RSA SecurID Ready Implementation Guide

Last Modified: September 7, 2007

Partner Information

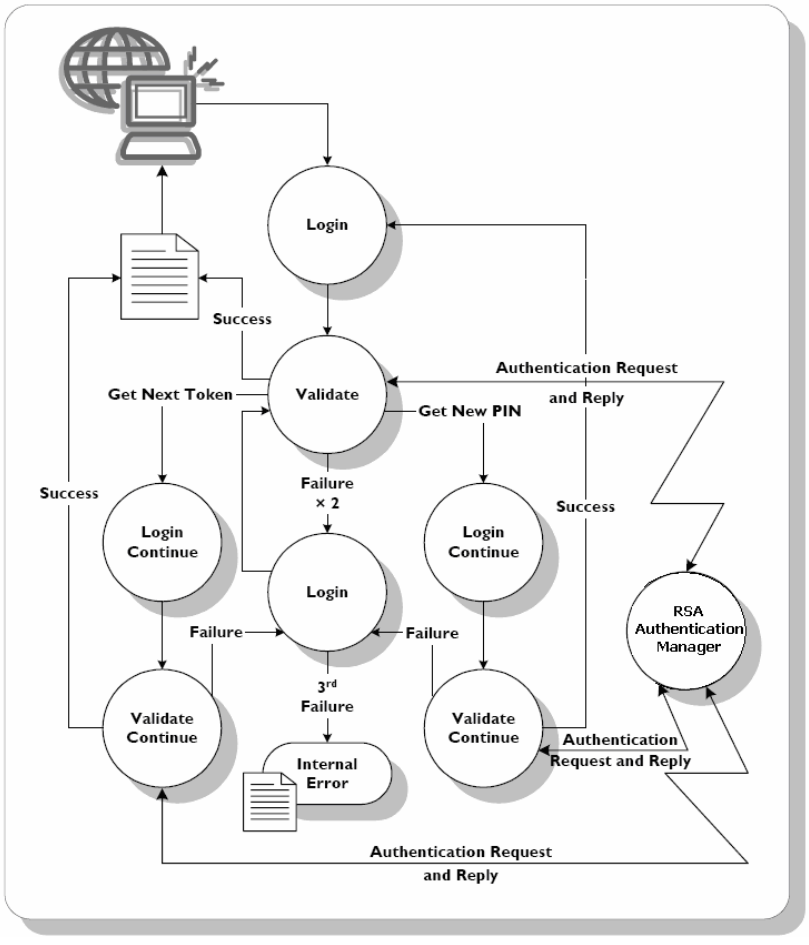
Product Information	
Partner Name	Microsoft
Web Site	www.microsoft.com
Product Name	Intelligent Application Gateway (formerly e-Gap Remote Access Appliance)
Version & Platform	2007
Product Description	Microsoft's Intelligent Application Gateway (IAG) 2007 is the comprehensive, secure remote access gateway that provides secure socket layer (SSL)-based application access and protection with endpoint security management. Providing granular access control, authorization, and deep content inspection from a broad range of devices and locations to a wide variety of line-of-business, intranet, and client/server resources.
Product Category	Perimeter Devices (SSL VPN)

Solution Summary

Microsoft Intelligent Application Gateway 2007 (IAG) utilizes RSA SecurID authentication for two factor authentication providing a higher level of security to access network resources.

IAG provides network administrators with the tools necessary to secure hosted applications and control data streams passed to the host server.

Partner Integration Overview	
Authentication Methods Supported	Native RSA SecurID Authentication
List Library Version Used	Library Version #5.03
RSA Authentication Manager Replica Support *	Full Replica Support
Secondary RADIUS Server Support	No
RSA Authentication Agent Host Type	Net OS
RSA SecurID User Specification	Designated Users, All Users, Default Method
RSA SecurID Protection of Administrative Users	No
RSA Software Token and RSA SecurID 800 Automation	No



Product Requirements

Operating System Support:

Partner Product Requirements: Intelligent Applications Gateway	
Microsoft Intelligent Applications Gateway 2007	3.7.0.0.14

Operating System	
Platform	**Required Patches**
Windows 2003 Server Enterprise Edition	SP2

Agent Host Configuration

To facilitate communication between Microsoft IAG 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 IAG 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 Microsoft IAG as Net OS. This setting is used by the RSA Authentication Manager to determine how communication with the Microsoft IAG 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.

RSA SecurID files

RSA SecurID Authentication Files	
Files	**Location**
sdconf.rec	%systemroot%/system32
Node Secret	Stored in Registry
sdstatus.12	%systemroot%/system32
sdopts.rec	Not implemented

Partner Product Configuration

Before You Begin

This section provides instructions for integrating Microsoft IAG 2007 with RSA SecurID Authentication. The 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.

Integration

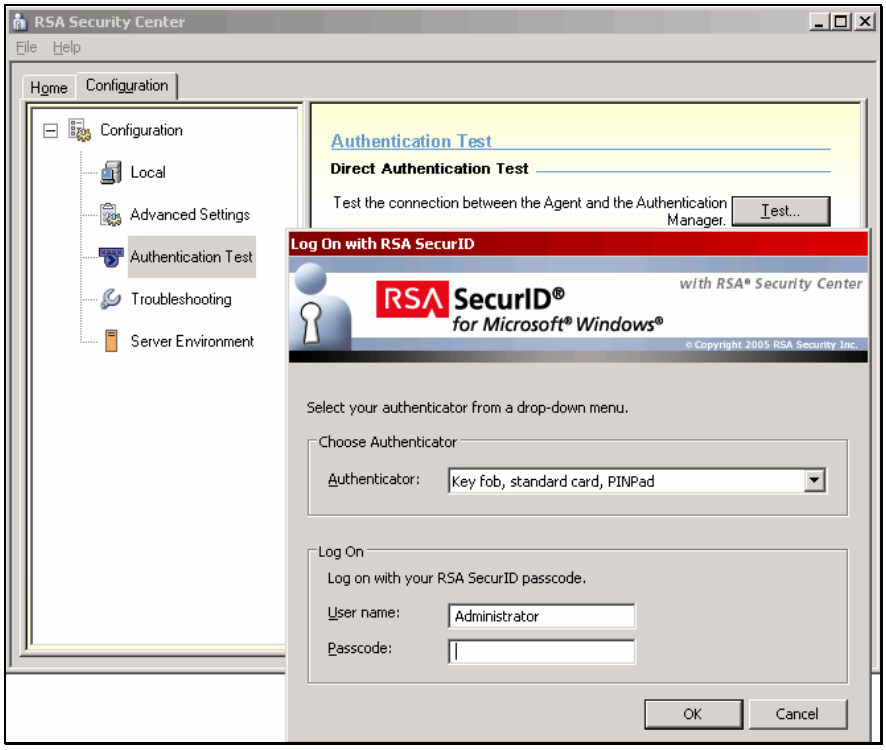
1. Create a new Agent Host through your RSA Authentication Manager.

   Note: Reference the RSA Authentication Manager documentation for configuration details.

2. Generate the sdconf.rec file on the RSA Authentication Manager and copy to the Microsoft IAG server.

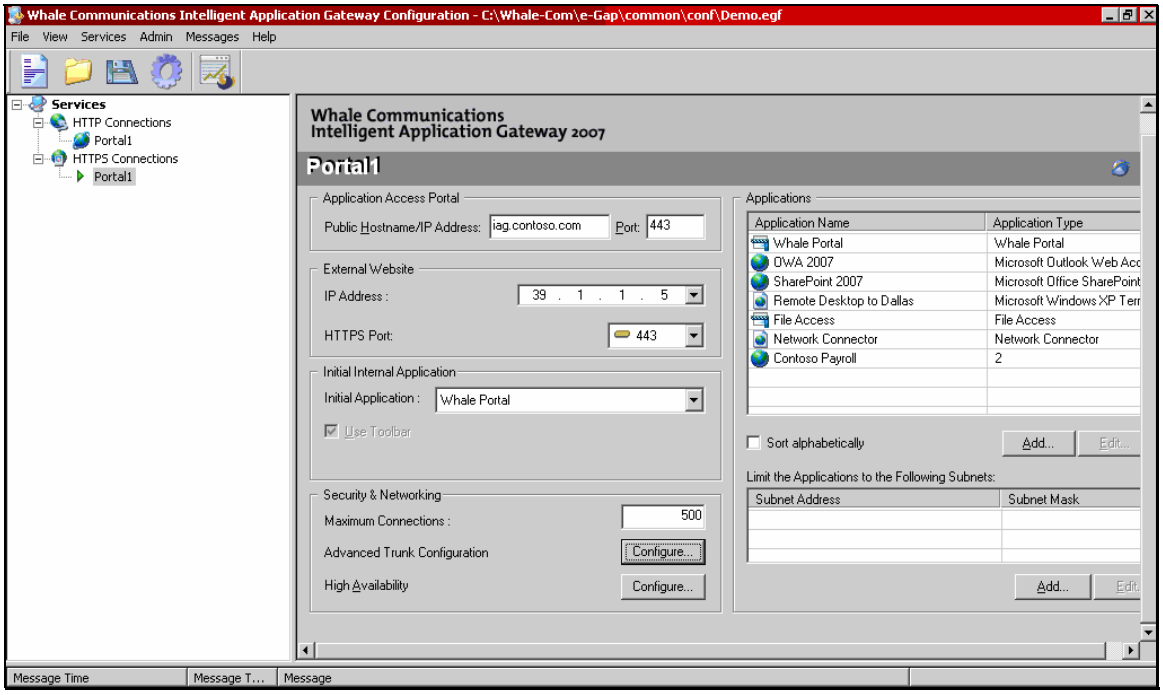
3. Install the RSA Authentication Agent v6.1.1 on the Microsoft IAG 2007 server according to the agent documentation.

4. Upon completion of the agent installation and subsequent reboot, access the RSA Security Center to test the client and establish the shared secret between the client and server.

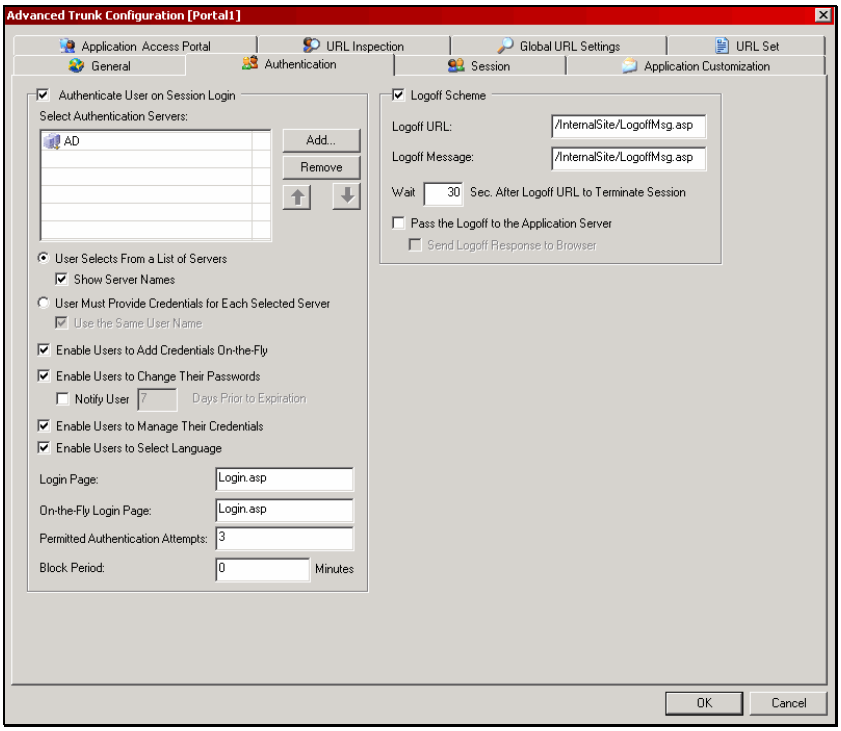


5. Follow the details below to implement SecurID authentication for Microsoft IAG 2007.

   - Open the IAG Configuration application and choose HTTPS Connections-Portal1.
   - Select the Configure button next to the Advanced Trunk Configuration text to add SecurID (ACE) authentication.

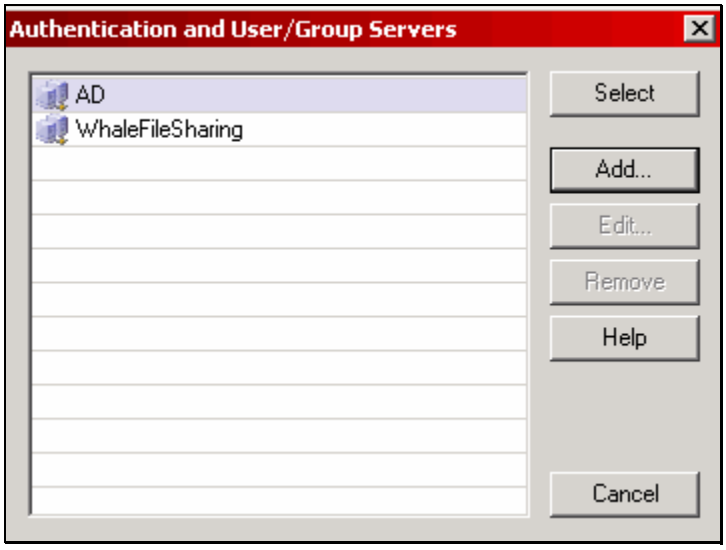


   - Choose Add, from the Authentication window.

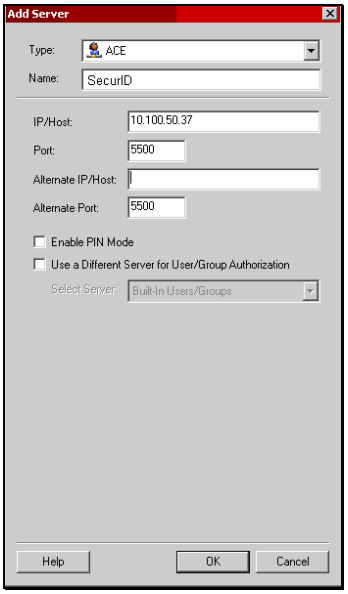


- When prompted for the Authentication and User/Group Servers list. Select Add…

Note: If an alternate authentication method is displayed in the window IAG will display the alternate authentication method in the IAG login window.



- Select ACE from the Type: drop down list and enter a name to distinguish the authentication method.
- Enter the IP/Host address of the RSA Authentication Manager in the IP/Host field provided.
- Select OK to complete the Add Server form.



Note: If the RSA Authentication Manager is not using the default application ports make changes as needed.

Certification Checklist For RSA Authentication Manager

Date Tested: September 7, 2007

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	6.1	Windows 2003 SP1
RSA Authentication Agent	6.1.1	Windows 2003 SP2
Microsoft Intelligent Applications Gateway 2007	3.7.0.0.14	Windows 2003 SP2

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	N/A
No RSA Authentication Manager	✓	No RSA Authentication Manager	N/A

Additional Functionality			
RSA Software 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
RSA SecurID 800 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
Credential Functionality			
Determine Cached Credential State	N/A	Determine Cached Credential State	N/A
Set Credential	N/A	Set Credential	N/A
Retrieve Credential	N/A	Retrieve Credential	N/A

DRP

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