RSA SecurID Ready Implementation Guide

Last Modified: 1/27/03

1. Partner Information

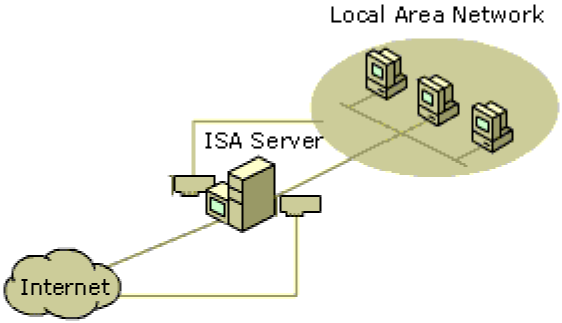
Partner Name	Microsoft Corporation
Web Site	http://www.microsoft.com/
Product Name	Internet Security and Acceleration (ISA) Server
Version & Platform	2000
Product Description	Microsoft® Internet Security and Acceleration (ISA) Server 2000 is an extensible enterprise firewall and Web cache server that integrates with the Microsoft Windows® 2000 operating system for policy-based security as well as accelerating and managing internetworking. Sophisticated management tools simplify policy definition, traffic routing, server publishing, and monitoring. ISA Server builds on Windows 2000 security, directory, virtual private networking (VPN), and bandwidth control. Whether deployed as separate firewall and cache servers or in integrated mode, ISA Server can be used to enhance network security, enforce consistent Internet usage policy, accelerate Internet access, and maximize employee productivity for organizations of all sizes.
Product Category	VPN

2. Contact Information

	Sales	Support
Phone	(781) 487.6400	(800) 936.4900
Web	www.microsoft.com/worldwide/	support.microsoft.com/

3. Solution Summary

Feature	Details
Authentication Methods Supported	Native RSA SecurID
RSA ACE/Agent Library Version	N/A, EAP module only
RSA ACE 5 Locking	Yes
Replica RSA ACE/Server Support	Full Replica Support
Secondary RADIUS/TACACS+ Server Support	No
Location of Node Secret on Client	In Registry
RSA ACE/Server Agent Host Type	Net OS
RSA SecurID User Specification	Designated users
RSA SecurID Protection of Administrators	No



4. Product Requirements

- ***Hardware requirements***

Component Name:	
CPU make/speed required	300 MHz or higher Pentium II-compatible processor
Memory	256 MB of RAM
HD space	20 MB of available hard-disk space formatted with the NTFS file system
Other	A Windows 2000-compatible network adapter for communicating with the internal network

- ***Software requirements***

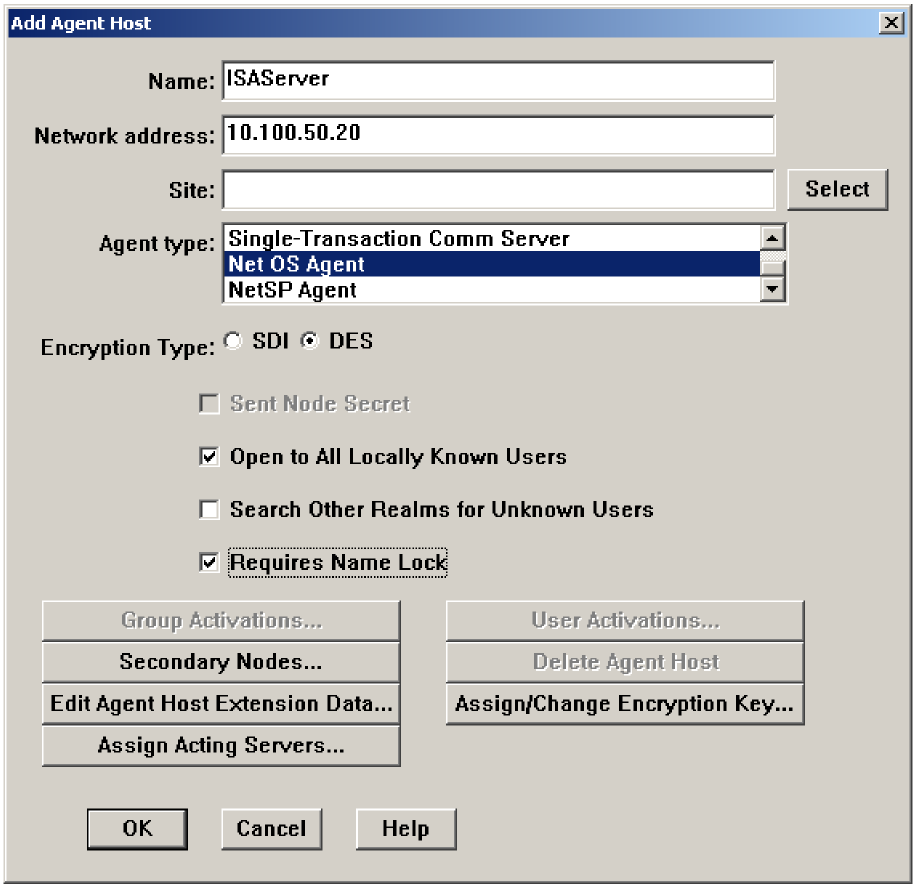
Component Name:	
Operating System	**Version (Patch-level)**
Windows 2000 Server	Service Pack 3 or later
Windows 2000 Advanced Server	Service Pack 3 or later
Windows 2000 Datacenter Server	Service Pack 3 or later
ISA Server 2000	Service Pack 1 and Feature Pack 1

5. RSA ACE/Server configuration

Perform the following steps to set up the ISA Server as an Agent Host within the RSA ACE/Server's database.

- On the RSA ACE/Server computer, click **Start**, click **Programs**, click **RSA ACE/Server**, and then click **Database Administration - Host Mode**.

- On the **Agent Host** menu, click **Add Agent Host...**.



Add Agent Host

Name: ISAServer

Network address: 10.100.50.20

Site:

Agent type: Single-Transaction Comm Server / **Net OS Agent** / NetSP Agent

Encryption Type: ○ SDI ● DES

□ Sent Node Secret

☑ Open to All Locally Known Users

□ Search Other Realms for Unknown Users

☑ Requires Name Lock

- In **Name**, type the name of the ISA Server computer.
- In **Network address**, type the IP address of the ISA Server computer.
- Under **Secondary Nodes**, define all hostname/IP addresses that resolve to the ISA Server machine.

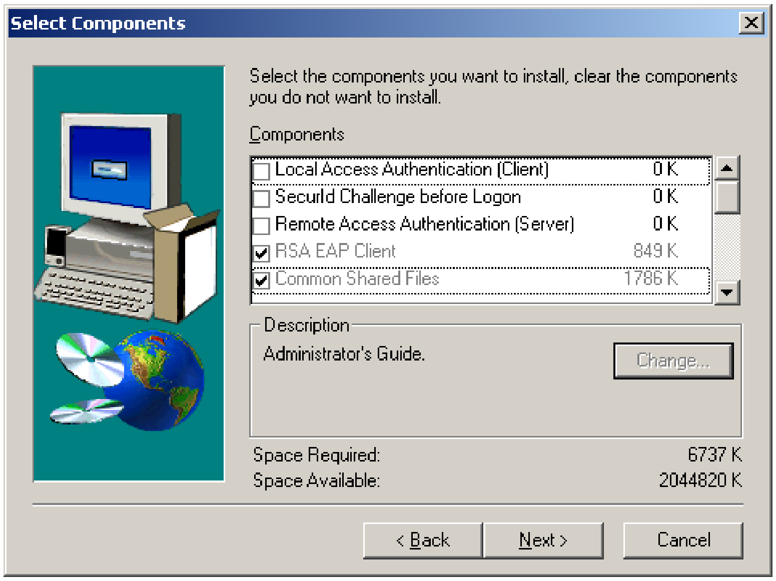
<u>Note</u>: It is important that all hostname and IP addresses resolve to each other. Please reference the RSA ACE/Server documentation for detailed info on this and other configuration parameters within this screen. Subsequently, you can also select the 'Help' button at the bottom of the screen.

6. Partner RSA ACE/Agent configuration

This section provides instructions for integrating the partners' product with RSA SecurID. This document is not intended to suggest optimum installations or configurations. It is assumed that the reader has both working knowledge of the two products to perform the tasks outlined in this section and access to the documentation for both in order to install the required software components. All products/components need to be installed and working prior to this integration. Perform the necessary tests to confirm that this is true before proceeding.

Server configuration:

1. **Install RSA EAP Client.** During the install procedure for RSA ACE/Agent 5.5 for Windows, you have the option to choose the components you want. Check the box to the left of 'RSA EAP Client'**. (**'Common Shared Files' are selected by default) The install process will also prompt you for the location of the sdconf.rec file located on the RSA ACE/Server (ace\data) and will copy it locally (winnt\system32).



Select Components

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

Components

☐ Local Access Authentication (Client)	0 K
☐ SecurId Challenge before Logon	0 K
☐ Remote Access Authentication (Server)	0 K
☑ RSA EAP Client	849 K
☑ Common Shared Files	1786 K

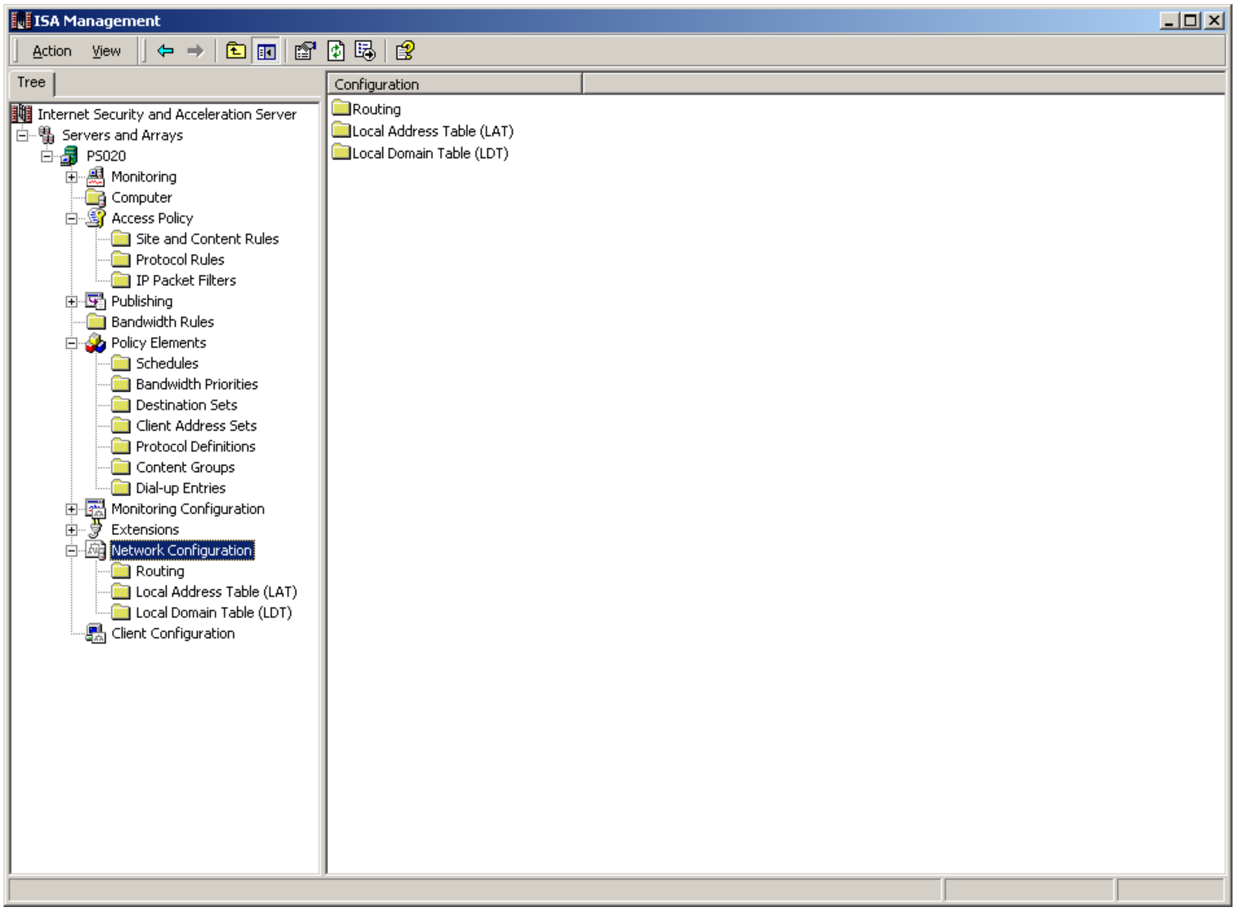
Description

Administrator's Guide.

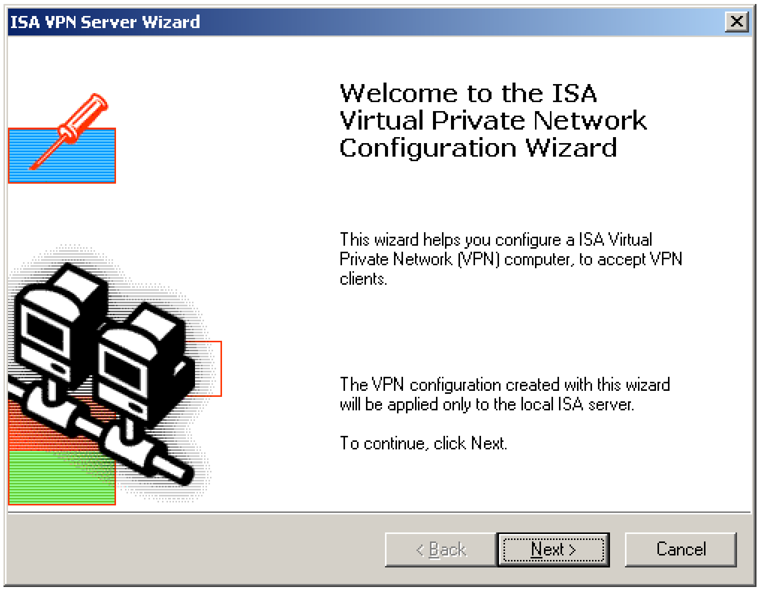
Space Required: 6737 K

Space Available: 2044820 K

2. **Configure ISA VPN Server**. From the ISA Management MMC, right click Network Configuration > Allow VPN client connections.



a. From the initial 'ISA VPN Server Wizard' window, click 'Next'.



ISA VPN Server Wizard

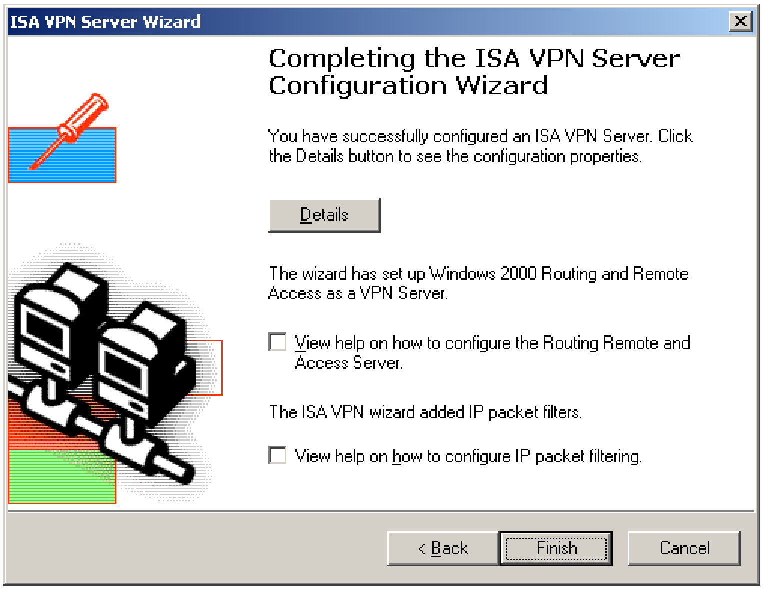
Welcome to the ISA Virtual Private Network Configuration Wizard

This wizard helps you configure a ISA Virtual Private Network (VPN) computer, to accept VPN clients.

The VPN configuration created with this wizard will be applied only to the local ISA server.

To continue, click Next.

b. Then click 'Finish'.



ISA VPN Server Wizard

Completing the ISA VPN Server Configuration Wizard

You have successfully configured an ISA VPN Server. Click the Details button to see the configuration properties.

The wizard has set up Windows 2000 Routing and Remote Access as a VPN Server.

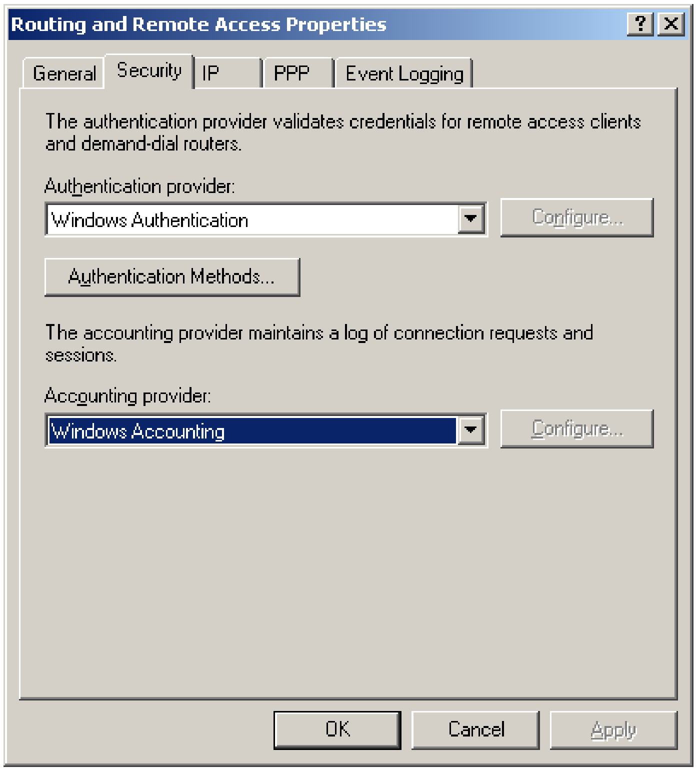
□ View help on how to configure the Routing Remote and Access Server.

The ISA VPN wizard added IP packet filters.

□ View help on how to configure IP packet filtering.

3. **Configure the Routing and Remote Access service to use EAP**.

   a. Right-click the RRAS server <servername> and pick **Properties**, and choose the **Security** tab. Under **Authentication methods,** check the **Extensible authentication protocol** box.

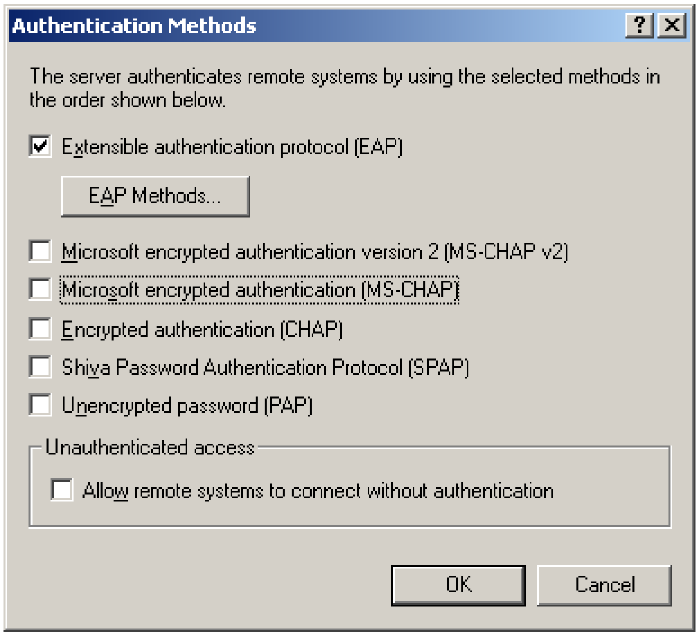


The authentication provider validates credentials for remote access clients and demand-dial routers.

Authentication provider: Windows Authentication

The accounting provider maintains a log of connection requests and sessions.

Accounting provider: Windows Accounting



The server authenticates remote systems by using the selected methods in the order shown below.

☑ Extensible authentication protocol (EAP)

☐ Microsoft encrypted authentication version 2 (MS-CHAP v2)

☐ Microsoft encrypted authentication (MS-CHAP)

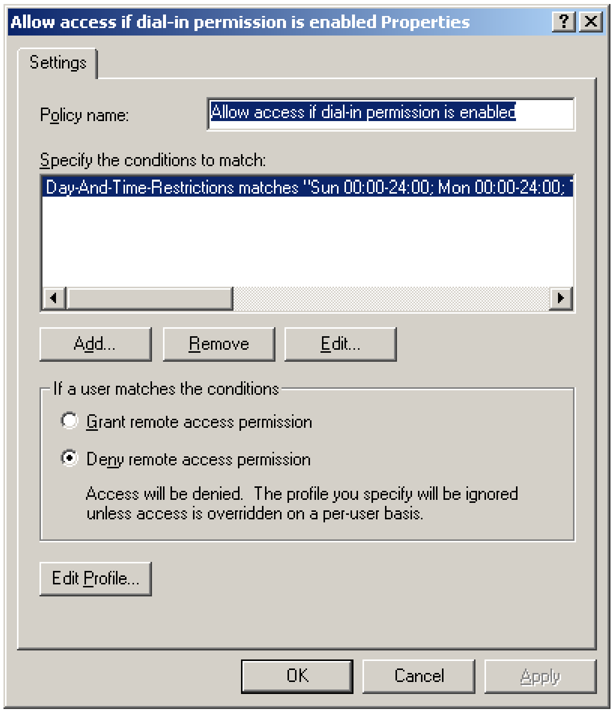
☐ Encrypted authentication (CHAP)

☐ Shiva Password Authentication Protocol (SPAP)

☐ Unencrypted password (PAP)

☐ Allow remote systems to connect without authentication

b. Then, also in the **RRAS** window, click on **Remote Access Policies**, right-click the **Allow access if dial-in permission is enabled** entry, and click **properties.** Check the **Extensible Authentication Protocol** box, and choose **RSA Security EAP** in the drop-down menu. Click **Ok.**



Allow access if dial-in permission is enabled Properties

Settings

Policy name: Allow access if dial-in permission is enabled

Specify the conditions to match:

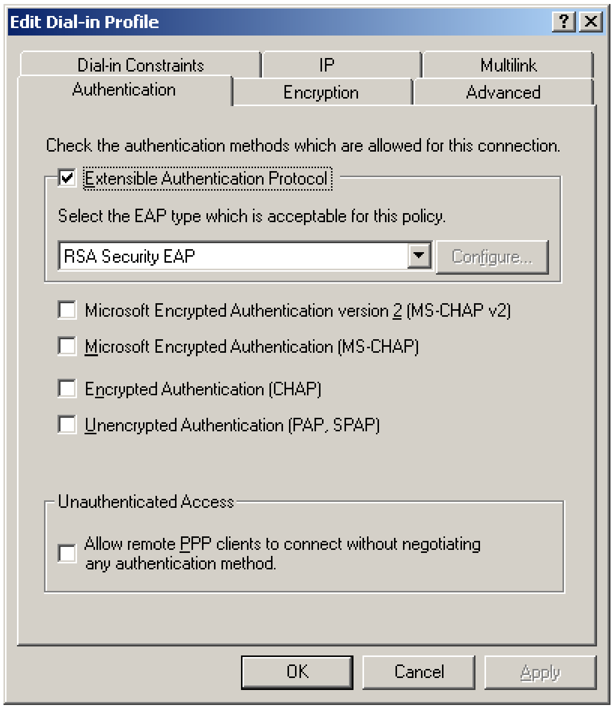
Day-And-Time-Restrictions matches "Sun 00:00-24:00; Mon 00:00-24:00;

If a user matches the conditions

○ Grant remote access permission

● Deny remote access permission

Access will be denied. The profile you specify will be ignored unless access is overridden on a per-user basis.



Edit Dial-in Profile

Dial-in Constraints | IP | Multilink | Authentication | Encryption | Advanced

Check the authentication methods which are allowed for this connection.

☑ Extensible Authentication Protocol

Select the EAP type which is acceptable for this policy.

RSA Security EAP

□ Microsoft Encrypted Authentication version 2 (MS-CHAP v2)

□ Microsoft Encrypted Authentication (MS-CHAP)

□ Encrypted Authentication (CHAP)

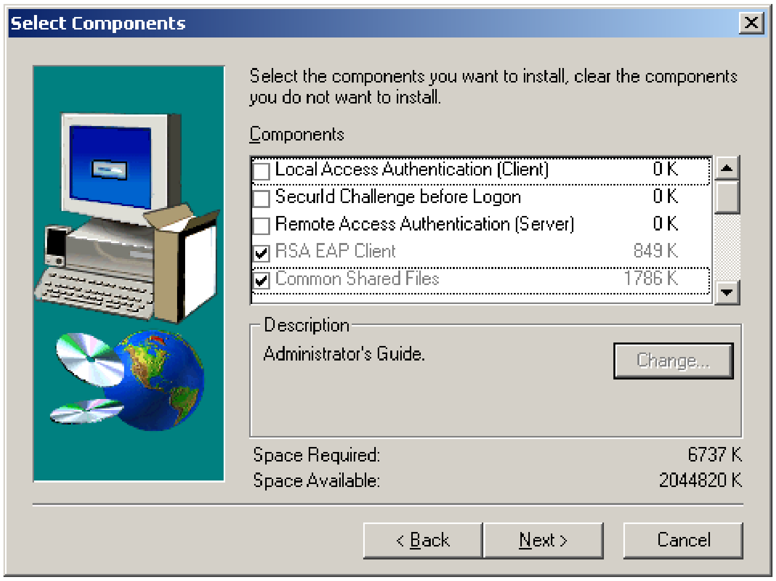
□ Unencrypted Authentication (PAP, SPAP)

Unauthenticated Access

□ Allow remote PPP clients to connect without negotiating any authentication method.

Client configuration:

1. **Install RSA EAP Client.** During the install procedure for RSA ACE/Agent 5.5 for Windows, you have the option to choose the components you want. Check the box to the left of 'RSA EAP Client'**.** **(**'Common Shared Files' are selected by default) The install process will also prompt you for the location of the sdconf.rec file located on the RSA ACE/Server (ace\data) and will copy it locally (winnt\system32).



Select Components

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

Components

☐ Local Access Authentication (Client)	0 K
☐ SecurId Challenge before Logon	0 K
☐ Remote Access Authentication (Server)	0 K
☑ RSA EAP Client	849 K
☑ Common Shared Files	1786 K

Description

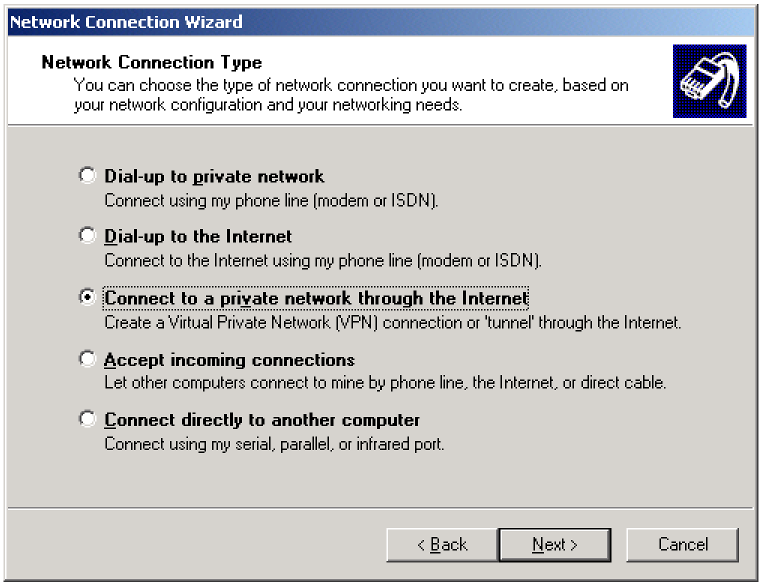
Administrator's Guide.

Space Required: 6737 K

Space Available: 2044820 K

2. **Configure VPN connection**.

   a. **Right**-click My Network Places, choose properties, and double-click on **Make New Connection**. Choose **Connect to a private network through the Internet,** and click **Next.** The next box offers the chance to set up the client to automatically dial the connection before establishing the VPN connection. Choose as appropriate.



Network Connection Wizard

Network Connection Type

You can choose the type of network connection you want to create, based on your network configuration and your networking needs.

○ Dial-up to private network
Connect using my phone line (modem or ISDN).

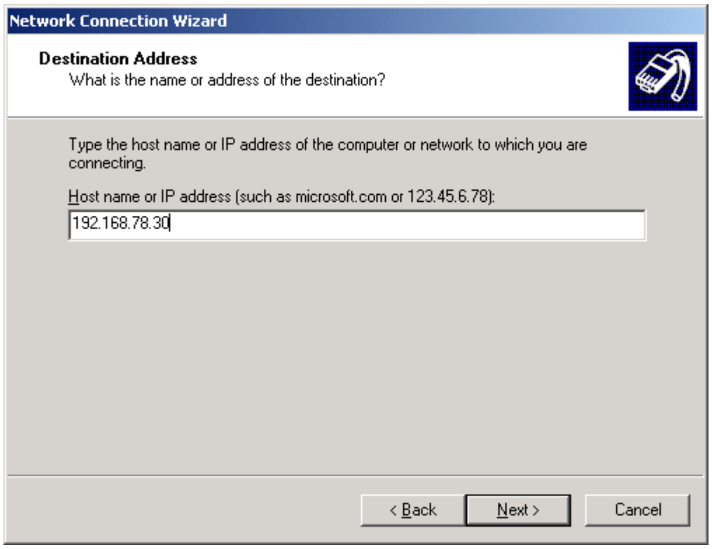
○ Dial-up to the Internet
Connect to the Internet using my phone line (modem or ISDN).

● Connect to a private network through the Internet
Create a Virtual Private Network (VPN) connection or 'tunnel' through the Internet.

○ Accept incoming connections
Let other computers connect to mine by phone line, the Internet, or direct cable.

○ Connect directly to another computer
Connect using my serial, parallel, or infrared port.

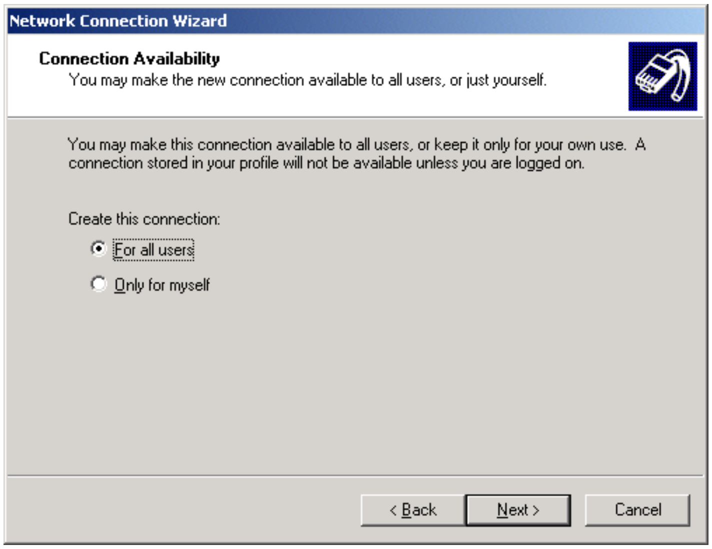
b. **Enter** the IP address of the VPN server. Click **Next.** Now, choose the availability of the VPN client (all users or only the current user)


Network Connection Wizard

Destination Address
What is the name or address of the destination?

Type the host name or IP address of the computer or network to which you are connecting.

Host name or IP address (such as microsoft.com or 123.45.6.78):
192.168.78.30


Network Connection Wizard

Connection Availability
You may make the new connection available to all users, or just yourself.

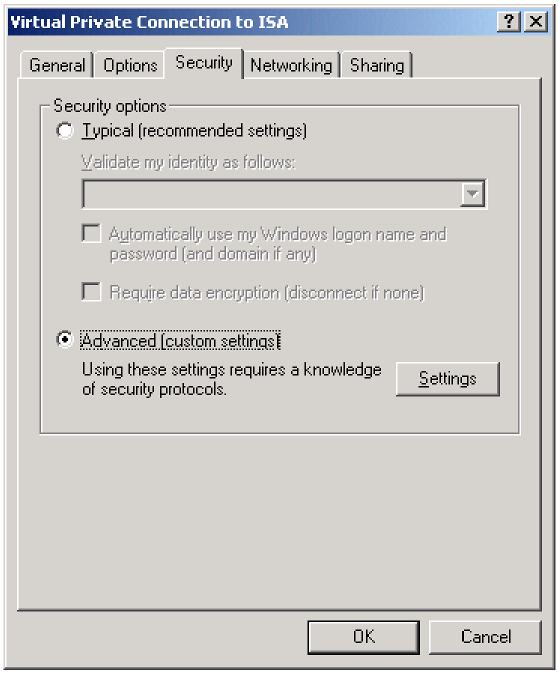
You may make this connection available to all users, or keep it only for your own use. A connection stored in your profile will not be available unless you are logged on.

Create this connection:

● For all users

○ Only for myself

4. **Configure VPN Client to use EAP.** In the **Properties** screen of the VPN connection, choose **Advanced (custom settings).** Then in the **Advanced Security Settings,** choose **Require encryption**, and **RSA Security EAP.** Now, simply double-click on the VPN connection to initiate the tunnel.



Virtual Private Connection to ISA

Security options

○ Typical (recommended settings)

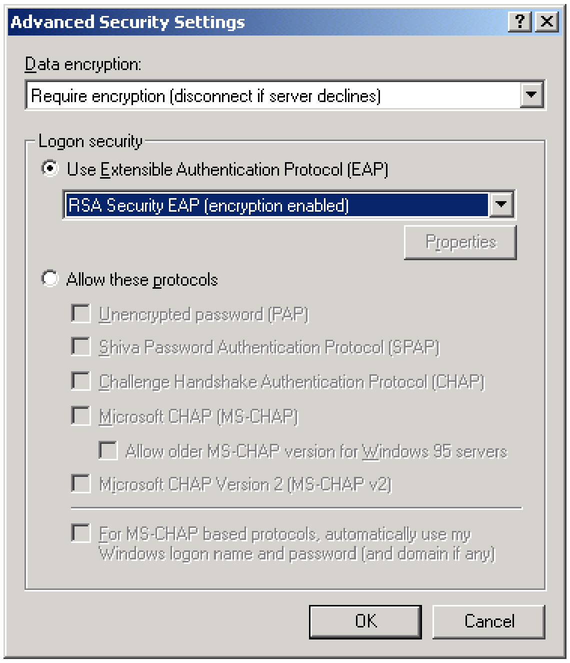
Validate my identity as follows:

□ Automatically use my Windows logon name and password (and domain if any)

□ Require data encryption (disconnect if none)

● Advanced (custom settings)

Using these settings requires a knowledge of security protocols.



Advanced Security Settings

Data encryption: Require encryption (disconnect if server declines)

Logon security

● Use Extensible Authentication Protocol (EAP)

RSA Security EAP (encryption enabled)

○ Allow these protocols

□ Unencrypted password (PAP)

□ Shiva Password Authentication Protocol (SPAP)

□ Challenge Handshake Authentication Protocol (CHAP)

□ Microsoft CHAP (MS-CHAP)

□ Allow older MS-CHAP version for Windows 95 servers

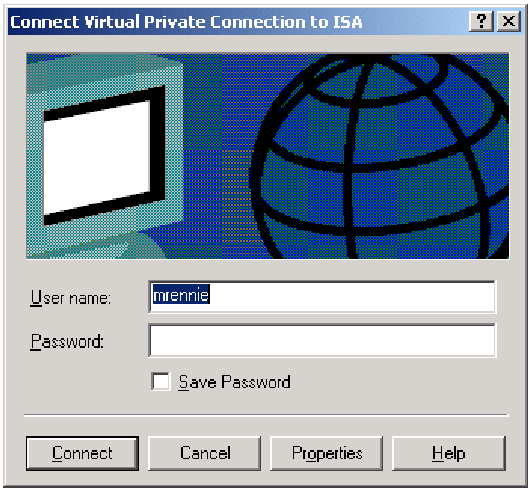
□ Microsoft CHAP Version 2 (MS-CHAP v2)

□ For MS-CHAP based protocols, automatically use my Windows logon name and password (and domain if any)

Note: VPN users need to be a member of the Dial-in users group

Sample authentication prompts:

- First prompt is from Windows. User name is the only info needed here.



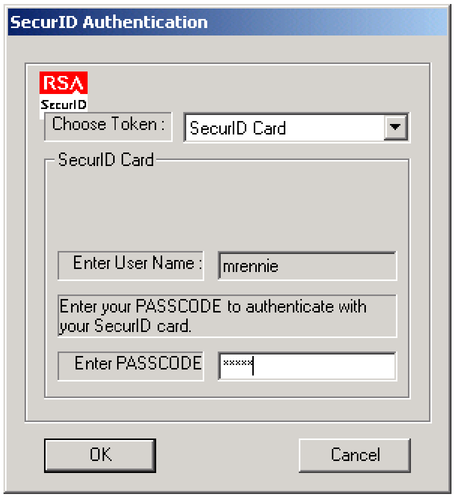
Connect Virtual Private Connection to ISA

User name: mrennie

Password:

□ Save Password

- Second prompt is from the RSA ACE/Server. The username is taken from the previous prompt.



SecurID Authentication

Choose Token : SecurID Card

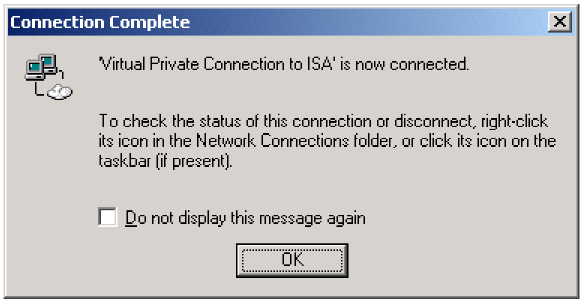
SecurID Card

Enter User Name : mrennie

Enter your PASSCODE to authenticate with your SecurID card.

Enter PASSCODE *****

- Connection Complete!



Connection Complete

'Virtual Private Connection to ISA' is now connected.

To check the status of this connection or disconnect, right-click its icon in the Network Connections folder, or click its icon on the taskbar (if present).

□ Do not display this message again

7. Certification Checklist

Date Tested: 01/28/2003

Product	Tested Version
RSA ACE/Server	5.03
RSA ACE/Agent	5.5 (EAP Client Only)
ISA Server	2000 (SP1) & (FP1)

Test	ACE	RADIUS
1st time auth. (node secret creation)	Pass	N/A
New PIN mode:		
System-generated		
Non-PINPAD token	Pass	N/A
PINPAD token	Pass	N/A
User-defined (4-8 alphanumeric)		
Non-PINPAD token	Pass	N/A
Password	Pass	N/A
User-defined (5-7 numeric)		
Non-PINPAD token	Pass	N/A
PINPAD token	Pass	N/A
SoftID token	Pass	N/A
Deny 4 digit PIN	Pass	N/A
Deny Alphanumeric	Pass	N/A
User-selectable		
Non-PINPAD token	Pass	N/A
PINPAD token	Pass	N/A
PASSCODE		
16 Digit PASSCODE	Pass	N/A
4 Digit Password	Pass	N/A
Next Tokencode mode		
Non-PINPAD token	Pass	N/A
PINPAD token	Pass	N/A
Failover	Pass	N/A
User Lock Test (RSA ACE Lock Function)	Pass	N/A
No RSA ACE/Server	Pass	N/A

MPR N/A (N/A=Non-available function)

8. Known Issues

- The VPN functionality of ISA Server with RSA SecurID documented in this Guide has been tested to work in tandem with the native RSA SecurID functionality implemented by Microsoft in Feature Pack 1 which allows for RSA SecurID protected of web servers via Web Publishing rules.