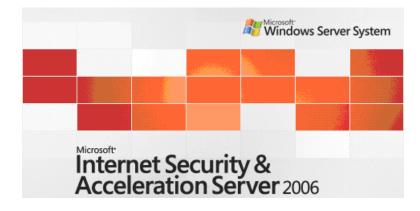


RSA SecurID Ready Implementation Guide

Last Modified: December 18, 2006

Partner Information

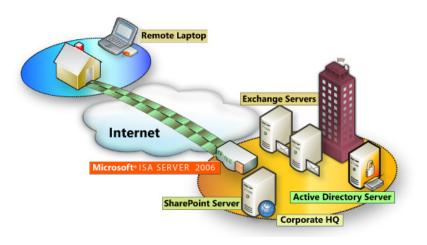
Product Information		
Partner Name	Microsoft	
Web Site	http://www.microsoft.com/ISAServer	
Product Name	Internet Security and Acceleration (ISA) Server	
Version & Platform	2006	
Product Description		
Product Category	Perimeter Defense (Firewalls, VPNs & Intrusion Detection)	





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 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 availal hard-disk space; additional space required for web carbon 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.

New Access Rule Wizard				
Microsoft Internet Security & Acceleration Server 2006	Welcome to the New Access Rule Wizard This wizard helps you create a new access rule. Access rules define the action that is taken, and the protocols that may be used, when specified clients from one network attempt to access specific destinations or content on another network.			
	Access rule name: Allow RSA SecurID To continue, click Next.			
	< <u>B</u> ack. <u>N</u> ext > Cancel			



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

New Access Rule Wizard	×
Rule Action Select how client requests for content from the specified destination are dealt with if the conditions specified in the rule are met.	
Action to take when rule conditions are met: Allow Deny	
< <u>B</u> ack <u>N</u> ext>	Cancel

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

New Access Rule Wizard		x
Protocols Select the protocols this rule applies to.		
<u>I</u> his rule applies to:		
Selected protocols		
Protocols:		Add Edit Remo <u>v</u> e
		Po <u>r</u> ts
	< <u>B</u> ack <u>N</u> e	ext > Cancel

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



	Protocols:		
	New - Edit Delete		
	RIP Rlogin RPC (all interfaces) RPC Server (all interfaces) RTSP RTSP SMTP SMTP SMTP Server SMTPS SMTPS SMTPS SMTPS SMTPS SMTPS SMTP SMTP		
	I Telnet Server	-	
	Add Close		
Access Rule Wiz	ard		
Protocols	cols this rule applies to.		
[his rule applies to:			
Selected protocols			•
Protocols:			
SecurID			<u>A</u> dd
		_	<u>E</u> dit
			Remo <u>v</u> e
		_	
			Po <u>r</u> ts

- 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



New Access Rule Wizard	×
Access Rule Sources This rule will apply to traffic originating from the sources specified in this p	bage.
This rule applies to traffic from these sources:	
🕹 Local Host	<u>A</u> dd
	<u>E</u> dit
	<u>R</u> emove
< <u>₿</u> ack <u>N</u> ext>	Cancel

w Access Rule Wizard	×
Access Rule Destinations This rule will apply to traffic sent from the rule sources to the destinations in this page.	specified
This rule applies to traffic sent to these destinations:	
Internal	<u>A</u> dd
VPN Clients	<u>E</u> dit
	<u>R</u> emove
1	
< <u>B</u> ack <u>N</u> ext>	Cancel

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



w Access Rule Wizard User Sets	
You can apply the rule to requests from all users. Or, you can limit acces specific user sets.	is to
This rule applies to requests from the following user sets:	
All Users	<u>A</u> dd
	<u>E</u> dit
	<u>R</u> emove
1	
< <u>B</u> ack <u>N</u> ext >	Cancel

- 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.

	Apply	Discard	To save changes and update the configuration, click Apply.
•			

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.
- When prompted for Component information, choose Remote Access Authentication (Server) and RSA Security EAP Client.



🔂 RSA Authentication Agent for Windows	×
Custom Setup Select the components you want to install.	RSA SECURITY
To change how a feature is installed, click an icon in the follow	ing list. Component Description This component enables a workstation to prompt for RSA SecurID logon credentials before opening a remote connection. This component requires 9357KB on your hard drive.
InstallShield	Next > Cancel

- 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 \rightarrow Test Authentication.
- In RSA SecurID Authentication Information dialog box, click RSA ACE/Server Test Directly.
 In RSA SecurID Authentication, type the User Name and the PASSCODE in appropriate fields.

Log On with R5A SecurID		
RS/	SecurID [®]	
If you have more	than one token, choose which token to use.	
Choose Token		
T <u>o</u> ken type:	Key fob or metal card	
Log On-	rr RSA SecurID passcode.	
<u>U</u> ser name: Passcode:	Administrator	
	OK Cancel	



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.





VPN Clients Properties	? ×
General Groups Protocols User Mapping	
Enable VPN client access	
Maximum number of VPN clients allowed:	
OK Cancel	Apply

- Proceed to the next step and choose Specify Windows Users.
 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.

VPN Client	s Propertie	5		<u>? ×</u>
General	Groups Pr	otocols User Ma	apping	
<u>S</u> elect	the domain g	roups for which re	mote access is allo	wed:
Nar	nespace	Group	Domain	Add
	Windows	VPN Users	PS020	<u>H</u> emove
i	VPN acce	ss (dial-in options) cess policy.'' If thi:	these domain grou set to ''Control acc s option is not avail	ess through
		OK	Cancel	Apply



- 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.

P5020 (local) Properties	×
General Security IP PPP Logging	
The authentication provider validates credentials for remote access clients and demand-dial routers.	
Authentication provider:	
Windows Authentication Configure	
Authentication Methods The accounting provider maintains a log of connection requests and sessions.	
Accounting provider:	
<none> Configure</none>	
The custom IPSec policy specifies a pre-shared key for L2TP connections. The Routing and Remote Access service should be started to set this option.	
Allow custom IPSec policy for L2TP connection	
Pre-shared <u>K</u> ey:	
OK Cancel Apply	

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.



Authentication Methods
The server authenticates remote systems by using the selected methods in the order shown below.
Extensible authentication protocol (EAP)
EAP Methods
Microsoft encrypted authentication version 2 (MS-CHAP v2) Microsoft encrypted authentication (MS-CHAP)
Encrypted authentication (CHAP)
Shiva Password Authentication Protocol (SPAP)
Unencrypted password (PAP)
Unauthenticated access
Allow remote systems to connect without authentication
OK Cancel
EAP Methods
EAP Methods The Extensible Authentication Protocol (EAP) extends the authentication methods available for Point-to-Point Protocol (PPP) connections.
The Extensible Authentication Protocol (EAP) extends the authentication
The Extensible Authentication Protocol (EAP) extends the authentication methods available for Point-to-Point Protocol (PPP) connections. EAP methods are configured through remote access policies. This server
The Extensible Authentication Protocol (EAP) extends the authentication methods available for Point-to-Point Protocol (PPP) connections. EAP methods are configured through remote access policies. This server has the following EAP methods installed. <u>Methods:</u> MD5-Challenge
The Extensible Authentication Protocol (EAP) extends the authentication methods available for Point-to-Point Protocol (PPP) connections. EAP methods are configured through remote access policies. This server has the following EAP methods installed. <u>Methods:</u> MD5-Challenge Protected EAP (PEAP) RSA EAP - Protected OTP
The Extensible Authentication Protocol (EAP) extends the authentication methods available for Point-to-Point Protocol (PPP) connections. EAP methods are configured through remote access policies. This server has the following EAP methods installed. <u>Methods:</u> MD5-Challenge Protected EAP (PEAP)
The Extensible Authentication Protocol (EAP) extends the authentication methods available for Point-to-Point Protocol (PPP) connections. EAP methods are configured through remote access policies. This server has the following EAP methods installed. <u>Methods:</u> MD5-Challenge Protected EAP (PEAP) RSA EAP - Protected OTP
The Extensible Authentication Protocol (EAP) extends the authentication methods available for Point-to-Point Protocol (PPP) connections. EAP methods are configured through remote access policies. This server has the following EAP methods installed. <u>Methods:</u> MD5-Challenge Protected EAP (PEAP) RSA EAP - Protected OTP
The Extensible Authentication Protocol (EAP) extends the authentication methods available for Point-to-Point Protocol (PPP) connections. EAP methods are configured through remote access policies. This server has the following EAP methods installed. <u>Methods:</u> MD5-Challenge Protected EAP (PEAP) RSA EAP - Protected OTP
The Extensible Authentication Protocol (EAP) extends the authentication methods available for Point-to-Point Protocol (PPP) connections. EAP methods are configured through remote access policies. This server has the following EAP methods installed. <u>Methods:</u> MD5-Challenge Protected EAP (PEAP) RSA EAP - Protected OTP
The Extensible Authentication Protocol (EAP) extends the authentication methods available for Point-to-Point Protocol (PPP) connections. EAP methods are configured through remote access policies. This server has the following EAP methods installed. <u>Methods:</u> MD5-Challenge Protected EAP (PEAP) RSA EAP - Protected OTP
The Extensible Authentication Protocol (EAP) extends the authentication methods available for Point-to-Point Protocol (PPP) connections. EAP methods are configured through remote access policies. This server has the following EAP methods installed. <u>Methods:</u> MD5-Challenge Protected EAP (PEAP) RSA EAP - Protected OTP

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



ERouting and Remote Access			
<u>File Action View H</u> elp			
Routing and Remote Access	Remote Access Policies		
Server Status	Name	Order	
🖻 🖷 🔂 P5020 (local)	SISA Server Default Policy	1	
Remote Access Clients (0)	Sconnections to Microsoft Routing and Remote .	2	
Ports	S Connections to other access servers	3	
Network Interfaces Remote Access Clients (0) Ports IP Routing			
Remote Access Policies			
🗄 💼 Remote Access Logging			
•			

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

ISA Server Default Policy Properties	<u>?</u> ×
Settings	
Specify the conditions that connection requests must match.	
Policy <u>c</u> onditions:	
Windows-Groups matches "PS020\VPN Users"	
Add Edit <u>R</u> emove If connection requests match the conditions specified in this policy, the	
associated profile will be applied to the connection.	
Edit <u>P</u> rofile	
Unless individual access permissions are specified in the user profile, this policy controls access to the network.	s
If a connection request matches the specified conditions: O De <u>n</u> y remote access permission	
• Grant remote access permission	
OK Cancel App	dy

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



dit Dial-in Profile			?×
Dial-in Constraints	IP		Multilink
Authentication	Encryption	ן ו	Advanced
Select the authentication meth	ods you want	to allow f	ior this connection.
EAP Methods			
Microsoft Encrypted Auth	nentication ve	rsion <u>2</u> (N	IS-CHAP v2)
📕 User can <u>c</u> hange i	password afte	er it has e	xpired
Microsoft Encrypted Auth	nentication (M	S-CHAP)	
🔲 Uger can change i	password afte	er it has e	xpired
Encrypted authentication	(CHAP)		
Unencrypted authenticat	ion (PAP, SP	AP)	
Unauthenticated access			
□ Allow clients to connect method.	without negot	iating an	authentication
	ОК	Car	ncel <u>A</u> pply

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.

Select EAP Providers	<u>?</u> ×
EAP types are negotiated in the order in which they are listed.	
EA <u>P</u> types:	
RSA EAP - Protected OTP	Move <u>U</u> p Move <u>D</u> own
Add Edit <u>R</u> emove OK	Cancel

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.



ew Connection Wizard
Network Connection Type What do you want to do?
Connect to the Internet Connect to the Internet so you can browse the Web and read email.
Connect to the network at my workplace Connect to a business network (using dial-up or VPN) so you can work from home, a field office, or another location.
Set up an advanced connection Connect directly to another computer using your serial, parallel, or infrared port, or set up this computer so that other computers can connect to it.
< <u>B</u> ack <u>N</u> ext > Cancel

3. Choose Virtual Private Network connection

New Connection Wizard
Network Connection How do you want to connect to the network at your workplace?
Create the following connection:
O Dial-up connection
Connect using a modem and a regular phone line or an Integrated Services Digital Network (ISDN) phone line.
<u>Virtual Private Network connection</u>
Connect to the network using a virtual private network (VPN) connection over the Internet.
< <u>B</u> ack <u>N</u> ext> Cancel

4. Define Connection name



New Connection Wizard
Connection Name Specify a name for this connection to your workplace.
Type a name for this connection in the following box. Company N <u>a</u> me
RSA
For example, you could type the name of your workplace or the name of a server you will connect to.
< <u>B</u> ack <u>N</u> ext > Cancel

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

New Connection Wizard	
VPN Server Selection What is the name or address of the VPN server?	T)
Type the host name or Internet Protocol (IP) address of the computer to which you are connecting.	
Host name or IP address (for example, microsoft.com or 157.54.0.1): 192.168.78.31]
< Back Next > Can	cel 1

6. Connection Availability



New Connection Wizard
Connection Availability You can make the new connection available to any user or only to yourself.
A connection that is created for your use only is saved in your user account and is not available unless you are logged on.
Create this connection for:
○ Anyone's use
My use only
< <u>B</u> ack <u>N</u> ext > Cancel

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

Connect RSA			? ×
		2	X
<u>U</u> ser name: <u>P</u> assword:			
Me only	er name and passw		ing users:
<u>C</u> onnect	Cancel	Pr <u>o</u> perties	<u>H</u> elp

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



R5A Properties
General Options Security Networking Advanced
Security options <u> </u>
⊻alidate 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 <u>Settings</u>
I <u>P</u> Sec Settings
OK Cancel

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.

Advanced Security Settings
Data encryption:
Require encryption (disconnect if server declines)
C Logon security
Use Extensible Authentication Protocol (EAP)
RSA EAP - Protected OTP (encryption enabled)
Properties
C 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
Mjcrosoft CHAP Version 2 (MS-CHAP v2)
Eor MS-CHAP based protocols, automatically use my
Windows logon name and password (and domain if any)
OK Cancel

11. Example of prompt



Log On with RSA Sec	urID	
RSA	SecurID®	with RSA [®] Security Center
S S	for Microsoft® Windows®	
		© Copyright 2005 RSA Security Inc.
_		
Select your authentic	ator from a drop-down menu.	
Choose Authentical	tor	
Authopticstow		
<u>A</u> uthenticator:	Key fob, standard card, PINPad	<u> </u>
Log On		
-	RSA SecurID passcode.	
Log on with your		
<u>U</u> ser name:	mrennie	
Passcode:	•••••	
L		
		OK Cancel



Certification Checklist

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			

Date Tested: November 6, 2006

Ν	landatory	y Functionality	
RSA Native Protocol RADIUS Protocol			
New PIN Mode			
Force Authentication After New PIN	\checkmark	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	\checkmark	No RSA Authentication Manager	N/A
	Additiona	I 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 \checkmark = Pass \times = Fail N/A = Non-Available Function			

