently running either RSA ACE/Agent 5.0, or RSA ACE/Agent 4.*x* with Network and Web authentication components installed, and you want to continue using these features, DO NOT install RSA ACE/Agent 5.5 for Windows.

4. Click **OK** to continue. Click **Cancel** to exit.
5. In the Information dialog box, click **OK**.

   The Welcome dialog box is displayed. RSA Security recommends that you exit all programs before you install the RSA ACE/Agent 5.5 for Windows.
6. Click **Next** to continue. Click **Cancel** to exit.
7. Check the appropriate customer location and click **Next**.
8. Click **Yes** to accept the Software License Agreement and display the Select Components screen.



Select Components

Select the components you want to install, clear the components you do not want to install.

Components

☑	Local Access Authentication (Client)	120 K
☑	SecurId Challenge before Logon	0 K
☑	Remote Access Authentication (Server)	360 K
☑	RSA EAP Client	628 K
☑	Common Shared Files	1868 K

Description

This component installs Local Authentication with the SecurId challenge preceding logon.

Space Required: 10229 K

Space Available: 3023980 K

9. Select the RSA ACE/Agent components that you want to install.

Component	Purpose
Local Access authentication (Client)	Installs the files that enable RSA SecurID challenges of Local logins to this computer.
SecurID Challenge Before Logon	This component prompts a user performing a local authentication to be RSA SecurID challenged *before* the user is prompted for their Windows login information.
Remote Access authentication (Server)	Installs the files that enable RSA SecurID challenges of Remote logins to this computer. You must have the Microsoft RAS service installed on the computer to use this feature.
RSA EAP Client	Installs the RSA EAP Client and enables the RSA ACE/Agent 5.5 for Windows RRAS to communicate with third-party Point to Point Protocol (PPP). To enable EAP, the client must be installed on all remote access machines used for dial-up authentication.
Common Shared Files	Installs the shared program files (for example, **.dll** files) that are used by all the RSA ACE/Agent components.
Administration Guide and Documentation	Copies the RSA ACE/Agent Installation and Administration Guide to the ***%SYSTEMROOT%*\system32\Aceclnt** directory. For up-to-date information about the documentation set, see the *RSA ACE/Agent 5.5 for Windows Readme*. This file is named **readme.pdf** and is located in the **\Aceclnt\nt_i386** directory.

Warning: RSA Security strongly recommends that you DO NOT install the **SecurID Challenge Before Logon** component if you plan to configure the RSA ACE/Agent 5.5 for Windows software to challenge all users. If you DO plan to configure the Agent in this manner, you should perform a test authentication before you re-start the Agent Host.

10. Click **Next**.

11. Enter or browse to the location of your RSA ACE/Server **sdconf.rec** configuration file. Click **Next**.

    The RSA ACE/Agent files are copied to the computer, and the RSA ACE/Agent Registration dialog box opens.

12. If you want to register with RSA Security, check **Register now**. If you choose to register at a later time, you can do so by clicking **Start** > **Programs** > **RSA ACE/Agent** > **Register**.

    The Setup Complete dialog box opens.

13. You are prompted to restart the computer. Do one of the following:
    - If you do not want to immediately register online, select **Yes, I want to restart my computer now**.
    - If you do want to register online, select **No, I will restart my computer later**.
14. Click **Finish**.

    The Agent is installed. If you have chosen to restart the computer later and to register, your browser displays RSA ACE/Agent Registration page. When you restart your computer, you must test the RSA SecurID authentication service and configure the security options in the RSA ACE/Agent control panel.

Installing in Silent Mode

You can install the RSA ACE/Agent 5.5 for Windows in a silent mode that requires no end-user interaction. In large organizations, this installation method is faster and allows for less confusion and fewer user errors. You must decide how to distribute the silent mode installation files (for example, as a batch file, a login script, a mail message, and so on). The file **server.iss** is located in the **\Aceclnt\nt_i386** directory in the RSA ACE/Agent 5.5 for Windows zip file. It contains extensive script comments to assist you in creating your own silent installation scripts, and can be used to perform a complete installation of the RSA ACE/Agent 5.5 for Windows.

Note: Thoroughly read the programmer’s comments contained in the **server.iss** file before you attempt to use it.

To create a silent mode installation:

For the purposes of this procedure, the silent installation directory is referred to as ***Install_Dir***.

1. Browse to the **\Aceclnt\nt_i386** directory for the **agent.exe**, and **server.iss** files. Copy these files to your ***Install_Dir*** directory.
2. Locate the **sdconf.rec** file, and copy it to a network location that is accessible to your users.
3. Browse to the ***Install_Dir*** directory.
4. Modify the **server.iss** file so that the **sdconf** parameter in this file matches your environment. On the **SDConf=** line, enter the UNC location (\\server\sharename) of your **sdconf.rec** file after the equal sign.
5. Locate the SdComponentDialog2-0 section in the **server.iss** file and enable appropriate installation components in that section.

6. Use the following command in your installation method (batch file, **Run** line, etc.):

   ```
   agent.exe -s -a -s -SMS
   -f1Install_Dir\script.iss [-f2\\server\sharename\results.log]
   ```

   where *results.log* is the name of the installation log file. The **f2** argument is optional.

7. Instruct your users on how to run the silent mode installation from their computers.

Next Steps

Once you have successfully installed the RSA ACE/Agent 5.5 for Windows software, read the appropriate chapter in this guide to learn how to configure and administer the features you installed.

- Local access authentication: the chapter "Configuring Local Access Authentication" in this book.
- Remote access authentication: the chapter "Configuring Remote Access Authentication" in this book.

3 Configuring Local Access Authentication

The Local properties sheet in the RSA ACE/Agent control panel controls local access security. If the Local access authentication component is installed, the message in the **Components** area of the Main properties sheet displays **Local: Security features installed**.

Enabling Local Access Authentication

Local access authentication is available for both Windows 2000 and Windows XP. You can configure Local access authentication to challenge the following users for their RSA SecurID PASSCODEs:

- All users
- Users who are members of an administrator-designated group
- Users who are not members of an administrator-designated group

To enable Local access authentication:

1. In the RSA ACE/Agent control panel, click the **Local** tab.

   The Local properties sheet is displayed.

2. Under **Challenge**, select which users you want to challenge for their RSA SecurID PASSCODEs.

To challenge	Complete these steps
No users	Click **Off** on the **Challenge** list.
All users who log in locally	Click **All users** on the **Challenge** list.
A group of users who log in locally	Click **Users in** on the **Challenge** list, and then select the local or domain group that you want to challenge.
All users who log in locally, except users in a certain group	Click **All users except** on the **Challenge** list, and then select the local or domain group that you do not want to challenge.

3. If your RSA ACE/Server database records include the user’s Windows domain name as part of the username (for example, **DOMAIN\jsmith** instead of simply **jsmith**), check **Send Domain Name and User Name to RSA ACE/Server**.

4. To force local users to re-authenticate every time their desktop screen savers activate, check **Enable Screen Saver Security**. This option takes effect only if screen saver password authentication is available on the computer and if password authentication has been enabled for the user account through the Desktop control panel.

5. If you selected **All Users** on the **Challenge** list, the **Reserve Password** feature is automatically selected to prevent you from enabling the challenge **All Users** feature without setting a reserve password.

   If you enable the challenge **All Users** feature without setting a reserve password and an interruption occurs in your RSA ACE/Server authentication service, all users will be locked out of the protected machine. For this reason, **always** set a reserve password when enabling the challenge **All Users** feature. See the following section "Using the Reserve Password"for more information.

6. Click **OK**.

7. Restart the computer for your changes to take effect.

Using the Reserve Password

The reserve password feature is supported **only** with Local access authentication. Remote access users must successfully use PASSCODE authentication if their accounts are configured to require it. However, administrators of RAS accounts that are protected by RSA SecurID should read this section to understand the security issues.

If there is a problem that prevents the RSA ACE/Agent 5.5 for Windows from communicating with the RSA ACE/Server, RSA SecurID users will not get access to the desktop on their Windows machine. This could present a problem if you plan to challenge all users for their PASSCODEs. You can configure your system to avoid this problem in any of the following ways:

- Set up one user account with administrator privileges that is not protected by a PASSCODE. RSA Security does not recommend this method because it creates a security hole: you now have an account with full access but which has less protection than accounts with fewer privileges.

- If the RSA ACE/Agent is installed on the same machine that is functioning as a Domain Controller, physically secure that machine and disable network logins to that machine. In the event of a problem, this machine could be used to disable the requirement for PASSCODE authentication.

- Use the **Reserve Password** feature of RSA ACE/Agent for Windows. If you have enabled the reserve password and the Windows system is unable to communicate with the RSA ACE/Server at the time of authentication, instead of displaying a message that the Server is unreachable, the system displays a prompt to enter a reserve password. A user who knows the reserve password can use it instead of PASSCODE authentication.

  The reserve password is the same for all users. If you enable the **Reserve Password** option and reveal the password to a user, change the reserve password as soon as the user has logged on to the protected machine. RSA Security recommends changing the reserve password after each use.

  The reserve password is encrypted and stored in the registry, but you can set or clear it through the RSA ACE/Agent control panel. No one can modify the reserve password using any of the Windows system tools for manipulating user passwords.

To enable the reserve password:

1. In the RSA ACE/Agent control panel, click the **Local** tab.
2. If it is not already selected, check **Enable Local Access Security**.
3. Click **Enable Reserve Password**.
4. Enter the reserve password you want to use in the **Password** field.

   The password must be from 6 to 12 characters in length. Reserve passwords are case-sensitive.
5. Press TAB, and enter the password again in the **Confirm** field.
6. Click **Apply**.
7. To test that the **Reserve Password** option is enabled, disconnect the network connection to the RSA ACE/Agent computer, log out, and log back in. You will be prompted to enter the reserve password.

To clear the reserve password:

1. In the RSA ACE/Agent control panel, click the **Local** tab.
2. Clear **Enable Reserve Password**.
3. Click **Apply**.

4 Configuring Remote Access Authentication

Remote access authentication protects access to corporate network resources through the Windows Remote Access Service (RAS). The Remote properties sheet of the RSA ACE/Agent control panel controls the security of RAS accounts. If the Remote access component of the RSA ACE/Agent 5.5 for Windows is installed, the message **Remote: Security Features Installed** displays in the **Components** area of the control panel's Main properties sheet.

Enabling Remote Access Authentication

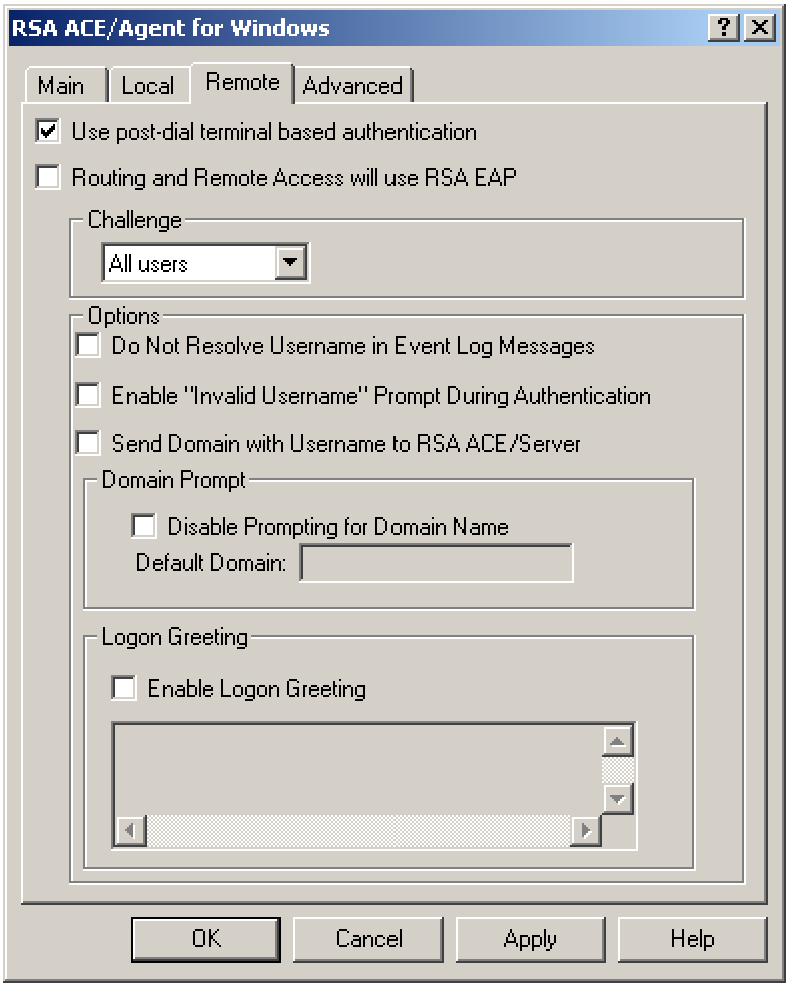
You can configure Remote access authentication to challenge the following users for their RSA SecurID passcodes:

- All users
- Users who are members of an administrator-designated group
- Users who are not members of an administrator-designated group

To configure Remote access authentication:

1. In the RSA ACE/Agent control panel, click the **Remote** tab.

The Remote properties sheet opens.



☑ Use post-dial terminal based authentication

□ Routing and Remote Access will use RSA EAP

Challenge

All users

Options

□ Do Not Resolve Username in Event Log Messages

□ Enable "Invalid Username" Prompt During Authentication

□ Send Domain with Username to RSA ACE/Server

Domain Prompt

□ Disable Prompting for Domain Name

Default Domain:

Logon Greeting

□ Enable Logon Greeting

2. Choose one of the following authentication methods.

- **Use Post-dial terminal based Authentication** if any of your remote client machines are unable to authenticate using RSA Security EAP.
- **Routing and Remote Access Service will use RSA EAP** if you plan to implement Remote access authentication using RSA Security EAP. In order to use this option, you must properly configure your remote access server, or your Microsoft Internet Authentication Server. See "Configuring RSA Security EAP" on page 30 for configuration instructions. In addition, you must install the EAP client component of the RSA ACE/Agent 5.5 for Windows on all remote access clients. See "Installing RSA Security EAP on Client Computers" on page 31. If you enable this setting, note that
  - ALL users are automatically RSA SecurID challenged.
  - The **Enable Invalid Username Prompt During Authentication** and the **Disable Prompting for Domain Name** options are automatically disabled, and you cannot enable them.

3. Under **Challenge**, select the users you want to challenge for their RSA SecurID PASSCODEs.

To challenge	Complete these steps
No users	Click **Off** from the **Challenge** list.
All users who access the protected computer	Click **All users** from the **Challenge** list.
A group of users who access the computer	Click **Users in** from the **Challenge** list. Click **Select** to display all Windows groups and then select the local or domain group that you want to challenge. **Note**: This option is NOT available for use with RSA Security EAP.
All users who access the computer, except users in a certain group	Click **All users except** on the **Challenge** list, and then select the local or domain group that you do not want to challenge. **Note**: This option is NOT available for use with RSA Security EAP.

4. If you do not want the Windows Application log to resolve usernames when users log in, check **Do Not Resolve Username in Event Log Messages**.

   For large Windows Domains, selecting this option helps to decrease the time it takes a user to log in. However, the RSA ACE/Agent 5.5 for Windows records the username as "N/A" in the User column of the Windows System log, which prevents you from filtering events in the log by user. The username is recorded for each login, but you can view it only if you select an event and display full details about the event in the Event Detail window. The username appears in the Description text box of the Event Detail window.

   Note: This option is available only if you choose to challenge **All users**.

5. To display a message if a username is entered incorrectly during authentication, check **Enable "Invalid Username" Prompt During Authentication**.

6. If your RSA ACE/Server database records include the user's Windows domain name as part of the username (for example, **DOMAIN\jsmith** instead of simply **jsmith**), check **Send Domain Name and User Name to RSA ACE/Server**.

7. To hide the **DOMAIN:** prompt from users during a remote login, check **Disable Prompting for Domain Name** and type the domain name to which remote users belong in the **Default Domain** field.

   At login, users will see only the **USERNAME** and **PASSCODE** prompts. After users enter valid PASSCODEs, they will be authenticated to the default domain.

8. To display a custom greeting message to users when they are prompted for their usernames and PASSCODEs, check **Enable Logon Greeting** and type your custom greeting in the scrollable box.

9. Click **Apply**.

Configuring RSA Security EAP

The RSA ACE/Agent 5.5 for Windows can only use the RSA Security Extensible Authentication Protocol. A dynamic link library file containing this version of EAP is loaded onto the remote access server when you install the Agent software on that machine. If you have checked **Routing and Remote Access Service will use RSA EAP** on the Remote properties sheet, make sure that your remote access server or your Microsoft Internet Authentication Server is properly configured to use RSA Security EAP.

Note: Before following the instructions for configuring RSA Security EAP on your Microsoft Internet Authentication Server, you should refer to the Microsoft Windows online Help for specific IAS configuration information pertinent to your Windows operating system.

To configure a remote access server to use RSA Security EAP:

1. Click **Start > Programs** > **Administrative Tools > Routing and Remote Access**.

   The Routing and Remote Access (RRAS) window is displayed. The console tree appears in the left frame.

2. Right-click the server in the console tree, and click **Properties**.

   The Properties dialog box opens.

3. Click the **Security** tab.

4. On the Authentication Provider drop-down menu, select **Windows Authentication**.

5. Click **Authentication Methods**.

6. Check the **Extensible Authentication Protocol** checkbox, and clear all the other methods.

7. Click **OK**, and return to the console tree.

8. In the console tree, click **Remote Access Policies**.

   The policies for this server appear in the right frame of the console.

9. Double-click the **Allow access if dial-in permission is enabled** policy.

   The Settings dialog box opens.

10. Click **Edit Profile**.

    The Edit Profile dialog box opens.

11. Click the **Authentication** tab.

12. Check the **Extensible Authentication Protocol** checkbox, and clear all the other methods.

13. On the EAP type drop-down menu, select **RSA Security EAP**.

14. Click the **Encryption** tab.

15. Check the **Strong** checkbox and clear the **No Encryption** and **Basic** checkboxes.

16. Click the **Advanced** tab.
17. Remove all connection attributes from the **Parameters** box.
18. Click **OK**.

The remote access server is now ready to use RSA Security EAP.

To configure a Microsoft Internet Authentication server to use RSA Security EAP:

1. Click **Start > Programs** > **Administrative Tools** > **Internet Authentication Service**.

   The Internet Authentication Service (IAS) window is displayed. The console tree appears in the left frame.

2. In the console tree, click **Remote Access Policies**.

   The policies for this server appear in the right frame of the console.

3. Double-click the **Allow access if dial-in permission is enabled** policy.

   The Settings dialog box opens.

4. Click **Edit Profile**.

   The Edit Profile dialog box opens.

5. Click the **Authentication** tab.
6. Check **Extensible Authentication Protocol**, and clear all other authentication methods.
7. On the EAP type drop-down menu, select **RSA Security EAP**.
8. Click the **Encryption** tab.
9. Check **Strong**, and clear all other encryption types.
10. Click the **Advanced** tab.
11. Remove all connection attributes from the **Parameters** box.
12. Click **OK**.

The IAS Server is now ready to use RSA Security EAP.

Installing RSA Security EAP on Client Computers

RSA Security EAP must be installed on each Windows 2000 or Windows XP remote client computer that is RSA SecurID challenged. You must be an administrator on the remote client machine to install the RSA Security EAP component. In addition, the client machine must be able to access the RSA Security web site.

Note: If you are unable to access the RSA Security web site on a remote client machine, you will need to physically distribute the zip file to the remote client machine after it has been downloaded.

To install RSA Security EAP:

1. On the client machine, open the zip file.
2. Follow steps 1 through 8 in the section "Installing the RSA ACE/Agent 5.5 for Windows Software" on page 17. Click **OK** or **Next** when appropriate at each of the installation wizard prompts.
3. In the Select Components screen, check **RSA EAP Client** only. Leave all other checkboxes blank.
4. Click **Next**.

   You do not need to provide the location of your RSA ACE/Server **sdconf.rec** file. Installing only the RSA Security EAP client on a remote machine does not require the **sdconf.rec** file.
5. Click **Next**.
6. You are prompted to restart the client computer. Select **Yes, I want to restart my computer now**.
7. Click **Finish**.

Configuring Remote Access Client Computers

No installation component of the RSA ACE/Agent 5.5 for Windows is needed on remote access clients that are not using RSA Security EAP. Note that only Windows 2000 and Windows XP remote access clients can use RSA Security EAP (RSA Security EAP is not supported on Windows 98 remote access clients). All Windows 2000 and Windows XP machines that will use RSA Security EAP must have the EAP client component installed and properly configured for either a dial-up connection, or an internet virtual private network (VPN) connection.

Use the Windows Network Connection wizard to create remote access connections. Then configure each connection (dial-up or VPN) to use RSA Security EAP. Refer to the appropriate configuration instructions below. For instructions on configuring remote connections that will not use RSA Security EAP, refer to the Microsoft Windows online Help.

To configure RSA Security EAP for dial-up connections:

1. Windows 2000: Click **Start** > **Settings** > **Network and Dial-up Connections** > **Dial-up Connection**. Then, select the name of the connection.

   Windows XP: Click **Start** > **Control Panel** > **Network Connections**.

   If you have a modem installed, click **Properties** in the Connect dialog box. If you do not have a modem installed, the properties dialog box opens automatically.
2. Click the **Security** tab.

   The Security properties sheet appears.
3. Click the **Advanced** radio button and then click the **Settings** button.

   The Advanced Security Settings dialog box opens.
4. On the top drop-down menu, click **Optional Encryption**.
5. Click the **Use Extensible Authentication Protocol (EAP)** radio button.

6. On the drop-down menu, click **RSA Security EAP (encryption enabled)**.
7. Click **OK** to accept the changes.

   The remote access client is now ready to use RSA Security EAP.

To configure RSA Security EAP for VPN connections:

1. Windows 2000: Click **Start** > **Settings** > **Network and Dial-up Connections**.

   Windows XP: Click **Start** > **Control Panel** > **Network Connections** > **VPN Connection**.
2. Select the name of the connection.

   The Connect dialog box opens.
3. Click **Properties**. Then select the **Security** tab.
4. On the Security properties sheet, select the **Advanced** radio button. Then click the **Settings** button.

   The Advanced Security Setting dialog box opens.
5. In the Data Encryption drop-down menu, select **Optional Encryption**.
6. Select the **Use Extensible Authentication Protocol** radio button. Then select **RSA Security EAP (encryption enabled)** in the drop-down menu.
7. Click **OK**.

Dialing In from Remote Computers

Instructions for establishing a remote access connection are listed below for each supported platform. Authentication instructions that pertain to each RSA SecurID token type are available as part of the RSA ACE/Server documentation set. Contact your RSA ACE/Server administrator to obtain specific instructions for each type of RSA SecurID token that you are currently deploying, or that you plan to deploy.

To learn how to adjust the default timeout values of RSA SecurID remote access prompts, see "Changing the Time-out Values of the Remote Access Prompts"on page 51.

Windows 98 (dial-up only):

1. At the remote computer, open **My Computer** and double-click the **Dial-Up Networking** icon.
2. Double-click the connection you want to dial.
3. Click **Connect**.

   A terminal screen opens and prompts for your username.

   If the screen is blank, press ENTER. The **Username** prompt displays.
4. Enter your username, and press ENTER.

   You can use the BACKSPACE key to delete mistyped characters. In the **Username** field, each deleted item will be automatically followed by a linefeed.

5. At the **DOMAIN** prompt, either press ENTER or follow the instructions for your particular Windows system.

6. Following the authentication instructions for your token type, enter your PASSCODE into the **PASSCODE** field, and press ENTER.

   If you are not required to enter a PASSCODE, the message **PASSCODE Not Required** displays.

7. Click **Continue** to gain access.

Windows 2000/Windows XP (dial-up):

1. Windows 2000: Click **Start** > **Settings** > **Network and Dial-up Connections**.

   Windows XP: Click **Start** > **Control Panel** > **Network Connections.**

2. Double-click the connection you want to dial.

   The Connect dialog box opens.

3. Enter your username and password information and, if applicable, your domain. This username might be different from your Windows username. If you are not sure, contact your RSA ACE/Server administrator.

4. Click **Dial**.

   When the modem connection is established, the SecurID Authentication dialog box opens.

5. Select your token type from the **Choose Token** list.

6. Follow the instructions for your token type, and click **OK**.

   If your PASSCODE is correct, you see an **Authentication Successful** message. If you see an **Access Denied** message, try to authenticate again. If you continue to see **Access Denied**, contact your RSA ACE/Server administrator.

Windows 2000/XP (VPN)

1. Windows 2000: At the remote computer, click **Start** > **Settings** > **Network and Dial-up Connections**.

   Windows XP: Click **Start** > **Control Panel** > **Network Connections**.

2. Select the VPN connection you want to use.

   The connect dialog box opens.

3. Enter your username and password. If necessary, enter your domain.

   If you are uncertain as to what they are, contact your RSA ACE/Server administrator.

4. Click **Connect**.

   When the VPN connection is established, the SecurID Authentication dialog box opens.

5. Select your token type from the **Choose Token** list.

6. Follow the instructions for your token type, and click **OK**.

   If your PASSCODE is correct, you see an **Authentication Successful** message. If you see an **Access Denied** message, try to authenticate again. If you continue to see **Access Denied**, contact your RSA ACE/Server administrator.

A Load Balancing with the sdopts.rec File

Load Balancing Overview

Version 5.5 of the RSA ACE/Agent software can balance authentication request loads automatically by sending a time request to each Server in the realm and determining a priority list based on the response time of each Server. The Server with the fastest response is given the highest priority and receives the greatest number of requests from that Agent Host, while other Servers get lower priorities and fewer requests. This arrangement lasts until the Agent software sends another time request. If the Servers respond to the next time request in a different order, the Agent Host changes its priorities accordingly.

In addition, the Agent Host can connect to its Servers through firewalls if the alternate IP addresses (aliases) for those Servers are either specified in the Agent Host's configuration record file (**sdconf.rec**), or are provided by a 5.*x* Server upon request by the Agent Host. The RSA ACE/Agent software automatically checks the alias IP address information before using those aliases to send its authentication requests to the Servers.

As an alternative to this automatic load-balancing process, Agent administrators have the option of balancing the load manually by specifying exactly which Servers each Agent Host should use to process requests. The specification also assigns a priority to each Server so that the Agent Host directs authentication requests to some Servers more frequently than to others. To use this option, the Agent administrator specifies priority settings in a flat text file named **sdopts.rec**, which resides on the Agent Host.

You can also use **sdopts.rec** to indicate additional firewall IP addresses to be used to contact Servers. Finally, you can specify an overriding IP address for the Agent Host if that host is a multi-homed server.

Creating an sdopts.rec File

You can use any text editor to create and edit an **sdopts.rec** file. After you set up the **sdopts.rec** file, save the file in ***%SYSTEMROOT%*\System32**. To protect the file from unintended changes, change the permission settings on your **sdopts.rec** file so that only administrators can modify it.

Important: Each time that you modify the **sdopts.rec** file, you must restart the Agent to register your changes.

The file can include the following types of lines:

- Comments, each line of which must be preceded by a semicolon.
- Keyword-value pairs, which can be any of the following:
  - **CLIENT_IP=<ip_address>:** Specifies an overriding IP address for the Agent Host. The Client_IP keyword can appear only once in the file. For information about overriding IP addresses, see "Setting an Overriding IP Address for an Agent Host" on page 39.
  - **USESERVER=<ip_address>, <priority>:** Specifies a Server that can or will receive authentication requests from the Agent Host according to the priority value specified. Use one setting for each Server that the Agent Host is to use. (For a limit on the number of Servers you can specify, see the note "Important" on page 36.) Each **USESERVER** keyword value must consist of the actual Server IP address, separated by a comma from the assigned Server priority. The priority specifies whether or how often a Server will receive authentication requests. The priority value must be one of those listed in the following table.

Priority	Meaning
2-10	Send authentication requests to this Server using a randomized selection weighted according to the assigned priority of the Server. The range is from 2–10: the higher the value, the more requests the Server receives. A Priority 10 Server receives about 24 times as many requests as a Priority 2 Server.
1	Use this Server as a last resort. Priority 1 Servers are used only if no Servers of higher priority are available.
0	Ignore this Server. A Priority 0 Server can be used only in special circumstances. First, it must be one of the four Servers listed in the **sdconf.rec** file. If so, the Priority 0 Server can be used only for the initial authentication of the Agent - unless all Servers with priorities of 1-10 listed in the **sdopts.rec** file are known by the Agent Host to be unusable. Generally, a priority value of 0 allows you to put an entry in the file for a Server without using that Server. You can change the Server's priority value if you later decide to use it. **Note:** Keywords must be uppercase. **Note:** If none of these servers with **USESERVER** statements are responsive, then the default server is the Master (if there is one) or the server that was used to create the sdconf.rec file.

Each Server you add to the **sdopts.rec** file with the **USESERVER** keyword must be assigned a priority. Otherwise, the entry is considered invalid. The IP addresses in the file are checked against the list of valid Servers that the Agent receives as part of its initial authentication with a 5.*x* Server.

Important: The maximum number of Servers you can specify in the **sdopts.rec** and **sdconf.rec** files *combined* is 11.

- **ALIAS=ip_address, alias_ip_address_1[, alias_ip_address_2, alias_ip_address_3]:** Specifies one or more alternate IP addresses (aliases) for a Server. Aliases for a Server can be specified in the Agent **sdconf.rec** file. Use the **ALIAS** keyword to specify the IP addresses of up to three additional firewalls through which the specified Server can be contacted by the Agent.

  The value for the **ALIAS** keyword must consist of the Server's actual IP address, followed by up to three alias IP addresses for that Server. The Agent will send its timed requests to both the actual and the alias IP addresses.

  Only the actual IP address specified by the **ALIAS** keyword must be known to the Server that is being specified. In addition, the actual IP address must be included on any Server list received by the Agent. The Server list provides actual and alias IP address information about all known Servers in the realm, and the Agent receives the Server list from a 5.*x* Server after the Server validates an authentication request.

- **ALIASES_ONLY[=ip_address]:** If you use this keyword, make certain that at least one Server has an alias IP address specified for it either in **sdconf.rec** or in **sdopts.rec**.

  When used without a value, the **ALIASES_ONLY** keyword specifies that the Agent should send its requests only to Servers that have alias IP addresses assigned to them. Exceptions can be made by including in the **sdopts.rec** file no more than 10 **IGNORE_ALIASES** keywords to specify which Servers must be contacted through their actual IP addresses. For an example showing these exceptions, see "Examples Featuring the ALIAS, ALIASES_ONLY, and IGNORE_ALIASES Keywords" on page 38.

  When you provide a Server's actual IP address as the value of **ALIASES_ONLY**, the keyword specifies that only the alias IP addresses of the Server should be used to contact that Server.

- **IGNORE_ALIASES[=ip_address]:** When used without a value, the **IGNORE_ALIASES** keyword specifies that all alias IP addresses found in the **sdopts.rec** file, the **sdconf.rec** file, or on the Server list provided by 5.*x* Servers will be ignored. Exceptions can be made by including no more than 10 **ALIASES_ONLY** keywords in the **sdopts.rec** file to specify which Servers must be contacted through their alias IP addresses. For an example showing these exceptions, see "Examples Featuring the ALIAS, ALIASES_ONLY, and IGNORE_ALIASES Keywords" on page 38.

  When you provide a Server's actual IP address as the value of **IGNORE_ALIASES**, the keyword specifies that only the actual IP address of the Server should be used to contact that Server.

An Example Featuring the USESERVER Keyword

The settings that you make in **sdopts.rec** can be in any order, but each setting must be listed separately in the file, one setting per line. Here is an example featuring only **USESERVER** keywords:

```
;Any line of text preceded by a semicolon is ignored
;(is considered a comment).
;Do not put a blank space between a keyword and its
;equal sign. Blank spaces are permitted after the
;equal sign, after the IP address, and after the
;comma that separates an IP address from a priority
;value.
USESERVER=192.168.10.23, 10
USESERVER=192.168.10.22, 2
USESERVER=192.168.10.20, 1
USESERVER=192.168.10.21, 0
```

The Server identified by the actual IP address 192.168.10.23 will receive many more authentication requests than Server 192.168.10.22 will. Server 192.168.10.20 will only be used if the Servers of higher priority are unavailable, and Server 192.168.10.21 will be ignored except in rare circumstances (as explained in the definition of Priority 0 in the **USESERVER** keyword's description).

Note: You can use the **USESERVER** and **ALIAS** keywords together in the **sdopts.rec** file, just as you can include whichever keywords defined for use in the file as you like. However, **USESERVER** keywords do not affect the alias addresses used to connect to Servers, and **ALIAS** keywords have no effect on which Servers are specified for use.

Examples Featuring the ALIAS, ALIASES_ONLY, and IGNORE_ALIASES Keywords

The settings that you make in **sdopts.rec** can be in any order, but each setting must be listed separately in the file, one setting per line. Here is an example featuring keywords related to Server alias addresses:

```
;Any line of text preceded by a semicolon is ignored
;(is considered a comment).
;Do not put a blank space between a keyword and its
;equal sign. Blank spaces are permitted after the
;equal sign, after the IP address, and after the
;comma that separates an IP address from a priority
;value.
USESERVER=192.168.10.23, 10
USESERVER=192.168.10.22, 2
USESERVER=192.168.10.20, 1
USESERVER=192.168.10.21, 0
ALIAS=192.168.10.23, 192.168.4.1, 192.168.4.2, 192.168.4.3
ALIAS=192.168.10.22, 192.168.5.2, 192.168.5.3
ALIAS=192.168.10.20, 192.168.5.1
ALIAS=192.168.10.21, 0, 192.168.1.1
ALIAS_ONLY=192.168.10.23
IGNORE_ALIASES=192.168.10.22
```

In this example, the default is to use alias or actual IP addresses, with a couple of exceptions. The Server with the actual IP address 192.168.10.23 has three alias addresses specified for it, while Servers 192.168.10.20 and 192.168.10.21 have only one alias apiece, and Server 192.168.10.22 has two alias addresses specified for it. The aliases specified by the **ALIAS** keywords are provided in addition to any aliases specified in **sdconf.rec** or on the Server list.

Note: You can use the **USESERVER** and **ALIAS** keywords together in the **sdopts.rec** file, just as you can include whichever keywords defined for use in the file as you like. However, **USESERVER** keywords do not affect the alias addresses used to connect to Servers, and **ALIAS** keywords have no effect on which Servers are specified for use.

The exceptions are that Server 192.168.10.23, as specified by the **ALIASES_ONLY** keyword, will only be contacted by the Agent through use of the Server's alias IP addresses. Server 192.168.10.22, specified by the **IGNORE_ALIASES** keyword, will only be contacted by the Agent through use of the Server's actual IP address.

Here is an example where the default is to ignore aliases, with two exceptions:

```
IGNORE_ALIASES
ALIASES_ONLY=192.168.10.23
ALIASES_ONLY=192.168.10.22
```

The **ALIASES_ONLY** exceptions specify that the Agent should send its requests to Server 192.168.10.23 and Server 192.168.10.22 only by using their alias IP addresses.

Here is an example where the default is to use aliases, with two exceptions:

```
ALIASES_ONLY
IGNORE_ALIASES=192.168.10.23
IGNORE_ALIASES=192.168.10.22
```

The **IGNORE_ALIASES** exceptions specify that the Agent should send its requests to Server 192.168.10.23 and Server 192.168.10.22 only by using their actual IP addresses.

Setting an Overriding IP Address for an Agent Host

When an RSA ACE/Agent runs on an Agent Host that has multiple network interface cards and therefore multiple IP addresses, the Agent administrator must specify a primary Agent Host IP address for encrypted communications between the Agent Host and the RSA ACE/Server.

Agent Hosts typically attempt to discover their own IP addresses. Left to itself, an Agent Host with multiple addresses might select one that is unknown to the Server, making communication between Agent and Server impossible. The Agent administrator can use the Client_IP= keyword in an **sdopts.rec** file to ensure that the primary IP address specified as the keyword value is always used to communicate with the Server.

Each Agent Host's primary IP address must be identified in its Agent Host record in the Server database. The Agent Host's other IP addresses can also be listed there (as "secondary nodes") for failover purposes.

If your RSA ACE/Server system uses auto-registration of Agent Hosts, each Agent Host's primary IP address is entered in that Agent Host's record automatically and updated whenever it changes. For more information, see the appendix "Automated Registration of Agent Hosts in the RSA ACE/Server Database" in this book.

If Agent Hosts are registered manually, however, it is the Server administrator's responsibility to ensure that the Agent's primary IP address in the Agent Host record in the Server database is identical to the primary IP address specified in the Agent Host's configuration records or in an **sdopts.rec** file. If these two settings do not match, communication between Agent Host and Server will fail. If secondary IP addresses are also specified for the Agent Host, these too must be entered in the record, and all addresses must be updated if they change.

The instructions in the following section, "Using the Client_IP Keyword," are addressed to RSA ACE/Agent administrators. They explain how to use the Client_IP keyword in an **sdopts.rec** file to identify an Agent Host's primary IP address, ensuring that this address is always used when the Agent Host communicates with the Server.

Some RSA ACE/Agents for Windows machines give administrators the option of specifying the overriding IP address for the Agent Host in the RSA ACE/Agent Control Panel. To use the Control Panel to specify the Agent Host's primary IP address, see "Setting an Overriding IP Address for an Agent Host" on page 39.

Using the Client_IP Keyword

You can either add the Client_IP keyword to an existing **sdopts.rec** file on the Agent Host or create an **sdopts.rec** file if none exists. See "Creating an sdopts.rec File" on page 35 for more information.

Note: The Dynamic Host Configuration Protocol allocates IP addresses to Agent Hosts dynamically. To avoid address conflicts, DHCP should not be enabled for Agent Hosts with multiple IP addresses. Conversely, there is no reason to use the Client_IP keyword for Agent Hosts that have single IP addresses, because these Agent Hosts have no alternative addresses to override.

To specify an IP address override in the **sdopts.rec** file, use the Client_IP keyword, as in this example:

```
CLIENT_IP=192.168.10.19
```

This statement in the file ensures that the Agent Host always uses the specified IP address to communicate with the RSA ACE/Server.

In the absence of Agent Host auto-registration, you, as the RSA ACE/Agent administrator, must ensure that the Server administrator knows the Agent Host's primary and secondary IP addresses when the Agent Host is first configured on the RSA ACE/Server system. Should any Agent Host address change at any time, inform the Server administrator in time to update the Agent Host record in the Server database.

B Automated Registration of Agent Hosts in the RSA ACE/Server Database

If your system is configured for automated Agent Host registration, running the Automated Agent Host Registration and Update utility on a new Agent Host will register it in the Server database, eliminating the need for an administrator to create the Agent Host record. In addition, running the Automated Agent Host Registration and Update utility any time the Agent Host's IP address has changed will update the IP address field of the Agent Host's record in the Server database. This update feature is especially useful for systems that use the Dynamic Host Configuration Protocol (DHCP) to assign IP addresses. The utility also permits a registered Agent Host to update its own information in the registry with relevant changes from the Server **sdconf.rec** configuration file.

Agent Hosts must have the Automated Agent Host Registration and Update utility installed to be able to use it. The RSA ACE/Server must be set to allow automated registration for the Server to accept registration information from new Agent Hosts; however, no Server setting controls the update feature. Use this document to install the Automated Agent Host Registration and Update utility.

To install and run the Automated Agent Host Registration and Update utility:

1. Copy the Primary Server's **sdconf.rec** and **server.cer** files to a temporary directory on the Agent Host.
2. Copy **sdadmreg_install.exe** from the **acesupp\sdadmreg\nt_i386** directory to the temporary directory that contains the **sdconf.rec** and **server.cer** files.
3. In Windows Explorer on the Agent Host, double-click **sdadmreg_install.exe**, and follow the displayed instructions.

   The **sdadmreg_install** utility installs **sdconf.rec**, **server.cer**, and **sdadmreg.exe** in the Agent Host's ***%SystemRoot%*\system32** directory (for example, **winnt\system32**).
4. Before you run **sdadmreg.exe**, verify that database brokers are running on the RSA ACE/Server.

   If the Server is installed on a Windows machine, starting any Server program, such as the Database Administration application, automatically starts the database brokers. If the Server is installed on a UNIX machine, start the database brokers by issuing the ***ACEPROG*/sdconnect start** command on the Server.
5. The Automated Agent Host Registration and Update utility will run when the Agent Host is restarted. To run the program at any time, double-click **sdadmreg.exe**.

6. After the Automated Agent Host Registration and Update utility starts, a service named ACE Auto-Registration joins the list of services running on the Agent Host.

   You might want to run the program:

   - Immediately after installing RSA ACE/Agent software on a Windows host. An Agent Host record will be added to the Server database if none already exists for the Agent Host, and if the Server is set to allow automated registration.
   - When the Agent Host gets a new IP address. The new IP address will be written to the Server database record for the Agent Host, provided that a node secret for the Agent Host has already been created by a successful authentication from the Agent Host to the Server.
   - When you want to have the Agent Host's registry information updated by the current **sdconf.rec** file on the Server. The updated registry setting will not take effect until the Agent Host is rebooted.

C Local Authentication with Third-Party Products

The RSA ACE/Agent 5.5 for Windows supports Local authentication for use with Citrix MetaFrame, Windows 2000 Terminal Server (WTS), and pcAnywhere. This appendix lists specific configuration information and limitations associated with these third party products.

For information about other configurations, visit RSA SecurCare Online (**www.rsasecurity.com/securcare/**).

Windows Terminal Server

The limitations listed below apply when using RSA ACE/Agent 5.5 for Windows with either Windows Terminal Server, or Windows Terminal Server and Citrix MetaFrame. When using either combination of these products with the RSA ACE/Agent 5.5 for Windows, the agent software is installed on the same server as WTS and MetaFrame. The most common approach for authentication in this scenario is local authentication to the WTS/MetaFrame server.

Limitations

Be aware that when you use RSA ACE/Agent 5.5 for Windows with Windows Terminal Server and optionally, Citrix Metaframe, the end user is presented with a Windows login prompt as well as an RSA SecurID PASSCODE prompt. The reason for this is that when loading our RSA ACE/Agent for Windows, it replaces the MS GINA currently in place with our SD GINA. Our SD GINA then calls the one that was replaced as the next GINA and prompts users for both the Windows and RSA SecurID logins.

D Troubleshooting

Authentication Messages

A user might get the following messages during authentication:

- Cannot load RSA ACE/Agent DLL.
- Initialization of sdagent.dll library failed.
- Unexpected error from RSA ACE/Agent.

See “RSA ACE/Agent Error and Event Viewer Log Messages” on page 51 for more information.

Windows 2000 and Windows XP Troubleshooting

If you are troubleshooting Windows 2000 or Windows XP, the log of informational and authentication error messages is stored in the rotating log file ***%SYSTEMROOT%*/aceclient.log**. When this file exceeds 1MB, it is renamed **aceclient*n*.log** (where *n* is a number between 1 and 9), and a new **aceclient.log** file is created.

***%SYSTEMROOT%*/aceclient.log** is the default location for the log file. You can change the location and the default maximum file size of the log file by editing the Windows registry.

To change the log file location:

1. Run the **Regedit** program.
2. Under the key **HKEY_LOCAL_MACHINE\SOFTWARE\ SDTI\ ACECLIENT**, create a new string value called **tracefile**.
3. In the **Value Data** field, enter the new path and filename for the log file (for example, **c:\ACElog\ACEhostname.log**.
4. Click **OK**.
5. Close **Regedit**.
6. Restart the computer to make your changes take effect.

To change the maximum allowed log file size:

1. Run the **Regedit** program.
2. Under the key **HKEY_LOCAL_MACHINE\SOFTWARE\SDTI\ACECLIENT**, create a new DWORD called **tracesize**.
3. In the **Value Data** field, enter the desired file size, in bytes (for example, a 2 MB log file would be 2,000,000 bytes).
4. Click **OK**.
5. Close **Regedit**.
6. Restart the computer to make your changes take effect.

Viewing sdconf.rec

If the RSA ACE/Agent for Windows and the RSA ACE/Server machines do not have compatible copies of the **sdconf.rec** file, the computers will not be able to communicate with each other.

To make sure you have the correct **sdconf.rec** file, open the RSA SecurID Authentication Information dialog box, or run the **sdtest** utility.

To view sdconf.rec file settings:

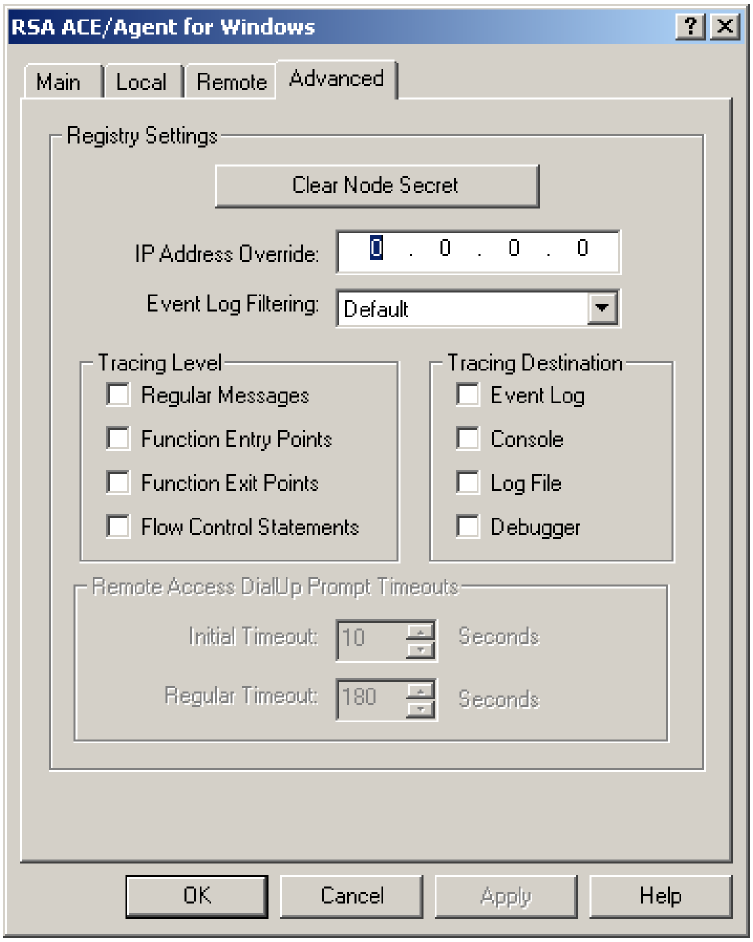
1. Click **Start** > **Settings** > **Control Panel**.
2. Double-click the **RSA ACE/Agent** icon.
3. On the Main tab, click **Test Authentication with RSA ACE/Server**.

   The RSA SecurID Authentication Information dialog box opens.

   If the dialog box fields contain illegible characters, the **sdconf.rec** file has been corrupted. Ask the RSA ACE/Server administrator for a new copy of **sdconf.rec** for the Agent.

Configuring Advanced Settings

To display the advanced configuration settings for the Agent, open the RSA ACE/Agent control panel, and click the **Advanced** tab.



IP Address Override: 0 . 0 . 0 . 0

Event Log Filtering: Default

Tracing Level

□ Regular Messages

□ Function Entry Points

□ Function Exit Points

□ Flow Control Statements

Tracing Destination

□ Event Log

□ Console

□ Log File

□ Debugger

Initial Timeout: 10 Seconds

Regular Timeout: 180 Seconds

The configuration settings on the Advanced properties sheet of the RSA ACE/Agent control panel are set to work well in most installations of the Agent. You should not reset them unless doing so will improve performance or help you or your RSA Security Technical Support representative to resolve a problem. The areas of advanced settings are

- Clearing the node secret from the Agent Host.
- Setting an IP address override for the Agent Host primary network interface.
- Filtering event messages out of the Windows Event Viewer Application Log.
- Setting tracing levels to debug Agent problems and control where the tracing information is recorded.
- Changing the time-out values for the remote access authentication prompts.

For more information about these advanced settings, see the following subsections.

Clearing and Replacing the Node Secret

The node secret is a symmetric encryption key known only to the RSA ACE/Agent and the RSA ACE/Server. The Server uses the secret to authenticate the Agent Host, and both machines use the secret to encrypt and decrypt packets of data as they are sent across the network.

The first time a user successfully authenticates or tests authentication from an Agent, the Server creates a node secret for that Agent and stores it in the Server database. A copy of the secret is encrypted and sent to the Agent, where the node secret is stored in the Windows registry.

If the node secret on the Agent Host computer is corrupted or does not match the node secret in the RSA ACE/Server database, encrypted communications between the Agent and the Server cannot work. If you see that the **Access Denied, Node Verification Failed** error is logged in the RSA ACE/Server Activity monitor, you must clear the node secret from the Agent Host. At the same time, your RSA ACE/Server administrator must disable the **Sent node secret** client setting specified for the Agent Host in the Server database. Finally, you must run the **sdtest** utility on the Agent Host to authenticate to the Server. (For instructions, see "Test Authentication Overview" on page 11.) When you authenticate successfully, the Server sends a new node secret to the Agent.

To clear and replace the node secret on the RSA ACE/Server Host:

1. Run the RSA ACE/Server Database Administration program.
2. Click **Agent Host > Edit Agent Host**, and select the Agent Host with the corrupted secret.

   The Agent Host record opens.
3. Clear **Sent Node Secret**.
4. Click **OK**.

To clear and replace the node secret on the RSA Agent Host:

1. Log in as a local Windows administrator.
2. Click **Start > Settings > Control Panel**.
3. Double-click the **RSA ACE/Agent** icon.
4. On the **Advanced** tab, click **Clear Node Secret**.
5. Click **Apply**.
6. On the Main tab, click **Test Authentication with RSA ACE/Server**.

   The RSA SecurID Authentication Information dialog box opens.
7. Choose an RSA SecurID token type.
8. Enter the username and PASSCODE for the token you are using.
9. Click **OK**.

   If your token is registered correctly in the RSA ACE/Server database, the system displays an **Authentication successful** message.The Agent and the Server established a new node secret when you authenticated.

Setting an IP Address Override

When an RSA ACE/Agent runs on an Agent Host that has multiple network interface cards and therefore multiple IP addresses, the Agent administrator must specify a primary Agent Host IP address for encrypted communications between the Agent Host and the RSA ACE/Server.

Agent Hosts typically attempt to discover their own IP addresses. Left to itself, an Agent Host with multiple addresses might select one that is unknown to the Server, making communication between Agent and Server impossible.

To specify the primary IP address of the Agent:

1. Click **Start** > **Settings** > **Control Panel**.
2. Double-click the **RSA ACE/Agent** icon.
3. On the **Advanced** tab, in the **IP Address Override** box, enter the IP address of the primary network interface of the Agent.
4. Click **Apply**.

Filtering Event Messages Out of the Windows Event Viewer Log

You can prevent certain RSA ACE/Agent event messages from being logged in the Windows Event Viewer Application Log. You might want to prevent certain event messages from being logged if your site has a large number of RSA SecurID users, and the logging of all events makes it difficult for you to search the log for messages related to a specific incident.

Default. Allows all event messages to be recorded in the log.

Low. Prevents event messages from being logged that pertain to successful PASSCODE authentication events, and those that pertain to required or disabled PASSCODE challenging.

Medium. In addition to preventing the logging of all event messages in the **Low** category, this setting prevents the logging of event messages pertaining to New PIN Mode and the Next Tokencode prompt.

High. In addition to preventing the logging of all event messages in the **Low** and **Medium** categories, this setting prevents the logging of **Service thread terminated, exiting** messages.

Note: You **cannot** use this setting to prevent RSA ACE/Agent *error messages* from being recorded in the Windows Event Viewer's Application Log. In addition, this setting has no effect on the logging of trace messages in the Event Viewer Log.

To set the event message filtering level in the Windows Event Viewer Application Log:

1. Click **Start** > **Settings** > **Control Panel**.
2. Double-click the **RSA ACE/Agent** icon.
3. On the **Advanced** tab, in the **Event Log Filtering** box, click the level of filtering that you want to apply to event messages in the log.
4. Click **Apply**.

Tracing and Logging Agent Code Activity

On the **Advanced** properties sheet of the RSA ACE/Agent control panel, you can enable tracing of Agent code activity and specify where tracing messages are to be logged. Trace logging is a useful debugging aid for you and your RSA Security Technical Support representatives.

Because tracing has an impact on Agent performance, do not enable tracing unless you must do so to detect and resolve a problem.

Note: Setting the **Event Log Level** on the **Advanced** properties sheet has no effect on the logging of tracing messages in the Windows Event Viewer logs.

To turn on tracing and specify where tracing messages will be logged:

1. Click **Start** > **Settings** > **Control Panel**.
2. Double-click the **RSA ACE/Agent** icon.
3. On the **Advanced** tab, under **Tracing Level**, check the checkbox of every type of tracing you want the system to perform.
4. Under **Tracing Destination**, check the checkbox of every location you want the tracing messages to be logged:
   - **Event Log.** Tracing messages are recorded in the Windows Event Viewer logs.
   - **Console.** The system opens a console window and records tracing messages directly to the window. You can scroll through the messages in the window.
   - **Log File.** Tracing messages are recorded in the ***%SYSTEMROOT%*/aceclient.log** file.
   - **Debugger.** Tracing messages are recorded in the system debugger.
5. Click **Apply** to turn on tracing.

Changing the Time-out Values of the Remote Access Prompts

If you display RSA SecurID username and PASSCODE prompts for remote users through the use of automated scripts, you might need to set different time-out values for the Remote access prompts. RSA SecurID users have to wait, sometimes as long as 60 seconds, before they can enter their latest PASSCODEs. (RSA SecurID Software Token users never need to wait for new tokencodes to display because their next tokencodes are generated automatically.) By changing the time-out values, you can prevent the Remote access prompts from timing out before users can send their PASSCODEs to the Agent.

Do **not** change the default time-out values unless your users experience problems with remote access.

You can change two remote access prompt time-out values on the Advanced properties sheet of the RSA ACE/Agent control panel:

- The **Initial Timeout** value is important for scripts. You can use it to decrease the initial wait time before a script begins to execute.
- The **Regular Timeout** value is set for all prompts that appear after the initial remote access prompt is displayed.

To change time-out values of the remote access prompts:

1. In the RSA ACE/Agent control panel, click the **Advanced** tab.

   The Advanced properties sheet opens.
2. In the Remote Access Prompt Time-outs area, in the **Initial Timeout** box, enter or select a number representing the number of seconds that must elapse before the initial Remote prompt times out.

   The minimum **Initial Timeout** value is 1 second and the maximum is 180 seconds. The default value is 10 seconds.
3. In the **Regular Timeout** box, enter or select a number representing the number of seconds that must elapse before all subsequent Remote prompts time out.

   The minimum **Regular Timeout** value is 5 seconds and the maximum is 180 seconds. The default value is 180 seconds.
4. Click **Apply**.

RSA ACE/Agent Error and Event Viewer Log Messages

The RSA ACE/Agent 5.5 for Windows logs events in the Windows Event Viewer Application Log under the source ACECLIENT. The messages are sorted into the following categories:

ACE/Agent. General RSA ACE/Agent events, such as **sdconf.rec** status, RSA ACE/Server communication errors, and memory allocation errors.

Local. Events generated by the Local access authentication module (SDGINA).

Remote. Events generated by the Remote access authentication module (SDRAS).

This section lists all error and event messages alphabetically.

ACECheck processing error for userid *username*

If the **ACECheck** function returns an error, an RSA ACE/Server time-out or some other communications error has occurred.

ACEClose processing error *errornumber*

If the **ACEClose** function returns an error, an RSA ACE/Server time-out or some other communications error has occurred.

ACENext processing error for userid *username*

If the **ACENext** function returns an error, an RSA ACE/Server time-out or some other communications error has occurred.

ACEPin processing error for userid *username*

If the **ACEPin** function returns an error, an RSA ACE/Server time-out or some other communications error has occurred.

All users challenged. PASSCODE required.

The specified service is configured to RSA SecurID-challenge all users of the service. The **Challenge** control on the RSA ACE/Agent control panel is set to **All Users**. The user was challenged to enter a PASSCODE.

An error occurred when accessing the Metabase.

The Agent failed while reading from or writing to the Metabase. If this message is displayed, first make sure you have the correct administrative privileges, and then reboot the Agent Host. If the error persists, re-install the Agent to override the existing settings. If that does not resolve the situation, you will have to uninstall, and then re-install the Agent.

Authentication failure.

The subject described in the Event Detail did not RSA SecurID-authenticate successfully and was therefore refused access.

Authentication Manager: Access Denied.

The user did not enter a valid RSA SecurID PASSCODE.

Authentication Manager: RSA ACE/Agent Library Failure.

The RSA ACE/Agent could not load the **aceclnt.dll** library file. The file is either corrupted, has been moved to another directory, or has been deleted from the system.

If the **aceclnt.dll** file is no longer on the system, you must re-install the RSA ACE/Agent.

Authentication Manager: Failed Authentication Attempt. User *username*.

The user entered an invalid PASSCODE, causing the "bad PASSCODE" counter to be incremented by 1 in the Windows registry. If this counter exceeds the configured number of bad PASSCODEs, the user's token will be deactivated until an administrator intervenes.

The number of allowed bad PASSCODEs is stored in the **sdconf.rec** file and can be viewed by running the **sdtest** program.

Authentication Manager: Invalid RSA ACE/Server configuration. User *username*.

The **sdconf.rec** file is not valid. The file is either corrupted, has been moved to another directory, or has been deleted from the system.

To correct the problem, get a new copy of **sdconf.rec** from your RSA ACE/Server administrator.

Authentication Manager: New PIN Accepted. User *username*.

The user successfully associated a new PIN with his or her token.

Authentication Manager: New PIN Rejected. User *username*.

The user did not successfully associate a new PIN with his or her token. If the user is attempting to create his or her own PIN, make sure the user understands the PIN length and syntax parameter settings for your RSA ACE/Server.

Authentication Manager: Next Tokencode Accepted. User *username*.

After entering a series of bad PASSCODEs, the user was prompted to enter the next tokencode from his or her token. The tokencode was valid and the user was authenticated successfully.

Authentication Manager: Next Tokencode Failed. User *username*.

After entering a series of bad PASSCODEs, the user was prompted to enter the next tokencode from his or her token. The tokencode was not valid and the user was denied access to the system.

Authentication Manager: Unsupported protocol.

The client attempted to access an unsupported version of RSA ACE/Server.

Authentication Manager: User Canceled New PIN Mode. User *username*.

The user was prompted to associate a new PIN with his or her token, but the user did not complete the new PIN procedure. Make sure the user understands how to use his or her token in New PIN mode.

Authentication Manager: User Canceled Transaction. User *username*.

The user was prompted to authenticate, but then canceled out of the Enter PASSCODE dialog box. This is a purely informational message.

Authentication Manager: User I/O Timeout. User *username*.

The user waited too long at the **Enter PASSCODE** prompt, so the RSA ACE/Agent canceled the transaction.

Authentication Manager: User Interface Library Failure.

The RSA ACE/Agent could not load the **sdui.dll** library file. The file is either corrupted, has been moved to another directory, or has been deleted from the system.

If the **sdui.dll** file is no longer on the system, you must re-install RSA ACE/Agent.

Cannot create socket during initialization in RSA SecurID Authentication

Socket services may not have started. Check the Event Log to find out if there is a problem with the network card or the TCP/IP services.

Also, make sure echo services are running on your RSA ACE/Server by doing one of the following:

- If the RSA ACE/Server is running on a Windows machine, open the RSA ACE/Server machine Network control panel, click the **Services** tab, and make sure **Simple TCP/IP Services** are installed. If they are not, add the **Simple TCP/IP Services**.
- If the RSA ACE/Server is running on a UNIX machine, make sure the **echo** service is running on the RSA ACE/Server machine. See your UNIX operating system documentation for information about starting the echo service.

Cannot create socket during initialization.

Make sure echo services are running on your RSA ACE/Server by doing one of the following:

- If the RSA ACE/Server is running on a Windows machine, open the RSA ACE/Server machine Network control panel, click the **Services** tab, and make sure **Simple TCP/IP Services** are installed. If they are not, add the **Simple TCP/IP Services**.
- If the RSA ACE/Server is running on a UNIX machine, make sure the **echo** service is running on the RSA ACE/Server machine. See your UNIX operating system documentation for information about starting the echo service.

Cannot load RSA ACE/Agent DLL

Test cannot find **aceclnt.dll** in the **\system32** directory. You must re-install RSA ACE/Agent software.

Could not initialize RSA ACE/Agent

Will be preceded by a number of RSA ACE/Agent error messages, such as **Cannot find sdconf.rec**. Try re-installing the **sdconf.rec** file in the ***%SYSTEMROOT%*\system32** directory.

Also check the security settings for the file. Make sure the account that the Web server is running has **Full Access** privileges to the HTML file.

Could not open registry key *keyname*

A serious registry corruption has occurred. You must re-install the RSA ACE/Agent software.

Credential Management error allocating memory.

The system does not have enough physical RAM, or there were too many other processes running in memory. If you receive this message often, add more physical memory to the computer.

Credential Management error creating BSAFE algorithm object.

The system probably does not have enough physical RAM, or there were too many other processes running in memory. If you receive this message often, add more physical memory to the computer.

Credential Management error generating random number.

The system probably does not have enough physical RAM, or there were too many other processes running in memory. If you receive this message often, add more physical memory to the computer.

The detailed BSAFE error is contained in the **Data** field of the Event Detail.

Data Manager: Not Enough Memory.

The system does not have enough physical RAM, or there were too many other processes running in memory. If you receive this message often, add more physical memory to the system.

Failed authentication for userid *username*.

The RSA ACE/Server did not grant the user access; the most common causes for this are wrong username or an invalid PASSCODE.

Failed to create event.

These are internal errors. The machine may not have enough free resources to add RSA SecurID authentication. Consider moving service(s) from this machine to another one.

Failed to create service thread, aborting.

There were too many other processes running, so the service did not start.

Failed to find required service WINSOCK.

The Windows socket interface was not found. Check the event log to find out if there is a problem with WINSOCK. Ensure that TCP/IP has been enabled on the machine.

File incorrect size: sdconf.rec.

It is likely that the **sdconf.rec** file was not copied in binary mode. Ask the RSA ACE/Server administrator for a new copy of **sdconf.rec**.

File not found: aceclnt.dll.

Software may have been installed incorrectly or **aceclnt.dll** may have been deleted. Re-install the RSA ACE/Agent software from the Microsoft Internet Information Server CD to correct the problem.

File not found: sdconf.rec.

The **sdconf.rec** file is not in the ***%SYSTEMROOT%*\system32** directory. It was either removed or never copied from the RSA ACE/Server. Ask your RSA ACE/Server administrator for a new copy of **sdconf.rec**.

Local: Security Features Available.

The machine meets the system and software requirements for the named security features.

Network Timeout-RSA ACE/Server was responding but has now stopped.

Make sure the RSA ACE/Server process is running on the server. Check for a network problem such as a router malfunction or unplugged network cable.

New PIN accepted for userid *username*.

The RSA ACE/Server verified the RSA SecurID user's new PIN.

New PIN rejected for userid *username*.

The PIN was rejected by the RSA ACE/Server. The user must re-authenticate to set the PIN. Check the Activity Log on the RSA ACE/Server.

New PIN requested from userid *username*.

The RSA ACE/Server has prompted the RSA SecurID user to create his or her own PIN or receive a system-generated PIN.

Next code accepted for userid *username*.

The Next Tokencode was accepted by the RSA ACE/Server and access was granted.

Next code rejected for userid *username*.

The user must attempt to authenticate again.

Next code requested from userid *username*.

The user's token was in Next Tokencode mode and the RSA ACE/Server asked for the second tokencode.

Remote: RAS not available.

The machine does not meet one or more of the system or software requirements needed to enable authentication of RAS connections. See "Remote Access Authentication Requirements" on page 15, and make sure the machine meets all the requirements.

RSA ACE/Agent initialization failed

The Agent cannot make the connection to the RSA ACE/Server. Make sure the RSA ACE/Server and network are operational and that all network interface cards and cables are properly installed and in good condition.

RSA ACE/Server is not responding

There is a network communications problem between the RSA ACE/Server and the RSA ACE/Agent, the server cannot be found (because the IP address is wrong, for example), or the RSA ACE/Server daemon is not running.

RSA ACE/Server is not responding. Run CLNTCHK to verify port and IP address of RSA ACE/Server

There is a network communications problem between the RSA ACE/Server and the RSA ACE/Agent, the RSA ACE/Server cannot be found (because the IP address is wrong, for example), or the RSA ACE/Server daemon is not running.

RSA SecurID challenge off. PASSCODE not required.

RSA SecurID authentication is not enabled on the specified service. The **Challenge** control on the RSA ACE/Agent control panel is set to **OFF**. The user was not challenged to enter a PASSCODE.

Session Manager: Failed Socket Accept Call.

There are too many sockets open.

Session Manager: Failed to Create Server Thread.

There are too many server threads running (too many users connecting at once). Try widening the intervals at which users attempt to log in.

Session Manager: Failed to Create Socket.

This message results from a memory shortage or WINSOCK error. The cause might be too many users connecting to the server at the same time.

Session Manager: Failed to Resolve Hostname.

Most likely a configuration error. The machine that is connecting has no DNS or NetBIOS name, or has an invalid IP address. Make sure your network is configured properly and that your host file entries are correct.

Session Manager: Not Enough Memory.

The system does not have enough physical RAM, or there were too many other processes running in memory. If you receive this message often, add more physical memory to the computer.

Session Manager: SSL Out of Memory Error.

The system does not have enough physical RAM, or there were too many other processes running in memory. If you receive this message often, add more physical memory to the computer.

Session Manager: Winsock startup error.

The Microsoft Windows Sockets failed to initialize. To troubleshoot WINSOCK problems, consult your Microsoft networking documentation.

Successful authentication.

The subject described in the Event Detail RSA SecurID-authenticated successfully and was granted access to the system.

The access control entry for *filename* was not found.

The Windows security entry for this file is corrupted. If you suspect that the ACL has become corrupted, see the Microsoft Windows Help, or contact Microsoft technical support.

The discretionary Access Control List for *filename* was not found.

The Windows security entry for this file is corrupted. If you suspect that the ACL has become corrupted, see the Microsoft Windows Help, or contact Microsoft technical support.

The user connected to port COM# has been disconnected because an internal authentication error. . .

The connection to the port has been lost due to an I/O flow error. Make sure that the Hardware Flow Control option is enabled in the **Modem Configure Settings** page of the RAS Control Panel.

Also make sure that the port speed setting in the RAS Control Panel is the same as the setting in the Port Control Panel.

The user connected to port *portname* has been disconnected. . .

There is a problem with RSA SecurID authentication. See the Event Detail topic for more specific information.

The user *server/username* disconnected from port *portnumber*.

The user closed the connection on the specified port.

The user *server/username* connected on port *portnumber* on date at time and disconnected on date at time. . .

A normal RSA ACE/Agent disconnection has occurred.

The user *username* has connected and been authenticated on port *portnumber*.

A normal (authenticated) RSA ACE/Agent-Server connection occurred.

The user was authenticated as *username1* by the third-party security host module but was. . .

The user has been disconnected because his or her login name and the RSA Security authentication name are not the same.

Unable to determine if user in challenge group. Checking cached group SID. User in challenge group. PASSCODE required.

The Domain Controller could not be contacted to verify the user's group membership, so the user's cached login information was used to determine the user's group membership. The cached information revealed that the user was in an RSA SecurID challenged group.

Unable to determine if user in challenge group. Checking cached group SID. User not in group. PASSCODE not required.

The Domain Controller could not be contacted to verify the user's group membership, so the user's cached login information was used to determine the user's group membership. The cached information revealed that the user was not in a challenged group.

Unable to determine if user in challenge group. Checking cached group SID. User in exception group. PASSCODE not required.

The Domain Controller could not be contacted to verify the user's group membership, so the user's cached login information was used to determine the user's group membership. The cached information revealed that the user was not required to authenticate.

Unable to determine if user in challenge group. Checking cached group SID. User not in exception group. PASSCODE required.

The Domain Controller could not be contacted to verify the user's group membership, so the user's cached login information was used to determine the user's group membership. The cached information revealed that the user was required to authenticate.

Unexpected error from RSA ACE/Agent.

The value returned by the RSA ACE/Server is not valid. Re-install the RSA ACE/Agent for Windows software. If the problem persists, check your hardware.

User <blank> canceled out of RSA SecurID Authentication routine.

The user canceled without entering a username.

User I/O Timeout-User took too long to respond.

The Windows system timed out after waiting for a response from the user.

User in challenge group. PASSCODE required.

The specified user is a member of the group designated for RSA SecurID authentication on the RSA ACE/Agent control panel. The user was challenged to enter a PASSCODE.

User in exception group. PASSCODE not required.

The specified user is a member of the group that is designated on the RSA ACE/Agent control panel to be exempt from RSA SecurID authentication. The user was not challenged to enter a PASSCODE.

User not in challenge group. PASSCODE not required.

The specified user is **not** a member of the group designated for RSA SecurID authentication on the RSA ACE/Agent control panel. The user was not challenged to enter a PASSCODE.

User not in exception group. PASSCODE required.

The specified user is **not** a member of the group that is designated on the RSA ACE/Agent control panel to be exempt from RSA SecurID authentication. The user was challenged to enter a PASSCODE.

User *username* canceled out of New PIN routine.

The user canceled the authentication attempt.

User *username* not in ***groupname*** group. PASSCODE is not required.

The user was not prompted for a PASSCODE. To challenge every local user who attempts to access the machine, enable the **Challenge All Users** option on the Local properties sheet of the RSA ACE/Agent control panel.

User *username* not in ***groupname*** group. PASSCODE not required.

The **Challenge All** switch is not on, and the user is not in the designated group.

User *username*: ACCESS DENIED. ATTEMPT 1.

The user was denied access. Check the RSA ACE/Server Activity Log for the specific reason.

User *username*: Access denied. Attempt to use invalid handle. Closing connection.

An internal error occurred. If the message re-occurs, call the RSA Security Technical Support Center.

User *username*: ACCESS DENIED. Next Tokencode failed.

The user must attempt to authenticate again.

User *username*: ACCESS DENIED. Server signature invalid.

This message indicates that the identity of the RSA ACE/Server could not be verified by the client. If you see this message, call the RSA Security Technical Support Center.

User *username*: ACE Check Error: Invalid group SID. PASSCODE required.

The user's group SID did not contain a valid group name. The user was challenged for an RSA SecurID PASSCODE.

User *username*: canceled out of Next Tokencode routine.

The user canceled out of the Next Tokencode process.

User *username*: canceled out of RSA SecurID Authentication routine.

The user canceled after entering a username.

User *username*: Domain not found. User challenged for PASSCODE.

The user may have entered the domain name incorrectly and will be challenged for a PASSCODE.

User *username*: New PIN accepted.

The user's New PIN was verified.

User *username*: New PIN rejected.

The PIN was rejected by the RSA ACE/Server. The user needs to re-authenticate to set the PIN. Check the RSA ACE/Server Activity Log.

User *username*: Not found. User challenged for PASSCODE.

The user is unknown to the system, but the user will be challenged for PASSCODE anyway.

User *username*: PASSCODE accepted.

The **Challenge All Users** option is not on, and the user is in the designated group.

User *username*: PASSCODE required. All users challenged.

The **Challenge All Users** option is enabled.

User *username*: Reserve password accepted.

User was asked for the reserve password and entered it correctly.

User *username*: Successfully logged on with Next Tokencode.

The Next Tokencode was accepted by RSA ACE/Server and access was granted to the user.

Glossary

access token

A Windows access token is created when a user logs in to the system. The token contains information such as the Windows security ID for the user account and all groups of which the user is a member, privileges, token type (primary or impersonation), and other information. An access token is used in all attempts by the user to access the securable objects in the system.

See also **PDC**.

dial-in

To connect to a computer over a telephone line only, **not** by using ISDN or X.25 lines.

domain

A domain is a name (for example, .**rsasecurity.com**) with which name server records are associated that describe subdomains or hosts. In this context, “domain” does **not** refer to a Windows domain.

Event Viewer Logs

The Event Viewer is the tool you can use to monitor events in your Windows system. Use the Event Viewer to view, manage, and archive the system, security, and application event records (logs). The event-logging service starts automatically when you run Windows.

GINA

The local Graphical Identification and Authentication interface on a Windows machine.

login process

The component that receives the login request from a user and invokes other security services to authenticate and log the user in to the system. These include both the local login process and the remote login process.

Next Tokencode mode

A series of incorrect tokencodes during authentication puts a token into this mode. While in this mode, after a correct code is finally entered, the user is prompted for another tokencode before being allowed access.

New PIN mode

When a user’s token is in this mode, the user is required to have a new PIN in order to gain access.

node secret

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

PASSCODE

The user’s PIN *plus* the current tokencode displayed on the RSA SecurID token. With a PINPAD card, the user enters his or her PIN directly into the token, and the token itself generates the PASSCODE.

PDC

Primary Domain Controller. In a Windows Server domain, the computer running Windows that authenticates domain logins and maintains the directory database for a domain. The PDC tracks changes made to accounts of all computers on a domain. It is the only computer to receive these changes directly. A domain has only one PDC.

PIN

The user's Personal Identification Number. The PIN, along with the tokencode, make up the RSA Security authentication system.

protocol

An agreed-upon convention for inter-computer communications across a network.

RAS

Remote Access Service. A Windows service that provides remote networking for telecommuters and mobile workers. Users can dial in to a RAS host to access their networks for services such as file and printer sharing and electronic mail.

RAS service is available to remote computers running Windows 2000 or Windows XP.

registry

The Windows registry is a database repository for information about a computer's configuration. It is organized in a hierarchical structure, and is comprised of subtrees and their keys, hives, and value entries.

RSA ACE/Agent for Windows

The RSA Security product that protects a Windows host and specific services running on that host. Although the Windows host may be a server with its own clients, to the RSA ACE/Server it is a client looking for authentication service.

RSA ACE/Agent Host

A computer that is protected by the RSA ACE/Agent software to prevent unauthorized access. Designated users of this computer must provide a valid RSA SecurID PASSCODE in order to log in or access services.

RSA ACE/Server

The RSA Security authentication management software running on a TCP/IP-networked host, providing authentication, administration, and audit-trail services. You must have the RSA ACE/Server software running on your network to use the Agent for RSA SecurID authentication.

RSA SecurID token

A hardware device or software application that generates an RSA SecurID tokencode. A time-based token can be an RSA SecurID PINPAD Card, an RSA SecurID Standard Card, an RSA SecurID Key Fob, or an RSA SecurID Software Token.

%SYSTEMROOT%

The root directory of a Windows machine. This directory contains critical data used by the operating system. This directory is usually named **windows** or **winnt**.

sdtest

The utility that displays the contents of the **sdconf.rec** file on an RSA ACE/Agent Host and lets you test authentication between the Agent and the RSA ACE/Server.

sdconf.rec

The configuration file that must be copied from the RSA ACE/Server Primary Server to its Agent Hosts running RSA ACE/Agent software.

sdlog

The encrypted audit trail database for RSA ACE/Server 2.X or later. It is more detailed than the Windows Event Details log. For RSA ACE/Server 1.X, this information is stored in a file named **log.rec**.

security host

The Microsoft term for a third-party authentication program like RSA ACE/Agent for Windows.

SDGINA

The RSA Security implementation of the local Graphical Identification and Authentication (GINA) interface on a Windows computer. Also referred to as Local access authentication.

SDRAS

The RSA Security implementation of the Remote Access Service (RAS) on Windows 2000 and Windows XP. Also referred to as Remote Access Authentication.

station

A dial-in client of a Windows workstation. A station can be a remote PC running Windows 2000, Windows XP, or Windows 98. RSA SecurID prompts are displayed if the workstation is protected by RSA SecurID.

tokencode

The code displayed by an RSA SecurID token. Together, the tokencode and the PIN comprise the RSA SecurID two-factor authentication.

two-factor authentication

The authentication method used by the RSA ACE/Server system. The user must enter a secret, memorized personal identification number (PIN) *plus* the current tokencode generated by the user’s assigned RSA SecurID token. With a PINPAD token, the user enters his or her PIN directly into the token, and then the token generates the PASSCODE.

Index