



RSA SecurID Ready Implementation Guide

Last Modified: December 18, 2006

Partner Information

Product 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



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 APIs for strong authentication to hosted web content.

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	In Registry
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 2004 (SP1)	
CPU	550 MHz Pentium III or faster processor
Memory	256 Mb or more recommended
Storage	NTFS-formatted local partition with 150 MB of available hard-disk space; additional space required for web cache content

Operating System	
Platform	Required Patches
Windows 2000 Server	Service Pack 4
Windows Server 2003	

Additional Software Requirements	
Application	Additional Patches
ISA Server 2004	Service Pack 1
Internet Explorer	6.0 or later
Microsoft Hot Fix Q821887	Windows 2000 Only

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
- RADIUS Secret (When using RADIUS Authentication Protocol)

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 2004 Web Listeners

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.

- Configure and test connectivity with the RSA Authentication Manager
- Enable the SecurID Web Filter.
- Configure a web publishing rule for which authentication via RSA SecurID is required.
- Configure and test connectivity with the RSA Authentication Manager

Microsoft has included all of the necessary APIs to allow direct integration with the RSA Authentication Manager. No agent installation is necessary in order to achieve interoperability for Web based authentication to the ISA Firewall protected resources.

Configure and test connectivity with the RSA Authentication Manager

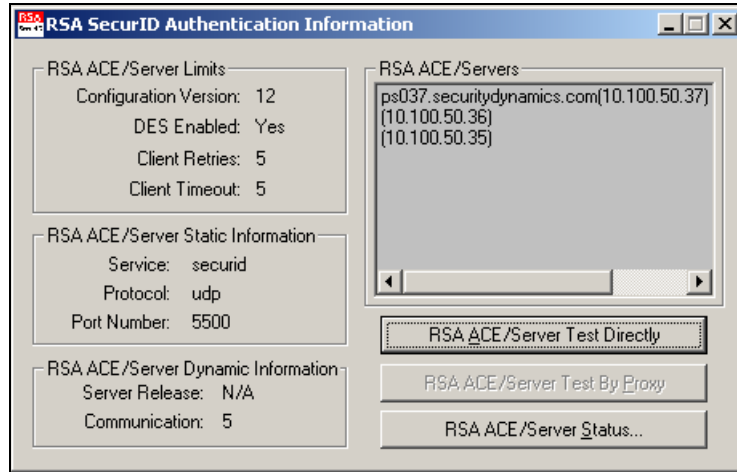
The Microsoft ISA Server includes a tool which you can use to verify that there is connectivity between the ISA Server computer and the RSA Authentication Manager computer. You can use this test client to verify connectivity, as well as establish the "Node Secret" used for encrypting communication with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

To test communication or test authentication with your RSA Authentication Manager, you must copy the RSA Test Authentication Utility from the tools directory on your ISA Server CD ROM to your ISA Server Program Directory.

1. Obtain the sdconf.rec file from your Authentication Manager Server, and save this file to the following location on the ISA Server Host: windir%\System32\
2. To run the sdtest.exe utility, type the following string from the Run or CMD prompt.

%Path to ISA installation directory%\sdtest.exe

3. In RSA SecurID Authentication Information dialog box, click RSA ACE/Server Test Directly.



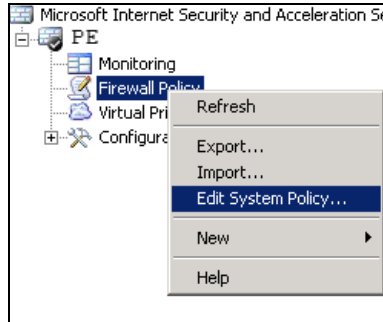
4. In RSA SecurID Authentication, type the User Name and the PASSCODE in appropriate fields.



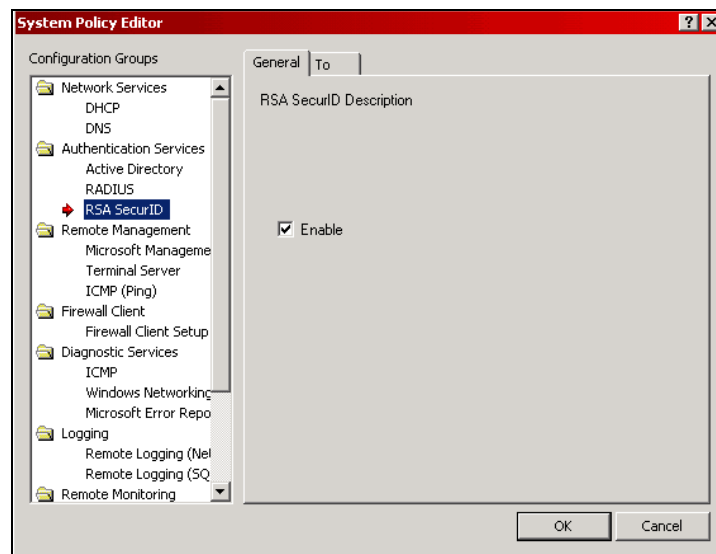
5. Your initial authentication will create the Node Secret within the Registry of your ISA Server.

Enable the SecurID Web Filter

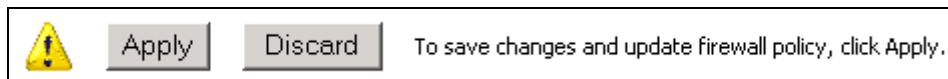
1. Open the ISA Server Management console.
2. Expand your ISA Server instance.
3. Right click on Firewall Policy. Choose Edit System Policy.




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. Clicking on the To tab, add the appropriate network to the allowed list to assure the ISA Server can communication with your Authentication Manager Servers.
7. Click "OK" to save your changes.



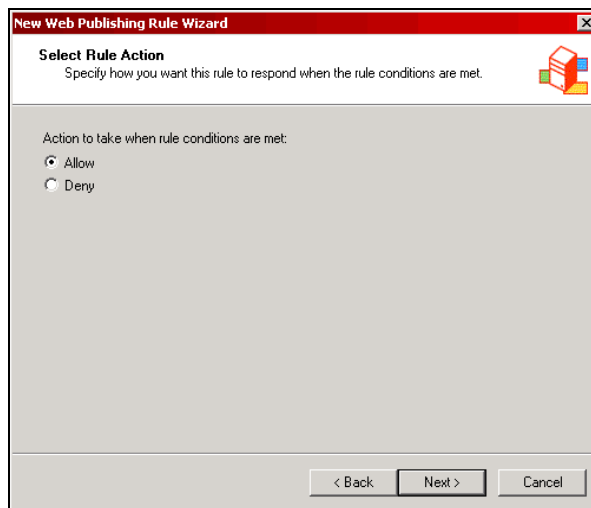
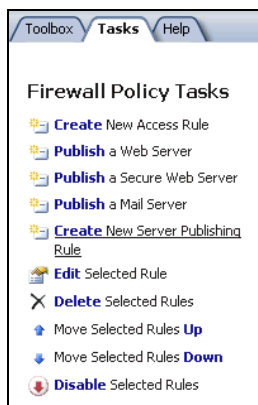
8. Within the Dashboard, Click Apply to save this change to your Firewall configuration.
9. Restart your ISA Server Firewall Services to apply these changes.



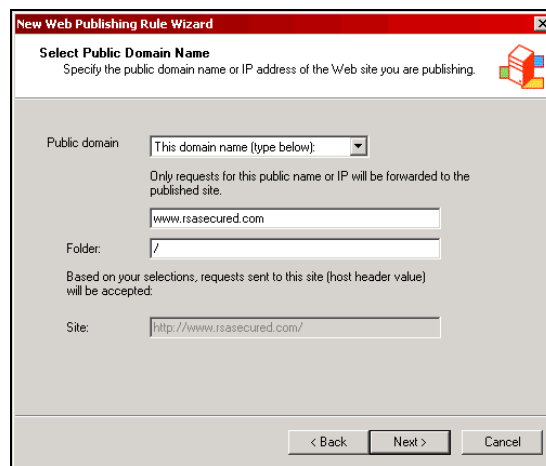
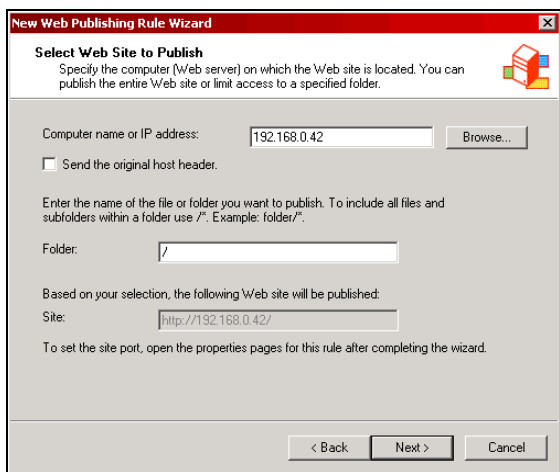
 **Note:** Once the ISA Server is configured to authenticate users with the SecurID method, you will have to restart the ISA Firewall services in order to load the "Node Secret" This restart also applies when removing and re-establishing the Node Secret with your RSA Authentication Manager.

Configure a Web Publishing rule with 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 Server Publishing Rule.
4. Enter the Name of the Web Publishing Rule.
5. Next select Rule Action as "Allow".

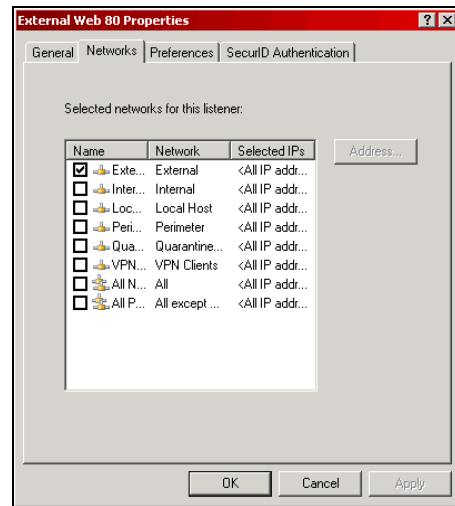
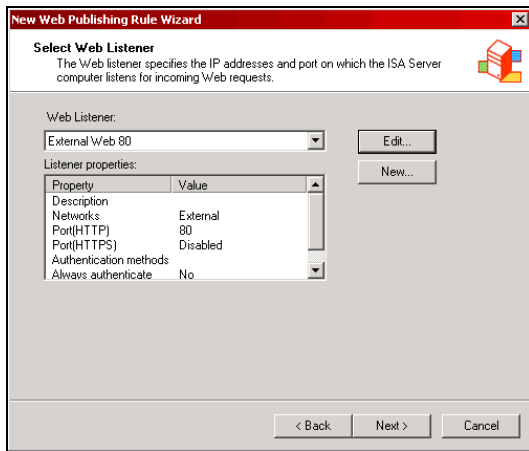


6. Enter the server information and folder you will be publishing with ISA Server 2004.
7. Enter domain information and folder information for published content.

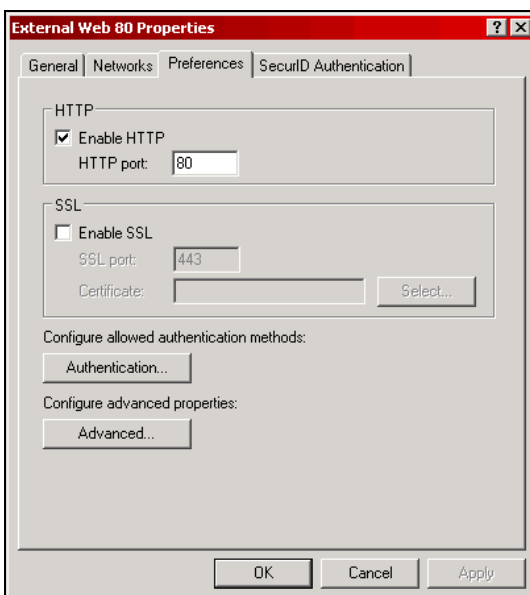


Select your Web Listener which will be used for hosting the Web Traffic.

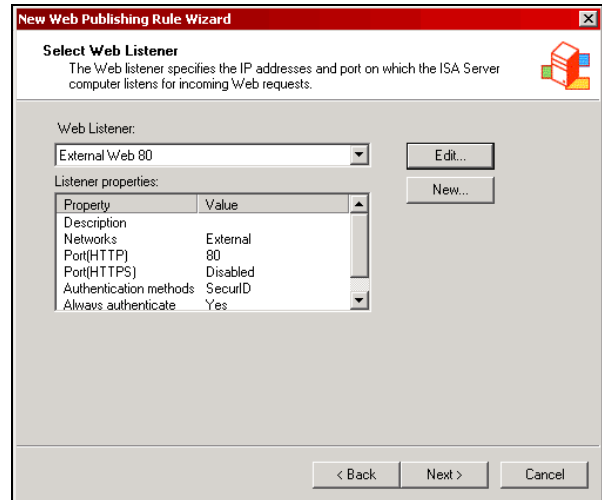
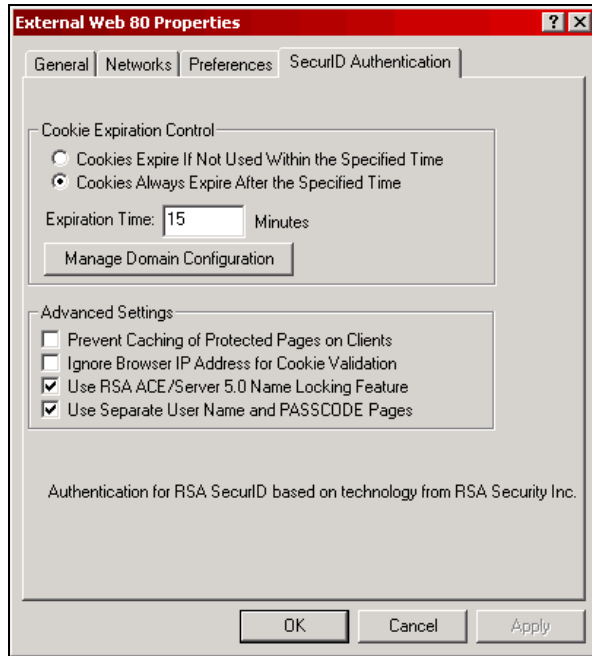
1. Click Edit to configure the Web Listener for SecurID Authentication.
2. From the Web Listener Properties dialog, click on the Networks tab.
3. Select the networks that the Web Listener will bind to, the selection will only refer to interfaces that will accept HTTP requests from end user desktops.



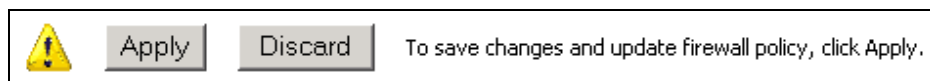
4. Click the Preferences Tab to configure HTTP Port, SSL Port and Authentication options.
5. Click the Authentication button to activate RSA SecurID as the authentication method.
6. From the list of authentication methods, select SecurID.
7. Click "Ask unauthorized users for identification".
8. Click "OK" to apply changes



9. To Modify the RSA SecurID Authentication options click on the SecurID Authentication tab within the Web Listener properties page.
10. Click “OK” to apply all changes to the Web Listener properties page and continue your Server Publishing rule configuration.
11. You should now see that the SecurID authentication method is enabled in the Web Listener. Click “Next” to continue with the configuration.



12. 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.
13. Click “Finish” to save the new Web Publishing Rule to the Dashboard.
14. 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

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, there is a message: "The page you are attempting to access requires you to authenticate using your SecurID token." followed by instructions: "Enter your User Name in the following field, and then click 'Send.' If you make a mistake, use 'Reset' to clear the field." The form contains a text input field labeled "Username:", and three buttons: "Send", "Reset", and "Cancel".

 **Note:** The RSA SecurID login screen will be different depending on whether the RSA name locking functionality is enabled. This is configured in the Agent Host record on the Authentication Manager and on the SecurID Authentication tab of the ISA Server Web Listener properties page.

Certification Checklist

Date Tested: September 27, 2005

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	6.1	Windows 2003 Server
ISA Server 2004	Standard Edition	Windows 2003 Server
ISA Server 2004	Enterprise Edition	Windows 2003 Server

Mandatory Functionality			
RSA Native Protocol		RADIUS Protocol	
New PIN Mode			
Force Authentication After New PIN	<input checked="" type="checkbox"/>	Force Authentication After New PIN	<input type="checkbox"/> N/A
System Generated PIN	<input checked="" type="checkbox"/>	System Generated PIN	<input type="checkbox"/> N/A
User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>	User Defined (4-8 Alphanumeric)	<input type="checkbox"/> N/A
User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>	User Defined (5-7 Numeric)	<input type="checkbox"/> N/A
User Selectable	<input checked="" type="checkbox"/>	User Selectable	<input type="checkbox"/> N/A
Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>	Deny 4 and 8 Digit PIN	<input type="checkbox"/> N/A
Deny Alphanumeric PIN	<input checked="" type="checkbox"/>	Deny Alphanumeric PIN	<input type="checkbox"/> N/A
PASSCODE			
16 Digit PASSCODE	<input checked="" type="checkbox"/>	16 Digit PASSCODE	<input type="checkbox"/> N/A
4 Digit Password	<input checked="" type="checkbox"/>	4 Digit Password	<input type="checkbox"/> N/A
Next Tokencode Mode			
Next Tokencode Mode	<input checked="" type="checkbox"/>	Next Tokencode Mode	<input type="checkbox"/> N/A
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	<input checked="" type="checkbox"/>	Failover	<input type="checkbox"/> N/A
Name Locking Enabled	<input checked="" type="checkbox"/>	Name Locking Enabled	<input type="checkbox"/>
No RSA Authentication Manager	<input checked="" type="checkbox"/>	No RSA Authentication Manager	<input type="checkbox"/> N/A
Additional Functionality			
RSA Software Token API Functionality			
System Generated PIN	<input type="checkbox"/> N/A	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
User Selectable	<input type="checkbox"/> N/A	User Selectable	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A
Domain Credential Functionality			
Determine Cached Credential State	<input type="checkbox"/> N/A	Determine Cached Credential State	<input type="checkbox"/>
Set Domain Credential	<input type="checkbox"/> N/A	Set Domain Credential	<input type="checkbox"/>
Retrieve Domain Credential	<input type="checkbox"/> N/A	Retrieve Domain Credential	<input type="checkbox"/>

EF

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

Known Issues

Troubleshooting Communications with ISA Server 2004

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

“RSA Authentication Manager is not responding”

If the error information details that the ISA Server is unable to communicate with the RSA Authentication Manager, check that the RSA Authentication Manager services are started and functioning correctly.

“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.

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 must also be applied to child nodes and values as well.