

RSA SecurID for Microsoft Windows Planning Guide 1.1



Contact Information

See our web site 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	5
Audience	5
Documentation	5
Getting Support and Service	5
Chapter 1: Introduction	7
Features of RSA SecurID for Microsoft Windows	7
Secure Resource Protection	7
A Simplified Authentication Process	8
A Choice of Challenge Options	8
RSA RADIUS Server	9
Support for Multiple Token Types	9
Features Designed to Enhance Usability	9
Customization Options	10
Emergency Access	10
Centralized Logging	11
Easy Deployment	11
Supported Platforms and Requirements	11
RSA Authentication Agent 6.1 for Microsoft Windows	11
RSA Authentication Agent 5.3 for Web	12
RSA Authentication Manager 6.1	13
Chapter 2: Planning Logical Deployment	15
Planning Which Authentication Solutions to Deploy	15
Local Authentication	15
Remote Authentication	16
Wireless Authentication	19
Planning Which Users to Challenge	19
Planning User Authentication	20
Windows Password Integration	20
Offline Authentication	20
Planning Emergency Access	21
Chapter 3: Sample Logical Deployment Scenarios	25
Scenario 1: Small Company	25
Discussion	26
Scenario 2: Medium-Sized Company	28
Discussion	29

Chapter 4: Planning Physical Deployment	33
Planning What to Install and Where to Install It.....	33
Deploying Local Authentication.....	33
Deploying Remote Authentication	35
Deploying Wireless Authentication.....	42
Planning an Installation Method	47
Interactive Installation	47
Silent Installation	47
Index	49

Preface

This book provides a framework for implementing RSA SecurID for Microsoft Windows in your organization. RSA SecurID for Microsoft Windows combines RSA Authentication Manager 6.1 with RSA Authentication Agent 6.1 for Microsoft Windows to enhance native Windows security with the strong, two-factor authentication of time-based RSA SecurID tokens.

Audience

This book is intended for network and security administrators, systems integrators, and information technology managers. 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 *RSA Authentication Agent 6.1.1 for Microsoft Windows Readme*. This file is named **readme.html** and is located in the root 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

Introduction

RSA SecurID for Microsoft Windows is a multicomponent solution that enhances native Windows security with the strong, two-factor authentication of time-based RSA SecurID tokens. The solution incorporates RSA Authentication Agent 6.1 for Microsoft Windows, RSA Authentication Agent 5.3 for Web, and RSA Authentication Manager 6.1.

Within this solution, RSA Authentication Agent 6.1 for Microsoft Windows requires users to provide RSA SecurID passcodes to authenticate to their Windows desktops, and to open remote connections to the Microsoft network.

RSA Authentication Agent 5.3 for Web requires users to authenticate with RSA SecurID passcodes to access the company's web resources. When a user attempts to access a protected resource or open a remote connection, the Authentication Agent intercepts the request and prompts the user for an RSA SecurID passcode instead of, or in addition to, a Microsoft Windows password, depending on how you configure your system. The Authentication Agent sends the user's logon information to the RSA Authentication Manager for validation.

The RSA Authentication Manager is the repository for users' authentication accounts. You can create the accounts manually, or import them from an existing Active Directory or LDAP database. During authentication, if the Authentication Manager receives logon information that matches the user's record in the Authentication Manager database, the user is authenticated and gains access to the protected resource.

This guide focuses on RSA Authentication Agent 6.1 for Microsoft Windows. For complete information about RSA Authentication Manager, see the *RSA Authentication Manager 6.1 Administrator's Guide* for your platform. For complete information about RSA Authentication Agent 5.3 for Web, see the *RSA Authentication Agent 5.3 for Web Installation and Configuration Guide* for your platform.

Features of RSA SecurID for Microsoft Windows

Secure Resource Protection

RSA SecurID for Microsoft Windows enhances Windows password security with two-factor authentication, a method that is built on patented time-synchronous technology and algorithms that have been proven secure over time.

RSA SecurID authentication is stronger protection than just a password because it combines something you have (your RSA SecurID tokencode) with something you know (your RSA SecurID PIN). When a user attempts to access protected resources, the RSA Authentication Agent challenges the user for an RSA SecurID passcode and sends it to the RSA Authentication Manager for verification. Authorized users gain access easily while unauthorized users are denied access.

The following table describes which resources the Authentication Agent protects.

Protected Resource	Description
Local Windows desktops	Local authentication requires users to provide RSA SecurID passcodes (the user's PIN followed by a tokencode) to authenticate to their local Windows desktops. For more information, see “Local Authentication” on page 15.
Remote connections to network resources	Remote authentication requires users to provide RSA SecurID passcodes before opening remote connections to protected networks. For more information, see “Remote Authentication” on page 16.
Remote wireless connections to network resources	Wireless authentication requires users to provide RSA SecurID passcodes before opening remote wireless connections to protected networks. For more information, see “Wireless Authentication” on page 19.

A Simplified Authentication Process

Windows password integration incorporates the Microsoft Windows password into the RSA SecurID logon process. Depending on how you use password integration, users provide Windows logon passwords once during an initial connected authentication, and again when the password expires (for example, after 90 days, or in accordance with your security policy). For all other authentications, users provide only their RSA SecurID passcodes. For more information, see [“Windows Password Integration”](#) on page 20.

The offline authentication feature adds consistency to the authentication process by extending RSA SecurID authentication to protected computers when the connection to the RSA Authentication Manager is not available. Whether online or offline, users authenticate in the same way. For more information, see [“Offline Authentication”](#) on page 20.

A Choice of Challenge Options

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

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

The RSA Authentication Agent uses default Windows groups or groups that you create yourself using the Windows Computer Management interface.

For more information, see [“Planning Which Users to Challenge”](#) on page 19.

RSA RADIUS Server

The RSA SecurID for Microsoft Windows solution includes RSA RADIUS Server, a RADIUS server shipped with RSA Authentication Manager that supports RSA Security EAP - Protected One Time Password (OTP) (EAP 32). RSA RADIUS Server also continues to support RSA Security EAP (EAP 15).

Incorporating RSA RADIUS Server into your remote authentication solution eliminates the need for the RSA Authentication Agent on the remote server. For more information, see [“Remote Authentication”](#) on page 16.

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

Note: Using RSA SecurID software tokens is less secure than using other types of authenticators because users can log on to their computers and the network with only their PINs. The other types of authenticators require users to either type in their PINs and passcodes or, for the RSA SecurID Authenticator SID800, physically connect the authenticator to the computer and then type in a PIN. Additionally, because software tokens are stored on the computer, users cannot remove their tokens when they leave their computers.

Features Designed to Enhance Usability

RSA Authentication Agent 6.1 for Microsoft Windows addresses usability with the following features:

RSA Security Center. RSA Authentication Agent 6.1 for Microsoft Windows includes the RSA Security Center, a graphical user interface for administrators and users.

Integration with other key RSA Security products. RSA Authentication Agent integrates with RSA Authenticator Utility, another key RSA Security product. Installing these products together enables you to use RSA SecurID Authenticator SID800 for RSA SecurID authentication. RSA Authentication Agent and RSA Authenticator Utility share the same graphical interface—the RSA Security Center.

PIN-only Unlock. RSA Authentication Agent includes a configurable option that allows users to unlock the workstations on their protected computers using only their PINs instead of their full passcodes. As an administrator, you can enable and disable this feature, and set a time-out period for the feature. After the time-out period expires, users must unlock their workstations by entering their full passcodes. You configure the feature and set the time-out period in the RSA Security Center, the configuration interface for the Authentication Agent. For information, see the Help topic “Understanding the Windows Logon Settings.”

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.
- Specify whether logon prompts request passwords or passcodes.
- Localize the following using a language appropriate for your location:
 - The Authentication Agent portion of the RSA Security Center
 - RSA Authentication Agent logon prompts
 - Authentication messages
- For more information, see the chapter “Customizing RSA Authentication Agent 6.1 for Microsoft Windows” in the *Installation and Administration Guide*.

Emergency Access

RSA Authentication Agent 6.1 for Microsoft Windows provides a variety of emergency access methods. The method you use depends on your situation. The following table lists common situations and which methods apply to each.

Situation	Emergency Access Method
Lost token for an online user	• Fixed password • One-time password
Lost token for an offline user	Offline emergency tokencode
Forgotten PIN for an online user	PIN reset by the Help Desk Administrator
Forgotten PIN for an offline user	Offline emergency passcode
Administrative access to an offline computer	• Exempt administrator account • Reserve password

For more information, see [“Planning Emergency Access”](#) on page 21.

Centralized Logging

RSA Authentication Agent 6.1 for Microsoft Windows logs all authentication events centrally in the RSA Authentication Manager database. Authentication events generated by offline authentication are recorded temporarily on the local computer. RSA Security recommends that you configure the RSA Authentication Manager so that offline authentication records are transferred to the central log on the RSA Authentication Manager database when the offline user comes back online.

Easy Deployment

You can efficiently install RSA Authentication Agent 6.1 for Microsoft Windows by creating and configuring a Microsoft Installer (.msi) installation package to distribute to client computers. For example, depending on the authentication solution you choose, you must install RSA Authentication Agent components on every client computer within the protected environment. Creating an installation package can help you manage this task. For more information, see [“Planning an Installation Method”](#) on page 47.

Supported Platforms and Requirements

RSA Authentication Agent 6.1 for Microsoft Windows

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

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

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

For additional requirements, see the chapter “Requirements and Preparations” in the *Installation and Administration Guide*.

RSA Authentication Agent 5.3 for Web

Supported Platforms

The RSA Authentication Agent 5.3 for Web is qualified to run on the following platforms:

- Windows Server 2003, Standard and Enterprise Editions, with Internet Information Services (IIS) 6.0
- Windows 2000 Server with Service Pack 4 and Internet Information Services (IIS) 5.0

Note: The computer cannot be an RSA Authentication Manager Primary or Replica. Running both IIS and RSA Authentication Manager on the same computer may decrease performance.

Host System Requirements

Your system must meet the following minimum requirements:

- Intel Pentium or higher.
- 32 MB of RAM.
- 10 MB of free disk space.
- TCP/IP networking.
- The disk partition containing the web server directories must be an NTFS partition. The FAT file system is not supported.
- Secure Sockets Layer (SSL) certificate.
For more information about how to obtain an SSL certificate from a Certificate Authority, such as VeriSign, go to the VeriSign web site at <http://www.verisign.com>.
- If users access protected web pages through a proxy server, the proxy must support the passing of cookies.

Client System Requirements

Browser Support. Users accessing protected web pages must have one of the following web browsers installed on their computers:

- Microsoft Internet Explorer 5.5 or 6.0
- Netscape Navigator 7.2

Note: For security purposes, instruct users to disable caching in their browsers.

Wireless Support. RSA SecurID Web authentication through wireless access protocol requires the following WAP 1.1 and 1.2.1 specifications:

- Caching of cookies
- WML Document Type Definition (DTD) version 1.1

RSA SecurID users must enable the cookie acceptance feature in their browsers. They must also use web browsers that support FORMs and Persistent Client State HTTP Cookies.

Microsoft Exchange Server ActiveSync Support. RSA Authentication Agent 5.3 for Web is qualified to run on Microsoft Exchange Server 2003 ActiveSync.

Additional Requirements

RSA Authentication Agent 5.3 for Web works in conjunction with RSA Authentication Manager (formerly RSA ACE/Server) 5.2 or later. The Web Agent administrator should be familiar with the RSA Authentication Manager system and its features.

In addition, make sure the RSA Authentication Manager administrator has registered users in the Authentication Manager database and has distributed tokens.

Note: If you intend to use the Web Agent software to protect the files of multihomed servers, you must account for the extra IP addresses in the RSA Authentication Manager database. The RSA Authentication Manager administrator has to define a secondary node for each additional IP address used on the Authentication Agent Host. In addition, you must specify an IP address override. If you are using RSA ACE/Agent for Windows 6.0 or earlier, you specify the override on the **Advanced** tab of the RSA Authentication Agent control panel. If you are using RSA Authentication Agent 6.1 for Microsoft Windows, you specify the override on the Advanced Settings page of the RSA Security Center. The override address must match the network address specified for the Authentication Agent Host in the Server database. For instructions on how to define secondary nodes, see the RSA Authentication Manager documentation.

For complete information, see the *RSA Authentication Agent 5.3 for Web Installation and Configuration Guide* for your platform.

RSA Authentication Manager 6.1

Supported Platforms

RSA Authentication Manager 6.1 is qualified to run on the following platforms:

- Microsoft Windows 2000 Server or Advanced Server (Service Pack 4) running a supported language
- Microsoft Windows 2003 Enterprise Server running a supported language
- Microsoft Windows 2003 Standard Server running a supported language

For information about supported languages, see the *Administrator's Guide*.

Hardware Requirements

Your system must meet the following minimum requirements:

- Intel Pentium 266 MHz or faster processor (Windows 2000 Server)
- Intel Pentium 733 MHz or faster processor (Windows 2003 Server, Standard or Enterprise Edition)
- At least 256 MB of physical memory + 2 MB per 1,000 users
- Two times physical memory swap file

- Local CD drive
- NTFS File System
- Monitor display set to at least 800 x 600 pixels

To achieve the highest authentication rates possible, you need the following:

- Dual Intel Pentium 4 (3.2 GHz or faster) processors
- 2048 MB of physical memory per processor

Disk Space Requirements

Your system must meet the following minimum requirements:

- 200 MB for RSA Authentication Manager software
- Additional 2 MB per 1,000 users
- 20 MB for RSA Authentication Manager Remote Administration software
- 50 MB for RSA Authentication Agent for Windows

For more information on disk space requirements, see the chapter “Database Maintenance” for your platform in the *RSA Authentication Manager 6.1 for Windows Installation Guide*.

2

Planning Logical Deployment

Logical deployment is how you use the software in your business environment. Planning logical deployment before you install the software ensures a smooth implementation that suits the needs of your company. For example, you need to decide:

- Which authentication solutions you want to deploy
- Which emergency access methods you want to use
- What is the authentication process for users (for example, will users authenticate the same way whether online or offline, and will users enter both Windows passwords and RSA SecurID passcodes, or RSA SecurID passcodes only?)

This chapter discusses these and other important issues.

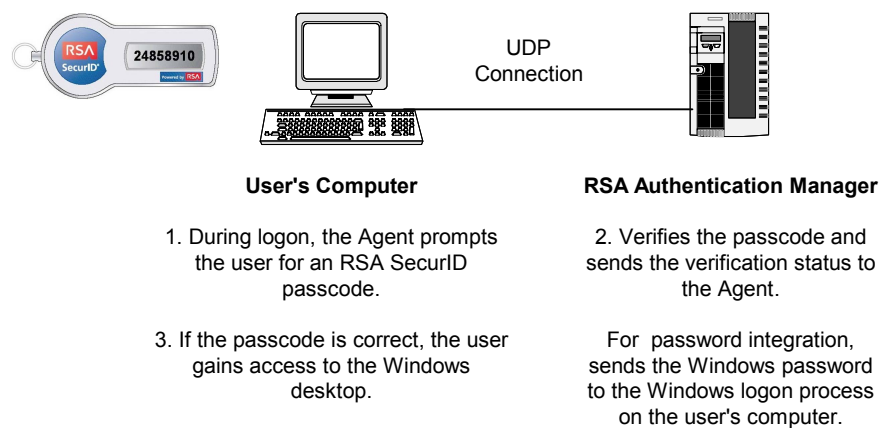
Planning Which Authentication Solutions to Deploy

You can deploy a single authentication solution, or a combination of solutions. The solutions that you deploy depend on which resources you want to protect.

This section summarizes each authentication solution.

Local Authentication

The local authentication component requires users to provide RSA SecurID passcodes to authenticate to their Windows desktops. The following figure shows the local authentication process.



For more information, see [“Deploying Local Authentication”](#) on page 33.

Remote Authentication

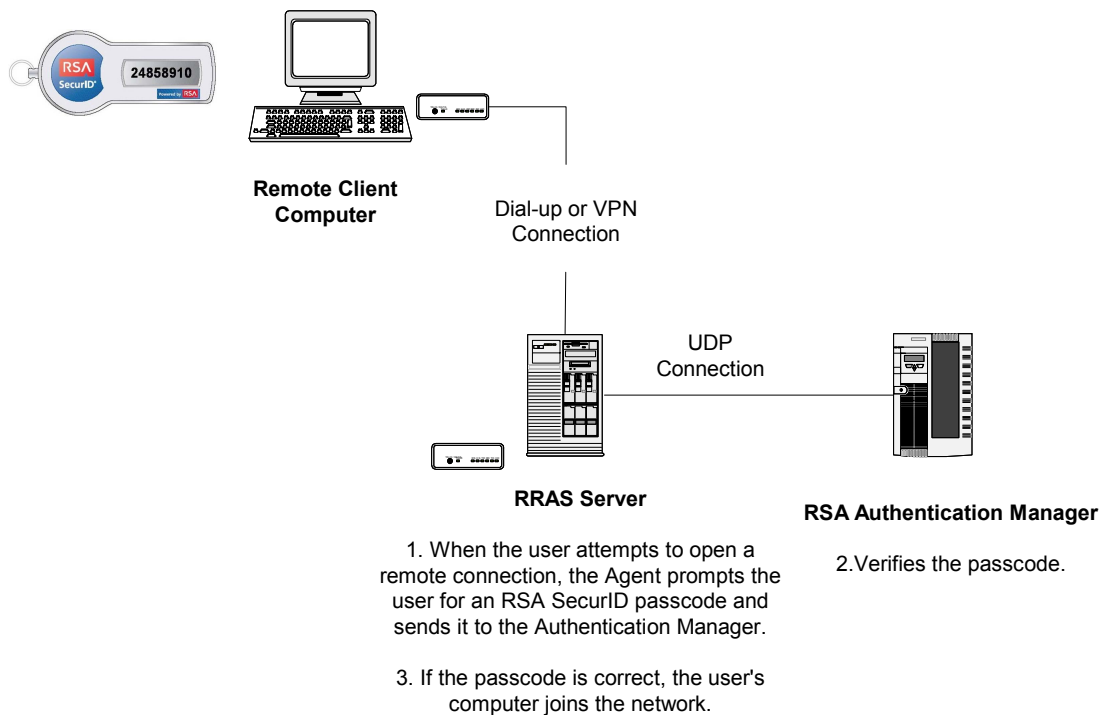
The remote authentication component requires users to authenticate with RSA SecurID passcodes before opening remote connections to the network using VPN clients or post-dial terminal windows.

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

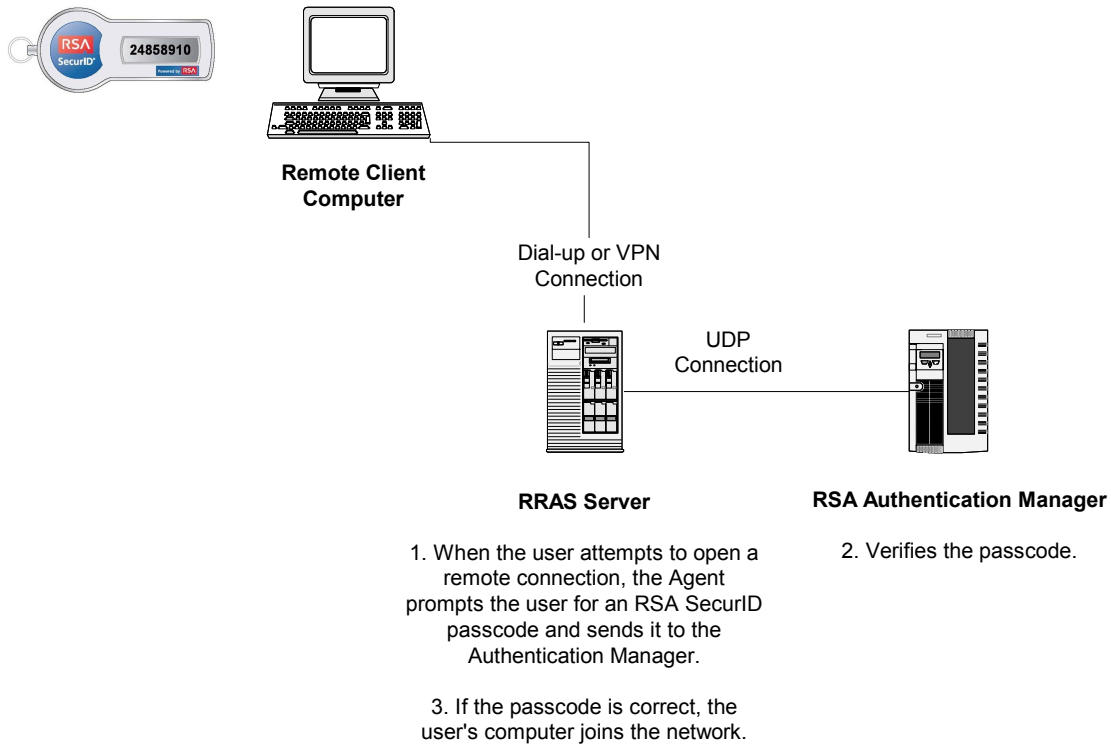
- Non-EAP
- EAP
 - Without a RADIUS server
 - With a RADIUS server
- Wireless PEAP

The following figures show the authentication process for each type of environment.

Remote Authentication Without EAP

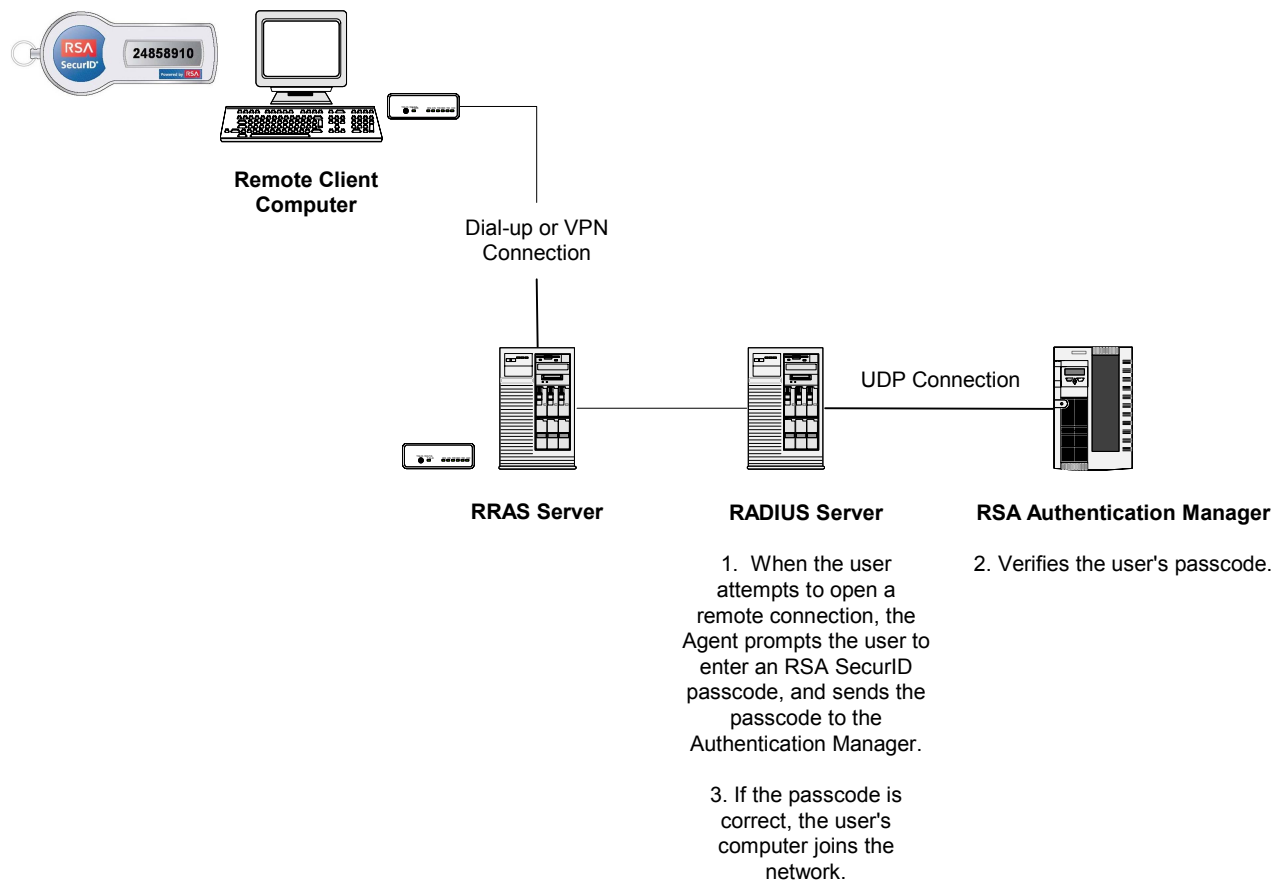


Remote Authentication Using EAP Without a RADIUS Server



Remote Authentication Using EAP With a RADIUS Server

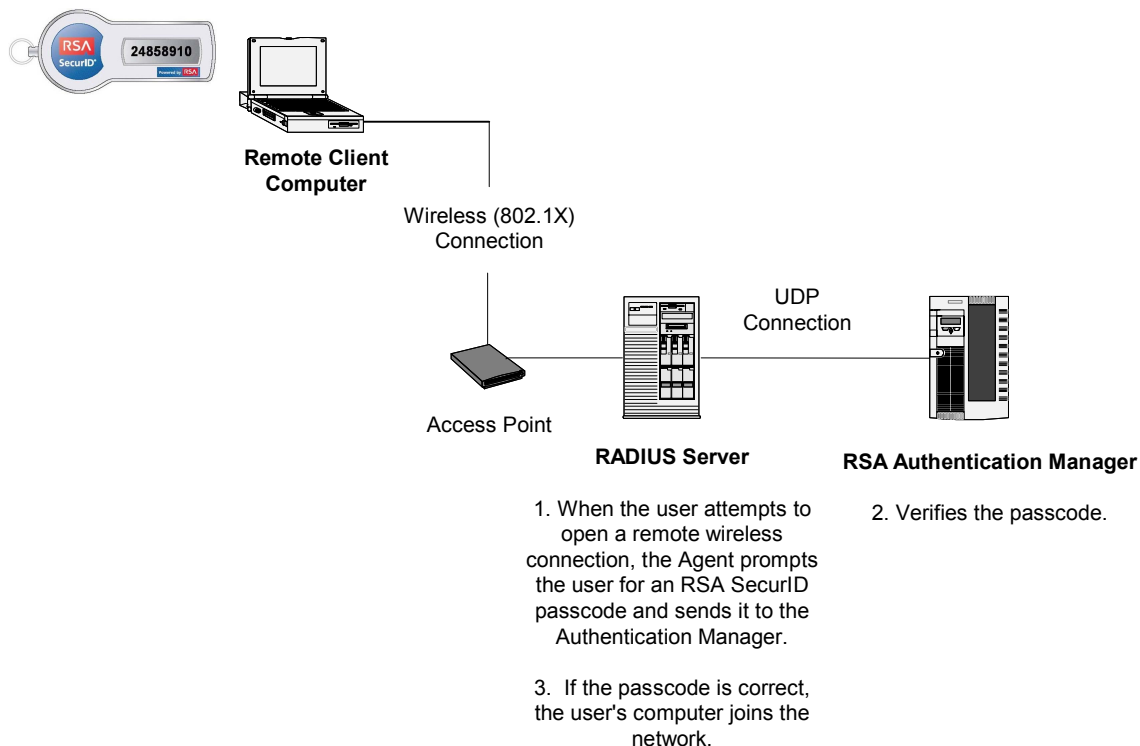
To illustrate the authentication process, the RADIUS server and the RSA Authentication Manager are shown on separate computers. However, you can install them both on a single computer. You can also use either Microsoft IAS RADIUS Server or RSA RADIUS Server. RSA RADIUS Server is shipped with RSA Authentication Manager 6.1. For more information about Microsoft IAS RADIUS Server and RSA RADIUS Server, see [“Deploying Remote Authentication”](#) on page 35.



Wireless Authentication

Wireless authentication requires users to authenticate with RSA SecurID passcodes before opening wireless connections to the company network.

The following figure shows the wireless authentication process. To illustrate the authentication process, the RADIUS server and the RSA Authentication Manager are shown on separate computers. However, you can install them both on a single computer. You can also use either Microsoft IAS RADIUS Server or RSA RADIUS Server, or a combination of both. RSA RADIUS Server is shipped with RSA Authentication Manager 6.1.



You can deploy wireless authentication using either of the following:

- RSA Security EAP - Protected OTP
- PEAP

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

For more information, see [“Deploying Wireless Authentication”](#) on page 42.

Planning Which Users to Challenge

You can configure RSA Authentication Agent to challenge:

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

The RSA Authentication Agent uses default Windows groups or groups that you create yourself using the Windows Computer Management interface.

If you want to use groups other than the Windows default groups, you need to create them before you configure RSA Authentication Agent. For instructions on creating groups, see your Windows documentation. For instructions on how to specify which users are challenged, see the Help topic “Specifying Users and Groups to Challenge With RSA SecurID.”

Planning User Authentication

Windows Password Integration

Windows password integration incorporates the Microsoft Windows password into the RSA SecurID logon process. The Windows passwords are stored with the users’ authentication data in the RSA Authentication Manager database and, for offline authentication, in the offline data.

For more information, see “Windows Password Integration” in the chapter “Overview and Key Features” in the *Installation and Administration Guide*.

Offline Authentication

Offline authentication is an authentication process that extends RSA SecurID authentication to protected computers when the connection to the RSA Authentication Manager is not available. Whether online or offline, users authenticate in the same way.

If offline authentication is enabled, when an RSA Authentication Agent connects to the RSA Authentication Manager, the Authentication Manager generates offline data and downloads it to the Authentication Agent computer. The Authentication Agent computer begins receiving offline data during the second connected authentication to the RSA Authentication Manager. For example, if you perform the authentication test described in “[Deploying Local Authentication](#)” on page 33 twice, then authenticate to the Authentication Manager, the Authentication Manager generates and downloads the offline data. When the local 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.

You enable, disable, and configure offline authentication through the RSA Authentication Manager Database Administration Application. You can enable and disable offline authentication system-wide, for individual Agents, or for groups of users. You can specify the amount of offline data the Authentication Manager generates either system-wide, or for groups of users. For example, if you configure the RSA Authentication Manager to generate seven offline days for the Sales group, every offline user in the Sales group gets seven offline days.

For more information, see the chapter “Offline Authentication” in the *Installation and Administration Guide*. Also see “Setting Up Offline Authentication and Windows Password Integration” in the chapter “Agents and Activation on Agent Hosts” in the *Installation and Administration Guide*.

Planning Emergency Access

Emergency access enables users and administrators to access protected resources when users lose their tokens, forget their PINs, or run out of offline days. The following tables describes the emergency access methods and tells where to find more information.

For Online Users

Emergency Access Method	Description	Supported Solutions	Characteristics	More Information
One-time passwords	Enables users to access their protected computers without a tokencode (for example, when they have lost their tokens)	Local	- Generated by the RSA Authentication Manager - Valid for one authentication - Must be combined with the user's RSA SecurID PIN	See "Temporary Passwords to Replace Lost Tokens" in the chapter "Registering Users for Authentication" in the <i>RSA Authentication Manager 6.1 Administrator's Guide</i> .
Fixed passwords	Enables users to access their protected computers without a tokencode (for example, when they have lost their tokens)	Local	- Created by an RSA Authentication Manager administrator - Valid until the user's lost token status is changed - Can be set to be the same as the offline emergency tokencode for offline users (for example, so a user who has lost his token can use the same password for working online and offline) - Must be combined with the user's RSA SecurID PIN	See "Temporary Passwords to Replace Lost Tokens" in the chapter "Registering Users for Authentication" in the <i>RSA Authentication Manager 6.1 Administrator's Guide</i> .

For Offline Users

Emergency Access Method	Description	Supported Solutions	Characteristics	More Information
Offline emergency tokencode	Enables users to access their protected computers without a tokencode (for example, when they have lost their tokens)	Local	• 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 • Can be set to be the same as the fixed password for online users (for example, so a user who has lost his token can use the same password for working online and offline)	See "Emergency Access" in the chapter "Overview" in the <i>Installation and Administration Guide</i> .
Offline emergency passcode	Enables users to access their protected computers without a PIN or tokencode (for example, when they have forgotten their PINs, when their PINs have been compromised, or when they have run out of offline days)	Local	• No PIN required • Changes the next time the user authenticates online • Expires after a specified amount of time	See "Emergency Access" in the chapter "Overview" in the <i>Installation and Administration Guide</i> .

For Administrators

Emergency Access Method	Description	Supported Solutions	Characteristics	More Information
Reserve password	Enables administrators to 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 "Setting a Reserve Password" in the chapter "Configuring Local Authentication" in the <i>Installation and Administration Guide</i> .
Exempt administrator account	Enables administrators to authenticate to protected computers as themselves with only a password	Local	• Created during Agent installation for the administrator performing the installation • Created for 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" in the chapter "Overview" in the <i>Installation and Administration Guide</i> .

3

Sample Logical Deployment Scenarios

This chapter presents two possible scenarios for deploying RSA SecurID for Microsoft Windows. Each scenario shows how you can use the software to satisfy business needs in your Windows environment. The scenarios are a small company with 50 employees, and a medium-sized company with 2,000 employees.

Scenario 1: Small Company

Suppose you manage a company that employs 50 people. As a company benefit, all employees work at home one day a week. Occasionally, some employees work while traveling. When employees work away from the office, they are offline from the network. To work away from the office, employees copy their files from the network to their laptops. To check their work e-mail accounts while away, employees use Microsoft Outlook Web Access.

Employees are not responsible for installing software on their computers. An administrator installs and configures software for non-administrators.

The following table shows what your company needs and what RSA SecurID for Microsoft Windows provides.

What Your Business Needs	What RSA SecurID for Microsoft Windows Provides
A simple, yet secure, way for users to authenticate	A consistent authentication process that is the same for online and offline authentications
A way to provide the RSA SecurID authentication process to users who work at home	A way to extend RSA SecurID two-factor authentication to computers that are not connected to the RSA Authentication Manager through the network
A secure way to protect remotely accessible web resources	RSA SecurID two-factor protection for web resources

The following tables shows where you can apply RSA SecurID authentication to this scenario, the components you need, and where to install them.

Component	Installation Location
Local Authentication Client	Each user's computer
Web Agent 5.3	Web server host

Discussion

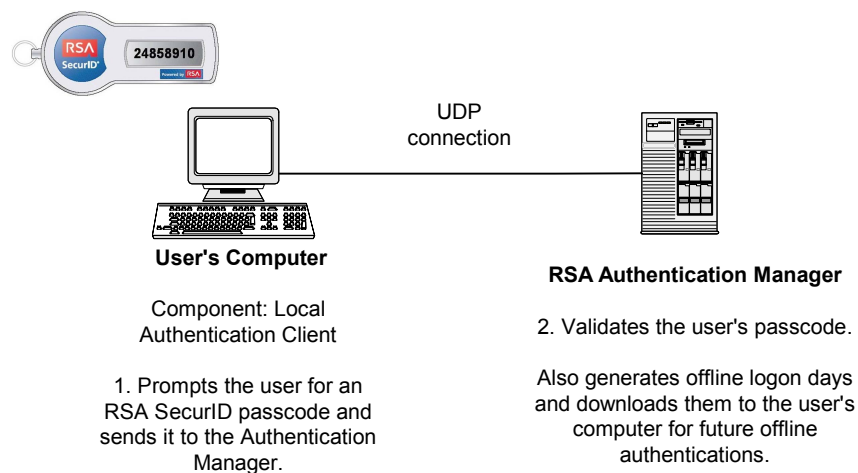
This scenario combines Windows password integration, and offline authentication to ensure a consistent authentication experience for users working inside and outside of the office.

Adding offline authentication extends the same RSA SecurID authentication process to users when they work away from the office. Users must enter RSA SecurID passcodes to authenticate offline to their Windows desktops whether they are online or offline to the network.

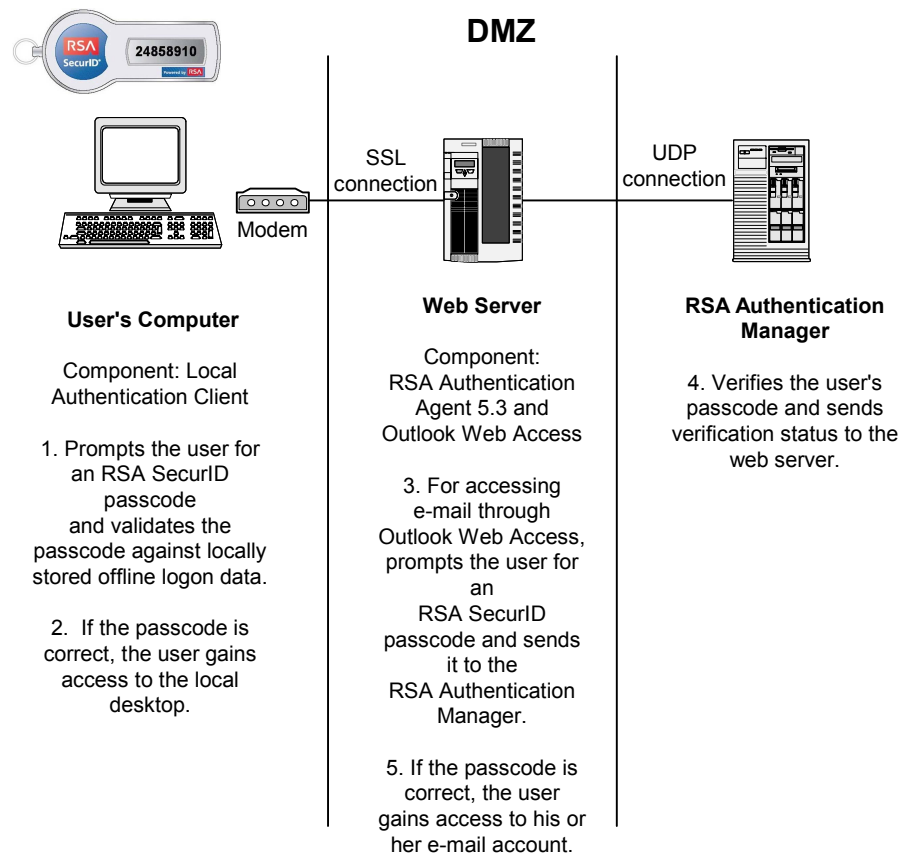
To protect web resources, this scenario uses RSA Authentication Agent 5.3 for Web. When offline users attempt to access their e-mail accounts through Microsoft Outlook Web Access, the Authentication Agent prompts the users for their RSA SecurID passcodes. Only authenticated users gain access to their company e-mail accounts.

Because administrators in your company install and configure software for non-administrative employees, the administrators need access to users' computers. To facilitate this, you can choose to challenge everyone for passcodes except administrators. You do this by creating a Windows group for the administrators, and challenging all users except members of the administrators group.

The following figure shows the online setup for users working in the office.



The following figure shows the setup for users working at home.



Scenario 2: Medium-Sized Company

Suppose you work for a company that employs 2,000 people. Twenty percent of the company's workers are sales representatives who use Internet Protocol Security Virtual Private Network (IPSec VPN) and Windows Terminal Services for Siebel to track customer account information remotely. A pilot group connects remotely using wireless connections. System administrators connect remotely using RRAS.

What Your Business Needs	What RSA SecurID for Microsoft Windows Provides
A secure way to protect remotely accessible domain resources	RSA SecurID two-factor protection for remotely accessible resources
A simple, yet secure, way for users to authenticate	- A way to integrate the Microsoft Windows password with RSA SecurID logon so users need to provide only their passcodes - An authentication process that is the same for online and offline authentications
An efficient way to install and configure RSA Authentication Agent client software	Support for Microsoft Installer (.msi)

The following tables show where you can apply RSA SecurID authentication to this scenario, the components you need, and where to install them.

Local Computers

Component	Installation Location
Local Authentication Client component	- Isolated lab computers - Offsite computers

Remote Connections

Component	Installation Location
Remote Authentication Server component	RRAS server

Wireless Connections

Component	Installation Location
Remote Authentication Server component	RADIUS server
RSA Security EAP client component	Every computer used to remotely access domain resources

Terminal Emulation Sessions

Component	Installation Location
Local authentication component	Terminal server

Discussion

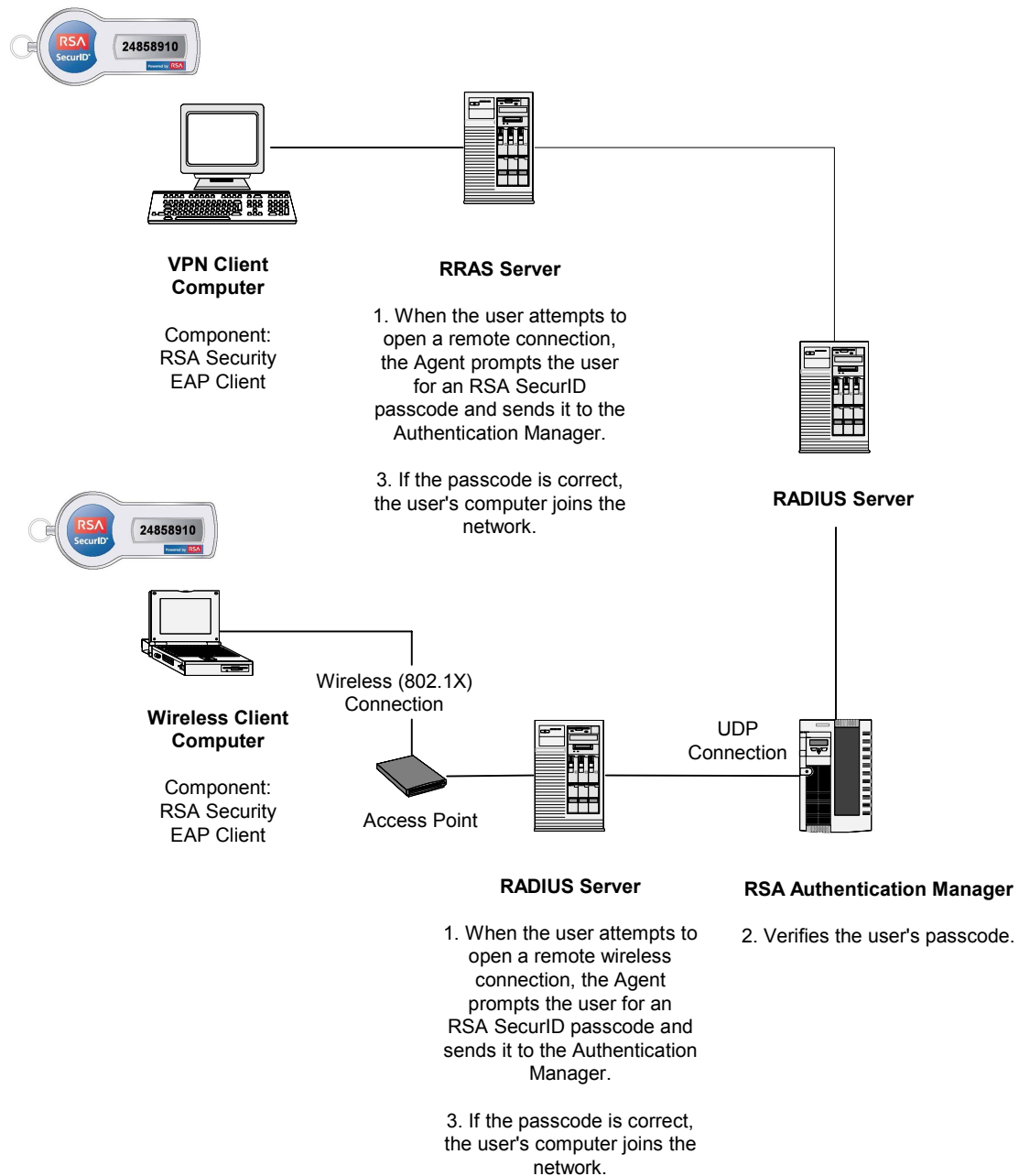
Remote and Wireless Connections

In this scenario, remote authentication requires users to authenticate with RSA SecurID passcodes before opening remote connections to the company domain.

Remote authentication requires sales representatives to authenticate before accessing their account data, and system administrators to authenticate before accessing the RRAS server (for example, to perform administration). Wireless authentication requires the pilot group to authenticate with passcodes before opening wireless connections.

For more information about remote authentication, see [“Deploying Remote Authentication”](#) on page 35. For more information about wireless authentication, see [“Deploying Wireless Authentication”](#) on page 42.

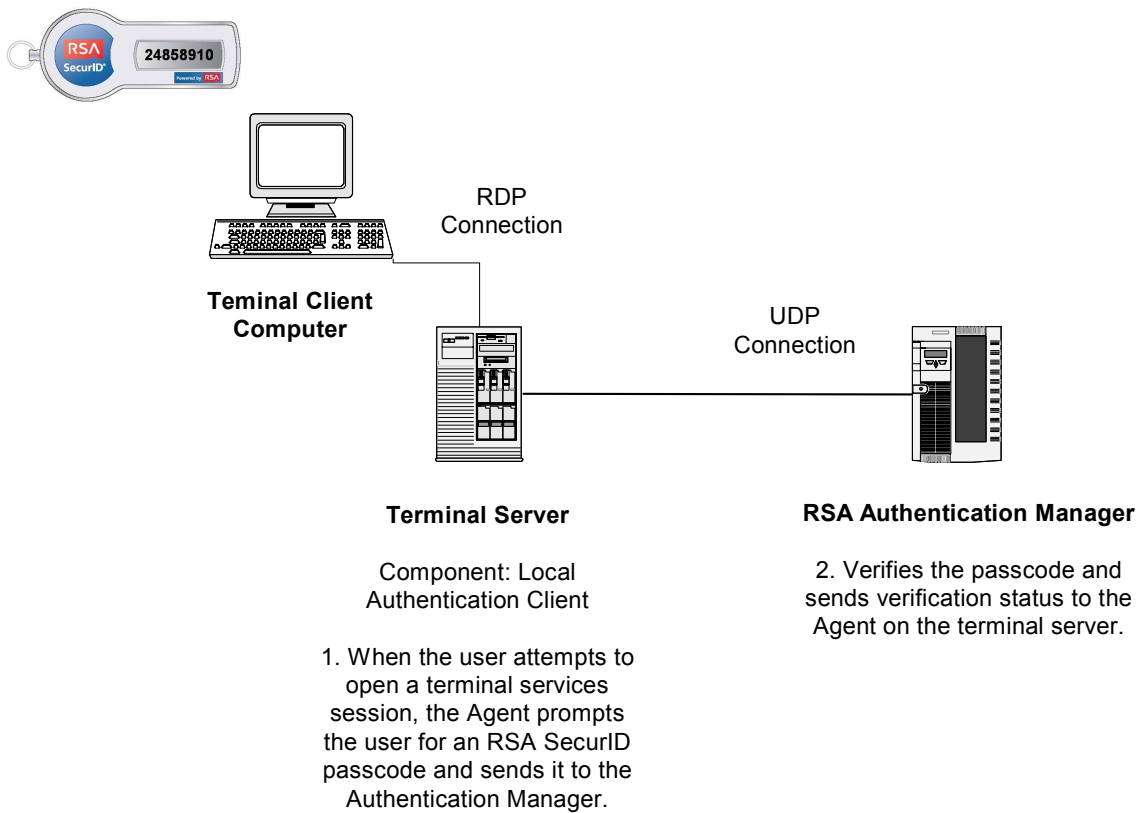
The following figure shows the setup for remote and wireless access within this scenario.



Terminal Services Sessions

Enabling local authentication on the terminal server requires sales representatives who use Windows Terminal Services for Siebel to authenticate with RSA SecurID passcodes before accessing customer account information. To facilitate this, you install the RSA Authentication Agent Local Authentication Client component on the terminal server.

The following figure shows the setup for terminal services users.



4

Planning Physical Deployment

Physical deployment is determining which software components to install and where to install them. This chapter discusses:

- The basic steps for deploying each authentication solution
- Which components you need to install and where you need to install them
- The options for installing the software

Planning What to Install and Where to Install It

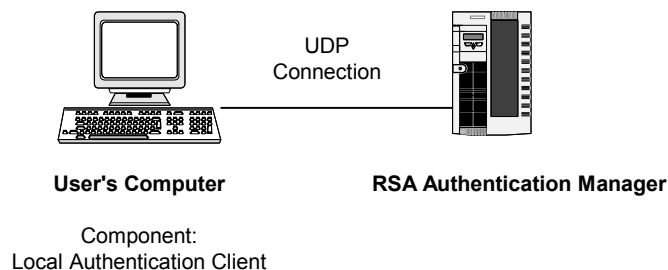
This section describes the basic steps for deploying each authentication solution manually. However, depending on the solution you want to deploy, you can save time by creating a silent installation. For information, see [“Planning an Installation Method”](#) on page 47.

Deploying Local Authentication

The following table tells what RSA Security components you need to install and where to install them.

Component	Location
RSA Authentication Manager	On a secure computer
Local Authentication Client component	Every computer you want to protect with RSA SecurID

The following figure shows the setup for local authentication.



The following table summarizes the basic steps to deploy local authentication and shows where in the *Installation and Administration Guide* to find more information.

Deployment Steps	Location of More Information in the <i>Installation and Administration Guide</i>
1. Install and set up RSA Authentication Manager 6.1.	The chapter “Requirements and Preparations”
2. Create Microsoft Windows challenge groups.	“Create Groups of Users to Challenge With RSA SecurID” in the chapter “Requirements and Preparations”
3. Install the Local Authentication Client component on every computer you want to protect.	The chapter “Installing RSA Authentication Agent 6.1 for Microsoft Windows”
4. If you are using Dynamic Host Configuration Protocol (DHCP) to assign IP addresses, install and configure the Automated Agent Host Registration and Update utility on the protected computers.	The appendix “Automated Registration of Agent Hosts in the RSA Authentication Manager Database”
5. Start RSA Security Center.	“Step 4: Start RSA Security Center” in the chapter “Installing RSA Authentication Agent 6.1 for Microsoft Windows”
6. Verify the status of the authentication environment and perform a test authentication.	“Step 5: Verify the Status of the Authentication Environment” and “Step 6: Test Authentication” in the chapter “Installing RSA Authentication Agent 6.1 for Microsoft Windows”
7. Configure local authentication.	The chapter “Configuring Local Authentication”

Deploying Remote Authentication

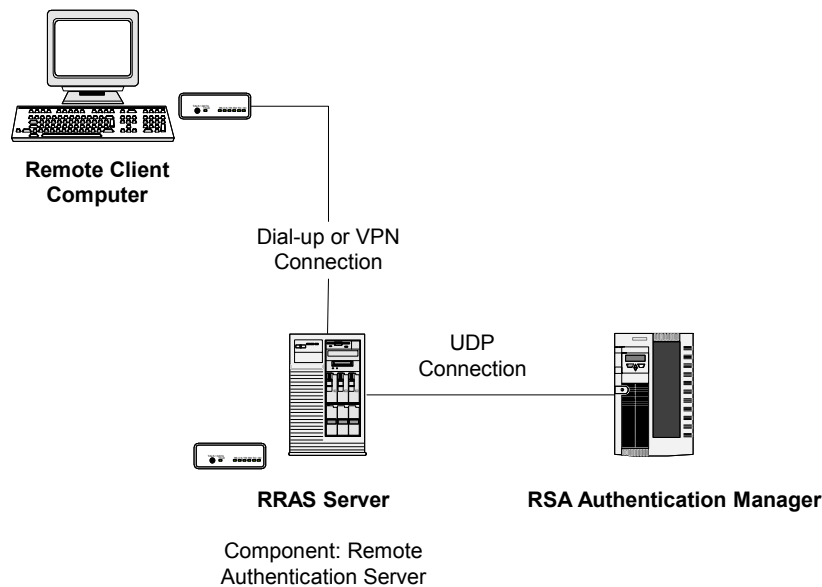
The type of authentication environment you have, as well as the remote authentication solution you want to deploy, determines which RSA Authentication Agent components you need to install. The type of environment you have is determined by whether or not you use EAP and which RADIUS server you use. You can use either Microsoft IAS RADIUS Server or RSA RADIUS Server. RSA RADIUS Server is shipped with RSA Authentication Manager and eliminates the need for the RSA Authentication Agent on the remote server. Both the Microsoft IAS RADIUS Server solution and RSA RADIUS Server solution support RSA Security EAP Protected One Time Password (OTP) (EAP 32). Additionally, both continue support for RSA Security EAP (EAP 15).

The following illustrations show the setup for these remote authentication solutions:

- Without EAP
- EAP without a RADIUS server
- EAP using Microsoft IAS RADIUS Server
- EAP using RSA RADIUS Server

Deploying Remote Authentication Without EAP

The following figure shows the setup for this environment.



The following table tells what RSA Security components you need to install and where to install them.

Component	Location
RSA Authentication Manager	On a secure computer
Remote Authentication Server component	RRAS server

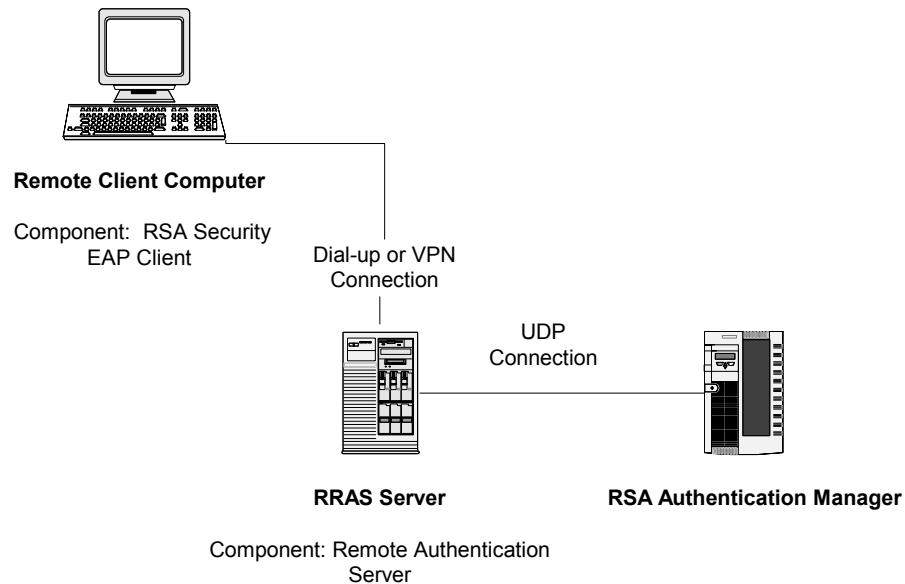
You may want to use this method instead of the method that incorporates EAP because this method does not require you to install software on client computers.

The following table summarizes the basic steps to deploy this remote authentication solution and shows where in the *Installation and Administration Guide* to find more information.

Deployment Steps	Location of More Information in the <i>Installation and Administration Guide</i>
1. Install and set up RSA Authentication Manager 6.1.	The chapter “Requirements and Preparations”
2. Create Microsoft Windows challenge groups.	“Create Groups of Users to Challenge With RSA SecurID” in the chapter “Requirements and Preparations”
3. Install the Remote Authentication Server component on the RRAS server.	The chapter “Installing RSA Authentication Agent 6.1 for Microsoft Windows.”
4. Start RSA Security Center.	“Step 4: Start RSA Security Center” in the chapter “Installing RSA Authentication Agent 6.1 for Microsoft Windows”
5. Verify the status of the authentication environment and perform a test authentication.	“Step 5: Verify the Status of the Authentication Environment” and “Step 6: Test Authentication” in the chapter “Installing RSA Authentication Agent 6.1 for Microsoft Windows”
6. Configure the RSA Authentication Agent on the RRAS server.	“Deploying Remote Authentication Without EAP” in the chapter “Configuring Remote Authentication”

Deploying Remote Authentication Using EAP Without a RADIUS Server

The following figure shows the setup for this environment.



The following table tells what RSA Security components you need to install and where to install them.

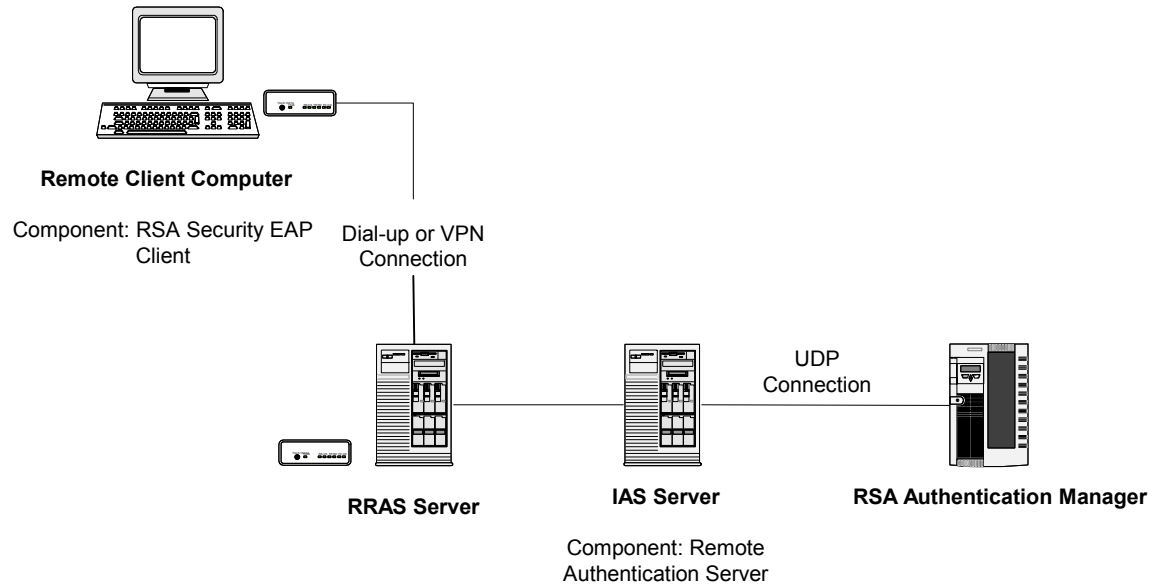
Component	Location
RSA Authentication Manager 6.1	On a secure computer
Remote Authentication Server component	On the RRAS server
RSA Security EAP client component	Every client computer you want to protect with RSA SecurID

The following table summarizes the basic steps to deploy this remote authentication solution and shows where in the *Installation and Administration Guide* to find more information.

Deployment Steps	Location of More Information in the <i>Installation and Administration Guide</i>
1. Install and set up RSA Authentication Manager 6.1.	The chapter “Requirements and Preparations”
2. Create access groups in Microsoft Active Directory.	“Deploying Remote Authentication Using EAP Without RADIUS” in the chapter “Configuring Remote Authentication”
3. Install the Remote Authentication Server component on the RRAS server.	The chapter “Installing RSA Authentication Agent 6.1 for Microsoft Windows.”
4. Start RSA Security Center.	“Step 4: Start RSA Security Center” in the chapter “Installing RSA Authentication Agent 6.1 for Microsoft Windows”
5. Verify the status of the authentication environment and perform a test authentication.	“Step 5: Verify the Status of the Authentication Environment” and “Step 6: Test Authentication” in the chapter “Installing RSA Authentication Agent 6.1 for Microsoft Windows”
6. Configure the RRAS server for RSA Security EAP or RSA Security EAP - Protected OTP.	“Deploying Remote Authentication Using EAP Without RADIUS” in the chapter “Configuring Remote Authentication”
7. Install the RSA Security EAP Client component on each remote client computer.	The chapter “Installing RSA Authentication Agent 6.1 for Microsoft Windows
8. Configure remote client computers for EAP.	“Deploying Remote Authentication Using EAP Without RADIUS” in the chapter “Configuring Remote Authentication”
9. Configure the RSA Authentication Agent on the RRAS server.	“Deploying Remote Authentication Using EAP Without RADIUS” in the chapter “Configuring Remote Authentication”

Deploying Remote Authentication Using EAP With Microsoft IAS RADIUS Server

The following figure shows the setup for this environment.



The following table tells what RSA Security components you need to install and where to install them.

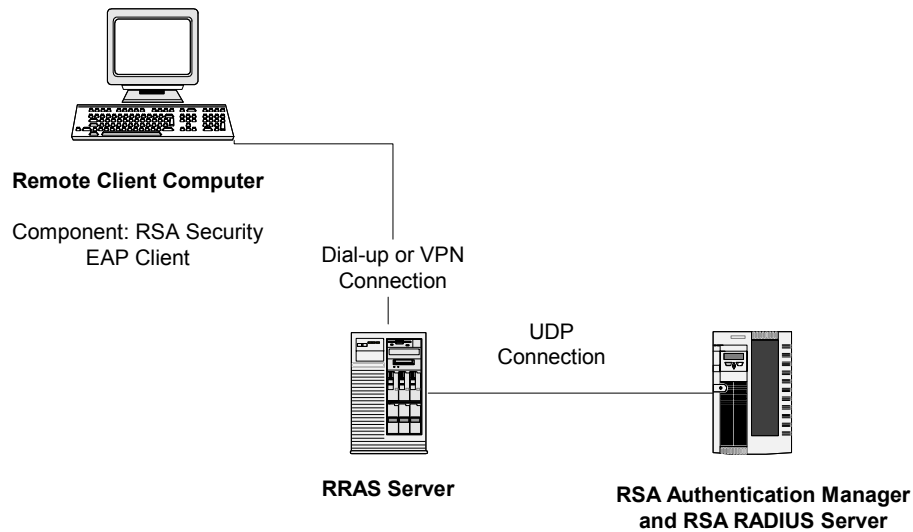
Component	Location
RSA Authentication Manager 6.1	On a secure computer
Remote Authentication Server component	Microsoft IAS server
RSA Security EAP Client component	Every remote client computer

The following table summarizes the basic steps to deploy this remote authentication solution and shows where in the *Installation and Administration Guide* to find more information.

Deployment Steps	Location of More Information in the <i>Installation and Administration Guide</i>
1. Install and set up RSA Authentication Manager 6.1.	The chapter “Requirements and Preparations”
2. Create access groups in Microsoft Active Directory.	“Deploying Remote Authentication Using EAP With Microsoft IAS RADIUS Server” in the chapter “Configuring Remote Authentication”
3. Configure the RRAS server for RADIUS.	“Deploying Remote Authentication Using EAP With Microsoft IAS RADIUS Server” in the chapter “Configuring Remote Authentication”
4. Install the Remote Authentication Server component on the Microsoft IAS server.	The chapter “Installing RSA Authentication Agent 6.1 for Microsoft Windows”
5. Start RSA Security Center.	“Step 4: Start RSA Security Center” in the chapter “Installing RSA Authentication Agent 6.1 for Microsoft Windows”
6. Verify the status of the authentication environment and perform a test authentication.	“Step 5: Verify the Status of the Authentication Environment” and “Step 6: Test Authentication” in the chapter “Installing RSA Authentication Agent 6.1 for Microsoft Windows”
7. Configure Microsoft IAS Server for RSA Security EAP - Protected OTP or RSA Security EAP.	“Deploying Remote Authentication Using EAP With Microsoft IAS RADIUS Server” in the chapter “Configuring Remote Authentication”
8. Install the RSA Security EAP Client component on each remote client computer.	The chapter “Installing RSA Authentication Agent 6.1 for Microsoft Windows”
9. Configure remote client computers for EAP.	“Deploying Remote Authentication Using EAP With Microsoft IAS RADIUS Server” in the chapter “Configuring Remote Authentication”
10. Configure the RSA Authentication Agent on the remote server.	“Deploying Remote Authentication Using EAP With Microsoft IAS RADIUS Server” in the chapter “Configuring Remote Authentication”

Deploying Remote Authentication Using EAP With RSA RADIUS Server

The following figure shows the setup for this environment.



The following table tells what RSA Security components you need to install and where to install them.

Component	Location
RSA Authentication Manager 6.1	On a secure computer
RSA RADIUS Server	On the same computer as the RSA Authentication Manager or on a separate computer
(Optional) Local Authentication Client	On the same computer as the RSA RADIUS Server
RSA Security EAP Client component	Every remote client computer

Note: Although EAP with RSA RADIUS Server does not require an Authentication Agent component on the RSA RADIUS Server Host, you may want to install 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” in the chapter “Configuring Advanced and Troubleshooting Settings” in the *Installation and Administration Guide*.

The following table summarizes the basic steps to deploy this remote authentication solution and shows where in the *Installation and Administration Guide* to find more information.

Deployment Steps	Location of More Information in the <i>Installation and Administration Guide</i>
1. Install and set up RSA Authentication Manager 6.1 with RSA RADIUS Server.	The chapter “Requirements and Preparations”
2. (Optional) Install the Local Authentication Client component on the RSA RADIUS Server computer and set the local authentication challenge to None .	“Managing the Node Secret on RSA RADIUS Server” in the chapter “Configuring Advanced and Troubleshooting Settings”
3. Configure the RSA RADIUS Server.	“Deploying Remote Authentication Using EAP With RSA RADIUS Server” in the chapter “Configuring Remote Authentication”
4. Install the RSA Security EAP Client component on each remote client computer.	The chapter “Installing RSA Authentication Agent 6.1 for Microsoft Windows”
5. Configure the RADIUS clients for RSA RADIUS Server.	“Deploying Remote Authentication Using EAP With RSA RADIUS Server” in the chapter “Configuring Remote Authentication”
6. Configure the client computers for EAP.	“Deploying Remote Authentication Using EAP With RSA RADIUS Server” in the chapter “Configuring Remote Authentication”

Deploying Wireless Authentication

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

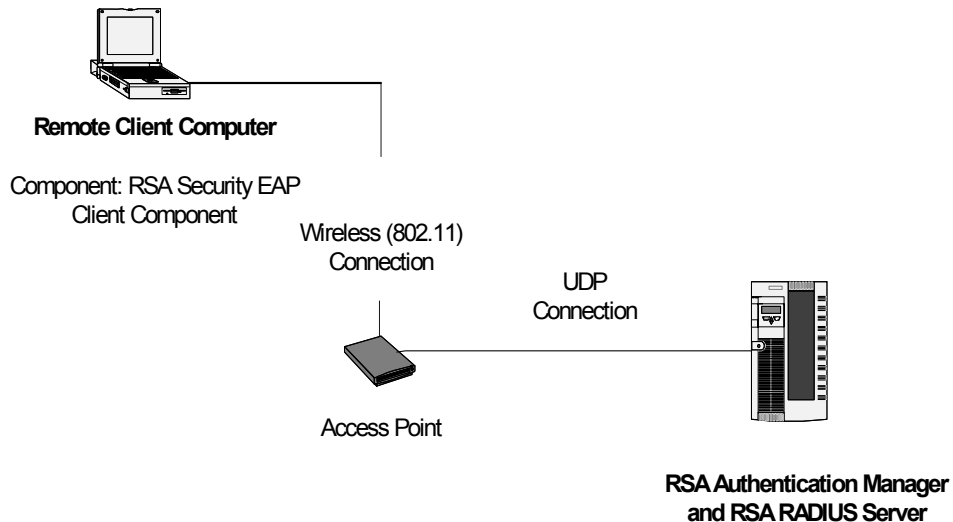
- RSA Security EAP - Protected OTP
- PEAP

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

Deploying RSA Security EAP - Protected OTP With RSA RADIUS Server

This section summarizes the setup for wireless authentication using RSA Security EAP - Protected OTP with RSA RADIUS Server. However, you can set up wireless authentication using Microsoft IAS RADIUS Server. For information, see “Deploying Wireless Authentication With RSA Security EAP - Protected OTP” in the chapter “Configuring Wireless Authentication” in the *Installation and Administration Guide*.

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



The following table tells what RSA Security components you need to install and where to install them.

Component	Location
RSA Authentication Manager 6.1	On a secure computer
RSA RADIUS Server	On the same computer as the RSA Authentication Manager or on a separate computer
(Optional) Local Authentication Client	On the same computer as the RSA RADIUS Server
RSA Security EAP Client component	Every remote client computer

Note: Although RSA Security EAP - Protected OTP with RSA RADIUS Server does not require an Authentication Agent component on the RSA RADIUS Server Host, you may want to install 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” in the chapter “Configuring Advanced and Troubleshooting Settings” in the *Installation and Administration Guide*.

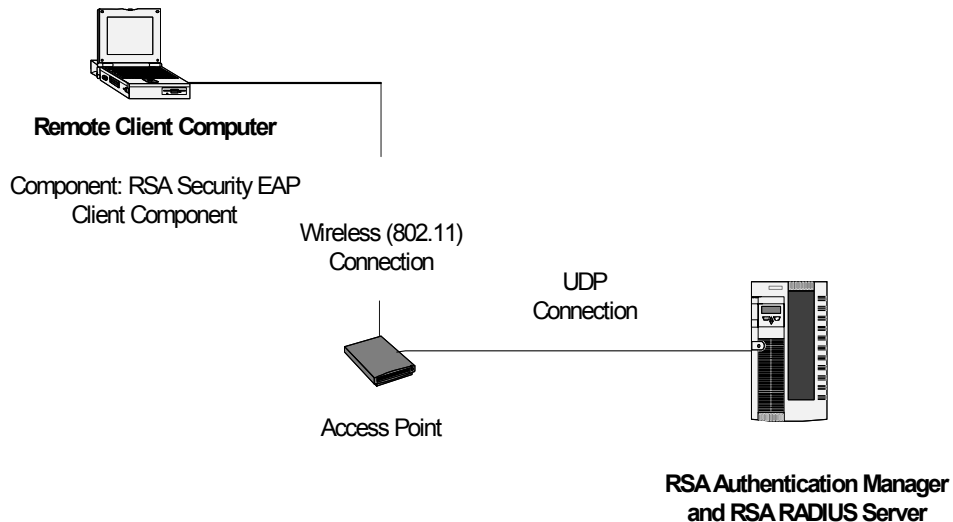
The following table summarizes the basic steps to deploy this remote authentication solution and shows where in the *Installation and Administration Guide* to find more information.

Deployment Steps	Location of More Information in the <i>Installation and Administration Guide</i>
1. Install and set up RSA Authentication Manager 6.1 and RSA RADIUS Server.	The chapter “Requirements and Preparations”
2. (Optional) Install the Local Authentication Client component on the RSA RADIUS Server computer and set the local authentication challenge to None .	“Managing the Node Secret on RSA RADIUS Server” in the chapter “Configuring Advanced and Troubleshooting Settings”
3. Configure the RSA RADIUS Server.	“Deploying RSA Security EAP - Protected OTP With RSA RADIUS Server” in the chapter “Configuring Wireless Authentication”
4. Set up the wireless LAN environment.	“Deploying RSA Security EAP - Protected OTP With RSA RADIUS Server” in the chapter “Configuring Wireless Authentication”
5. Install the RSA Security EAP Client component on each remote client computer.	The chapter “Installing RSA Authentication Agent 6.1 for Microsoft Windows”
6. Configure the client computers.	“Deploying RSA Security EAP - Protected OTP With RSA RADIUS Server” in the chapter “Configuring Wireless Authentication”

Deploying PEAP With RSA RADIUS Server

This section summarizes the setup for wireless authentication using PEAP and RSA RADIUS Server. However, you can set up wireless authentication using Microsoft IAS RADIUS Server. For information, see “Deploying Wireless Authentication With PEAP” in the chapter “Configuring Wireless Authentication” in the *Installation and Administration Guide*.

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



The following table tells what RSA Security components you need to install and where to install them.

Component	Location
RSA Authentication Manager 6.1	On a secure computer
RSA RADIUS Server	On the same computer as the RSA Authentication Manager or on a separate computer
(Optional) Local Authentication Client	On the same computer as the RSA RADIUS Server
RSA Security EAP Client component	Every remote client computer

Note: Although PEAP with RSA RADIUS Server does not require an Authentication Agent component on the RSA RADIUS Server Host, you may want to install 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” in the chapter “Configuring Advanced and Troubleshooting Settings” in the *Installation and Administration Guide*.

The following table summarizes the basic steps to deploy this remote authentication solution and shows where in the *Installation and Administration Guide* to find more information.

Deployment Steps	Location of More Information in the <i>Installation and Administration Guide</i>
1. Install and set up RSA Authentication Manager 6.1 and RSA RADIUS Server.	The chapter “Requirements and Preparations”
2. (Optional) Install the Local Authentication Client component on the RSA RADIUS Server computer and set the local authentication challenge to None .	“Managing the Node Secret on RSA RADIUS Server” in the chapter “Configuring Advanced and Troubleshooting Settings”
3. Obtain certificates for wireless authentication.	“Deploying RSA Security EAP - Protected OTP With RSA RADIUS Server” in the chapter “Configuring Wireless Authentication”
4. Configure the RSA RADIUS Server.	“Deploying Wireless Authentication With PEAP” in the chapter “Configuring Wireless Authentication”
5. Set up the wireless LAN environment.	“Deploying Wireless Authentication With PEAP” in the chapter “Configuring Wireless Authentication”
6. Install the RSA Security EAP Client component on each remote client computer.	The chapter “Installing RSA Authentication Agent 6.1 for Microsoft Windows”
7. Configure the remote client computers.	“Deploying Wireless Authentication With PEAP” in the chapter “Configuring Wireless Authentication”

Planning an Installation Method

For some solutions (for example, local authentication), you must install an Agent component on every user's computer. Depending on the number of computers in your system, this task can be time consuming. Therefore, RSA Security provides two ways to install RSA Authentication Agent 6.1 for Microsoft Windows:

- Interactive installation
- Silent installation

Interactive Installation

You perform an interactive installation by running the installation wizard on each individual client computer and providing settings information in response to the installation prompts. There are two types of interactive installations:

Typical. Installs the Local Authentication Client component.

Custom. Installs any or all of the following components, according to which components you select:

- Local Authentication Client component with or without the Automated Agent Host Registration Utility
- Remote Authentication Server component
- RSA Security EAP Client

Silent Installation

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 Local 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 silent mode installation:

1. Use files provided by RSA Security to create a network installation package.
2. Copy the installation package to a shared location on the network or domain controller.
3. Edit the installation package, if necessary, to customize the installation.

By default, the installation package installs the Local Authentication Client component. However, you can edit the installation package to silently install any of the Authentication Agent components.

For complete instructions, see "Creating a Silent Mode Installation" in the chapter "Installing RSA Authentication Agent 6.1 for Microsoft Windows" in the *Installation and Administration Guide*.

Index

A

authentication process, 8

B

browser support, 12

C

challenge options, 8

D

deploying
 local authentication, 33
 remote authentication, 35
deployment, 11
 logical, 15
 physical, 33
disk space requirements, 14

F

features, 7

H

hardware requirements, 13

I

installation
 interactive, 47
 silent, 47
interactive installation, 47
introduction, 7

L

local authentication
 deploying, 33
 overview, 15
logical deployment, 15

M

Microsoft ActiveSync
 support for, 13

O

offline authentication, 20

P

password integration, 20
physical deployment, 33
planning
 authentication solutions, 15
 logical deployment, 15
 reserve access methods, 21
 which users to challenge, 19
platforms supported by RSA Authentication
 Manager, 13
platforms, supported, 11
protection, resources, 7

R

remote authentication
 deploying, 35
 overview, 16
requirements
 disk space, 14
reserve access methods, 21
resource protection, 7

S

scenarios
 large company, 28
 small company, 25
silent installation, 47
supported platforms, 11

W

WAP
 support for, 12