RSA SecurID Ready Implementation Guide

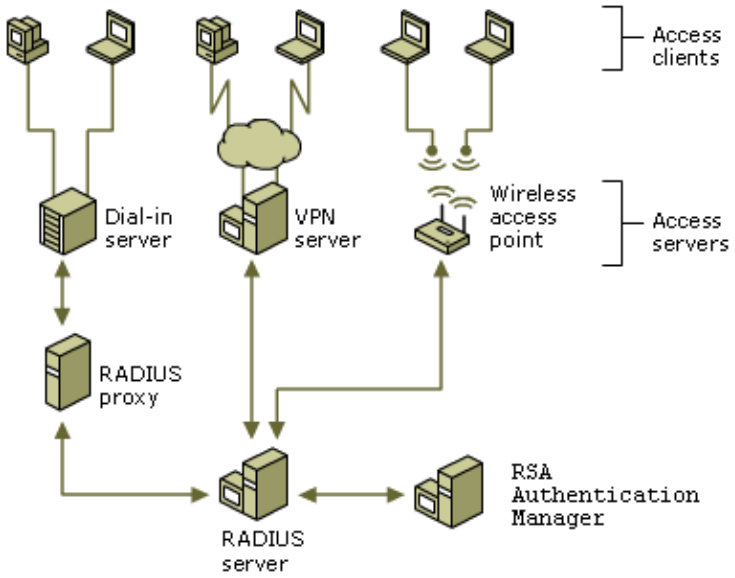
Last Modified: March 13, 2006

Partner Information

Product Information	
Partner Name	Microsoft Corporation
Web Site	www.microsoft.com
Product Name	Microsoft Internet Authentication Service (IAS)
Version & Platform	Windows Server 2003
Product Description	Internet Authentication Service (IAS) in Microsoft® Windows® Server 2003, Standard Edition; Windows Server 2003, Enterprise Edition; and Windows Server 2003, Datacenter Edition is the Microsoft implementation of a Remote Authentication Dial-in User Service (RADIUS) server and proxy. As a RADIUS server, IAS performs centralized connection authentication, authorization, and accounting for many types of network access including wireless, authenticating switch, and remote access dial-up and virtual private network (VPN) connections. As a RADIUS proxy, IAS forwards authentication and accounting messages to other RADIUS servers.
Product Category	RADIUS Servers

Solution Summary

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 (unlimited)
Location of Node Secret on Agent	'None stored'
RSA Authentication Agent Host Type	Communication Server
RSA SecurID User Specification	Designated Users
RSA SecurID Protection of Administrative Users	No
RSA Software Token and SD800 Automation	No
Use of Cached Domain Credentials	No



Product Requirements

Partner Product Requirements: Microsoft IAS	
CPU	733MHz
Memory	256MB
Storage	2GB

Operating System	
Platform	**Version**
Microsoft Windows 2003	Standard or Enterprise Edition with Internet Authentication Service Windows Component installed.

Agent Host Configuration

To facilitate communication between Microsoft Internet Authentication Service (IAS) and the RSA Authentication Manager / RSA SecurID Appliance, an Agent Host record must be added to the RSA Authentication Manager and RSA RADIUS database. The Agent Host record identifies the Microsoft Internet Authentication Service (IAS) 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 adding the Agent Host Record, you should configure Microsoft Internet Authentication Service (IAS) as Communication Server. This setting is used by the RSA Authentication Manager to determine how communication with the Microsoft Internet Authentication Service (IAS) 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.

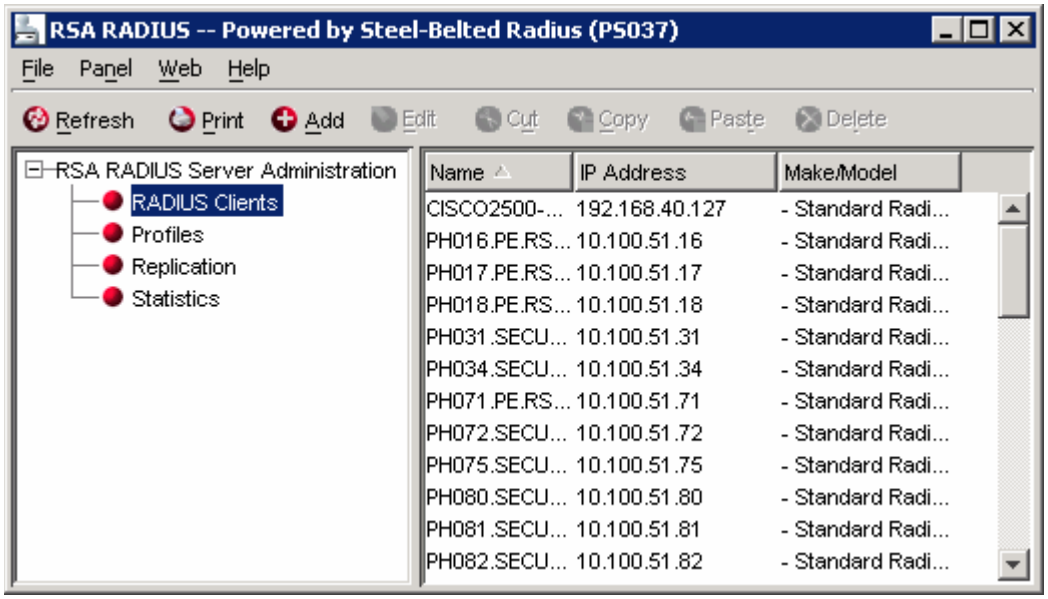
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

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.

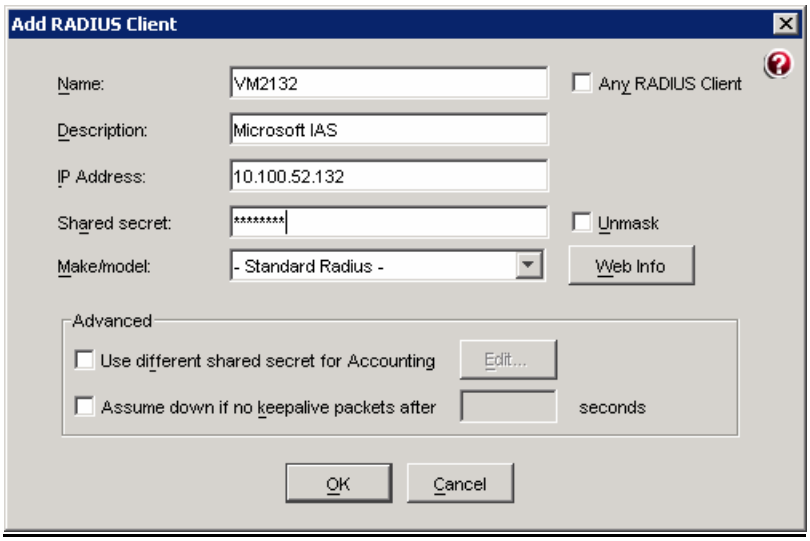
Documenting the Solution

Adding the Microsoft IAS Server as a RADIUS Client

1. Open RSA Authentication Manager GUI.



2. On the **RADIUS** menu, choose **Manage RADIUS Server**. Right click on **RADIUS Clients**. Select **Add**.



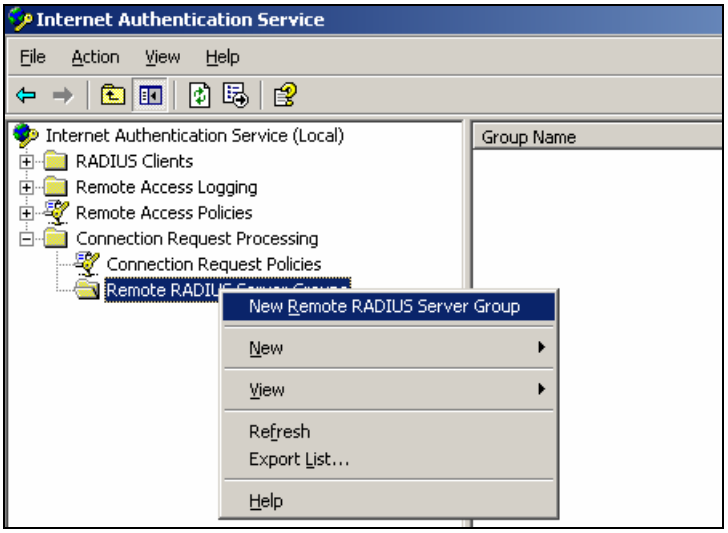
- **Name:** Enter the IAS Server Host name.
- **IP Address:** Enter the unique IP address that **resolves** to the IAS Server Host name.
- **Shared secret:** A value that will be entered into the IAS server in order to encrypt the communication between the two servers.
- **Make/model:** Standard RADIUS.

Note: It is important that all hostname and IP addresses resolve to each other. Please reference the RSA Authentication Manager documentation for detailed information on this and other configuration parameters within this screen.

3. Click OK.

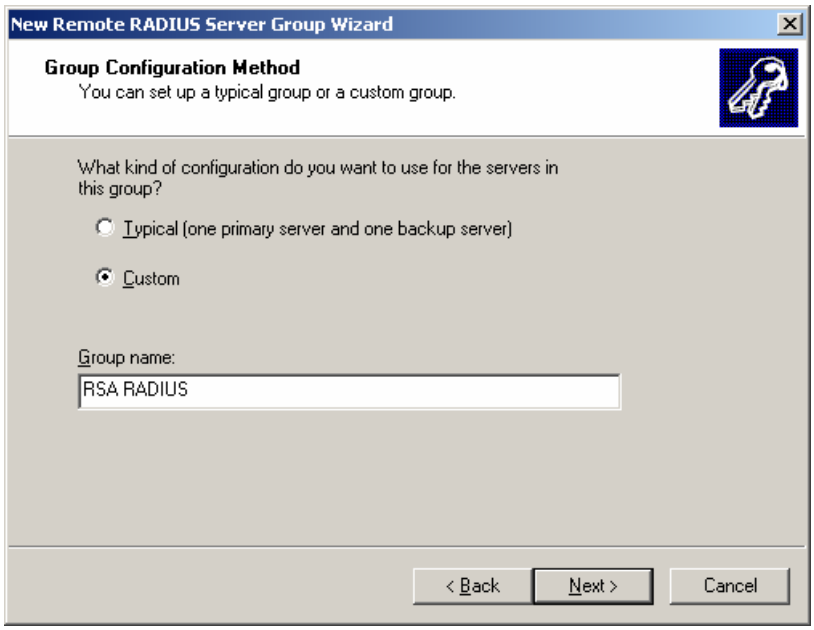
Activating SecurID authentication via RADIUS

1. From the IAS Server Management Console, expand **Connection Request Policies.** Right Click **Remote RADIUS Server Groups**. Then Launch the **New Remote RADIUS Server Group Wizard**.

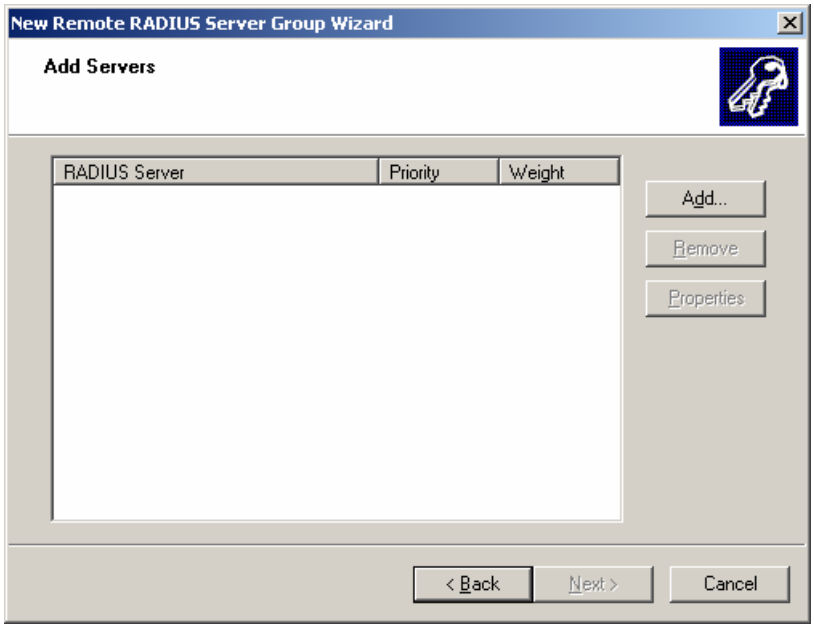


2. Following the Wizard, click **Next** to begin creating your RSA Authentication Manager server group.

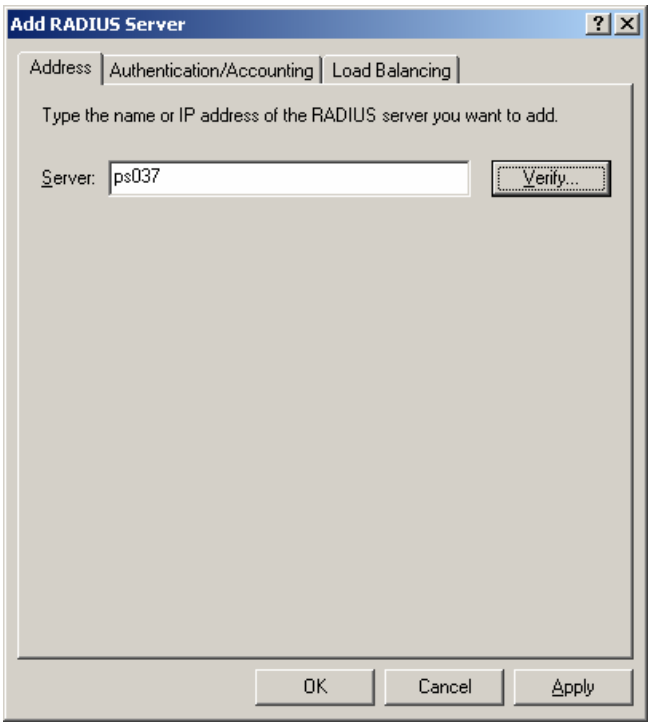
3. Select **Custom** to manually configure your RADIUS Servers.
4. Enter a group name and then click **Next** to continue.



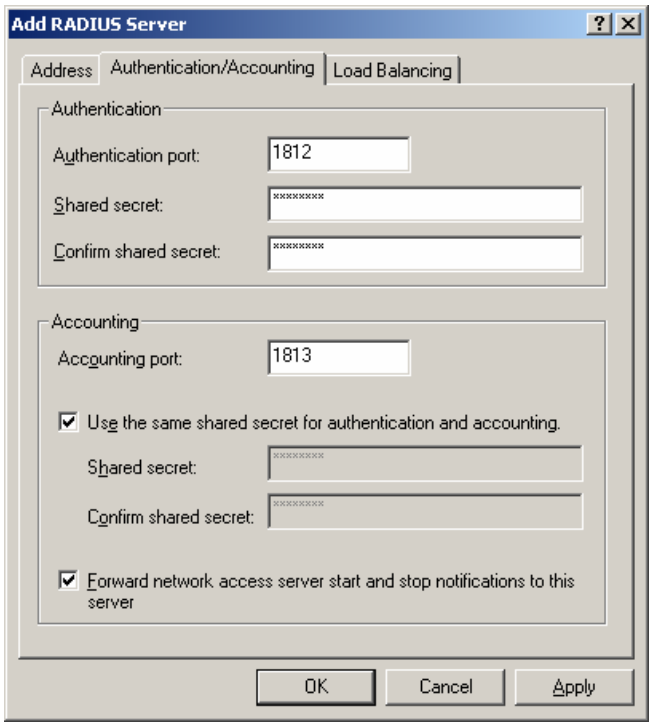
5. Click **Add** to enter your RADIUS Server information.



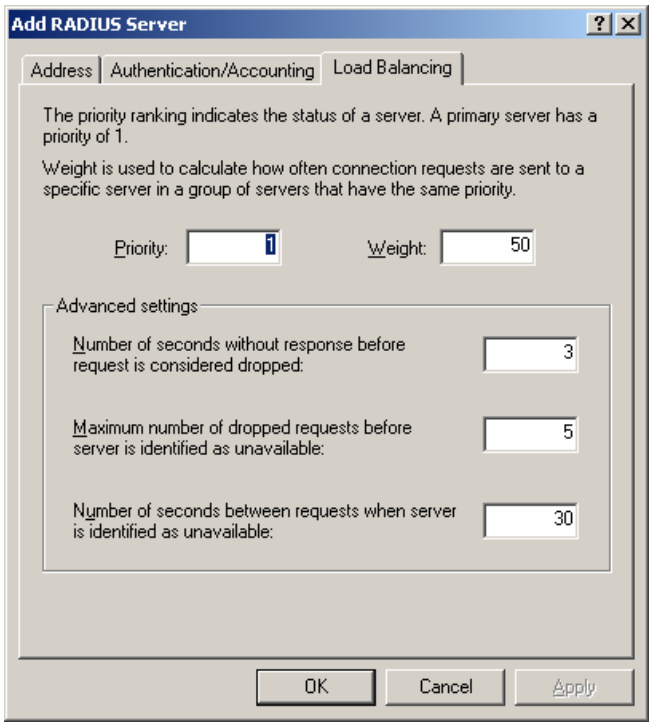
6. Under the **Address** tab enter the details of your Primary RSA Authentication Manager.
7. Using the **Verify** button you are able to confirm that the hostname you have entered is resolvable via DNS or WINS.



8. Select the **Authentication/Accounting** tab and enter the appropriate RADIUS authentication, accounting and shared secret values for communication with your RSA Authentication Manager.

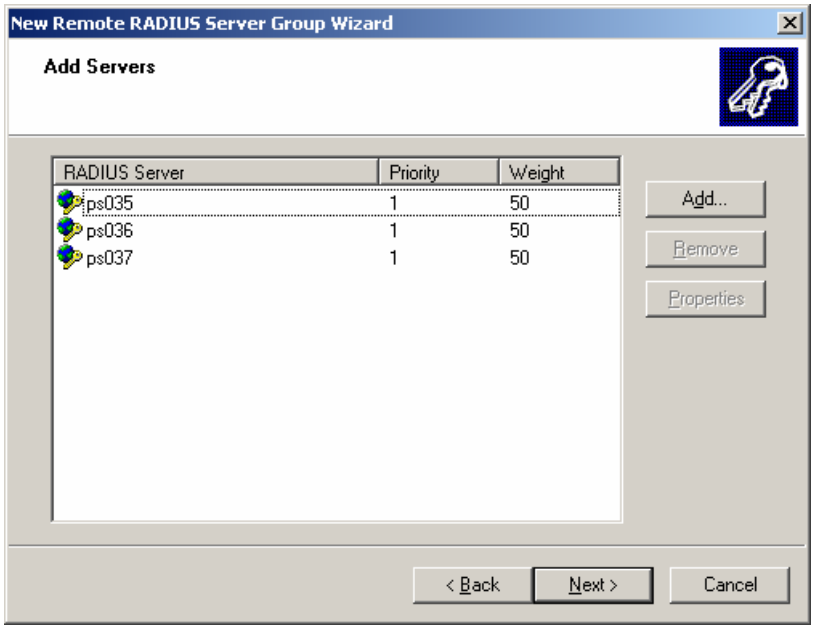


9. Select the **Load Balancing** Tab to enter information related to how this server group should failover or distribute authentication load. These settings will be the same for both Primary and Replica Authentication Managers.
10. Enter “1” for **Priority**,
11. Enter “50” for **Weight**.
12. Leave the default settings for all fields under **Advanced Settings**.



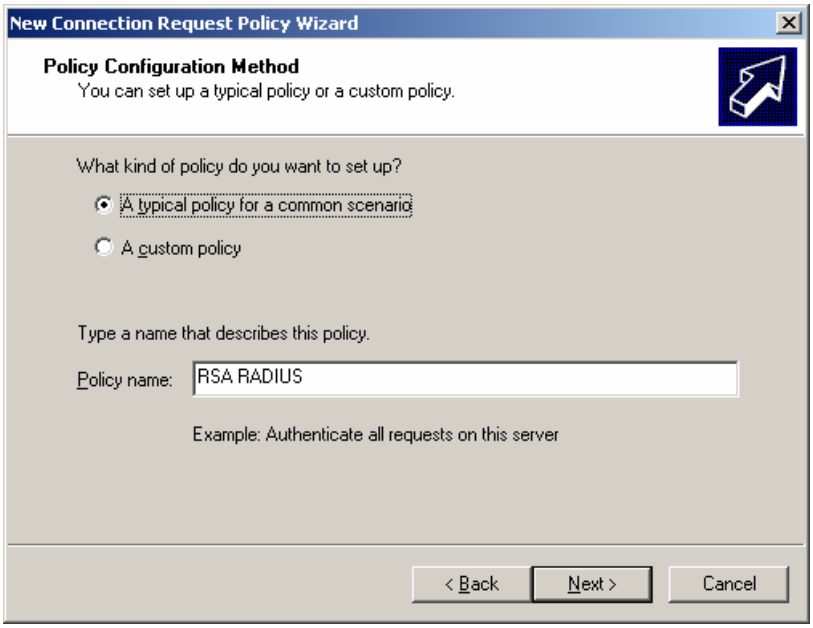
13. Repeat steps 5-12 to define failover RSA Authentication Managers. (Optional)

14. Once your RSA Authentication Manager Servers have been entered into the server group. Click **Next** to continue.

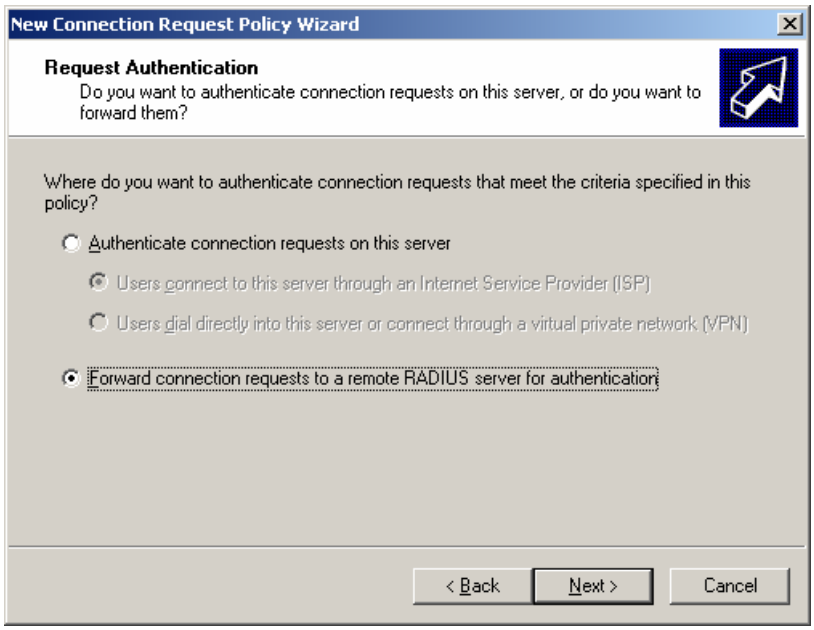


15. You have now completed the **RADIUS Server Group Wizard**. At this point you will be asked if you want to launch the New Connection Request Policy Wizard. You can either accept this option or start the process manually by right clicking on the New **Connection Request Policies** icon and selecting **New Connection Request Policy** Wizard option.

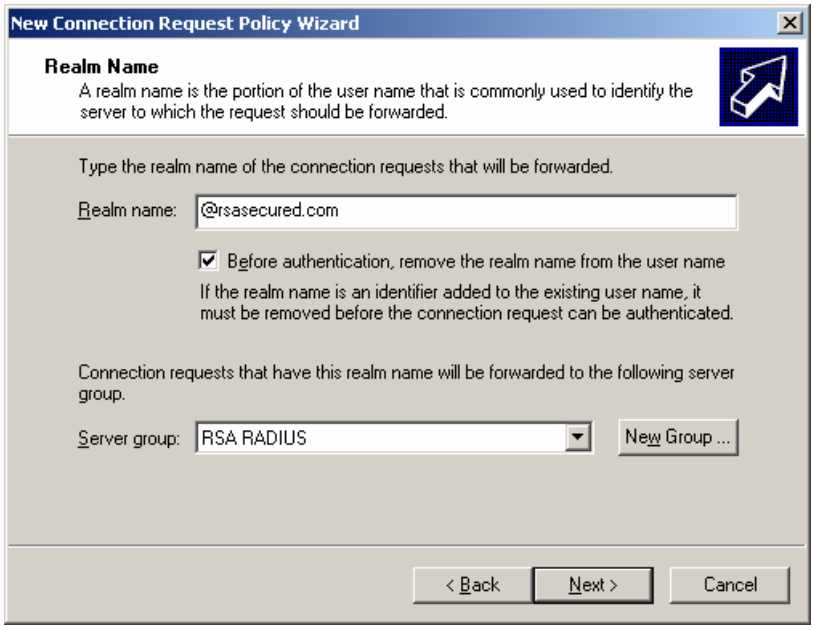
16. In the **New Connection Request Policy Wizard**, Select **A typical policy for a common scenario** as the **Policy Configuration Method** and assign an appropriate **Policy name**.



17. On the following screen select **Forward connection requests to a remote RADIUS server for authentication**.

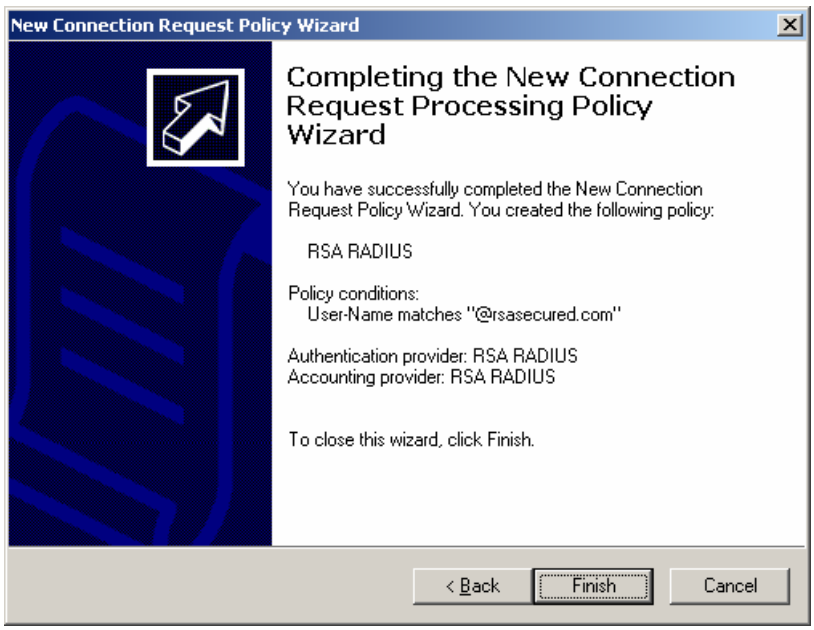


18. Depending on the format of your user's login names, populate the **Realm name:** field with the standard element of their username.
19. Toggle the checkbox on the screen to remove the Realm Name information from the user name.



Note: The Realm Name information must be removed prior to being forwarded to the RSA Authentication Manager. In this example users will log in with their Windows User Principle Name (UPN) e.g. mrennie@rsasecured.com. Within the RSA Authentication Manager database, this user has been defined as just 'mrennie'. It is therefore necessary to have the @rsasecured.com component removed from their submitted name prior to forwarding to the RSA Authentication Manager for RADIUS authentication.

20. Selecting **Next>** should complete the **New Connection Request Policy** Wizard and associate it with the Remote RADIUS Server group you created previously.

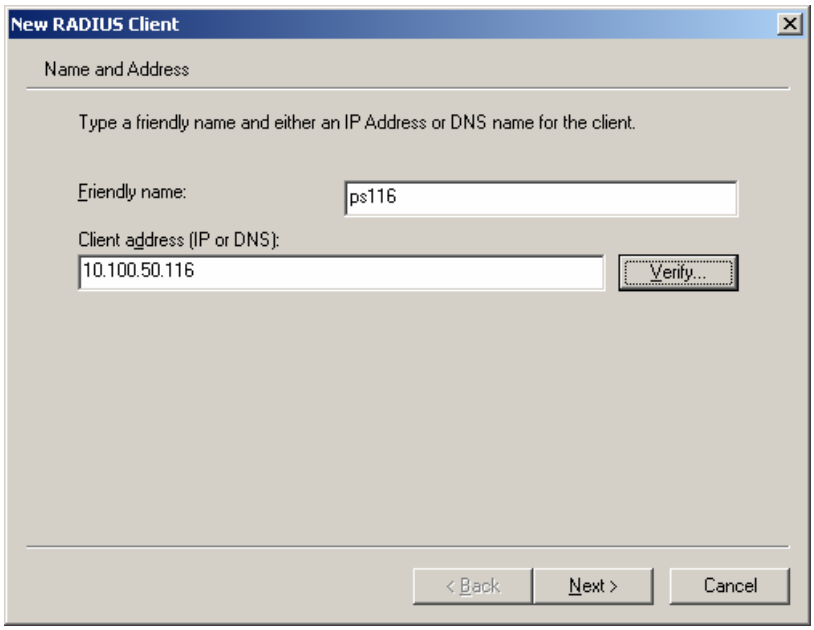


Configuring a Remote RADIUS Client

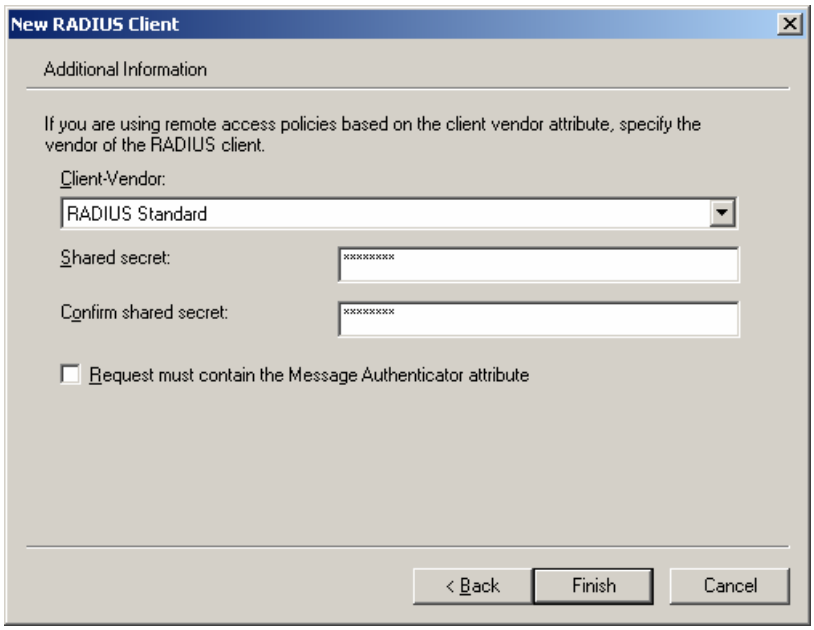
The final Microsoft IAS Server configuration task you must carryout to test your configuration is to define a Remote RADIUS Client.

1. From the IAS Server Management Console right click on the **RADIUS Clients** folder and select **New RADIUS Client**.

2. In the resulting screen input the **Friendly name:** of your device and its **Client address**.



3. Accept the default **Client-Vendor: RADIUS Standard**.
4. Enter and confirm a **Shared secret** for communication with the Remote RADIUS Client.
5. Select **Finish** completing the RADIUS Client definition.



Certification Checklist

Date Tested: March 13, 2006

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	6.1	Windows Server 2003
Microsoft IAS	2003	Windows Server 2003

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

MPR

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