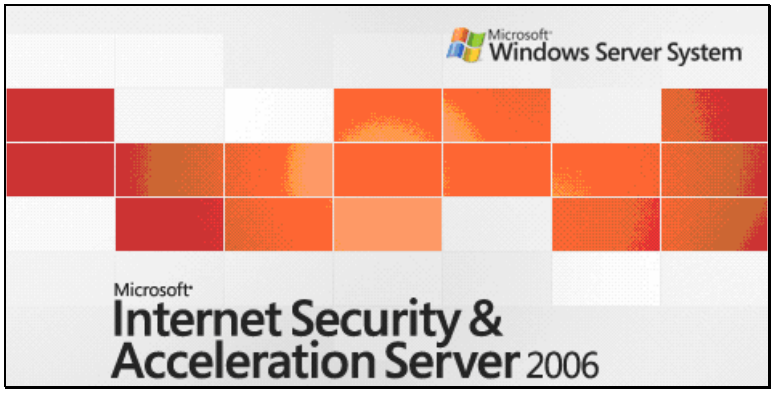
RSA SecurID Ready Implementation Guide

Last Modified: September 25, 2007

Partner Information

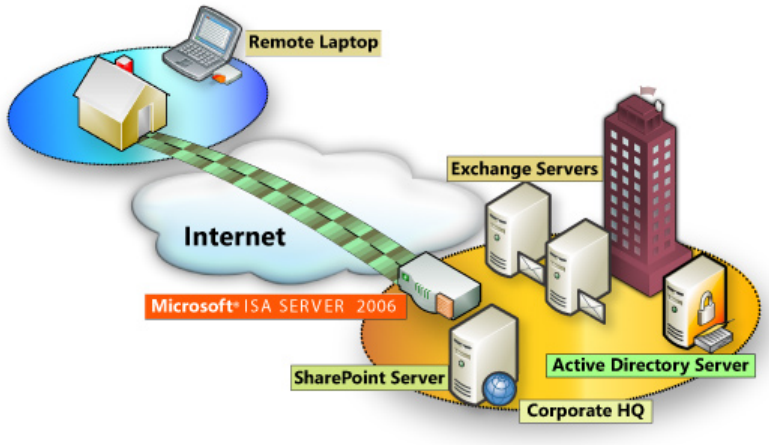
Product Information	
Partner Name	Microsoft
Web Site	http://www.microsoft.com/ISAServer
Product Name	Internet Security and Acceleration (ISA) Server
Version & Platform	2006
Product Description	ISA Server 2006 contains a full-featured, application-layer-aware firewall that helps protect organizations 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

Microsoft ISA Server 2006 supports Native RSA SecurID APIs for strong authentication to hosted web content. While ISA Server does not support RSA Security EAP authentication by default, this functionality can be added to the ISA Server by installing the RSA Authentication Agent software.

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	windows\system32
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

Test 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 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
- Configure Web Listener to use RSA SecurID for authentication
- Configure a Web Publishing Rule with RSA SecurID authentication
- Test the RSA SecurID authentication method for Web Listener

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.

Test connectivity with the RSA Authentication Manager

Microsoft has made available for download the RSA sdtest.exe utility which is used to verify connectivity between the ISA Server computer and the RSA Authentication Manager computer. It can be downloaded by clicking on this link:

http://www.microsoft.com/downloads/details.aspx?FamilyID=7b0ca409-55d0-4d33-bb3f-1ba4376d5737&DisplayLang=en

It is recommended that you download the RSA test utility and follow the instructions below before continuing.

Configure connectivity with the RSA Authentication Manager

Place the sdconf.rec in the following location: C:\Program Files\Microsoft ISA Server\sdconfig

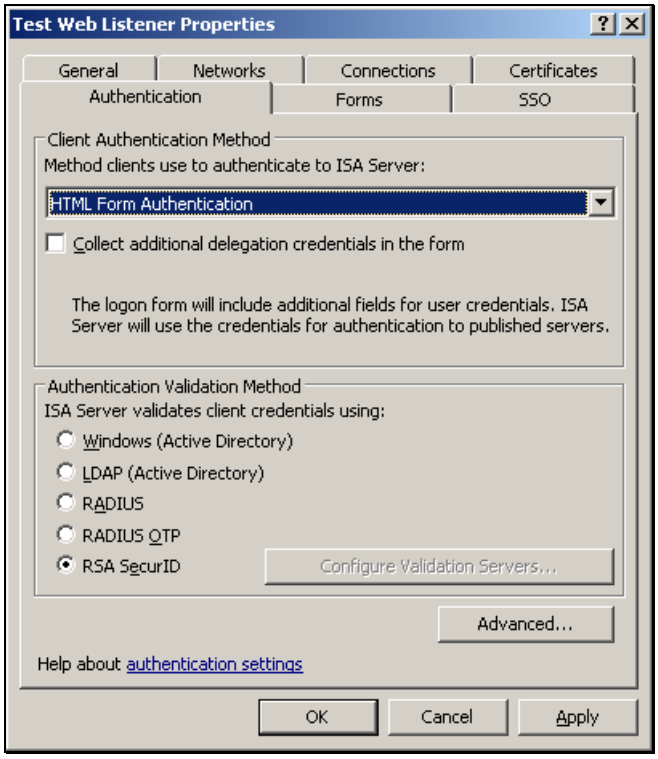
Important: Location of the sdconf.rec is different when using the RSA Test Authentication Utility versus configuring ISA Server 2006 for RSA SecurID authentication.

- RSA Test Authentication Utility: C:\WINDOWS\system32

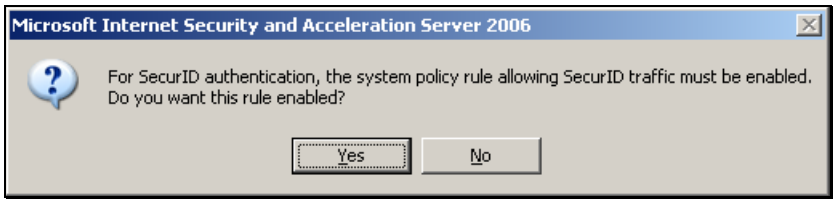
- Microsoft ISA Server 2006: C:\Program Files\Microsoft ISA Server\sdconfig

Configure Web Listener to use RSA SecurID for authentication

1. Open ISA Server Management. Start > All Programs > Microsoft ISA Server > ISA Server Management.
2. Expand Microsoft Internet Security and Acceleration Server 2006, expand <Server_Name>, and then click Firewall Policy.
3. On the Toolbox tab, click Network Objects.
4. Expand Web Listeners, and then click the applicable Web listener (or create a new one).
5. On the toolbar beneath Network Objects, click Edit.
6. Click the Authentication tab.



7. In Client Authentication Method, select HTML Form Authentication.
8. In Authentication Validation Method, click RSA SecurID.
9. Click OK, then Yes to the following prompt:

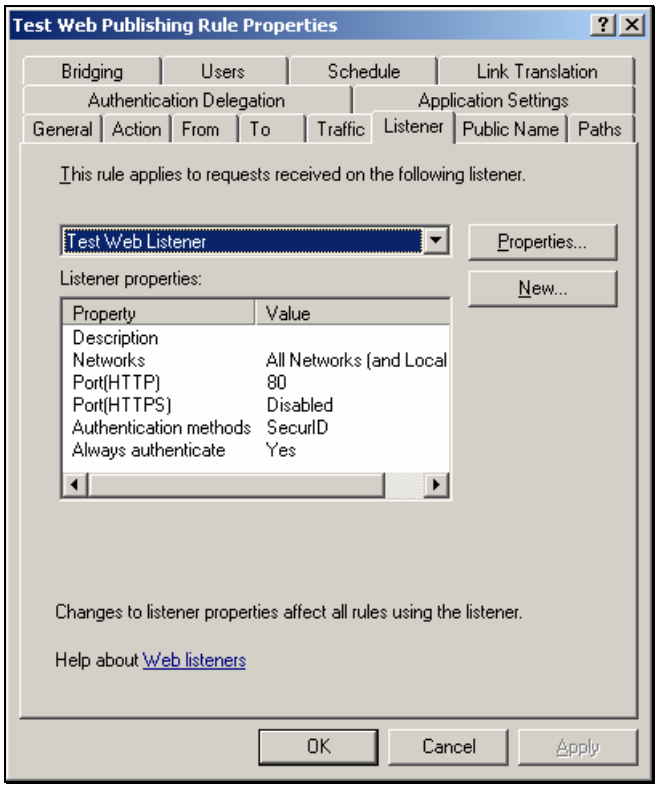


Configure a Web Publishing Rule with RSA SecurID authentication

1. Open the ISA Server Management console and expand your ISA Server instance.
2. Click on Firewall Policy.
3. From the ISA Server Dashboard Tasks list choose Publish Web Sites.
4. Enter the Name of the Web Publishing Rule.
5. Next select Rule Action as Allow.
6. Select the Publishing Type specific to your scenario.
7. Select the Server Connection Security specific to your scenario.

> **Important: Authentication over HTTP is disabled by default (only authentication over HTTPS is allowed). To change this, check the box under "Web Listener Properties" – "Authentication" – "Advanced" – "Allow client authentication.**

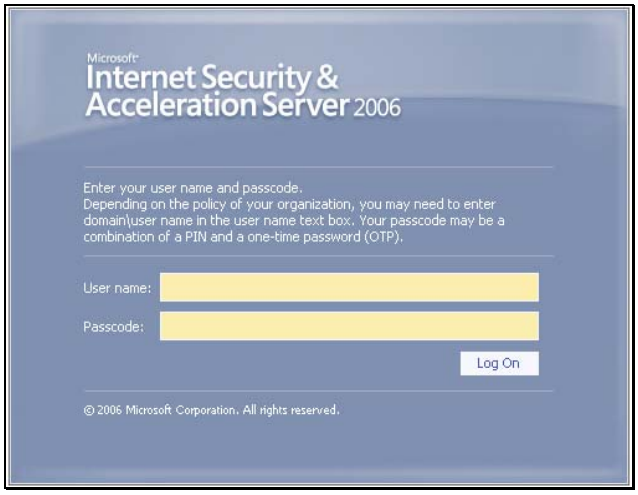
8. Enter the Internal Publishing Details specific to your scenario.
9. Enter the Public Name Details specific to your scenario.
10. Select the Web Listener that you previously configured to use RSA SecurID authentication.



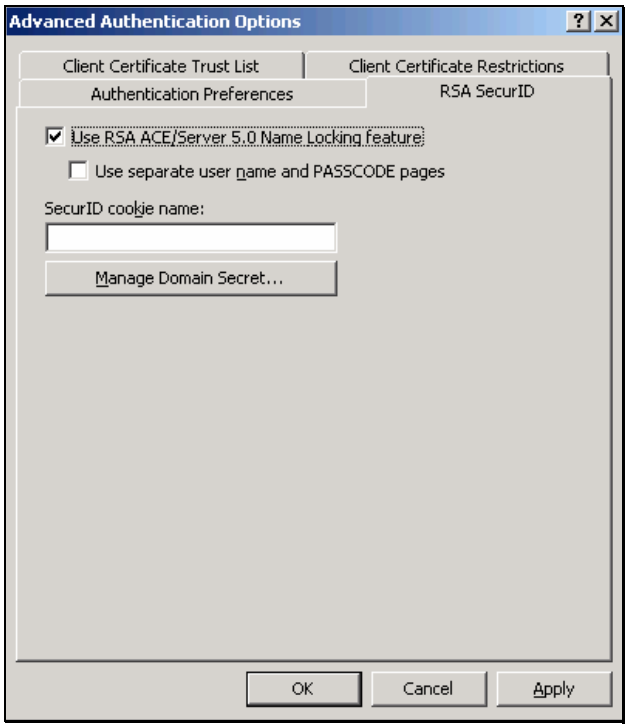
11. Select the Web Listener that you previously configured to use RSA SecurID authentication.
12. Select the Authentication Delegation specific to your scenario.
13. Select the User Set specific to your scenario.
14. Finished.

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 User name and Passcode as directed to login to the ISA Server hosted web content.



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



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

* ISA Server 2006 correctly enforces the functionality; however, the PIN parameters are not displayed to the user. This issue has been reported to Microsoft.

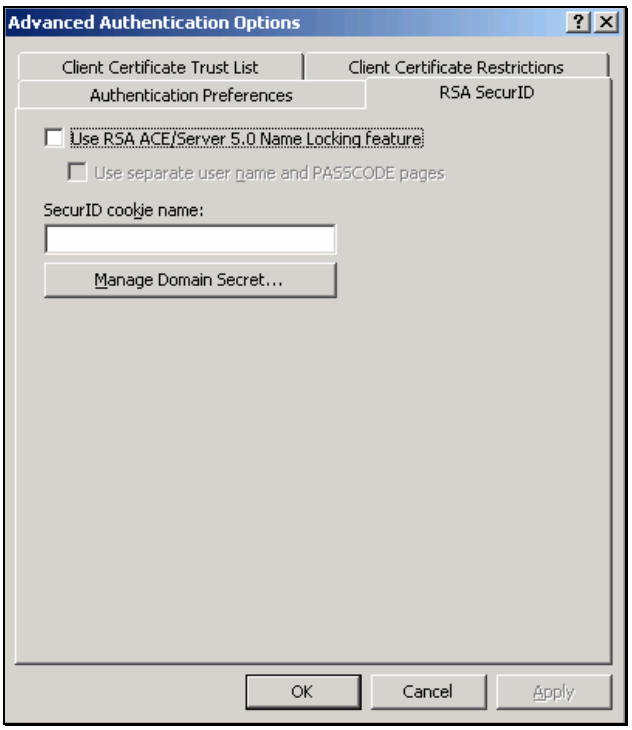
Known Issues

- Authentication over HTTP is disabled by default (only authentication over HTTPS is allowed). If you want to change this, there is a checkbox under “Web Listener Properties” – “Authentication” – “Advanced” – “Allow client authentication over HTTP”.
- ISA Server 2006 also supports RADIUS and RADIUS OTP authentication. Both were tested against RSA RADIUS and found to not support New Pin and Next Tokencode mode functionality.

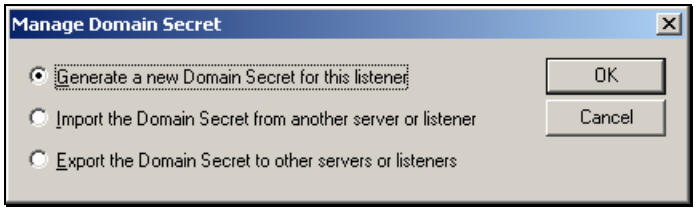
Appendix

To create, import, or export a domain secret for RSA SecurID authentication

1. Open ISA Server Management. Click Start, point to All Programs, point to Microsoft ISA Server, and then click ISA Server Management.
2. Expand Microsoft Internet Security and Acceleration Server 2006, expand <Server_Name>, and then click Firewall Policy.
3. On the Toolbox tab, click Network Objects.
4. Expand Web Listeners, and then click the applicable Web listener.
5. On the toolbar beneath Network Objects, click Edit.
6. Click the Authentication tab.
7. Click Advanced.
8. Click on the RSA SecurID tab.

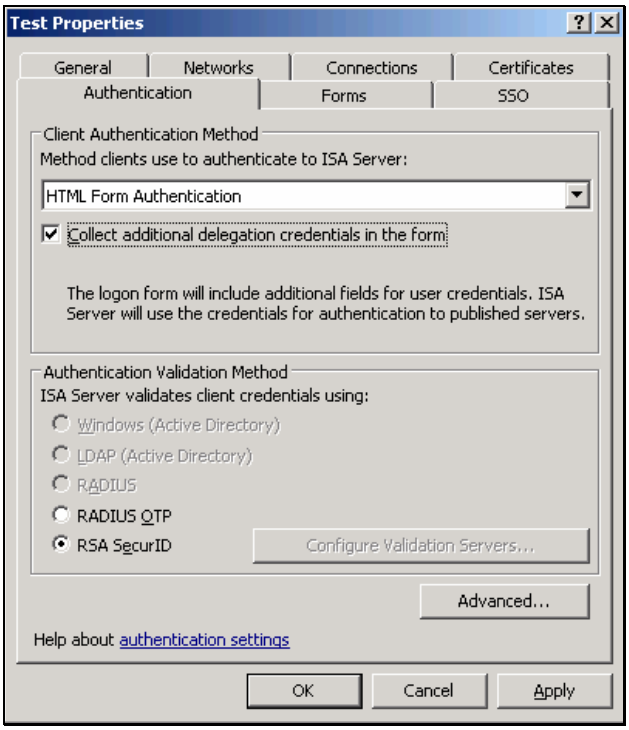


9. In SecurID cookie name, type a name for the domain's cookies (for example, mscookie).
10. Click Manage Domain Secret to create, import, or export a domain secret.

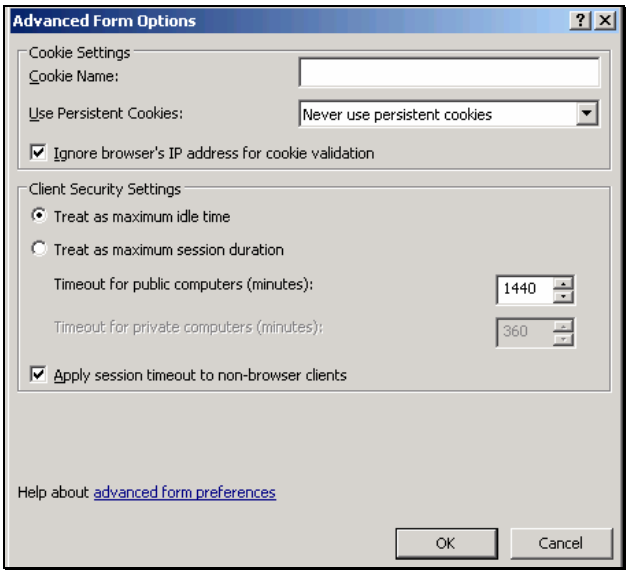


Authentication Delegation

1. Open ISA Server Management. Click Start, point to All Programs, point to Microsoft ISA Server, and then click ISA Server Management.
2. Expand Microsoft Internet Security and Acceleration Server 2006, expand <Server_Name>, and then click Firewall Policy.
3. On the Toolbox tab, click Network Objects.
4. Expand Web Listeners, and then click the applicable Web listener.
5. On the toolbar beneath Network Objects, click Edit.
6. Select the Authentication tab and if not already set, change the Client Authentication Method to HTML Form Authentication.
7. Set the Collect additional delegation credentials in the form by checking the appropriate box.
8. Set the Authentication Validation Method by checking the RSA SecurID option.



9. Select the Forms tab from the Listener properties and click the Advanced button.
10. By default cookies will timeout after 10 minutes resulting in the clients being prompted by the system after minutes of inactivity. To extend this timeout value modify the Client Security Settings, Timeout for public computers. The maximum value is 1440 minutes which equates to one day.



11. Click the OK button once you have set the maximum idle time in minutes and select the SSO tab.
12. On the SSO tab enable Single Sign On and specify the same fully qualified domain name used to configure the Web agent.