Alcatel-Lucent
8950 AAA

RSA SecurID Ready Implementation Guide

Last Modified: January 17, 2013

Partner Information

Product Information	
Partner Name	Alcatel-Lucent
Web Site	www.8950aaa.com
Product Name	8950 AAA
Version & Platform	8.0
Product Description	The 8950 AAA server provides authentication, authorization, and accounting capabilities for communication services access management, providing flexibility and visibility with policy management and intuitive real-time dashboard. The Alcatel-Lucent 8950 AAA is an Authentication, Authorization and Accounting (AAA) server for major service providers, ISPs and Enterprises due to its proven performance and its flexible, extensible PolicyFlow™ architecture built on Java™-based programming languages. In addition, 8950 AAA provides an expanded graphic interface for overall server configuration, management and monitoring. 8950 AAA server delivers expanded functionality to address your deployment of wireless LANs and other networks deploying 802.1x, DIAMETER, and EAP protocols to support fixed-mobile roaming and blended multimedia services.

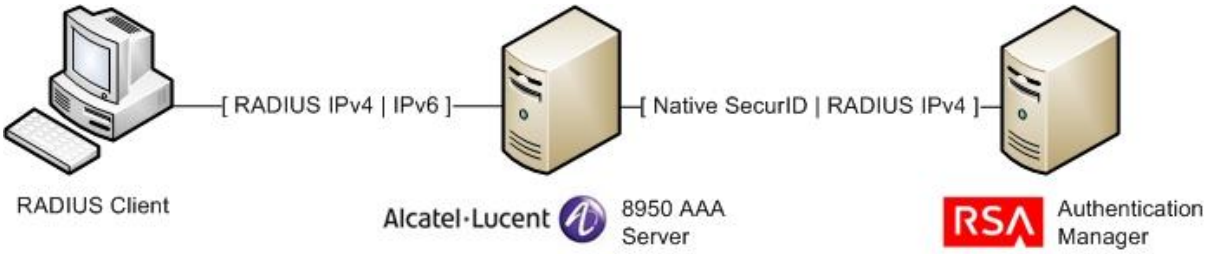
Solution Summary

The 8950 AAA has a flexible and extensible PolicyFlow plug-in architecture and adds an expanded graphic interface for overall server management and maintenance of user accounts. The PolicyAssistant enables most users to be up and authenticating by filling in a few simple forms. 8950 AAA also includes many new plug-ins and significant extensions to the PolicyFlow logic.

The 8950 AAA supports two factor authentication using RSA Authentication Manager. This feature enables remote-access providers to provide additional services to corporate customers who need token card-based security for their users. The selection of card type and security server address can be determined on a realm or per-user basis.

The 8950 AAA employs a dual IP stack to support both IPv4 and IPv6 address types. This feature enables RSA Authentication Manager to provide authentication services to hosts on IPv6 networks.

RSA SecurID supported features 8950 AAA version 8.0	
RSA SecurID Authentication via Native RSA SecurID Protocol	Yes
RSA SecurID Authentication via RADIUS Protocol	Yes
On-Demand Authentication via Native SecurID Protocol	Yes
On-Demand Authentication via RADIUS Protocol	Yes
RSA Authentication Manager Replica Support	Yes
Secondary RADIUS Server Support	Yes
RSA SecurID Software Token Automation	No
RSA SecurID SD800 Token Automation	No
RSA SecurID Protection of Administrative Interface	No



Authentication Agent Configuration

Authentication Agents are records in the RSA Authentication Manager database that contain information about the systems for which RSA SecurID authentication is provided. All RSA SecurID-enabled systems require corresponding Authentication Agents. Authentication Agents are managed using the RSA Security Console.

The following information is required to create an Authentication Agent:

- Hostname
- IP Addresses for network interfaces

Set the Agent Type to "Standard Agent" when adding the Authentication Agent. This setting is used by the RSA Authentication Manager to determine how communication with 8950 AAA will occur.

A RADIUS client that corresponds to the Authentication Agent must be created in the RSA Authentication Manager in order for 8950 AAA to communicate with RSA Authentication Manager. RADIUS clients are managed using the RSA Security Console.

The following information is required to create a RADIUS client:

- Hostname
- IP Addresses for network interfaces
- RADIUS Secret

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 documentation for additional information about creating, modifying and managing Authentication Agents and RADIUS clients.

Important: <base_dir> is used throughout this guide to specify where the 8950 AAA software is installed. The default path on Windows is c:\AAA or /opt/AAA on UNIX. Please use the appropriate path to your installation directory.

RSA SecurID files

RSA SecurID Authentication Files	
Files	**Location**
sdconf.rec	<base_dir>\run\ace
Node Secret	<base_dir>\run\ace
JAStatus.1	<base_dir>\run\ace
sdopts.rec	<base_dir>\run\ace

Note: The appendix of this document contains more detailed information regarding these files.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the 8950 AAA 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.

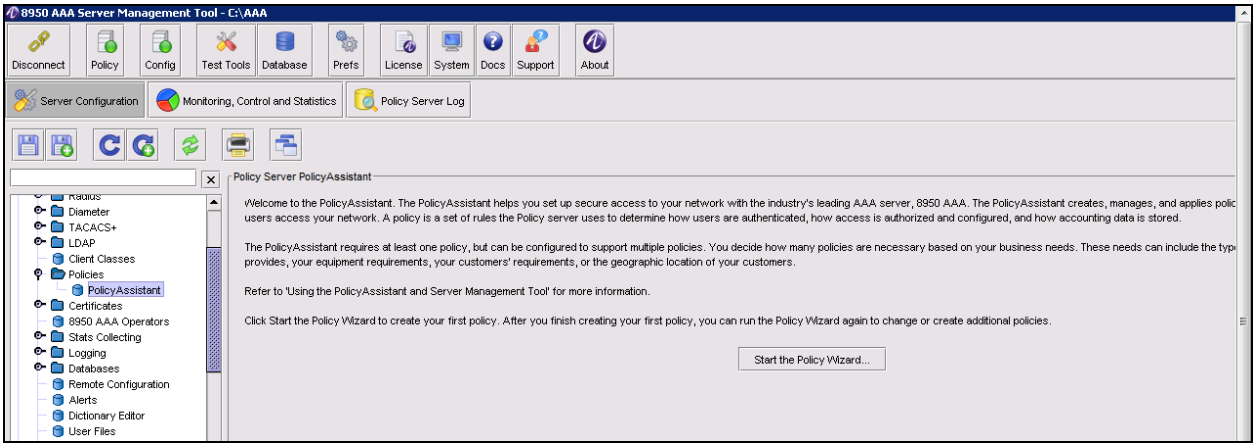
All 8950 AAA components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

8950 AAA Configuration

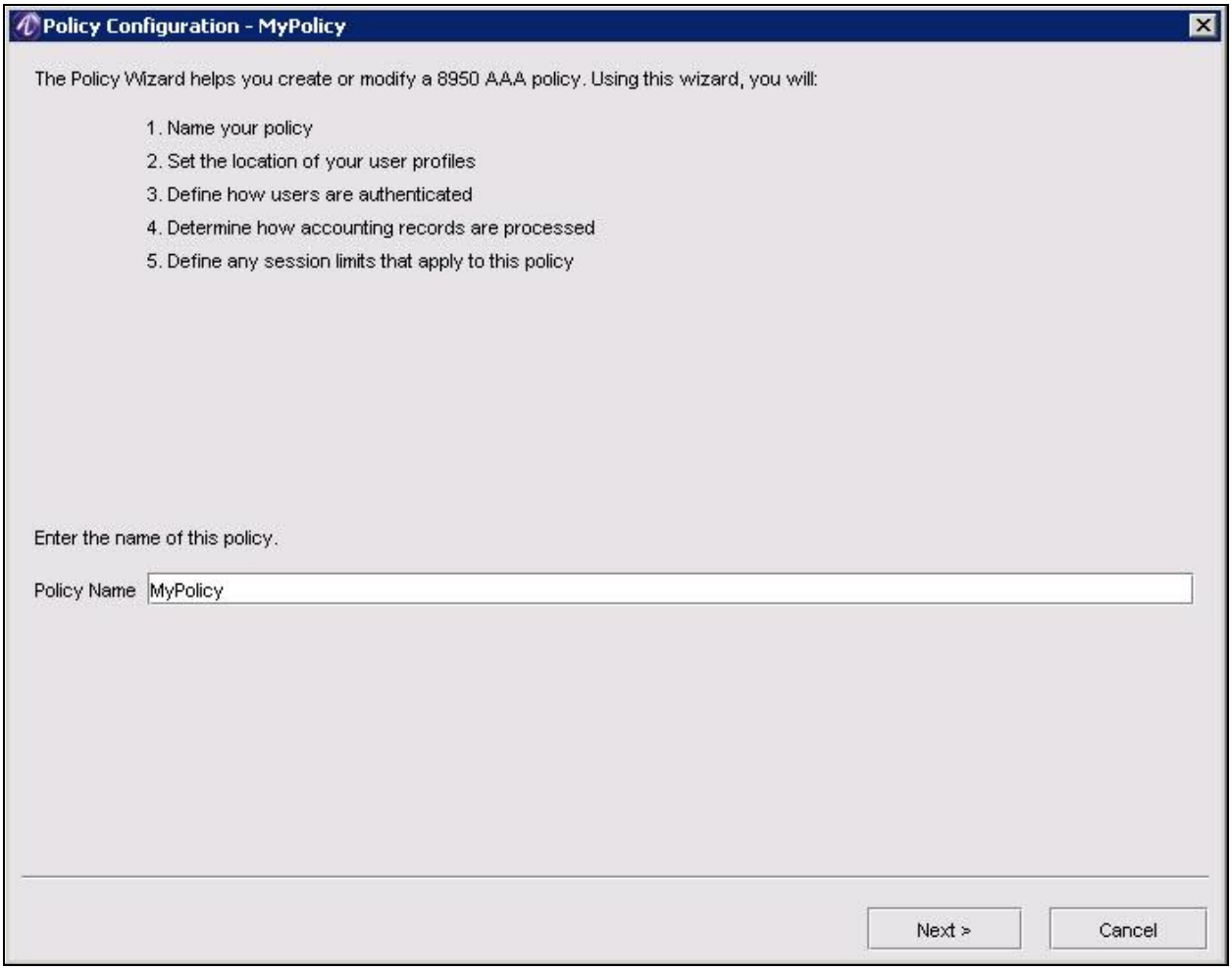
The 8950 AAA can communicate with the RSA Authentication Manager via Native SecurID or Radius. When communication with the RSA Authentication Manager via Radius you will need to configure the 8950 AAA as a Radius Proxy server. To configure the 8950 AAA you will need to create a policy, (either for Native SecurID or a Radius Proxy server), policy rule, and a Radius client. When the configurations are complete save the sets and restart the policy server.

Creating Native SecurID Policy

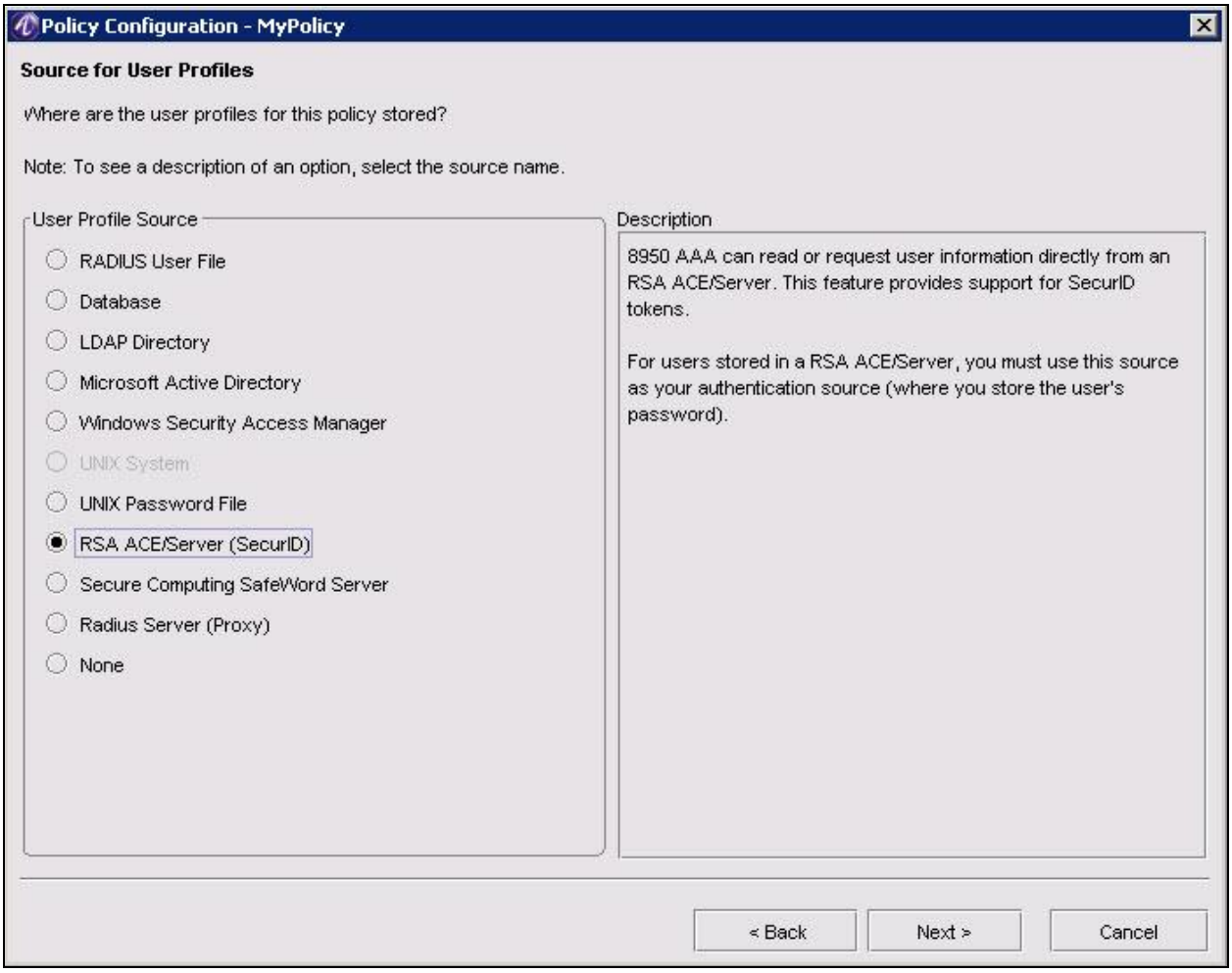
1. Copy the configuration file (**sdconf.rec**) to the <base_dir>\run\ace directory of the 8950 AAA server. The default installation directory on Windows is c:\AAA\run\ace. The default directory on UNIX is /opt/AAA/run/ace.
2. Launch the Server Management Tool and start the Policy Assistant by selecting **Policies > Policy Assistant** in the left window pane.
3. Click **Start the Policy Wizard**.



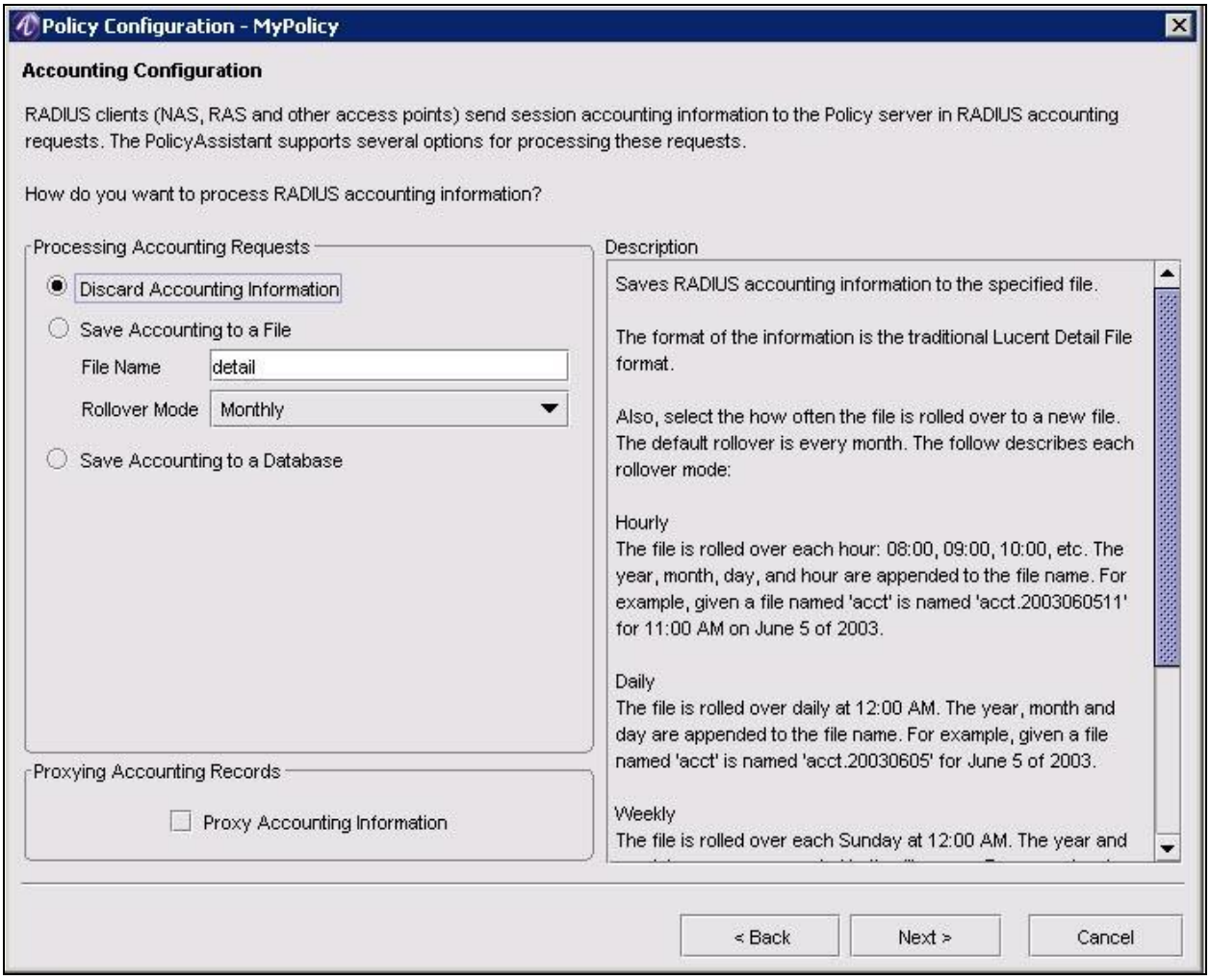
4. Enter a name for your new policy. Click **Next.**



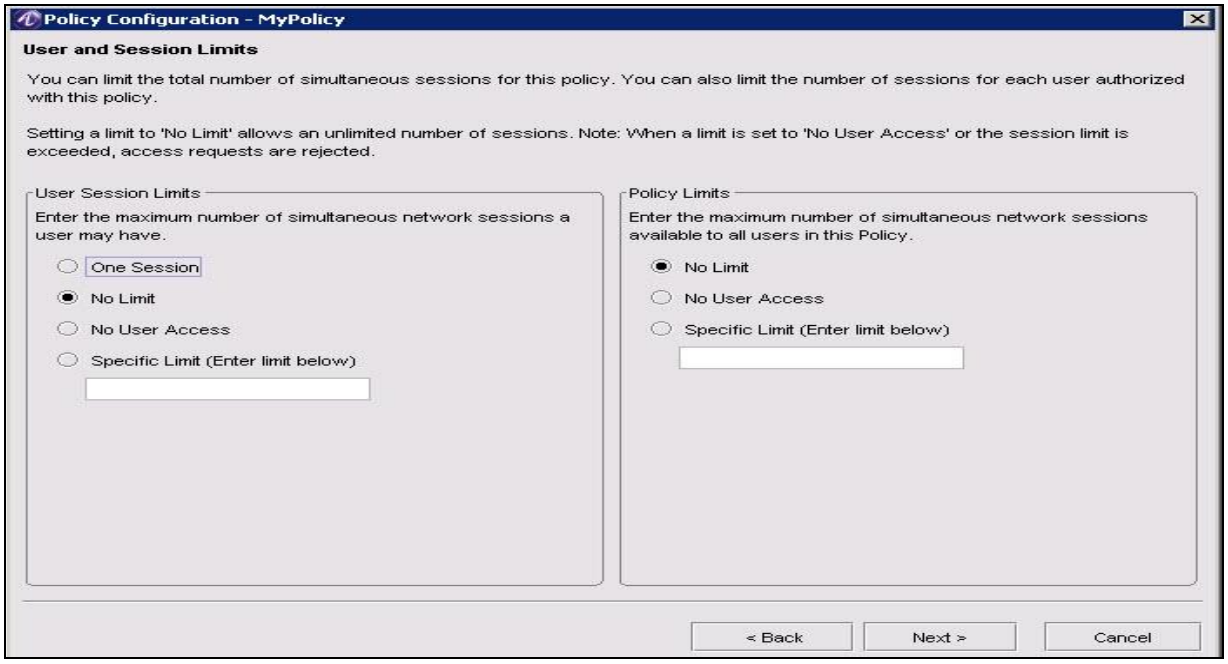
5. Select **RSA ACE/Server (SecurID)** from the list of User Profile Sources. Click **Next.**



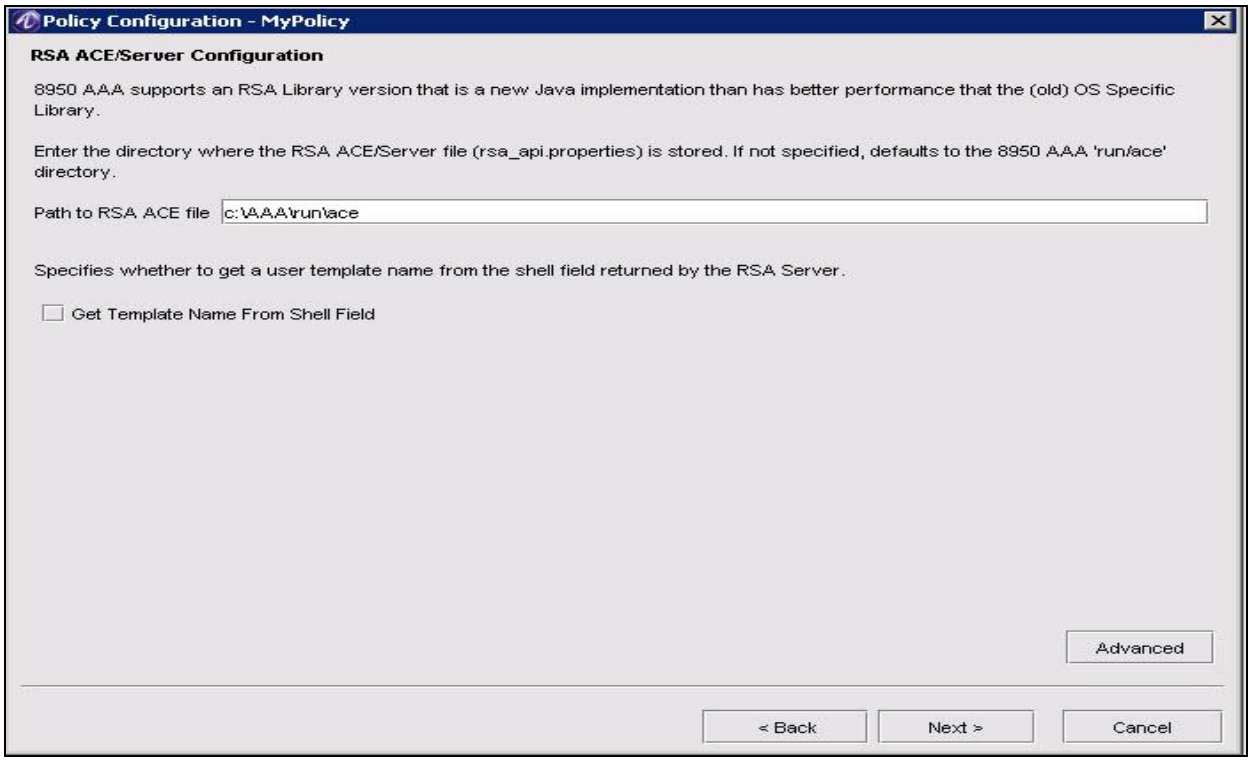
6. Enter selections for Accounting Configuration (for testing purposes we discard accounting information as shown below). Click **Next.**



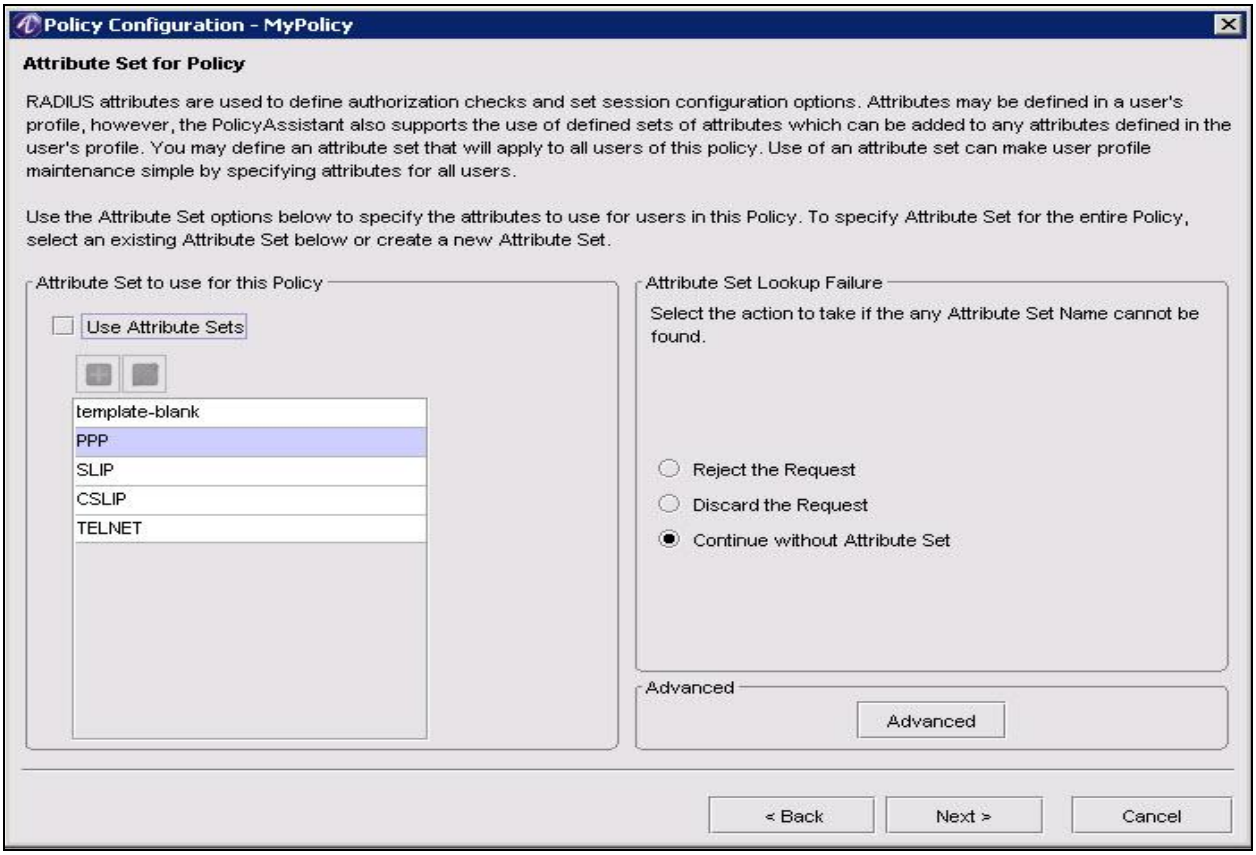
7. Enter your choices for **User Session Limits** and **Policy Limits**. Click **Next.**



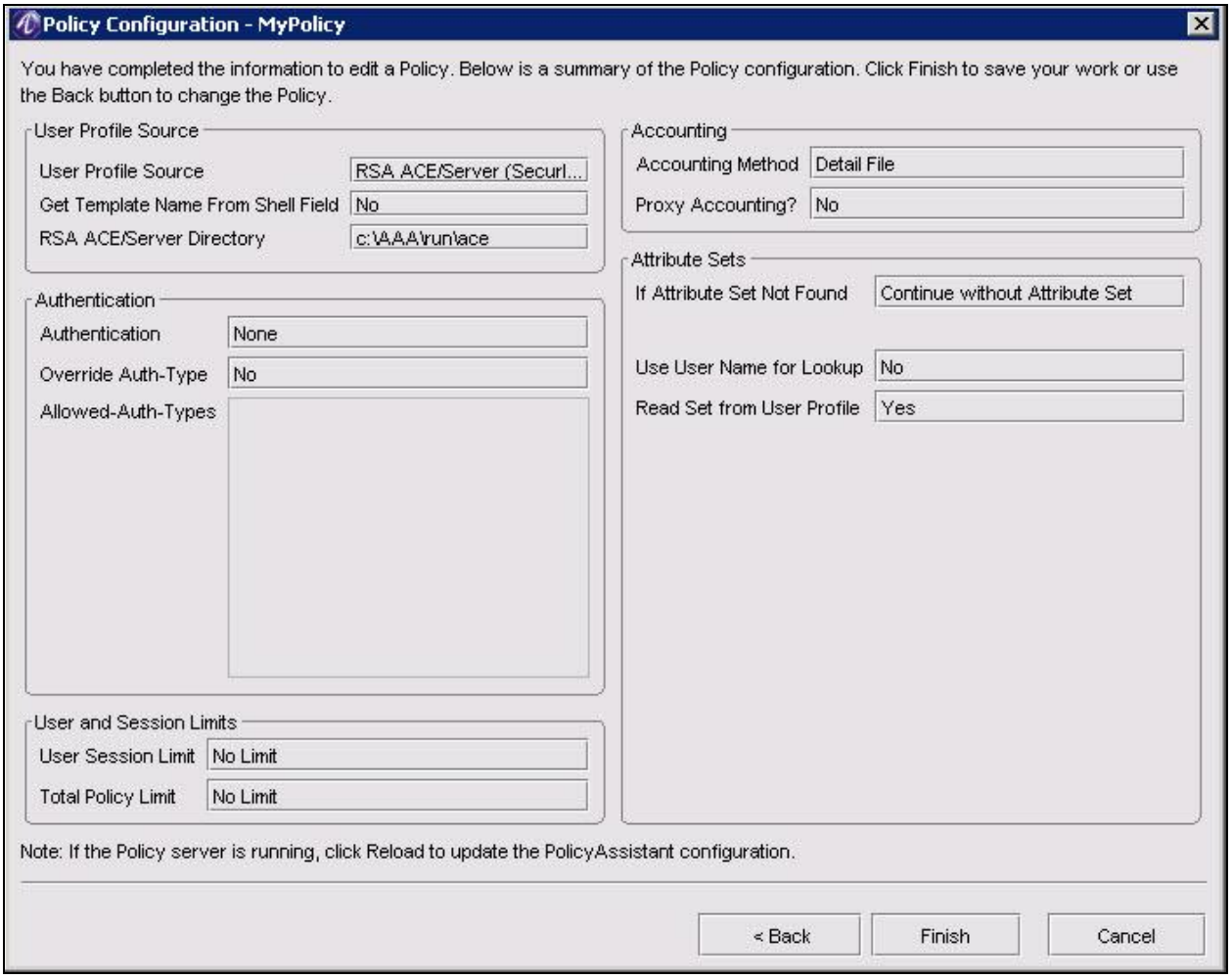
8. Enter the path to where the RSA ACE/Server file (rsa_api.properties) resides. The default path is: <base_dir>\run\ace. Click **Next**.



9. Configure attribute settings relative to your environment (for testing purposes we unchecked **Use Attribute Sets**). Select **Continue without Attribute Set** under the Attribute Set Lookup Failure pane. Click **Next.**



10. Review your selections and make any changes if needed. Click **Finish.**



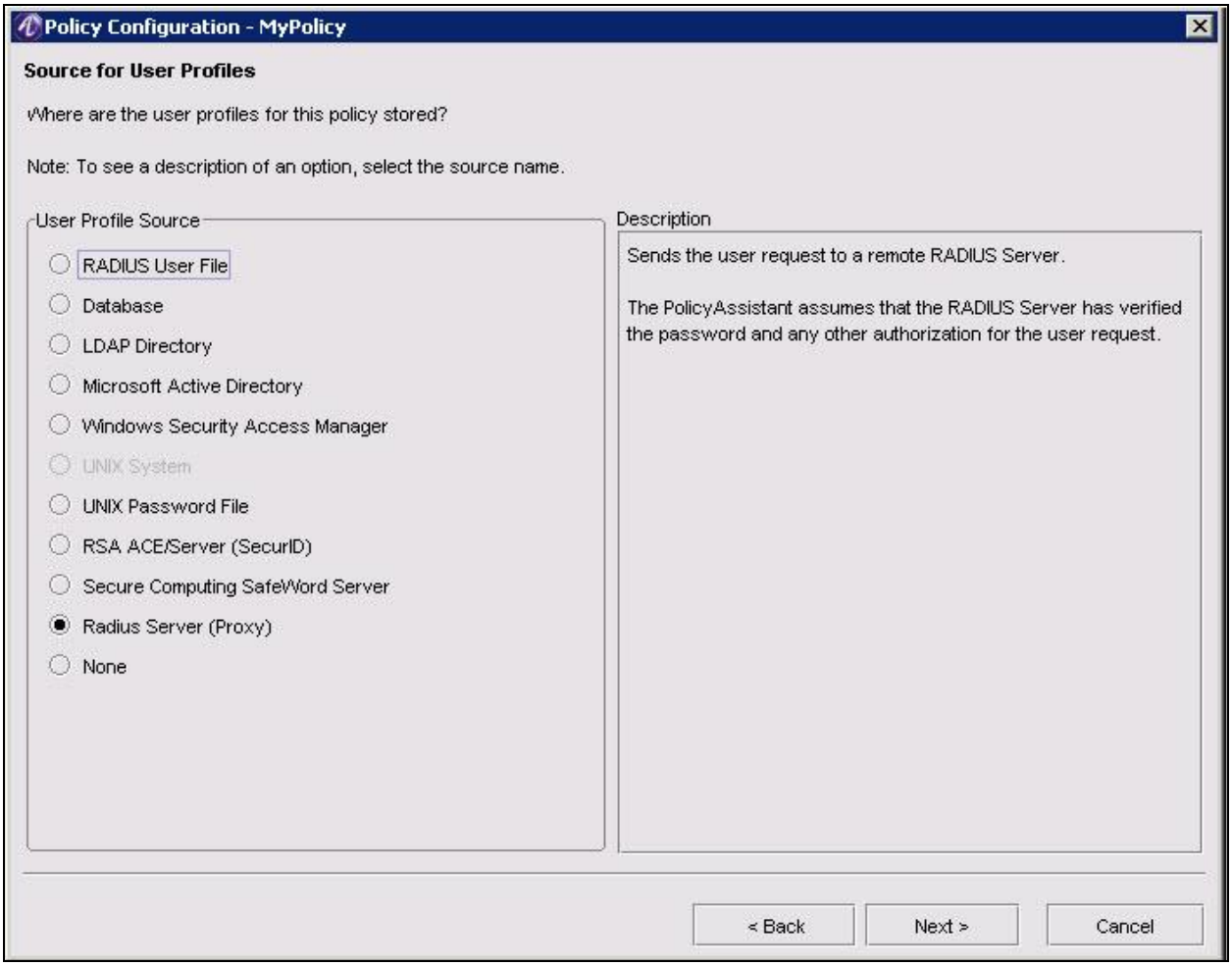
11. Save the configuration by clicking the **floppy icon** from the tool bar.
12. Under the **Policy Server icon** select **Restart Server**.

13. Follow the steps in the section **Create a Policy Rule**.
14. Follow the steps in the section **Add a RADIUS Client**.

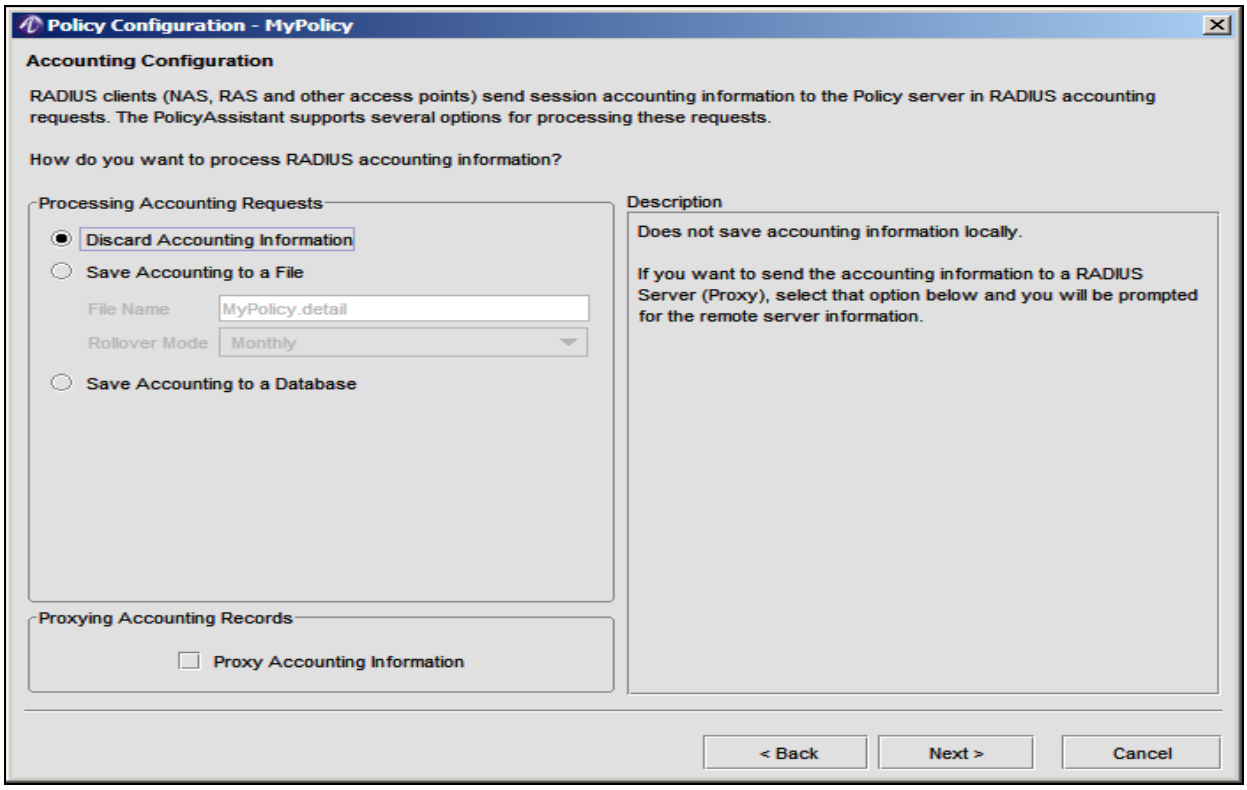
8950 AAA is now configured to receive a RADIUS request and forward to the RSA Authentication Manager via Native SecurID.

Creating a Radius ProxyPolicy

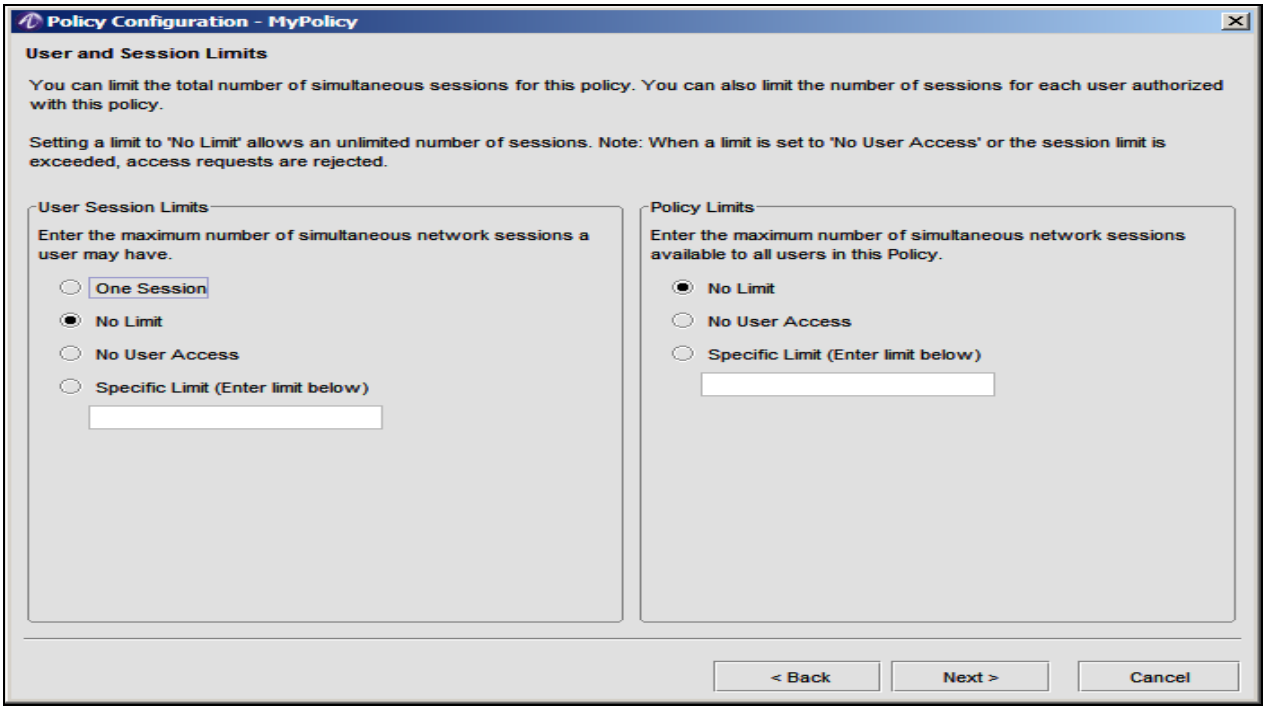
1. Launch the Server Management Tool and start the Policy Assistant by selecting **Policies > Policy Assistant** in the left window pane.
2. Click **Start the Policy Wizard**.
3. Enter a name for your new policy. Click **Next.**
4. Select **Radius Server (Proxy)** from the list of User Profile Sources. Click **Next.**



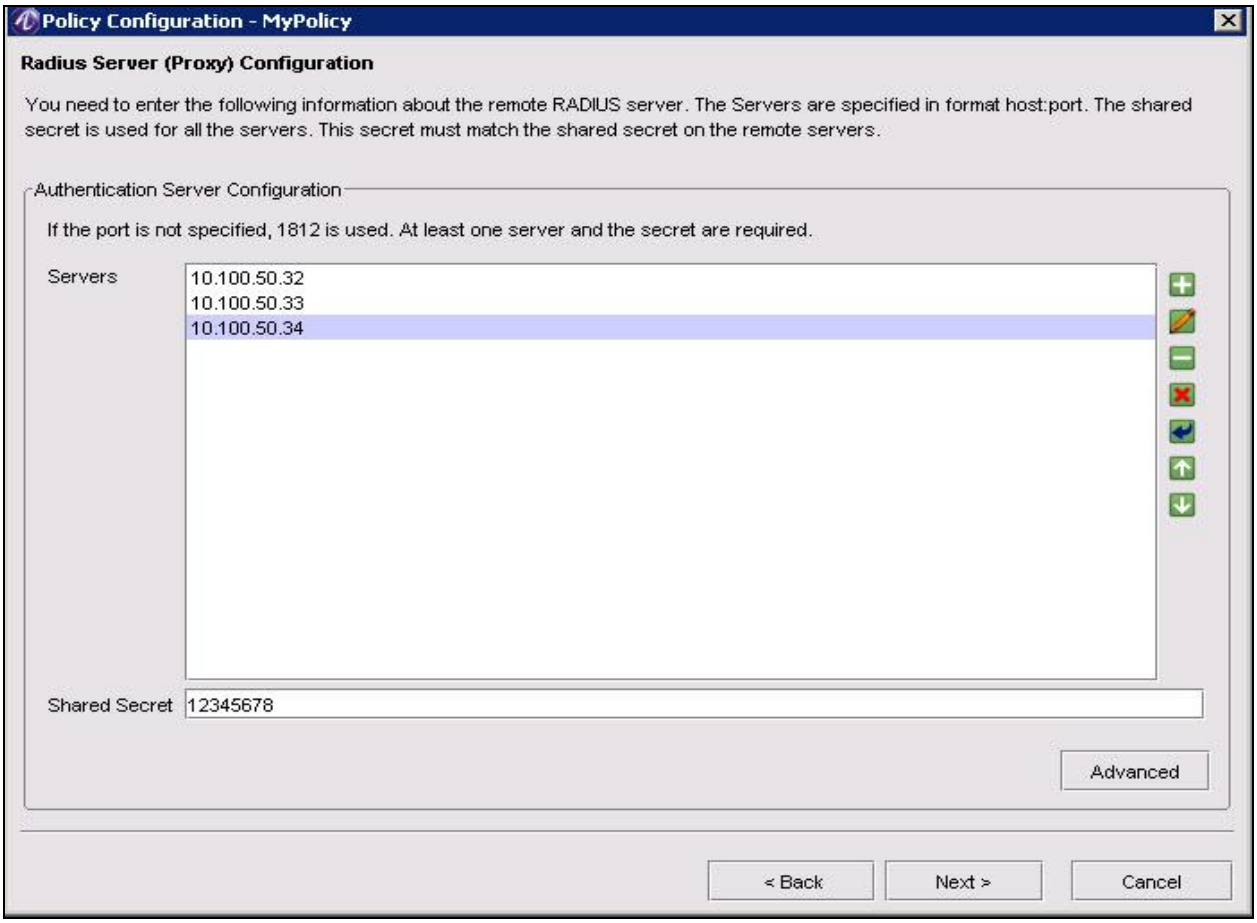
5. Enter selections for Accounting Configuration (for testing purposes we discard accounting information as shown below). Click **Next.**



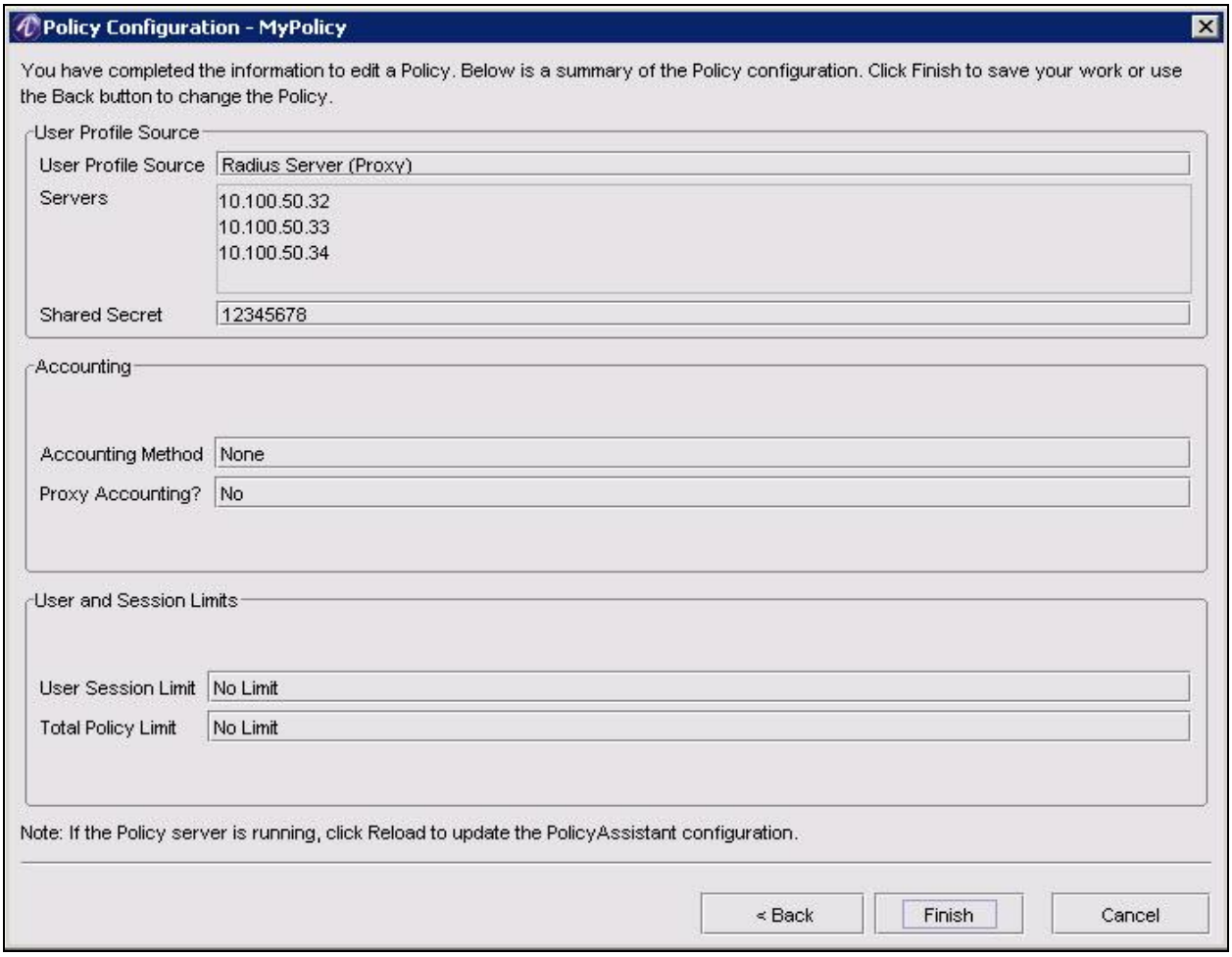
6. Enter your choices for User Session Limits and Policy Limits. Click **Next.**



7. Select the plus symbol and add the addresses of the RSA Authentication Manager and Replicas.
8. Enter the **Shared Secret** specified when creating the Radius Client in the RSA Security Console and click **Next**.



9. Review your selections and make any changes if needed. Click **Finish.**

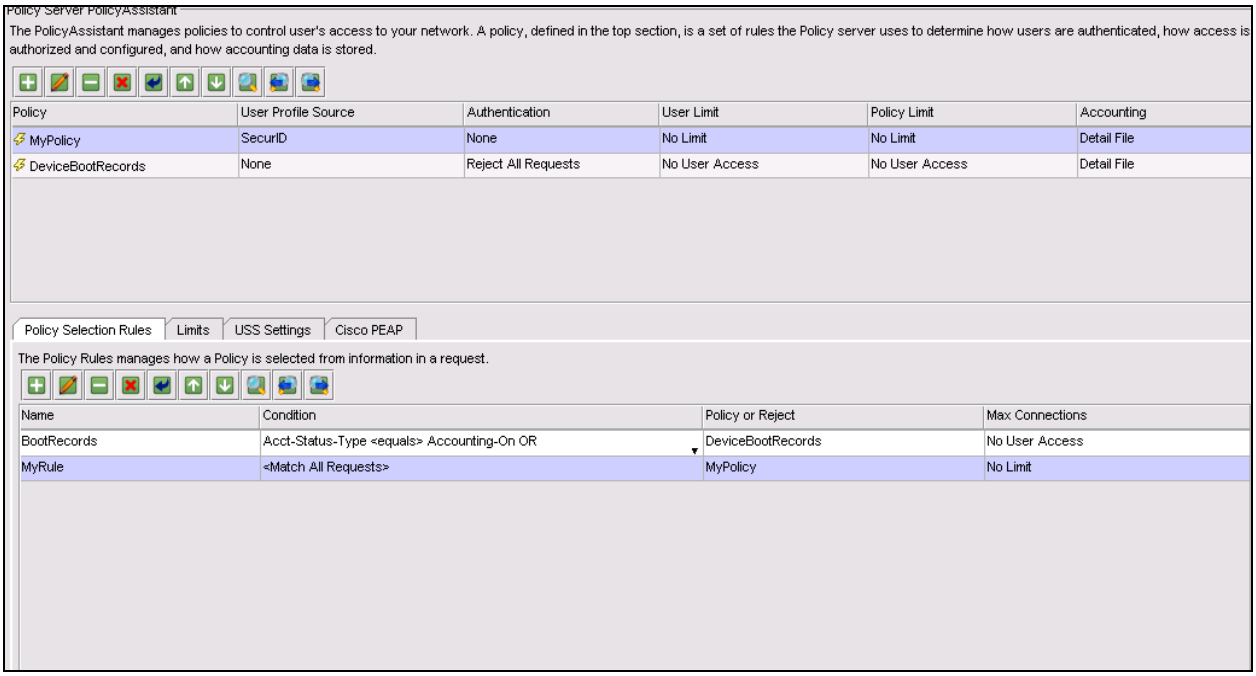


10. Follow the steps in the section **Create a Policy Rule**.
11. Follow the steps in the section **Add a RADIUS Client**.

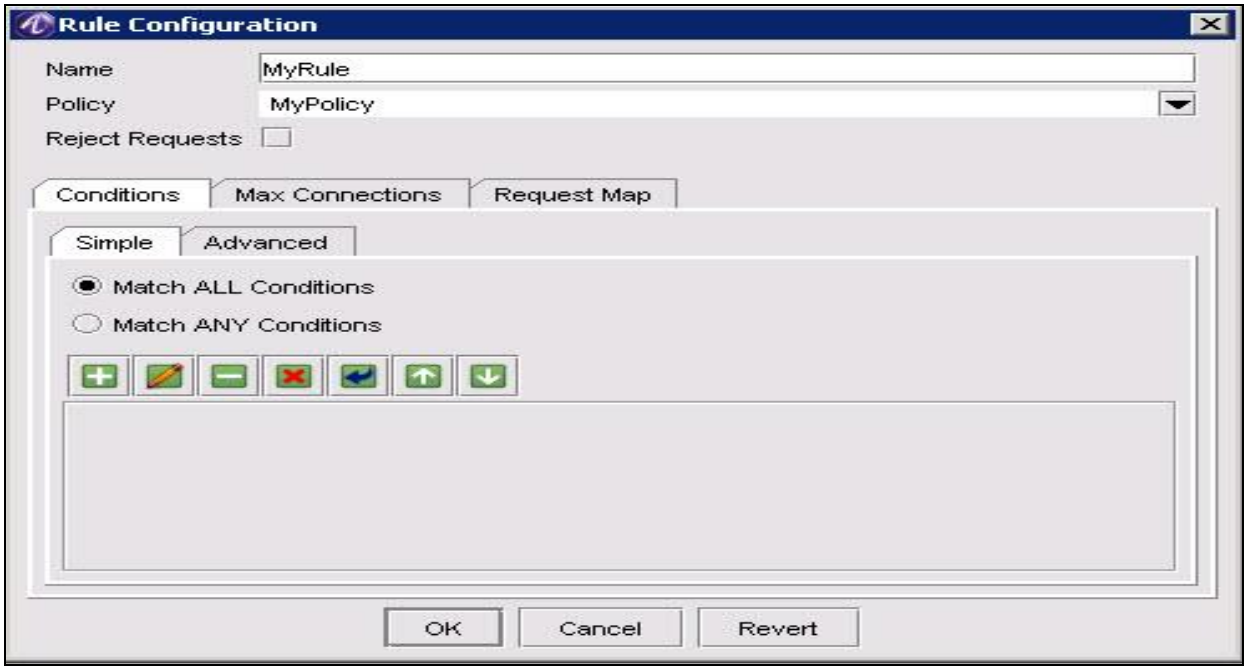
8950 AAA is now configured to receive a RADIUS request and forward RADIUS request to the RSA Authentication Manager.

Create a Policy Rule

1. Create a policy rule by selecting the plus symbol in the Policy Selection Rules screen.



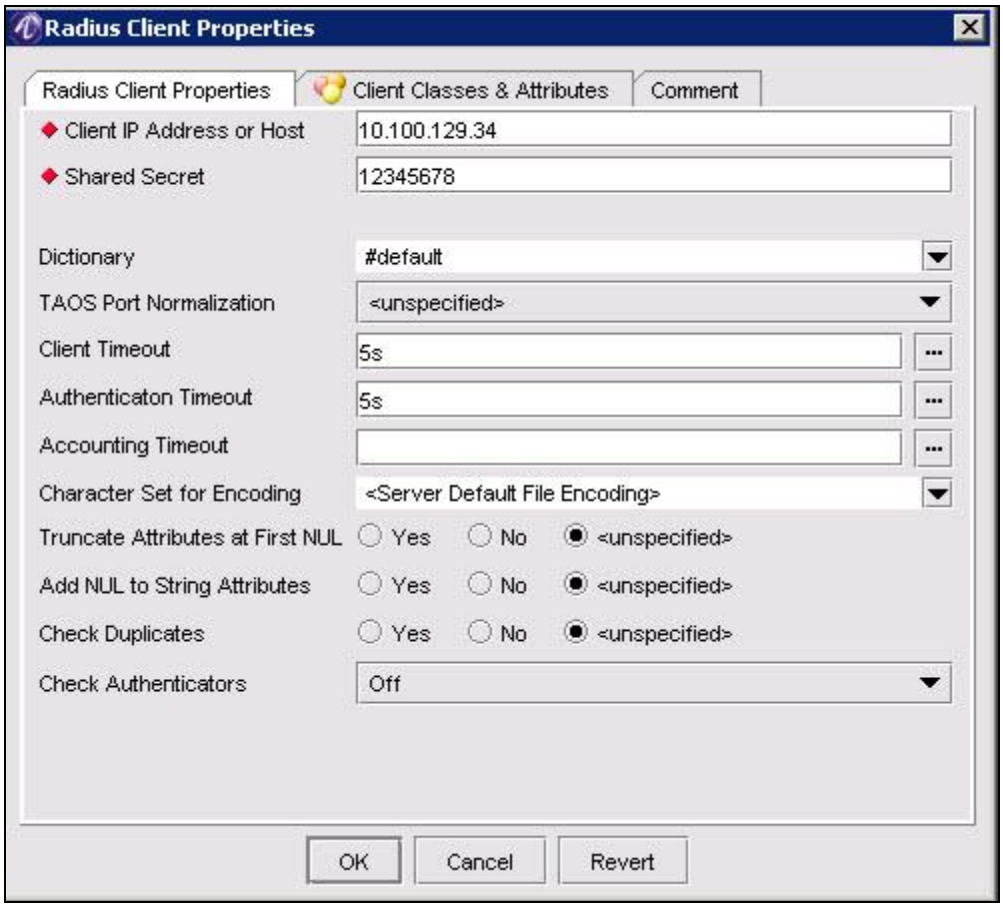
2. Enter a name for the rule and select the desired policy from the pull down.



3. Select the radio button for **Match All Conditions**.
4. Click **OK**.

Add a Radius Client

1. Expand the **Radius** folder from the navigation bar on the left and select **Radius Clients**.
2. Click the plus symbol to add a new client.
3. Enter the **Client IP Address, Shared Secret** and select the appropriate dictionary file.



4. Click **OK**.
5. Save the configuration by clicking the **floppy icon** from the tool bar.
6. Select **Restart Server** under the Policy Server icon.

Certification Checklist for RSA Authentication Manager

Date Tested: January 17, 2013

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	7.1 SP4	Windows 2003 (SP2)
8950 AAA	8.0	Windows XP Pro 32bit
CRYTPOCard RADIUS Client	1.0	Windows XP

Mandatory Functionality			
RSA Native Protocol		**RADIUS Protocol**	
New PIN Mode			
Force Authentication After New PIN	✓	Force Authentication After New PIN	✓
System Generated PIN	✓	System Generated PIN	✓
User Defined (4-8 Alphanumeric)	✓	User Defined (4-8 Alphanumeric)	✓
User Defined (5-7 Numeric)	✓	User Defined (5-7 Numeric)	✓
Deny 4 and 8 Digit PIN	✓	Deny 4 and 8 Digit PIN	✓
Deny Alphanumeric PIN	✓	Deny Alphanumeric PIN	✓
Deny Numeric PIN	✓	Deny Numeric PIN	✓
Deny PIN Reuse	✓	Deny PIN Reuse	✓
Passcode			
16-Digit Passcode	✓	16-Digit Passcode	✓
4-Digit Fixed Passcode	✓	4-Digit Fixed Passcode	✓
Next Tokencode Mode			
Next Tokencode Mode	✓	Next Tokencode Mode	✓
On-Demand Authentication			
On-Demand Authentication	✓	On-Demand Authentication	✓
On-Demand New PIN	✓	On-Demand New PIN	✓
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	✓	Failover	✓
No RSA Authentication Manager	✓	No RSA Authentication Manager	✓

GLS

✓ = Pass ✗ = Fail N/A = Not Applicable to Integration

Note: Complete testing was performed using clients on both IPv4 and IPv6 networks.

Note: Tested with CRYPTOCard Simple RADIUS Test Client.

Appendix

Partner Integration Details	
RSA SecurID API	8.1.1 API details below
RSA Authentication Agent Type	Standard Agent
RSA SecurID User Specification	Designated Users
Display RSA Server Info	No
Perform Test Authentication	No
Agent Tracing	Yes

API Details:

The AuthRsaAce plugin within the 8950 AAA server uses the RSA Authentication Agent API 8.1.1 for Java. The API determines which files to use and how to log are based on settings in an rsa_api.properties file. By default, the rsa_api.properties file is located in the <base_dir>\run\ace directory. More information about the AuthRsaAce plugin can be found in the Plugin Quick Reference Guide located in the <base_dir>\doc\plugins directory.

Node Secret:

The node secret (securid) is created in the <base_dir>\run\ace directory. This file should be deleted when clearing the node secret and the Policy Server should be restarted.

sdconf.rec:

The sdconf.rec file is placed in the <base_dir>\run\ace directory. This is configurable through the rsa_api.properties file.

sdopts.rec:

The sdopts.rec file is placed in the <base_dir>\run\ace directory. This is configurable through the rsa_api.properties file.

JAStatus.1:

The JAStatus.1 file is created in the <base_dir>\run\ace directory after a successful authentication. This is configurable through the rsa_api.properties file.

Agent Tracing:

Agent debugging can be enabled through the rsa_api.properties file located in the <base_dir>\run\ace directory.

IPv6 support:

The 8950 AAA employs a dual IP stack to support both IPv4 and IPv6 address types. This feature enables 8950 to proxy authentication requests from hosts on IPv6 networks to RSA Authentication Manager servers on IPv4 networks.