

RSA Authentication Agent 6.1 for Microsoft 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, Confidence Inspired, e-Titlement, IntelliAccess, Keon, RC2, RC4, RC5, RSA, the RSA logo, RSA Secured, the RSA Secured logo, RSA Security, SecurCare, SecurID, SecurWorld, Smart Rules, The Most Trusted Name in e-Security, Transaction Authority, and Virtual Business Units are either registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. All other goods and/or services mentioned are trademarks of their respective companies.

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	9
Audience	9
Documentation	9
Getting Support and Service	9
Chapter 1: Overview	11
Protected Resources	11
Key Features	12
Support for Multiple Token Types	12
Integration with Microsoft Active Directory	13
Integration with RSA SecurID Authenticator Utility	13
Workstation Unlock with RSA SecurID PIN	14
Protection for Wireless Networks.....	14
Customization Options	14
Challenge Options.....	15
Compatibility with Remote Access Applications.....	15
Offline Authentication	15
Exempt Administrator Account.....	15
Windows Password Integration	16
Exceptions to Common Behavior	17
Restarting in Safe Mode	17
Using a Single User Name to Access More Than One Protected Resource	17
Forcing a Password Change on Windows XP	17
Chapter 2: Requirements and Preparations	19
Supported Platforms.....	19
General Requirements.....	19
Ports	20
Local Authentication Requirements and Setup.....	21
Domain Authentication Requirements and Setup	21
Remote Authentication Requirements and Setups.....	22
Non-EAP Setups	23
EAP Setups	23
Wireless Authentication Requirements and Setups	25
Terminal Services Requirements and Setup	27
RSA Authentication Manager Platforms and Requirements	28
Interoperability Requirements.....	28
Compatibility with Previous Versions and Third-Party Software	28
Interoperability with RSA Security Authenticator Utility	29
Interoperability with Web-Based Secure Sockets Layer Virtual Private Networks..	30
Limitations	30
Smart Cards.....	30
Cross-Realm Limitations	30

Preparations.....	30
Set Up the RSA Authentication Manager.....	30
Create Groups of Users to Challenge with RSA SecurID	31
Create Groups for Remote Access Application Hosts.....	32
Choose Emergency Access Methods.....	32
Prepare the Active Directory Database for Storing Offline Data	34
Enable Non-Administrative Users to Install RSA Authentication Agent 6.1 for Microsoft Windows	35
Prepare RSA SecurID Users	35
Chapter 3: Installing RSA Authentication Agent 6.1 for Microsoft Windows.....	37
What to Install.....	38
Local Authentication.....	38
Domain Authentication.....	38
Remote Authentication	39
Wireless Authentication.....	40
Terminal Services Authentication	41
Step 1: Install the RSA Certificate Utility	41
Step 2: Create Certificates.....	42
Step 3: Install RSA Authentication Agent 6.1 for Microsoft Windows	43
Types of Installations.....	44
Installing RSA Authentication Agent 6.1 for Microsoft Windows in Interactive Mode	44
Creating and Running a Network Installation Package	46
Cloning RSA Authentication Agent Hosts	50
Step 4: Start RSA Security Center	51
Step 5: Verify the Status of the Authentication Environment	51
Step 6: Test Authentication.....	51
Next Steps	52
Chapter 4: Configuring Local Authentication.....	53
Step 1: Select a Local Authentication Challenge Setting	53
Step 2: Set a Reserve Password	53
Step 3: Configure Local Authentication	54
Chapter 5: Configuring Domain Authentication.....	55
Step 1: Select a Domain Authentication Challenge Setting.....	55
Step 2: Test Domain Authentication.....	56
Step 3: Configure the RSA Authentication Agent on the Domain Controller.....	56
Reconnection After Offline Authentication.....	57
Configurable Session Certificate Lifetime	57
Step 4: Configure the RSA Authentication Agent on Domain Clients.....	57
Configuring Cross-Domain Authentication	58
Using Domain Authentication with Remote Access Authentication.....	59
Using the Verify Option	59

Using the Exclude Option.....	61
Saving Changes to a Roaming Profile	63
Chapter 6: Configuring Remote Authentication.....	65
Deploying Remote Authentication Without EAP	65
Deploying Remote Authentication With EAP	66
Deploying Remote Authentication Using EAP Without RADIUS	66
Deploying Remote Authentication Using EAP With Microsoft IAS RADIUS Server...	67
Deploying Remote Authentication Using EAP With RSA RADIUS Server	68
Changing the Time-Out Values for Remote Access Prompts.....	69
Authenticating from Remote Computers	69
Chapter 7: Configuring Wireless Authentication.....	71
Deploying Wireless Authentication With RSA Security EAP - Protected OTP	71
Deploying RSA Security EAP - Protected OTP With RSA RADIUS Server.....	71
Deploying RSA Security EAP - Protected OTP With	
Microsoft IAS RADIUS Server	73
Deploying Wireless Authentication with PEAP	74
Deploying PEAP With RSA RADIUS Server.....	74
Deploying PEAP With Microsoft IAS RADIUS Server	76
Authenticating Using Wireless Connections	79
Chapter 8: Configuring Advanced and Troubleshooting Settings.....	81
Configuring Advanced Settings.....	81
Clearing and Replacing the Node Secret	81
Clearing Offline Data.....	82
Setting an IP Address Override	83
Filtering Event Messages Out of the Windows Event Viewer Log.....	83
Configuring Troubleshooting Settings.....	83
Chapter 9: Offline Authentication.....	85
Offline Authentication with Local Authentication	85
Password Changes	86
Clock Changes	86
Offline Authentication with Domain Authentication.....	86
Managing Offline Days.....	88
Recharging Offline Days	88
Checking the Supply of Offline Days.....	90
Changing an Offline User's Challenge Status	90
Emergency Access	91
Automatic Authentication to Protected Domains After Offline Authentication.....	91
Setting Up Offline Authentication for Remote Users.....	92
Scenario 1	92
Scenario 2	93
Scenario 3	93

Chapter 10: Customizing RSA Authentication Agent 6.1 for Microsoft Windows	95
Adding Your Company Branding to the RSA Authentication Agent Logon Prompts	95
Customizing the Authentication Prompt	96
Specifying a Language for Installation	96
Chapter 11: Protecting Terminal Servers and Performing Common Windows Operations	97
Protecting Terminal Servers	97
Using RSA SecurID Authenticator SID800 in Terminal Server Environments	98
Using RSANetUse and RSARunAs	98
Issuing RSARunAs	100
Using Windows net use and runas	101
Issuing the Windows net use or runas From the Command Line	101
Performing GUI-Based Windows Operations	102
Mapping a Drive to a Protected Network	103
RSA Authentication Agent Prompting Behavior	103
Chapter 12: Troubleshooting	105
Specific Authentication Problems	105
Active Directory Password Takes Longer than Usual to Appear	105
Domain Authentication Fails	105
Installer Sees "...Network Authentication Service Terminated..." Message After Restart	105
Users Receive Error Messages During Authentication	106
Users See "Unable to Log You On..." During Logon to a Protected Domain	106
Remote Access Prompts Time Out Too Soon	106
Test Authentication Succeeds, But Actual Authentication Fails	106
Node Verification Fails	106
General Authentication Problems	107
Verify the Accuracy of the Computer Clock	107
Verify the sdconf.rec File	107
Windows Troubleshooting	108
RSA Authentication Agent Error and Event Viewer Log Messages	109
Chapter 13: Upgrading, Repairing, and Uninstalling	123
Upgrading to RSA Authentication Agent 6.1 for Microsoft Windows	123
Repairing an RSA Authentication Agent 6.1 for Microsoft Windows Installation	124
Uninstalling RSA Authentication Agent 6.1 for Microsoft Windows	124
Removing the sdeap.dll File	124
Appendix A: Load Balancing with the sdopts.rec File	125
Overview of Load Balancing	125
Creating an sdopts.rec File	125
Using the sdopts.rec File for Manual Load Balancing	128
An Example Featuring the USESERVER Keyword	128



- Examples Featuring the ALIAS, ALIASES_ONLY, and IGNORE_ALIASES
 - Keywords 129
 - Using the AVOID Keyword In Dynamic Load Balancing 130
 - Using the CLIENT_IP Keyword to Set an Overriding IP Address 130
 - Maintaining the Primary IP Address of the Authentication Agent Host in the RSA Authentication Manager 131
- Appendix B: Automated Registration of Agent Hosts 133**
 - Overview of Automated Registration of Agent Hosts 133
 - Running the Automated Agent Host Registration and Update Utility..... 134
- Appendix C: GINA Implementation in RSA Authentication Agent 6.1 for Microsoft Windows..... 135**
 - Overview 135
 - Supported Third-Party GINAs 135
 - Directly Supported GINAs 135
 - Indirectly Supported GINAs..... 136
 - Manually Configuring GINA Chaining 136
 - Unsupported GINAs 137
 - Installing the RSA Authentication Agent GINA 138
- Appendix D: Configuring Web Servers for RSA SecurID Authentication 139**
 - Configuring Web Servers for Domain Authentication With Remote Access Authentication..... 139
 - Configuring Microsoft Outlook Web Access in Front-End/Back-End Environments 140
- Index 141**

Preface

This book describes how to install and administer RSA Authentication Agent 6.1 for Microsoft Windows. RSA Authentication Agent 6.1 for Microsoft Windows works with RSA Authentication Manager 6.1 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, system integrators, and information technology managers. It is intended only for advanced security administrators and other trusted personnel. Do not make this guide available to other users.

Documentation

For documentation and product support information, as well as last-minute technical information not included in the documentation, see the *Readme* ([authagt_readme.html](#)). It is located in the `\AcedInt\nt_i386` directory of the RSA Authentication Agent 6.1 for Microsoft Windows .zip file.

Getting Support and Service

RSA SecurCare Online	https://knowledge.rsasecurity.com
Customer Support Information	www.rsasecurity.com/support
RSA Secured Partner Solutions Directory	www.rsasecured.com

RSA SecurCare Online offers a Knowledgebase that contains answers to common questions and solutions to known problems. It also offers information on new releases, important technical news, and software downloads.

The RSA Secured Partner Solutions Directory provides information about third-party hardware and software products that have been certified to work with RSA Security products. The directory includes Implementation Guides with step-by-step instructions and other information about interoperation of RSA Security products with these third-party products.

1

Overview

Protected Resources

RSA Authentication Agent 6.1 for Microsoft Windows works with RSA Authentication Manager 6.1 to protect your company's resources. The Authentication Agent intercepts requests to access protected resources and prompts users for their RSA SecurID passcodes. Passcodes are RSA SecurID PINs followed by a tokencode - the code generated by an RSA SecurID authenticator. When a user enters a passcode at the authentication prompt, the Authentication Agent sends the passcode to the Authentication Manager for validation. If the passcode is correct, the user gains access to the protected resource.

RSA Authentication Agent 6.1 for Microsoft Windows comprises the following components:

- Local Authentication Client
- Domain Authentication Client
- Domain Authentication Server
- Remote Authentication Server
- RSA Security EAP Client

The following table describes the resources RSA Authentication Agent 6.1 for Microsoft Windows protects.

Protected Resource	Description
Local Windows desktops	Requires users to provide RSA SecurID passcodes to log on to their local Windows desktops. For requirements, see the “Local Authentication Requirements and Setup” on page 21. For configuration information, see Chapter 4, “Configuring Local Authentication.”
Microsoft Windows domain resources and domain client desktops	Requires users to provide RSA SecurID passcodes to log on to domain client computers using their domain accounts, and to access domain resources on protected domain controllers. For requirements, see “Domain Authentication Requirements and Setup” on page 21. For configuration information, see Chapter 5, “Configuring Domain Authentication.”

Protected Resource	Description
Remote connections to network resources	Requires users to provide RSA SecurID passcodes before opening remote connections to protected networks using virtual private network (VPN) clients or post-dial terminal windows. For requirements, see “Remote Authentication Requirements and Setups” on page 22. For configuration information, see Chapter 6, “Configuring Remote Authentication.”
Wireless connections to network resources	Requires users to provide RSA SecurID passcodes before opening wireless connections to protected networks. For requirements, see “Wireless Authentication Requirements and Setups” on page 25. For configuration information, see Chapter 7, “Configuring Wireless Authentication.”
Common Windows operations	Adds RSA SecurID protection to the common Windows operations of logging on to terminal servers, issuing the Windows net use and runas commands. Additionally, the Authentication Agent includes the RSANetUse and RSARunAs commands. For more information, see Chapter 11, “Protecting Terminal Servers and Performing Common Windows Operations.”

For a list of components to install for each of these solutions, see Chapter 3, [“Installing RSA Authentication Agent 6.1 for Microsoft Windows.”](#)

Key Features

Support for Multiple Token Types

RSA Authentication Agent 6.1 for Microsoft Windows supports the following types of authenticators:

- RSA SecurID key fobs
- RSA SecurID standard cards
- RSA SecurID PINPads
- RSA SecurID software tokens
- RSA SecurID Authenticator SID800

You cannot use software tokens to log on to protected Windows desktops. However, once you log on to the desktop using a different type of authenticator, you can use software tokens to log on to the network.

Using RSA SecurID software tokens is less secure than using other types of authenticators because Software token users can log on to the network with only their RSA SecurID PINs. The other types of authenticators require users to either type in their RSA SecurID PINs and passcodes or, for the RSA SecurID Authenticator SID800, physically connect the authenticator to the USB port on the Authentication Agent Host computer and type in their RSA SecurID PINs.

Additionally, because software tokens are stored either in a database or on users' computers, users cannot remove their tokens when they leave their computers.

Integration with Microsoft Active Directory

RSA Authentication Agent 6.1 for Microsoft Windows leverages Microsoft Active Directory in the following ways:

- In domain authentication environments, facilitates greater security of the Windows logon password. For information, see [“Windows Password Integration”](#) on page 16.
- Facilitates deploying domain authentication with remote authentication. For information, see [“Using Domain Authentication with Remote Access Authentication”](#) on page 59.
- Facilitates remote authentication using EAP and PEAP. For more information, see Chapter 6, [“Configuring Remote Authentication.”](#)
- Provides a storage location for data that extends RSA SecurID authentication to users when the connection between the Authentication Agent Host and the RSA Authentication Manager is not available. For more information, see Chapter 9, [“Offline Authentication.”](#)

Integration with RSA SecurID Authenticator Utility

RSA Authentication Agent 6.1 for Microsoft Windows is interoperable with RSA Authenticator Utility. Deploying these products together enables you to enhance the RSA SecurID solution to more specifically suit your company's needs.

The Authentication Agent works with the Authenticator SID800 (a USB token) in the following ways:

- When the Authenticator SID800 is disconnected, users can read the tokencode displayed on the Authenticator and then manually enter it into the RSA SecurID logon prompt.
- When the Authenticator SID800 is connected to the USB port on the Authentication Agent Host, the Authentication Agent automatically reads the tokencode and submits it to the authentication process. At the authentication prompt, users enter only their RSA SecurID PINs.

RSA Authentication Agent 6.1 for Microsoft Windows and RSA Authenticator Utility share a dynamic user interface called the RSA Security Center. When installed together on the same computer, the two products appear as one. You administer both RSA Authentication Agent and RSA Authenticator Utility from the RSA Security Center. The options available from the RSA Security Center depend on which software you install. For example, when you open the RSA Security Center to configure the Authentication Agent, options for configuring RSA Authenticator Utility are present if you installed it.

Both RSA Authentication Agent and RSA Authenticator Utility have their own Graphical Identification and Authentication API (GINA) to protect desktop logons. When you install RSA Authentication Agent and RSA Authenticator Utility on the same computer, the GINA provided by RSA Authentication Agent takes precedence.

Workstation Unlock with RSA SecurID PIN

RSA Authentication Agent 6.1 for Microsoft Windows includes an option that allows users to unlock their protected workstations using only their RSA SecurID PINs instead of their full passcodes. As an administrator, you can enable and disable this feature, set a time-out period for the feature, and set the number of times users can enter incorrect PINs before they are prompted for full passcodes. You configure the option in the RSA Security Center. For more information, see the RSA Security Center Help topic “Configuring Workstation Unlock With RSA SecurID PIN.”

Protection for Wireless Networks

By supporting RSA Security EAP - Protected One Time Password (RSA Security EAP - Protected OTP) (EAP 32) and Protected EAP (PEAP), RSA Authentication Agent offers two ways to protect your wireless environment. By using RSA Security EAP - Protected OTP, you eliminate the need for authentication certificates and additional tunneling. For more information, see Chapter 7, “[Configuring Wireless Authentication](#).”

Customization Options

You can customize RSA Authentication Agent 6.1 for Microsoft Windows in the following ways:

Use your own company branding on logon prompts. You can customize the Authentication Agent logon prompts to include your own company branding. For more information, see “[Adding Your Company Branding to the RSA Authentication Agent Logon Prompts](#)” on page 95.

Specify whether logon prompts request passwords or passcodes. For local and domain authentication, you can customize RSA SecurID local and domain logon prompts to request either passwords or passcodes. For more information, see the RSA Security Center Help topic “Customizing the Logon Prompt.”

Specify a language for installation. During installation, the Authentication Agent determines the primary language used by the Microsoft Windows operating system on the installation host computer. If the Authentication Agent has language files that matches the primary language of the operating system, the Authentication Agent applies the language files. If the Authentication Agent does not have language files that match the locale, it applies English language files. However, you can specify language files for installation even though that language is not the primary language of the operating system.

The language files localize the following:

- The Authentication Agent portion of the RSA Security Center
- RSA Authentication Agent logon prompts
- Prompts after logon, such as **RSANetUse** and **RSARunAs** prompts
- Authentication messages

Currently, in addition to English, the Authentication Agent supports Japanese. If you need a language pack that was not shipped with RSA Authentication Agent 6.1 for Microsoft Windows, RSA Security can create the language pack for you. For information, contact your RSA Security representative.

For more information about the customization options, see Chapter 10, “[Customizing RSA Authentication Agent 6.1 for Microsoft Windows](#).”

Challenge Options

You can configure RSA Authentication Agent to challenge all users or only specific groups of users. The Authentication Agent uses Windows groups (for example, Domain Users or Dial-in Users), or groups that you create yourself using the Microsoft Computer Management interface. For more information, see “[Create Groups of Users to Challenge with RSA SecurID](#)” on page 31.

Compatibility with Remote Access Applications

Many remote access applications either have RSA SecurID capabilities installed on them (for example, a web server running RSA Authentication Agent 5.3 for Web), or are not equipped to perform the tasks required for RSA SecurID authentication. If computers hosting these remote access applications are part of a Windows domain protected by RSA Authentication Agent, remote authentication and domain authentication are incompatible. You can solve this problem by using the Windows Computer Management interface to create groups of remote access application hosts. You then use the RSA Security Center on the domain controller to tell the Authentication Agent how to address the remote access application hosts during authentication. For more information, see “[Using Domain Authentication with Remote Access Authentication](#)” on page 59.

Offline Authentication

Offline authentication extends RSA SecurID authentication to users when the connection to the RSA Authentication Manager is not available (for example, when users work away from the office, or when network conditions make the connection temporarily unavailable). For more information, see Chapter 9, “[Offline Authentication](#).”

Exempt Administrator Account

The exempt administrator account is an emergency access method that enables you to authenticate to your computer using your administrator account with only a password instead of an RSA SecurID passcode.

When you install the Authentication Agent, the RSA Authentication Agent installation wizard prompts you to select a challenge option. One of the options is **Do not challenge the administrator**. If you select this option, the Authentication Agent installation creates a group that is exempt from challenge and adds your Well-Known Security Identifier (SID) to the group.

Because the exempt administrator account is identified by a Well-Known Security Identifier (SID) instead of a user name, it is difficult for a malicious user to target the account to gain unauthorized access to the protected computer. If you decide not to create an exempt administrator account during installation, you can create one later. You do this by logging on to the client computer as the administrator who installed the Authentication Agent software, and using the Microsoft Windows interface to create a challenge-exempt group for the administrator.

For a list of other emergency access methods, see [“Choose Emergency Access Methods”](#) on page 32.

Windows Password Integration

Windows password integration integrates the Microsoft Windows password into the RSA SecurID logon process. With password integration, users provide their Windows logon passwords only during their initial online authentication. At this time, the passwords are stored with the users’ authentication data in the RSA Authentication Manager database and, for offline authentication, in the offline data. During subsequent authentications, users enter only their user names and RSA SecurID passcodes. The Authentication Agent gets the Windows password from the Authentication Manager and passes it to the Windows logon system.

In a domain environment, if an administrator changes a user’s Windows password, the Authentication Agent gets the updated password the next time the user authenticates. For example, after a user performs an initial logon, an administrator can change the user’s password in Active Directory to one that is long and complex. Active Directory notifies your domain controllers about the password change. The RSA Authentication Manager picks up the new password from the domain controllers and stores it in the user’s account in the RSA Authentication Manager database. The next time the user authenticates, the Authentication Agent obtains the Windows password from the Authentication Manager and passes it to the Windows logon process. The user never sees the new password, and therefore never needs to learn it.

Important: For Windows password integration to work, you must either configure the RSA Authentication Agent to send domain names and user names to the RSA Authentication Manager or make sure that Windows user names and passwords match the corresponding user names and passwords in the Authentication Manager database.

You enable and disable Windows password integration through the RSA Authentication Manager Database Administration Application. For more information, see “Setting Up Offline Authentication and Windows Password Integration” in Chapter 7, “Agents and Activation on Agent Hosts” in the *RSA Authentication Manager 6.1 Administrator’s Guide*.

You can enable Windows password integration system-wide, on a per Agent basis, or by groups. For example, to enable an Authentication Agent, you create an Agent record in the RSA Authentication Manager database. You can enable Windows password integration for all of the Authentication Agents in the database, or for some of the Authentication Agents but not for others. Similarly, you can enable Windows password integration for some groups of users but not for others.

Exceptions to Common Behavior

Restarting in Safe Mode

Ordinarily, when you restart a computer that is protected by RSA Authentication Agent, you have to authenticate with an RSA SecurID passcode. However, when you restart a protected computer in **Safe Mode**, or in **Safe Mode With Command Prompt**, the RSA Authentication Agent Logon GINA and other third-party GINAs are disabled. Therefore, you can authenticate using only Windows passwords.

However, when you restart a protected computer in **Safe Mode With Networking**, the RSA Authentication Agent Logon GINA continues to function and users can authenticate with RSA SecurID passcodes.

Using a Single User Name to Access More Than One Protected Resource

If a user has the same user name for more than one protected resource (for example, for a local account on a domain client computer and for a domain account on a protected domain controller) or for two different protected domains, Windows password integration behaves as follows:

- If the user's Windows passwords are the same, RSA Authentication Agent prompts the user for an RSA SecurID passcode instead of a Windows password.
- If the user has different Windows passwords for each account, RSA Authentication Agent remembers the most recently used Windows password, and prompts the user to enter the other Windows password to access the second protected resource.

Forcing a Password Change on Windows XP

Ordinarily, selecting **User must change password at next logon** for an offline user on the domain controller forces the user to enter a new password the next time the user authenticates online. Additionally, offline data is updated whenever an offline user authenticates online. However, due to Microsoft behavior, on Windows XP the user is not prompted for a new password the next time he or she authenticates online. Instead, the user is prompted for a new password during the second online authentication. The user must then perform a third online authentication to update offline data.

2

Requirements and Preparations

This chapter lists supported platforms and requirements for RSA Authentication Agent 6.1 for Microsoft Windows. It also describes the setup for the following authentication solutions:

- Local authentication
- Domain authentication
- Remote authentication in the following types of environments:
 - Microsoft IAS RADIUS Server
 - RSA RADIUS Server
- Wireless authentication
- Terminal services authentication

Supported Platforms

RSA Authentication Agent 6.1 for Microsoft Windows is supported on the following platforms.

Servers	Clients	Terminal Servers
• Windows Server 2003 Standard • Windows Server 2003 SBS • Windows 2003 Enterprise Server • Windows 2000 Professional • Windows 2000 Advanced Server • Windows 2000 Server	• Windows Server 2003 Standard • Windows 2003 Server SBS • Windows 2003 Enterprise Server • Windows 2000 Professional • Windows 2000 Advanced Server • Windows 2000 Server • Windows XP Professional SP2 • Windows XP Tablet SP2	• Windows Terminal Server • Citrix MetaFrame XPs

General Requirements

RSA Authentication Agent 6.1 for Microsoft Windows has the following general requirements:

- 733 MHz or faster Pentium processor
- 256 MB of RAM
- 50 MB of free disk space
- TCP/IP networking

For additional requirements, see the following sections:

- [“Local Authentication Requirements and Setup”](#) on page 21
- [“Domain Authentication Requirements and Setup”](#) on page 21
- [“Remote Authentication Requirements and Setups”](#) on page 22
- [“Wireless Authentication Requirements and Setups”](#) on page 25

Ports

The following table lists the ports that must be available for use by RSA Authentication Agent 6.1 for Microsoft Windows.

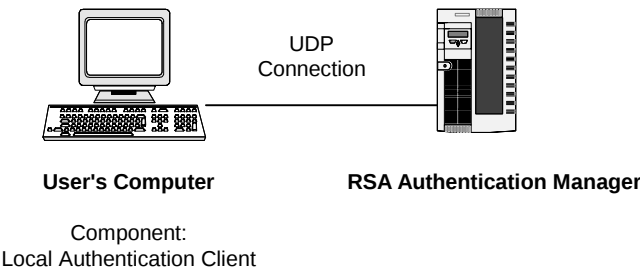
Port	Description
5580/tcp	Protected domain controllers and the RSA Authentication Manager use this port to listen. Local authentication clients and domain authentication clients connect to this port, but do not use it to listen.
5500/udp	The RSA Authentication Manager uses this port to listen. The Authentication Agent connects to this port during authentication.
2334/tcp	Domain clients use this port to listen.
2335/tcp	Domain controllers use this port to listen.

For Windows XP, you need to configure the Windows XP firewall to allow connections from all trusted domain controllers to these ports.

Local Authentication Requirements and Setup

For local authentication, there are no requirements in addition to the ones listed in [“General Requirements”](#) on page 19.

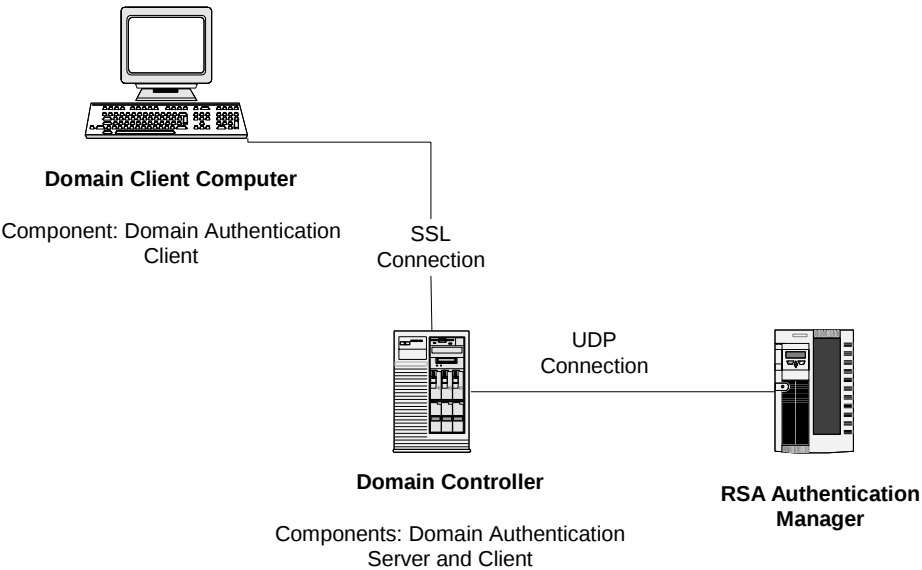
The following figure shows the setup for local authentication.



Domain Authentication Requirements and Setup

For domain authentication, there are no requirements in addition to the ones listed in [“General Requirements”](#) on page 19.

The following figure shows the setup for domain authentication.



On Windows XP SP2 domain client computers, although the firewall may have been stopped, the service may restart itself and prevent the Domain Authentication Client component from communicating with the Domain Authentication Server component on the domain controller. If this occurs, domain authentication for online users fails. Domain authentication for offline users succeeds, but Active Directory passcodes cannot be communicated, and the prompt for the Active Directory password takes longer than usual to appear. If you do not plan to use the Windows firewall service on the domain client computer, RSA Security recommends that you disable the service.

Remote Authentication Requirements and Setups

In addition to the requirements listed in [“General Requirements”](#) on page 19, your remote environment must meet the following requirements:

- TCP/IP networking must be enabled.
- Dial-in access must be enabled.
- 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 required so that users can respond to the **user name** and **PASSCODE** authentication prompts.

Important: To maintain a high level of security, the RRAS server must be physically secure.

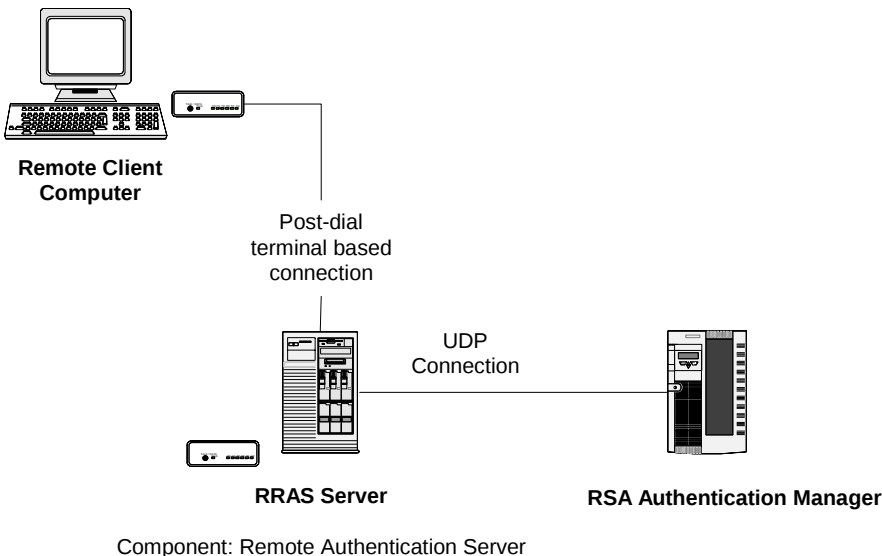
You can deploy remote authentication in the following types of environments:

- Non-EAP
- EAP

Non-EAP Setups

RRAS Without EAP Using a Post-Dial Terminal Based Connection

The following figure shows the setup for remote authentication in a non-EAP environment.

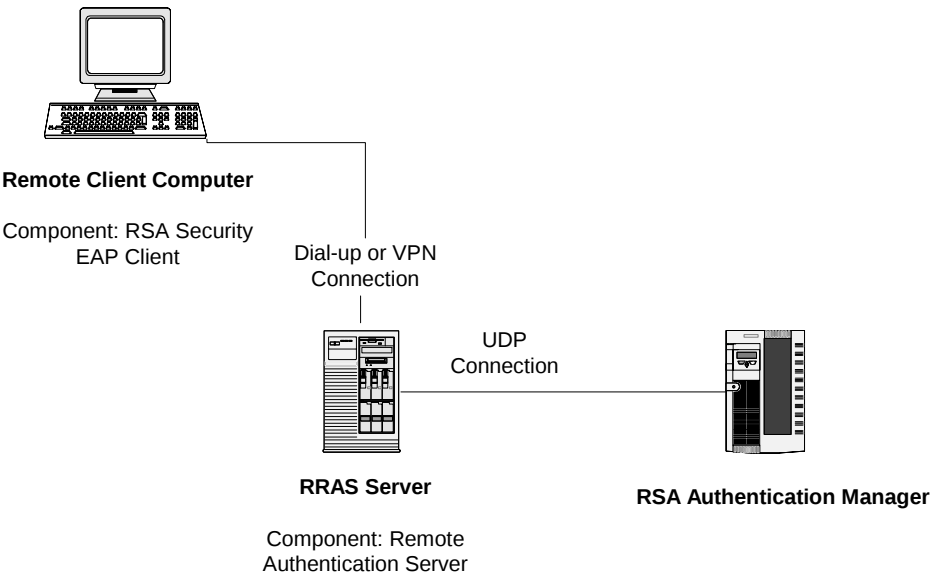


EAP Setups

Remote authentication supports RSA Security EAP Protected One-Time Password (OTP) (EAP 32). It also continues support for RSA Security EAP (EAP 15).

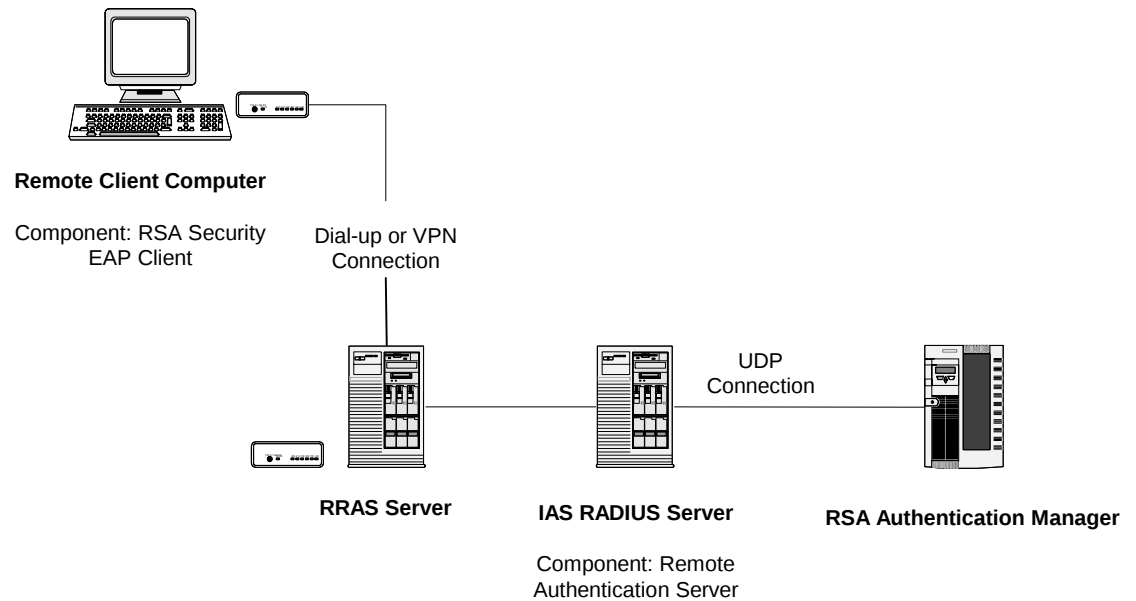
Non-RADIUS Environments

The following figure shows the setup for a non-RADIUS environment with EAP.



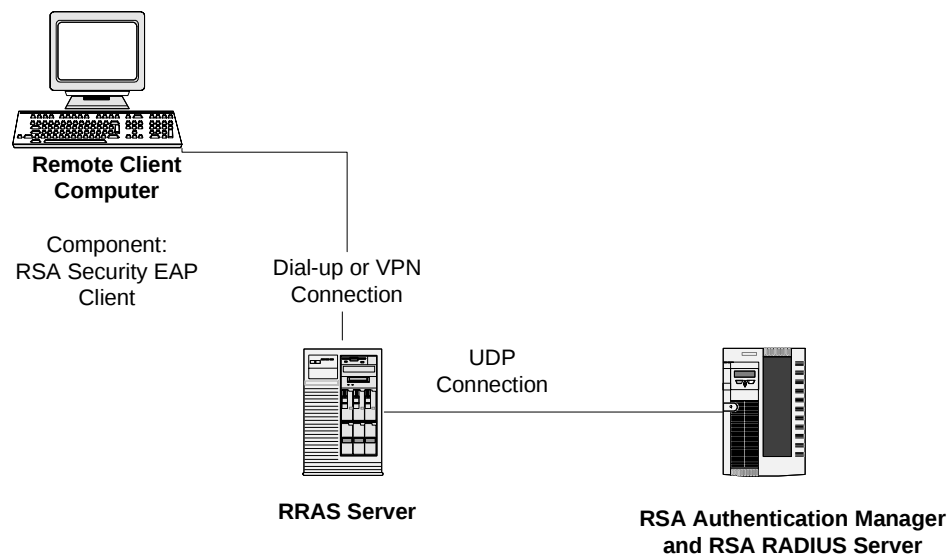
Microsoft IAS RADIUS Server Environments

The following figure shows the setup for Microsoft IAS RADIUS Server with EAP.



RSA RADIUS Server Environments

The following figure shows the setup for RRAS with EAP in either a dial-up or VPN environment.



Wireless Authentication Requirements and Setups

In addition to the requirements listed in “[General Requirements](#)” on page 19, your wireless environment must meet the following requirements:

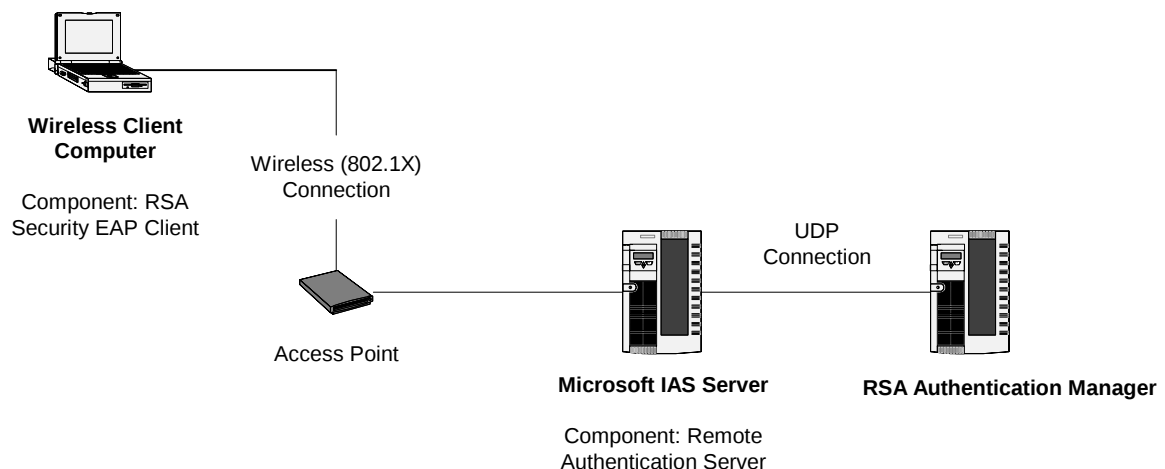
- TCP/IP networking must be enabled.
- Computers that act as clients must have wireless LAN cards that support:
 - IEEE 802.11 wireless networking
 - IEEE 802.1x authentication
 - Microsoft PEAP protocol
- Computers that act as servers must have connections to access points that support the 802.1X PEAP protocol and 802.11B networking technology.

For more information on setting up wireless LAN connections with access points that support 802.1X PEAP, see the documentation provided by Microsoft and your access point vendor.

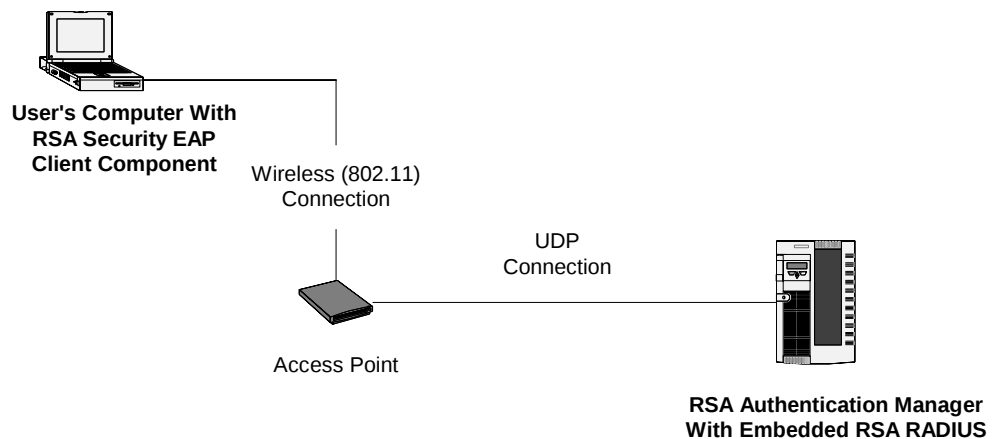
You can deploy wireless authentication in the following environments:

- Microsoft IAS RADIUS Server
- RSA RADIUS Server

The following figure shows the setup for the Microsoft IAS RADIUS Server environment.



The following figure shows the setup for the RSA RADIUS Server environment.



You can deploy wireless authentication with RSA RADIUS Server using one of the following protocols:

RSA Security EAP - Protected OTP - Does not require authentication certificates or additional tunneling.

PEAP - Requires authentication certificates.

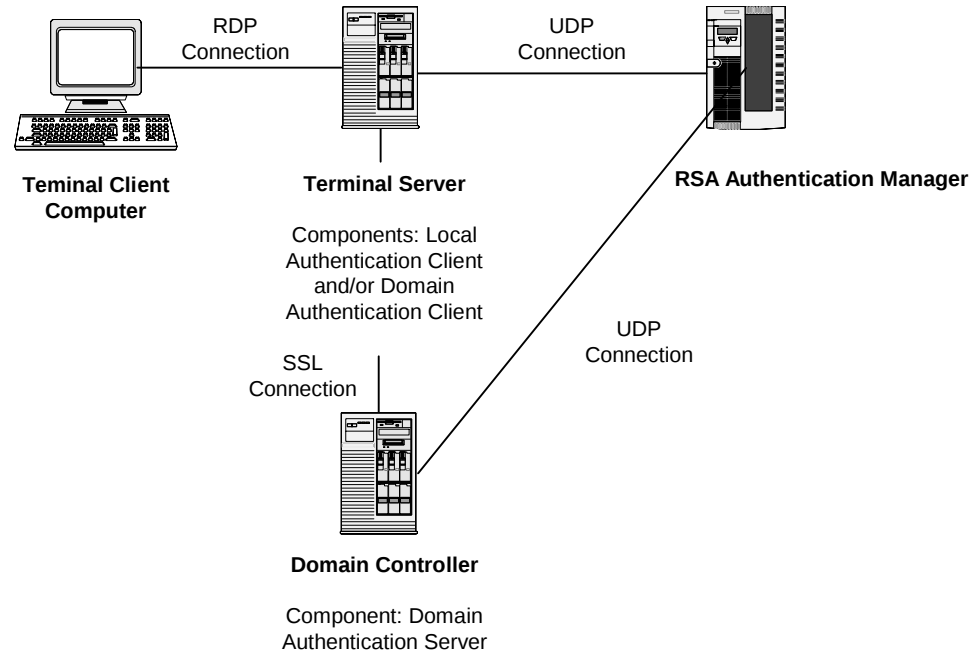
For more information, see Chapter 7, [“Configuring Wireless Authentication.”](#)

Terminal Services Requirements and Setup

Terminal services authentication is supported on the following platforms:

- Windows Terminal Server
- Citrix MetaFrame XPs

The following figure shows the setup for terminal services authentication.



For more information, see [“Protecting Terminal Servers and Performing Common Windows Operations”](#) on page 97.

RSA Authentication Manager Platforms and Requirements

RSA Authentication Agent 6.1 for Microsoft Windows works with RSA Authentication Manager 6.1. It does not work with previous versions of RSA Authentication Manager. However, RSA Authentication Manager 6.1 works with previous versions of the Authentication Agent.

Before you enable RSA SecurID authentication, you must understand the RSA Authentication Manager system and its features. These features include New PIN mode, client activation, and group memberships. For information about these or any RSA Authentication Manager administration features, see the *RSA Authentication Manager 6.1 Administrator's Guide*, or contact your RSA Authentication Manager administrator.

Interoperability Requirements

Compatibility with Previous Versions and Third-Party Software

Third-party applications and RSA Authentication Agent installed on the same computer may be incompatible if two versions of the **aceclnt.dll** file exist on the system in different locations.

The following table describes some key compatibility scenarios.

Software Currently Installed	Software You Plan to Install	Compatibility Issues	Suggested Actions
Third-party application that uses a version of the aceclnt.dll file earlier than 6.0 from the \system32 directory	RSA Authentication Agent 6.1	No issues.	Before proceeding, verify that the third-party application is supported by the vendor even after RSA Authentication Agent 6.1 updates the version of the aceclnt.dll used by the third-party application.
Third-party application that uses a version of the aceclnt.dll file earlier than 6.0 from a directory other than \system32	RSA Authentication Agent 6.1	Can coexist with suggested actions.	- Before proceeding, verify that the third-party application is supported by the vendor even after RSA Authentication Agent 6.1 updates the version of the aceclnt.dll used by the third-party application. - Copy the RSA Authentication Agent 6.1 .dll file to the third-party application.
RSA Security Agents that uses an aceclnt.dll file earlier than 6.0 from \system32	RSA Authentication Agent 6.1	No issues.	Upgrade.

Software Currently Installed	Software You Plan to Install	Compatibility Issues	Suggested Actions
RSA Authentication Agent for Web	RSA Authentication Agent 6.1	No issues.	
RSA Authentication Agent 6.0	RSA Authentication Agent 6.1	No issues.	Upgrade.
RSA Authentication Agent 6.1	RSA Authentication Agent 6.0 or earlier	Not supported.	Do not downgrade.
RSA Authentication Agent 6.1	RSA Agent for Web	No issues.	
RSA Authentication Agent 6.1	Third-party application that uses a version of the RSA Security aceclnt.dll file earlier than 6.0 from the \system32 directory	Can coexist with suggested actions.	Verify on a test installation that the third-party application does not overwrite the version 6.1 aceclnt.dll. If the third-party application does not overwrite the file, proceed as long as the vendor supports the third-party application under this scenario.
RSA Authentication Agent 6.1	Third-party application that uses a version of the RSA Security aceclnt.dll file earlier than 6.0 from a directory other than \system32	Can coexist with suggested actions.	- Before proceeding, verify that the third-party application is supported by the vendor even after RSA Authentication Agent 6.1 updates the version of the aceclnt.dll used by the third-party application. - Copy the RSA Authentication Agent 6.1 .dll file to the third-party application.
Java applications that use the 5.0.3 API for Java	RSA Authentication Agent 6.1	Can coexist with suggested actions.	Copy the Java application node secret to /system32 and change the path of the node secret in the Java application to \system32 .
RSA Authentication Agent 6.1	Java applications that use 5.0.3 API for Java	Can coexist with suggested actions.	Configure the node secret path in the Java API properties to point to \system32 .

Interoperability with RSA Security Authenticator Utility

There is no required order for installing RSA Authentication Agent 6.1 for Microsoft Windows and RSA Security Authenticator Utility on the same computer. Regardless of which product you install first, if you are using RSA Authentication Agent with RSA Authenticator Utility, the Authentication Agent logon interface replaces the Authenticator Utility logon interface.

Interoperability with Web-Based Secure Sockets Layer Virtual Private Networks

To use domain authentication with a web-based secure sockets layer virtual private network (SSL VPN), you must use an SSL VPN that assigns domain IP addresses to client computers. Domain authentication does not work with web-based SSL VPNs that provide access to the domain without actually adding the client computer to the domain.

Limitations

Smart Cards

The RSA SecurID for Microsoft Windows solution does not support smart card-based logon. RSA Security recommends that you disable the smart card service on client computers that host RSA Authentication Agent 6.1 for Microsoft Windows.

Cross-Realm Limitations

Password integration and downloading of offline data work across domains, but they do not work across realms. For example, if you have multiple domains within a single RSA Authentication Manager realm, and you enable cross-domain trust, users are not prompted for their Windows password when they access the remote realm, and users can download offline data from the remote realm. However, if you have domains that are in separate RSA Authentication Manager realms, even though you enable cross-domain trust, users are prompted for their Windows password when they access the remote realm, and users cannot download offline data from the remote realm. For more information about password integration, see [“Windows Password Integration”](#) on page 16. For more information about offline authentication, see [“Offline Authentication”](#) on page 15.

Preparations

This section describes tasks you must perform before you can use RSA Authentication Agent 6.1 for Microsoft Windows.

Set Up the RSA Authentication Manager

Before you use RSA Authentication Agent, you or your RSA Authentication Manager administrator must complete these tasks:

- If you have not already done so, install the RSA Authentication Manager.
- For instructions, see the *RSA Authentication Manager 6.1 Installation Guide* for your platform.
- Copy the **sdconf.rec** configuration file from the RSA Authentication Manager to the computers on which you plan to install these RSA Authentication Agent components:
 - Local Authentication Client component
 - Domain Authentication Server component
 - Remote Authentication Server component

For more information, see [“Step 3: Install RSA Authentication Agent 6.1 for Microsoft Windows”](#) on page 43.

- Verify that the RSA Authentication Manager is available.
- Register the RSA Authentication Agent host as an Agent of the RSA Authentication Manager. See [“Automated Registration of Agent Hosts”](#) on page 133 and “Creating and Modifying Agent Hosts” in Chapter 4, “Agents and Activation on Agent Hosts” in the *RSA Authentication Manager 6.1 Administrator’s Guide*.

Note: If you install the Authentication Agent on a multihomed server, you can provide an IP address override for the Authentication Agent. See [“Setting an IP Address Override”](#) on page 83.

- Register RSA SecurID users in the RSA Authentication Manager database and distribute RSA SecurID tokens to those users.
See the chapter, “Registering Users for Authentication” in the *RSA Authentication Manager 6.1 Administrator’s Guide*.
- Determine whether the user names in the RSA Authentication Manager database records have the users’ Windows domain names attached (for example, **DOMAIN\user name**).

Create Groups of Users to Challenge with RSA SecurID

You determine the degree to which the Authentication Agent protects resources by specifying which users to challenge for RSA SecurID passcodes. You can configure the Authentication Agent to challenge:

- No users
- All users
- A group of users
- All users except a certain group of users

The RSA Authentication Agent uses Windows groups to control access to resources. These groups can be default Windows groups (for example, Domain Users or Dial-in Users), or groups that you create 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 Authentication Agent.

RSA Authentication Agent supports the AGDLP method for nesting groups in domain settings. This method involves placing the user account (A) into a global (G) group, then placing the global group into a domain local (DL) group, and then assigning permission (P) to the domain local group.

For detailed instructions on creating groups, see your Windows documentation. For instructions on specifying which users to challenge, see the RSA Security Center Help topic “Specifying Who to Challenge.”

Create Groups for Remote Access Application Hosts

If your domain is protected with RSA Authentication Agent 6.1 for Microsoft Windows, and includes remote access applications, domain authentication and remote access authentication are incompatible. You can solve this problem by using the Active Directory Users and Computers interface to create groups of remote access application hosts. You can then use the RSA Security Center on the domain controller to tell the Authentication Agent how to address the remote access application hosts during authentication.

For instructions on creating groups, see your Windows documentation. For more information about using domain authentication with remote authentication, see [“Using Domain Authentication with Remote Access Authentication”](#) on page 59.

Choose Emergency Access Methods

RSA Authentication Agent 6.1 for Microsoft Windows supports several emergency access options that enable users and administrators to access protected resources when they lose their tokens, forget their PINs, or run out of offline days. Before you install and configure RSA Authentication Agent, decide which emergency access methods you want to use. The following tables describe the emergency access methods and show where to find more information.

For Offline Users

Emergency Access Method	Description	Supported Solutions	Characteristics	Reference
Offline emergency tokencode	Users can access their protected computers without a tokencode (for example, when they have lost their tokens)	- Local - Domain	- Must be combined with the user’s RSA SecurID PIN - Changes the next time the user authenticates online - Expires after a specified amount of time	See “Emergency Access” on page 91.
Offline emergency passcode	Users can access their protected computers without an RSA SecurID PIN or tokencode (for example, when they have forgotten their PINs, or when their PINs have been compromised)	- Local - Domain	- No RSA SecurID PIN required - Changes the next time the user authenticates online - Expires after a specified amount of time	See “Emergency Access” on page 91.

For Online Users

Emergency Access Method	Description	Supported Solutions	Characteristics	More Information
One-time passwords	Users can access their protected computers without a tokencode (for example, when they have lost their tokens)	• Local • Domain	• Must be combined with the user's RSA SecurID PIN • Generated by the RSA Authentication Manager • Valid for one authentication	See "Temporary Passwords to Replace Lost Tokens" in Chapter 7, "Registering Users for Authentication" in the <i>RSA Authentication Manager 6.1 Administrator's Guide</i> .
Fixed passwords	Users can access their protected computers without a tokencode (for example, when they have lost their tokens)	• Local • Domain	• Must be combined with the user's RSA SecurID PIN • Created by an RSA Authentication Manager administrator • Valid until the user's lost token status is changed	See "Temporary Passwords to Replace Lost Tokens" in Chapter 7, "Registering Users for Authentication" in the <i>RSA Authentication Manager 6.1 Administrator's Guide</i> .

For Administrators

Emergency Access Method	Description	Supported Solutions	Characteristics	More Information
Reserve password	Administrators can authenticate to a user's computer as that user without entering a passcode	Local	- Set by an administrator on each Agent Host - Never expires	See “Step 2: Set a Reserve Password” on page 53.
Exempt administrator account	Administrators can authenticate to protected computers as themselves with only a password	- Local - Domain	- Created during Agent installation for the administrator performing the installation - Created on each Agent Host - Protected by simple Windows password security - Identifies the account by a Well-Known Security Identifier (SID) instead of a user name	See “Exempt Administrator Account” on page 15.

Prepare the Active Directory Database for Storing Offline Data

By default, in domain environments, offline data is stored on the domain controller in **C:\windows\SYSVOL\sysvol\domain_name\rsa security\DomainHost\dayfiles**. However, during installation, you can choose to store the data in a Windows Active Directory database, or in the RSA Security file system.

To store offline data:

- The Active Directory schema must allow updates.
- The account of the administrator who updates the schema must have permissions for modifying the schema.

To prepare the Active Directory database for storing offline data:

- Add a new text attribute to the Active Directory schema as follows:
 - Data type: **string**
 - Length: **100 bytes**

- Assign a name to the attribute.

You use the attribute name when you install RSA Authentication Agent.

For more information about installing RSA Authentication Agent, see Chapter 3, [“Installing RSA Authentication Agent 6.1 for Microsoft Windows.”](#) For more information about offline authentication, see Chapter 9, [“Offline Authentication.”](#)

Enable Non-Administrative Users to Install RSA Authentication Agent 6.1 for Microsoft Windows

You can use the Microsoft Management Console (MMC) to provide users who are not administrators of their own computers with elevated privileges that enable them to install RSA Authentication Agent themselves. Although configuring elevated privileges enables users to install RSA Authentication Agent, it does not enable users to uninstall the Authentication Agent or perform other administrative tasks.

You can configure elevated privileges on each user's computer individually, or you can use the MMC on your domain controller to set the privileges. When domain users log on to their computers, the domain controller pushes the elevated privileges out to each domain client computer.

Important: Advanced users could take advantage of the permissions these settings grant to change their privileges and gain permanent access to restricted files and folders. To ensure that this does not happen, remove the policies immediately after the installation is complete. Because the application is installed per computer, if you remove the policy, the application can still perform a repair with elevated privileges.

For more information, see the Windows documentation or, access the Microsoft web site and search on "Allow Users Who Are Not Administrators to Install .msi Packages."

Prepare RSA SecurID Users

Before you use RSA Authentication Agent 6.1 for Microsoft Windows, prepare your RSA SecurID users as follows:

- Register users who will be challenged for passcodes as RSA SecurID users in the RSA Authentication Manager database, and activate their tokens.

For instructions, see "Creating and Modifying Agent Hosts" in Chapter 4, "Agents and Activation on Agent Hosts" in the *RSA Authentication Manager 6.1 Administrator's Guide*.

Important: The Windows user names for RSA SecurID users must be registered in the RSA Authentication Manager database. These user names cannot contain spaces and must not exceed forty eight characters.

- Give assigned and enabled tokens to users who will be challenged for passcodes.
- Provide authentication instructions to users.

3

Installing RSA Authentication Agent 6.1 for Microsoft Windows

This chapter describes how to do the following:

- Install the RSA Certificate Utility.
- Create certificates needed for domain authentication.
- Install RSA Authentication Agent 6.1 for Microsoft Windows.
- Open the RSA Security Center.
- Verify the status of the RSA Authentication Manager, and test authentication.

The sections describing installation tasks are sequentially numbered. If a section does not pertain to your environment, continue to the next section.

Important: If you plan to use domain authentication, you need to install the Certificate Utility and create certificates *before* you install RSA Authentication Agent 6.1 for Microsoft Windows.

CAUTION: Installing RSA Authentication Agent 6.1 for Microsoft Windows does not affect previous installations of RSA Authentication Agent 5.3 for Web. However, installing RSA Authentication Agent 6.1 for Microsoft Windows removes the Web authentication components from previous versions of the Authentication Agent for Windows. If you are currently running a version of RSA Authentication Agent with Web authentication components, and you want to continue using these features, do not install RSA Authentication Agent 6.1 for Microsoft Windows.

What to Install

The following sections summarize the components you need to install.

Local Authentication

Components to Install	Location
Local Authentication Client component	Each computer for which you want to protect the desktop

When you run the RSA Authentication Agent installation wizard, you can select the Automated Agent Host Registration and Update utility for installation along with the Local Authentication Client component. You need this utility only if you are using Dynamic Host Configuration Protocol (DHCP) to assign IP addresses. Because local authentication is the only solution that supports DHCP for assigning IP addresses, the Registration and Update utility is not offered for installation with any of the other Authentication Agent components.

When you select the Automated Agent Host Registration and Update utility for installation along with the Local Authentication Client component, the installation program prompts you for the **server.cer** file. This file is created when the RSA Authentication Manager is installed. By default, it is located in the **ACEDATA** directory on the Authentication Manager host computer.

If you do not want to install the Automated Agent Host Registration and Update utility when you install the Local Authentication Client component, you can manually install it later. For more information, see Appendix B, “[Automated Registration of Agent Hosts](#).”

Domain Authentication

Important: Do not install the Domain Authentication Server component on a computer that is not a domain controller. If you do, you will be unable to access the computer desktop.

Components to Install	Location
Certificate Utility	Any secure computer
Domain Authentication Server component	- The primary domain controller - Each backup domain controller - In an Active Directory forest, every domain controller in the forest
Domain Authentication Client component	- The primary domain controller or file server* - Each backup domain controller or file server* - Each domain client computer

*When you install the Domain Authentication Server component, the Domain Authentication Client component is also installed.

Important: If you are planning to enable cross-domain trust, see “[Configuring Cross-Domain Authentication](#)” on page 58 before you install RSA Authentication Agent.

Remote Authentication

The following sections summarize what you need to install for remote authentication in the following types of environments:

- Non-EAP
- EAP
- Wireless PEAP

Non-EAP Environments

Type of Environment	Components to Install	Location
RRAS without EAP	Remote Authentication Server component	RRAS server

EAP Environments

You can deploy remote authentication in the following EAP environments:

Non-RADIUS. Does not use a RADIUS server.

Microsoft IAS RADIUS Server. Incorporates Microsoft IAS RADIUS Server. This solution uses the RSA Security Center, a graphical interface, to configure remote authentication.

RSA RADIUS Server. Uses RSA RADIUS Server, which is shipped with RSA Authentication Manager. This solution eliminates the need for the Authentication Agent on the remote server and does not use the RSA Security Center to configure remote authentication.

All remote authentication EAP solutions support RSA Security EAP Protected One-Time Password (OTP) (EAP 32). They also continue to support RSA Security EAP (EAP 15).

The following table lists the Authentication Agent components you need to install and where to install them for each EAP solution.

Authentication Solution	Components to Install	Location
EAP without RADIUS	Remote Authentication Server component	RRAS server
	RSA Security EAP Client component	Each remote client computer
EAP with Microsoft IAS RADIUS Server	Remote Authentication Server component	Microsoft IAS Server
	RSA Security EAP Client component	Each remote client computer

Authentication Solution	Components to Install	Location
EAP with RSA RADIUS Server	RSA Security EAP Client component	Each remote client computer
	(Optional) Local Authentication Client component	RSA RADIUS Server

Note: EAP with RSA RADIUS Server does not require an Authentication Agent component on the RSA RADIUS Server computer, and does not use the RSA Security Center to configure remote authentication. However, you may want to install (but not configure) the Local Authentication Client component on the computer that hosts RSA RADIUS Server to provide a way to easily manage the node secret. For more information, see [“Managing the Node Secret on RSA RADIUS Server”](#) on page 82.

Wireless Authentication

Authentication Solution	Components to Install	Location
RSA Security EAP - Protected OTP with RSA RADIUS Server	RSA Security EAP Client component	Each remote client computer
	(Optional) Local Authentication Client component	RSA RADIUS Server
Wireless PEAP with Microsoft IAS Server	Remote Authentication Server component	Microsoft IAS Server
	RSA Security EAP Client component	Each remote client computer
Wireless PEAP with RSA RADIUS Server	RSA Security EAP Client component	Each remote client computer
	(Optional) Local Authentication Client component	RSA RADIUS Server

Note: Wireless authentication with RSA RADIUS Server does not require an Authentication Agent component and does not use the RSA Security Center to configure remote authentication. However, you may want to install (but not configure) the Local Authentication Client component to provide a way to easily manage the node secret. For more information, see [“Managing the Node Secret on RSA RADIUS Server”](#) on page 82.

Terminal Services Authentication

Authentication Solution	Components to Install	Location
Local authentication	Local Authentication Client component	Terminal server
Domain authentication	Domain Authentication Client component	Terminal server

Step 1: Install the RSA Certificate Utility

Note: If you do not plan to use domain authentication, start with [“Step 3: Install RSA Authentication Agent 6.1 for Microsoft Windows”](#) on page 43.

Domain authentication uses sets of digital certificates to prevent unauthorized users from gaining access to authentication data as it is transmitted across the network. Before you can use domain authentication, you need to install the RSA Certificate Utility and use it to create these certificates.

To install the RSA Certificate Utility, you must be an administrator on the host computer. You can install the RSA Certificate Utility on any physically secure computer.

To install the RSA Certificate Utility:

1. Log on to your system as an administrator.
2. Copy the **Certificate Utility.msi** file from the RSA Authentication Agent 6.1 for Microsoft Windows .zip file to your computer.
3. If you are running the Windows RRAS service, stop the service.
4. Double-click **Certificate Utility.msi**.
The RSA Certificate Utility installation wizard starts.
5. Follow the instructions on your screen to install the RSA Certificate Utility.
By default, the installation puts the Certificate Utility (the **sdcacool.exe** file) in the **C:\Program Files > RSA Security > RSA Authentication Agent** directory.

For more information about the Certificate Utility, see the RSA Certificate Utility Help topic “About the RSA Certificate Utility.”

Step 2: Create Certificates

Note: If you do not plan to use domain authentication, go directly to [“Step 3: Install RSA Authentication Agent 6.1 for Microsoft Windows”](#) on page 43.

Domain authentication uses digital certificates to protect authentication data transmitted across the network. These certificates work together to enable secure communication of passcodes and session certificates between the protected domain controller and the domain client computers. Before you install the RSA Authentication Agent, you need to create the following certificates:

Root certificate (sdroot.crt). When you create the root certificate, the Certificate Utility automatically creates a root key (**sdroot.key**). The root certificate key signs the server certificate described in the next paragraph. You must have only one root certificate for each domain environment.

Server certificates for each domain controller (*.crt). You must create unique server certificates for every domain controller in the protected environment. For example, if you have one Primary domain controller and two backup domain controllers, you must create unique server certificates for each one. You create the certificates on a secure computer using the Certificate Utility. When you create a server certificate, the Certificate Utility automatically creates a server certificate key (*.key).

Server certificate files must have the same name as the computer on which they will be installed. For example, the server certificate for a computer named **THOR** would be **thor.crt**.

The following table shows where you need to install these certificates.

Type of Certificate	Location
Root certificate	On the domain controller computer(s)
	On the domain client computers
Server certificate	On the domain controller computer(s)

To start the Certificate Utility:

Click **Start > Programs > RSA Security > RSA Authentication Agent > Certificate Utility**.

For instructions on creating these certificates, see the Certificate Utility Help topics “Creating Root Certificates” and “Creating Server Certificates.”

Step 3: Install RSA Authentication Agent 6.1 for Microsoft Windows

Before you install the Authentication Agent, you need to be aware of the following important issues:

- Do not install RSA Authentication Agent 6.1 components on computers that also host components from previous versions of RSA Authentication Agent (RSA ACE/Agent for Windows). For example, if you use a RADIUS server other than the one provided with RSA Authentication Manager 6.1, do not install RSA Authentication Agent 6.1 client components on the RADIUS server host. For more information, see [“Local Authentication Requirements and Setup”](#) on page 21.
- RSA Authentication Agent 6.1 for Microsoft Windows is not compatible with previous versions of RSA Authentication Agent (RSA ACE/Agent for Windows). If you install RSA Authentication Agent 6.1 for Microsoft Windows on a computer that hosts a previous version, the components from the previous version are either upgraded or removed. If, during this installation, you select the same components as in the previous installation, the components are upgraded and retain their previous configuration settings. Previous-version components that you do not select during this installation are removed.

For information about interoperability with other RSA Security products, see [“Interoperability Requirements”](#) on page 28. For information about upgrading, see Chapter 13, [“Upgrading, Repairing, and Uninstalling.”](#)

- Installing RSA Authentication Agent 6.1 for Microsoft Windows does not affect previous installations of RSA Authentication Agent 5.3 for Web. However, installing RSA Authentication Agent 6.1 for Microsoft Windows removes the Web authentication components from previous versions of the Authentication Agent for Windows. If you are currently running a version of RSA Authentication Agent with Web authentication components, and you want to continue using these features, do not install RSA Authentication Agent 6.1 for Microsoft Windows.
- If you have not already done so, copy the **sdconf.rec** file from the RSA Authentication Manager to the computer on which you want to install RSA Authentication Agent. The installation programs prompts you for the location of the file.
- If you plan to use domain authentication, you need to install the Certificate Utility and create certificates *before* you install RSA Authentication Agent 6.1 for Microsoft Windows. For instructions see [“Step 1: Install the RSA Certificate Utility”](#) on page 41, and the previous section [“Step 2: Create Certificates.”](#)
- When you install the Domain Authentication Server component, the installation program prompts you to select a location for storing offline data. By default, offline data is stored in the replicated directory **C:\WINDOWS\SYSVOL\sysvol**. At the prompt, you can accept the default location, change the location to a different replicated directory, or store offline data in a field that you specify in an Active Directory database. If you want to store the data in an Active Directory database, you must prepare the database before installing the Domain Authentication Server component. For instructions, see [“Prepare the Active Directory Database for Storing Offline Data”](#) on page 34.

- The Authentication Agent includes Japanese language files. During installation, the Authentication Agent determines the primary language used by the Microsoft Windows operating system on the installation host computer. If the primary language of the operating system is Japanese, the Authentication Agent applies the Japanese language files. If the primary language of the operating system is a language other than Japanese, the Authentication Agent applies English language files.

You can specify the Japanese language files for installation even if Japanese is not the primary language of the operating system. However, to do this, you must run the installation in one of the following ways:

- Interactively from a command line. For more information, see [“Installing RSA Authentication Agent 6.1 for Microsoft Windows in Interactive Mode”](#) on page 44.
- Silently. For more information, see [“Creating and Running a Network Installation Package”](#) on page 46.

Types of Installations

There are two types of installations:

Interactive. An interactive installation prompts you for parameters as you proceed. For instructions on performing an interactive installation, see the following section, [“Installing RSA Authentication Agent 6.1 for Microsoft Windows in Interactive Mode.”](#)

Silent. A silent installation uses a batch file to execute the RSA Authentication Agent Microsoft Installer (.msi) package. You create the package by executing an installation package creation program that prompts you to select installation and configuration settings. By default, the .msi installation package installs the Domain Authentication Client component. However, you can customize the installation package to install any of the RSA Authentication Agent components. For instructions, see [“Creating and Running a Network Installation Package”](#) on page 46.

Installing RSA Authentication Agent 6.1 for Microsoft Windows in Interactive Mode

To install the RSA Authentication Agent software, you must be an administrator on the host computer, or have administrator privileges for installing the software. For more information, see [“Enable Non-Administrative Users to Install RSA Authentication Agent 6.1 for Microsoft Windows”](#) on page 35.

RSA Authentication Agent 6.1 for Microsoft Windows is available as a .zip file that you must download from the RSA Security download site. The following procedure assumes that you have successfully downloaded the .zip file and have extracted it to a network location available to all computers that will host RSA Authentication Agent software.

To install RSA Authentication Agent 6.1 for Microsoft Windows:

1. Copy the **RSA Authentication Agent for Windows.msi** file from the RSA Authentication Agent 6.1 for Microsoft Windows .zip file to each computer that will host an Authentication Agent component.
2. If you have not already done so, copy the **sdconf.rec** file from the **ACEDATA** directory on the Primary RSA Authentication Manager to each computer on which you plan to install these RSA Authentication Agent components:
 - Local Authentication Client
 - Domain Authentication Server
 - Remote Authentication Server
3. If you are installing domain authentication, make sure you have access to the certificates you created in [“Step 2: Create Certificates”](#) on page 42.
4. Log on to your system as an administrator.
5. If you are running the Windows RRAS service, stop the service.
6. To start the installation, do one of the following:
 - If you want to let the installation program determine which language files to install, double-click **RSA Authentication Agent for Windows.msi**.
The Authentication Agent includes Japanese language files. During installation, the Authentication Agent determines the primary language used by the Microsoft Windows operating system on the installation host computer. If the primary language of the operating system is Japanese, the Authentication Agent applies the Japanese language files. If the primary language of the operating system is a language other than Japanese, the Authentication Agent applies English language files.
 - If you want to install the Japanese language files on a system where the operating system language is not Japanese, at a command line, enter the following:

```
msiexec /I "RSA Authentication Agent for Windows.msi"  
LANG_JPN=1
```


The installation wizard starts.
7. Follow the instructions on your screen to advance through the Welcome pages and accept the Software License Agreement.
8. Choose the type of installation:
 - Typical.** Installs the Domain Authentication Client component.
 - Custom.** Installs one or more of these authentication components, depending on which ones you select:
 - Local Authentication Client
 - Domain Authentication Server
 - Domain Authentication Client
 - Remote Authentication Server
 - RSA Security EAP client

When you select the Local Authentication Client component, you can also choose to install the Automated Agent Host Registration and Update utility. For more information, see [“Local Authentication”](#) on page 38.

9. If you choose the Custom installation, at the **Select Components** screen, select the components you want to install.
10. Click **Next**, and follow the instructions on the screen to complete the installation.

Important: If you are installing the Domain Authentication Server component, you must import the server certificate before restarting your computer. If you do not import the certificate before restarting, you will not be able to access your computer.

If you choose not to register the software immediately after installing it, you can register later by clicking **Start > Programs > RSA Authentication Agent > Register**.

11. Restart the computer.

Creating and Running a Network Installation Package

To speed the process of installing RSA Authentication Agent 6.1 for Microsoft Windows, you can create a preconfigured .msi network installation package. You can distribute the installation package, or put it in a shared location on the network to enable users to install RSA Authentication Agent silently, without user intervention.

By default, the installation package installs only the Domain Authentication Client component. However, you can select to install other Agent components instead of or in addition to the default. Even if you do not plan to deploy all of the components at one time, you may want to select them for installation so you can enable them in the future.

To create a network installation package, you use the **CreateInstallPackage.bat** and **RSA Authentication Agent for Windows.msi** files included with the RSA Authentication Agent software. These files work together to run a wizard that prompts you for configuration settings and creates the installation package.

You can configure the installation package to install the Local Authentication Client and Domain Authentication Client components in either enabled or disabled states. The following tables describe the configuration options the installation package creation program presents for specifying enabled or disabled states.

Local Authentication

Configuration Option	Result
Exclude the Administrator from RSA SecurID challenge	Enables local authentication and challenges all users except those with Windows Administrator status. If you do not select this option, local authentication will not be enabled until you use the RSA Security Center to choose a challenge option.

Domain Authentication

Configuration Option	Result
Enable Domain Authentication	Enables domain authentication on the domain client host

Important Considerations

- You must install the Domain Authentication Server component manually. Do not install it through a network installation package. During installation, you must import the server certificate, and a network package installation does not enable you to do this.
- For domain authentication, you must install the Domain Authentication Server component before you install the Domain Authentication Client component. Otherwise, you will be locked out of your system.
- Even if you chose to configure RSA Authentication Agent logon after installation, as soon as you install RSA Authentication Agent logon components, your system uses the RSA Authentication Agent logon prompts instead of the Windows prompts.
- In addition to prompting you for basic configuration settings, the installation package creation program prompts you about the following:
 - Whether you want to copy the reserve password from an existing installation.
 - If you are installing the Local Authentication Client component, whether you want to install the Automated Agent Host Registration and Update utility. For more information, see [“Local Authentication”](#) on page 38.
 - For all components other than the Remote Authentication Server component and the RSA Security EAP Client component, whether you want to specify a custom bitmap to use in the logon dialog boxes. For more information, see [“Adding Your Company Branding to the RSA Authentication Agent Logon Prompts”](#) on page 95.

- Whether you want to allow users to log on to their protected desktops with only their RSA SecurID PINs instead of their full passcodes.
- Whether you want enable the system to update passwords in a Novell database when Microsoft Windows passwords are updated.
- The Authentication Agent includes Japanese language files. During installation, the Authentication Agent determines the primary language used by the Microsoft Windows operating system on the installation host computer. If the primary language of the operating system is Japanese, the Authentication Agent applies the Japanese language files. If the primary language of the operating system is a language other than Japanese, the Authentication Agent applies English language files.

You can specify the Japanese language files for installation even if Japanese is not the primary language of the operating system. To do this, you must add a line to the file **packageOptionsFile.txt** as described in the procedure [“To configure the network installation package to install the Japanese language files when Japanese is not the primary language of the operating system:”](#) on page 49.

Creating a Network Installation Package

To create a network installation package:

1. If you want to configure domain authentication, make sure you have access to the certificates you created in [“Step 2: Create Certificates”](#) on page 42.
2. Copy the **CreateInstallPackage.bat** and **RSA Authentication Agent for Windows.msi** files from the RSA Authentication Agent for Windows .zip file to a secure location.

Note: By default, the network installation packages you create are configured to run from the location where you create them. Therefore, you may want to copy the **CreateInstallPackage.bat** and **RSA Authentication Agent for Windows.msi** files to the location where you will run them. If you want to run the installation packages from a different location, you must edit the installation package after you create it. For more information, see the procedure [“To configure the network installation package to run from a location other than where you created it:”](#) on page 49.

3. Double-click the **CreateInstallPackage.bat** file, and then follow the instructions on your screen to create the network installation package.

You can choose to install all or any combination of the following components:

- Domain Authentication Client
- Local Authentication Client

When you select the Local Authentication Client component, you can also choose to install the Automated Agent Host Registration and Update utility. For more information, see [“Local Authentication”](#) on page 38.

- Remote Authentication Server
- RSA Security EAP Client

This procedure creates the **silentInstallPackage** folder. The folder contains the following files:

- **sdconf.rec** (depending on the authentication components you selected)
- **sdroot.crt** (depending on the authentication components you selected)
- **packageOptionsFile.txt**
- **silentInstall.bat**
- **server.cer**
- **gina_banner.bmp**

This file is included only if you specified that you want to use a custom bitmap for use in logon dialog boxes.

You can create as many network packages as you want (for example, one for each type of configuration you want to install). However, you must create the packages in different directories.

To configure the network installation package to install the Japanese language files when Japanese is not the primary language of the operating system:

1. Use a text editor to open the file **packageOptionsFile.txt**.
2. Add the following line to the file:

```
LANG_JPN=1
```

3. Save and close the file.

To configure the network installation package to run from a location other than where you created it:

Open the **SilentInstall.bat** file in a text editor and do one of the following:

- If you want to run the installation package by double-clicking **SilentInstall.bat**, uncomment the following line:
- If you want to run the installation package from a command line, edit the following line to include the location from which the installation package will be run:

```
msiexec /qn /i "RSA Authentication Agent for Windows.msi"
```

```
msiexec /qn /i  
"installation_pkg_location\RSA Authentication Agent for  
Windows.msi"
```

Running the Network Installation Package

The files in the network installation package that you create interact with the **RSA Authentication Agent for Windows.msi** file provided with the RSA Authentication Agent software to run the installation package.

To run an installation package from the location where it was created:

Do one of the following:

- Double-click **silentInstall.bat**.
- At the command prompt, enter **silentInstall.bat**.
- Write a start-up script that includes the following line:

```
msiexec /qn /i
"drive:\file_location\RSA Authentication Agent for
Windows.msi"
```

To run an installation package from a location other than where it was created:

1. If you have not already done so, configure the network installation package as described in the previous procedure, "[To configure the network installation package to run from a location other than where you created it:](#)"
2. Copy the **silentInstallPackage** folder to the location from which you want to run the installation.
3. Depending on how you configured the installation package, do one of the following:
 - Double-click **silentInstall.bat**.
 - At the command prompt, enter **silentInstall.bat**.
 - Write a start-up script that includes the following line:

```
msiexec /qn /i
"drive:\file_location\RSA Authentication Agent for
Windows.msi"
```

Cloning RSA Authentication Agent Hosts

You can deploy RSA Authentication Agent 6.1 for Microsoft Windows by cloning. Because the **sdconf.rec** file and the root certificate required to install RSA Authentication Agent are not computer-specific, you can deploy RSA Authentication Agent within an organization by installing and configuring the RSA Authentication Agent on a single source computer, and then cloning the source computer.

The **sdconf.rec** file and the root certificate are company-specific. If you want to use cloning to deploy RSA Authentication Agent to different companies, contact each company for their **sdconf.rec** files and the root certificates and create a specific source installation for each company.

Step 4: Start RSA Security Center

You configure RSA Authentication Agent through RSA Security Center.

RSA Security Center has a **Home** tab and a **Configuration** tab.

The **Home** tab links to pages for performing non-administrative tasks such as viewing the number of offline days on the Authentication Agent Host. If you installed only the Remote Authentication Server component, the **Home** tab does not appear.

The **Configuration** tab links to pages for performing administrative tasks such as configuring the Authentication Agent for domain authentication. Only users who are administrators on their local computers can access the **Configuration** tab.

To start RSA Security Center:

1. Log on to the computer as an administrator.
2. Click **Start > Programs > RSA Security > RSA Security Center**.

The RSA Security Center includes online Help.

Step 5: Verify the Status of the Authentication Environment

In this step, you verify information about the authentication environment and the RSA Authentication Manager. For instructions, see the RSA Security Center Help topic “Verifying The Status of the Authentication Environment.”

Step 6: Test Authentication

Note: This section tests the authentication environment for local and remote authentication. If you plan to configure only domain authentication, go to Chapter 5, “[Configuring Domain Authentication](#).”

Testing authentication is important because, in addition to verifying the authentication environment, it creates a node secret for the Authentication Agent and stores it in the RSA Authentication Manager database. The node secret is required for communication between the Authentication Agent and the RSA Authentication Manager. For more information, see “[Clearing and Replacing the Node Secret](#)” on page 81.

To test the authentication environment for local or remote authentication, perform one of these authentication tests:

- Tokens that already have PINs
For instructions, see the RSA Security Center Help topic “Testing Authentication if the Token Has an RSA SecurID PIN.”
- Tokens that do not have PINs
For instructions, see the RSA Security Center Help topic “Testing Authentication if the Token Does Not Have an RSA SecurID PIN.”

To test domain authentication:

1. Open the RSA Security Center on the Authentication Agent Host, and click the **Configuration** tab.
2. In the left pane, click **Authentication Test**.

For more information, see the RSA Security Center Help.

Next Steps

Configure the features you installed. For more information, see:

- Local authentication, see Chapter 4, [“Configuring Local Authentication”](#)
- Domain authentication, Chapter 5, [“Configuring Domain Authentication”](#)
- Remote authentication, Chapter 6, [“Configuring Remote Authentication”](#)
- Wireless authentication, Chapter 7, [“Configuring Wireless Authentication.”](#)

4

Configuring Local Authentication

Local authentication requires users to provide valid RSA SecurID passcodes to log on to their local Windows desktops. This chapter describes the steps for enabling and configuring local authentication. It also describes the main local authentication configuration options.

Installing local authentication on computers that run Microsoft Terminal Services or Citrix MetaFrame servers requires users to provide RSA SecurID passcodes to authenticate to terminal servers. For more information, see Chapter 11, [“Protecting Terminal Servers and Performing Common Windows Operations.”](#)

Important: The instructions in this chapter assume you have already installed the Local Authentication Client component and tested authentication to create a node secret. Without a node secret, the Authentication Agent cannot communicate with the Authentication Manager. If you need installation instructions, see [“Step 3: Install RSA Authentication Agent 6.1 for Microsoft Windows”](#) on page 43.

Step 1: Select a Local Authentication Challenge Setting

Selecting a local authentication challenge setting tells the Authentication Agent which local users to challenge for RSA SecurID passcodes. For example, if you challenge all users, the Authentication Agent prompts all local users who attempt to access the computer desktop for a valid RSA SecurID passcode. Alternately, if you challenge only specific groups of users, the Authentication Agent prompts only those users for RSA SecurID passcodes. For more information, see the RSA Security Center Help topic “Selecting a Local Authentication Challenge Setting.”

Step 2: Set a Reserve Password

The reserve password feature is an emergency access method that enables you, the administrator, to authenticate to a user’s protected computer as that user without entering an RSA SecurID passcode.

If the reserve password feature is enabled, and the Windows system is unable to communicate with the RSA Authentication Manager at the time of authentication, instead of displaying a message that the Authentication Manager is unreachable, the system prompts you to enter a reserve password instead of a passcode.

The reserve password is encrypted and stored in the registry. However, you set and clear the reserve password only through the RSA Security Center. The reserve password is case sensitive and must include at least:

- One number
- One letter

If you select **All Users** as the local authentication challenge option, and the network connection fails, no one, including an administrator, can access the local desktop on the protected computer. For this reason, RSA Security strongly recommends either setting a reserve password, or using another emergency access method for administrators. For information on other emergency access methods, see [“Choose Emergency Access Methods”](#) on page 32.

For instructions on setting the reserve password, see the RSA Security Center Help topic “Setting a Reserve Password.”

Step 3: Configure Local Authentication

Once you specify which local users to challenge and, if appropriate, set a reserve password, local authentication is fully functional. All additional local authentication options assume default settings. However, you may want to change the default settings to better suit your environment. The Local Authentication page in the RSA Security Center guides you to the settings for configuring local authentication. For more information, see the RSA Security Center Help topic “Configuring Local Authentication.”

5

Configuring Domain Authentication

Domain authentication requires users to provide RSA SecurID passcodes to log on to domain client computers using domain accounts, and to perform the following tasks:

- Log on to the domain.
- Mount a network drive in the domain as an alternate user.
- Access a protected domain using the **net use** and **runas** commands.

For more information, see Chapter 11, [“Protecting Terminal Servers and Performing Common Windows Operations.”](#)

Once a user authenticates to a protected domain, for as long as the session certificate remains valid, the user can access different resources within the domain without having to reauthenticate. Additionally, you can configure cross-domain authentication so users can cross between protected domains without having to reauthenticate, and between a protected domain and an unprotected domain. For instructions, see [“Configuring Cross-Domain Authentication”](#) on page 58. For information about cross-realm limitations, see [“Cross-Realm Limitations”](#) on page 30.

Enabling firewalls on the domain controller or domain client computers may cause the authentication process to take longer. For more information about possible behavior when firewalls are enabled, see [“Active Directory Password Takes Longer than Usual to Appear”](#) and [“Domain Authentication Fails”](#) on page 105.

This chapter describes the steps for enabling and configuring domain authentication. It also describes the main domain authentication configuration options, and scenarios that require configuration that you must perform outside of the RSA Security Center.

The instructions in this chapter assume you have:

- Installed the RSA Certificate Utility and created the root and server certificates.
For instructions, see [“Step 1: Install the RSA Certificate Utility”](#) on page 41, and [“Step 2: Create Certificates”](#) on page 42.
- Installed the domain authentication components.
For instructions, see [“Step 3: Install RSA Authentication Agent 6.1 for Microsoft Windows”](#) on page 43.

Step 1: Select a Domain Authentication Challenge Setting

Selecting a challenge setting tells the Authentication Agent which domain users to challenge for RSA SecurID passcodes. For example, if you challenge all users, anyone who attempts to access domain resources is prompted to enter a valid RSA SecurID passcode. Alternately, if you challenge only specific users, only those users are prompted to enter RSA SecurID passcodes. For instructions, see the RSA Security Center Help topic “Selecting a Domain Authentication Challenge Setting.”

Step 2: Test Domain Authentication

To test domain authentication, you run the domain authentication service in one of the following test modes:

Silent authentication test mode. Verifies the connection between the domain controller and the domain client computer.

The domain authentication service establishes an SSL session and sends one message to the client computer. The domain authentication service logs a success or failure entry about the message transmission, and then drops the connection. The user of the client computer is not prompted to enter a passcode.

Interactive authentication test mode. Verifies the connections between the domain controller and the domain client computer, and the connection between the domain controller and the RSA Authentication Manager.

The domain authentication service performs all of the steps for normal authentication, including prompting the user for a passcode. However, in test mode the user is granted access to the protected domain resources even if the user exceeds the number of allowed bad passcodes or cancels the authentication. For example, if your system allows a maximum of three bad passcodes, and the user receives an **Access Denied** message three times or cancels out of the authentication, the user is still granted access to the protected resource even though the authentication failed.

You test domain authentication through the RSA Security Center. For instructions, see the RSA Security Center Help topic “Testing Domain Authentication.”

Important: After testing domain authentication, set the authentication mode back to **Normal**. For instructions, see the RSA Security Center Help topic “Setting the Domain Authentication Environment.”

Step 3: Configure the RSA Authentication Agent on the Domain Controller

Once you select a domain authentication challenge setting, domain authentication is functional. All additional configuration options assume default settings. However, you may want to change the default settings to better suit your environment. The Domain Server Configuration page in the RSA Security Center guides you to the settings for configuring the Authentication Agent on the domain controller. For more information, see the RSA Security Center Help topic, “Configuring the Authentication Agent on the Domain Server.”

The following sections describe the main domain authentication configuration options.

Reconnection After Offline Authentication

You can configure the RSA Authentication Agent to automatically reconnect users to protected domains after they have authenticated offline using either RSA SecurID passcodes or emergency codes.

Suppose a user logs on to a protected laptop while it is offline. Without logging out, the user connects the laptop to a network docking station. If reconnection after offline authentication is enabled, the user gains access to the protected domain without being prompted again for authentication credentials.

You set reconnection after offline authentication from the RSA Security Center Domain Access Settings page. For more information, see the RSA Security Center Help topic “Allowing Reconnection After Offline Authentication.”

Configurable Session Certificate Lifetime

Domain authentication uses the following digital certificates to protect authentication data transmitted across the network:

- The root certificate (**sdroot.crt**) that enables secure communication of passcodes and session certificates between the protected domain controller and the domain client computers.
- The server certificates for each domain controller (domain environment) or file server (workgroup environment).

For more information, see [“Step 2: Create Certificates”](#) on page 42.

When a user successfully authenticates to a protected domain, the domain controller issues a session certificate to the user. The certificate is used to authenticate the user transparently when the user attempts to access resources within the domain. The session certificate proves that the user already authenticated successfully and should not be prompted again to enter an RSA SecurID passcode until the session certificate expires.

By default, the lifetime of session certificates is 5 minutes. However, you can use the RSA Security Center to configure the lifetime of session certificates (1 - 999 minutes).

You configure the session certificate lifetime from the RSA Security Center Domain Access Settings page. For more information, see the RSA Security Center Help topic “Setting the Session Lifetime.”

Step 4: Configure the RSA Authentication Agent on Domain Clients

Configuring the Authentication Agent on domain client computers determines how users authenticate using their domain accounts to the Windows desktop on domain client computers. The Domain Client Configuration page in the RSA Security Center guides you to the settings for configuring the Authentication Agent on domain client computers. For more information, see the RSA Security Center Help topic, “Configuring the Authentication Agent on the Domain Client.”

Configuring Cross-Domain Authentication

You can configure domain authentication so users can cross between protected domains without having to reauthenticate with RSA SecurID passcodes.

You can also configure authentication between protected and unprotected domains. With cross-domain authentication, users who cross into unprotected domains are not prompted for RSA SecurID passcodes. Users who cross into protected domains are prompted for RSA SecurID passcodes.

To configure cross-domain authentication between protected domains:

1. Use the RSA Certificate Utility to create one root certificate and two server certificates (one for each domain controller).
Use the same root certificate to create both server certificates.
2. Install the Domain Authentication Server component on both domain controllers.
Use the same root certificate for both installations.
3. Install the Domain Authentication Client component on the domain clients in both domains.
Use the root certificate you generated in step1 for all of the installations.
4. Configure the RSA Authentication Agent on each domain controller to challenge the appropriate users.
5. If the domain controllers share the same RSA Authentication Manager, and you want to use Windows password integration and the Recharge Offline Days tool across domains, copy the **domaininfo.dat** file from the older domain controller to the newer one.
6. To stop and restart the offline authentication service, click **Control Panel > Administrative Tools > Services > RSA Authentication Agent Offline DomainHost**.
By default, the **domaininfo.dat** file is located in the **C:\Windows\SYSTEM32\sysvol\Domain\RSA Security\DomainHost** directory.

To configure cross-domain authentication between a protected and unprotected domain:

1. Use the RSA Certificate Utility to create one root certificate, and two server certificates (one server certificate for the protected domain, and another for the unprotected domain).
For instructions, see [“Step 2: Create Certificates”](#) on page 42.
Use the same root certificate to create both server certificates.
2. Install the Domain Authentication Server component on both domain controllers.
Use the same root certificate for both installations.
3. On each domain controller, create accounts for all users who will access the domain.

4. Install the Domain Authentication Client component on the client computers in both domains.
For all of the installations, use the root certificate you generated in step 1.
5. Configure RSA Authentication Agent in the protected domain to challenge the appropriate users.
6. Configure the RSA Authentication Agent on the domain controller in the unprotected domain so **Challenge** is set to **OFF**.

Using Domain Authentication with Remote Access Authentication

If your domain is protected with RSA Authentication Agent 6.1 for Microsoft Windows, and includes remote access applications, domain authentication and remote access authentication are incompatible. You can solve this problem by using the Windows Active Directory Users and Computers interface to create groups of remote access application hosts, and then using the RSA Security Center on the domain controller to tell the Authentication Agent how to address the hosts during authentication.

If an RSA SecurID application is installed on your remote access application, (for example, RSA Authentication Agent 5.3 for Web), you use the **Verify** option to tell the Authentication Agent to verify whether the remote access application host recently made a valid authentication request to the RSA Authentication Manager. If no RSA SecurID application is installed on your remote access application, you use the **Exclude** option to tell the Authentication Agent not to challenge requests from the remote access application host.

Using the Verify Option

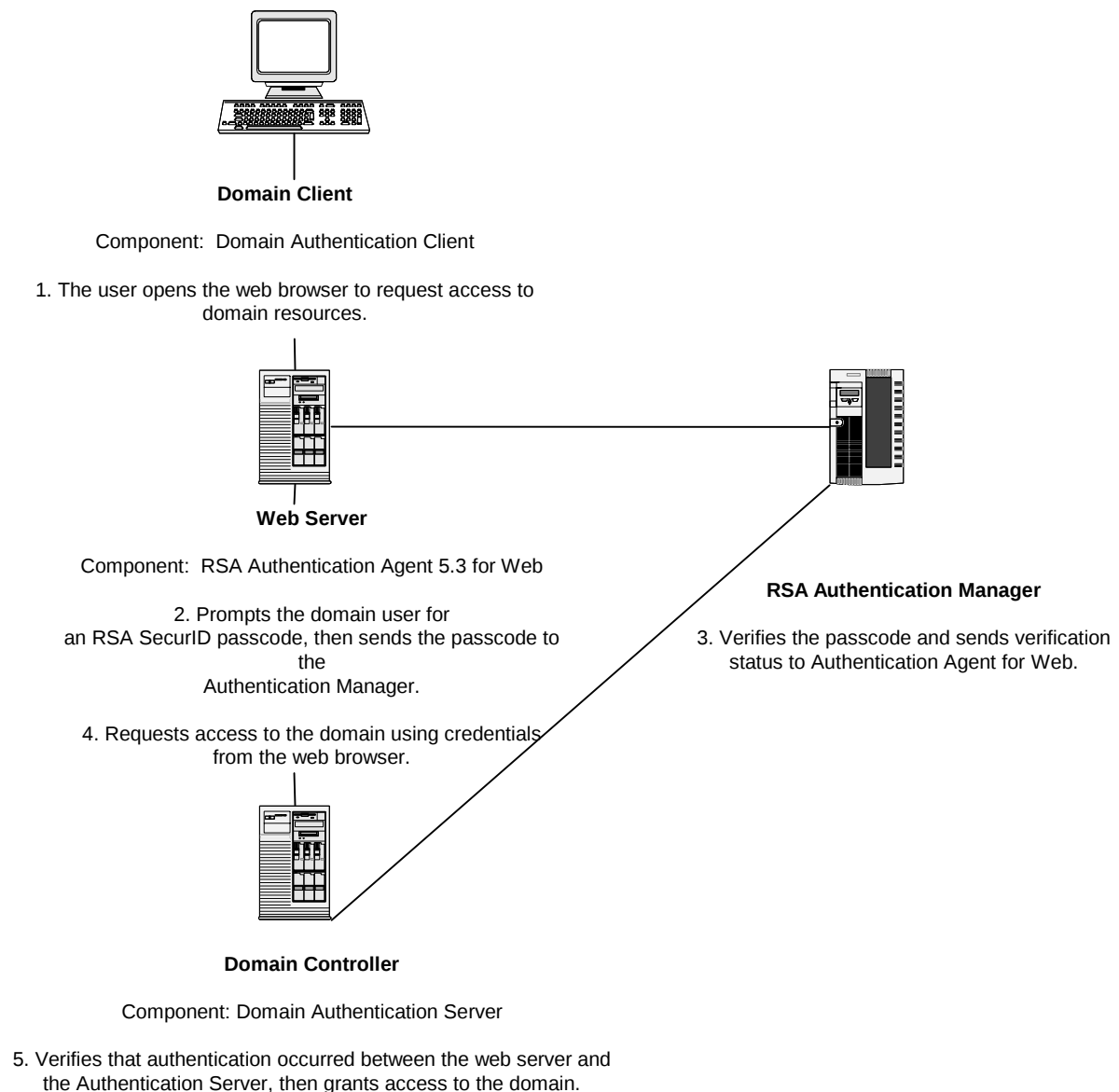
Assume that a remote user goes through a web server that is protected with RSA Authentication Agent 5.3 for Web to access a domain that is protected with RSA Authentication Agent 6.1 for Microsoft Windows. The user authenticates to the protected web server, and the web server passes the authentication request to the RSA Authentication Manager. However, if the web server is part of a protected Windows domain, and the web site is configured to require Windows authentication, the user must also authenticate to the domain controller. The web server, however, is not equipped to perform RSA SecurID authentication through the protected domain controller.

You can solve this problem by first creating a group for the remote access application server host (in this scenario, the web server), and then selecting **Verify** in the RSA Security Center. Selecting **Verify** instructs the Authentication Agent on the domain controller to verify whether the remote access application server recently made a valid authentication request to the RSA Authentication Manager. If so, the user gains access to the domain. For instructions on selecting the **Verify** option, see the RSA Security Center Help topic “Enabling Domain Authentication With Remote Authentication.”

For verification to work for a particular Agent Host, the RSA Authentication Manager administrator must select **Create Verifiable Authentications** for the host in the RSA Authentication Manager Database Administration application. This option is disabled by default. Also, the Authentication Agent on the verified computer must be configured to communicate to the same RSA Authentication Manager realm as the domain controller. For more information, see the chapter “Agent and Activation on Agent Hosts” in the *RSA Authentication Manager 6.1 Administrator’s Guide*.

Verification Process

Users can gain access to the domain through verification only within 10 minutes of authenticating to the remote access application.



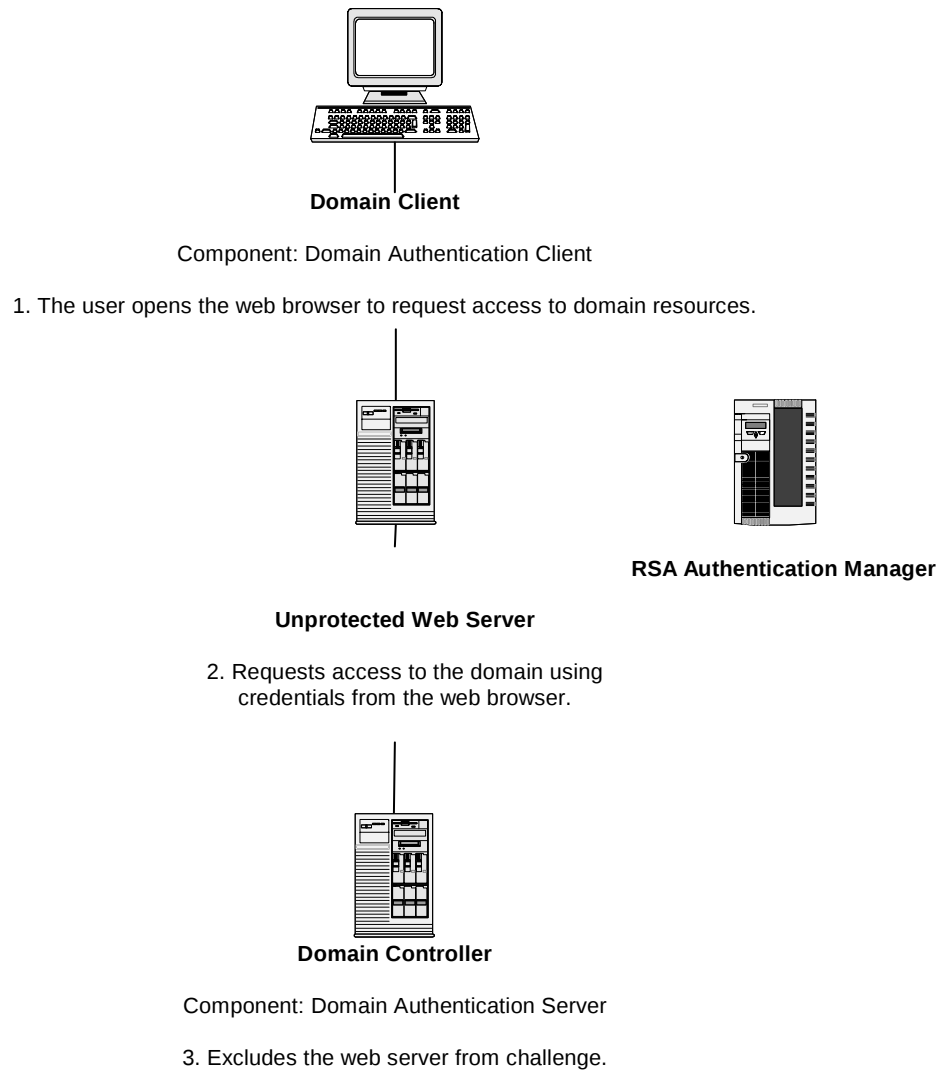
Important: To use **Verify**, you must configure your web server appropriately. For instructions, see Appendix D, “[Configuring Web Servers for RSA SecurID Authentication](#).”

Using the Exclude Option

Assume a remote user attempts to access a protected domain through a web server that is not protected by RSA Authentication Agent 5.3 for Web and, therefore, does not have RSA SecurID capabilities. The web server has no way to communicate with the RSA Authentication Manager. You can solve this problem by first creating a group for the web server, and then selecting **Exclude** in the RSA Security Center to instruct the Authentication Agent on the domain controller to exclude from challenge all authentication requests from the web server. For instructions on selecting the **Exclude** option, see the RSA Security Center Help topic “Enabling Domain Authentication With Remote Authentication.”

Exclusion Process

Important: To use **Exclude**, you must configure your web server appropriately. For instructions, see Appendix D, [“Configuring Web Servers for RSA SecurID Authentication.”](#)



If a remote access application host is in two groups, and one group is set for verification while the other is set for exclusion, the **Verify** option is active and the **Exclude** option is ignored.

Saving Changes to a Roaming Profile

If you use domain authentication in an environment where users have roaming profiles, you will not have problems saving your roaming profile unless your session certificate expires. To prevent this from happening, use RSA Security Center on the domain controller to set the session certificate to never expire. For instructions, see the Help topic “Setting the Session Lifetime.”

6

Configuring Remote Authentication

Remote authentication requires users to provide valid RSA SecurID passcodes to establish remote connections to the network using VPN clients or post-dial terminal windows. When a user attempts to establish a remote connection, the RSA Authentication Agent prompts the user for RSA SecurID credentials. Authorized users establish connections easily, but unauthorized users are denied the connection.

This chapter describes the steps for enabling and configuring remote authentication in the following types of environments:

- Non-EAP
- EAP

It also describes key remote configuration options.

Important: The instructions in this chapter assume you have already installed the RSA Authentication Agent remote authentication components required for your environment and tested authentication to create a node secret. Without a node secret, the Authentication Agent cannot communicate with the Authentication Manager. For instructions, see [“Step 3: Install RSA Authentication Agent 6.1 for Microsoft Windows”](#) on page 43.

Deploying Remote Authentication 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 client computers.

In post-dial terminal based environments, the Authentication Agent supports the following group deployments:

- 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 where a user is logged on, 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 where a user is logged on, 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: Select a Remote Authentication Challenge Setting

Selecting a challenge setting tells the Authentication Agent which remote users to challenge for RSA SecurID passcodes. For example, if you challenge all users, anyone who attempts to open a remote connection is prompted to enter a valid RSA SecurID passcode. If you challenge only specific users, when these users attempt to open a remote connection, they are prompted to enter their RSA SecurID passcodes. For instructions, see the RSA Security Center Help topic “Specifying Who to Challenge.”

Step 2: Configure the RSA Authentication Agent on the Remote Server

The Post-dial Configuration page in the RSA Security Center guides you to the settings for configuring the Authentication Agent on the remote server in a post-dial terminal based environment. For more information, see the RSA Security Center Help topic “Configuring the Authentication Agent for Post-Dial Connections.”

Step 3: Configure the Remote Client Computers for Post-Dial Terminal Based Connections

To configure the remote client computers for post-dial terminal based authentication, follow the instructions in your Microsoft documentation. For the type of security, select **Show terminal window**.

Deploying Remote Authentication With EAP

You can configure the following EAP solutions:

Non-RADIUS. Does not use a RADIUS server.

Microsoft IAS RADIUS Server. Uses Microsoft IAS RADIUS Server. This solution uses the RSA Security Center to configure remote authentication.

RSA RADIUS Server. Uses RSA RADIUS Server, which is shipped with the RSA Authentication Manager. This solution does not require the Authentication Agent remote authentication component.

Deploying Remote Authentication Using EAP Without RADIUS

Step 1: Create Access Groups in Microsoft Active Directory

Create user groups to control access for the types of connections you want to use. For instructions, see your Microsoft Active Directory documentation.

Step 2: Configure the RRAS Server for EAP

Follow the instructions in your Microsoft documentation to configure the RRAS server for EAP. Do the following:

- Configure **Server Security Authentication** to use **Windows Authentication**.
- Configure a remote access policy that matches your selections for **Remote Access Type** and **User Group**.

- Edit the Access Policy Authentication methods to add one or both of the following EAP types:
 - **RSA Security EAP**
 - **RSA Security EAP - Protected OTP**
- Because RSA Security EAP uses 128-bit encryption keys, for the encryption type, select **Strongest**, and clear all other encryption options.

Step 3: Configure the Remote Client Computers for EAP

Follow the instructions in your Microsoft documentation to configure your connections. For each connection, you must configure the security type to use one of the following:

- **RSA Security EAP**
- **RSA Security EAP - Protected OTP**

Step 4: Configure the RSA Authentication Agent on the Remote Server

The Remote EAP Configuration page in the RSA Security Center guides you to the settings for configuring the Authentication Agent on the remote server in an EAP environment. For more information, see the RSA Security Center Help topic “Configuring the Authentication Agent for EAP.”

Deploying Remote Authentication Using EAP With Microsoft IAS RADIUS Server

Step 1: Create Access Groups in Microsoft Active Directory

Create user groups to control access for the types of connections you want to use. For instructions, see your Microsoft Active Directory documentation.

Step 2: Configure the RRAS Server for RADIUS

Follow the instructions in your Microsoft documentation to configure the RRAS server for RADIUS. Do the following:

- Configure **Server Security Authentication** to use **RADIUS Authentication**.
- Configure the RADIUS server connection parameters.

Step 3: Configure the Microsoft IAS RADIUS Server for EAP

Follow the instructions in your Microsoft documentation to configure the Microsoft IAS RADIUS server for EAP. Do the following:

- Configure the RRAS server as a RADIUS client.
- Configure a remote access policy that matches your selections for **Remote Access Type** and **User Group**.

- Follow the instructions in your Microsoft documentation to configure your connections. For each connection, you must configure the security type to use one of the following:
 - **RSA Security EAP**
 - **RSA Security EAP - Protected OTP**
- Because RSA Security EAP uses 128-bit encryption keys, for the encryption type, select **Strongest**, and clear all other encryption options.

Step 4: Configure the Remote Client Computers for EAP

Follow the instructions in your Microsoft documentation to configure your connections. For each connection, you must configure the security type to use one of the following:

- **RSA Security EAP**
- **RSA Security EAP - Protected OTP**

Step 5: Configure the RSA Authentication Agent on the Remote Server

The Remote EAP Configuration page in the RSA Security Center guides you to the settings for configuring the Authentication Agent on the remote server in an EAP environment. For more information, see the RSA Security Center Help topic “Configuring the Authentication Agent for EAP.”

Deploying Remote Authentication Using EAP With RSA RADIUS Server

Step 1: Configure the RSA RADIUS Server

For each of your RADIUS client systems, do the following:

- Use the RADIUS Administrator to configure the IP address, ports, secret, and system type.
- Configure an Agent Host as a Communication Server type, and check **Open to All Locally Known Users** for each RADIUS client.

Note: If the option **CheckUserAllowedByClient** in the **securid.ini** file on the RADIUS Server host equals 0, you do not have to perform this step. The **securid.ini** file is in the **Program Files\RSA Security\RSA RADIUS\Service** directory.

- Define profiles to restrict user access.
RSA RADIUS Server does not use Windows groups to control access. By default, all access attempts are authenticated. If you want to restrict access based on RADIUS attribute values, use the RSA RADIUS Administration program to configure access profiles. You must also define the profiles in the RSA Authentication manager and assign the profiles to users.

Step 2: Configure the RADIUS Clients for RSA RADIUS

On each RADIUS client, configure the IP address, ports, and secret to match the RSA RADIUS Server settings.

Step 3: Configure the Remote Client Computers for EAP

Follow the instructions in your Microsoft documentation to configure connections with PEAP. For the EAP type, select one of the following:

- **RSA Security EAP**
- **RSA Security EAP - Protected OTP**

Changing the Time-Out Values for Remote Access Prompts

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

For example, RSA SecurID hardware token users have to wait up to 60 seconds for their next token codes to display. The remote access prompts may time out before users can send their passcodes to the Authentication Agent. In this case, you can change the time-out values to prevent the prompts from timing out too soon.

The two remote access prompt time-out values are the following:

Initial time-out. Sets the wait time, in seconds, before the initial remote access prompt appears.

Regular time-out. Sets the number of seconds before remote access prompts time out.

For instructions on changing these values, see the RSA Security Center Help topic “Changing the Time-out Values of the Remote Authentication Prompts.”

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

Authenticating from Remote Computers

Users can authenticate from remote computers using these types of connections:

- Post-dial terminal based without EAP
- Dial-up or VPN with EAP

For authentication instructions specific to the types of RSA SecurID tokens you plan to deploy, see *Authenticating With an RSA SecurID Token*. This document is distributed with the RSA Authentication Manager software.

For instructions on changing the default time-out values of RSA SecurID remote access prompts, see the previous section, “[Changing the Time-Out Values for Remote Access Prompts](#)” and the RSA Security Center Help topic “Changing the Time-out Values of the Remote Authentication Prompts.”

If you are using RSA Security EAP - Protected OTP or RSA Security EAP and a user attempts to establish a remote connection, the system presents the user with an 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.

7

Configuring Wireless Authentication

Wireless authentication requires users to provide valid RSA SecurID passcodes to establish wireless connections to protected networks. When a user attempts to establish a wireless connection, the RSA Authentication Agent prompts the user for RSA SecurID credentials. Authorized users establish connections easily, but unauthorized users are denied the connection.

This chapter describes the steps for enabling and configuring remote authentication in the following types of environments:

- Non-EAP
- EAP

Important: The instructions in this chapter assume you have already installed the RSA Authentication Agent remote authentication components required for your environment and tested authentication to create a node secret. Without a node secret, the Authentication Agent cannot communicate with the Authentication Manager. For instructions, see [“Step 3: Install RSA Authentication Agent 6.1 for Microsoft Windows”](#) on page 43.

Deploying Wireless Authentication With RSA Security EAP - Protected OTP

By using RSA Security EAP - Protected OTP, you eliminate the need for authentication certificates and additional tunneling.

There are two wireless Protected OTP solutions.

RSA RADIUS Server. Uses RSA RADIUS Server, which is shipped with RSA Authentication Manager. This solution does not use the RSA Security Center to configure remote authentication.

Microsoft IAS RADIUS Server. Uses Microsoft IAS RADIUS Server. This solution uses the RSA Security Center to configure remote authentication.

Deploying RSA Security EAP - Protected OTP With RSA RADIUS Server

Step 1: Set Up the Wireless LAN Environment

To set up the wireless LAN environment:

- Configure the authentication protocol for 802.1x
- Enable the EAP protocol.

- Configure the encryption mode for 128-bit encryption.
RSA Security EAP - Protected OTP returns 128-bit keys that can be used with WEP, Temporal Key Integrity Protocol (TKIP), and Advanced Encryption Standard (AES) as described in Wi-Fi Protected Access (WPA) or WPA2 specifications.
- Configure the RADIUS authentication settings so the access point uses the IP address and secret of the RADIUS Server.

For specific instructions, see your access point software documentation.

Step 2: Configure the RSA RADIUS Server

To configure the RSA RADIUS Server:

- For each wireless access point system:
 - Use the RADIUS Administrator to configure the IP address, ports, secret, and system type.
 - Configure an Agent Host as a Communication Server type, and check **Open to All Locally Known Users** for each RADIUS client.

Note: If the option **CheckUserAllowedByClient** in the **securid.ini** file on the RADIUS Server host equals 0, you do not have to perform this step. The **securid.ini** file is in the **Program Files\RSA Security\RSA RADIUS\Service** directory.

- Define profiles to restrict user access
RSA RADIUS Server does not use Windows groups to control access. By default, all access attempts are authenticated. If you want to restrict access based on RADIUS attribute values, use the RSA RADIUS Administration program to configure access profiles. You must also define the profiles in the RSA Authentication Manager and assign the profiles to users. If you do not assign a profile to a user, RSA RADIUS Server defines and applies a **Default** profile.

Step 3: Configure the Remote Client Computers

Follow the instructions in your Microsoft documentation to configure wireless connections. Configure the following:

- Association Phase
 - For Authentication, select **WPA** or to open authentication with keys provided automatically.
 - For data encryption, select **WEP**, **TKIP**, or **AES**.
- Authentication Phase
 - Enable **IEEE 802.1x Authentication**.
 - Select **RSA Security EAP - Protected OTP** as the EAP type.
 - Clear **Authenticate As Computer**.

Deploying RSA Security EAP - Protected OTP With Microsoft IAS RADIUS Server

Step 1: Set Up the Wireless LAN Environment

To set up the wireless LAN environment, configure each wireless access point as follows:

- Configure the authentication protocol for 802.1x
- Enable the EAP protocol.
- Configure the encryption mode for 128-bit encryption.
RSA Security EAP - Protected OTP returns 128-bit keys that can be used with WEP, Temporal Key Integrity Protocol (TKIP), and Advanced Encryption Standard (AES) as described in Wi-Fi Protected Access (WPA) or WPA2 specifications.
- Configure the RADIUS authentication settings so the access point uses the IP address and secret of the RADIUS Server.

For specific instructions, see your access point software documentation.

Step 2: Create Access Groups in Microsoft Active Directory

Create user groups to control access for the types of connections you want to use. For instructions, see your Microsoft Active Directory documentation.

Step 3: Configure the Microsoft IAS RADIUS Server

Follow the instructions in your Microsoft documentation to configure the Microsoft IAS RADIUS server for PEAP. Do the following:

- Configure each wireless access point as a RADIUS client.
- Configure a remote access policy that matches your selections for **Remote Access Type** and **User Group**.
- Edit the access policy authentication methods to add all of the EAP types:
 - **RSA Security EAP - Protected OTP**
 - **RSA Security EAP**
- Because RSA Security EAP uses 128-bit encryption keys, for the encryption type, select **Strongest**, and clear all other encryption options.

Step 4: Configure the Remote Client Computers

Follow the instructions in your Microsoft documentation to configure wireless connections with PEAP. Configure the following:

- Association Phase
 - Configure authentication for WPA or to open authentication with keys provided automatically.
 - Configure data encryption for WEP, TKIP, or AES.

- Authentication Phase
 - Enable **IEEE 802.1x Authentication**.
 - Select **RSA Security EAP - Protected OTP** as the EAP type.
 - Clear **Authenticate As Computer**.

Step 5: Configure the RSA Authentication Agent on the Remote Server

The Remote EAP Configuration page in the RSA Security Center guides you to the settings for configuring the Authentication Agent on the remote server in an EAP environment. For more information, see the RSA Security Center Help topic “Configuring the Authentication Agent for EAP.”

Deploying Wireless Authentication with PEAP

There are two PEAP solutions:

RSA RADIUS Server. Uses RSA RADIUS Server, which is shipped with RSA Authentication Manager. This solution does not use the RSA Security Center to configure remote authentication.

Microsoft IAS RADIUS Server. Uses Microsoft IAS RADIUS Server. This solution uses the RSA Security Center to configure remote authentication.

Deploying PEAP With RSA RADIUS Server

Step 1: Obtain Certificates for the Server and Clients

When you use wireless authentication with PEAP, both servers and clients use certificates to verify their identities to one another.

Server certificates must meet the following requirements:

- The certificate must be in PKCS#12 .pfx file format with a private key and all of the certificates necessary to establish the chain to the issuing certificate authority (CA).
- The certificates cannot be self-signed.
- The **certinfo.ini** file in the **Program Files\RSA Security\RSA RADIUS Service** directory on the RSA RADIUS Server host must point to the .pfx file.
- Key usage must be set in one of the following ways:
 - Key usage unspecified.
 - **digitalSignature** or **keyEncipherment** is set with either no extended key usage or **serverAuth**, **msSGC** or **nsSGC**.

Client certificates must meet the following requirements:

- Key usage must be set in one of the following ways:
 - Key usage unspecified.
 - **digitalSignature** is set with either no extended key usage or **clientAuth** is specified.
- If the certificate is a Netscape certificate, the client bit must be set. If the certificate is a CA certificate only, select only extended key usage.

Step 2: Configure the RSA RADIUS Server

To configure the RSA RADIUS Server:

- For each wireless access point system:
 - Use the RADIUS Administrator to configure the IP address, ports, secret, and system type.
 - Configure an Agent Host as a Communication Server type, and check **Open to All Locally Known Users** for each RADIUS client.

Note: If the option **CheckUserAllowedByClient** in the **securid.ini** file on the RADIUS Server host equals 0, you do not have to perform this step. The **securid.ini** file is in the **Program Files\RSA Security\RSA RADIUS\Service** directory.

- Install the server certificate and configure the **certinfo.ini** file on the RSA RADIUS Server to include the name and password of the server certificate. The **certinfo.ini** file is in the **Program Files\RSA Security\RSA RADIUS Service** directory.
- Define profiles to restrict user access
RSA RADIUS Server does not use Windows groups to control access. By default, all access attempts are authenticated. If you want to restrict access based on RADIUS attribute values, use the RSA RADIUS Administration program to configure access profiles. You must also define the profiles in the RSA Authentication Manager and assign the profiles to users. If you do not assign a profile to a user, RSA RADIUS Server defines and applies a **Default** profile.

Step 3: Set Up the Wireless LAN Environment

To set up the wireless LAN environment, configure each wireless access point as follows:

- Configure the authentication protocol for 802.1x
- Enable the EAP protocol.
- Configure the encryption mode for 128-bit encryption.
PEAP returns 128-bit keys that can be used with WEP, Temporal Key Integrity Protocol (TKIP), and Advanced Encryption Standard (AES) as described in Wi-Fi Protected Access (WPA) or WPA2 specifications.
- Configure the RADIUS authentication settings so the access point uses the IP address and secret of the RADIUS Server.

For specific instructions, see your access point software documentation.

Step 4: Configure the Remote Client Computers

Follow the instructions in your Microsoft documentation to configure wireless connections with PEAP. Configure the following:

- Association Phase
 - For Authentication, select **WPA** or to open authentication with keys provided automatically.
 - For data encryption, select **WEP**, **TKIP**, or **AES**.
- Authentication Phase
 - Enable **IEEE 802.1x Authentication**.
 - Select **Protected EAP (PEAP)** as the EAP type.
 - Clear **Authenticate As Computer**.
- PEAP Properties
 - Select **RSA Security EAP** or **RSA Security EAP - Protected OTP**
 - Check **Enable Fast Reconnect**

Deploying PEAP With Microsoft IAS RADIUS Server

Step 1: Create Access Groups in Microsoft Active Directory

Create user groups to control access for the types of connections you want to use. For instructions, see your Microsoft Active Directory documentation.

Step 2: Obtain Certificates for the Server and Clients

When you use wireless authentication with PEAP, both servers and clients use certificates to verify their identities to one another.

All certificates must meet the following minimum requirements:

- X.509 format
- Secure Sockets Layer (SSL) encryption
- Transport Layer Security (TLS) encryption

Additionally, all certificates must be configured with at least one purpose object identifier. For example, a certificate that is used to authenticate from a client to a server must be configured with the Client Authentication purpose. The purpose is recorded in the certificate's Extended Key Usage (EKU) extension. During authentication, the authenticator examines the certificate to verify that its purpose object identifier matches the way the certificate is being used.

Server certificates must meet the following requirements:

- The certificate must chain to one of the following:
 - A trusted Microsoft root CA.
 - A Microsoft standalone root or third-part root certificate authority in an Active Directory domain. The Active Directory domain must have an NTAAuthCertificates store that contains the published root certificate.

- If the certificate is a Netscape certificate, the client bit must be set. If the certificate is a CA certificate only, extended key usage must be selected.
- The certificate must be configured with the Server Authentication purpose.
- The certificate must pass the checks that are performed by the CryptoAPI certificate store, and must pass all of the requirements in the remote access policy.
- The name in the subject line of the certificate must match the name that is configured for the connection on the client.
- The Subject Alternative Name (SubjectAltName) extension contains the fully qualified domain name of the server.

If a client is configured to trust a specific server certificate by name, users are prompted to decide whether to trust certificates with different names. If a user rejects a certificate, authentication fails. If the user accepts the certificate, the certificate is added to the trusted root store on the user's computer.

Client certificates must meet the following requirements:

- The certificate must be issued by an enterprise CA or must map to a user account or computer account in Active Directory.
- The user or the computer certificate on the client must chain to a trusted root CA.
- The certificate must include the Client Authentication purpose.
- The certificate must pass the checks that are performed by the CryptoAPI certificate store, and must pass all of the requirements in the remote access policy.
- The certificate must pass the certificate object identifier checks that are specified in the Internet Authentication Service (IAS) remote access policy.
- The certificate must not be a registry-based smart card certificate or a certificate that is protected with a password.
- The Subject Alternative Name (Subject AltName) extension in the certificate must contain the user principal name (UPN) of the user.

You can get certificates automatically by using the Microsoft Windows Certificate Authority and the IIS Server Auto-enrollment feature. For more information, see your Microsoft Windows documentation.

Step 3: Set Up the Wireless LAN Environment

To set up the wireless LAN environment, configure each wireless access point as follows:

- Configure the authentication protocol for 802.1x
- Enable the EAP protocol.
- Configure the encryption mode for 128-bit encryption.
PEAP returns 128-bit keys that can be used with WEP, Temporal Key Integrity Protocol (TKIP), and Advanced Encryption Standard (AES) as described in Wi-Fi Protected Access (WPA) or WPA2 specifications.
- Configure the RADIUS authentication settings so the access point uses the IP address and secret of the RADIUS Server.

For specific instructions, see your access point software documentation.

Step 4: Configure the Microsoft IAS RADIUS Server for PEAP

Follow the instructions in your Microsoft documentation to configure the Microsoft IAS RADIUS server for PEAP. Do the following:

- Configure each wireless access point as a RADIUS client.
- Configure a remote access policy that matches your selections for **Remote Access Type** and **User Group**.
- Edit the access policy authentication methods to add all of the EAP types:
 - **Protected EAP (PEAP)**
 - **RSA Security EAP - Protected OTP**
 - **RSA Security EAP**
- Because RSA Security EAP uses 128-bit encryption keys, for the encryption type, select **Strongest**, and clear all other encryption options.

Step 5: Configure the Remote Client Computers for PEAP

Follow the instructions in your Microsoft documentation to configure wireless connections with PEAP. Configure the following:

- Association Phase
 - Configure authentication for WPA or to open with keys provided automatically.
 - Configure data encryption for WEP, TKIP, or AES.
- Authentication Phase
 - Enable **IEEE 802.1x Authentication**.
 - Select **Protected EAP (PEAP)** as the EAP type.
 - Clear **Authenticate As Computer**.
- PEAP Properties
 - Select **RSA Security EAP** or **RSA Security EAP - Protected OTP**
 - Check **Enable Fast Reconnect**

Step 6: Configure the RSA Authentication Agent on the Remote Server

The Remote EAP Configuration page in the RSA Security Center guides you to the settings for configuring the Authentication Agent on the remote server in an EAP environment. For more information, see the RSA Security Center Help topic “Configuring the Authentication Agent for EAP.”

Authenticating Using Wireless Connections

For authentication instructions specific to the types of RSA SecurID tokens you plan to deploy, see *Authenticating with an RSA SecurID Token*. This document is distributed with the RSA Authentication Manager software.

Initiating a wireless connection causes a Windows tool tip to appear on the Windows taskbar. To continue authentication, users must click the tool tip. At the authentication prompt, users must enter their user names within 30 seconds. Otherwise, the tool tip reappears and users must click it to restart authentication.

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

8

Configuring Advanced and Troubleshooting Settings

Configuring Advanced Settings

The advanced settings enable you to:

- Clear the node secret from the Authentication Agent Host.
See the following section, [“Clearing and Replacing the Node Secret.”](#)
- Clear offline data from an Agent Host.
See [“Clearing Offline Data”](#) on page 82.
- Set an IP address override for the Authentication Agent Host primary network interface.
See [“Setting an IP Address Override”](#) on page 83.
- Filter event messages out of the Windows Event Viewer Application Log.
See [“Filtering Event Messages Out of the Windows Event Viewer Log”](#) on page 83.

Clearing and Replacing the Node Secret

The node secret is a symmetric encryption key used by the Authentication Agent and the Authentication Manager to encrypt and decrypt packets of data as they travel across the network.

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

If the node secret on the Authentication Agent Host is corrupted or does not match the node secret in the RSA Authentication Manager database, encrypted communications between the Authentication Agent and the Authentication Manager cannot work. If this happens, the Authentication Manager logs the message **Access Denied, Node Verification Failed** in the RSA Authentication Manager Activity monitor. For more information about node verification failure, see [“Node Verification Fails”](#) on page 106.

To solve a node verification failure, you must clear the node secret from the Authentication Agent Host and, at the same time, instruct the RSA Authentication Manager administrator to clear the node secret specified for the Authentication Agent Host in the RSA Authentication Manager database. You then use the RSA Security Center to perform a test authentication on the Authentication Agent Host to create a new node secret for the Authentication Agent and store it in the Authentication Manager database.

For instructions on how to clear and replace the node secret on the RSA Authentication Agent Host, see the RSA Security Center Help topic “Clearing and Replacing the Node Secret.”

For instructions on how to clear and replace the node secret in the RSA Authentication Manager database, see the RSA Authentication Manager Help topic “Editing an Agent Host.”

Important: If you are using offline authentication, after you clear the node secret from an Agent Host, you must download additional offline data. Clearing the node secret on an Agent Host removes offline data from the Host.

Managing the Node Secret on RSA RADIUS Server

When RSA RADIUS Server is installed, it automatically creates a node secret and adds itself as an Agent Host in the RSA Authentication Manager database. You do not have to perform an authentication from the RSA RADIUS Server Host to generate the node secret.

Ordinarily, to clear or replace a node secret on an Agent Host, you use the RSA Security Center. However, because RSA RADIUS Server does not require an RSA Authentication Agent component to communicate with the Authentication Manager, the RSA Security Center does not exist on the RSA RADIUS Server Host, and there is no way to easily manage the node secret. For this reason, RSA Security recommends that you install the RSA Authentication Agent Local Authentication Client component on the RSA RADIUS Server, and set the Local Authentication challenge to **None**. You can then use the RSA Security Center only to manage the node secret.

Clearing Offline Data

Clearing offline data removes it from the Agent Host. Without offline data, the user cannot access the protected resource without connecting through the network.

You need to clear offline data under the following circumstances:

- You changed the offline settings on the RSA Authentication Manager (for example, you disabled offline authentication for an Agent, or you changed the number of offline days the Authentication Manager generates and downloads).
- You change the authenticator properties for an Agent user (for example, you clear the user’s PIN, or resynchronize the user’s authenticator).
- You want to reassign a protected computer to a different user.

Once you remove offline data from an Agent Host, the next time that computer successfully authenticates to the RSA Authentication Manager, the Authentication Manager generates new offline data and downloads it to the Agent Host. For instructions on clearing offline data, see the RSA Security Center Help topic “Clearing Offline Data.”

Setting an IP Address Override

When an RSA Authentication Agent runs on a host that has multiple network interface cards and, therefore, multiple IP addresses, you need to specify a primary Agent Host IP address for encrypted communications between the Authentication Agent Host and the RSA Authentication Manager. Agent Hosts typically attempt to discover their own IP addresses. In doing so, an Agent Host with multiple addresses might select one that is unknown to the RSA Authentication Manager, making communication between the RSA Authentication Agent and RSA Authentication Manager impossible.

For instructions on how to specify the primary IP address of the Authentication Agent, see the RSA Security Center Help topic “Setting an IP Address Override.”

Filtering Event Messages Out of the Windows Event Viewer Log

If your site has a large number of RSA SecurID users, logging all events can make it difficult to search the log for messages related to a specific incident. If that is the case, you can prevent certain event messages from being logged.

Note: You cannot use this setting to prevent the logging of error messages in the Windows Event Viewer Application Log. In addition, this setting does not prevent the logging of trace messages in the Event Viewer Log.

For instructions on how to filter messages, see the RSA Security Center Help topic “Filtering Event Messages Out of the Windows Event Viewer Log.”

Configuring Troubleshooting Settings

Trace logging is a useful debugging aid for you and your RSA Security Customer Support representatives. Because tracing has an impact on Authentication Agent performance, and to prevent possible “denial of service” problems, do not enable tracing unless you need to diagnose and resolve a problem.

You enable tracing and specify where tracing messages are logged from the Troubleshooting page in the RSA Security Center. For instructions, see the RSA Security Center Help topic “Understanding the Troubleshooting Settings.” These settings have no effect on tracing messages logged to the Windows Event Viewer logs.

9

Offline Authentication

Offline authentication extends RSA SecurID authentication to users when the connection to the RSA Authentication Manager is not available (for example, when users work away from the office, or when network conditions make the connection temporarily unavailable). You enable, disable, and configure offline authentication through the RSA Authentication Manager Database Administration Application. You can enable and disable offline authentication and set the number of offline days offline users receive for individual Authentication Agents, groups of users, or system-wide.

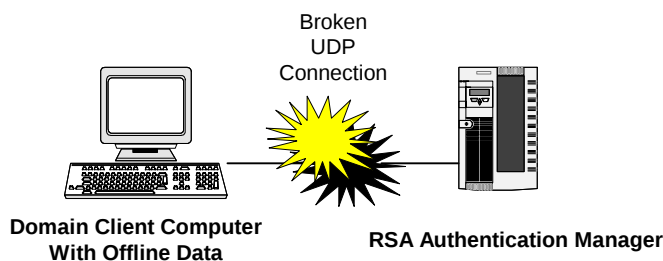
Offline Authentication with Local Authentication

If offline authentication is enabled with local authentication, when an RSA Authentication Agent connects to the RSA Authentication Manager, the Authentication Manager generates offline data (also called offline days) and downloads it to the Authentication Agent Host. Local Authentication Client hosts begin receiving offline data during their second connected authentication to the RSA Authentication Manager. For example, if you perform the authentication test described in [“Step 6: Test Authentication”](#) on page 51, and then authenticate to the Authentication Manager, the Authentication Manager generates and downloads the offline data.

By default, offline data is stored in **C:\DocumentsandSettings\All Users\Application Data\RSA Security\Local\dayfiles**. However, you can specify the location during installation. If you specify a location, offline data is stored in **specified_path\RSA Security\Local\dayfiles**. Only users with administrative privileges can view these encrypted files.

When a user authenticates offline, the Authentication Agent verifies the user’s authentication information against the offline data stored on the user’s computer. If the user’s authentication information is correct, the user gains access to the protected computer.

The following figure shows the system setup for offline authentication to a local computer.



Password Changes

Users who change their passwords while offline can still authenticate even though the new password does not match the password in the offline data. In this scenario, after presenting the RSA SecurID prompt, the system prompts users for their new passwords.

Note: Offline authentication does not support one-time passwords. For more information on lost token passwords, see “Temporary Passwords to Replace Lost Tokens” in Chapter 7, “Registering Users for Authentication” in the *RSA Authentication Manager 6.1 Administrator’s Guide*.

Clock Changes

Offline authentication monitors clock changes and maintains a system clock offset between the PC clock and the offline data. Users who change their PC clocks while offline instead of adjusting time zones can still authenticate.

CAUTION: If a user changes the PC clock by altering the BIOS, that user will not be able to authenticate.

Offline Authentication with Domain Authentication

If offline authentication is enabled for domain authentication, domain users can authenticate to:

- The domain when the connection between the RSA Authentication Manager and the domain controller is unavailable.
- Their local desktops using their domain accounts when the connection between the domain client and the domain controller is unavailable.

During a connected authentication, the RSA Authentication Manager generates offline data and downloads it to both the domain controller and the domain client computer. The data downloaded to the domain controller is a different type of data than what is downloaded to the domain clients, and uses less space.

Domain authentication server hosts begin receiving offline data during their second connected authentication to the RSA Authentication Manager. For example, if you perform the authentication test described in “[Step 6: Test Authentication](#)” on page 51, and then authenticate to the Authentication Manager, the Authentication Manager generates and downloads the offline data. Domain Authentication Client hosts begin receiving offline data during their first connection to the Authentication Manager.

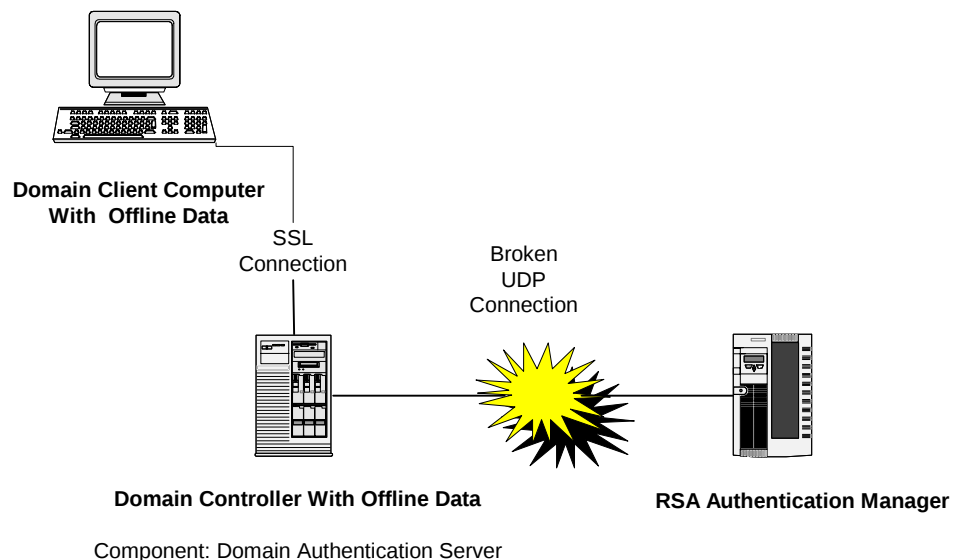
By default, the offline data is stored on the domain controller in **C:\windows\SYSVOL\systol\domain_name\rsa security\DomainHost\dayfiles**. However, during installation, you can choose to store the data in Windows Active Directory, or in the RSA Security file system. If you want to store the data in an Active Directory database, you must prepare the database before installing the Domain Authentication Server component. For instructions, see “[Prepare the Active Directory Database for Storing Offline Data](#)” on page 34.

On domain clients, by default, offline data is stored in **C:\Documents and Settings\All Users\Application Data\RSA Security\Domain\dayfiles**. If you choose to specify the storage location, offline data is stored in **specified_path\RSA Security\domain\dayfiles**. Only users with administrative privileges can view these encrypted files.

If the domain controller loses connection with the RSA Authentication Manager, the RSA Authentication Agent compares the authentication information with the offline data stored on the domain computers.

Important: For offline authentication to be fully functional in domain environments, **Allow access to the domain after offline authentication** must be enabled in the RSA Security Center. For more information, see the Help topic “Allowing Access to the Domain After Offline Authentication.”

The following figure shows the system setup for offline authentication to a protected domain.



If the connection between the domain client and the domain controller is broken, offline authentication works the same way it does for local computers so that users can log on locally to their domain client desktops.

Managing Offline Days

Recharging Offline Days

When a user's supply of offline days is low, offline days are automatically recharged when:

- The user authenticates to the network directly.
- After the user authenticates offline, the user connects to the network directly during the same authentication session (for example, if the Authentication Agent on the user's computer is configured for automatic reconnection after offline authentication).
- After authenticating offline, the user authenticates to the network remotely.

Even if the user's supply of offline days is full, offline days are automatically updated when:

- While authenticated online, the user changes his or her Windows password.
- While the user is connected online, an administrator issues a new policy to the Authentication Agent on the user's computer allowing emergency codes.

For information about emergency codes, see [“Emergency Access”](#) on page 91.

Offline days are not automatically recharged if the authentication session has expired (the user remains online for 24 hours or more). In this situation, the user has to recharge offline days manually. Additionally, unlocking a workstation with only an RSA SecurID PIN does not initiate an automatic recharge.

The following sections describe the recharge scenarios.

Recharging When a Network Connection Exists

The Authentication Agent recognizes that a network connection exists and attempts to download offline days.

Recharging When No Network Connection Exists

1. The Authentication Agent attempts to automatically download offline days, but recognizes that no network connection exists.
2. The Authentication Agent sets the RSA Security Center icon to alert state to indicate that the user needs more offline days.
3. The Authentication Agent notifies the user to connect to the network and presents the user with a link to open the RSA Security Center.
4. The user clicks the link to open the RSA Security Center.
A message on the RSA Security Center Offline Days Status page tells the user to connect to the network.

5. The user attempts to connect to the network and the Authentication Agent does one of the following:
 - If the connection to the network is successful, automatically downloads offline days and sets the RSA Security Center icon to normal state.
 - If the connection to the network fails, informs the user that a problem occurred and to try again later. The RSA Security Center icon remains in alert state and the notification message appears for 15 seconds or until the user dismisses it.

Recharging When the User's Authentication Session Has Expired

1. The Authentication Agent attempts to automatically download offline days, but recognizes that the authentication session has expired.
For example, the user has been logged on to the network for more than 24 hours.
2. The Authentication Agent sets the RSA Security Center icon to alert state to indicate that the supply of offline days is low.
3. The Authentication Agent notifies the user to manually recharge offline days and presents the user with a link to open the RSA Security Center.
4. The user clicks the link to open the RSA Security Center.
A **Recharge** button appears on the RSA Security Center Offline Days Status page, and a message tells the user to manually recharge offline days.
5. The user clicks **Recharge** and the Authentication Agent prompts the user for a passcode.
6. After the user enters the passcode, the Authentication Agent does one of the following:
 - Downloads offline days and sets the RSA Security Center icon to normal state.
 - Informs the user that a problem occurred and to try again later. The RSA Security Center icon remains in alert state and the notification message appears for 15 seconds or until the user dismisses it.

The RSA Authentication Manager administrator sets:

- The Authentication Agents that are allowed to use offline authentication
- The number of offline days issued
- The number that triggers the low supply warning.

For more information, see “Setting Up Offline Authentication and Windows Password Integration” in Chapter 4, “Agents and Activation on Agent Hosts” in the *RSA Authentication Manager 6.1 Administrator's Guide*.”

Checking the Supply of Offline Days

Users can check their supply of offline days by looking at the RSA Security Center icon in the notification area of the Windows taskbar. The state of the icon tells the general status of the supply:

- A key indicates the supply of offline days has not dropped below a specified number.
- A key with an exclamation point warns that the number of offline days has dropped below a specified number.

Users can find out the exact number of offline days they have by right-clicking the RSA Security Center icon, then clicking **View Offline Days**.

Changing an Offline User's Challenge Status

When a user downloads offline data, his or her user name is added to a file on the local computer. This file is named **challengedinfo.dat** and is stored, by default, in **C:\Documents and Settings\All Users\Application Data\RSA Security\Domain** on Domain Authentication Client hosts and in **C:\Documents and Settings\All Users\Application Data\RSA Security\Local** on local authentication component hosts. The file contains a list of local users to be challenged for RSA SecurID passcodes when they authenticate offline.

If you change an offline domain user's challenge status, for example, by removing the user from a challenge group, you also need to delete the user's name from the **challengedinfo.dat** file on the user's computer. Otherwise, the user still receives a challenge when attempting to access the desktop using a domain account.

To remove a user's name from the challengedinfo.dat file:

1. Open the Microsoft Management Console and stop the RSA Offline Authentication Service.
If you are on a domain authentication client, the service is named **RSA Authentication Agent Offline Domain**.
If you are on a local authentication host, the service is named **RSA Authentication Agent Offline Local**.
2. Manually change the permissions (for the administrator only) of the **challengedinfo.dat** file to make it editable.
3. Open the **challengedinfo.dat** file in a standard text editor, and delete the user name.
Each line of the file contains one user name.
4. Restart the RSA Offline Authentication Service.

Emergency Access

Offline users can substitute offline emergency codes for passcodes. For example, if offline users:

Forget their PINs or run out of offline days, they can authenticate with an offline emergency passcode. Users enter the offline emergency passcode instead of an RSA SecurID passcode.

Lose their tokens or are locked out because of too many failed authentication attempts, they can authenticate with an offline emergency tokencode. Users combine the offline emergency tokencode with their RSA SecurID PINs to authenticate. The first time a user attempts to perform a connected authentication after performing an offline authentication with an offline emergency tokencode, the user's token is put into lost token temporary password mode. The temporary password is the same as the offline emergency tokencode. The temporary password may have an expiration date set by the Help Desk administrator. Before the password expires, the user must contact the Help Desk administrator to replace the lost token with a new one, or to return the locked token to non-lost status.

Users get the offline emergency codes by calling their Help Desk administrator.

Automatic Authentication to Protected Domains After Offline Authentication

You can configure the RSA Authentication Agent to automatically authenticate users to protected domains after they have authenticated offline using either RSA SecurID passcodes or emergency codes.

Suppose a user logs on to a protected laptop while it is offline. Without logging out, the user connects the laptop to a network docking station. The user gains access to the protected domain without being prompted again for authentication credentials.

For instructions on how to configure automatic authentication after offline authentication, see the RSA Security Center Help topic "Allowing Reconnection After Offline Authentication."

Setting Up Offline Authentication for Remote Users

To accommodate different work environments, you can set up different ways to deploy offline authentication to remote users.

Scenario 1

Suppose you want to set up offline authentication for users who work both in the office and remotely. You can deploy offline authentication to these users by requiring them to perform an initial online authentication at the office before taking their computers offline.

To set up offline authentication before remote users leave the office:

1. Connect the user's computer to the network.
2. (Optional) Add the user's computer to the domain.
3. Instruct the user to perform a connected authentication to the RSA Authentication Manager.

Note: Local Authentication Client hosts begin receiving offline data during their second connected authentication to the RSA Authentication Manager. For example, if you perform the authentication test described in [“Step 6: Test Authentication”](#) on page 51, and then authenticate to the Authentication Manager, the Authentication Manager generates and downloads the offline data. Domain Authentication Client hosts begin receiving offline data during their first connection to the RSA Authentication Manager.

4. If the user's token is in New PIN mode, instruct the user to authenticate a second time, using the new RSA SecurID PIN.
If the authentication is successful, the RSA Authentication Manager downloads offline data to the user's computer.
5. Verify that offline data has been downloaded to the user's computer by doing one of the following:
 - Point the cursor to the RSA Security Center icon on the Windows taskbar to see the number of offline days available to the user.
For information about the RSA Security Center icon, see the following section, [“Managing Offline Days.”](#)
 - Use Windows Explorer to verify that the offline data is stored in the user's computer. For information about where offline data is stored, see [“Offline Authentication with Local Authentication”](#) on page 85, and [“Offline Authentication with Domain Authentication”](#) on page 86. The directories where offline data is stored are hidden directories. To see the offline data files, you must log on as an administrator and configure Windows Explorer to view hidden files.

Scenario 2

Suppose you want to protect a shared computer with local authentication and set up offline authentication for several different users. Instead of requiring each user to perform a connected authentication and download offline authentication data in the office, you can instruct users to download their offline data remotely.

To configure a shared computer for local offline authentication:

1. Create a challenge group that includes the names of everyone who will share the computer.
For information, see [“Create Groups of Users to Challenge with RSA SecurID”](#) on page 31.
2. Set a reserve password for the computer.
For information, see [“Choose Emergency Access Methods”](#) on page 32. Also see [“Step 2: Set a Reserve Password”](#) on page 53.
3. Use the RSA Security Center to specify the challenge for the group you created.
For information, see the RSA Security Center Help topic “Specifying Who to Challenge.”
4. Instruct the remote user to contact the administrator for the reserve password and then to log on to the computer.
When a user attempts to access the computer while it is offline, the user is prompted first for the reserve password, and then for the Windows password.
5. Instruct the user to connect to the network remotely.
6. Instruct the user to do one of the following:
 - Lock the computer, and then unlock it by providing an RSA SecurID passcode when prompted.
 - Map to a network drive that requires the user to authenticate with an RSA SecurID passcode.

Both procedures download offline data to the user’s computer. From this point forward, the user must provide RSA SecurID passcodes to authenticate locally.

Scenario 3

You may want to deploy both RSA Authentication Agent and offline authentication to remote users who cannot come into the office to install the Authentication Agent and perform an initial online authentication. Because users are added to the offline authentication challenge list only after downloading their initial set of offline days, remote users can access their desktops using their Windows passwords, and then open a remote connection to download offline days. (For more information about the challenge list, see [“Changing an Offline User’s Challenge Status”](#) on page 90.) Once a user downloads an initial set of offline days, that user is challenged for RSA SecurID passcodes for all subsequent authentications to the desktop.

To deploy offline authentication to remote domain users who cannot visit the office:

1. Instruct the user to install RSA Authentication Agent using the silent installation procedure.

A silent installation uses a batch file to execute the RSA Authentication Agent for Microsoft Installer (.msi) package. You create the package by executing an installation package creation program that prompts you to select installation and configuration settings. For information, see [“Creating and Running a Network Installation Package”](#) on page 46.

2. Instruct the user to log on to the desktop using a Windows password, and then connect remotely to the network.

3. Instruct the user to do one of the following:

- Lock the computer, and then unlock it by providing an RSA SecurID passcode when prompted.
- Map to a network drive that requires the user to authenticate with an RSA SecurID passcode.

Both procedures download offline data to the user’s computer.

Important: Remote users can recharge their offline data remotely, but must do so before the last offline day has expired. Otherwise, they must perform a connected authentication to download more offline days. Users can continue to recharge their supplies of offline days in this manner until their RSA SecurID tokens expire.

10

Customizing RSA Authentication Agent 6.1 for Microsoft Windows

Adding Your Company Branding to the RSA Authentication Agent Logon Prompts

Logon dialog boxes associated with RSA Authentication Agent display a bitmap image (.bmp) of the RSA Security logo. You can substitute your company logo on the logon dialog boxes as well as on the dialog boxes that open after you press CTRL+ALT+DEL.

If the color palette for the current display has 256 colors or fewer, make sure to use a 16-color bitmap. If the display is configured for more than 256 colors, the custom bitmap palette is not restricted.

The bitmap you substitute must be exactly 440 pixels wide and 80 pixels high.

When you replace the RSA Security branding with your own bitmap, the phrase, “Secured by RSA SecurID” is added to the lower right side of the logon dialog box.

To specify a custom bitmap:

1. Copy your custom bitmap to a folder on your hard drive.
The file must reside on a drive that is available at system startup.
2. From the **Start** menu, click **Run**, type **regedit**, and then click **OK**.
3. In the registry, scroll to **HKEY_LOCAL_MACHINE\SOFTWARE\RSA Security\RSA Authentication Agent\Current Version\Settings\SDGINA** and the key value **CustomBitMap**.
4. Create a string value of **CustomBitMap** that points to the location of the custom bitmap.
Specify the full path name. For example,
C:\Program Files\RSA Security\RSA Authenticator
Utility\mycorporate_logo.bmp
5. Deploy the custom bitmap to users' computers using any standard deployment method.

Customizing the Authentication Prompt

By default, the RSA Authentication Agent logon prompt instructs users to enter an RSA SecurID passcode. However, some users may not use RSA SecurID authenticators or may not be members of a challenge group. These users log on by entering their Windows passwords.

For local and domain authentication, you can select whether you want the authentication prompt to request a password or a passcode. You make the selection on a per Agent basis from RSA Security Center. For more information, see the RSA Security Center Help topic “Customizing the Authentication Prompt.”

Specifying a Language for Installation

During installation, the Authentication Agent determines the primary language used by the Microsoft Windows operating system on the installation host computer. If the Authentication Agent has language files that matches the primary language of the operating system, the Authentication Agent applies the language files. If the Authentication Agent does not have language files that match the locale, it applies English language files. However, you can specify language files for installation even though that language is not the primary language of the operating system.

The language files localize the following:

- The Authentication Agent portion of the RSA Security Center
- RSA Authentication Agent logon prompts
- Prompts after logon, such as **RSANetUse** and **RSARunAs** prompts
- Authentication messages

Currently, in addition to English, the Authentication Agent supports Japanese. If you need a language pack that was not shipped with RSA Authentication Agent 6.1 for Microsoft Windows, RSA Security can create the language pack for you. For information, contact your RSA Security representative.

11

Protecting Terminal Servers and Performing Common Windows Operations

RSA Authentication Agent 6.1 for Microsoft Windows protects terminal servers and adds RSA SecurID authentication and, optionally, Windows password integration, to common Windows operations.

Protecting Terminal Servers

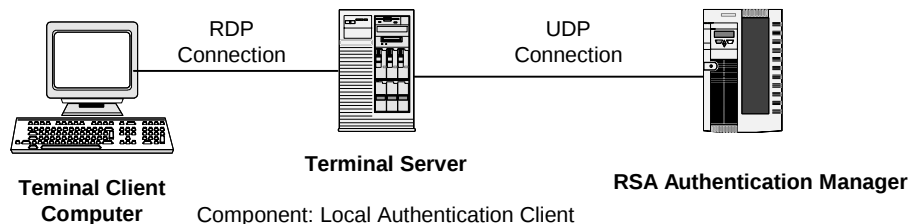
You can use RSA Authentication Agent 6.1 for Windows to protect Citrix MetaFrame XPs terminal servers and Windows 2000 and 2003 Terminal Servers (WTS). Users attempting to access a protected terminal server must authenticate with RSA SecurID passcodes.

To protect a terminal server, you install the RSA Authentication Agent Local Authentication Client component or Domain Authentication Client component on the terminal server host.

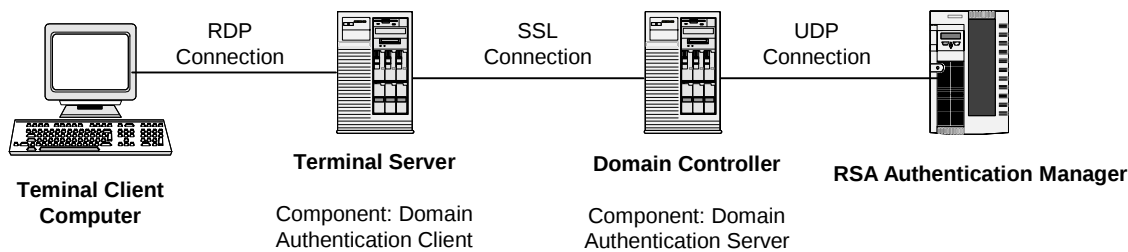
Important: When you configure the remote desktop connection on the terminal client computer, do not enter a password in the **Password** field. If you do, the user will not be able to authenticate from the terminal client to the protected terminal server.

The following figures show three possible setups for protecting terminal servers:

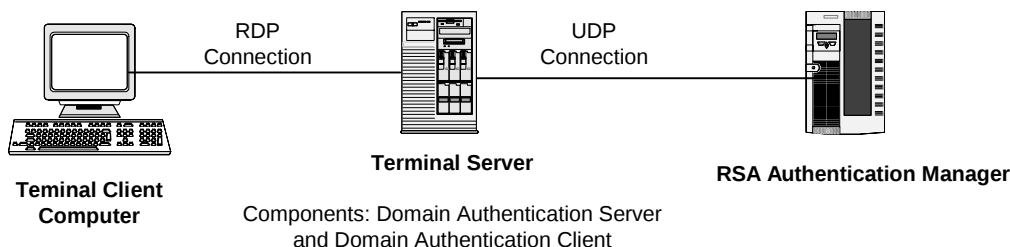
Terminal Server and Authentication Manager Directly Connected



Terminal Server as Proxy to the Domain Controller



Terminal Server Installed on the Domain Controller



Using RSA SecurID Authenticator SID800 in Terminal Server Environments

You cannot use RSA SecurID Authenticator SID800 to authenticate from terminal server client computers. You can, however, use RSA SecurID Authenticator SID800 to authenticate to terminal server hosts.

If you log on to your desktop using RSA SecurID Authenticator SID800, you can perform Windows operations using a different type of token.

When you use the RSA SecurID Authenticator SID800, you are prompted only for an RSA SecurID PIN. The Authentication Agent retrieves the tokencode from the Authenticator and submits it to the authentication process automatically.

Using RSANetUse and RSARunAs

RSA Authentication Agent for Microsoft Windows provides the **RSANetUse** and **RSARunAs** utilities. These utilities emulate the Windows **net use** and **runas** utilities, but add RSA SecurID authentication and, optionally, password integration using a simplified authentication process. When you invoke **RSANetUse** or **RSA RunAs**, you are prompted for an RSA SecurID passcode instead of a Windows password.

RSA Security recommends that only users who are set up for RSA SecurID authentication use the **RSANetUse** and **RSARunAs** commands.

You can issue **RSANetUse** and **RSARunAs** from the command line, or from a menu. Issuing the commands from a menu opens a graphical interface. When issued from the command line, **RSANetUse** and **RSARunAs** do not support New PIN mode.

If you are using USB authenticators or software tokens, when you execute **RSANetUse** and **RSARunAs** from a menu and use the graphical interface, the tokencode is automatically read from the authenticator and passed to the RSA Authentication Manager. You need to enter only your RSA SecurID PIN into the authentication prompt. However, when you execute **RSANetUse** and **RSARunAs** from the command line, you must read the tokencode displayed on the USB authenticator, and manually enter the passcode into the authentication prompt. If you are using a software token, you must open the software token console and read the tokencode from the display, then manually enter it into the authentication prompt.

Issuing RSANetUse From the Start Menu

1. Log on to your computer using your own credentials.
2. Click **Start > Programs > RSA Security > RSA Authentication Agent Tools > Mapping a Drive**.
3. At the prompt, specify the drive and folder you want to access.
If you want to connect using an alternate user name, click **Connect using a different user name**.
4. When the system prompts you, specify which user identity you want to use, and enter an RSA SecurID passcode for the user identity, and then click **OK**.

Note: If you have already authenticated as the user identity, and the authentication session is still valid, you are not prompted to reauthenticate.

5. At the Map Network Drive dialog box, click **Finish**.
6. When the system prompts you, enter the Windows password for the identity you are using.

Note: If your system is configured for Windows password integration, and the Windows password is stored in the RSA Authentication Manager database, you are not prompted for the Windows password.

Issuing RSANetUse From the Command Line

You issue **RSANetUse** from the command line in the same way that you issue its Windows counterpart. However, **RSANetUse** adds the option **/passcode** for RSA SecurID authentication. When issued from the command line, **RSANetUse** does not support New PIN mode.

To issue RSANetUse from the command line:

1. Log on to your computer using your own credentials.
2. Issue the **RSANetUse** command, entering the user name you want to use and a passcode for the user identity.
For example:

```
>/rsanetuse X: \\computername\shared /passcode:passcode  
/user:username@domain.com
```

If you do not provide a user name, the system assumes you are using the user account with which you are currently logged on.

If you do not provide a passcode, the system prompts you for one.
3. When the system prompts you, enter the Windows password for the user identity.

Note: If your system is configured for Windows password integration, and the Windows password is stored in the RSA Authentication Manager database, you are not prompted for the Windows password.

Issuing RSARunAs

You can issue **RSARunAs** from a menu, or from a command line.

Issuing RSARunAs From a Menu

The **RSARunAs** command appears in all of the menus where the Windows **runas** command appears. If you issue the command from a menu, the system uses a graphical interface to prompt you to authenticate. If you issue **RSARunAs** from a command line, you authenticate from the command line.

To issue RSARunAs from a menu:

1. Log on to your computer using your own credentials.
2. Right-click the executable you want to run as an alternate user, and then click **RSARunAs**.
3. When the system prompts you, specify which user identity you want to use, and enter an RSA SecurID passcode for the user identity.
If you have already authenticated as the user identity, and the authentication session is still valid, you are not prompted to reauthenticate.
4. When the system prompts you, enter the Windows password for the user identity.

Note: If your system is configured for Windows password integration, and the Windows password is stored in the RSA Authentication Manager database, you are not prompted for the Windows password.

When you authenticate successfully to a protected computer or domain, and then issue **RSARunAs** to access resources within the same domain, you gain access without having to reauthenticate as long as your session certificate remains valid. If the session certificate expires, you are prompted to reauthenticate.

Issuing RSARunAs From the Command Line

You can use **RSARunAs** from the command line with all of the options that are available for Windows **runas**.

You can use **RSARunAs** from the command line with the following options:

- **/nopprofile**
- **/profile**
- **/env**
- **/netonly**
- **/user**
- **/program**

The options behave the same way they do with the Windows **runas** command.

RSARunAs does not support the following options:

- **/savecred**
- **/smartcard**

RSARunAs issued from a command line does not support New PIN mode.

To issue **RSARunAs** from the command line:

1. Log on to your computer using your own credentials.
2. Issue the **RSARunAs** command, entering the user name you want to use and a passcode for the user identity.

For example:

```
>/rsarunas /user:username@domain.com command
```

If you do not provide a user name, the system assumes you are using the currently logged on user account.

3. When you are prompted, enter the passcode for the user identity you want to use.
4. When the system prompts you, enter the Windows password for the user identity.

Note: If your system is configured for Windows password integration, and the Windows password is stored in the RSA Authentication Manager database, you are not prompted for the Windows password.

Using Windows **net use** and **runas**

When you issue the Windows **net use** and **runas** utilities to access resources in a protected network, you are prompted to authenticate with RSA SecurID passcodes. The authentication process for Windows **net use** and **runas** is more complicated than the process for **RSANetUse** and **RSARunAs**.

When you authenticate successfully to a protected domain, then issue the **net use** command to access a shared resource within the same domain, as long as the session certificate remains valid, you gain access to the resource without having to reauthenticate.

Issuing the Windows **net use** or **runas** From the Command Line

To authenticate with Windows **net use** from the command line:

1. Log on to your computer using your own credentials.
2. Issue the **net use** or **runas** command from the command line.
3. When the system prompts you, enter the Windows credentials for the user identity you want to use.

4. Dismiss the error message that the system generates.

Note: The system issues a message telling you that to issue the command, you must authenticate with an RSA SecurID passcode for the substitute user identity. The message may not appear in the foreground on your desktop. Find and click the message icon on the Windows taskbar to bring the message to the foreground.

5. When the system prompts you, enter an RSA SecurID passcode for the user identity.
6. When you see a success message, dismiss it and reissue the command.
7. When the system prompts you, reenter the Windows password for the user identity.

Performing GUI-Based Windows Operations

Ordinarily, when you authenticate to a protected computer or resource, you are prompted for your RSA SecurID passcode first, and then for your Windows password. However, when you perform GUI-based Windows operations (for example, mapping a network drive or running a program using the **Run As...** option on the Windows **Start** menu) as an alternate user on a protected server, you may be prompted for your Windows password first, and then for your RSA SecurID passcode. After you enter your passcode, you may see the message **Retry your failed operation**. If you provided your Windows password at the prompt, you do not need to perform any further action.

To authenticate when performing GUI-based Windows operations:

1. Open the interface for performing the Windows operation.
2. When the system prompts you, enter a Windows password for the alternate user. The system issues a message telling you that the operation failed and reprompts you for the Windows password.

Important: Do not reenter the Windows password until you perform the next step and receive a message that RSA SecurID authentication was successful. If you do, the operation will fail again.

3. At the prompt, enter an RSA SecurID passcode for the alternate user identity.

Important: The RSA SecurID authentication prompt may not appear on your desktop. Find the RSA SecurID authentication icon on the Windows taskbar and click the icon to open the prompt.

4. Reenter the Windows password for the substitute user identity.

Mapping a Drive to a Protected Network

When you attempt to map a drive to a protected network, you are prompted to authenticate with RSA SecurID passcodes.

To authenticate when mapping a drive:

1. Log on to your computer using your own credentials.
2. Attempt to map a drive. For example, on the Windows tool bar, click **Tools > Map Network Drive**.
3. At the prompt, specify the drive letter for the connection and the folder to which you want to connect.
4. At the prompt, enter your RSA SecurID passcode.
If you have already authenticated as the substitute user, and the authentication session is still valid, you are not prompted to reauthenticate.
5. If the system prompts you, enter the Windows password for the substitute user.
If your system is configured for Windows password integration, and the Windows password is stored in the RSA Authentication Manager database, you are not prompted for the Windows password.

RSA Authentication Agent Prompting Behavior

The following table describes RSA Authentication Agent prompting behavior in scenarios for users whose session certificates have expired or who are logging on as alternate users:

Scenario	Prompt Behavior
A user is running a single session on the terminal server.	The Authentication Agent prompts the user on the desktop for that session.
A user is running multiple sessions. Within some of the sessions, the user is running net use or runas commands.	The Authentication Agent prompts the user on the desktops for all sessions running net use and runas commands.
A user is running multiple sessions. None of the sessions are using net use or runas commands.	The Authentication Agent prompts the user on the desktops for all of the sessions.
The user is not running any sessions, but a session is running for the user through either a net use or runas command.	The Authentication Agent prompts on the desktop for the session running the net use or runas command.

12

Troubleshooting

The following information is accurate at the time of release. For additional issues and solutions information, go to RSA SecurCare Online at <https://knowledge.rsasecurity.com>.

Note: RSA SecurCare Online is only available to customers who have a valid Software Service Contract.

Specific Authentication Problems

Active Directory Password Takes Longer than Usual to Appear

If this problem occurs during domain authentication on a domain authentication client computer running Windows XP SP2, check the domain client firewall settings. Although the firewall service on Windows XP SP2 clients may have been stopped, the service may restart itself and prevent the Domain Authentication Client component from communicating with the Domain Authentication Server component on the domain controller. If this occurs, domain authentication for online users fails. Domain authentication for offline users succeeds, but Active Directory passcodes cannot be communicated, and the prompt for the Active Directory password takes longer than usual to appear. To prevent this situation, disable, rather than stop, the firewall service on the domain authentication client.

Domain Authentication Fails

If domain authentication fails on a domain authentication client computer running Windows XP SP2, check the domain client firewall settings. Although the firewall service on Windows XP SP2 clients may have been stopped, the service may restart itself and prevent the Domain Authentication Client component from communicating with the Domain Authentication Server component on the domain controller. If this occurs, domain authentication for online users fails. Domain authentication for offline users succeeds, but Active Directory passcodes cannot be communicated, and the prompt for the Active Directory password takes longer than usual to appear. To prevent this situation, disable, rather than stop, the firewall service on the domain authentication client.

Installer Sees "...Network Authentication Service Terminated..." Message After Restart

If you install RSA Authentication Agent and, after restarting the computer, see the message **The RSA Authentication Agent Network Authentication Service terminated with service-specific error 3221235590**, verify that the root certificate (**sdroot.crt**) file used for installation is valid.

Users Receive Error Messages During Authentication

Users may see the following messages during authentication:

- **Cannot load RSA Authentication Agent DLL.**
- **Unexpected error from RSA Authentication Agent.**

For information about these messages, see [“RSA Authentication Agent Error and Event Viewer Log Messages”](#) on page 109.

Users See “Unable to Log You On...” During Logon to a Protected Domain

Users see the message **Unable to log you on because of the account restrictions** when they attempt to log on to a protected domain from a domain client computer that does not have the Domain Authentication Client component installed on it.

To access a protected domain, users have to log on from a domain client computer that is set up for domain authentication.

Remote Access Prompts Time Out Too Soon

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

For more information, see the RSA Security Center Help topic “Changing the Time-Out Values of the Remote Authentication Prompts.”

Test Authentication Succeeds, But Actual Authentication Fails

If the test authentication succeeds, but actual authentication fails, restart the RSA Authentication Agent host.

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

Node Verification Fails

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

The following events can cause node verification failure:

- The RSA Authentication Manager successfully authenticates a user and sends the node secret to the RSA Authentication Agent, along with a successful authentication message. The Authentication Agent either times out or fails (for example, due to a power failure) before storing the node secret.
- An administrator uninstalls the Authentication Agent, and then installs it again. When the Authentication Agent is uninstalled, the node secret is removed.

- The Authentication Agent is not identified in the RSA Authentication Manager database. This event may generate either a **Node Verification Failed** error message or an **Agent Host Unknown** error message.
- You are using RSA Authentication Manager Replicas, and the Replica that sent the node secret to the Authentication Agent has not yet notified other Replicas. In this case, some users can successfully authenticate and others cannot.
- You are using Replicas, and one or more Replicas are not running. In this case, some users can successfully authenticate and others cannot.
- You clear the node secret on either the Authentication Agent or the Authentication Manager, but not on both.
- You clear the node secret on both the Authentication Agent and the Authentication Manager, but do not restart the Authentication Agent.
- You enter an invalid user name on the first authentication after clearing the node secret.

To correct a node verification failure, you must clear the node secret from the Authentication Agent Host. At the same time, your RSA Authentication Manager administrator must clear the node secret specified for the Authentication Agent Host in the RSA Authentication Manager database. You must then perform a test authentication on the Authentication Agent Host.

Important: You must clear the node secret on both the Authentication Agent Host and the RSA Authentication Manager host.

For instructions on how to clear the node secret on the Authentication Agent, see [“Clearing and Replacing the Node Secret”](#) on page 81. For instructions on how to clear the node secret on the RSA Authentication Manager, see the RSA Authentication Manager Help topic “Editing an Agent Host.”

General Authentication Problems

This section tells you how to diagnose general authentication problems.

Verify the Accuracy of the Computer Clock

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

Verify the `sdconf.rec` File

If the RSA Authentication Agent for Windows and the RSA Authentication Manager 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 Security Center.
2. On the **Main** tab, click **Test Authentication with RSA Authentication Manager**.

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 Authentication Manager administrator for a new copy of **sdconf.rec** for the Authentication Agent.

Windows Troubleshooting

If you are troubleshooting Windows, the information and authentication error messages log is stored in the rotating file **%SYSTEMROOT%\aceclient.log**. When this file exceeds 1 MB, it is renamed **aceclientn.log** (where *n* is a number between one and nine), 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 **logfile**.
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 the registry editor.
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 Authentication Agent Error and Event Viewer Log Messages

This section lists all RSA Authentication Agent error and event messages alphabetically.

ACECheck processing error for userid *user name*.

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

ACEClose processing error *errornumber*.

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

ACENext processing error for userid *user name*.

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

ACEPin processing error for userid *user name*.

If the **ACEPin** function returns an error, an RSA Authentication Manager 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 Security Center is set to **All Users**. The user was challenged to enter a passcode.

An error occurred when accessing the Metabase.

The Authentication Agent failed while reading from or writing to the Metabase. Make sure you have the correct administrative privileges, and then reboot the Authentication Agent Host. If the error persists, reinstall the Authentication Agent to override the existing settings. If that does not resolve the situation, you must uninstall and then reinstall the Authentication Agent.

Authentication Agent initialization failed.

The Authentication Agent cannot make the connection to the RSA Authentication Manager. Verify that the RSA Authentication Manager and the network are operating and that all network interface cards and cables are properly installed and in good condition.

Authentication failure.

The subject described in the Event Detail did not successfully authenticate with RSA SecurID and, therefore, did not gain access.

Authentication Manager: Access Denied.

The user entered an invalid RSA SecurID passcode.

Authentication Manager is not responding.

A network communications problem occurred between the RSA Authentication Manager and the RSA Authentication Agent, or the Authentication Manager cannot be found (for example, because the IP address is wrong), or the RSA Authentication Manager daemon is not running.

Make sure the Domain Authentication Server component host has been added to the RSA Authentication Manager database as an Agent Host.

Authentication Manager: Failed Authentication Attempt. User *user name*.

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 is deactivated until an administrator intervenes.

The number of allowed bad passcodes is stored in the **sdconf.rec** file.

Authentication Manager: Invalid RSA Authentication Manager configuration. User *user name*.

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 Authentication Manager administrator.

Authentication Manager: New PIN Accepted. User *user name*.

The user successfully associated a new RSA SecurID PIN with the token.

Authentication Manager: New PIN Rejected. User *user name*.

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

Authentication Manager: Next Tokencode Accepted. User *user name*.

After entering a series of bad passcodes, the user was prompted to enter the next tokencode displaying on the token. The tokencode was valid and the user was authenticated successfully.

Authentication Manager: Next Tokencode Failed. User *user name*.

After entering a series of bad passcodes, the user was prompted to enter the next tokencode displaying on the token. The tokencode was not valid and the user was denied access to the system.

Authentication Manager: RSA Authentication Agent Library Failure.

The RSA Authentication 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 Authentication Agent.

Authentication Manager: Unsupported protocol.

The client attempted to access an unsupported version of RSA Authentication Manager.

Authentication Manager: User Canceled New PIN Mode. User *user name*.

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

Authentication Manager: User Canceled Transaction. User *user name*.

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

Authentication Manager: User I/O Timeout. User *user name*.

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

Authentication Manager: User Interface Library Failure.

The RSA Authentication 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 reinstall RSA Authentication Agent.

AVOID command has invalid IP address in SDOPTS.REC file.

The IP address associated with the AVOID parameter in the **sdopts.rec** file is not valid. For information about creating a correctly formatted **sdopts.rec** file, see [“Creating an sdopts.rec File”](#) on page 125.

Cannot AVOID default IP Address in SDOPTS.REC file.

The AVOID parameter does not work with the default IP address specified in the **sdopts.rec** file. For information about creating a correctly formatted **sdopts.rec** file, see [“Creating an sdopts.rec File”](#) on page 125.

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 Authentication Manager by doing one of the following:

- If the RSA Authentication Manager is running on a Windows computer, open the Network control panel, and confirm that **Simple TCP/IP Services** are installed. If they are not, add the **Simple TCP/IP Services**.
- If the RSA Authentication Manager is running on a UNIX computer, confirm that the **echo** service is running on the RSA Authentication Manager 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 Authentication Manager by doing one of the following:

- If the RSA Authentication Manager is running on a Windows computer, open the Network control panel, and confirm that **Simple TCP/IP Services** are installed. If they are not, add the **Simple TCP/IP Services**.
- If the RSA Authentication Manager is running on a UNIX computer, confirm that the **echo** service is running on the RSA Authentication Manager computer. See your UNIX operating system documentation for information about starting the **echo** service.

Cannot load RSA Authentication Agent DLL.

Test cannot find **aceclnt.dll** in the **\system32** directory. You must reinstall RSA Authentication Agent software.

Could not initialize RSA Authentication Agent.

This message is preceded by a number of RSA Authentication Agent error messages, such as **Cannot find sdconf.rec**. Try reinstalling the **sdconf.rec** file in the **%SYSTEMROOT%\system32** directory.

Also check the security settings for the file. Confirm that 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 reinstall the RSA Authentication Agent software.

Credential Management error allocating memory.

The system does not have enough physical RAM, or too many other processes were 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 too many other processes were 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 too many other processes were 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 download error aceuser1 encountered for user: %2.

The specified location does not have enough room to download offline data, or the specified location does not exist.

Data download error encountered for user: %1.

An error occurred while offline data was being downloaded for the specified user.

Data Manager: Not Enough Memory.

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

Duplicate AVOID statements in SDOPTS.REC file.

There are two identical AVOID statements in the **sdopts.rec** file. For information about creating a correctly formatted **sdopts.rec** file, see [“Creating an sdopts.rec File”](#) on page 125.

Failed authentication for userid *user name*.

The RSA Authentication Manager did not grant the user access. The most common causes for this are an incorrect user name or an invalid passcode.

Failed to create event.

This message indicates that there 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.

Too many other processes were 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 a problem exists with WINSOCK. Ensure that TCP/IP has been enabled on the computer.

File incorrect size: sdconf.rec.

The **sdconf.rec** file was probably not copied in binary mode. Ask the RSA Authentication Manager 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. Reinstall the RSA Authentication 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 Authentication Manager. Ask your RSA Authentication Manager administrator for a new copy of **sdconf.rec**.

Initialization of the Offline Authentication Service Failed.

The offline authentication service failed to start. If this error recurs, restart the computer.

Local: Security Features Available.

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

Network Timeout - RSA Authentication Manager was responding but has now stopped.

Make sure the RSA Authentication Manager 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 *user name*.

The RSA Authentication Manager verified the RSA SecurID user's new RSA SecurID PIN.

New PIN rejected for userid *user name*.

The RSA SecurID PIN was rejected by the RSA Authentication Manager. The user must reauthenticate to set the RSA SecurID PIN. Check the Activity Log on the RSA Authentication Manager.

New PIN requested from userid *user name*.

The RSA Authentication Manager has prompted the RSA SecurID user to create an RSA SecurID PIN or receive a system-generated RSA SecurID PIN.

Next code accepted for userid *user name*.

RSA Authentication Manager accepted the tokencode and granted access.

Next code rejected for userid *user name*.

The user must attempt to authenticate again.

Next code requested from userid *user name*.

The user's token was in Next Tokencode mode and the RSA Authentication Manager asked for the second tokencode.

Offline Authentication: Access Denied.

The user's attempt to authenticate offline was unsuccessful.

Offline Authentication: Access Denied - Passcode Reuse Attack Detected.

Someone attempted to reuse a passcode that the user entered to authenticate offline.

Offline Authentication: Access Denied - Previous Tokencode.

The user's attempt to authenticate offline was unsuccessful because the user entered the previously issued tokencode instead of the current one.

Offline Authentication: Authentication Failure Limit Reached. Only Emergency Access Authentication Allowed.

The user's attempt to authenticate offline was unsuccessful and the user has been locked out of the system. The user must contact the Help Desk for an emergency access code.

Offline Authentication: Domain Agent Host Could Not Verify Disconnected Authentication for User.

The domain server cannot verify that offline authentication occurred successfully from the domain client.

Offline Authentication: Emergency Access Passcode Accepted.

The user successfully authenticated using an emergency access passcode.

Offline Authentication: Emergency Access Tokencode Accepted.

The user successfully authenticated using an emergency access tokencode.

Offline Authentication: Passcode Accepted.

The user has successfully authenticated offline.

Remote: RAS not available.

The computer does not meet one or more of the system or software requirements for enabling authentication of RAS connections. See "[Remote Authentication Requirements and Setups](#)" on page 22, and verify that the computer meets all the requirements.

RSA SecurID challenge off. PASSCODE not required.

RSA SecurID authentication is not enabled on the specified service. The **Challenge** option in the RSA Security Center is set to **None**. The user was not challenged to enter a passcode.

Session Manager: Failed Socket Accept Call.

Too many sockets are open.

Session Manager: Failed Socket Connect Call.

The user attempted to log on to a protected domain from a domain client computer that does not have the RSA Authentication Agent domain client component installed.

Session Manager: Failed to Create Server Thread.

Too many users are connected at once. Try lengthening the intervals at which users attempt to log on.

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.

This is probably a configuration error. The computer that is connecting has no DNS or NetBIOS name, or has an invalid IP address. Verify that 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 too many other processes were 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 Offline Authentication service ended abnormally.

The offline authentication service stopped due to an uncommon condition.

The Offline Authentication service was started. Port: %1.

The offline authentication service was started and is listening on the specified local port.

The Offline Authentication service was stopped.

The offline authentication service was stopped.

The Offline Authentication Time Offset was adjusted to %1.

The clock setting on either the RSA Authentication Agent or RSA Authentication Manager were changed.

The RSA Authentication Agent Network Authentication Service terminated with service-specific error 3221235590.

Verify that the root certificate (**sdroot.crt**) file used for installation is valid.

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. Verify that the **Hardware Flow Control** option is enabled in the **Modem Configure Settings** page of the RAS Control Panel.

Also verify 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. . .

A problem occurred with RSA SecurID authentication.

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

The user closed the connection on the specified port.

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

A user disconnected from the RSA Authentication Agent.

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

A user authenticated to the RSA Authentication Manager.

The user was authenticated as *user name1* by the third-party security host module but was. . .

The user has been disconnected because the user's logon name and the RSA Security authentication name are not the same.

Unable to contact the RSA Authentication Manager Download Service.

The Authentication Manager Download Service is not accepting connections from the RSA Authentication Manager. Verify that the RSA Authentication Manager is running.

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 logon 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 logon information was used to determine the user's group membership. The cached information revealed that the user was not in a challenge 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 logon 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 logon 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 Authentication Agent.

The RSA Authentication Manager returned an invalid value. Reinstall the RSA Authentication Agent for Windows software. If the problem persists, check your hardware.

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. 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 for exemption 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. 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 for exemption from RSA SecurID authentication. The user was challenged to enter a passcode.

User *user name* canceled out of New PIN routine.

The user canceled the authentication attempt in New PIN mode.

User *user name* canceled out of RSA SecurID Authentication routine.

The user canceled without entering a user name.

User *user name* entered an invalid PIN while attempting to unlock the workstation.

The user entered an invalid PIN while attempting to unlock the workstation while the Workstation Unlock With RSA SecurID PIN feature is enabled.

User *user name* exceeded the allowed number of incorrect attempts to unlock the workstation with only a PIN.

The user exceeded the allowed number of incorrect attempts to unlock the workstation with only a PIN. The Workstation Unlock with RSA SecurID PIN feature has been disabled for this logon session.

User *user name* 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, select **All Users** on the Challenge Settings page in the RSA Security Center.

User *user name* not in *groupname* group. PASSCODE not required.

The **All Users** challenge option is not active, and the user is not in the designated group.

User *user name*: ACCESS DENIED. ATTEMPT 1.

The user was denied access. Check the RSA Authentication Manager Activity Log for the specific reason.

User user name: Access denied. Attempt to use invalid handle. Closing connection.

An internal error occurred. If the message recurs, call the RSA Security Customer Support Center.

User user name: ACCESS DENIED. Next Tokencode failed.

The user failed to authenticate in Next Tokencode mode and must attempt to authenticate again.

User user name: ACCESS DENIED. Server signature invalid.

This message indicates that the identity of the RSA Authentication Manager could not be verified by the Authentication Agent. If you see this message, call RSA Security Customer Support.

User user name: 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 user name: canceled out of Next Tokencode routine.

The user canceled out of the Next Tokencode process.

User user name: canceled out of RSA SecurID Authentication routine.

The user canceled RSA SecurID authentication after entering a user name.

User user name: Domain not found. User challenged for PASSCODE.

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

User user name: New PIN accepted.

The user's new RSA SecurID PIN was verified.

User user name: New PIN rejected.

The RSA SecurID PIN was rejected by the RSA Authentication Manager. The user needs to reauthenticate to set the RSA SecurID PIN. Check the RSA Authentication Manager Activity Log.

User user name: Not found. User challenged for PASSCODE.

The user is unknown to the system, but the user will still be challenged for a passcode.

User user name: PASSCODE accepted.

The user's passcode was accepted.

User *user name*: PASSCODE required. All users challenged.

The **All Users** challenge option is selected, and the user must authenticate with RSA SecurID passcodes.

User *user name*: Reserve password accepted.

The user was prompted for the reserve password and entered it correctly.

User *user name*: Successfully logged on with Next Tokencode.

RSA Authentication Manager accepted the next tokencode and granted access to the user.

USESERVER and AVOID cannot both be used in sdopts file.

The **sdopts.rec** file is trying to use both USESERVER and AVOID. For information about creating a correctly formatted **sdopts.rec** file, see [“Creating an sdopts.rec File”](#) on page 125.

13

Upgrading, Repairing, and Uninstalling

Upgrading to RSA Authentication Agent 6.1 for Microsoft Windows

You upgrade when you install RSA Authentication Agent 6.1 for Microsoft Windows without first uninstalling your previous installation. You can upgrade to RSA Authentication Agent 6.1 for Microsoft Windows from versions 5.5, 5.6, and 6.0.

- If you plan to upgrade to RSA Authentication Agent 6.1 from versions 5.5, 5.6, or 6.0, do not uninstall your existing installation.
- If you have a version of that is earlier than version 5.5, you must uninstall it before upgrading to RSA Authentication Agent 6.1.

Uninstalling the previous installation removes the node secret from the Authentication Agent Host and clears previous configuration settings.

If you install RSA Authentication Agent 6.1 for Microsoft Windows on a computer that hosts a previous version, the components from the previous version are either upgraded or removed. If, during this installation, you select the same components as in the previous installation, the components are upgraded and retain their previous configuration settings. The node secret used for communication between the RSA Authentication Agent and the RSA Authentication Manager is also retained. Previous-version components that you do not select during this installation are removed.

If you uninstall a previous version, you must instruct the RSA Authentication Manager administrator to remove the node secret for the Authentication Agent from the RSA Authentication Manager database. For more information, see [“Clearing and Replacing the Node Secret”](#) on page 81.

Do not install a previous version of RSA Authentication Agent for Windows on a computer that hosts RSA Authentication Agent 6.1 for Microsoft Windows. Doing so corrupts the 6.1 installation. If this occurs, you must repair the 6.1 installation as described in the following section [“Repairing an RSA Authentication Agent 6.1 for Microsoft Windows Installation.”](#)

Installing RSA Authentication Agent 6.1 for Microsoft Windows does not affect previous installations of RSA Authentication Agent for Web.

Repairing an RSA Authentication Agent 6.1 for Microsoft Windows Installation

Repairing an installation replaces missing files in a damaged installation.

Important: If you installed the Authentication Agent from a network drive, to repair the Authentication Agent, you must remap the drive and perform the repair from that drive. A repair returns RSA Authentication Agent settings to their default states.

To repair an installation:

1. Copy the **RSA Authentication Agent for Windows.msi** file from the RSA Authentication Agent 6.1 for Microsoft Windows .zip file to the Authentication Agent server and client computers.
2. Log on to your system as an administrator.
3. If you are running the Windows RRAS service, stop the service.
4. To start the installation wizard, double-click **RSA Authentication Agent for Windows.msi**.
5. Follow the instructions on your screen to advance through the Welcome pages and accept the Software License Agreement.
6. On the Program Maintenance screen, select **Repair**, and click **Next**.
7. Follow the instructions on your screen to complete the repair process.

Uninstalling RSA Authentication Agent 6.1 for Microsoft Windows

Important: If you installed the Authentication Agent from a network drive, to uninstall the Authentication Agent, you must remap the drive and perform the uninstallation from that drive.

To uninstall the Authentication Agent:

1. Click **Start > Settings > Control Panel > Add/Remove Programs**.
2. Scroll to **RSA Authentication Agent for Windows**, and click **Remove**.
3. Restart the computer.

Note: If you cancel the uninstallation process at any time, the installation reverts back to the way it was before you began the uninstallation.

Removing the sdeap.dll File

Before you remove the **sdeap.dll** file from an Authentication 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 restart your system, the Connection Manager may not function.

A

Load Balancing with the `sdopts.rec` File

Overview of Load Balancing

You can configure the RSA Authentication Agent to automatically balance authentication request loads either dynamically or manually.

With dynamic load balancing, the Authentication Agent sends a time request to each RSA Authentication Manager in the realm and determines a priority list based on the response time of each Authentication Manager. The Authentication Manager with the fastest response time gets the highest priority and receives the greatest number of authentication requests. Other Authentication Managers get lower priorities and fewer requests. This arrangement lasts until the Authentication Agent sends another time request or times out.

To perform dynamic load balancing, the Authentication Agent connects to the RSA Authentication Manager through firewalls by using alternate IP addresses (aliases) for the Authentication Managers. The Authentication Managers provide the aliases to the Authentication Agent upon request. The addresses are stored in the configuration record file (`sdconf.rec`) on the Authentication Agent Host. You can prevent an Authentication Manager from being used for authentications in dynamic load balancing by including an **AVOID** statement in the `sdopts.rec` file. The `sdopts.rec` file is a text file stored on the Authentication Agent Host.

With manual load balancing, you specify the RSA Authentication Manager that each Agent Host uses. You also assign a priority to each Authentication Manager so that the Authentication Agent directs authentication requests to some Authentication Managers more frequently than to others. You specify the priority settings by including the **USESERVER** statement in the `sdopts.rec` file.

You can also use the `sdopts.rec` file to specify additional firewall IP addresses and an overriding IP address for the Authentication Agent Host if it is a multihomed server.

Creating an `sdopts.rec` File

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

Important: Each time you modify the `sdopts.rec` file, you must restart the Authentication Agent to register the 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 Authentication 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 130.
 - **USESERVER=ip_address, priority**. Specifies an RSA Authentication Manager that can or will receive authentication requests from the Authentication Agent according to the specified priority value. Use one setting for each RSA Authentication Manager that the Authentication Agent uses. The combined maximum number of Authentication Managers you can specify in the **sdopts.rec** and **sdconf.rec** files is 11.

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

Priority	Meaning
2–10	Send authentication requests to this RSA Authentication Manager using a randomized selection based on the assigned priority of the Authentication Manager. The range is from 2–10. The higher the value, the more requests the Authentication Manager receives. A Priority 10 Authentication Manager receives about 24 times as many requests as a Priority 2 Authentication Manager.
1	Use this RSA Authentication Manager only if no Authentication Managers of higher priority are available.
0	Ignore this RSA Authentication Manager. A Priority 0 Authentication Manager can be used only in special circumstances: • First, it must be one of the four Authentication Managers listed in the sdconf.rec file. • Next, the Priority 0 Authentication Manager can be used only for the initial authentication of the Authentication Agent, unless all Authentication Managers with priorities of 1–10 listed in the sdopts.rec file are known by the Authentication Agent to be unusable. Generally, a priority value of 0 allows you to put an entry in the file for an Authentication Manager without using it. You can change the priority value if you decide to use the Authentication Manager. Note: You must enter keywords in uppercase. If none of the servers with USESERVER statements are responsive, then the default server is the Master (if one exists) or the Authentication Manager that was used to create the sdconf.rec file.

You must assign a priority to each RSA Authentication Manager that you add to the **sdopts.rec** file. Otherwise, the entry is invalid. The IP addresses in the file are verified against the list of valid RSA Authentication Managers that the Authentication Agent receives as part of its initial authentication.

- **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 Authentication Manager in addition to the aliases listed for the Authentication Manager 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 Authentication Manager, followed by up to three aliases for that Authentication Manager. The Authentication Agent sends timed requests to both the actual and the aliases.

Only the actual IP address specified by the **ALIAS** keyword must be known by the specified RSA Authentication Manager. In addition, the actual IP address must be included on any Authentication Manager list received by the Authentication Agent. The Authentication Manager list provides actual and alias IP address information about all known Authentication Managers in the realm. The Authentication Agent receives the list from the Authentication Manager after the Authentication Manager validates an authentication request.

- **ALIASES_ONLY=ip_address.** When you provide an actual IP address of an RSA Authentication Manager as the value, this keyword tells the Authentication Agent to use only the alias IP addresses to contact the Authentication Manager.

When you do not provide a value, this keyword tells the Authentication Agent to send requests only to the RSA Authentication Managers that have alias IP addresses assigned to them. You can create exceptions by including in the **sdopts.rec** file no more than 10 **IGNORE_ALIASES** keywords to specify which Authentication Managers 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 129.

If you use this keyword, make sure that at least one RSA Authentication Manager 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 you do not provide a value, this keyword specifies that all alias IP addresses found in the **sdopts.rec** and **sdconf.rec** files, or on the RSA Authentication Manager list, are ignored. You can create exceptions by including no more than 10 **ALIASES_ONLY** keywords in the **sdopts.rec** file to specify which Authentication Managers 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 129.

When you provide an actual IP address as the value, this keyword tells the Authentication Agent to use only the actual IP address to contact the Authentication Manager.

- **AVOID=ip_address.** When you provide an actual IP address of an RSA Authentication Manager as a value, this keyword tells the Authentication Agent to exclude this Authentication Manager from use during dynamic load balancing.

Important: Use the **AVOID** keyword only for dynamic load balancing. Do not use it with the **USESERVER** keyword for manual load balancing.

Using the sdopts.rec File for Manual Load Balancing

You configure manual load balancing by including the **USESERVER** keyword in the **sdopts.rec** file to specify which RSA Authentication Manager each Agent Host uses.

An Example Featuring the USESERVER Keyword

You can list the settings in the **sdopts.rec** file in any order, but you must list each setting separately, one setting per line. The following example shows how to use the **USESERVER** keywords in the **sdopts.rec** file:

```
;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 Authentication Manager identified by the actual IP address 192.168.10.23 receives more authentication requests than RSA Authentication Manager 192.168.10.22. RSA Authentication Manager 192.168.10.20 is used only if the Authentication Managers of higher priority are unavailable. RSA Authentication Manager 192.168.10.21 is 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 the Authentication Managers, and **ALIAS** keywords have no effect on which Authentication Managers are specified for use.

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

You can list the settings in the **sdopts.rec** file in any order, but you must list each setting separately, one setting per line. This example shows how to use the **ALIAS** keywords in the **sdopts.rec** file:

```
;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 either alias or actual IP addresses, with some exceptions. The RSA Authentication Manager with the actual IP address 192.168.10.23 has three alias addresses specified for it, while Authentication Managers 192.168.10.20 and 192.168.10.21 have only one alias apiece. RSA Authentication Manager 192.168.10.22 has two alias addresses. The aliases specified by the **ALIAS** keywords are additions to any aliases specified in the **sdconf.rec** file and in the RSA Authentication Manager list.

As shown in the example, 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 the Authentication Managers, and **ALIAS** keywords have no effect on which Authentication Managers are specified for use.

The exceptions in the example are that RSA Authentication Manager 192.168.10.23, as specified by the **ALIASES_ONLY** keyword, will be contacted only through its alias IP addresses. RSA Authentication Manager 192.168.10.22, specified by the **IGNORE_ALIASES** keyword, will be contacted only by using its actual IP address.

In the following example, 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 Authentication Agent should send its requests to RSA Authentication Manager 192.168.10.23 and 192.168.10.22 by using only their alias IP addresses.

In the following example, 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 Authentication Agent should send its requests to RSA Authentication Manager 192.168.10.23 and 192.168.10.22 by using only their actual IP addresses.

Using the AVOID Keyword In Dynamic Load Balancing

In dynamic load balancing, you exclude an RSA Authentication Manager from use for authentication by including the **AVOID** keyword in the **sdopts.rec** file. When you provide an actual IP address of an RSA Authentication Manager as a value, this keyword tells the Authentication Agent to exclude this Authentication Manager from use during dynamic load balancing.

Use the **AVOID** keyword only for dynamic load balancing. Do not use it with the **USESERVER** keyword for manual load balancing. If the **AVOID** keyword is included in an **sdopts.rec** file that includes a **USESERVER** statement, the **AVOID** statement is considered an error.

If you use the **AVOID** statement with the IP address of the default RSA Authentication Manager, the statement is ignored unless another Authentication Manager is available. The default Authentication Manager is the one on which the **sdconf.rec** file was created. If an Authentication Manager is designated as the master, however, it becomes the default Authentication Manager regardless of where the **sdconf.rec** file was created.

The following example shows how to use the **USESERVER** keywords in the **sdopts.rec** file:

```
AVOID=192.100.123.5
```

In this example, the RSA Authentication Manager with the IP address 192.100.123.5 will not be used for authentication.

Using the CLIENT_IP Keyword to Set an Overriding IP Address

When the RSA Authentication Agent runs on a 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 Authentication Agent and the RSA Authentication Manager.

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 Authentication Manager, making communication between Agent and Authentication Manager impossible.

Some Agent Hosts allow administrators to specify an overriding IP address in the RSA Security Center. For instructions, see [“Setting an IP Address Override”](#) on page 83. You can also specify an overriding primary IP address by including the **CLIENT_IP** keyword in an **sdopts.rec** file on the Authentication Agent Host. If no **sdopts.rec** file exists on the Authentication Agent Host, you can create one by following the instructions in [“Creating an sdopts.rec File”](#) on page 125.

Note: The Dynamic Host Configuration Protocol allocates IP addresses to Agent Hosts dynamically. To avoid address conflicts, do not enable DHCP for Agent Hosts with multiple IP addresses. Conversely, do not use the **CLIENT_IP** keyword for Agent Hosts that have single IP addresses, because these hosts have no alternative addresses to override.

To specify an IP address override in the **sdopts.rec** file, follow this example:

```
CLIENT_IP=192.168.10.19
```

This statement ensures that the Authentication Agent Host always uses the specified IP address to communicate with the RSA Authentication Manager.

Maintaining the Primary IP Address of the Authentication Agent Host in the RSA Authentication Manager

Each Agent Host’s primary IP address must be identified in its Agent Host record in the RSA Authentication Manager database. You can also list other IP addresses for the host as “secondary nodes” for failover.

If your RSA Authentication Manager system automatically registers Agent Hosts, the primary IP address of each Agent Host is automatically entered in the Authentication Agent record on the RSA Authentication Manager. The address is updated in the record whenever it changes. For more information, see Appendix B, [“Automated Registration of Agent Hosts.”](#)

If your system does not use auto-registration, you must ensure that the RSA Authentication Manager administrator knows the primary and secondary IP address of the Authentication Agent Host as soon as the Authentication Agent Host is initially configured. If an Agent Host address changes, inform the RSA Authentication Manager administrator immediately so that the administrator can update the Authentication Agent Host record in the RSA Authentication Manager.

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

B

Automated Registration of Agent Hosts

Overview of Automated Registration of Agent Hosts

Running the Automated Agent Host Registration and Update utility (**sdadmreg.exe**) on a new Agent Host registers the Host in the RSA Authentication Manager database and eliminates the need for an administrator to manually create the Authentication Agent Host record. Additionally, running the Automated Agent Host Registration and Update utility any time the Authentication Agent Host's IP address changes updates the IP address for the Authentication Agent Host in the RSA Authentication Manager database. This feature is 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 changes from the RSA Authentication Manager **sdconf.rec** configuration file.

To use the Automated Agent Host Registration and Update utility, you must install the utility on the Authentication Agent Hosts. Additionally, the RSA Authentication Manager administrator must configure the Authentication Manager to allow automated registration. For instructions, see the RSA Authentication Manager Help topic "Changing System Parameters."

When you run the RSA Authentication Agent installation wizard, you can select the Automated Agent Host Registration and Update utility for installation along with the Local Authentication Client component. Because local authentication is the only solution that supports DHCP for assigning IP addresses, the Registration and Update utility is not offered for installation with any of the other Agent Host components (for example, the Remote Authentication Server component or the Domain Authentication Server component).

Note: Although you can configure the RSA Authentication Manager to enable offline authentication and password integration system-wide, when you use Automated Agent Host Registration to register a new Agent in the RSA Authentication Manager database, the new Agent is registered with offline authentication and password integration disabled.

Running the Automated Agent Host Registration and Update Utility

RSA Security recommends that you run the Automated Agent Host Registration and Update utility:

- Immediately after installing RSA Authentication Agent software on a Windows host. If the RSA Authentication Manager is configured for automated registration, an Agent Host record is added to the RSA Authentication Manager database (unless a record for the Authentication Agent already exists).
- When the Authentication Agent Host gets a new IP address. The new IP address is written to the Authentication Agent Host record in the RSA Authentication Manager database, provided that a node secret for the Authentication Agent Host has already been created by a successful authentication from the Authentication Agent Host to the RSA Authentication Manager.
- When you want to have the Authentication Agent Host registry updated by the current **sdconf.rec** file on the RSA Authentication Manager. The updated registry setting does not take effect until you restart the Authentication Agent Host.

To run the Automated Agent Host Registration and Update utility:

1. Before you run **sdadmreg.exe**, verify that database brokers are running on the RSA Authentication Manager.

If the RSA Authentication Manager is installed on a Windows computer, starting any RSA Authentication Manager program, such as the Database Administration application, automatically starts the database brokers.

If the RSA Authentication Manager is installed on a UNIX computer, start the database brokers by issuing the **ACEPROG/sdconnect start** command on the RSA Authentication Manager. **ACEPROG** represents the directory path of the RSA Authentication Manager executables directory.

2. To run the Automated Host Registration and Update utility, do one of the following:

- Restart the Authentication Agent Host.
The Automated Agent Host Registration and Update utility runs when the Authentication Agent Host is restarted.
- 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 Authentication Agent Host.



GINA Implementation in RSA Authentication Agent 6.1 for Microsoft Windows

Overview

RSA Authentication Agent 6.1 for Microsoft Windows implements a Graphical Identification and Authentication .dll (GINA) to protect desktop logons. RSA Authentication Agent Logon GINA (**AceGina.dll**) does not replace Microsoft's GINA (**msgina.dll**). Instead, **AceGina.dll** is tightly integrated with **msgin.dll** and relies on it to manage some of the Windows authentication tasks. Because **AceGina.dll** does not replace **msgina.dll**, third-party products that capture the Microsoft Windows password as it is passed into **msgina.dll** still work.

Because **AceGina.dll** delegates tasks to **msgina.dll**, **AceGina.dll** must be the last GINA in the GINA chain (if one exists).

Supported Third-Party GINAs

Some software vendors implement their GINAs as chaining GINAs. This means that after a GINA finishes executing its authentication tasks, it can pass authority to another GINA down the GINA chain. Chaining GINAs can pass authority to **AceGina.dll** provided that the chaining GINAs have documented support for GINA chaining, and that **AceGin.dll** is the last in the chain.

RSA Authentication Agent 6.1 for Microsoft Windows directly supports some chaining GINAs by placing **AceGina.dll** correctly in the GINA chain during the installation of RSA Authentication Agent. RSA Authentication Agent indirectly supports other chaining GINAs by enabling you to manually configure your registry to enable the third-party GINAs to chain to **AceGina.dll**.

Directly Supported GINAs

Directly supported GINAs are GINAs that the RSA Authentication Agent installer correctly places in the GINA chain. RSA Authentication Agent 6.1 for Microsoft Windows directly supports the following third-party chaining GINAs:

- Check Point VPN SecureRemote/SecureClient (**Ckpginashim.dll**)
- Cisco VPN Client (**Csgina.dll**)
- Citrix MetaFrame (**Ctxgina.dll**)
- Symantec pcAnywhere (**Awgina.dll**)

If these products are on your system, when you install RSA Authentication Agent 6.1 for Microsoft Windows, the RSA Authentication Agent installer places **AceGina.dll** in the correct location in the GINA chain. For more information, see [“Installing the RSA Authentication Agent GINA”](#) on page 138.

Indirectly Supported GINAs

Indirectly supported GINAs are GINAs that can coexist with RSA Authentication Agent 6.1 for Microsoft Windows, but are not placed in the GINA chain by the Authentication Agent installer. You can use RSA Authentication Agent 6.1 for Microsoft Windows with third-party chaining GINAs that are not directly supported by manually configuring your registry to enable chaining to **AceGina.dll**. For registry keys and values, see the following section [“Manually Configuring GINA Chaining.”](#)

Manually Configuring GINA Chaining

You can manually configure your registry to enable chaining with indirectly supported third-party GINAs. You can also edit the registry to repair the GINA chain if RSA Authentication Agent or the third-party GINA installer creates a configuration that renders either **AceGina.dll** or the third-party GINA inoperable.

The following tables contain registry keys and values for directly supported and indirectly supported GINAs.

Check Point VPN SecureRemote/Secure Client

HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\GinaDLL = Ckpginashim.dll

HKLM\SOFTWARE\Checkpoint\SecureRemote\Support3rdPartyGina = 1

HKLM\SOFTWARE\Checkpoint\SecureRemote\ThirdPartyGina = AceGina.dll

Cisco VPN Client

HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\GinaDLL = Csgina.dll

HKLM\SOFTWARE\Cisco Systems\VPN Client\GinaInstalled = 1

HKLM\SOFTWARE\Cisco Systems\VPN Client\PreviousGinaPath = AceGina.dll

Citrix MetaFrame

HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\GinaDLL = Ctxgina.dll

HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\CtxGinaDLL = AceGina.dll

pcAnywhere (v 9 and 10.0 on W2K or XP)

HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\GinaDLL = Awgina.dll

HKLM\SOFTWARE\Symantec\pcANYWHERE\CurrentVersion\System\GinaDLL = AceGina.dll

Novell Client

HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\GinaDLL = AceGina.dll

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SDSupercededGina = Nwgina.dll

XpaSystems pGina

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL = AceGina.dll

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SDSupercededGina = Pgina.dll

SafeBoot Client

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL = AceGina.dll

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SDSupercededGina = Sbgina.dll

Symantec Norton Ghost Client

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL = AceGina.dll

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SDSupercededGina = Ginastub.dll

Unsupported GINAs

Some vendors implement GINAs as replacement GINAs. This means that another GINA up the chain can pass authority to the replacement GINA. The replacement GINA must be last in the chain. Because **AceGina.dll** must be the last GINA in the chain, it cannot coexist with replacement GINAs. To use RSA Authentication Agent 6.1 for Microsoft Windows on a system that has a third-party replacement GINA, you must replace the third-party GINA with **AceGina.dll**. For more information, see the following section [“Installing the RSA Authentication Agent GINA.”](#)

Important: RSA Security recommends that you uninstall the third-party GINA instead of replacing it with **AceGina.dll** when you install RSA Authentication Agent. Uninstalling the third-party replacement GINA software after you install **AceGina.dll** may prevent **AceGina.dll** from functioning. If you plan to install an unsupported third-party GINA, RSA Security recommends that you uninstall RSA Authentication Agent first.

Installing the RSA Authentication Agent GINA

If no previously installed third-party GINAs exist on the system, the RSA Authentication Agent 6.1 for Microsoft Windows installer registers **AceGina.dll** as the GINA on the Windows system.

If a supported third-party GINA is already installed on the system, the RSA Authentication Agent installer configures the GINA to chain, or pass authority, to **AceGina.dll**. **AceGina.dll** does not replace the third-party GINA.

If an unsupported third-party GINA is already installed on the system, the RSA Authentication Agent installer issues a warning about it and prompts you to either cancel the installation or replace the third-party GINA with **AceGina.dll**. If you choose to abort the installation, **AceGina.dll** is not installed and no change is made to the system. If you replace the current GINA with **AceGina.dll**, the installer unregisters the third-party GINA and registers **AceGina.dll** on the Microsoft Windows system. Any functionality from the third-party GINA that is replaced by **AceGina.dll** is lost.

Note: Although the RSA Authentication Agent gives you the option of replacing the third-party GINA, RSA Security recommends that you uninstall the third-party GINA before you install RSA Authentication Agent.

If you attempt to install a third-party GINA after **AceGina.dll** has been installed, the behavior of **AceGina.dll** depends on whether the third-party GINA installer can correctly chain to **AceGina.dll**.

D

Configuring Web Servers for RSA SecurID Authentication

Configuring Web Servers for Domain Authentication With Remote Access Authentication

If your domain is protected with RSA Authentication Agent 6.1 for Microsoft Windows, and includes remote access applications, domain authentication and remote access authentication are incompatible. You can solve this problem by using the Active Directory Users and Computers interface to create groups for the remote access application hosts, and then use the RSA Security Center on the domain controller to tell the Authentication Agent how to address the hosts during authentication.

Selecting **Verify** on the Challenge Settings page in the RSA Security Center tells the Authentication Agent on the domain controller to verify that the remote application host recently made a valid authentication request to the RSA Authentication Manager, and then to allow access to the domain. Selecting **Exclude** tells the Authentication Agent not to challenge authentication requests from the remote access application host. For more information, see [“Using Domain Authentication with Remote Access Authentication”](#) on page 59.

To use **Verify** and **Exclude**, you must configure your application server to use basic authentication. Because basic authentication sends authentication requests in cleartext, in a web server environment, you must also configure your browser (for example, Outlook Web Access) to use the Secure Sockets Layer (SSL) protocol or Secure Hypertext Transfer Protocol (S-HTTP).

Important: RSA Security strongly recommends that whenever you configure an application server to use basic authentication, you use either SSL or S-HTTP.

To configure a web server environment for Verify and Exclude:

1. Configure the web browser to use SSL.
2. Configure the application server (web server) to use basic authentication.
3. Protect the application server (web server) with RSA SecurID authentication by installing and configuring RSA Authentication Agent 5.3 for Web.
For instructions, see your RSA Authentication Agent 5.3 for Web documentation.
4. Configure the RSA SecurID URL for anonymous access.

Configuring Microsoft Outlook Web Access in Front-End/Back-End Environments

In addition to performing the configuration steps described in the previous section [“Configuring Web Servers for Domain Authentication With Remote Access Authentication,”](#) you must perform additional configuration for front-end/back-end environments in which the front-end web server performs the RSA SecurID challenge, and the back-end performs the Windows challenge.

To configure a domain authentication with remote authentication in a front-end/back-end environment:

1. Add an Agent record to the RSA Authentication Manager database for the front-end server, and configure it to create verifiable authentications.
2. Copy the record and name the copy after the back-end server.
3. Create a group for both the front-end and back-end servers, and use the RSA Security Center on the domain controller to instruct the Authentication Agent to verify the group.

For instructions, see the RSA Security Center Help topic “Enabling Domain Authenticating With Remote Authentication.”

Index

A

- aceclient.log file, 108
- AceGina
 - installing, 138
- Active Directory
 - and Windows password integration, 16
 - creating groups of remote access
 - application hosts, 32, 59, 139
 - with domain authentication, 38
 - with offline authentication, 34, 86
 - with remote authentication, 66, 67, 73, 76
- advanced settings, configuring, 81
- authenticating
 - GUI-based Windows operations, 102
 - Windows commands, 101
- authentication
 - offline, 15, 85
 - Safe Mode, 17
 - terminal services, 97
- Authentication Agent hosts, cloning, 50
- Authentication Manage, setting up, 30
- authentication prompts, changing time-out values, 69
- authentication solutions, 19
- Authenticator Utility, interoperability with Authentication Agent, 29
- Automated Agent Host Registration and Update Utility
 - running, 134
- Automated Agent Host Registration and Update utility, 133
 - installing automatically, 38
- automatic recharge of offline days, 88

C

- Certificate Utility
 - installing, 41
 - starting, 42
- certificates
 - creating for domain authentication, 42
 - for wireless authentication, 74, 76
 - root, 42
 - server, 42
- chaining GINAs, 135
- challenge groups, creating, 31
- challenge options, 15

- challenge status, changing, 90
- challengedinfo.dat file, 90
- changing
 - offline users' challenge status, 90
 - time-out values for authentication prompts, 69, 106
- clearing
 - offline data, 82
- clearing, node secret, 81
- cloning Authentication Agent hosts, 50
- commands
 - net use, 101
 - RSANetUse, 98
 - RSARunAs, 98
 - runas, 101
- common behavior, exceptions, 17
- communication devices, requirements, 22
- configuring
 - advanced settings, 81
 - domain authentication, 55
 - front end and back end environments, 140
 - IAS for RSA Security EAP - Protected OTP, 73
 - local authentication, 53
 - remote authentication, 65
 - RSA Security EAP - Protected OTP on IAS, 73
 - web servers for domain authentication with remote authentication, 139
 - wireless authentication, 71
- creating
 - certificates for domain authentication, 42
 - groups, 31
 - installation package, 48
- cross realm limitations, 30
- cross-domain trust
 - between a protected and an unprotected domain, 58
 - between protected domains, 58
- custom installation, 45

D

- directly supported third-party GINAs, 135
- dismissing tool tips automatically, 79

- domain authentication
 - configuring, 55
 - enabling, 55
 - testing, 56
 - with remote authentication, 59

E

- elevating privileges, 35
- emergency access, 91
- emergency codes
 - offline, 91
 - passcode, 91
 - tokencode, 91
- emergency passcode, 91
- emergency tokencode, 91
- enabling
 - domain authentication, 55
 - local authentication, 53
- error messages, 109
- Event Viewer
 - log messages, 109
 - log settings, 83
- exceptions to common behavior, 17
- excluding remote access application
 - hosts, 61
- exempt administrator account, 15
- exempt group for remote access application
 - hosts, 32

F

- files, language, 44
- front-end and back-end environments,
 - configuring, 140

G

- GINA registry settings, 136, 137
- GINAs
 - chaining, 135
 - directly supported, 135
 - indirectly supported, 136
 - replacement, 137
 - supported, 135
 - unsupported, 137
- groups, creating, 31
- GUI-based Windows operations,
 - authenticating, 102

I

- IAS Server, configuring for PEAP, 78
- icon, RSA Security Center, 90

- indirectly supported third-party GINAs, 136
- installation
 - silent, 46
 - typical and custom, 45
- installation language, 14, 96
- installation package
 - configuring to run from a different
 - location, 49
 - creating, 48
 - running, 50
 - running from where it was created, 50
- installing, 138
 - Automated Agent Host Registration and
 - Update utility, automatically, 38
 - Certificate Utility, 41
 - RSA Authentication Agent GINA, 138
- interoperability
 - Authenticator Utility, 29
 - previous versions and third-party
 - software, 28
 - web-based SSL virtual private
 - networks, 30

K

- key features, 12

L

- language components, configuring the
 - network installation package, 49
- language files, 44
- language, for installation, 14, 96
- limitations
 - cross-realm, 30
 - smart cards, 30
- load balancing, 125
- local authentication
 - configuring, 53
 - enabling, 53
- logon scripts
 - RSANetUse, 99
 - RSARunAs, 100
- logs
 - Event Viewer, 109
 - filtering event messages, 83
 - setting up for tracing, 83
 - Windows, 108

M

- Microsoft IAS Server, configuring for
 - PEAP, 78

Microsoft Management Console, elevating privileges, 35

N

net use command, 101
network installation package
 configuring to install language components, 49
 configuring to run from a different location, 49
 running, 50
 running from where it was created, 50
node secret, clearing and replacing, 81, 106
node verification failure, 106

O

offline authentication, 15, 85, 92
 for remote users, 92
offline data
 clearing, 82
offline days
 checking the supply, 90
 managing, 88
 recharging
 automatically, 88
 manually, 89
 when there is a network connection, 88
 when there is no network connection, 88
offline days status, 90
offline emergency codes
 passcode, 91
 tokencode, 91
offline users' challenge status, changing, 90
overriding IP address, setting, 130

P

passcode, emergency, 91
password integration, 16
PEAP
 configuring Microsoft IAS Server, 78
 configuring remote client computers, 76
ports, required, 20
preparations
 creating groups of users to challenge, 31
 RSA Authentication Manager, 30
 RSA SecurID users, 35
 wireless environment, 71, 73, 75, 77

previous versions and third-party software, interoperability with Authentication Agent, 28
previous versions, when to uninstall, 123
privileges, elevating, 35
profiles, roaming, 63
protected domains, cross-domain trust, 58

R

recharging offline days
 manually, 89
 when there is a network connection, 88
 when there is no network connection, 88
registry settings, GINA, 136, 137
remote access application hosts
 excluding, 61
 verifying, 59
remote access application hosts, exempt group, 32
remote authentication
 configuring, 65
 requirements, 22
 with domain authentication, 59
remote client computers, configuring for PEAP, 76
remote client computers, configuring for RSA Security EAP - Protected OTP, 72
remote users, 92
removing the sdeap.dll file, 124
replacement GINAs, 137
replacing the node secret, 81
required ports, 20
requirements
 communication devices, 22
 remote authentication, 22
 RRAS without EAP, 23
 wireless authentication, 25
reserve password, 53
restarting in Safe Mode, 17
roaming profiles, 63
root certificates, 42
RRAS without EAP, requirements, 23
RSA Authentication Agent GINA, 138
RSA Authentication Agent, installing, 44
RSA Authentication Manager
 setting up, 30
RSA SecurID users, preparing, 35
RSA Security Center, 51
RSA Security Center icon, 90

RSA Security EAP - Protected OTP
 configuring remote client
 computers, 72
 RSANetUse, 98
 RSARunAs, 98, 100
 runas command, 101
 running an installation package, 50

S

Safe Mode, authentication, 17
 sdconf.rec file
 copying from the RSA Authentication
 Manager, 30
 viewing, 107
 sdeap.dll, removing, 124
 sdopts.rec file, creating, 125
 server certificates, 42
 settings
 Event Viewer log, 83
 node secret, 106
 silent installation, 46
 single user name for multiple resources, 17
 smart cards, limitations, 30
 solutions
 RRAS without EAP, 23
 wireless authentication with PEAP, 25
 solutions, authentication, 19
 starting the Certificate Utility, 42
 status, offline days, 90
 supported third-party GINAs, 135

T

terminal services, authentication, 97
 third-party GINAs
 directly supported, 135
 indirectly supported, 136
 supported, 135
 unsupported, 137
 time-out values, changing, 69, 106

tokencode, emergency, 91
 tool tips, automatically dismissing, 79
 trace logs, setting up, 83
 troubleshooting, 105
 typical installation, 45

U

uninstalling, 123
 unsupported third-party GINAs, 137
 upgrading, 123

V

verifying remote access application
 hosts, 59
 virtual private networks, interoperability with
 Authentication Agent, 30

W

web servers, configuring for RSA SecurID
 authentication, 139
 when to uninstall previous versions, 123
 Windows
 logs, 108
 troubleshooting, 108
 Windows commands, authenticating, 101
 Windows password integration, 16
 Windows tool tips, automatically
 dismissing, 79
 wireless authentication
 certificate requirements, 74, 76
 configuring, 71
 deploying with PEAP, 74
 deploying with RSA Security EAP -
 Protected OTP, 71
 requirements, 25
 wireless environment, setting up, 71, 73, 75,
 77