

RSA ACE/Agent 5.6 for Windows Installation and Administration Guide



Contact Information

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

RSA Security Inc.
www.rsasecurity.com

RSA Security Ireland Limited
www.rsasecurity.ie

Trademarks

ACE/Agent, ACE/Server, Because Knowledge is Security, BSAFE, ClearTrust, Keon, RC2, RC4, RC5, RSA, the RSA logo, RSA Secured, RSA Security, SecurCare, SecurID, Smart Rules, The Most Trusted Name in e-Security, and Virtual Business Units are registered trademarks, and e-Titlements, the RSA Secured logo, SecurWorld, and Transaction Authority are trademarks of RSA Security Inc. in the U.S. and/or other countries. All other trademarks mentioned herein are the property of their respective owners.

License agreement

This software and the associated documentation are proprietary and confidential to RSA Security, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright below. This software and any copies thereof may not be provided or otherwise made available to any other person.

Neither this software nor any copies thereof may be provided to or otherwise made available to any third party. No title to or ownership of the software or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by RSA Security.

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.

Contents

Preface	7
Audience	7
Documentation	7
Getting Support and Service	7
Chapter 1: Requirements and Preparations	9
Overview	9
Local Access Authentication Platforms and Requirements	10
Remote Access Authentication Platforms and Requirements.....	10
RRAS Without EAP Using a Post-Dial Terminal Based Connection	11
RRAS With RSA Security EAP	12
IAS With RSA Security EAP	14
Wireless LAN Access Authentication Platforms and Requirements	16
RSA ACE/Server Platforms and Requirements.....	17
Preparations.....	17
Set Up the RSA ACE/Server	17
Create Groups of Users to Challenge With RSA SecurID	18
Prepare RSA SecurID Users	18
Chapter 2: Installing RSA ACE/Agent 5.6 for Windows	21
Step 1: Install RSA ACE/Agent 5.6 for Windows.....	21
Installing RSA ACE/Agent 5.6 for Windows Directly.....	22
Creating a Silent Mode Installation	24
Step 2: Start the RSA ACE/Agent Control Panel	25
Step 3: Verify Your Environment.....	25
Verifying the Status of the RSA ACE/Server.....	25
Testing Authentication.....	27
Next Steps	28
Chapter 3: Configuring Local Access Authentication	29
Step 1: Configure the RSA ACE/Agent.....	29
Step 2: Set a Reserve Password	31
Chapter 4: Configuring Remote Access Authentication	33
Configuring RRAS Without EAP	34
Step 1: Configure the RSA ACE/Agent	34
Next Steps	35
Configuring RRAS With RSA Security EAP	36
Step 1: Set up Groups in Microsoft Active Directory	36
Step 2: Configure the RSA ACE/Agent on the RRAS Server.....	36
Step 3: Configure the RRAS Server for RSA Security EAP	37
Next Steps	38

Configuring IAS With RSA Security EAP	39
Step 1: Set up Groups in Microsoft Active Directory	39
Step 2: Configure the RSA ACE/Agent on the IAS Server	39
Step 3: Configure the IAS Server for RSA Security EAP	40
Next Steps	41
Configuring Wireless LAN Access Authentication With PEAP	41
Step 1: Set Up Your Wireless LAN Environment	41
Step 2: Set up Groups in Microsoft Active Directory	42
Step 3: Configure the RSA ACE/Agent	42
Step 4: Configure the IAS Server for PEAP	43
Next Steps	43
Configuring the Desktops	44
Configuring Post-Dial Terminal Based Authentication Without EAP	44
Installing the RSA Security EAP on Desktop Computers	44
Configuring Desktops for RSA Security EAP	45
Configuring Desktops for PEAP	46
Authenticating from Remote Computers	46
Chapter 5: Configuring Advanced Settings	49
Clearing and Replacing the Node Secret	50
Setting an IP Address Override	51
Filtering Event Messages Out of the Windows Event Viewer Log	52
Tracing and Logging Agent Code Activity	52
Changing the Time-Out Values	53
Chapter 6: Troubleshooting	55
Specific Authentication Problems	55
Users Receive Error Messages During Authentication	55
Remote Access Prompts Time Out Too Soon	55
Test Authentication Succeeds But Actual Authentication Fails	56
Node Verification Fails	56
General Authentication Problems	57
Verify the Accuracy of the PC Clock	57
Verify the sdconf.rec File	57
Windows Troubleshooting	57
RSA ACE/Agent Error and Event Viewer Log Messages	58
Chapter 7: Upgrading to and Uninstalling RSA ACE/Agent 5.6 for Windows	69
Upgrading to RSA ACE/Agent 5.6 for Windows	69
Uninstalling RSA ACE/Agent 5.6 for Windows	69
Removing Shared Programs	69

Appendix A: Load Balancing with the sdopts.rec File	71
Creating an sdopts.rec File	71
An Example Featuring the USESERVER Keyword	74
Examples Featuring the ALIAS, ALIASES_ONLY, and IGNORE_ALIASES Keywords	75
Using the Client_IP Keyword to Set an Overriding IP Address	76
Maintaining the Primary IP Address of the Agent Host in the RSA ACE/Server	77
Appendix B: Automated Registration of Agent Hosts in the RSA ACE/Server Database	79
Appendix C: Local Authentication with Third-Party Products	81
Appendix D: Using Windows Groups with RSA Security EAP	83
Step 1: Create a New Group in Active Directory	83
Step 2: Create a New Remote Access Policy	83
Index	85

Preface

This book explains how to install and administer RSA ACE/Agent 5.6 for Windows. RSA ACE/Agent 5.6 for Windows works with the RSA ACE/Server to enhance native Windows security by integrating the strong, two-factor authentication of time-based RSA SecurID tokens.

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 general users.

Documentation

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 5.6 for Windows Readme*. This file is named **readme.html** and is located in the **\Aceclnt\nt_i386** directory of the RSA ACE/Agent 5.6 for Windows zip file.

Getting Support and Service

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

1

Requirements and Preparations

Overview

RSA ACE/Agent 5.6 for Windows works with the RSA ACE/Server to enhance native Windows security with the strong, two-factor authentication of time-based RSA SecurID tokens. Specifically, RSA ACE/Agent 5.6 for Windows protects

- Local login to desktops on the network.
This feature set is called Local Access Authentication. For more information, see Chapter 3, [“Configuring Local Access Authentication.”](#)
- Remote post-dial terminal based or a virtual private network (VPN) connections to Microsoft’s Routing and Remote Access Service (RRAS) server.
This feature is part of the Remote Access Authentication component. For more information, see Chapter 4, [“Configuring Remote Access Authentication.”](#)
- Remote wireless connections to a Microsoft Wireless LAN.
RSA ACE/Agent protects remote connections that use Protected EAP (PEAP). This feature is part of the Remote Access Authentication component. For more information, see Chapter 4, [“Configuring Remote Access Authentication.”](#)

RSA Security does not support wireless LAN access authentication using EAP.

RSA ACE/Agent 5.6 for Windows enables local and remote authentication services to send login requests and credentials to an RSA ACE/Server. When a user attempts to establish a remote connection, the RSA ACE/Agent challenges the user for RSA SecurID credentials and sends the credentials to the RSA ACE/Server. Authorized RSA SecurID users establish the connection easily, but unauthorized users are denied.

You can choose to challenge all users, or only specific groups of users.

RSA ACE/Agent can use Windows groups (for example, Domain Users or Dial-in Users), or groups that you create yourself using the Windows Computer Management interface. For more information, see Chapter 3, [“Configuring Local Access Authentication”](#) and Chapter 4, [“Configuring Remote Access Authentication.”](#)

Note: RSA ACE/Agent 5.6 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.

Local Access Authentication Platforms and Requirements

For this solution, you install the Local Access Authentication Client component on each individual desktop. These platforms are supported:

- Windows Server 2003 (Enterprise and Standard)
- Windows 2000 Professional
- Windows 2000 Server
- Windows XP Professional

Important: See the *RSA ACE/Agent 5.6 for Windows Readme* to find out which service packs are required.

Your system must meet the following requirements for successful installation. However, depending on the volume of usage, increased resources may improve performance.

- 128 MB of RAM
- 5 MB of free disk space
- TCP/IP networking

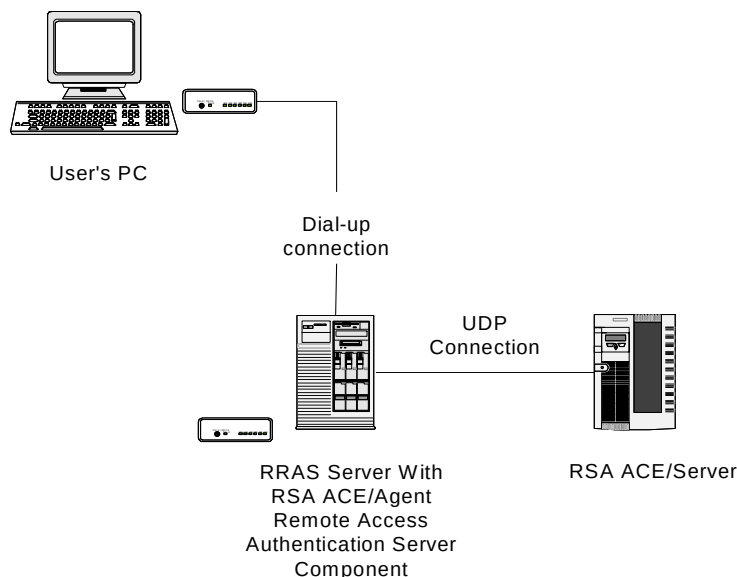
Remote Access Authentication Platforms and Requirements

You can configure these Remote access authentication solutions:

- Routing and Remote Access Service (RRAS) server without EAP using a post-dial terminal based connection
- Routing and Remote Access Service (RRAS) server with RSA Security EAP using either a post-dial terminal based connection or a VPN connection.
- Internet Authentication Service (IAS) server with RSA Security EAP using either a post-dial terminal based connection or a VPN connection.

RRAS Without EAP Using a Post-Dial Terminal Based Connection

The following figure shows the setup for RRAS without EAP in a post-dial terminal based environment.



These platforms are supported:

Servers	Clients
- Windows Server 2003 (Enterprise and Standard) - Windows 2000 Server	Does not apply for this solution

Important: See the *RSA ACE/Agent 5.6 for Windows Readme* to find out which service packs are required.

Your system must meet the following requirements for successful installation. However, depending on the volume of usage, increased resources may improve performance.

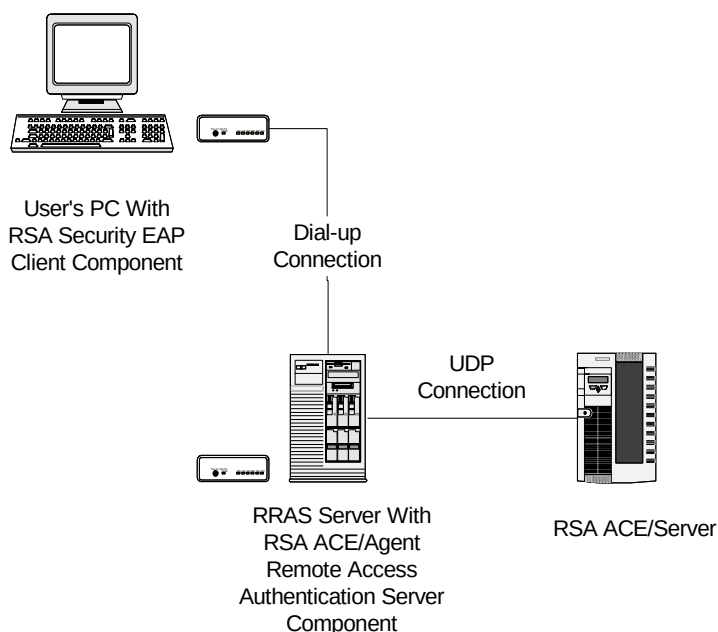
- 128 MB of RAM.
- 5 MB of free disk space.
- TCP/IP networking.
- Dial-in access enabled.
- The RRAS server should be physically inaccessible to unauthorized persons. Otherwise, someone could unload the RSA ACE/Agent .dll files and eliminate RSA SecurID authentication.

- The device that handles incoming RRAS connections (for example, your modem) must be connected to a port that the RRAS 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 users (or a Software Token automated logon script) can respond to the **Username** and **PASSCODE** authentication prompts.

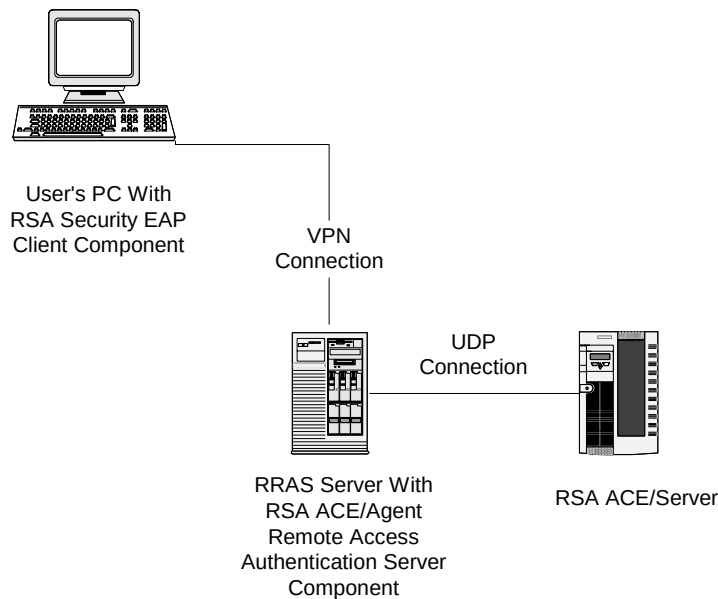
RRAS With RSA Security EAP

You can use RRAS with RSA Security EAP in post-dial terminal based or VPN environments.

The following figure shows the setup for RRAS with RSA Security EAP in a post-dial terminal based environment.



The following figure shows the setup for RRAS with EAP in a VPN environment:



These platforms are supported:

Servers	Clients
- Windows Server 2003 (Enterprise and Standard) - Windows 2000 Server	- Windows Server 2003 - Windows 2000 Professional - Windows 2000 Server - Windows XP Professional

Important: See the *RSA ACE/Agent 5.6 for Windows Readme* to find out which service packs are required.

Your system must meet the following requirements for successful installation. However, depending on the volume of usage, increased resources may improve performance.

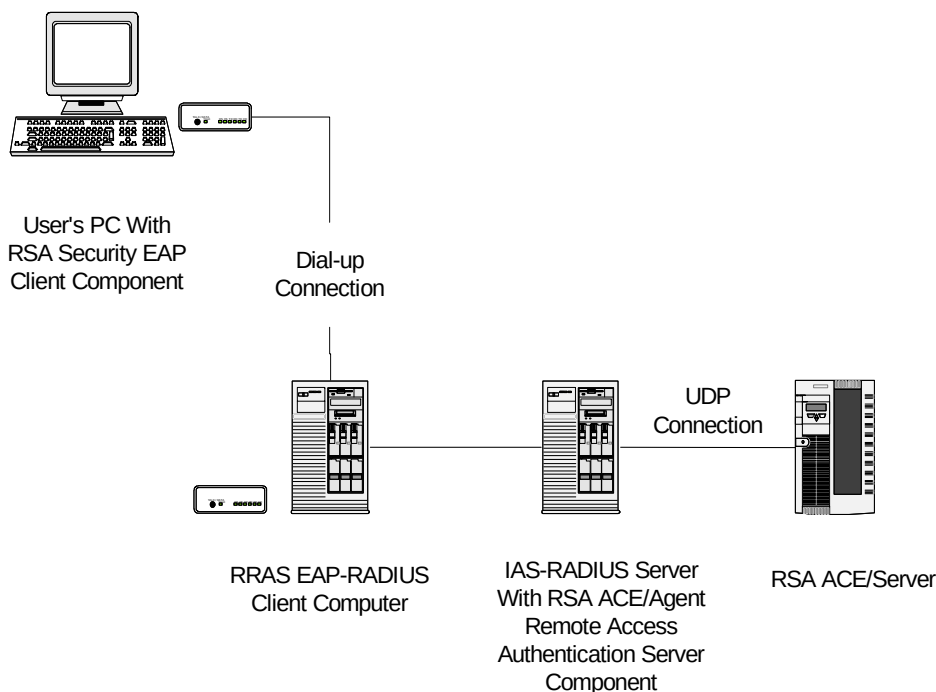
- 128 MB of RAM.
- 5 MB of free disk space.
- TCP/IP networking.
- Dial-in access enabled.
- The RRAS server should be physically inaccessible to unauthorized persons. Otherwise, someone could unload the RSA ACE/Agent .dll files and eliminate RSA SecurID authentication.

- The device that handles incoming RRAS connections (for example, your modem) must be connected to a port that the RRAS 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 users (or a Software Token automated logon script) can respond to the **Username** and **PASSCODE** authentication prompts.

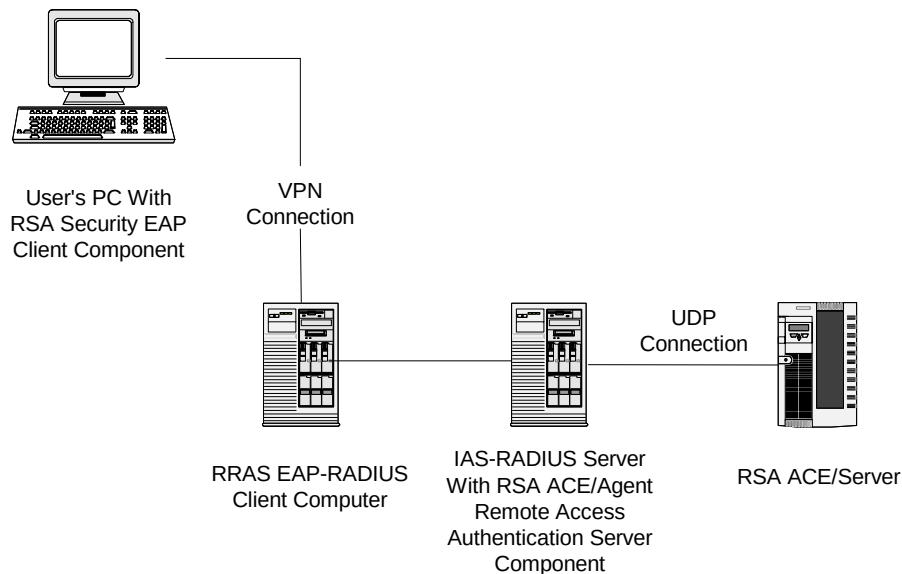
IAS With RSA Security EAP

You can use IAS with RSA Security EAP in either a post-dial terminal based or VPN environment.

The following figure shows the setup for IAS with EAP in a post-dial terminal based environment:



The following figure shows the setup for IAS with EAP in a VPN environment:



These platforms are supported:

Servers	Clients
- Windows Server 2003 (Enterprise and Standard) - Windows 2000 Server	- Windows Server 2003 - Windows 2000 Professional - Windows 2000 Server - Windows XP Professional

Important: See the *RSA ACE/Agent 5.6 for Windows Readme* to find out which service packs are required.

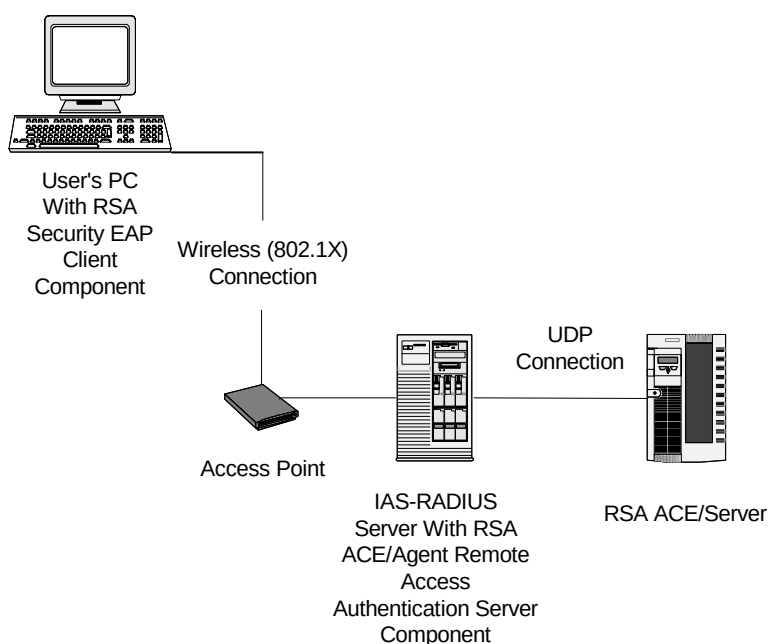
Your system must meet the following requirements for successful installation. However, depending on the volume of usage, increased resources may improve performance.

- 128 MB of RAM.
- 5 MB of free disk space.
- TCP/IP networking.
- Dial-in access enabled.
- The RRAS server should be physically inaccessible to unauthorized persons. Otherwise, someone could unload the RSA ACE/Agent .dll files and eliminate RSA SecurID authentication.

- The device that handles incoming RRAS connections (for example, your modem) must be connected to a port that the RRAS 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 users (or a Software Token automated logon script) can respond to the **Username** and **PASSCODE** authentication prompts.

Wireless LAN Access Authentication Platforms and Requirements

The following figure shows the setup for a wireless environment:



These platforms are supported:

Servers	Clients
• Windows Server 2003 (Enterprise and Standard)	• Windows XP Professional

Important: See the *RSA ACE/Agent 5.6 for Windows Readme* to find out which service packs are required.

Your system must meet the following requirements for successful installation. However, depending on the volume of usage, increased resources may improve performance.

- 128 MB of RAM
- 5 MB of free disk space
- TCP/IP networking
- Computers that act as clients must have wireless LAN cards that support 802.1X PEAP, and computers that act as servers must have connections to access points that support 802.1X PEAP.

RSA ACE/Server Platforms and Requirements

RSA ACE/Agent 5.6 works with currently supported versions of RSA ACE/Server.

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. For information about these or any RSA ACE/Server administration tasks, see the RSA ACE/Server documentation, or contact your RSA ACE/Server administrator.

Preparations

This section describes tasks you must perform before you can use RSA ACE/Agent 5.6 for Windows.

Set Up the RSA ACE/Server

Before you use RSA ACE/Agent, you or your RSA ACE/Server administrator must complete these tasks:

- If you have not already done so, install the RSA ACE/Server. For instructions, see your RSA ACE/Server documentation.
- Copy the configuration **sdconf.rec** file from the RSA ACE/Server to the **%SYSTEMROOT%\system32** directory on the computer on which you plan to install RSA ACE/Agent.
- Verify that the RSA ACE/Server is available.
- Register the RSA ACE/Agent Host as an Agent of the RSA ACE/Server. See [“Automated Registration of Agent Hosts in the RSA ACE/Server Database”](#) on page 79.

Note: You can provide an IP address override for the Agent if you install it on a multi-homed server. See [“Setting an IP Address Override”](#) on page 51.

- Register RSA SecurID users in the RSA ACE/Server database and distribute RSA SecurID tokens to those users.
- Determine whether the usernames in the RSA ACE/Server database records have the users' Windows domain names attached (for example, **DOMAIN\username**).

Create Groups of Users to Challenge With RSA SecurID

You determine the degree to which Windows resources are protected by specifying which users are challenged by RSA SecurID. You can configure RSA ACE/Agent to challenge:

- All users
- A group of users
- All users except a certain group of users

The RSA ACE/Agent uses Windows groups to control access to computers. These groups can be default Windows groups (for example, Domain Users or Dial-in Users), or groups that you create yourself using the Windows Computer Management interface.

If you want to use groups other than the Windows default groups, you need to create them before you configure RSA ACE/Agent. For instructions on creating groups, see your Windows documentation. For instructions on how to specify which users are challenged, see Chapter 3, “[Configuring Local Access Authentication](#)” and Chapter 4, “[Configuring Remote Access Authentication](#).”

Note: RSA Security EAP challenges all users. If you are using RSA Security EAP and want to exempt groups of users from the challenge, you must create the groups in Microsoft Active Directory, and create a remote access policy that uses a version of EAP other than RSA Security EAP for those groups. For information, see Appendix D, “[Using Windows Groups with RSA Security EAP](#).”

Prepare RSA SecurID Users

Before you use RSA ACE/Agent 5.6 for Windows, prepare your RSA SecurID users in these ways:

- Register users who will be challenged for passcodes as RSA SecurID users in the RSA ACE/Server database, and activate their tokens. For instructions, see the RSA ACE/Server documentation.

Important: The Windows usernames for RSA SecurID users must be registered in the RSA ACE/Server database. These usernames **cannot** contain spaces and **must not** exceed forty characters. Run the Computer Management application in the Administrative Tools to register the usernames to the Windows system.

- Give assigned and enabled tokens to users who will be challenged for passcodes.
- Tell users who will be challenged remotely how to configure their remote computers, and how to authenticate. These sections contain information you may want to copy and distribute to users:
 - [“Configuring the Desktops”](#) on page 44
 - [“Authenticating from Remote Computers”](#) on page 46

2

Installing RSA ACE/Agent 5.6 for Windows

This chapter describes how to install and start RSA ACE/Agent 5.6 for Windows, and verify your authentication environment.

Warning: Installing RSA ACE/Agent 5.6 for Windows removes both the Network and Web access authentication components from previous versions. If you are currently running either RSA ACE/Agent 5.0, or RSA ACE/Agent 4.x with Network and Web authentication components, and you want to continue using these features, do not install RSA ACE/Agent 5.6 for Windows.

Step 1: Install RSA ACE/Agent 5.6 for Windows

There are two types of installations:

- A direct installation which prompts installers for setting information.
If you want to install RSA ACE/Agent directly, see the following section, [“Installing RSA ACE/Agent 5.6 for Windows Directly.”](#)
- A silent mode installation which an administrator creates, then distributes to other people (for example, IT personnel or end users) to install. The administrator preconfigures the installation settings so installers are not prompted for the information during the installation.
If you want to create a silent installation, see [“Creating a Silent Mode Installation”](#) on page 24.

For Local access authentication, you install the Local Access Authentication Client component on each desktop you want to protect with RSA SecurID. Every desktop connects directly to the RSA ACE/Server, and every desktop has the RSA ACE/Agent control panel.

For Remote access authentication, you install the Remote Access Authentication (Server) component on your server (for example, the IAS server). If you are using EAP or PEAP, you install the RSA Security EAP client component on each desktop. The desktops do not connect directly to the RSA ACE/Server, and they do not require the RSA ACE/Agent control panel. Although the system allows you to install the control panel on Remote access authentication client computers, RSA Security recommends that you do not install the control panel unless you are instructed to do so by an RSA Security support representative.

To install the Agent, you must be an administrator on the host computer.

Installing RSA ACE/Agent 5.6 for Windows Directly

This table summarizes what you need to install for each solution and where to install it.

Authentication Method	What to Install	Where to Install
Local access authentication	Local Access Authentication (Client) component	Each desktop
RRAS without EAP in a post-dial terminal based environment	Remote Access Authentication (Server) component	RRAS server
RRAS with EAP in a post-dial terminal based or VPN environment	Remote Access Authentication (Server) component	RRAS server
	RSA Security EAP Client component	Each desktop
IAS with EAP in a post-dial terminal based or VPN environment	Remote Access Authentication (Server) component	IAS server
	RSA Security EAP Client component	Each desktop
Wireless PEAP	Remote Access Authentication (Server) component	IAS server
	RSA Security EAP Client component	Each desktop

RSA ACE/Agent 5.6 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 put it in a directory on your network that is accessible to all machines on which you will install the RSA ACE/Agent 5.6 for Windows.

To install RSA ACE/Agent 5.6 for Windows:

1. Log in to your system as an administrator.
2. If you are running the Windows RRAS service, stop the service.
3. In the **Aceclnt\nt_i386** directory, double-click **Agent.exe**.
The **RSA ACE/Agent 5.6 for Windows Setup** screen opens, and the installation wizard starts.
4. Follow the instructions on your screen to advance through the Welcome dialog and accept the Software License Agreement.

5. At the **Select Components** screen, select the components you want to install.

Component	Purpose
Local Access Authentication (Client)	Enables RSA SecurID protection for local logins to this computer. When you select this component, the Common Shared Files component is automatically selected.
SecurID Challenge Before Logon	Prompts a user performing a local authentication with an RSA SecurID challenge <i>before</i> the user is prompted for Windows login information. Important: When you select this component, the Agent automatically challenges all users, including administrators. Additionally, when you select this component, you cannot use reserve passwords. If you select this component, and there is a problem that interrupts communication with the RSA ACE/Server, all users will be locked out of their desktops.
Remote Access Authentication (Server)	Installs the Remote Access Authentication (Server) component. When you select this component, the Common Shared Files component is automatically selected.
RSA Security EAP Client	Installs the RSA EAP Client component. To enable EAP, you must install this component on all remote access client machines.
Common Shared Files	Installs the shared program files (for example, .dll files) that are used by all the RSA ACE/Agent components. When you select the Local Access Authentication (Client) component, or the Remote Access Authentication (Server) component, this component is automatically selected.
Administration Guide and Documentation	(Optional) Copies the <i>RSA ACE/Agent 5.6 for Windows Installation and Administration Guide</i> to the %SYSTEMROOT%\system32\Aaceclnt directory. Check the <i>RSA ACE/Agent 5.6 for Windows Readme</i> for up-to-date information about the documentation set. The <i>RSA ACE/Agent 5.6 for Windows Readme</i> file is named readme.html and is located in the \Aaceclnt\nt_i386 directory.
Control Panel Applet	Installs the RSA ACE/Agent control panel. When you select the Local Access Authentication (Client) component, or the Remote Access Authentication (Server) component, this component is automatically selected. Do not select this component if you are installing the RSA Security EAP Client component unless you are instructed to do so by RSA Security Customer Support.

6. Click **Next**, and follow the instructions on the screen to complete the installation. If you choose not to register the software immediately after installing it, you can register later by clicking **Start > Programs > RSA ACE/Agent > Register**.
7. Reboot the computer.

Creating a Silent Mode Installation

A silent mode installation requires no interaction from the installer. An administrator uses a set of scripts to create installation files, then distributes the installation files to others (such as IT personnel or end users) to install. The administrator pre-configures the installation settings so installers are not prompted for the information during the installation. In large organizations, this installation method is faster, less confusing, and results in fewer errors.

The file **server.iss** contains comments to help you create silent mode installation scripts. The **server.iss** file is located in the **\Aceclnt\nt_i386** directory in the RSA ACE/Agent 5.6 for Windows **.zip** file.

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

If you are upgrading from a previous version, the installation program automatically selects the components to match those in the previous installation. If you want to remove components, you must uninstall the previous installation.

You must decide how to distribute the silent mode installation files (for example, as a batch file, login script, mail message, or other), and tell users how to run the silent mode installation. You also may want to tell IT personnel or end users how to configure their own client computers. These sections contain information you may want to copy and distribute:

- [“Configuring the Desktops”](#) on page 44
- [“Authenticating from Remote Computers”](#) on page 46

To create a silent mode installation:

In this procedure, the silent installation directory is referred to as **Install_Dir**.

1. Copy the **agent.exe**, and **server.iss** files from the **\Aceclnt\nt_i386** directory of the RSA ACE/Agent 5.6 for Windows **.zip** file 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 Uniform Naming Convention (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.

6. Use this command in your installation method (batch file, login script, mail message, or other):

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

For information about the command options, see your InstallShield documentation.

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

Step 2: Start the RSA ACE/Agent Control Panel

You configure Local and Remote access authentication and advanced settings through the RSA ACE/Agent control panel.

Regardless of which features you installed, the control panel has a **Main** tab and an **Advanced** tab. The **Installed RSA Agents** section on the **Main** tab lists all RSA Security Agents installed on the Agent Host. You can install more than one Agent on the same computer.

If you installed the Local Access Authentication (Client) and Remote Access Authentication (Server) components, the control panel has corresponding **Local** and **Remote** tabs. If you expect either the Local access authentication or Remote access authentication features to be available, but the corresponding tab is missing, verify which features you installed and enabled.

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 labeled tabs to view the properties sheet for each available feature set.

Step 3: Verify Your Environment

Verifying your environment includes verifying the status of the RSA ACE/Server, and testing authentication.

Verifying the Status of the RSA ACE/Server

The following procedure enables you to view information about the RSA ACE/Server that verifies whether the Agent Host has been properly registered in the RSA ACE/Server database, and whether a network connection between the RSA ACE/Server and the Agent Host can be established.

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 shows the following information:

- **Configuration Version.** The version of the **sdconf.rec** file that is in use. When this file is created by a version 5.0 Server or later, this number is 12 or higher.
- **DES Enabled.** Whether your configuration environment supports legacy protocols. If it does, the value is **YES**.
- **Client Retries.** The number of times the Agent sends authentication data to the RSA ACE/Server before a time-out occurs.
- **Client Timeout.** The amount of time (in seconds) that the Agent waits before resending authentication data to the Server.
- **Server Release.** The version number of the RSA ACE/Server.

The **Server Release** field may be blank. The version number of the RSA/ACE Server becomes available only after you use the RSA ACE/Agent to authenticate to the RSA ACE/Server. If you are using an RSA ACE/Server that is version 5.0 or earlier, the **Server Release** field does not display the version number.

- **Communication.** The version of the protocol used for communication between the Server and the Agent.

If you have questions about 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** section lists each RSA ACE/Server that is known to the Agent. When you select a Server from this list, if an alias IP address has been assigned to the Server, it appears in the **Server Alias Addresses** panel.
- The **Server Information** section shows the type of the RSA ACE/Server (Master, Slave, or Primary) you selected from the list. The Server Active Address is the IP address that the Agent uses to communicate with the RSA ACE/Server. This address could be the actual IP address of the RSA ACE/Server you have selected, or it could also be an alias IP address assigned to the RSA ACE/Server. The address "00.000.00.00" indicates that the Agent has not yet received communication from the RSA ACE/Server.
- The **Server Usage** section indicates any of the following conditions.
 - **Available for Authentications.** The selected RSA ACE/Server is used for authentications.
 - **Unused.** The selected RSA ACE/Server is not used for authentications.
 - **For Failover only.** The selected RSA ACE/Server has been reserved for failover use only.
 - **Default Server during initial requests.** The selected RSA ACE/Server is used, since no other server is available.

Testing Authentication

Authentication instructions for each of your token types are provided in the **aceservdoc** directory on the RSA ACE/Server CD. The instructions are available in both Microsoft Word and PDF format (**ace_authentication.doc** and **ace_authentication.pdf**). If you are using RSA SecurID Software Token 2.0, read 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.

RSA Security recommends that you test authentication only when the challenge option is set to **OFF**. If you installed RSA ACE/Agent 5.6 as an upgrade, the 5.6 installation retains the challenge option setting from the previous installation.

Note: This test verifies only the ability to connect to the RSA ACE/Server, and does not verify the validity of the test credentials. Therefore, the owner of the test token does not have to be assigned to 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 Test Directly**.
The RSA SecurID Authentication dialog box opens.
3. On the **Choose Token** list, select **SecurID Card**.
4. In the **Enter Username** field, enter the username of the registered RSA SecurID user assigned to the token.
5. In the **Enter PASSCODE** field, enter the passcode (the PIN followed by the tokencode generated by the RSA SecurID token).
6. Click **OK**.
If the system is correctly implemented and configured, it displays a message that the user was authenticated successfully.
If you see other messages, see the RSA ACE/Server documentation for more information.

To test authentication on a token that does not have 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.
If you have questions about any of the information, ask your RSA ACE/Server administrator.
2. Click **RSA ACE/Server Test Directly**.
The RSA SecurID Authentication dialog box opens.
3. On the **Choose Token** list, select **SecurID Card**.
4. In the **Enter Username** field, enter the username of the registered RSA SecurID user assigned to the token.
5. In the **Enter PASSCODE** dialog box, enter the tokencode generated by your RSA SecurID token, then click **OK**.
If the system is correctly implemented and configured, it displays a message that the user must create or be assigned a new PIN.
If you see other messages, see the RSA ACE/Server documentation for more information.
6. 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.
7. In the **Enter Username** field, enter the username of the registered RSA SecurID user assigned to the RSA SecurID token you are using.
8. In the **Enter PASSCODE** field, enter the passcode (the PIN followed by the tokencode generated by your RSA SecurID token).
9. Click **OK**.

Next Steps

Configure the features you installed. For:

- Local access authentication, see Chapter 3, "[Configuring Local Access Authentication](#)."
- Remote access authentication, see Chapter 4, "[Configuring Remote Access Authentication](#)."

3

Configuring Local Access Authentication

The Local Access Authentication component authenticates RSA SecurID users who attempt to log in to desktops that are on the network. After a user enters his or her Windows username, the Agent prompts the user to enter a valid RSA SecurID passcode. Authorized RSA SecurID users gain access easily, but unauthorized users are denied access to the desktop.

Local access authentication also supports authentications to any computer running the Windows XP Remote Desktop service. In this environment, users can be challenged by RSA SecurID when accessing a remote machine running the Desktop service.

If the Local Access Authentication component is installed, the control panel has a **Local** tab. The Local properties sheet controls local access security.

Step 1: Configure the RSA ACE/Agent

You can configure Local access authentication to challenge:

- All users
- Only members of an administrator-designated group
- All users *except* members of a designated group

These group deployments are supported:

- Local groups in the Security Accounts Manager of a local computer, including all users in the local group, and all users in a domain global group that is part of the local group
- Domain local groups that are part of a domain into which a user is logged, including all users in the local group, and all users in the domain global group that is part of the local group
- Domain global groups that are part of a domain into which a user is logged, including all users in that domain group.

Domain trust groups are not supported. RSA Security recommends that you test all group environments to ensure that they work properly with RSA SecurID.

To configure Local Access Authentication:

1. In the RSA ACE/Agent control panel, click the **Local** tab.
2. Under **Challenge**, select the users you want to challenge.

Users to challenge	Steps
No users	Select OFF on the Challenge list.
All users who log in locally	Select All users on the Challenge list.
A group of users who log in locally	Select 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	Select All users except on the Challenge list, and then select the local or domain group that you do not want to challenge.

Note: If you select **All Users** on the **Challenge** list, the **Reserve Password** feature is automatically selected. If you enable the challenge **All Users** feature without setting a reserve password and there is a problem that interrupts communication with the RSA ACE/Server, all users, including administrators, are locked out of their desktops. For this reason, always set a reserve password when you enable the **Challenge All Users** feature. For more information, see the following section, [“Step 2: Set a Reserve Password.”](#)

3. If your RSA ACE/Server database records include users' Windows domain names as part of their usernames (for example, **DOMAIN\jsmith** instead of just **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 Windows Control Panel.
5. Click **OK**.
6. Restart the computer.

Step 2: Set a 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.

If there is a problem that interrupts communication with the RSA ACE/Server, RSA SecurID users cannot access their desktops. This could present a problem if you challenge all users for their passcodes.

You can avoid this problem by configuring your system in any of these 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 compromises security by creating an account with full access, but with 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 the machine and disable network logins to the machine. If a problem occurs, the machine can be used to disable the requirement for passcode authentication.
- Use the Reserve Password feature. If you have enabled the reserve password feature, 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 prompts the user 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 feature and reveal the password to a user, change the reserve password as soon as the user has logged in 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. You cannot modify the reserve password by using the Windows system tools for manipulating user passwords.

Important: Reserve passwords are not used if you have installed the **SecurID Challenge Before Logon** component.

To enable the reserve password:

1. In the RSA ACE/Agent control panel, click the **Local** tab.
2. Select a challenge option other than **OFF**.
3. Click **Enable Reserve Password**.
4. In the **Password** field, enter the reserve password.

The password must be between 6 and 12 characters, and must contain at least one digit and one letter.

Note: Reserve passwords are case-sensitive.

5. Reenter the password in the **Confirm** field, and click **Apply**.
6. To test that the Reserve Password feature is enabled, disconnect the network connection to the RSA ACE/Agent computer, log out, and log back in. You are prompted to enter the reserve password.
If the test fails, reboot the Agent Host and repeat the test.

To clear the reserve password:

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

4

Configuring Remote Access Authentication

The Remote Access Authentication (Server) component authenticates RSA SecurID users who attempt to establish remote connections to corporate network resources. When a user attempts to establish a remote connection, the RSA ACE/Agent prompts the user for RSA SecurID credentials. Authorized RSA SecurID users gain access easily, but unauthorized users are denied access to the RRAS gateway.

If the Remote Access Authentication (Server) component is installed, the control panel has a **Remote** tab. The Remote properties sheet controls the security of RRAS accounts.

This chapter tells you how to configure these Remote access authentication solutions:

- RRAS without EAP in a post-dial terminal based environment. See the following section, [“Configuring RRAS Without EAP.”](#)
- RRAS with RSA Security EAP in a post-dial terminal based or VPN environment. See [“Configuring RRAS With RSA Security EAP”](#) on page 36.
- IAS with RSA Security EAP in a post-dial terminal based or VPN environment. See [“Configuring IAS With RSA Security EAP”](#) on page 39.
- Wireless LAN access authentication with PEAP. See [“Configuring Wireless LAN Access Authentication With PEAP”](#) on page 41.

RSA Security does not support wireless LAN access authentication with EAP.

RRAS without EAP supports these challenge options:

- All users
- Only members of an administrator-designated group
- All users *except* members of a designated group

However, RSA Security EAP challenges all users and does not support challenge options. For information on how to use groups to determine which users are challenged using RSA Security EAP, see Appendix D, [“Using Windows Groups with RSA Security EAP.”](#)

Configuring RRAS Without EAP

This section describes how to configure RRAS without EAP in a post-dial terminal based environment. You may want to use this method instead of EAP because this method does not require you to install software on desktop computers.

In post-dial terminal based environments, only these group deployments are allowed:

- Local groups in the Security Accounts Manager of a local computer, including all users in the local group, and all users in a domain global group that is part of the local group
- Domain local groups that are part of a domain into which a user is logged, including all users in the local group, and all users in the domain global group that is part of the local group
- Domain global groups that are part of a domain into which a user is logged, including all users in that domain group.

Domain trust groups are not supported. RSA Security recommends that you test all group environments to ensure that they work properly with RSA SecurID.

Step 1: Configure the RSA ACE/Agent

To configure the RSA ACE/Agent on the RRAS server:

1. In the RSA ACE/Agent control panel, click the **Remote** tab.
2. Check **Use Post-dial terminal based Authentication**.
This option sets the Remote access authentication method to post-dial terminal based authentication. Use this method if you do not want to install RSA ACE/Agent software on client desktops.
3. Under **Challenge**, select the users you want to challenge for RSA SecurID passcodes.

Users to challenge	Steps
No users	Select OFF from the Challenge list.
All users	Select All users from the Challenge list.
A group of users	Select 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.
All users except users in a certain group	Select All users except on the Challenge list, and then select the local or domain group that you do not want to challenge.

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 decrease the time it takes a user to log in. However, RSA ACE/Agent 5.6 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 dialog box. The username appears in the **Description** section of the Event Detail dialog box.

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

Note: Selecting this option automatically disables the **Do Not Resolve Username in Event Log Messages** option.

6. If users are allowed to enter usernames that do not include domain names (for example, **jsmith** instead of **DOMAIN\jsmith**), and the RSA ACE/Server uses domain names, check **Send Domain With Username to RSA ACE/Server**. This option converts usernames to NetBIOS format before sending them to the RSA ACE/Server.

Important: At login, users will see only the **USERNAME** and **PASSCODE** prompts. After users enter valid passcodes, they will be authenticated to the default domain. If the RSA ACE/Server records a username in a format other than NetBIOS format or fully qualified domain name format (for example, **jsmith** instead of **DOMAIN\jsmith** or **jsmith@company_name.com**), instruct that user not to use fully qualified domain names.

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.
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**.

Next Steps

Configure the desktops for post-dial terminal based authentication. For instructions, see [“Configuring Post-Dial Terminal Based Authentication Without EAP”](#) on page 44.

Configuring RRAS With RSA Security EAP

The procedures in this section apply for both post-dial terminal based and VPN environments.

Step 1: Set up Groups in Microsoft Active Directory

RSA Security EAP challenges all users. If you are using RSA Security EAP and want to exempt groups of users from the challenge, you must create the groups in Microsoft Active Directory, and create a remote access policy that uses a version of EAP other than RSA Security EAP for those groups. For instructions, see Appendix D, [“Using Windows Groups with RSA Security EAP.”](#)

Step 2: Configure the RSA ACE/Agent on the RRAS Server

To configure the RSA ACE/Agent on the RRAS server:

1. In the RSA ACE/Agent control panel, click the **Remote** tab.
2. Check **Routing and Remote Access Service will use RSA Security EAP**.
This option sets the Remote access authentication method to RSA Security EAP. If you enable this setting
 - All users are automatically challenged for RSA SecurID passcodes.
 - The **Enable “Invalid Username Prompt” During Authentication** and the **Disable Prompting for Domain Name** options are automatically disabled, and you cannot enable them.
3. 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 decrease the time it takes a user to log in. However, RSA ACE/Agent 5.6 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 dialog box. The username appears in the **Description** section of the Event Detail dialog box.
4. If users are allowed to enter usernames that do not include domain names (for example, **jsmith** instead of **DOMAIN\jsmith**), and the RSA ACE/Server uses domain names, check **Send Domain With Username to RSA ACE/Server**.
This option converts usernames to NetBIOS format before sending them to the RSA ACE/Server.
5. If users are allowed to enter fully qualified domain names (for example, **jsmith@company_name.com** instead of **DOMAIN\jsmith**), and the RSA ACE/Server uses NetBIOS format, check **Convert Fully Qualified User Names**.
This option converts fully qualified domain names to NetBIOS format before sending them to the RSA ACE/Server.

Important: If the RSA ACE/Server records a username in a format other than NetBIOS format or fully qualified domain name format (for example, **jsmith** instead of **DOMAIN\jsmith** or **jsmith@company_name.com**), instruct that user not to use fully qualified domain names.

If a user enters a username in the NetBIOS format (**DOMAIN\jsmith**), the **Convert Fully Qualified User Names** option has no effect.

For optimum security, RSA Security recommends that usernames recognized by IAS match the usernames sent to the RSA ACE/Server. To ensure this, check both the **Send Domain Name and User Name to RSA ACE/Server** option and the **Convert Fully Qualified User Names** option.

6. 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.
7. Click **Apply**.

Step 3: Configure the RRAS Server for RSA Security EAP

This section tells how to configure RSA Security EAP on Windows 2000 Server and Windows Server 2003.

To configure the RRAS server to use RSA Security EAP on Windows 2000 Server:

1. Click **Start > Programs > Administrative Tools > Routing and Remote Access**.
The Routing and Remote Access (RRAS) dialog box opens. The console tree appears in the left frame.
2. Right-click the server in the console tree, and click **Properties**.
3. In the Properties dialog box, click the **Security** tab.
4. On the **Authentication Provider** drop-down menu, select **Windows Authentication**.
5. Click **Authentication Methods**.
6. Check **Extensible Authentication Protocol**, and clear all the other methods.
7. Click **OK** to return to the Properties dialog box.
8. On the **Accounting Provider** drop-down menu, select **Windows Accounting**.
9. Click **OK** to return to the console tree.
10. In the console tree, click **Remote Access Policies**.
The policies for this server appear in the right frame of the console.
11. Double-click the **Allow access if dial-in permission is enabled** policy.
12. In the Settings dialog box, click **Edit Profile**.
13. In the Edit Profile dialog box, click the **Authentication** tab.
14. Check **Extensible Authentication Protocol**, and clear all the other methods.

15. On the **EAP type** drop-down menu, select **RSA Security EAP**.
16. Click the **Encryption** tab.
17. Check **Strong**, and clear all other encryption options.
18. Click the **Advanced** tab.
19. Remove all connection attributes from the **Parameters** box.
20. Click **OK**.

To configure the RRAS server to use RSA Security EAP on Windows Server 2003:

1. Click **Start > Programs > Administrative Tools > Routing and Remote Access**.
The Routing and Remote Access (RRAS) dialog box displays. The console tree appears in the left frame.
2. Right-click the server in the console tree, and click **Properties**.
3. In the Properties dialog box, click the **Security** tab.
4. On the **Authentication Provider** drop-down menu, select **Windows Authentication**.
5. Click **Authentication Methods**.
6. Check **Extensible Authentication Protocol**, and clear all the other methods.
7. Click **OK** to return to the Properties dialog box.
8. On the **Accounting Provider** drop-down menu, select **Windows Accounting**.
9. Click **OK** to return to the console tree.
10. In the console tree, click **Remote Access Policies**.
The policies for this server appear in the right frame of the console.
11. Double-click the **Allow access if dial-in permission is enabled** policy.
12. In the Settings dialog box, click **Edit Profile**.
13. In the Edit Profile dialog box, click the **Authentication** tab.
14. Click **EAP Methods**.
15. In the Select EAP Providers dialog box, click **Add**.
16. In the Add EAP Methods dialog box, select **RSA Security EAP** as the method, and click **OK**.
17. Click the **Encryption** tab.
18. Check **Strong**, and clear all other encryption options.
19. Click the **Advanced** tab.
20. In the **Attributes** section, remove all connection attributes.
21. Click **OK**.

Next Steps

Install the RSA Security EAP client on each desktop. For instructions, see [“Installing the RSA Security EAP on Desktop Computers”](#) on page 44.

Configuring IAS With RSA Security EAP

These procedures apply for both post-dial terminal based and VPN environments.

Step 1: Set up Groups in Microsoft Active Directory

RSA EAP challenges all users. If you are using EAP and want to exempt groups of users from the challenge, you must create the groups in Microsoft Active Directory, and create a remote access policy that uses a version of EAP other than RSA Security EAP for those groups. For instructions, see Appendix D, [“Using Windows Groups with RSA Security EAP.”](#)

Step 2: Configure the RSA ACE/Agent on the IAS Server

To configure the RSA ACE/Agent on the IAS Server:

1. In the RSA ACE/Agent control panel, click the **Remote** tab.
2. Check **Routing and Remote Access Service will use RSA Security EAP**.
If you enable this setting
 - All users are automatically challenged for RSA SecurID passcodes.
 - The **Enable Invalid Username Prompt During Authentication** and the **Disable Prompting for Domain Name** options are automatically disabled, and you cannot enable them.
3. 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 decrease the time it takes a user to log in. However, RSA ACE/Agent 5.6 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 dialog box. The username appears in the **Description** section of the Event Detail dialog box.
4. If users are allowed to enter usernames that do not include domain names (for example, **jsmith** instead of **DOMAIN\jsmith**), and the RSA ACE/Server uses domain names, check **Send Domain With Username to RSA ACE/Server**.
This option converts usernames to NetBIOS format, which is the format recognized by IAS, before sending them to the RSA ACE/Server.
5. If users are allowed to enter fully qualified domain names (for example, **jsmith@company_name.com** instead of **DOMAIN\jsmith**), and the RSA ACE/Server uses NetBIOS format, check **Convert Fully Qualified User Names**.
This option converts fully qualified domain names to NetBIOS format before sending them to the RSA ACE/Server.

Important: If the RSA ACE/Server records a username in a format other than NetBIOS format or fully qualified domain name format (for example, **jsmith** instead of **DOMAIN\jsmith** or **jsmith@company_name.com**), instruct that user not to use fully qualified domain names.

If a user enters a username in the NetBIOS format (**DOMAIN\jsmith**), the **Convert Fully Qualified User Names** option has no effect.

For optimum security, RSA Security recommends that usernames recognized by IAS match the usernames sent to the RSA ACE/Server. To ensure this, check both **Send Domain Name and User Name to RSA ACE/Server** option and **Convert Fully Qualified User Names**.

6. 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.
7. Click **Apply**.

Step 3: Configure the IAS Server for RSA Security EAP

This section tells how to configure RSA Security EAP on Windows 2000 Server and Windows Server 2003.

To configure the IAS server to use RSA Security EAP on Windows 2000 Server:

1. Click **Start > Programs > Administrative Tools > Internet Authentication Service**.
The Internet Authentication Service (IAS) dialog box opens. 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 **Allow access if dial-in permission is enabled**.
4. In the Settings dialog box, click **Edit Profile**.
5. In the Edit Profile dialog box, 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**.

To configure the IAS server to use RSA Security EAP on Windows Server 2003:

Note: Before you configure RSA Security EAP on your Microsoft IAS server, see the Microsoft Windows Help for IAS configuration information for your Windows operating system.

1. Click **Start > Programs > Administrative Tools > Internet Authentication Service**.
The Internet Authentication Service (IAS) dialog box displays. 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 **Allow access if dial-in permission is enabled**.
4. In the Settings dialog box, click **Edit Profile**.
5. In the Edit Profile dialog box, click the **Authentication** tab.
6. On the **Authentication** tab, click **EAP Methods**.
7. In the Select EAP Provider dialog box, click **Add**.
8. In the EAP Methods dialog box, select **RSA Security EAP**, and click **OK**.
9. Click the **Encryption** tab.
10. Check **Strong**, and clear all other encryption types.
11. Click the **Advanced** tab.
12. In the **Attributes** section, remove all connection attributes.
13. Click **OK**.

Next Steps

Install the RSA Security EAP client on each desktop. For instructions, see [“Installing the RSA Security EAP on Desktop Computers”](#) on page 44.

Configuring Wireless LAN Access Authentication With PEAP**Step 1: Set Up Your Wireless LAN Environment**

To set up your wireless LAN environment:

- Set up security for the authentication server by defining **802.1X-2001** as the EAP protocol version.
- Define the Microsoft IAS server as the RADIUS server, and specify **EAP Authentication** as the authentication method.
- Add the access point as a RADIUS client in the IAS server.
- Create a 128-bit Radio Data Encryption Wired Equivalent Privacy (WEP) key.

- Define **Full Encryption** as the use of data encryption.
- Select **Open** and **Network-EAP** as the accepted authentication types, and make EAP required.

For specific instructions, see your access point software documentation.

Step 2: Set up Groups in Microsoft Active Directory

RSA Security EAP challenges all users. If you are using RSA Security EAP and want to exempt groups of users from the challenge, you must create the groups in Microsoft Active Directory, and create a remote access policy that uses a version of EAP other than RSA Security EAP for those groups. For instructions, see Appendix D, [“Using Windows Groups with RSA Security EAP.”](#)

Step 3: Configure the RSA ACE/Agent

To configure the RSA ACE/Agent for Remote Access Authentication:

1. In the RSA ACE/Agent control panel, click the **Remote** tab.
2. Check **Routing and Remote Access Service will use RSA Security EAP**. This sets the Remote access authentication method to RSA Security EAP. If you enable this setting
 - All users are automatically challenged for RSA SecurID passcodes.
 - The **Enable “Invalid Username Prompt” During Authentication** and the **Disable Prompting for Domain Name** options are automatically disabled, and you cannot enable them.
3. 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 decrease the time it takes a user to log in. However, RSA ACE/Agent 5.6 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 dialog box. The username appears in the **Description** section of the Event Detail dialog box.
4. If users are allowed to enter usernames that do not include domain names (for example, **jsmith** instead of **DOMAIN\jsmith**), and the RSA ACE/Server uses domain names, check **Send Domain Name With Username to RSA ACE/Server**.
 This option converts usernames to NetBIOS format before sending them to the RSA ACE/Server.
5. If users are allowed to enter fully qualified domain names (for example, **jsmith@company_name.com** instead of **DOMAIN\jsmith**), and the RSA ACE/Server uses NetBIOS format, check **Convert Fully Qualified User Names**.
 This option converts fully qualified domain names to NetBIOS format before sending them to the RSA ACE/Server.

Important: If the RSA ACE/Server records a username in a format other than NetBIOS format or fully qualified domain name format (for example, **jsmith** instead of **DOMAIN\jsmith** or **jsmith@company_name.com**), instruct that user not to use fully qualified domain names.

If a user enters a username in the NetBIOS format (**DOMAIN\jsmith**), the **Convert Fully Qualified User Names** option has no effect.

For optimum security, RSA Security recommends that usernames recognized by IAS match the usernames sent to the RSA ACE/Server. To ensure this, check both the **Send Domain Name With Username to RSA ACE/Server** option and the **Convert Fully Qualified User Names** option.

6. 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.
7. Click **Apply**.

Step 4: Configure the IAS Server for PEAP

To configure the IAS server for PEAP:

1. Click **Start > Programs > Administrative Tools > Internet Authentication Service**.
The Internet Authentication Service (IAS) dialog box opens. The console tree appears in the left frame.
2. In the console tree, right-click **Remote Access Policies**, and select **New Remote Access Policy**.
3. For the policy configuration method, click **Use the wizard to set up a typical policy for a common scenario**, and enter a policy name.
4. For the access method, click **Wireless**.
5. Grant access to the appropriate groups or users.
6. Select **Protected EAP**, and click **Configure**.
7. Click **Add** to assign RSA Security EAP as the EAP type.
8. Click **OK**, and then click **Finish**.

Next Steps

Install the RSA Security EAP client on each desktop. For instructions, see [“Installing the RSA Security EAP on Desktop Computers”](#) on page 44.

Configuring the Desktops

This sections explains how to configure:

- Post-dial terminal based authentication without EAP.
See the following section, [“Configuring Post-Dial Terminal Based Authentication Without EAP.”](#)
- Post-dial terminal based authentication or VPN authentication with EAP.
See [“Configuring Desktops for RSA Security EAP”](#) on page 45.
- Wireless authentication with PEAP.
See [“Configuring Desktops for PEAP”](#) on page 46.

It also explains how to install RSA Security EAP on desktop computers. See [“Installing the RSA Security EAP on Desktop Computers”](#) on page 44.

Important: If you use a software token, you must regularly verify that your PC clock is accurate. If the time on your PC clock drifts from its past setting, you may be unable to authenticate.

Configuring Post-Dial Terminal Based Authentication Without EAP

To configure post-dial terminal based authentication without EAP:

1. Do one of the following:
 - For Windows 2000 Server and Windows 2000 Professional, click **Start > Settings > Network and Dial-up Connections**.
 - For Windows Server 2003 and Windows XP Professional, click **Start > Control Panel > Network Connections > Network Connections**.
2. Right-click the name of your connection, and click **Properties**.
3. On the **Security** tab, check **Show terminal window**.
4. Click **OK**.

Installing the RSA Security EAP on Desktop Computers

To use RSA Security EAP, you need to install the RSA Security EAP Client component on each desktop. To install RSA Security EAP

- You must be an administrator on the desktop computer.
- The desktop computer must be able to access the RSA Security web site to get the RSA EAP installation component. Alternately, you can put the RSA Security EAP installation components in a shared location on the network, or on storage medium such as a floppy diskette or CD.

For instructions on installing the RSA Security EAP component, see [“Step 1: Install RSA ACE/Agent 5.6 for Windows”](#) on page 21. Check only **RSA EAP Client**, and leave all other checkboxes blank.

After you install RSA Security EAP, you must configure the desktops for EAP. For instructions, see the following section, [“Configuring Desktops for RSA Security EAP.”](#)

Configuring Desktops for RSA Security EAP

This section explains how to configure desktop computers for post-dial terminal based connections and VPN connections using RSA Security EAP on:

- Windows 2000 Professional and Windows 2000 Server
- Windows Server 2003 and Windows XP Professional

To configure connections on Windows 2000 Professional and Windows 2000 Server:

1. If you have not already done so, install the RSA Security EAP client component on each desktop.
For instructions, see the preceding section, [“Installing the RSA Security EAP on Desktop Computers.”](#)
2. Click **Start > Settings > Network and Dial-up Connections**.
3. Right-click the name of your connection, and click **Properties**.
4. On the **Securities** tab, select **Advanced**, and then click **Settings**.
5. In the Advanced Security Settings dialog box, in the **Data encryption** menu, click **Optional Encryption**.
6. In the **Logon security** section, select **Use Extensible authentication Protocol (EAP)**.
7. From the drop-down menu, select **RSA SecurityEAP (encryption enabled)**.
8. Click **OK** until you exit all the dialog boxes.

To configure connections on Windows Server 2003 and Windows XP Professional:

1. If you have not already done so, install the RSA Security EAP client component on each desktop.
For instructions, see [“Installing the RSA Security EAP on Desktop Computers”](#) on page 44.
2. Click **Start > Control Panel > Network Connections**.
3. Right-click the name of your connection, and click **Properties**.
4. On the **Securities** tab, select **Advanced**, and then click **Settings**.
5. In the Advanced Security Settings dialog box, in the **Data encryption** menu, click **Optional Encryption**.
6. On the **Authentication** tab, select **RSA Security EAP** as the EAP type.
7. Click **OK**.

Configuring Desktops for PEAP

To configure wireless connections with PEAP on Windows XP Professional:

1. If you have not already done so, install the RSA Security EAP client component on each desktop.
For instructions, see [“Installing the RSA Security EAP on Desktop Computers”](#) on page 44.
2. Click **Start > Control Panel > Network Connections**.
3. Right-click the name of your connection, and click **Properties**.
4. On the **Wireless Networks** tab, select your network and click **Configure**.
5. On the **Association** tab, check **Data Encryption (WEP enabled)** and **The key is provided for me automatically**.
6. On the **Authentication** tab, in the **EAP type** menu, select **Protected EAP (PEAP)**, and click **Properties**.
7. In the Protected EAP Properties dialog box, select **Validate server certificate**, and select **RSA Security EAP** as the authentication method.

Note: You must have a trusted root authority to validate the certificate.

8. Click **OK** until you exit all dialog boxes.

Authenticating from Remote Computers

This section tells how to authenticate from remote computers using these types of connections:

- Post-dial terminal based without EAP
- Post-dial terminal based or VPN with EAP
- Wireless LAN with PEAP

For authentication instructions specific to the types of RSA SecurID tokens you plan to deploy, see the RSA ACE/Server documentation or contact your RSA ACE/Server administrator.

For instructions on changing the default time-out values of RSA SecurID remote access prompts, see [“Changing the Time-Out Values”](#) on page 53.

If you are using RSA Security EAP and a user attempts to establish a remote connection, the system presents the user with a single RSA SecurID prompt in place of the standard Windows Logon screen. Also, the greeting appears only after users successfully authenticate. In previous versions, the greeting appears to all users before they successfully authenticate. If you are using wireless PEAP, the system presents the user with an RSA SecurID username prompt and an RSA SecurID passcode prompt in place of the standard Windows Logon screen.

Initiating a wireless connection causes a Windows balloon tip to appear on the Windows system tray. To continue authentication, users must click the balloon tip. At the authentication prompt, users must enter their usernames within 30 seconds. Otherwise, the balloon tip reappears and users must click it to restart authentication.

By default, the RSA ACE/Agent automatically removes balloon tips that occur at the next prompt while users are entering their passcodes. If you are concerned that automatically removing balloon tips might inadvertently prevent users from responding to other balloon tips that may occur during authentication, rename the file **sdbstop.exe** in the Windows **\System32** directory. For example, rename **sdbstop.exe** to **sdbstop.sav**.

To authenticate with a post-dial terminal based connection without EAP:

1. Log in to your computer using your Windows username and password.
2. Do one of the following:
 - For Windows 2000 Server and Windows 2000 Professional, click **Start > Settings > Network and Dial-up Connections**.
 - For Windows 2003 Server and Windows XP Professional, click **Start > Control Panel > Network Connections**.
3. Select the correct connection, and then click **Dial**.
A terminal screen prompts you for your username. If the screen is blank, press ENTER to display the prompt.
4. At the prompt, enter your RSA ACE/Server username.
This username may be different from your Windows username.
5. If you are prompted to enter your domain, enter it according to the instructions for your operating system.
6. At the prompt, enter your passcode.
If your passcode is correct, you are granted access.
7. Click **Continue** to close the terminal window.

To authenticate with a post-dial terminal based or VPN connection with EAP:

1. Log in to your computer using your Windows username and password.
2. Do one of the following:
 - For Windows 2000 Server and Windows 2000 Professional, click **Start > Settings > Network and Dial-up Connections**.
 - For Windows Server 2003 and Windows XP Professional, click **Start > Control Panel > Network Connections**.
3. Double-click the connection you want to use.
4. In the RSA SecurID Authentication dialog box, select your token type from the **Choose Token** list, and enter your RSA ACE/Server username and passcode.
If your passcode is correct, you see an **Authentication Successful** message. If your passcode is incorrect, you see **Access Denied**.

To authenticate with a wireless LAN connection with PEAP:

1. Log in to your computer using your Windows username and password.
2. Click **Start > Control Panel > Network and Internet Connections > Network Connections**.
3. Select the wireless connection you want to use.
4. Click **Connect**.

Note: Initiating a wireless connection causes a Windows balloon tip to appear on the Windows system tray. To start authentication, click the balloon tip. At the authentication prompt, enter your username within 30 seconds. If you do not enter your username within 30 seconds, the balloon tip reappears and you must click on it to restart authentication.

5. At the prompt, enter your RSA ACE/Server username.
6. At prompt, select your token type from the **Choose Token** list, and enter your passcode. (Your username is already filled in.)
If your passcode is correct, you see an **Authentication Successful** message. If your passcode is incorrect, you see **Access Denied**.

Note: If you are roaming, you are rechallenged every time you change access points. For example, if you authenticated to an access point that fails, you are rechallenged when another access point takes over.

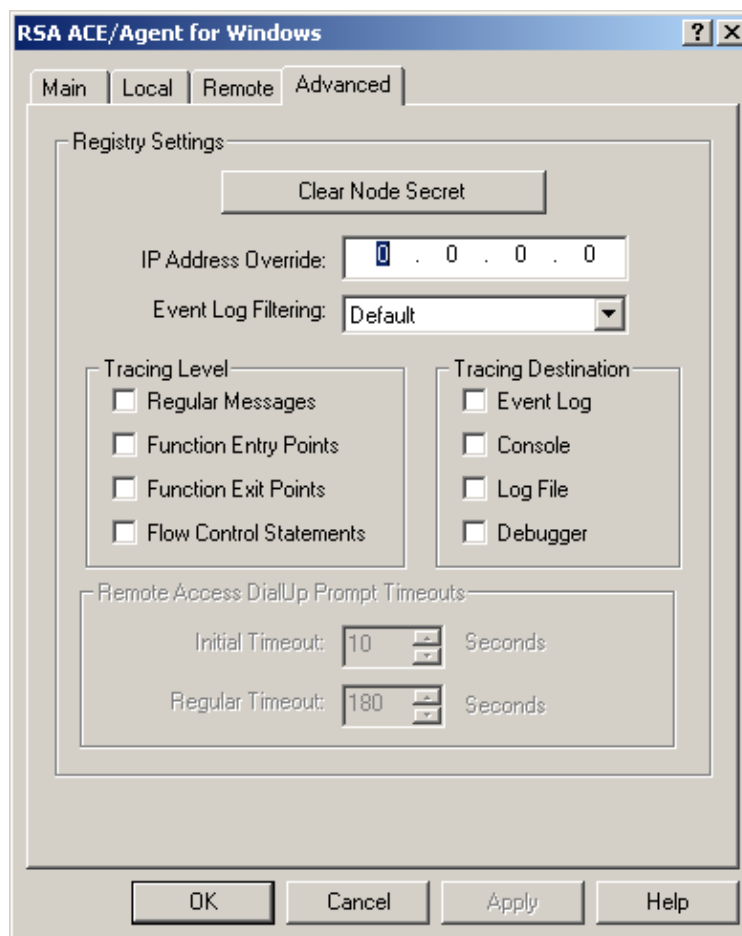
5

Configuring Advanced Settings

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

The default configuration settings in the following figure work well in most installations.

Important: Do not change these settings unless doing so will improve performance or help you or your RSA Security Customer Support representative resolve a problem.



The settings enable you to

- Clear the node secret from the Agent Host.
See the following section, [“Clearing and Replacing the Node Secret.”](#)
- Set an IP address override for the Agent Host primary network interface.
See [“Setting an IP Address Override”](#) on page 51.

- Filter event messages out of the Windows Event Viewer Application Log.
See [“Filtering Event Messages Out of the Windows Event Viewer Log”](#) on page 52.
- Set tracing levels to debug Agent problems and control where the tracing information is recorded.
See [“Tracing and Logging Agent Code Activity”](#) on page 52.
- Change the time-out values for the Remote access authentication prompts.
See [“Changing the Time-Out Values”](#) on page 53.

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 RSA ACE/Server uses the secret to authenticate the Agent Host, and both computers use the secret to encrypt and decrypt packets of data they send across the network.

The first time a user successfully authenticates or tests authentication from an Agent, the RSA ACE/Server creates a node secret for that Agent and stores it in the RSA ACE/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 is corrupted or does not match the node secret in the RSA ACE/Server database, encrypted communications between the Agent and the RSA ACE/Server cannot work. If this happens, the message **Access Denied, Node Verification Failed** is logged in the RSA ACE/Server Activity monitor. For more information about node verification failure, see [“Node Verification Fails”](#) on page 56.

To solve a node verification failure, you must clear the node secret from the Agent Host and, at the same time, instruct your RSA ACE/Server administrator to clear the node secret specified for the Agent Host in the RSA ACE/Server database, then perform a test authentication on the Agent Host.

Important: You must clear the node secret on both the RSA ACE/Agent Host and the RSA ACE/Server Host.

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**, and double-click the **RSA ACE/Agent** icon.
3. On the **Advanced** tab, click **Clear Node Secret**.
4. Click **Apply**.

5. Restart the Agent Host.

Important: If you do not restart the Agent Host before performing the test authentication, the authentication may appear successful, but local authentication will fail.

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 RSA ACE/Server established a new node secret when you authenticated.

To clear and replace the node secret in the RSA ACE/Server database, see the RSA ACE/Server Help.

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 RSA ACE/Server, making communication between the RSA ACE/Agent and RSA ACE/Server impossible.

To specify the primary IP address of the Agent:

1. Open the RSA ACE/Agent control panel.
2. On the **Advanced** tab, in the **IP Address Override** box, enter the IP address of the primary network interface of the Agent.
3. Click **Apply**.

Filtering Event Messages Out of the Windows Event Viewer Log

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

Note: You cannot use this setting to prevent RSA ACE/Agent error messages from being recorded in the Windows Event Viewer 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. Open the RSA ACE/Agent control panel..
2. On the **Advanced** tab, in the **Event Log Filtering** list, select the level of filtering that you want to apply to event messages in the log.

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

Low. Prevents messages that pertain to successful passcode authentication, and required or disabled passcode challenging from being logged.

Medium. In addition to filtering out all event messages in the **Low** category, this setting prevents messages pertaining to New PIN Mode and Next Tokencode mode from being logged.

High. In addition to filtering out all messages in the **Low** and **Medium** categories, this setting prevents **Service thread terminated, exiting** messages from being logged.

3. Click **Apply**.

Tracing and Logging Agent Code Activity

Trace logging is a useful debugging aid for you and your RSA Security Customer Support representatives. You can use the control panel to enable tracing of Agent code activity and to specify where tracing messages are logged.

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

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

To turn on tracing and specify where tracing messages are logged:

1. Open the RSA ACE/Agent control panel.
2. Click the **Advanced** tab.
3. Under **Tracing Level**, check the types of tracing you want the system to perform.

4. Under **Tracing Destination**, check the locations where you want the tracing messages logged:
 - **Event Log.** Tracing messages are recorded in the Windows Event Viewer log.
 - **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 and logging.

Changing the Time-Out Values

The control panel **Advanced** tab has these remote access prompt time-out values:

- **Initial Timeout.** Sets the wait time before the initial Remote access authentication prompt displays.
- **Regular Timeout.** Sets the number of seconds before Remote access authentication prompts time out.

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

For information about why you would need to change the time-out values, see [“Remote Access Prompts Time Out Too Soon”](#) on page 55.

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

1. Open the RSA ACE/Agent control panel,
2. Click the **Advanced** tab.
3. In the **Remote Access Prompt Time-outs** section, in the **Initial Timeout** box, enter or select the number of seconds that must elapse before the initial Remote prompt displays.
The minimum **Initial Timeout** value is 1 second and the maximum is 180 seconds. The default value is 10 seconds.
4. In the **Regular Timeout** box, enter or select the number of seconds that must elapse before remote prompts time out.
The minimum **Regular Timeout** value is 5 seconds and the maximum is 180 seconds. The default value is 180 seconds.
5. Click **Apply**.

6

Troubleshooting

This chapter helps you solve problems that may prevent users from successfully authenticating.

It also provides information about Windows troubleshooting, and alphabetically lists the RSA ACE/Agent Error and Events Log messages.

Specific Authentication Problems

Users Receive Error Messages During Authentication

Users may see the following messages during authentication:

- Cannot load RSA ACE/Agent DLL.
- Unexpected error from RSA ACE/Agent.

For information about these messages, see [“RSA ACE/Agent Error and Event Viewer Log Messages”](#) on page 58.

Remote Access Prompts Time Out Too Soon

If you are using RRAS without EAP, and you use automated scripts to display RSA SecurID username and passcode prompts for remote users, you may need to set different time-out values for the prompts.

RSA SecurID Hardware Token users have to wait up to 60 seconds for their next token codes to display. (RSA SecurID Software Token users do not need to wait for new token codes to display because their next token codes are generated automatically.) By changing the remote access prompt time-out values, you can prevent the remote access prompts from timing out before users can send their passcodes to the Agent.

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

There are two remote access prompt time-out values on the control panel Advanced properties sheet:

- **Initial Timeout** - Sets the wait time before the initial remote access prompt displays (in other words, before the script begins to execute).
- **Regular Timeout** - Sets the time-out value for all prompts that appear after the initial remote access prompt is displayed.

For instructions on changing these values, see [“Changing the Time-Out Values”](#) on page 53.

Test Authentication Succeeds But Actual Authentication Fails

If the test authentication succeeds, but actual authentication fails, reboot the RSA ACE/Agent Host.

The Agent Host gets the node secret when the Host is booted. Therefore, if the Agent Host is booted before a node secret exists, the Agent remains unaware of the node secret even after it is passed to the Agent Host.

Node Verification Fails

If the node secret on the Agent Host is corrupted or does not match the node secret in the RSA ACE/Server database, encrypted communications between the Agent and the RSA ACE/Server cannot work. If this happens, the message **Access Denied, Node Verification Failed** is logged in the RSA ACE/Server Activity monitor.

These events can cause node verification failure:

- The RSA ACE/Server successfully authenticates a user and sends the node secret to the RSA ACE/Agent along with a successful authentication message. However, the Agent either times out or fails (for example, due to a power failure) before storing the node secret.
- An administrator uninstalls the Agent, and then installs it again. When the Agent is uninstalled, the node secret is removed.
- The Agent is not identified in the RSA ACE/Server database. This event may generate either a **Node Verification Failed** error message or an **Agent Host Unknown** error message.
- You are using RSA ACE/Server Replicas, and the Replica that sent the node secret to the Agent has not yet notified other Replicas. In this case, some users will successfully authenticate while others will not.
- You are using Replicas, and one or more Replicas are down. In this case, some users will successfully authenticate while others will not.
- You clear the node secret on either the Agent or the RSA ACE/Server, but not on both.
- You clear the node secret on both the Agent and the RSA ACE/Server, but do not restart the Agent.
- You enter an invalid username on the first authentication after clearing the node secret.

To solve a node verification failure, you must clear the node secret from the Agent Host. At the same time, your RSA ACE/Server administrator must clear the node secret specified for the Agent Host in the RSA ACE/Server database. Then you must perform a test authentication on the Agent Host.

Important: You must clear the node secret on both the Agent Host and the RSA ACE/Server Host.

For instructions on how to clear the node secret on the Agent, see “[Clearing and Replacing the Node Secret](#)” on page 50. For instruction on how to clear the node secret on the RSA ACE/Server, see the RSA ACE/Server Help. For instructions on testing authentication, see “[Testing Authentication](#)” on page 27.

General Authentication Problems

This section tells you how to diagnose general authentication problems.

Verify the Accuracy of the PC Clock

If a user cannot authenticate, make sure the clock on the user’s PC is accurate. If the PC clock drifts from its previous setting, the user may not be able to authenticate.

Verify the **sdconf.rec** File

If the RSA ACE/Agent for Windows and the RSA ACE/Server computers 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, verify the file settings by opening the RSA SecurID Authentication Information dialog box.

To view the **sdconf.rec** file:

1. Open the RSA ACE/Agent control panel.
2. 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.

Windows Troubleshooting

If you are troubleshooting Windows, the log of information and authentication error messages is stored in the rotating file **%SYSTEMROOT%\aceclient.log**. When this file exceeds 1MB, it is renamed **aceclientn.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 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.

RSA ACE/Agent Error and Event Viewer Log Messages

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 challenge all users with RSA SecurID. 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. Make sure you have the correct administrative privileges, and then reboot the Agent Host. If the error persists, reinstall the Agent to override the existing settings. If that does not resolve the situation, you will have to uninstall, and then reinstall 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 entered an invalid 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 reinstall the RSA ACE/Agent.

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

The user entered an invalid passcode, causing the “bad passcode” counter to increment 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 computer, open the 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 computer, make sure the **echo** service is running on the RSA ACE/Server computer. 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 computer, open the Network control panel, click the **Services** tab, and confirm **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 computer, make sure the **echo** service is running on the RSA ACE/Server computer. 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

This message is 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 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 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 computer may not have enough free resources to add RSA SecurID authentication. Consider moving service(s) from this computer 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 computer.

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 computer 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 computer does not meet one or more of the system or software requirements needed to enable authentication of RAS connections. See [“Remote Access Authentication Platforms and Requirements”](#) on page 10, and make sure the computer 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 (for example, because the IP address is wrong), 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 (for example, because the IP address is wrong), 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 computer 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 authenticated successfully using RSA SecurID 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 Access Control List (ACL) has become corrupted, see the Microsoft Windows Help, or contact Microsoft Customer 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 Access Control List (ACL) has become corrupted, see the Microsoft Windows Help, or contact Microsoft Customer 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) connection occurred between the Agent and the RSA ACE/Server.

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 computer, enable the **Challenge All Users** under the **Local** tab 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 Customer 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 Agent. If you see this message, call RSA Security Customer Support.

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 a 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.

7

Upgrading to and Uninstalling RSA ACE/Agent 5.6 for Windows

Upgrading to RSA ACE/Agent 5.6 for Windows

When you upgrade from a previous version, the installation program automatically selects installation components to match those in the previous installation. Therefore, if you want to remove components, you must uninstall the previous installation.

Important: If you want to continue to use Network authentication and Web Access authentication, which are not available with RSA ACE/Agent 5.6 for Windows, do not uninstall them.

If you install RSA ACE/Agent 5.6 for Windows while components from a previous installation remain active on the Agent host, the node secret is not removed. The active Agent continues to use the node secret. If you uninstall all previously installed Agents and their components from the Agent host, the node secret is removed. The new installation creates a new node secret.

Uninstalling RSA ACE/Agent 5.6 for Windows

To uninstall the Agent:

1. Click **Start > Settings > Control Panel > Add/Remove Programs**.
2. From the list of programs, select **RSA ACE/Agent for Windows**.
3. Restart the computer.

Removing Shared Programs

Uninstalling the Agent does not remove shared programs that are in use. If you cannot remove a shared program immediately because it is in use, you may be able to remove it after you reboot your system. However, if you are using components from previous versions of the RSA ACE/Agent (for example, the Web Agent or Network authentication), RSA Security recommends that you do not remove shared programs.

Important: Before you remove the **sdeap.dll** file from an Agent desktop computer, you must edit all connections so that they no longer use RSA Security EAP. If you remove the **sdeap.dll** file before editing the connections, when you reboot your system, the Connection Manager may not function.

A

Load Balancing with the `sdopts.rec` File

RSA ACE/Agent 5.6 can balance authentication request loads automatically by sending a time request to each RSA ACE/Server in the realm and determining a priority list based on the response time of each RSA ACE/Server. The RSA ACE/Server with the fastest response is given the highest priority and receives the greatest number of requests from that Agent Host, while other RSA ACE/Servers get lower priorities and fewer requests. This arrangement lasts until the Agent software sends another time request, or times out.

In addition, the Agent Host can connect to its RSA ACE/Servers through firewalls if the alternate IP addresses (aliases) for those RSA ACE/Servers are either specified in the configuration record file (`sdconf.rec`) of the Agent Host, or are provided by the RSA ACE/Server upon request by the Agent Host.

Alternatively, Agent administrators can balance loads manually by specifying exactly which RSA ACE/Servers each Agent Host should use to process requests. The specification also assigns a priority to each RSA ACE/Server so that the Agent Host directs authentication requests to some RSA ACE/Servers more frequently than to others. To use this option, the Agent administrator specifies priority settings in the `sdopts.rec` file, a flat text file stored on the Agent Host.

You can also use the `sdopts.rec` file to indicate additional firewall IP addresses, and to specify an overriding IP address for the Agent Host if that Host is a multi-homed server.

Creating an `sdopts.rec` File

You can create and edit an `sdopts.rec` file using any text editor. After you set up the `sdopts.rec` file, save the file in `%SYSTEMROOT%\System32` on the Agent Host. To protect the file from unauthorized changes, change the permission settings so only administrators can modify the file.

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

The file can include:

- Comment lines, each 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 [“Using the Client IP Keyword to Set an Overriding IP Address”](#) on page 76.

- **USESERVER=<ip_address>, <priority>**. Specifies an RSA ACE/Server that can or will receive authentication requests from the Agent Host according to the specified priority value. Use one setting for each RSA ACE/Server that the Agent Host uses. The maximum number of RSA ACE/Servers you can specify in the **sdopts.rec** and **sdconf.rec** files *combined* is 11.

Each **USESERVER** keyword value must consist of the actual RSA ACE/Server IP address, separated by a comma from the assigned priority. The priority specifies whether or how often an RSA ACE/Server receives authentication requests. The following table lists the priority values you can specify.

Priority	Meaning
2-10	Send authentication requests to this RSA ACE/Server using a randomized selection weighted according to the assigned priority of the RSA ACE/Server. The range is from 2–10: the higher the value, the more requests the RSA ACE/Server receives. A Priority 10 RSA ACE/Server receives about 24 times as many requests as a Priority 2 RSA ACE/Server.
1	Use this RSA ACE/Server as a last resort. Priority 1 RSA ACE/Servers are used only if no RSA ACE/Servers of higher priority are available.
0	Ignore this RSA ACE/Server. A Priority 0 RSA ACE/Server can be used only in special circumstances. First, it must be one of the four RSA ACE/Servers listed in the sdconf.rec file. Next, the Priority 0 RSA ACE/Server can be used only for the initial authentication of the Agent, unless all RSA ACE/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 an RSA ACE/Server without using that RSA ACE/Server. You can change the priority value of the RSA ACE/Server if you later decide to use it. Note: Keywords must be uppercase. If none of the 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 RSA ACE/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 RSA ACE/Servers that the Agent receives as part of its initial authentication with an RSA ACE/Server.

Important: The maximum number of RSA ACE/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 an RSA ACE/Server in addition to the aliases listed for the RSA ACE/Server in the **sdconf.rec** file. You can specify up to three additional aliases in the **sdopts.rec** file.

The value for the **ALIAS** keyword must consist of the actual IP address for the RSA ACE/Server, followed by up to three alias IP addresses for that RSA ACE/Server. The Agent sends 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 specified RSA ACE/Server. In addition, the actual IP address must be included on any RSA ACE/Server list received by the Agent. The RSA ACE/Server list provides actual and alias IP address information about all known RSA ACE/Servers in the realm, and the Agent receives the RSA ACE/Server list from the RSA ACE/Server after the RSA ACE/Server validates an authentication request.

- **ALIASES_ONLY[=ip_address]**. When you provide an actual IP address for an RSA ACE/Server as the value of **ALIASES_ONLY**, this keyword specifies that only the alias IP addresses of the RSA ACE/Server should be used to contact that RSA ACE/Server.

When you do not provide a value, this keyword specifies that the Agent should send its requests only to RSA ACE/Servers that have alias IP addresses assigned to them. You can make exceptions by including in the **sdopts.rec** file no more than 10 **IGNORE_ALIASES** keywords to specify which RSA ACE/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 75.

If you use this keyword, make sure at least one RSA ACE/Server has an alias IP address specified for it in either the **sdconf.rec** file, or in the **sdopts.rec** file.

- **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 RSA ACE/Server list provided by the RSA ACE/Servers are ignored. Exceptions can be made by including no more than 10 **ALIASES_ONLY** keywords in the **sdopts.rec** file to specify which RSA ACE/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 75.

When you provide an actual IP address of an RSA ACE/Server as the value of **IGNORE_ALIASES**, the keyword specifies that only the actual IP address of the RSA ACE/Server should be used to contact that RSA ACE/Server.

An Example Featuring the USESERVER Keyword

The settings in the **sdopts.rec** file can be in any order, but each setting must be listed separately, one setting per line. This example shows how to use the **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 RSA ACE/Server identified by the actual IP address 192.168.10.23 receives many more authentication requests than RSA ACE/Server 192.168.10.22. RSA ACE/Server 192.168.10.20 is used only if the RSA ACE/Servers of higher priority are unavailable, and RSA ACE/Server 192.168.10.21 are 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. However, **USESERVER** keywords do not affect the alias addresses used to connect to RSA ACE/Servers, and **ALIAS** keywords have no effect on which RSA ACE/Servers are specified for use.

Examples Featuring the **ALIAS**, **ALIASES_ONLY**, and **IGNORE_ALIASES** Keywords

The settings in the **sdopts.rec** file can be in any order, but each setting must be listed separately in the file, one setting per line. This example shows how to use the alias 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
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 RSA ACE/Server with the actual IP address 192.168.10.23 has three alias addresses specified for it, while RSA ACE/Servers 192.168.10.20 and 192.168.10.21 have only one alias apiece, and RSA ACE/Server 192.168.10.22 has two alias addresses specified for it. The aliases specified by the **ALIAS** keywords are additions to any aliases specified in **sdconf.rec** or on the RSA ACE/Server list.

Note: You can use the **USESERVER** and **ALIAS** keywords together in the **sdopts.rec** file. However, **USESERVER** keywords do not affect the alias addresses used to connect to RSA ACE/Servers, and **ALIAS** keywords have no effect on which RSA ACE/Servers are specified for use.

The exceptions are that RSA ACE/Server 192.168.10.23, as specified by the **ALIASES_ONLY** keyword, will be contacted only through the alias IP addresses. RSA ACE/Server 192.168.10.22, specified by the **IGNORE_ALIASES** keyword, will be contacted only by using the RSA ACE/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 RSA ACE/Server 192.168.10.23 and RSA ACE/Server 192.168.10.22 by using only 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 RSA ACE/Server 192.168.10.23 and RSA ACE/Server 192.168.10.22 by using only their actual IP addresses.

Using the Client_IP Keyword to Set an Overriding IP Address

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

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

Some RSA ACE/Agent Hosts allow administrators to specify the overriding IP address for the Agent Host in the RSA ACE/Agent control panel. For instructions, see [“Setting an IP Address Override”](#) on page 51. You can also specify an overriding primary IP address by including the Client_IP= keyword in an **sdopts.rec** file on the Agent Host. If there is no **sdopts.rec** file on the Agent Host, you can create one by following the instructions in [“Creating an sdopts.rec File”](#) on page 71.

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, follow 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.

Maintaining the Primary IP Address of the Agent Host in the RSA ACE/Server

Each Agent Host primary IP address must be identified in its Agent Host record in the RSA ACE/Server database. Other IP addresses for the Host also can be listed there (as “secondary nodes”) for failover purposes.

If your RSA ACE/Server system uses auto-registration of Agent Hosts, the primary IP address of each Agent Host is entered in the record for the Agent Host on the RSA ACE/Server automatically and updated whenever it changes. For more information, see Appendix B, “[Automated Registration of Agent Hosts in the RSA ACE/Server Database.](#)” In the absence of Agent Host auto-registration, you must ensure that the RSA ACE/Server administrator knows the primary and secondary IP address of the Agent Host when the Agent Host is first configured on the RSA ACE/Server system. Should any Agent Host address change at any time, inform the RSA ACE/Server administrator in time to update the Agent Host record in the RSA ACE/Server database.

If Agent Hosts are registered manually, the RSA ACE/Server administrator must make sure the primary IP address in the Agent Host record in the RSA ACE/Server database matches the one specified in the Agent Host configuration records or **sdopts.rec** file. If the addresses do not match, communication between the Agent Host and the RSA ACE/Server fails. If secondary IP addresses are specified for the Agent Host, these too must be entered in the record, and all addresses must be updated if they change.

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 RSA ACE/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 RSA ACE/Server database. This 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 RSA ACE/Server **sdconf.rec** configuration file.

You must install the Automated Agent Host Registration and Update utility on Agent Hosts to be able to use it. Additionally, the RSA ACE/Server must be set to allow automated registration so the RSA ACE/Server can accept registration information from new Agent Hosts.

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

1. Copy the **sdconf.rec** and **server.cer** files on the Primary RSA ACE/Server 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 RSA ACE/Server is installed on a Windows computer, starting any RSA ACE/Server program, such as the Database Administration application, automatically starts the database brokers. If the RSA ACE/Server is installed on a UNIX computer, start the database brokers by issuing the **ACEPROG/sdconnect start** command on the RSA ACE/Server, where **ACEPROG** represents the directory path of the RSA ACE/Server executables directory.

5. The Automated Agent Host Registration and Update utility runs when the Agent Host is restarted. To run the program at any time, double-click **sdadmreg.exe**. 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. RSA Security recommends you run the program:
 - Immediately after installing RSA ACE/Agent software on a Windows host. An Agent Host record will be added to the RSA ACE/Server database if none already exists for the Agent Host, and if the RSA ACE/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 RSA ACE/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 RSA ACE/Server.
 - When you want to have the Agent Host's registry information updated by the current **sdconf.rec** file on the RSA ACE/Server. The updated registry setting will not take effect until the Agent Host is rebooted.



Local Authentication with Third-Party Products

The RSA ACE/Agent 5.6 for Windows supports Local authentication with Citrix MetaFrame XPS and Windows 2000 and 2003 Terminal Servers (WTS).

To use RSA ACE/Agent 5.6 for Windows with either Windows Terminal Server, or Windows Terminal Server and Citrix MetaFrame XPS, you install the Agent on the same server as WTS and MetaFrame, and users perform local authentication to the WTS/MetaFrame server.

When you use RSA ACE/Agent 5.6 for Windows with Windows Terminal Server, the system presents the user with a Windows login prompt as well as an RSA SecurID passcode prompt. This occurs because installing RSA ACE/Agent for Windows replaces the MS GINA with the RSA Security SD GINA. The SD GINA calls the MS GINA as the next GINA and prompts users for both the Windows and RSA SecurID logins.

For information about other configurations, visit RSA SecurCare Online (<https://knowledge.rsasecurity.com>).

D

Using Windows Groups with RSA Security EAP

RSA EAP challenges all users. If you are using EAP and want to exempt groups of users from the challenge, you must create the groups in Microsoft Active Directory, and create a remote access policy that uses a version of EAP other than RSA Security EAP for those groups.

Important: This procedure works only if Active Directory is set up in native mode. If Active Directory is set up in mixed mode, you must configure a remote access policy that uses a version of EAP other than RSA Security EAP for each user you do not want to challenge.

Step 1: Create a New Group in Active Directory

1. On the server, click **Start > Programs > Administrative Tools > Active Directory Users and Computers**.
2. Right-click **New Group**.
3. In the New Object - Group dialog box, enter the group information.
4. Open the new group.
5. On the **Members** tab in **Groups Properties**, click **Add**.
6. Add users to the group.

Step 2: Create a New Remote Access Policy

1. Launch IAS or RRAS (whichever you are using).
2. On the **Tree** tab, right-click **Remote Access Policies**.
3. Select **New - Remote Access Policy**.
4. In the Add Remote Access Policy dialog box, click **Add**.
5. Select **Windows-Groups**, then click **Add**.
6. In the Select Groups dialog box, select the group you created in the preceding section, "[Step 1: Create a New Group in Active Directory](#)" and click **OK**.
7. In the Add Remote Access Policy dialog box, verify that the Windows group matches the group you selected in the previous step, and click **Next**.
8. Select **Grant remote access permission**, and click **Next**.
9. Click **Edit Profile**, and click the **Authentication** tab.

10. Check the **Extensible Authentication Protocol** checkbox, and clear all the other methods.
11. On the **EAP type** drop-down menu, select a method other than **RSA Security EAP**.
12. Click the **Encryption** tab.
13. Check the **Strong** checkbox and clear the **No Encryption** and **Basic** checkboxes.
14. Click the **Advanced** tab.
15. Remove all connection attributes from the **Parameters** box.
16. Click **OK**.

Index

A

aceclient.log file, 57
 advanced settings, configuring, 49
 authentication prompts, changing time out values, 53
 Automated Agent Host Registration and Update utility, 79

B

balloon tips, automatically dismissing, 47

C

challenge options
 local access authentication, 30
 remote access authentication, 33
 changing timeout values for authentication prompts, 53, 55
 Citrix MetaFrame, 81
 clearing
 node secret, 50
 reserve password, 32
 communication devices, requirements, 12, 14, 16
 configuring
 advanced settings, 49
 desktops for EAP, 45
 desktops for PEAP, 46
 desktops for post terminal window based authentication, 44
 IAS for EAP, 39
 IAS for PEAP, 43
 local access authentication, 29
 PEAP on IAS, 43
 remote access authentication, 33
 RRAS for EAP, 36
 RRAS without EAP, 34
 wireless LAN authentication with PEAP, 41
 control panel, 25
 creating groups, 18

D

desktops
 configuring for EAP, 45
 configuring for PEAP, 46
 configuring for post terminal window based authentication, 44
 installing EAP, 44
 direct installation, 21

E

EAP
 configuring desktops, 45
 configuring on IAS, 39
 configuring on RRAS, 36
 installing on desktops, 44
 end users, information for, 24
 error messages, 58
 Event Viewer
 log messages, 58
 log settings, 52

G

groups, creating, 18

I

IAS
 configuring with EAP, 39
 requirements for EAP, 14
 information for end users, 24
 installation
 direct, 21
 silent mode, 24

L

LAN environment, setting up, 41
 load balancing, 71
 local access authentication
 challenge options, 30
 configuring, 29
 requirements, 10
 Local Access Authentication component, described, 29
 local authentication with third-party products, 81
 logs
 Event Viewer, 58
 filtering event messages, 52
 setting up for tracing, 52
 Windows, 57

N

node secret, clearing and replacing, 50, 56
 node verification failure, 56

O

overriding IP address, setting, 76
 overview, 9

P

- passwords, reserve, 31
- PEAP
 - configuring desktops, 46
 - configuring wireless LAN authentication, 41
- post terminal window based authentication
 - configuring desktops, 44
- preparations
 - creating groups of users to challenge, 18
 - LAN environment, 41
 - RSA ACE/Server, 17
 - RSA SecurID users, 18

R

- remote access authentication
 - challenge options, 33
 - configuring, 33
 - solutions, 10
- removing shared programs, 69
- replacing the node secret, 50
- requirements
 - communication devices, 12, 14, 16
 - IAS with EAP, 14
 - local access authentication, 10
 - RRAS with EAP, 12
 - RRAS without EAP, 11
 - RSA ACE/Server, 17
 - wireless LAN authentication, 16
- reserve password
 - clearing, 32
 - setting, 31
- RRAS
 - configuring for EAP, 36
 - configuring without EAP, 34
- RRAS with EAP, requirements, 12
- RRAS without EAP, requirements, 11
- RSA ACE/Agent, installing, 21
- RSA ACE/Server
 - requirements, 17
 - setting up, 17
- RSA SecurID users, preparing, 18

S

- sdconf.rec file
 - copying from the RSA ACE/Server, 17
 - viewing, 57
- sdopts.rec file, creating, 71
- setting the reserve password, 31
- settings
 - Event Viewer log, 52
 - node secret, 56
- shared programs, removing, 69
- silent mode installation, 24
- solutions
 - IAS with EAP, 14
 - local access authentication, 29
 - remote access authentication, 10
 - RRAS with EAP, 12
 - RRAS without EAP, 11
 - wireless LAN authentication with PEAP, 16

T

- third-party products, local authentication, 81
- time-out values, changing, 53, 55
- trace logs, setting up, 52
- troubleshooting, 55

U

- uninstalling the Agent, 69
- upgrading to RSA ACE/Agent 5.6, 69

W

- Windows
 - logs, 57
 - troubleshooting, 57
- Windows Terminal Server, 81
- wireless LAN authentication
 - configuring, 41
 - requirements, 16