



## RSA SecurID Ready Implementation Guide

Last Modified: February 16, 2006

### Partner Information

---

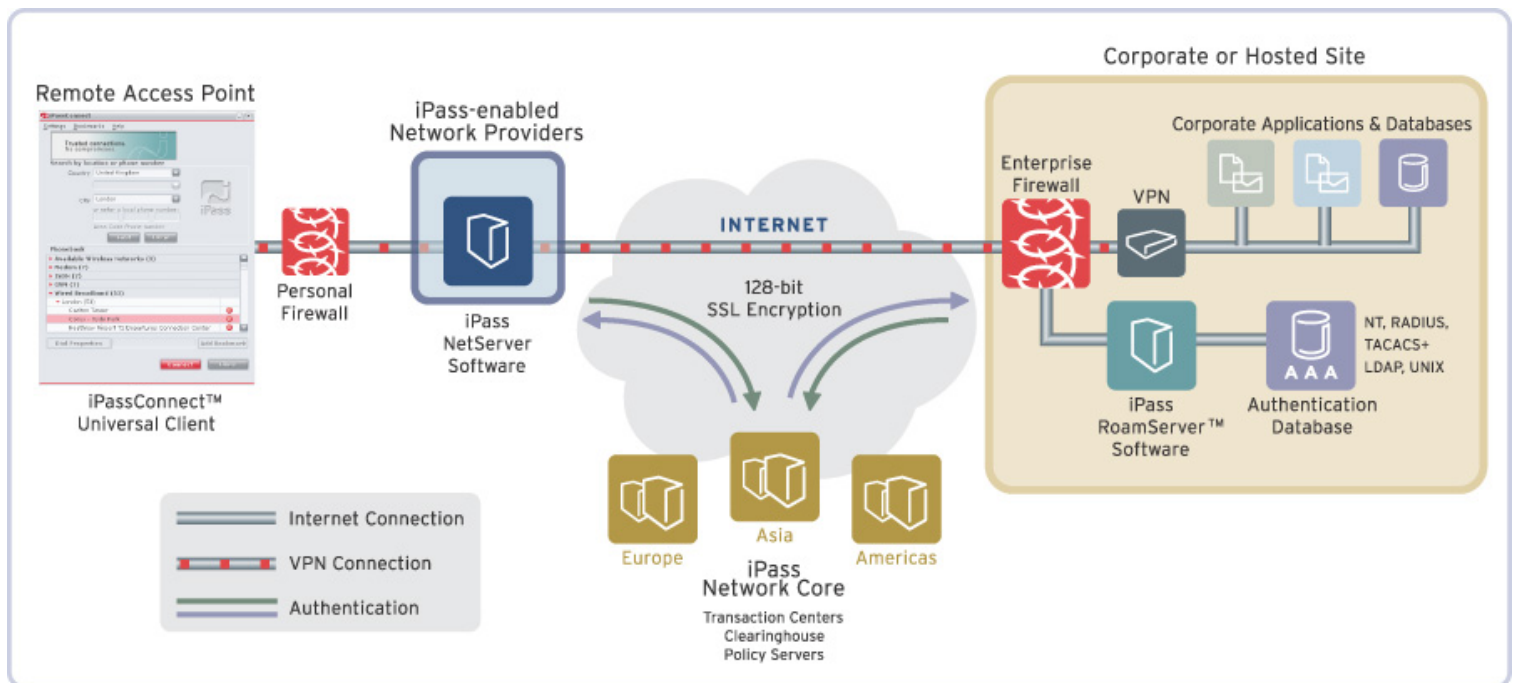
Product Information	
Partner Name	iPass Inc.
Web Site	<a href="http://www.ipass.com">www.ipass.com</a>
Product Name	iPass Enterprise Connectivity Services a.k.a. Global Internet Roaming via the "Software-enabled Virtual Network"
Version & Platform	- RoamServer version 5.1.0 - iPassConnect version 3.41 (Windows 2000/XP)
Product Description	The iPass global network provides easy dial-up access to the Internet from more than 40,000 points of presence (POPs) in over 150 countries around the world. iPass provides this service by using the networks of top-tier broadband and dial-up providers such as T-Mobile, SBC, STSN, Wayport, inter-touch, Arescom, Equant, Worldcom, Sprint, and through a unique third-party Internet clearinghouse and settlement system. With one service, individual and corporate users can securely access email, the web and corporate data from anywhere in the world with a local telephone call or wireless/wired broadband connection at a supported broadband access venue, gaining significant cost savings over solutions requiring internal modem banks and long-distance, toll-free connection charges, or individual accounts with broadband providers around the world. iPass supplies users with a friendly, easy-to-use client software (called iPassConnect) containing all the worldwide access points.
Product Category	Remote access



## Solution Summary

The iPass RoamServer software acts as a RADIUS client to the RSA Authentication Manager to authenticate users stored in the RSA Authentication Manager database. RoamServer can point to a primary, secondary, tertiary, etc RADIUS for failover purposes as well. Configuring the RoamServer to act as a RADIUS client is explained below in a few easy steps. Also, configuring the RSA Authentication Manager for the proper RADIUS client information about RoamServer is straight-forward and does not deviate from the normal process of RSA Authentication Manager client-server configuration.

Partner Integration Overview	
Authentication Methods Supported	RADIUS
List Library Version Used	N/A
RSA Authentication Manager Name Locking	N/A
RSA Authentication Manager Replica Support	N/A
Secondary RADIUS Server Support	Yes (no limit)
Location of Node Secret on Agent	None stored
RSA Authentication Agent Host Type	Net OS
RSA SecurID User Specification	Designated Users
RSA SecurID Protection of Administrative Users	Yes
RSA Software Token API Integration	No
Use of Cached Domain Credentials	No



## Product Requirements

---

<b>Partner Product Requirements: iPass RoamServer 5.1.0</b>	
<b>CPU</b>	400 MHz or faster
<b>Memory</b>	256 MB or greater
<b>Storage</b>	100 MB
<b>Firmware Version</b>	N/A

<b>Operating System</b>	
<b>Platform</b>	<b>Required Patches</b>
Windows 2000 Server Family	Service Pack 4 or later
Windows Server 2003 Family	Service Pack 1 or later
Linux (RedHat)	6.1 kernel 2.2.12 & 6.2 kernel 2.4.14 w/Workstation Pkg.
Sun Solaris (UNIX)	5.8, and 5.9 (SPARC)

<b>Partner Product Requirements: iPassConnect 3.41</b>	
<b>CPU</b>	500 MHz or faster
<b>Memory</b>	256 MB or greater
<b>Storage</b>	150 MB minimum
<b>Firmware Version</b>	N/A

<b>Operating System</b>	
<b>Platform</b>	<b>Required Patches</b>
Windows 2000 Professional	Service Pack 4 or later
Windows XP Professional	Service Pack 1 or later

## Agent Host Configuration

---

To facilitate communication between the **RoamServer 5.1.0** 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 **RoamServer 5.1.0** within its database and contains information about communication and encryption.

To create the Agent Host record, you will need the following information.

- Hostname of the RoamServer host
- IP Addresses for the RoamServer host
- RADIUS shared secret for both the RoamServer and RSA Authentication Manager Node Secret File.

When adding the Agent Host Record, you should configure the **RoamServer 5.1.0** as a **Net OS Agent**. This setting is used by the RSA Authentication Manager to determine how communication with the RoamServer 5.1.0 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

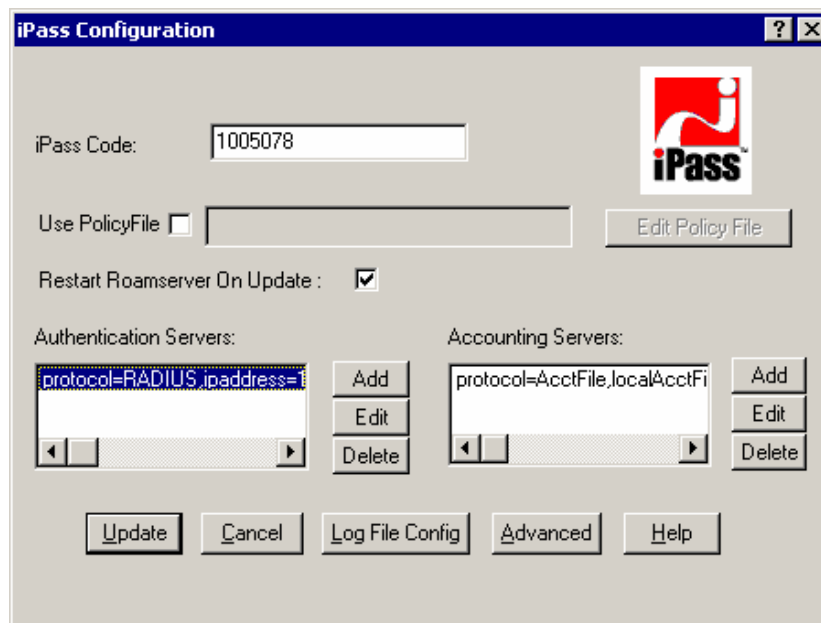
## Before You Begin

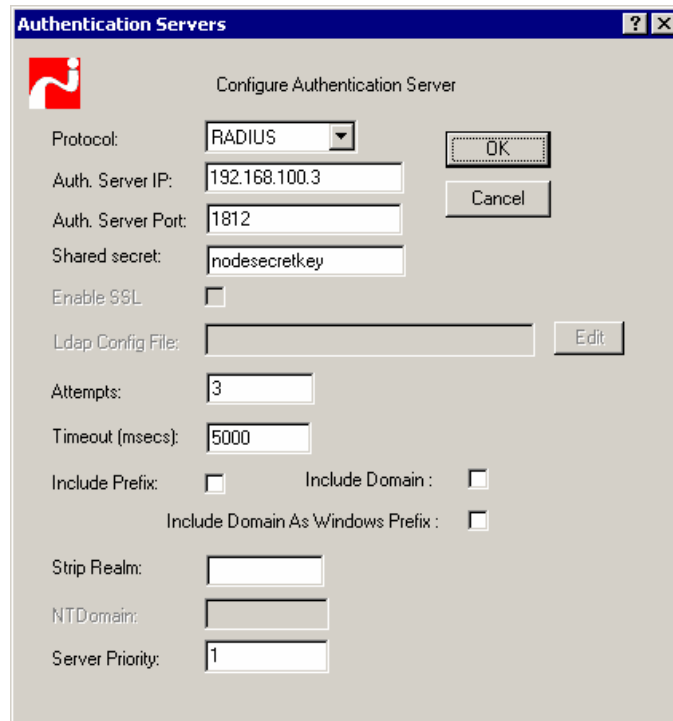
This section provides instructions for configuring the iPass RoamServer 5.1.0 with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

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 configuration. Perform the necessary tests to confirm that this is true before proceeding.

1. Open the RoamServer configuration window (Windows RoamServer shown below). Click the “Add” button to add an “Authentication Servers:” server object.





2. Choose the RADIUS protocol, enter in the IP address of the RSA Authentication Manager server, and ensure the port of 1812 (default) is correct. In the "Shared secret" field, enter the same shared secret that you used in the RSA Authentication Manager Agent Host configuration node secret value (see above in "Agent Host Configuration").
3. Make sure there is a check-mark next to "Restart RoamServer on Update" and then click the Update button to commit changes to the RoamServer configuration and restart the RoamServer service. The RoamServer will automatically restart and the changes will take effect. Note that if there is no check-mark, then you must manually restart the RoamServer before any changes will take effect.

**Example of a SecurID logon screen in iPassConnect:**

Clients using SecurID authentication with iPassConnect must enter the SecurID PASSCODE (PIN+TOKENCODE) into the password field of iPassConnect as shown below:



# Certification Checklist

Date Tested: February 16, 2006

Certification Environment		
Product Name	Version Information	Operating System
<b>RSA Authentication Manager</b>	6.1	Windows Server 2003 ENT SP1
<b>RSA Authentication Agent</b>	N/A	N/A
<b>RSA Software Token</b>	N/A	N/A
<b>iPass RoamServer</b>	5.1.0	Windows Server 2003 ENT SP1
<b>iPassConnect</b>	3.41	Windows 2000 SP4 Windows XP SP1 and SP2

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

BSJ/MPR

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

## Known Issues

---

Currently, due to the nature of the iPass authentication transaction, iPass does not support “challenge-response” authentication modes for strong authentication systems. This includes SecurID “new PIN mode” and “next tokencode mode”. iPass only supports two-factor strong authentication in the “response-only” mode via the RADIUS protocol. Users would need to enter the “passcode” into the password field at the time of initiating the connection attempt. Please contact iPass for more details on these limitations.