



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 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 of VPN Users
- Install RSA Authentication Agent for Microsoft Windows 6.0
- Test connectivity between the RSA Authentication Manager and ISA Server
- Configure the VPN Server to use the RSA EAP Authentication Method

Before you begin configuration of the ISA Server or RSA Authentication Agent, you must first create a Firewall Access Rule to allow communication from the ISA Server to your VPN Client and the RSA Authentication Manager 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.

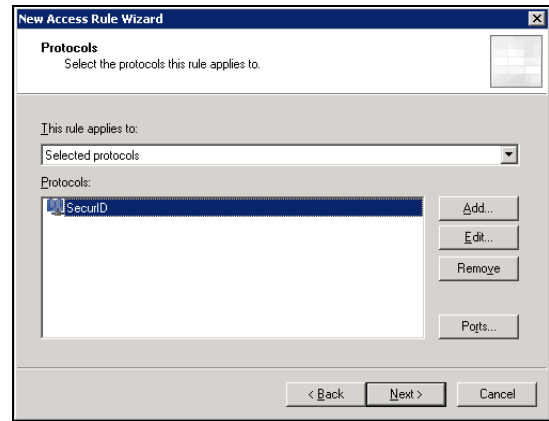
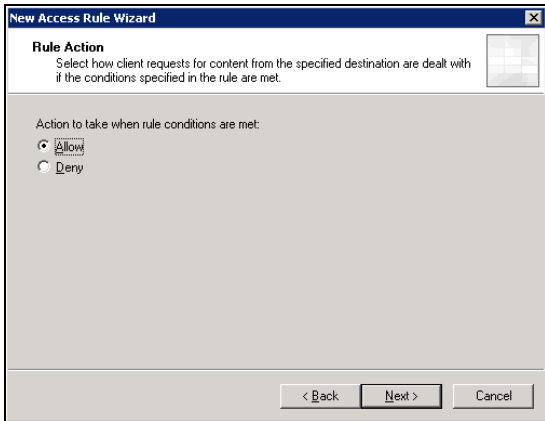
VPN Client Configuration

The ISA Server 2004 VPN Service requires the use of the RSA Authentication Agent for Microsoft Windows 6.0 for interoperability. Due to this fact the VPN Client must also have the RSA Authentication Agent for Microsoft Windows 6.0 EAP Component installed for interoperability to take place.

For installation and configuration instructions for VPN Clients, please refer to the RSA Authentication Agent documentation included with the product.

Create a Firewall Access Rule for RSA SecurID Authentication

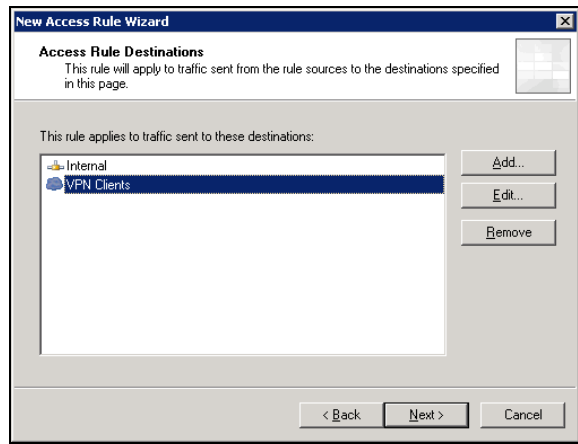
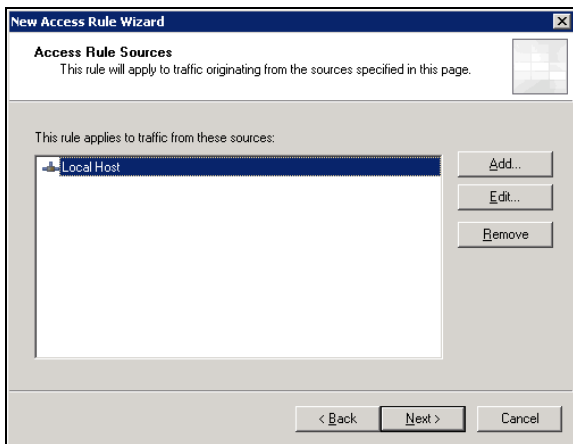
1. Open the ISA Server Management console and expand your ISA Server instance.
2. Click on Firewall Policy.
3. From the ISA Server Dashboard Task list choose Create New Access Rule.
4. Enter the Name of the New Access Rule.
5. Action to take when conditions are met should be set to Allow.
6. On the Protocol 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.



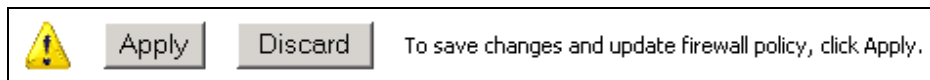
8. On the next two screens you will be asked to specify the Source and Destination hosts for your new Access Rule. Select the following objects by clicking the Add button and expanding the Networks container.

Access Rule Sources: Select: Local Host

Access Rule Destinations: Internal + VPN Clients



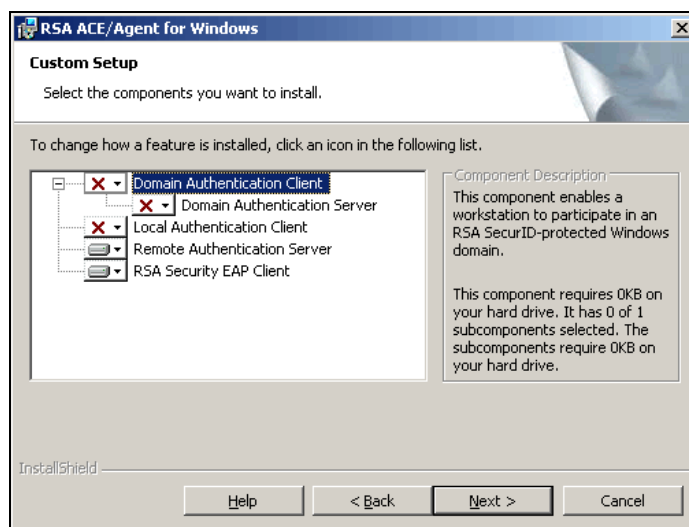
9. When prompted to select User Sets for this Access Rule, leave the default value of All Users.
10. Review your settings and click Finish to save this Access Rule to your ISA Firewall Console.
11. Within the Dashboard, click "Apply" to make changes recognized by the ISA Server and save this new rule to your Firewall configuration.



Installation of the RSA Authentication Agent 6.0 EAP Components

In order to configure RSA SecurID Authentication for ISA Server 2004 VPN Users, you must install and configure an RSA Authentication 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.

12. Install the RSA Authentication Agent for Microsoft Windows 6.0 following all prompts.
13. When prompted for Component information, choose Remote Access Authentication (Server) and RSA EAP Client.




14. Continue through prompts and provide your sdconf.rec file from your RSA Authentication Manager.
15. You must reboot your ISA Server once the installation has completed.

Test connectivity with the RSA Authentication Manager

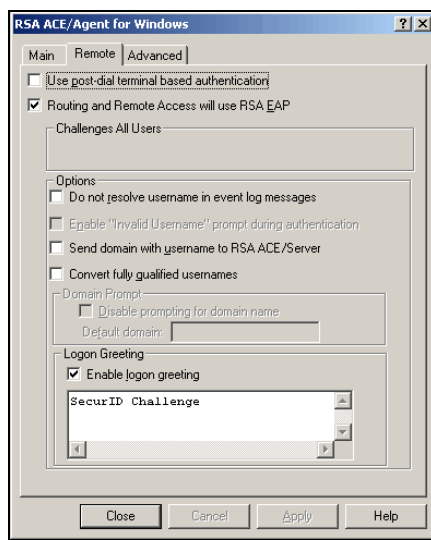
To test communication or test authentication with your RSA Authentication Manager, run the sdtest.exe utility. This utility is included in your RSA Authentication Agent installation and can be accessed through the Start Menu as shown below.

16. From the Start Menu, expand RSA ACE/Agent → Test Authentication.
17. In RSA SecurID Authentication Information dialog box, click RSA ACE/Server Test Directly.
18. 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.

19. Open the RSA Authentication Agent Control Panel application and select the Remote tab.
20. Enable "Routing and Remote Access will use RSA EAP" and click Apply.



21. Restart your Microsoft Firewall Service to apply changes.

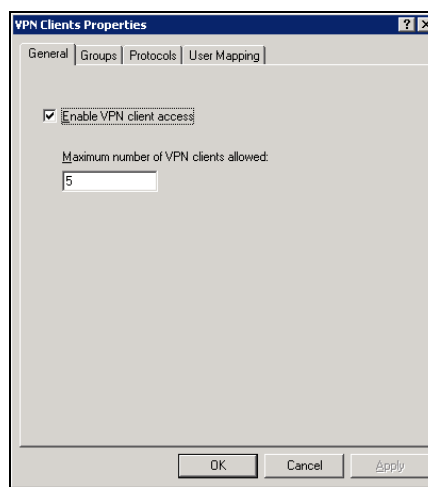
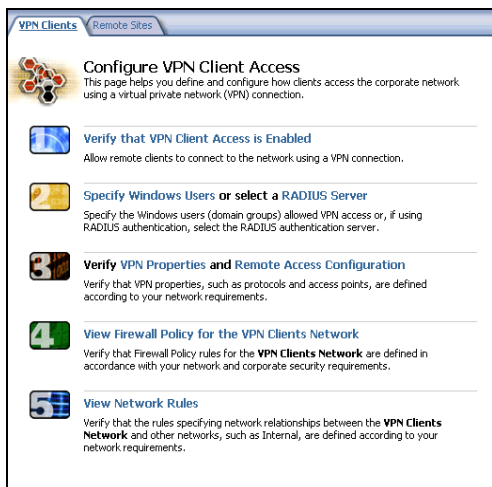
 **Note:** Restarting your Microsoft Firewall Service will also restart your Routing and Remote Access Services as well.

Configure the VPN Server to use the RSA EAP Authentication Method

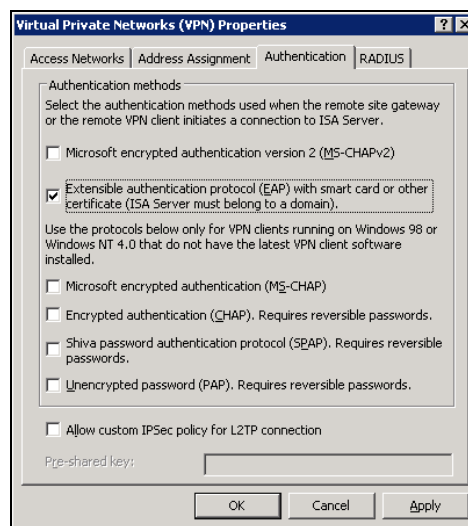
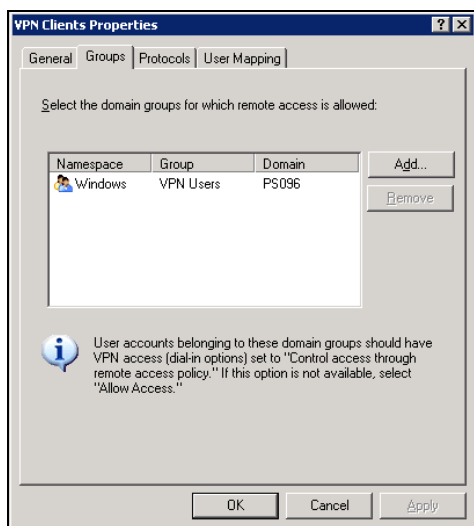
The VPN Server is configured in two different steps. For the following steps you will need access to both the ISA Management Console as well as the MMC interface for the Routing and Remote Access Service.

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.

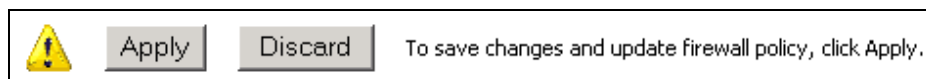
1. Open ISA Server Management and select Virtual Private Networks (VPN).
2. Select Verify that VPN Client Access is Enabled, assure the selection is checked, and click OK.



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

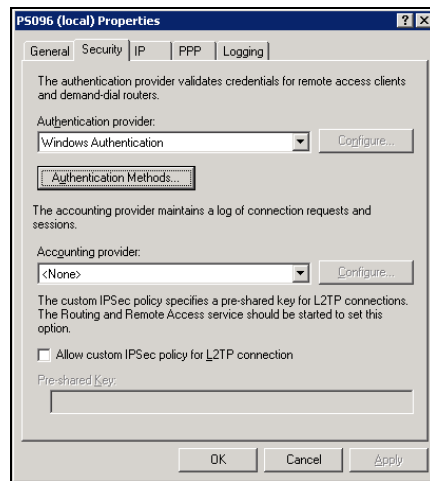


- Next confirm that your Firewall Policies and Network Rules are configured to allow your VPN Clients access to your internal network. As your VPN environment should already be in a working state, no changes should be necessary at this time.
- Within the ISA Server Dashboard, click "Apply" to make changes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

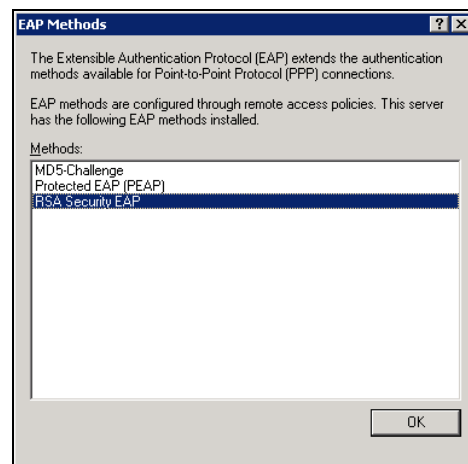
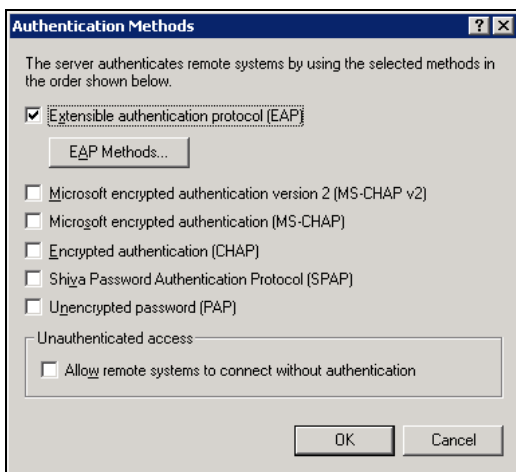


- Next open the Routing and Remote Access Administration Console.

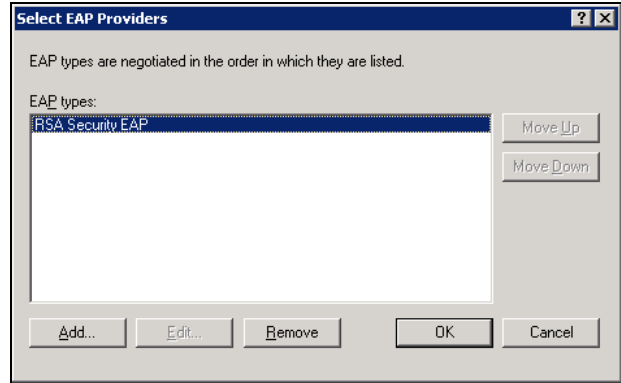
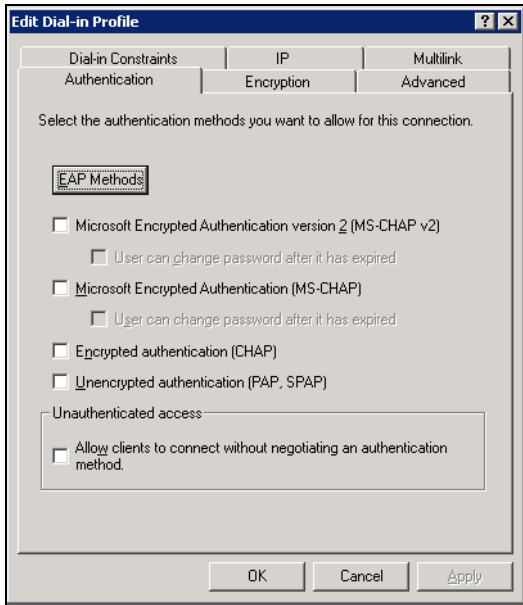
10. Right click on your server object and select Properties.
11. After selecting the Security Tab, Verify that the Windows Authentication provider is selected and then click on Authentication Methods.



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. Then select EAP Methods.
18. 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.



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"/>

MR / EF

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

Known Issues

ISA Server 2004 compatibility with the RSA Security EAP Agent

When using the RSA ACE/Server 5.2 for authentication, you must use the RSA ACE/Agent 5.6.1 as the RSA Authentication Agent for Microsoft Windows 6.1 is not backwards compatible. This solution has been fully tested against the RSA Authentication Manager 6.1 solution, as well as the RSA ACE/Server version 5.2.

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 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.