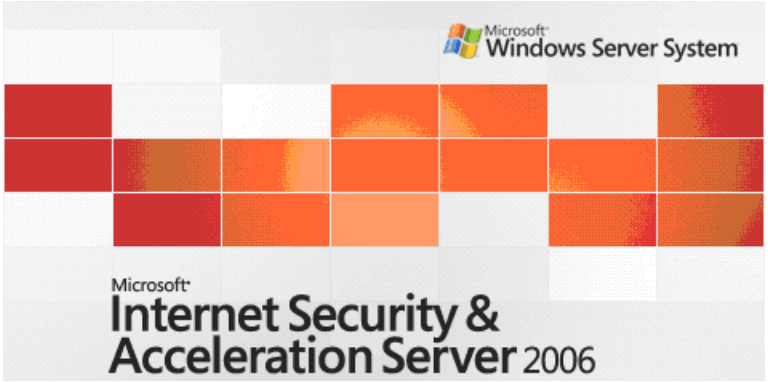
RSA SecurID Ready Implementation Guide

Last Modified: March 31, 2008

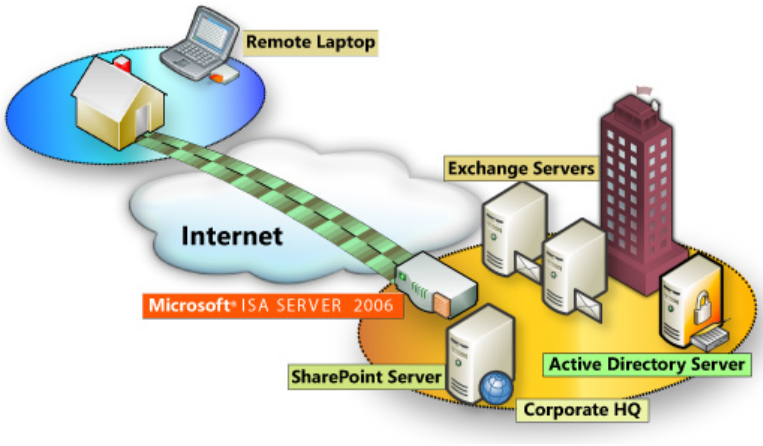
Partner Information

Product Information	
Partner Name	Microsoft
Web Site	http://www.microsoft.com/ISAServer
Product Name	Internet Security and Acceleration (ISA) Server
Version & Platform	2006
Product Description	ISA Server 2006 contains a full-featured, application-layer-aware firewall that helps protect organizations of all sizes from attack by both external and internal threats. ISA Server 2006 performs deep inspection of Internet protocols such as Hypertext Transfer Protocol (HTTP), which enables it to detect many threats that traditional firewalls cannot detect. The integrated firewall and VPN architecture of ISA Server supports stateful filtering and inspection of all VPN traffic. The firewall also provides VPN client inspection for Microsoft Windows Server 2003-based quarantine solutions, helping to protect networks from attacks that enter through a VPN connection. In addition, a completely new user interface, wizards, templates, and a host of management tools help administrators avoid common security configuration errors.
Product Category	Perimeter Defense (Firewalls, VPNs & Intrusion Detection)



Solution Summary

Partner Integration Overview	
Authentication Methods Supported	Native RSA SecurID Authentication
List Library Version Used	5.0.3
RSA Authentication Manager Name Locking	Yes
RSA Authentication Manager Replica Support	Full Replica Support
Secondary RADIUS Server Support	N/A
Location of Node Secret on Agent	C:\Program Files\Microsoft ISA Server\sdconfig
RSA Authentication Agent Host Type	Net OS
RSA SecurID User Specification	All Users
RSA SecurID Protection of Administrative Users	No
RSA Software Token API Integration	No
Use of Cached Domain Credentials	No



Product Requirements

Partner Product Requirements: ISA Server 2006	
CPU	733 MHz Pentium III or faster processor
Operating System	Windows Server 2003 with Service Pack 1
Memory	512MB or more recommended
Storage	NTFS-formatted local partition with 150 MB of available hard-disk space; additional space required for web cache content

Agent Host Configuration

To facilitate communication between the **Microsoft ISA Server** and the RSA Authentication Manager / RSA SecurID Appliance, an Agent Host record must be added to the RSA Authentication Manager database. The Agent Host record identifies the **Microsoft ISA Server** within its database and contains information about communication and encryption.

To create the Agent Host record, you will need the following information.

- Hostname
- IP Addresses for all network interfaces

When adding the Agent Host Record, you should configure the **Microsoft ISA Server** as a **Net OS** Agent. This setting is used by the RSA Authentication Manager to determine how communication with the Microsoft ISA Server will occur.

Note: Hostnames within the RSA Authentication Manager / RSA SecurID Appliance must resolve to valid IP addresses on the local network.

Please refer to the appropriate RSA Security documentation for additional information about Creating, Modifying and Managing Agent Host records.

Partner Authentication Agent Configuration

Before You Begin

This section provides instructions for integrating the partners' product with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All vendor products/components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Configuration of ISA Server 2006 VPN Connections

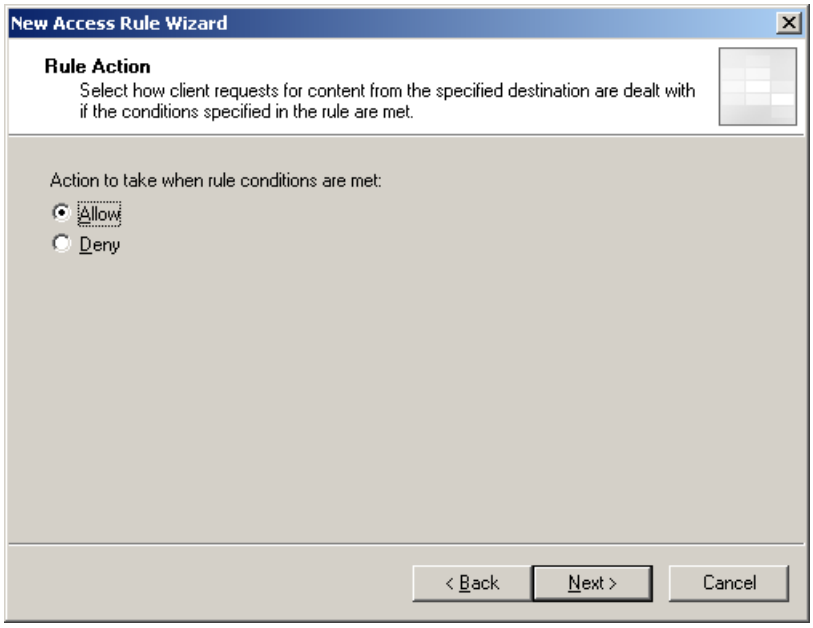
Once you have configured the ISA Server as an Agent Host within RSA Authentication Manager's Database Administration, you must perform the following steps to configure ISA for RSA SecurID authentication.

- Create Firewall Access Rule for RSA SecurID Authentication
- Install RSA Authentication Agent 6.1 for Microsoft Windows
- Test connectivity between the RSA Authentication Manager and ISA Server
- Configure the VPN Server to use the RSA EAP Authentication Method
- Configure the VPN Client to use the RSA EAP Authentication Method

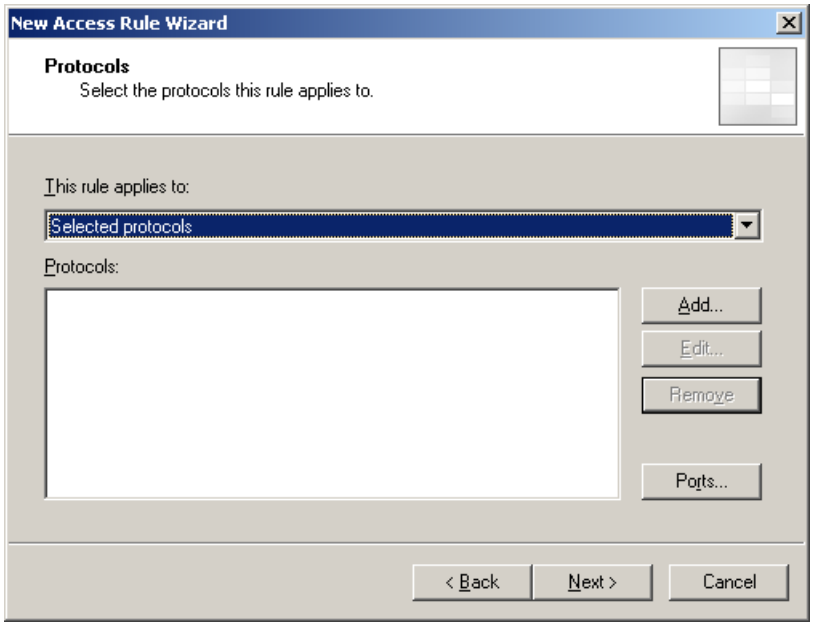
Create a Firewall Access Rule for RSA SecurID Authentication

1. Open the ISA Server Management console and expand your ISA Server instance.
2. Click on Firewall Policy.
3. From the ISA Server Dashboard Task list choose Create New Access Rule.
4. Enter the Name of the New Access Rule.

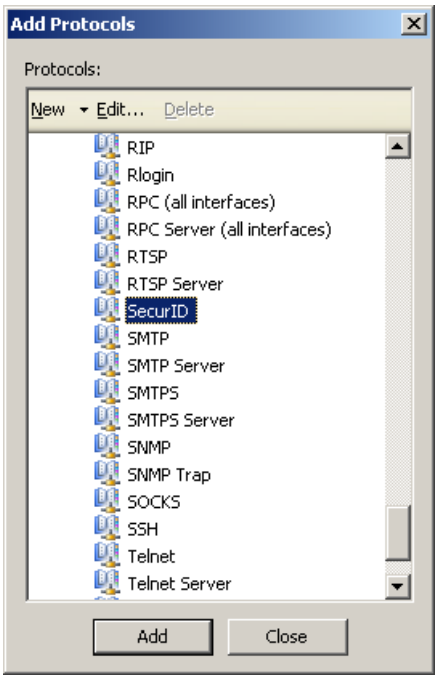
5. Action to take when conditions are met should be set to Allow.

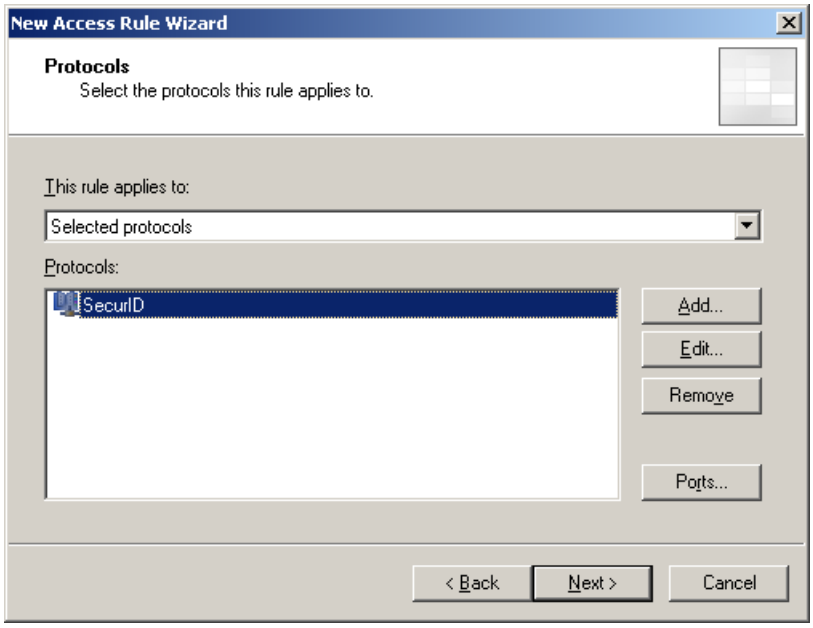


6. On the Protocol selection screen, choose Selected Protocols from the drop down list.



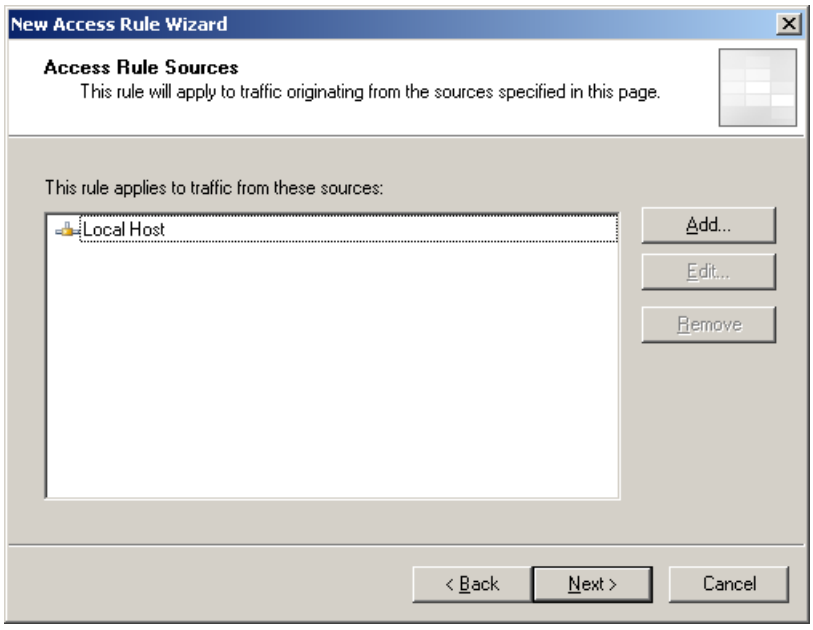
7. Click Add to display the Network Protocol list and expand All Protocols; choose SecurID.

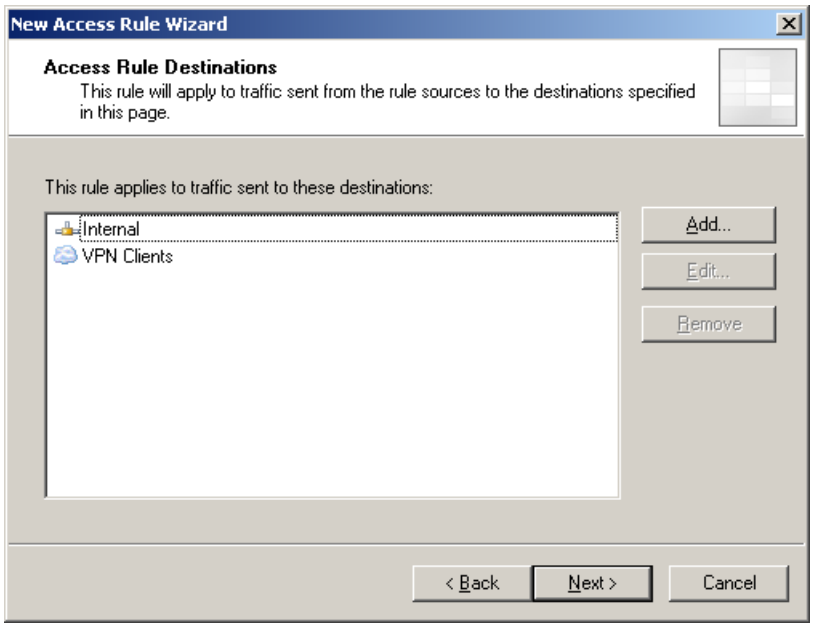




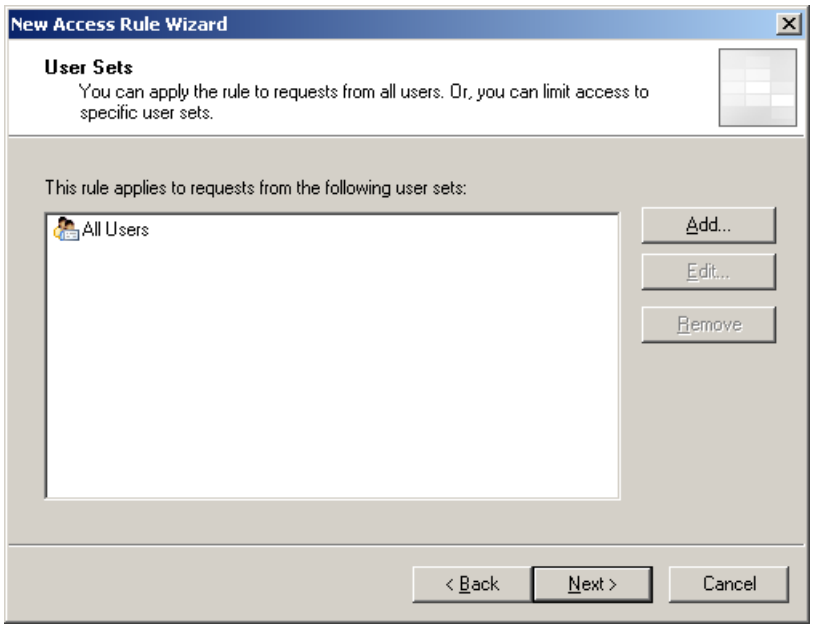
8. On the next two screens you will be asked to specify the Source and Destination hosts for your new Access Rule. Select the following objects by clicking the Add button and expanding the Networks container.

   - Access Rule Sources: Select: Local Host
   - Access Rule Destinations: Internal + VPN Clients

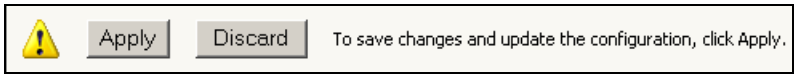




9. When prompted to select User Sets for this Access Rule, leave the default value of All Users.



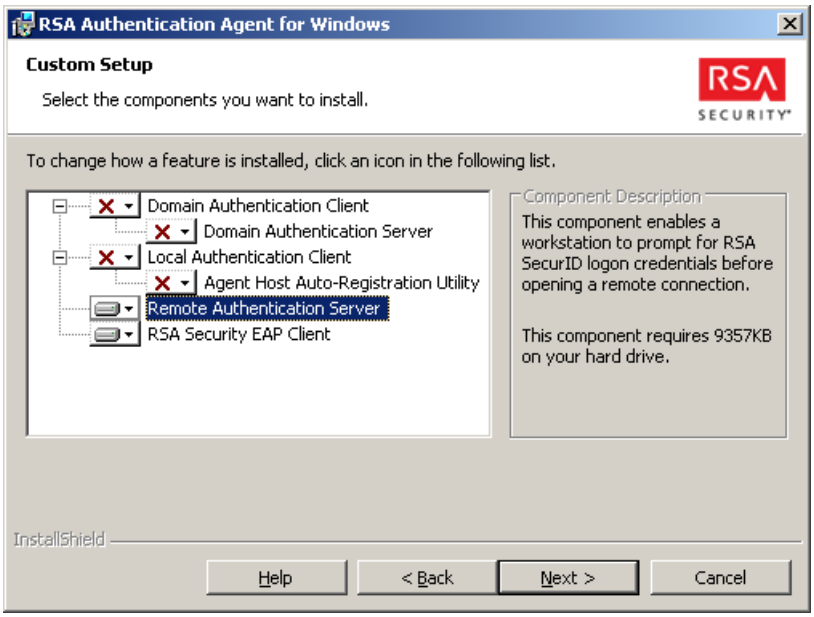
10. Review your settings and click Finish to save this Access Rule to your ISA Firewall Console.
11. Within the Dashboard, click “Apply” to make changes recognized by the ISA Server and save this new rule to your Firewall configuration.



Install RSA Authentication Agent 6.1 for Microsoft Windows

In order to configure RSA SecurID Authentication for ISA Server 2006 VPN Users, you must install and configure an RSA Authentication Agent on the ISA Server and VPN Client. The instructions for both are identical. The Agent installs the RSA Security EAP provider to be used by the Microsoft RRAS Service and VPN Client application for authentication and VPN session establishment.

1. Install the RSA Authentication Agent for Microsoft Windows 6.1 following all prompts.
2. When prompted for Component information, choose Remote Access Authentication (Server) and RSA Security EAP Client.



3. Continue through prompts and provide your sdconf.rec file from your RSA Authentication Manager.
4. You must reboot your once the installation has completed.

Test connectivity between the RSA Authentication Manager and ISA Server

To test communication or test authentication with your RSA Authentication Manager, run the sdtest.exe utility. This utility is included in your RSA Authentication Agent installation and can be accessed through the Start Menu as shown below.

1. From the Start Menu, expand RSA ACE/Agent → Test Authentication.
2. In RSA SecurID Authentication Information dialog box, click RSA ACE/Server Test Directly.
3. In RSA SecurID Authentication, type the User Name and the PASSCODE in appropriate fields.

Note: Your first successful authentication will create the Node Secret within the Registry of your ISA Server. Once the Node Secret has been created, you must manually restart your Microsoft Firewall Service to load this into memory. As you will be restarting the Microsoft Firewall Service in the next step, you do not need to do so at this time.

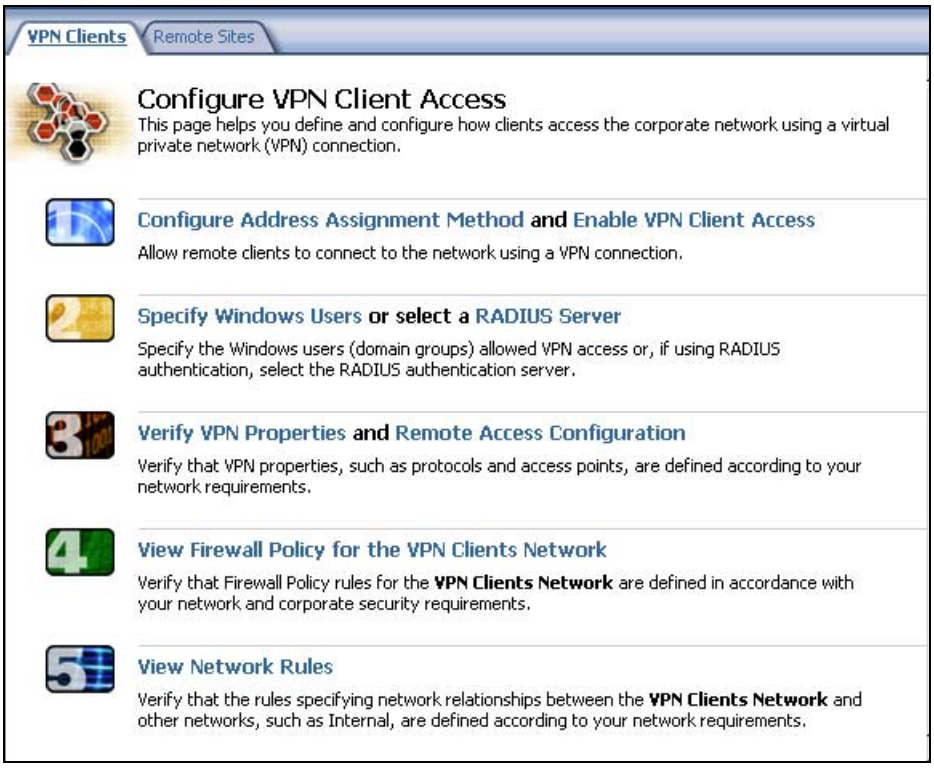
Note: Restarting your Microsoft Firewall Service will also restart your Routing and Remote Access Services as well.

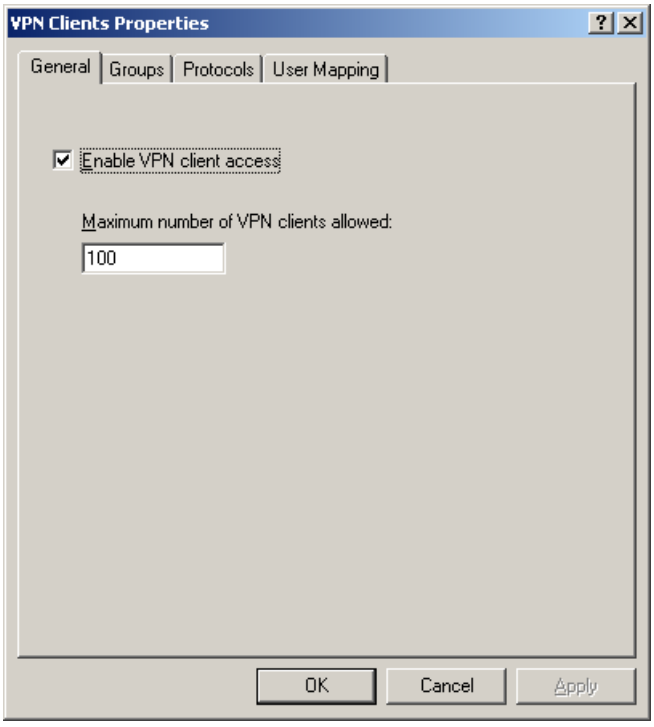
Configure the VPN Server to use the RSA EAP Authentication Method

The VPN Server is configured in two different steps. For the following steps you will need access to both the ISA Management Console as well as the MMC interface for the Routing and Remote Access Service.

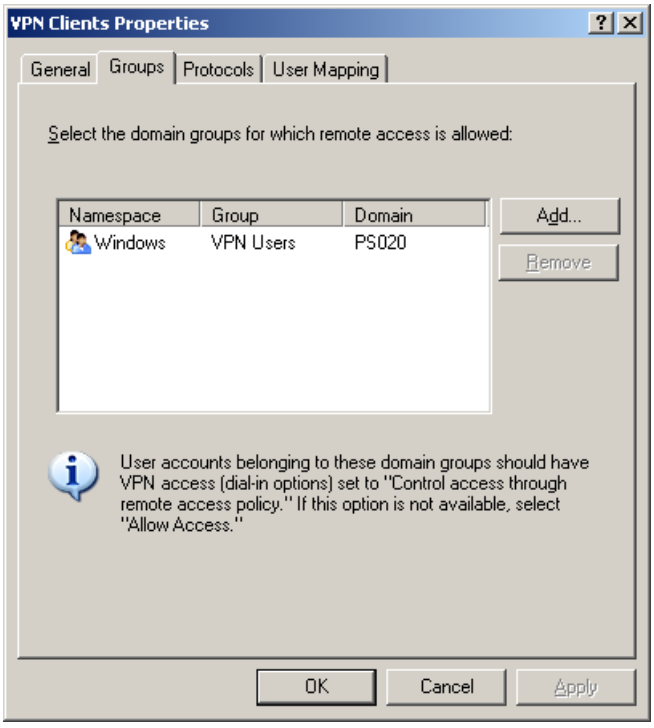
As VPN connectivity via Password authentication is a pre-requisite for this configuration, some of the following steps may have already been completed. You should verify the configuration is complete as follows.

1. Open ISA Server Management and select **Virtual Private Networks (VPN).**
2. Select **Verify VPN Properties** that VPN Client Access is Enabled, assure the selection is checked, and click OK.



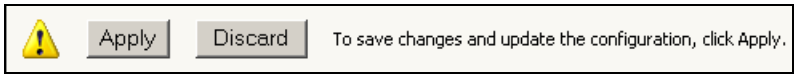


3. Proceed to the next step and choose Specify Windows Users.
4. Select your local or domain user group that will be allowed VPN access. Your RSA SecurID users should be members of the Local or Domain Group listed in this dialog.
5. Next select, Remote Access Configuration.
6. In the configuration dialog, select the Authentication tab and make sure that Extensible Authentication Protocol (EAP) is the only method selected.

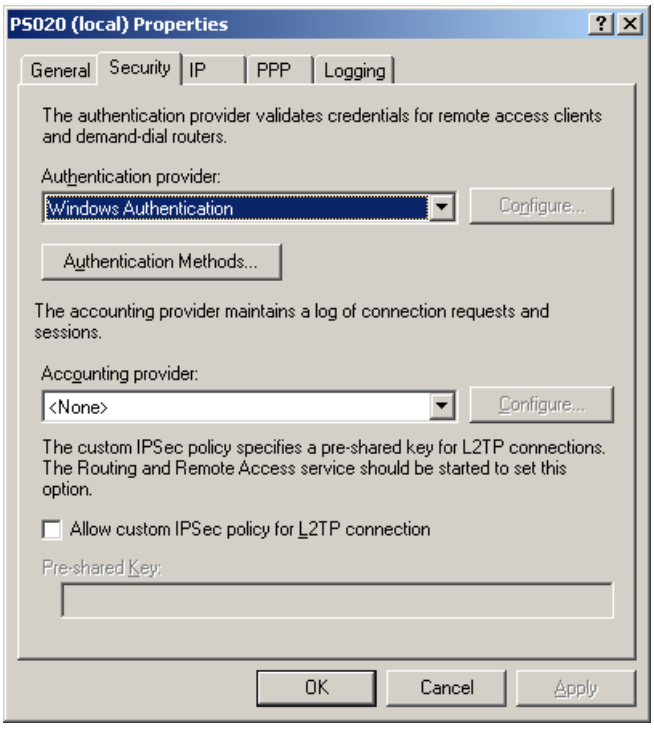


7. Next confirm that your Firewall Policies and Network Rules are configured to allow your VPN Clients access to your internal network. As your VPN environment should already be in a working state, no changes should be necessary at this time.

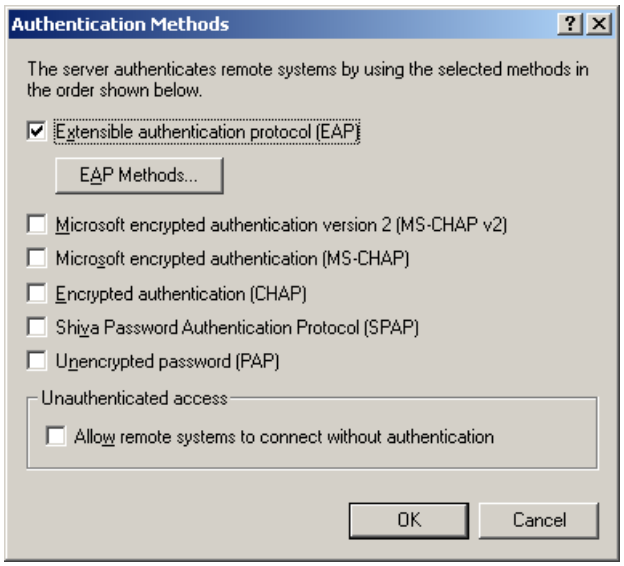
8. Within the ISA Server Dashboard, click “Apply” to make changes recognized by the ISA Server and save this new rule to your Firewall configuration.

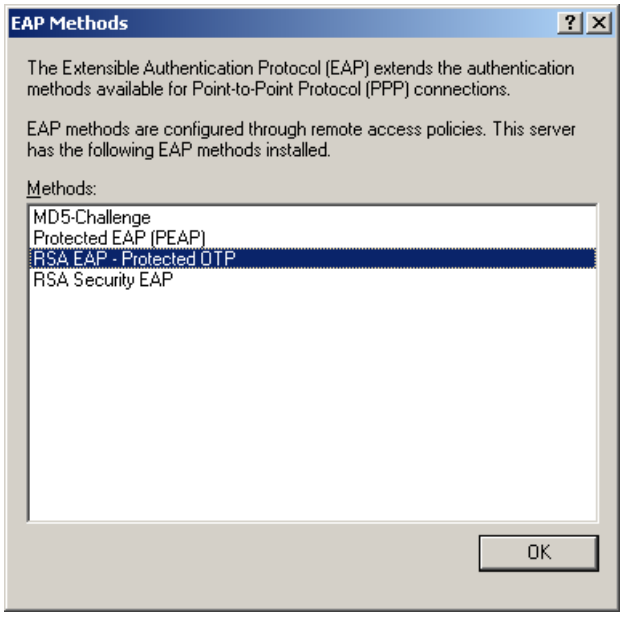


9. Next open the Routing and Remote Access Administration Console.
10. Right click on your server object and select Properties.
11. After selecting the Security Tab, Verify that the Windows Authentication provider is selected and then click on Authentication Methods.

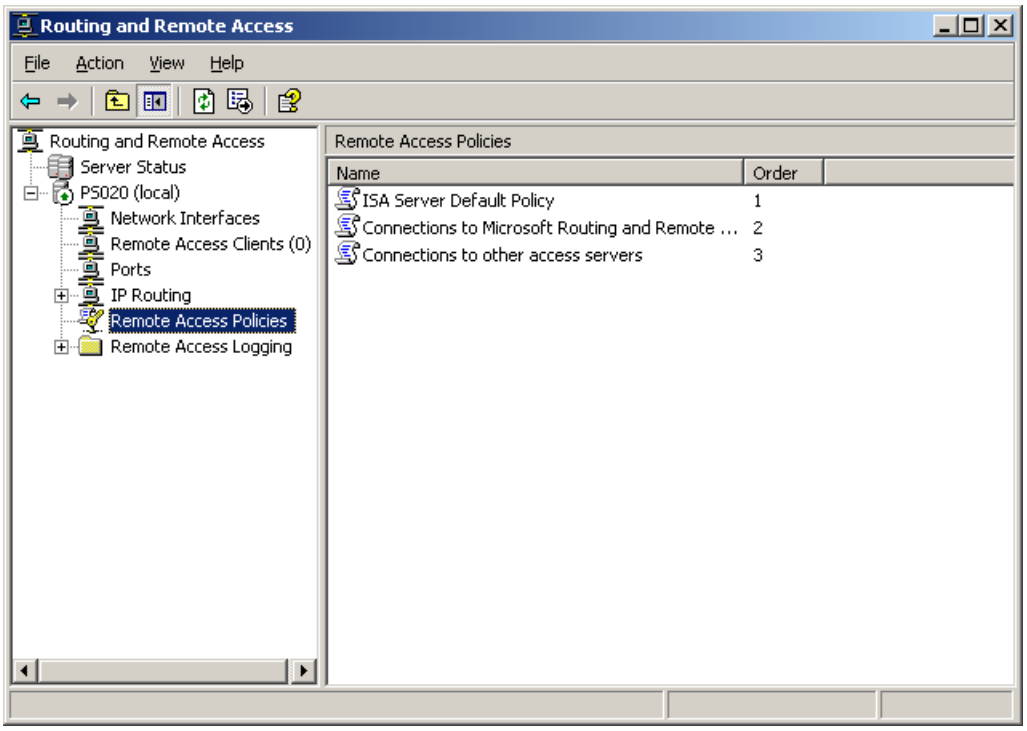


12. In the Authentication Methods make sure that only Extensible Authentication Methods (EAP) is checked. You can also verify that the RSA Security EAP Provider is installed correctly by clicking the EAP Methods button.

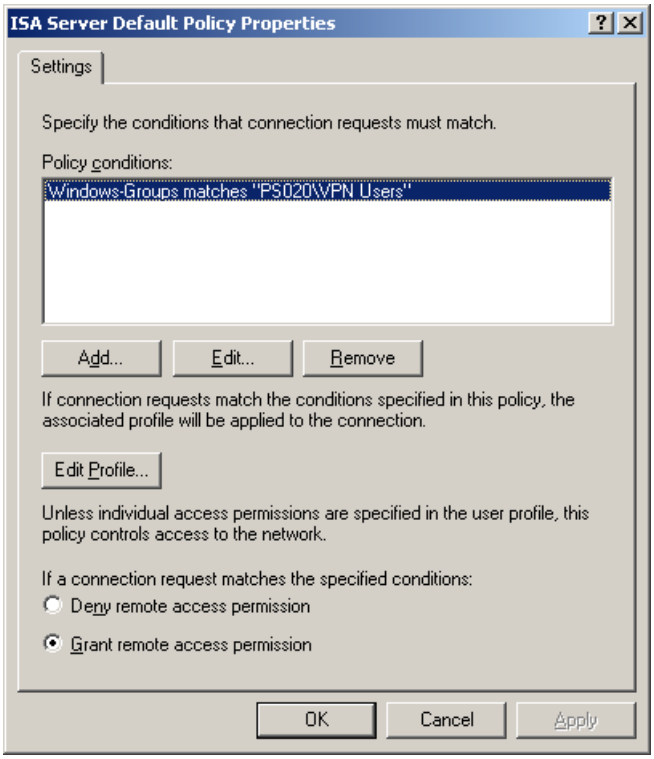




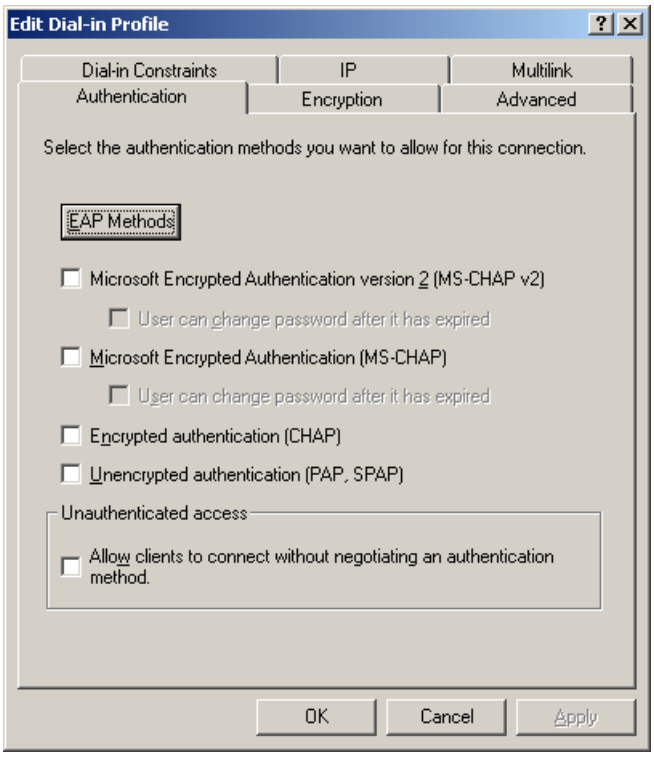
13. Click OK to save changes.
14. From the Routing and Remote Access Administration Console, select Remote Access Policies.



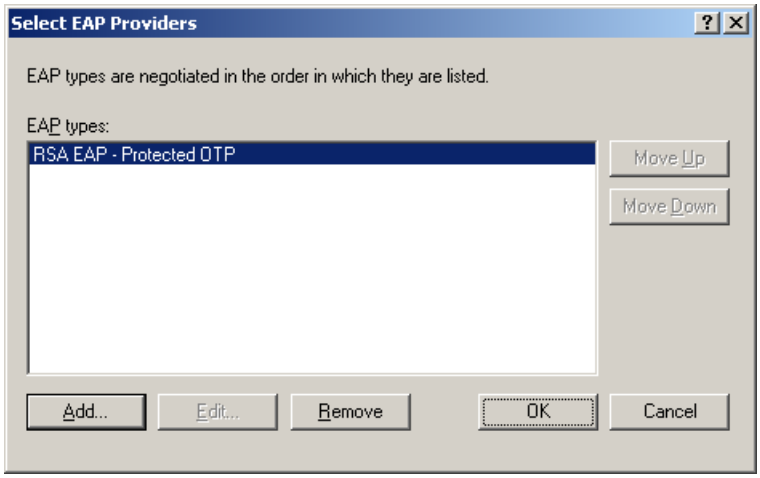
15. On the right side of the screen, right click ISA Server Default Policy and select Properties.



16. From the settings dialog, select Edit Profile.
17. Click the Authentication Tab and uncheck all options.



18. Select EAP Methods. When Selecting EAP Providers, your selection box will initially have no listing. Add the RSA Security EAP Provider by clicking Add.

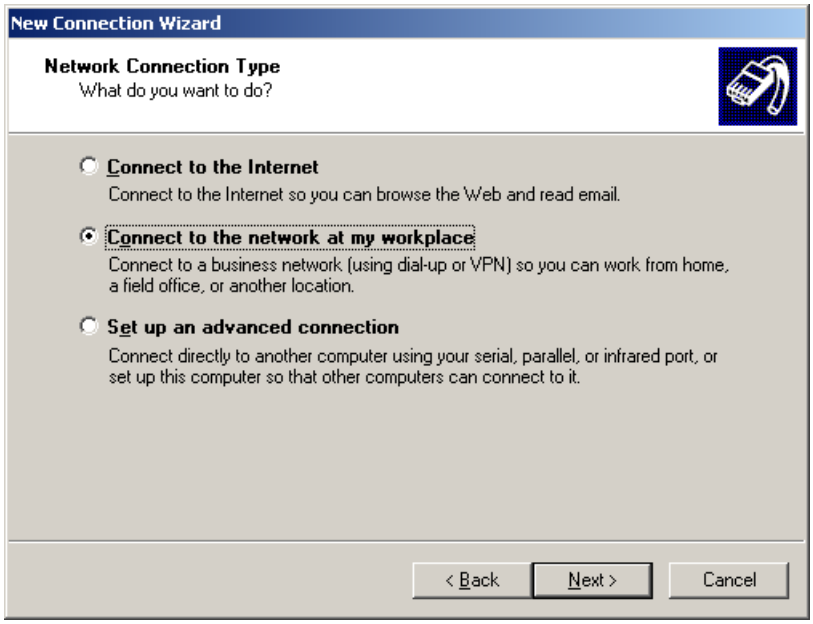


19. Click OK to save changes.

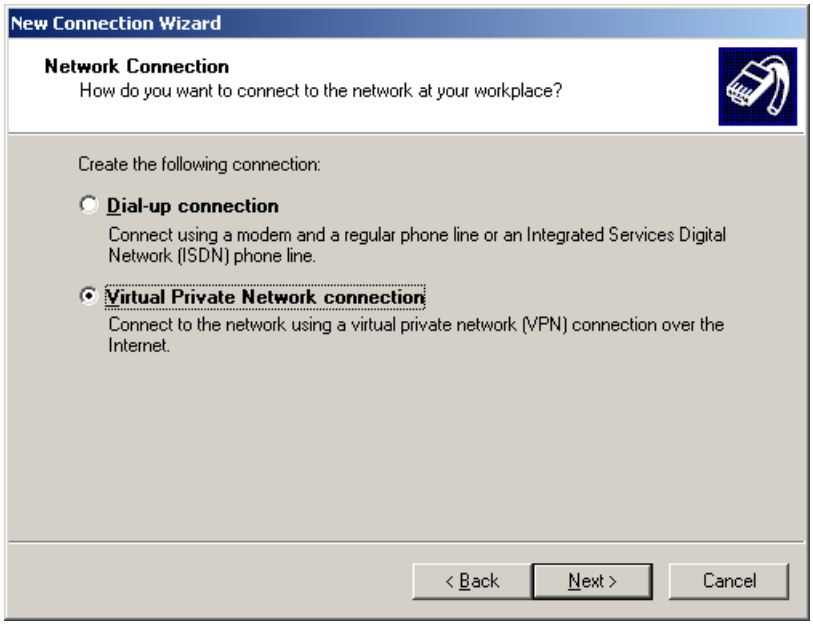
Configure the VPN Client to use the RSA EAP Authentication Method

The configuration steps will differ depending on the VPN client used. For documentation purposes, the remote access client built into Windows XP was used.

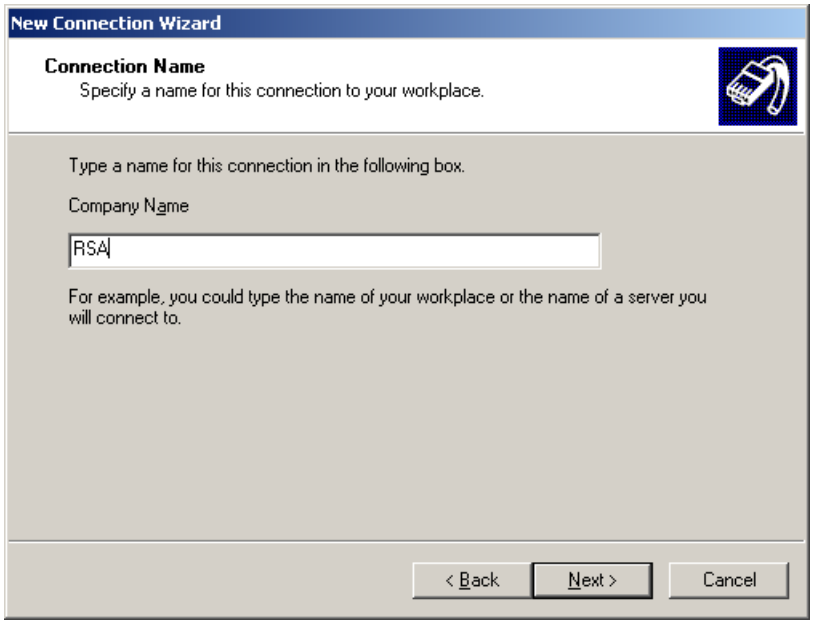
1. Start > Programs > Accessoriess > Communications > New Connection Wizard
2. Choose Connect to the network at my workplace.



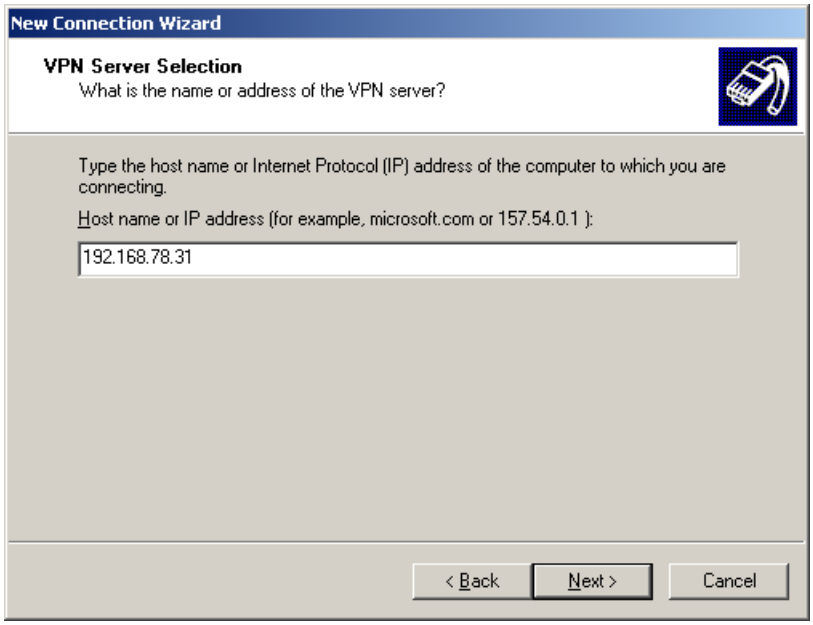
3. Choose Virtual Private Network connection



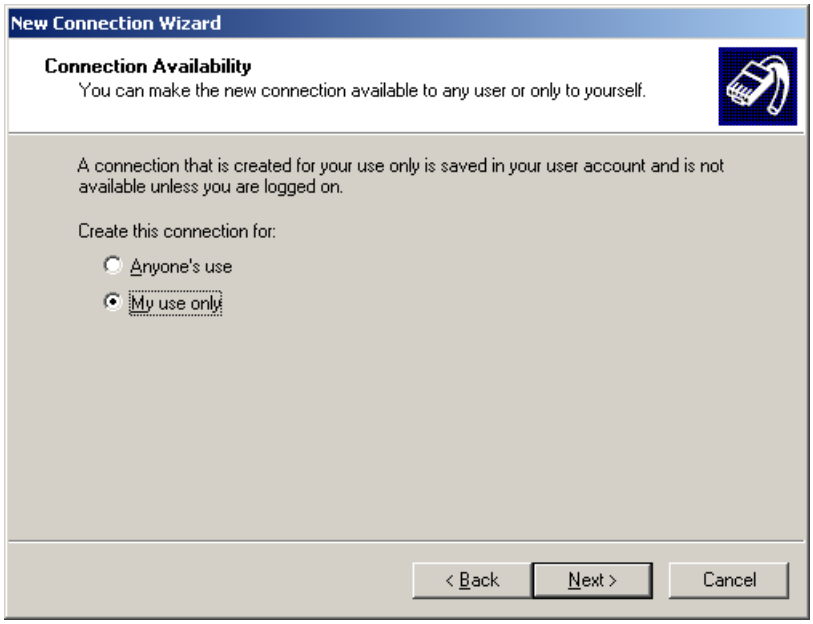
4. Define Connection name



5. Define VPN Servers connection interface. This is typically the outside interface.

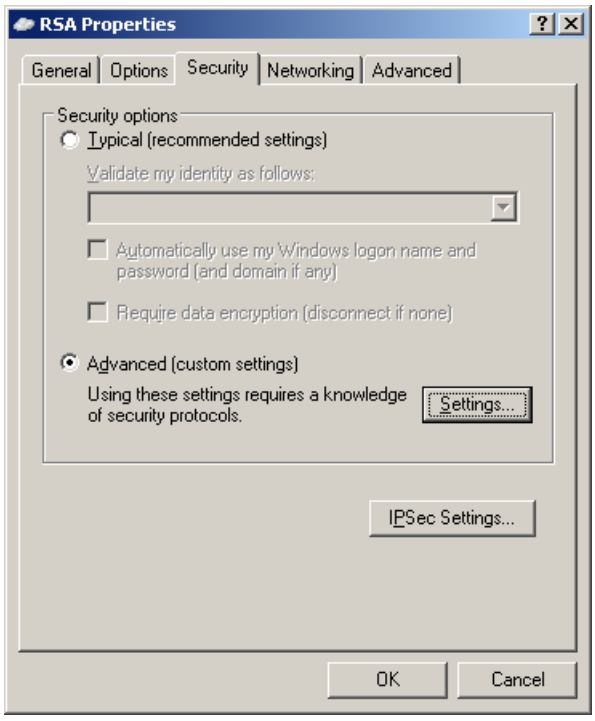


6. Connection Availability

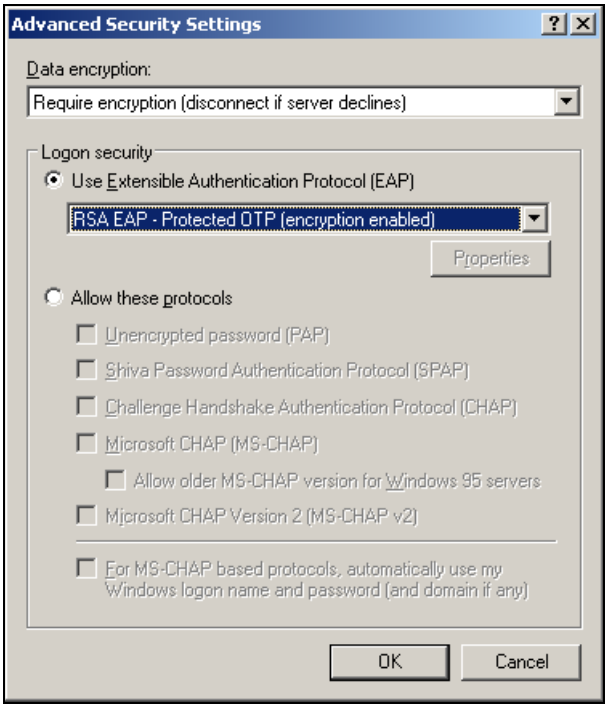


7. Click Next to finish the initial configuration
8. Open the connection that you just created.

9. Click Properties > Security. Select **Advanced (custom settings)**



10. Click Settings, select Use Extensible Authentication Protocol (EAP), and choose RSA EAP- Protected OTP (encryption enabled) from the drop down. Click OK and OK again to finish.



11. Example of prompt


Log On with RSA SecurID
RSA SecurID®
for Microsoft® Windows®
with RSA® Security Center
© Copyright 2005 RSA Security Inc.
Select your authenticator from a drop-down menu.
Choose Authenticator
Authenticator:
Key fob, standard card, PINPad
Log On
Log on with your RSA SecurID passcode.
User name:
mrennie
Passcode:
OK
Cancel

Certification Checklist

Date Tested: November 6, 2006

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	6.1	Windows 2003 Server
ISA Server 2006	Standard Edition	Windows 2003 Server
ISA Server 2006	Enterprise Edition	Windows 2003 Server

Mandatory Functionality			
RSA Native Protocol		**RADIUS Protocol**	
New PIN Mode			
Force Authentication After New PIN	✓	Force Authentication After New PIN	N/A
System Generated PIN	✓	System Generated PIN	N/A
User Defined (4-8 Alphanumeric)	✓	User Defined (4-8 Alphanumeric)	N/A
User Defined (5-7 Numeric)	✓	User Defined (5-7 Numeric)	N/A
User Selectable	✓	User Selectable	N/A
Deny 4 and 8 Digit PIN	✓	Deny 4 and 8 Digit PIN	N/A
Deny Alphanumeric PIN	✓	Deny Alphanumeric PIN	N/A
PASSCODE			
16 Digit PASSCODE	✓	16 Digit PASSCODE	N/A
4 Digit Password	✓	4 Digit Password	N/A
Next Tokencode Mode			
Next Tokencode Mode	✓	Next Tokencode Mode	N/A
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	✓	Failover	N/A
Name Locking Enabled	✓	Name Locking Enabled	
No RSA Authentication Manager	✓	No RSA Authentication Manager	N/A

Additional Functionality			
RSA Software Token API Functionality			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
User Selectable	N/A	User Selectable	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A
RSA SD800 Token Automation			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
User Selectable	N/A	User Selectable	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A

MPR

✓ = Pass ✗ = Fail N/A = Non-Available Function

7.1 Certification Checklist

Date Tested: March 31, 2008

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	7.1	Windows 2003 SP1
RSA Authentication Agent	6.1.1 (53)	Windows XP SP2
RSA Software Token	3.07 (39)	Windows XP SP2
Microsoft ISA 2006	5.0.5720.100	Windows 2003 SP1

Mandatory Functionality			
RSA Native Protocol		**RADIUS Protocol**	
New PIN Mode			
Force Authentication After New PIN	✓	Force Authentication After New PIN	N/A
System Generated PIN	✓	System Generated PIN	N/A
User Defined (4-8 Alphanumeric)	✓	User Defined (4-8 Alphanumeric)	N/A
User Defined (5-7 Numeric)	✓	User Defined (5-7 Numeric)	N/A
Deny 4 and 8 Digit PIN	✓	Deny 4 and 8 Digit PIN	N/A
Deny Alphanumeric PIN	✓	Deny Alphanumeric PIN	N/A
Deny Numeric PIN	✓	Deny Numeric PIN	N/A
PIN Reuse	✓	PIN Reuse	N/A
Passcode			
16 Digit Passcode	✓	16 Digit Passcode	N/A
4 Digit Fixed Passcode	✓	4 Digit Fixed Passcode	N/A
Next Tokencode Mode			
Next Tokencode Mode	✓	Next Tokencode Mode	N/A
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	✓	Failover	N/A
No RSA Authentication Manager	✓	No RSA Authentication Manager	N/A
Additional Functionality			
RSA Software Token Automation			
System Generated PIN	✓	System Generated PIN	N/A
User Defined (8 Digit Numeric)	✓	User Defined (8 Digit Numeric)	N/A
PIN Expiration	✓	PIN Expiration	N/A
Next Tokencode Mode	✓	Next Tokencode Mode	N/A
RSA SecurID 800 Token Automation			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
PIN Expiration	N/A	PIN Expiration	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A

DRP

✓ = Pass ✗ = Fail N/A = Non-Available Function