



RSA SecurID Ready Implementation Guide

Last Modified: September 24, 2004

1. Partner Information

Partner Name	Microsoft
Web Site	http://www.microsoft.com/ISAServer
Product Name	Internet Security and Acceleration (ISA) Server
Version & Platform	2004
Product Description	ISA Server 2004 provides advanced protection, ease of use, and fast and secure access for all types of networks. It is particularly well suited for protecting networks that are running Microsoft applications, such as Microsoft Outlook Web Access (OWA), Microsoft Internet Information Services, Office SharePoint Portal Server, Routing and Remote Access Service, Active Directory services, and others.
Product Category	Perimeter Defense



2. Contact Information

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

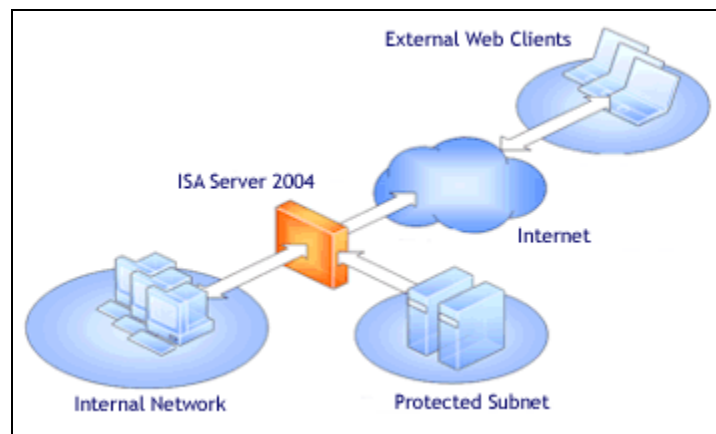
3. Solution Summary

ISA Server 2004 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 2004 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 support 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.

Microsoft ISA Server 2004 supports Native SecurID API's for strong authentication to hosted web content. While there is no built in support for RSA Security EAP authentication for VPN users, this functionality can be added to the ISA Server by installing the RSA ACE/Agent software.

Feature	Details
Authentication Methods Supported	Native RSA SecurID
RSA ACE/Agent Library Version	5.03
RSA ACE 5 Locking	Yes
Replica RSA ACE/Server Support	Full Replica Support
Secondary RADIUS Server Support	N/A
Location of Node Secret on Client	In Registry
RSA ACE/Server Agent Host Type	Net OS
RSA SecurID User Specification	All Users
RSA SecurID Protection of Partner Product Administrators	No
RSA Software Token Integration	No



4. Product Requirements

Hardware requirements

Component Name: ISA Server 2004	
CPU make/speed required	550 MHz Pentium III or faster processor
Memory	256 megabytes (MB) of RAM or more recommended
HD space	NTFS-formatted local partition with 150 MB of available hard-disk space; additional space required for Web cache content

Software requirements

Component Name: ISA Server 2004	
Operating System	Version (Patch-level)
Windows 2000 Server	Service Pack 4
Windows Server 2003	
Software	Version (Patch-level)
Internet Explorer	6.0 or later
Microsoft Hot Fix Q821887	Windows 2000 Only

Note:

The ISA Server 2004 VPN functionality was tested and certified using a patched version of the RSA ACE/Agent 5.6 software. To obtain the RSA ACE/Agent 5.6.1 maintenance build, please contact RSA Security Customer Support and reference tst00040883.

Certification Environment (As Tested)

Component Name: ISA Server 2004	
Software Version	Additional Information
Windows Server 2003	Enterprise Edition (IIS and RRAS Services Enabled)
ISA Server 2004	Full installation
Internet Explorer	6.0 SP1 with all patches applied

Before you begin

Before attempting the integration you should review your Security Policies related to authentication and authorization. Once your firewall is configured for password authentication on your Web Publishing rules it is fairly simple to enable SecurID authentication. For information on configuring your Firewall rules, best security practices or initial configuration of the ISA Web Listeners, Please consult your Microsoft administration documentation or training manuals.

When configuring the ISA Server VPN Service for RSA SecurID Authentication, it is required that you have your VPN infrastructure configured and working with Windows Password Authentication before attempting to enable RSA SecurID Authentication. Making sure this functionality is working prior to attempting interoperability will assure successful integration.

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, go to **Start > Programs > RSA ACE/Server**, and then **Database Administration - Host Mode**.

1. On the **Agent Host** menu, choose **Add Agent Host....**

The screenshot shows the 'Edit Agent Host' dialog box. The 'Name' field contains 'ISAServer2004'. The 'Network address' field contains '10.2.1.1'. The 'Site' field is empty with a 'Select' button. The 'Agent type' dropdown menu is open, showing 'Single-Transaction Comm Server', 'Net OS Agent' (selected), and 'NetSP Agent'. The 'Encryption Type' section has 'SDI' and 'DES' radio buttons, with 'DES' selected. There are four checkboxes: 'Node Secret Created' (checked), 'Open to All Locally Known Users' (checked), 'Search Other Realms for Unknown Users' (unchecked), and 'Requires Name Lock' (unchecked). At the bottom, there are buttons for 'Group Activations...', 'Secondary Nodes...', 'Edit Agent Host Extension Data...', 'Assign Acting Servers...', 'User Activations...', 'Delete Agent Host', 'Assign/Change Encryption Key...', and 'Create Node Secret File...'. At the very bottom are 'OK', 'Cancel', and 'Help' buttons.

- In **Name**, type the hostname of the ISA Server.
- In **Network address**, type the IP address of the ISA Server.
- For **Agent Type**, select NET OS.
- Under **Secondary Nodes**, define all hostname/IP addresses that resolve to the ISA Server.

Note: It is important that all hostname and IP addresses resolve to each other. Please reference the RSA ACE/Server documentation for detailed information 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 ISA Server 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.

Configuration of ISA Server 2004 Web Listeners

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

- Configure and test connectivity between the RSA ACE/Server and ISA Server.
- Enable the SecurID Web Filter.
- Configure a Web publishing rule for which authentication for RSA SecurID is required.

Configure and test connectivity with the RSA ACE/Server

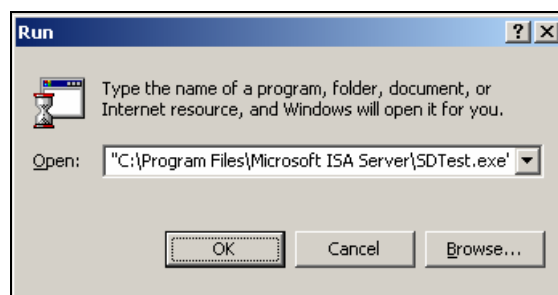
Microsoft has included all of the necessary API's to allow direct integration with the RSA ACE/Server and SecurID authentication. No agent installation is necessary in order to achieve interoperability for Web based authentication to the ISA Firewall protected resources.

Once you have obtained the `sdconf.rec` from your RSA ACE/Server the save a copy to `%windir%\System32\`

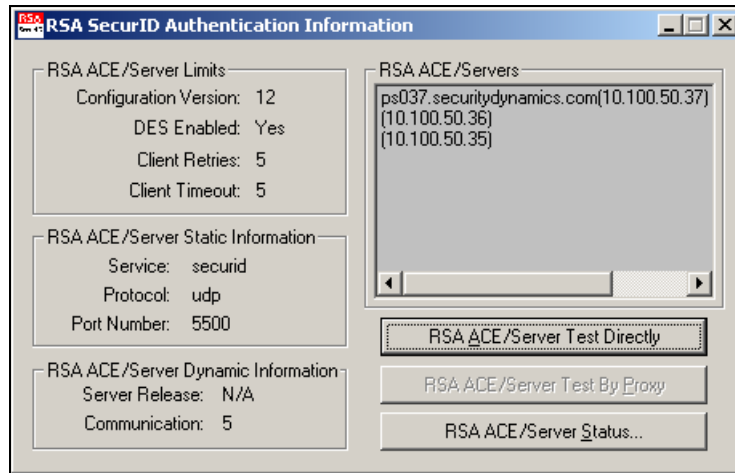
The Microsoft ISA Server includes a tool which you can use to verify that there is connectivity between the ISA Server computer and the ACE/Server computer. You can use this test client to verify connectivity, as well as establish the "Node Secret" used for encrypting communication with the RSA ACE/Server.

To test communication or test authentication with your RSA ACE/Server, run the `sdtest.exe` utility. This utility is included in the default ISA Server 2004 installation and can be run from the ISA installation directory as shown below.

1. From a command line, type `%Path to ISA installation directory%\sdtest.exe`.



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.

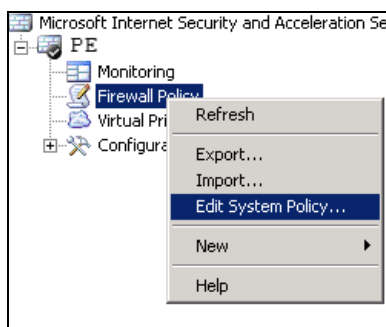


4. Here is an example of the successful authentication dialog. Your initial authentication will create the Node Secret within the Registry of your ISA Server.

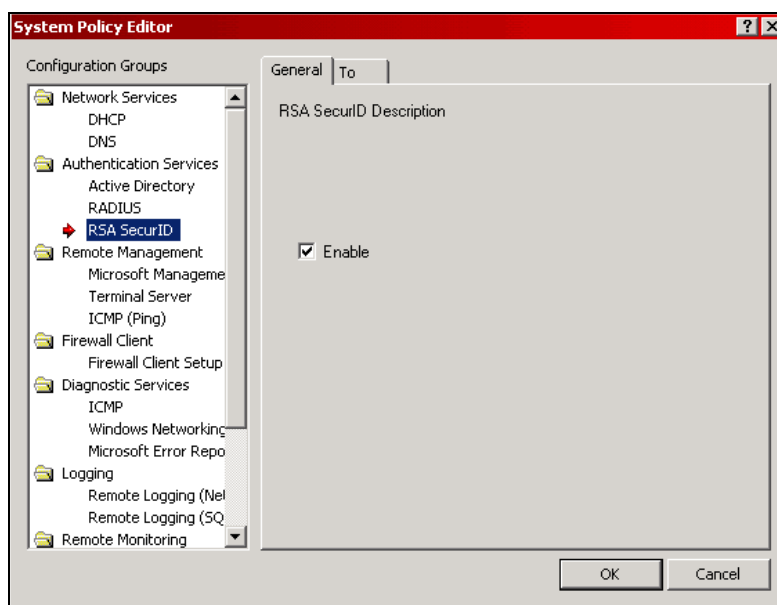


Enable the SecurID Web Filter

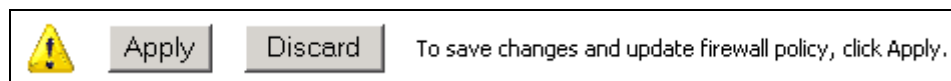
1. Open the ISA Server Management console.
2. Expand your ISA Server instance.
3. Right click on **Firewall Policy**. Choose **Edit System Policy**.



4. From the System Policy Editor select RSA SecurID from the Authentication Services section.
5. Click "Enable" to configure the ISA Server to use SecurID authentication.
6. Click "OK" to save your changes, restart your ISA Server to apply the changes and load the Node Secret into the service.



7. Within the Dashboard, Click apply to save this change to your Firewall configuration.

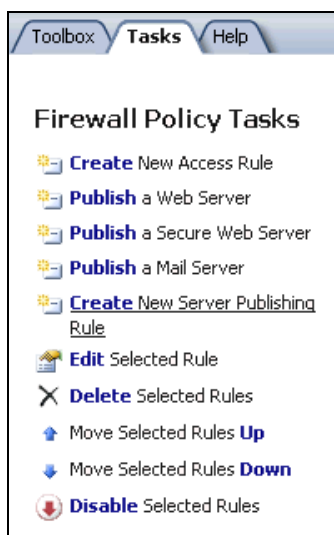


Note:

Once the ISA Server is configured to authenticate users with the SecurID method, you will have to restart your server for the ISA Firewall services to load the "Node Secret" This restart also applies when removing and re-establishing the Node Secret with your RSA ACE/Server.

Configure a Web publishing rule with RSA SecurID authentication

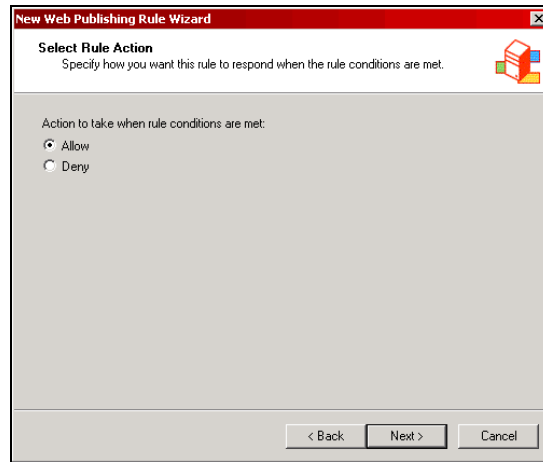
5. Open the ISA Server Management console.
6. Expand your ISA Server instance.
7. Click on **Firewall Policy**.
8. From the ISA Server Dashboard Task list choose **Create New Server Publishing Rule**.



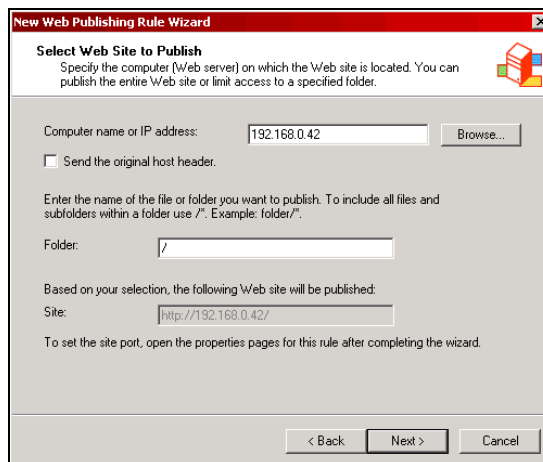
9. Enter the Name of the Web Publishing Rule.



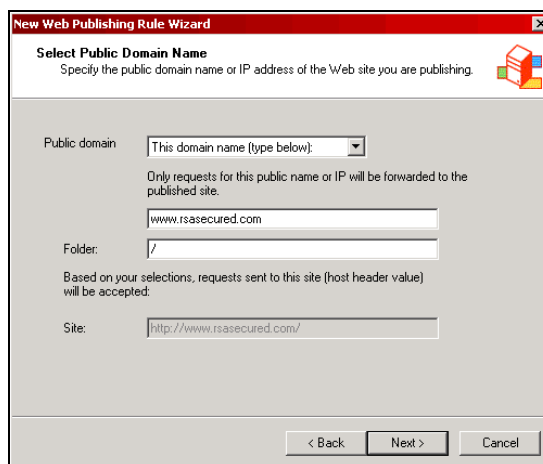
10. Select Rule Action as **“Allow”**.



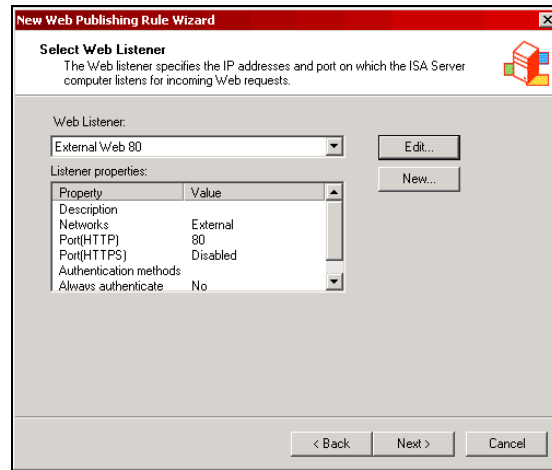
11. Enter the server information and folder you will be publishing with ISA Server 2004.



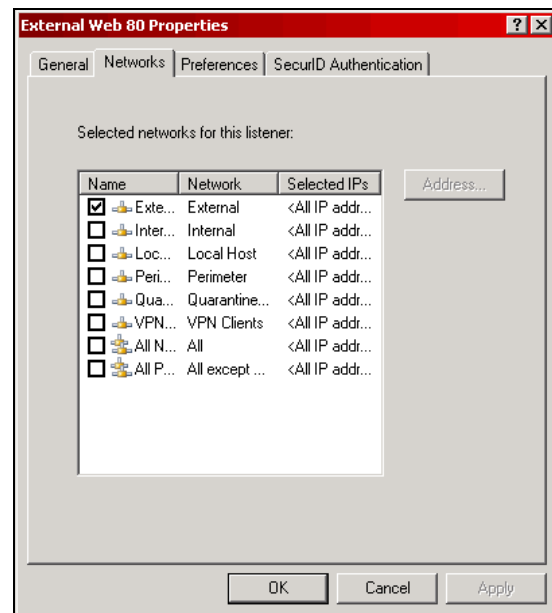
12. Enter domain information and folder information for published content.



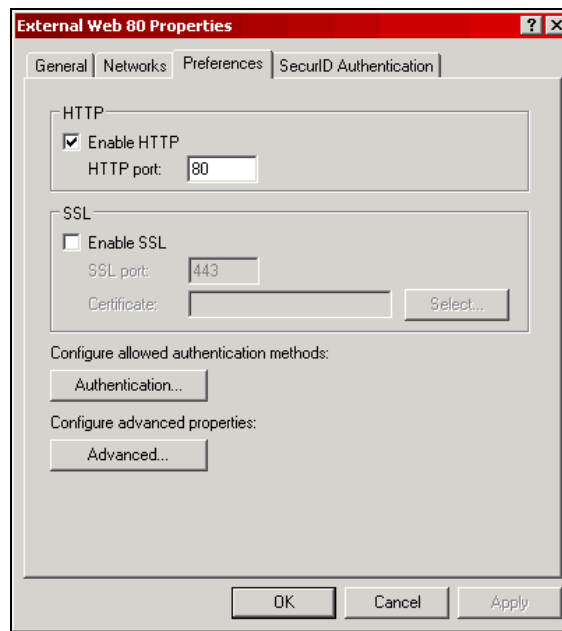
13. Select your Web Listener that will be used for hosting the Web Traffic. Click Edit to configure the Web Listener for SecurID Authentication.



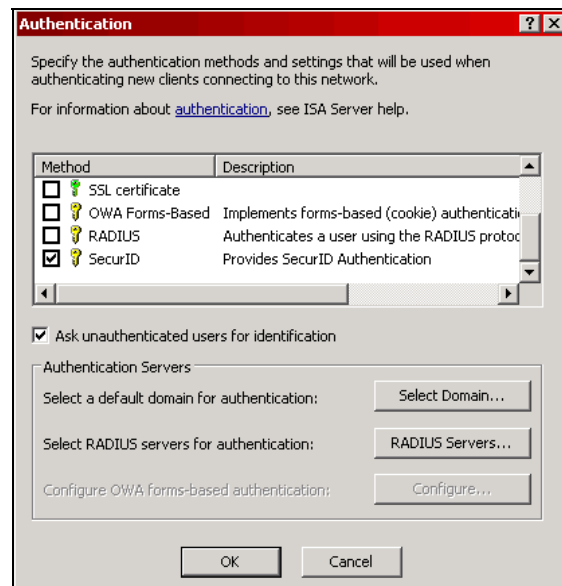
14. From the Web Listener Properties dialog, click on the **Networks** tab.
15. Select the networks that the Web Listener will bind to, the selection will only refer to interfaces that will accept HTTP requests from end user desktops.



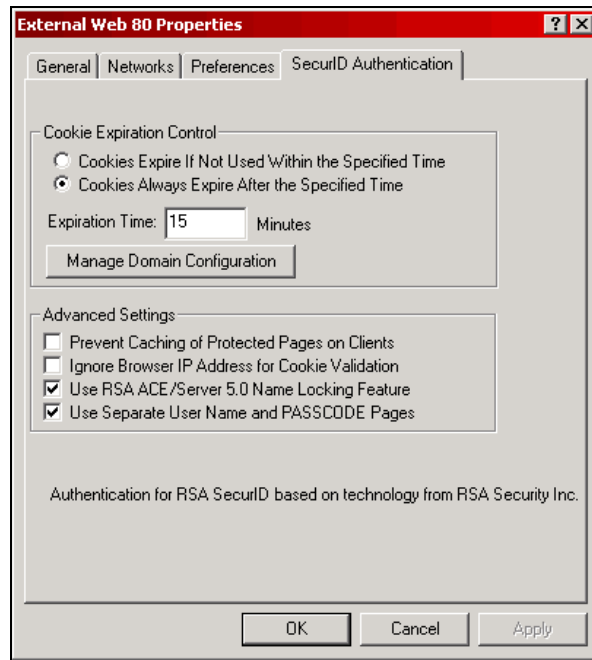
16. Click the Preferences Tab to configure HTTP Port, SSL Port and Authentication options.
17. Click the **Authentication** button to activate RSA SecurID as the authentication method.



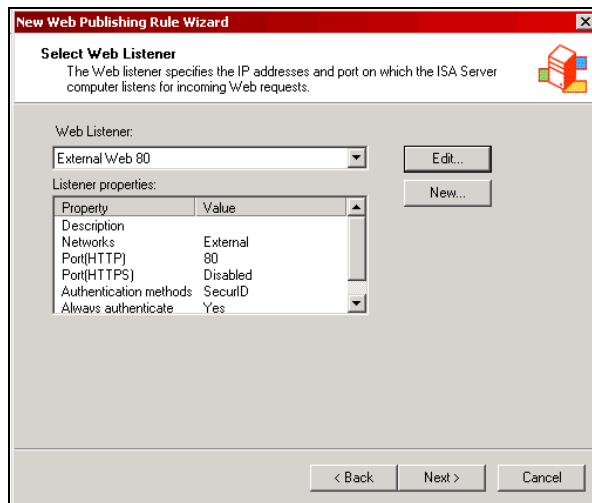
18. From the list of authentication methods, select SecurID.
19. Click "Ask unauthorized users for identification".
20. Click "OK" to apply changes



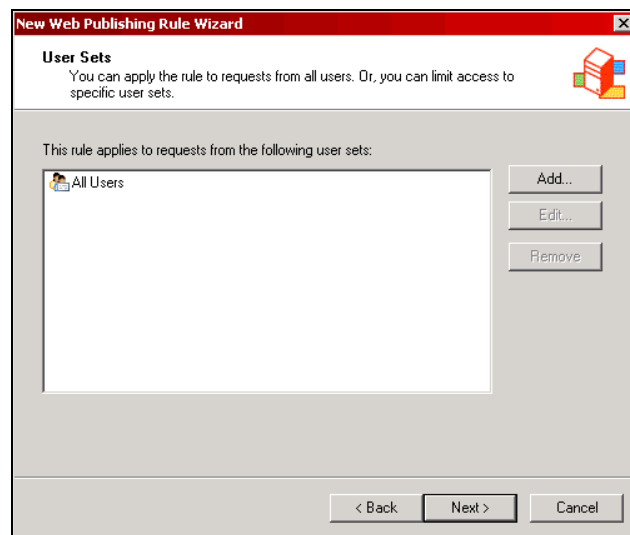
21. To Modify the RSA SecurID Authentication options click on the **SecurID Authentication** tab within the Web Listener properties page.



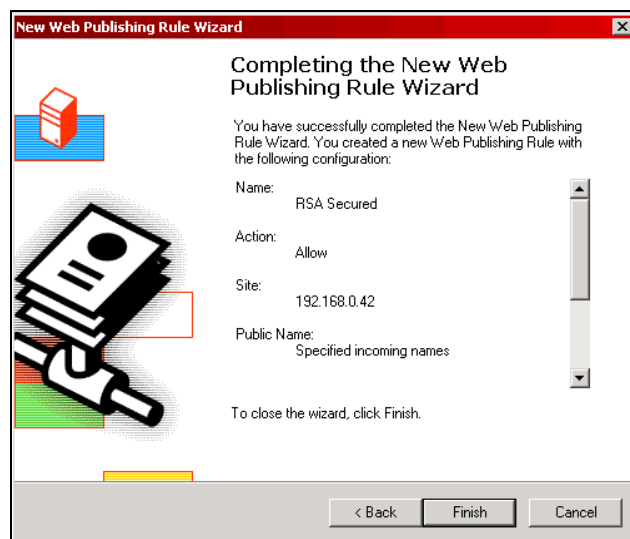
22. Click "OK" to apply all changes to the Web Listener properties page and continue your Server Publishing rule configuration.
23. You should now see that the SecurID authentication method is enabled in the Web Listener. Click "Next" to continue with the configuration.



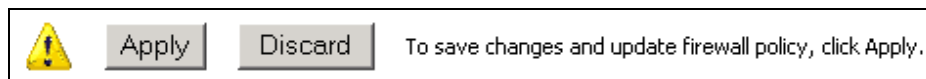
24. Add “All Users” to the “User Sets” for this Firewall Rule. This will configure the Firewall rule to apply this to all users requesting this resource.



25. Click “Finish” to save the new Web Publishing Rule to the Dashboard.

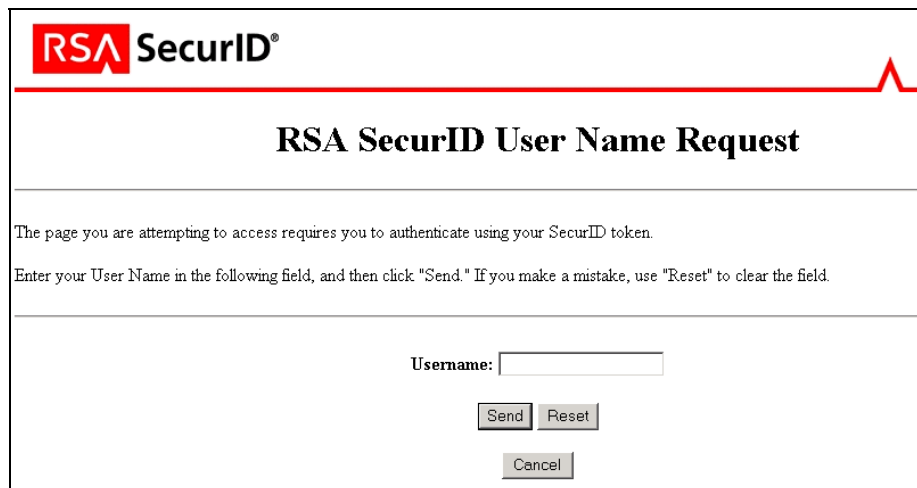


26. Within the Dashboard, click “Apply” to make changes recognized by the ISA Server and save this new rule to your Firewall configuration.



Test the RSA SecurID authentication method for Web Listener

1. Opening a web browser from an external web client and pointing the browser to the ISA Server's protected resource will prompt you for authentication with the following screen. Enter Username and or Passcode as directed to login to the ISA Server hosted web content.



The screenshot shows the RSA SecurID login interface. At the top left is the RSA SecurID logo. The main heading is "RSA SecurID User Name Request". Below this, a message states: "The page you are attempting to access requires you to authenticate using your SecurID token." A second message says: "Enter your User Name in the following field, and then click 'Send.' If you make a mistake, use 'Reset' to clear the field." There is a text input field labeled "Username:". Below the field are three buttons: "Send", "Reset", and "Cancel".

Note:

The RSA SecurID login screen will be different depending on the RSA name locking functionality you have selected in the SecurID Authentication tab within the Web Listener properties page.

Configuration of ISA Server 2004 VPN Connections

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

- Create Firewall Access Rule for RSA SecurID Authentication of VPN Users.
- Install RSA ACE/Agent 5.6.1 and test connectivity between the RSA ACE/Server and ISA Server.
- Configure the VPN Server to use the RSA EAP Authentication Method.

Before you begin configuration of the ISA Server or RSA ACE/Agent, you must first create a Firewall Access Rule to allow communication from the ISA Server to your VPN Client and the RSA ACE/Server using the RSA SecurID protocol. This new Access Rule is necessary as your ISA Server has a rule restricting communication of VPN Clients with internal network resources.

VPN Client Configuration

The ISA Server 2004 VPN Service requires the use of the RSA ACE/Agent 5.6.1 maintenance release for interoperability. Due to this fact the VPN Client must also have the RSA ACE/Agent 5.6.1 EAP Component installed for interoperability to take place.

For installation and configuration instructions for VPN Clients, please refer to the RSA ACE/Agent 5.6.1 documentation included in the maintenance release.

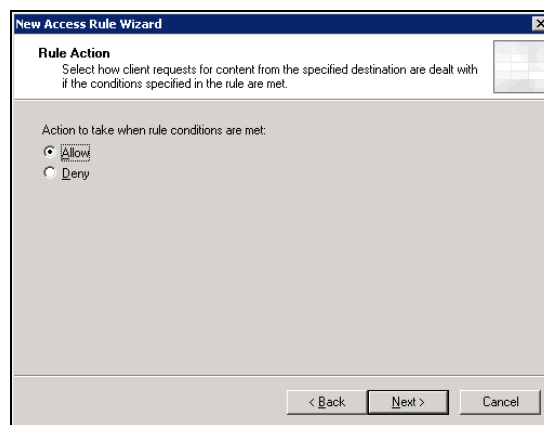
Please see the Known issues section at the end of this guide for further information on how to obtain this maintenance release.

Create a Firewall Access Rule for RSA SecurID Authentication

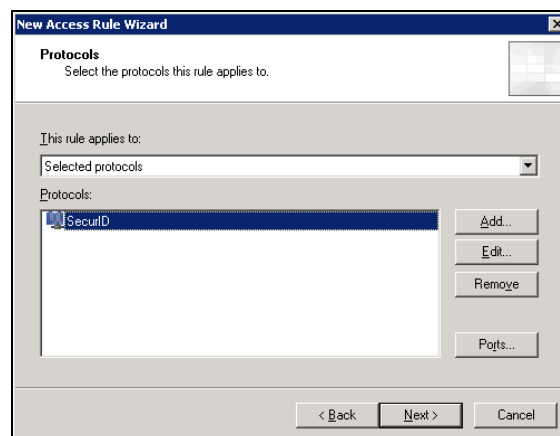
1. Open the ISA Server Management console.
2. Expand your ISA Server instance and click on **Firewall Policy**.
3. From the ISA Server Dashboard Task list choose **Create New Access Rule**.
4. Enter the Name of the New Access Rule.



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

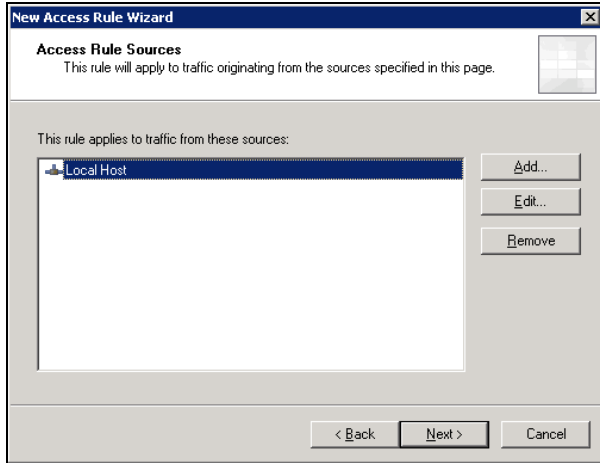


6. On the Protocol selection screen, choose Selected Protocols from the drop down list.
7. Click Add to display the Network Protocol list and expand **All Protocols**; choose SecurID.

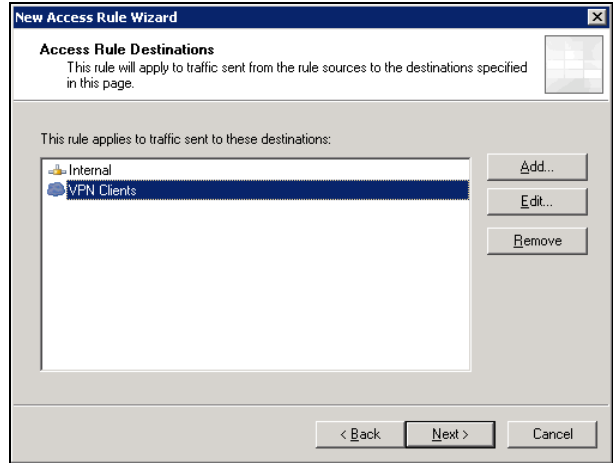


- On the next two screens you will be asked to specify the Source and Destination hosts for your new Access Rule. Select the following objects by clicking the Add button and expanding the Networks container.

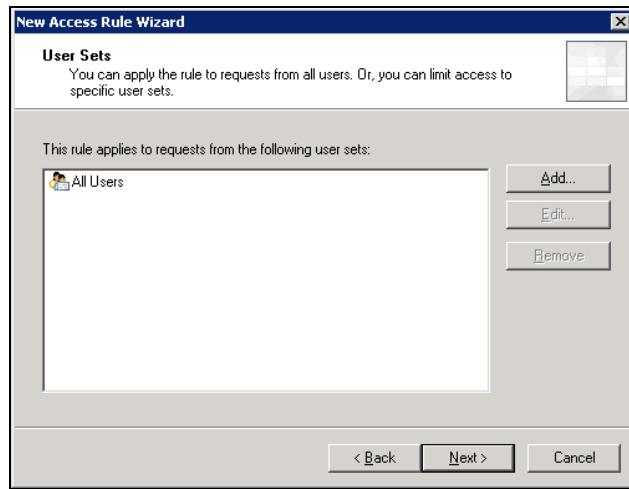
Access Rule Sources
Select: **Local Host**



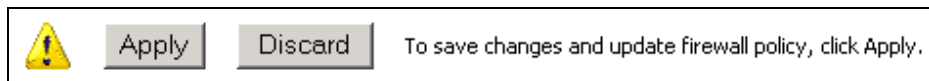
Access Rule Destinations
Select: **Internal and VPN Clients**



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



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



Configure Agent and test connectivity with the RSA ACE/Server

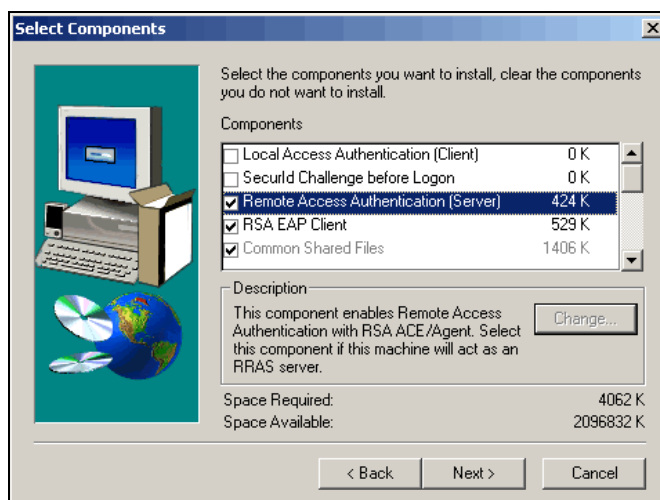
In order to configure RSA SecurID Authentication for ISA Server 2004 VPN Users, you must install and configure an RSA ACE/Agent on the ISA Server and VPN Client. The Agent installs the RSA Security EAP provider to be used by the Microsoft RRAS Service and VPN Client application for authentication and VPN session establishment.

Note:

The ISA Server 2004 VPN functionality was tested and certified using a patched version of the RSA ACE/Agent 5.6 software. To obtain the RSA ACE/Agent 5.6.1 maintenance build, please contact RSA Security Customer Support and reference tst00040883.

Installation of the RSA ACE/Agent 5.6.1 on ISA Server 2004

1. Install the RSA ACE/Agent 5.6.1 following prompts.
2. When prompted for Component information, choose Remote Access Authentication (Server) and RSA EAP Client. Common Shared Files will be selected by default.

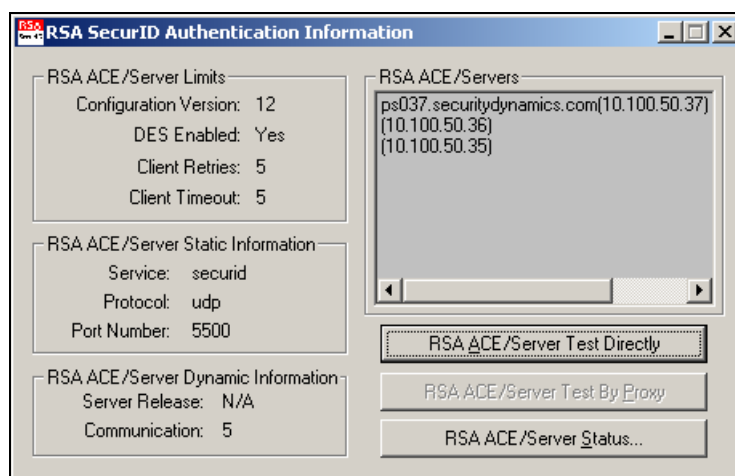


3. Continue through prompts and provide your sdconf.rec file from your RSA ACE/Server.
4. You must reboot your ISA Server once the installation has completed.

Configure and test connectivity with the RSA ACE/Server

To test communication or test authentication with your RSA ACE/Server, run the `sdtest.exe` utility. This utility is included in your RSA ACE/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**.

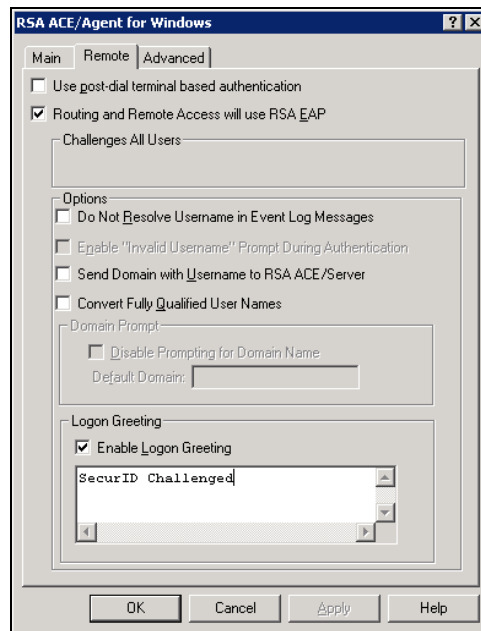


3. In RSA SecurID Authentication, type the **User Name** and the **PASSCODE** in appropriate fields.



4. 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.

- Open the RSA ACE/Agent Control Panel application and select the Remote tab.
- Enable the following Routing and Remote Access will use RSA EAP.



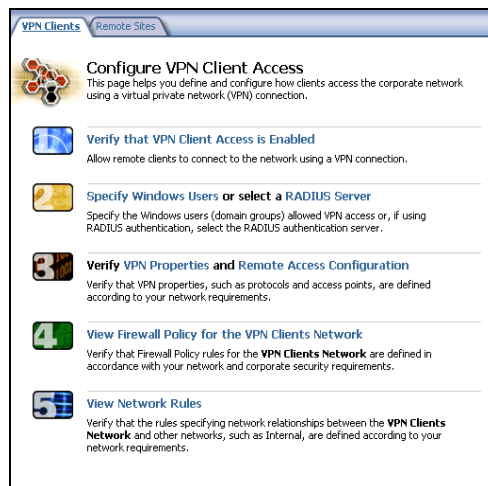
- Restart your Microsoft Firewall Service to apply changes. Restarting your Microsoft Firewall Service will also restart your Routing and Remote Access Services as well.

Configure the ISA Server VPN Service

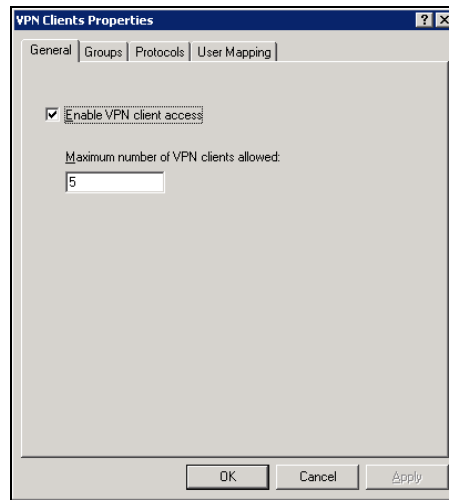
The VPN Server is configured in two different steps. For the following steps you will need access to both the ISA Management Console as well as the MMC interface for the Routing and Remote Access Service.

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.

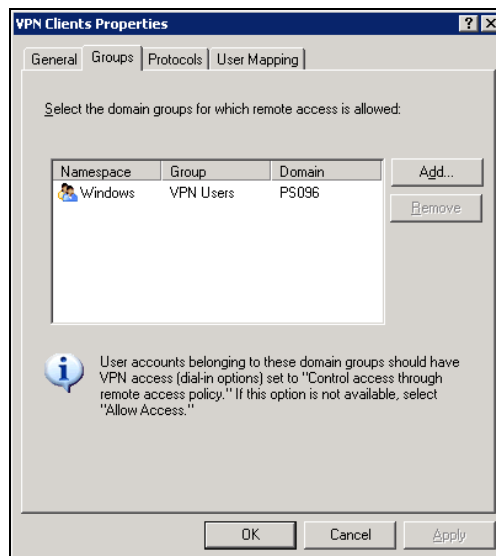
- Open ISA Server Management and select **Virtual Private Networks (VPN)**.



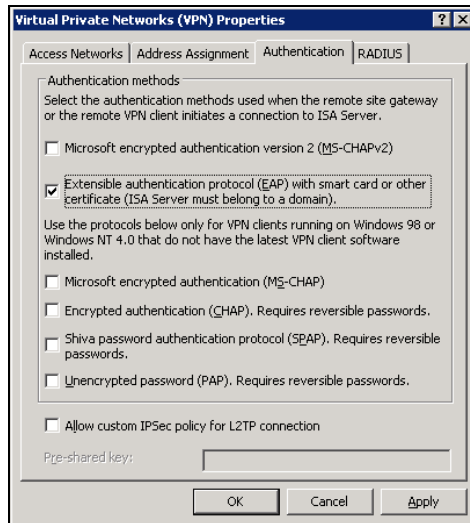
2. Select **Verify that VPN Client Access is Enabled**.
3. Verify that VPN Client Access is enabled and click OK to save changes.



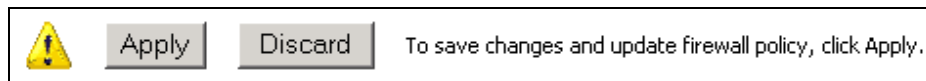
4. Proceed to the next step and choose **Specify Windows Users**.
5. Select your local or domain user group that will be allowed VPN access. Your RSA SecurID users should be members of the Local or Domain Group listed in this dialog.



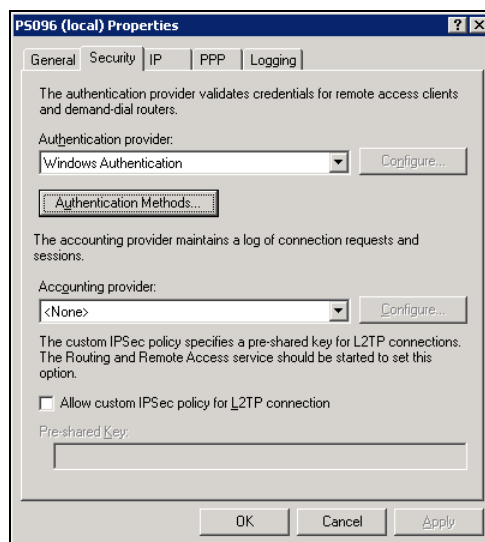
6. Next select, Remote Access Configuration.
7. In the configuration dialog, select the Authentication Tab and make sure that **Extensible Authentication Protocol (EAP)** is the only method selected.



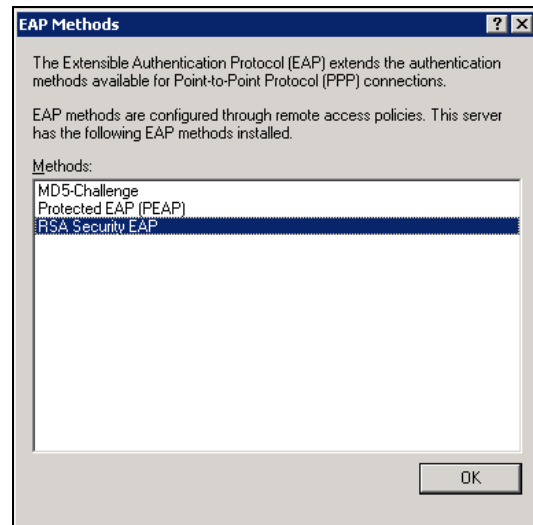
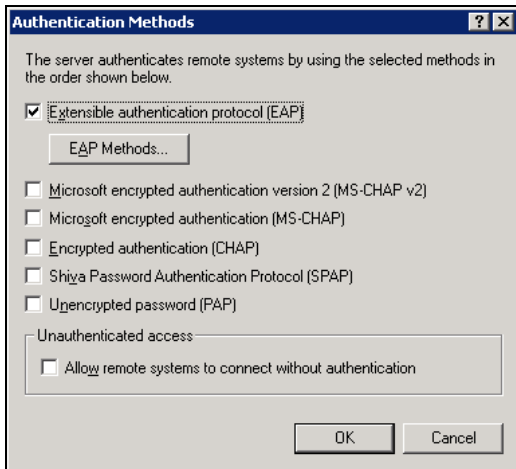
8. Next Confirm that your Firewall Policies and Network Rules are configured to allow your VPN Clients access to your internal network. As your VPN environment should already be in a working state, no changes should be necessary at this time.
12. Within the ISA Server Dashboard, click “Apply” to make changes recognized by the ISA Server and save this new rule to your Firewall configuration.



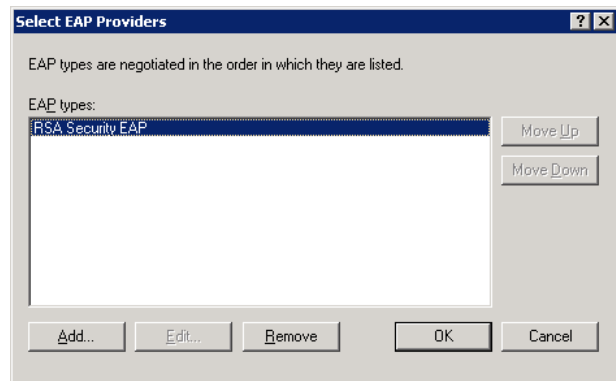
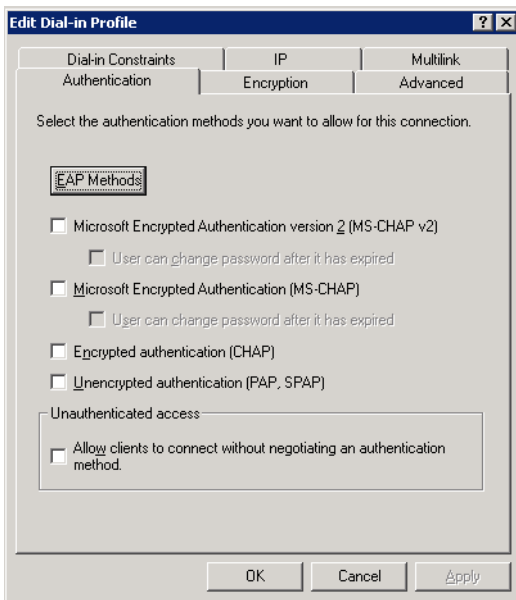
9. Open your Routing and Remote Access Administration Console.
10. Right click on your server object and select Properties.
11. After selecting the Security Tab, Verify that the Windows Authentication provider is selected and then click on Authentication Methods.



- 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.



- Click **OK** to save changes.
- From the Routing and Remote Access Administration Console, select **Remote Access Policies**.
- On the right side of the screen, right click **ISA Server Default Policy** and select **Properties**.
- From the settings dialog, select **Edit Profile**.
- Click the Authentication Tab and uncheck all options. Then select **EAP Methods**.
- When Selecting EAP Providers, your selection box will initially have no listing. Add the **RSA Security EAP Provider** by clicking **Add**.



- Click **OK** to save changes.

7. Certification Checklist

Date Tested: September 24, 2004

Product	Tested Version
RSA ACE/Server	5.2
RSA Authentication Manager	6.0
RSA ACE/Agent	5.6.1 ^(*)
ISA Server	2004

(*) See Known Issues

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

EF

Pass, Fail or N/A (N/A=Non-available function)

8. Known Issues

ISA Server 2004 compatibility with the RSA Security EAP Agent

1. Due to a known issue with the RSA ACE/Agent 5.6 EAP Component. The ISA Server 2004 VPN functionality was tested and certified using a patched version of the agent software.

To obtain the RSA ACE/Agent 5.6.1 maintenance build, please contact RSA Security Customer Support and reference tst00040883.

Troubleshooting communication with the RSA ACE/Server

If you receive an Access denied message, then check the Event viewer for the following error information.

1. "RSA ACE/Server is not responding"
If the error information details that the ISA Server is unable to communicate with the RSA ACE/Server, check that the RSA ACE/Server services are started and functioning correctly.
2. "Multi-homed host detected; Primary IP assumed is x.x.x.x."
If x.x.x.x is not the IP address on the ISA Server computer which is used to communicate with the RSA ACE server, you may need to add a registry value to change the communication address of the ISA Server. For more information on this workaround, please contact RSA Security Customer Support.
3. Persistent "Node Verification Failures"
A registry permissions issue has been reported where the ISA Server is not able to access the node secret information from the Windows System Registry. In order to correct this problem, you must modify the permissions on the following Registry Key:

<HKEY_LOCAL_MACHINE\SOFTWARE\SDTI>

For Windows 2000 – Add Read/Write Permissions for "Local System"

For Windows 2003 – Add Read/Write Permissions for "Network Service"

All Permission changes should be such that child nodes will inherit these changes.

Additional software required for installation of ISA Server 2004

These patches are required for installation on Windows 2000 platforms only. This information is current as of the publishing of the document. Please verify current requirements with Microsoft before attempting the installation and configuration of the ISA Server 2004 software.

Software	Version (Patch-level)
Internet Explorer	6.0 or later
Microsoft Hot Fix Q821887	Windows 2000 Only