



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.



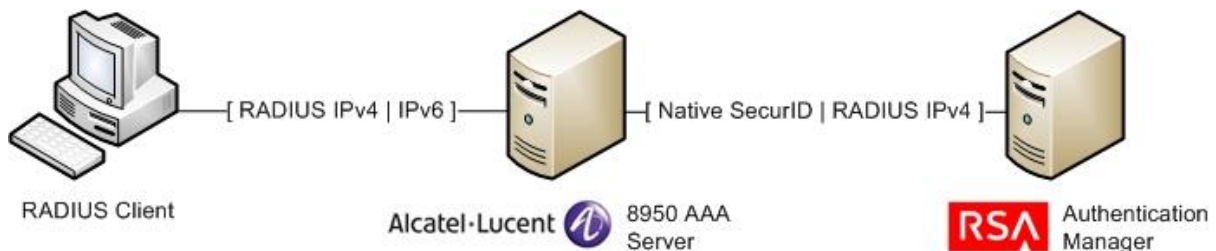
Solution Summary

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
JASstatus.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.

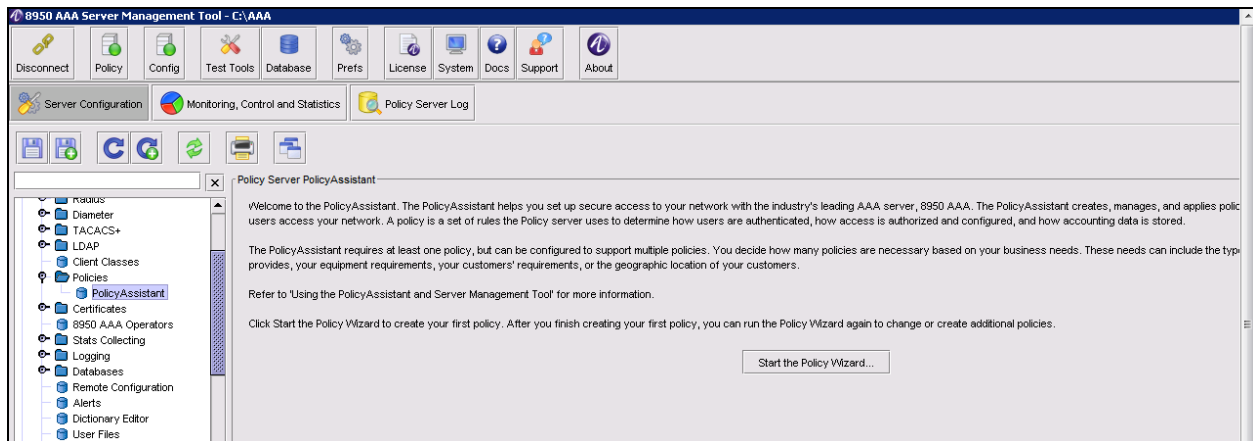
All 8950 AAA components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

8950 AAA Configuration

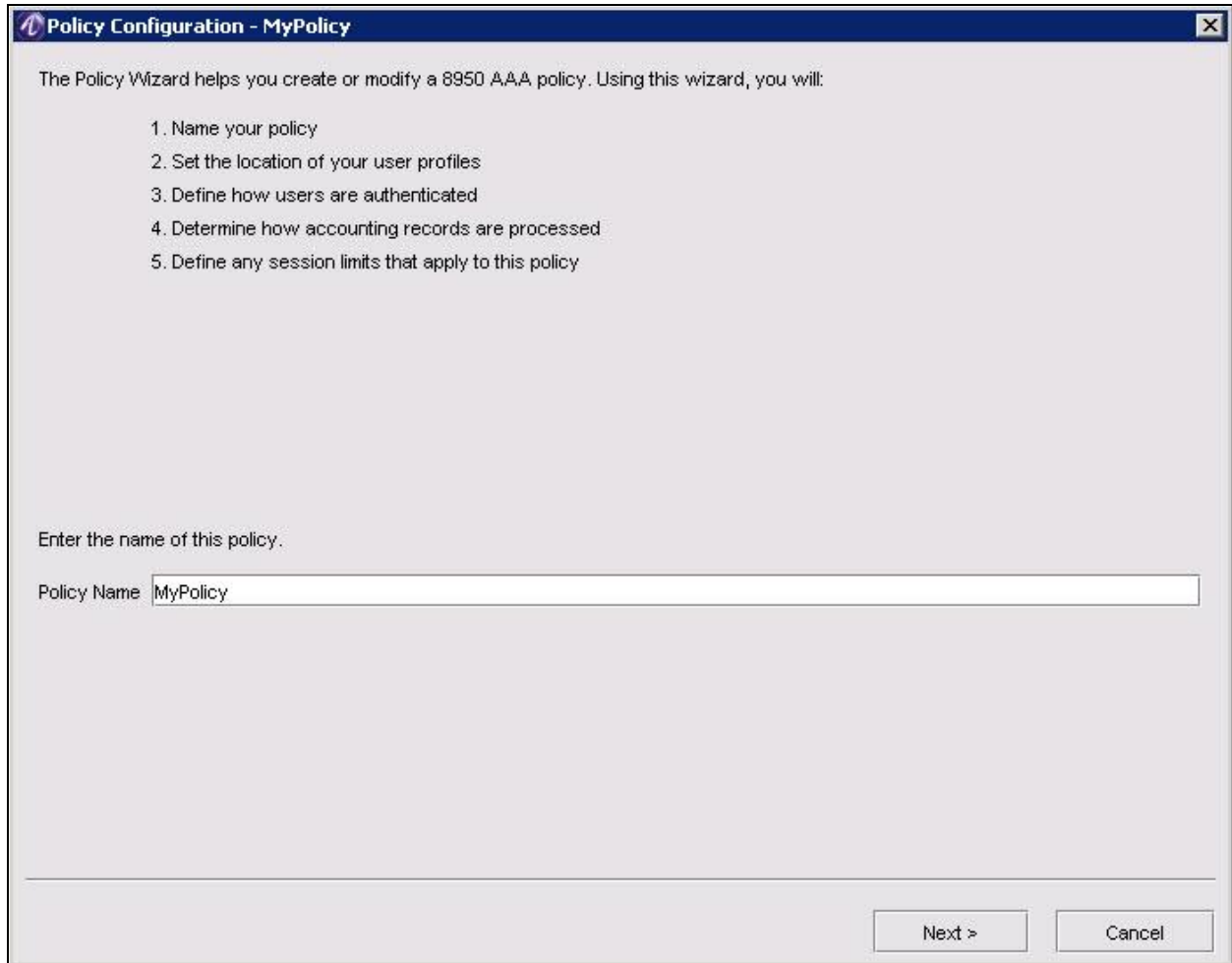
The 8950 AAA can communicate with the RSA Authentication Manager via Native SecurID or Radius. When communication with the RSA Authentication Manager via Radius you will need to configure the 8950 AAA as a Radius Proxy server. To configure the 8950 AAA you will need to create a policy, (either for Native 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**.



Policy Configuration - MyPolicy

The Policy Wizard helps you create or modify a 8950 AAA policy. Using this wizard, you will:

1. Name your policy
2. Set the location of your user profiles
3. Define how users are authenticated
4. Determine how accounting records are processed
5. Define any session limits that apply to this policy

Enter the name of this policy.

Policy Name

Next > Cancel

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

Policy Configuration - MyPolicy

Source for User Profiles

Where are the user profiles for this policy stored?

Note: To see a description of an option, select the source name.

User Profile Source	Description
<input type="radio"/> RADIUS User File	
<input type="radio"/> Database	
<input type="radio"/> LDAP Directory	
<input type="radio"/> Microsoft Active Directory	
<input type="radio"/> Windows Security Access Manager	
<input type="radio"/> UNIX System	
<input type="radio"/> UNIX Password File	
<input checked="" type="radio"/> RSA ACE/Server (SecurID)	8950 AAA can read or request user information directly from an RSA ACE/Server. This feature provides support for SecurID tokens. For users stored in a RSA ACE/Server, you must use this source as your authentication source (where you store the user's password).
<input type="radio"/> Secure Computing SafeWord Server	
<input type="radio"/> Radius Server (Proxy)	
<input type="radio"/> None	

< Back Next > Cancel

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

Policy Configuration - MyPolicy

Accounting Configuration

RADIUS clients (NAS, RAS and other access points) send session accounting information to the Policy server in RADIUS accounting requests. The PolicyAssistant supports several options for processing these requests.

How do you want to process RADIUS accounting information?

Processing Accounting Requests:

- Discard Accounting Information
- Save Accounting to a File
 - File Name:
 - Rollover Mode:
- Save Accounting to a Database

Proxying Accounting Records:

- Proxy Accounting Information

Description:

Saves RADIUS accounting information to the specified file.

The format of the information is the traditional Lucent Detail File format.

Also, select the how often the file is rolled over to a new file. The default rollover is every month. The follow describes each rollover mode:

Hourly
The file is rolled over each hour: 08:00, 09:00, 10:00, etc. The year, month, day, and hour are appended to the file name. For example, given a file named 'acct' is named 'acct.2003060511' for 11:00 AM on June 5 of 2003.

Daily
The file is rolled over daily at 12:00 AM. The year, month and day are appended to the file name. For example, given a file named 'acct' is named 'acct.20030605' for June 5 of 2003.

Weekly
The file is rolled over each Sunday at 12:00 AM. The year and

< Back Next > Cancel

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

Policy Configuration - MyPolicy

User and Session Limits

You can limit the total number of simultaneous sessions for this policy. You can also limit the number of sessions for each user authorized with this policy.

Setting a limit to 'No Limit' allows an unlimited number of sessions. Note: When a limit is set to 'No User Access' or the session limit is exceeded, access requests are rejected.

User Session Limits
Enter the maximum number of simultaneous network sessions a user may have.

- One Session
- No Limit
- No User Access
- Specific Limit (Enter limit below)

Policy Limits
Enter the maximum number of simultaneous network sessions available to all users in this Policy.

- No Limit
- No User Access
- Specific Limit (Enter limit below)

< Back Next > Cancel

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**.

Policy Configuration - MyPolicy

RSA ACE/Server Configuration

8950 AAA supports an RSA Library version that is a new Java implementation than has better performance than the (old) OS Specific Library.

Enter the directory where the RSA ACE/Server file (rsa_api.properties) is stored. If not specified, defaults to the 8950 AAA 'run/ace' directory.

Path to RSA ACE file:

Specifies whether to get a user template name from the shell field returned by the RSA Server.

- Get Template Name From Shell Field

Advanced

< Back Next > Cancel

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**.

Policy Configuration - MyPolicy

Attribute Set for Policy

RADIUS attributes are used to define authorization checks and set session configuration options. Attributes may be defined in a user's profile, however, the PolicyAssistant also supports the use of defined sets of attributes which can be added to any attributes defined in the user's profile. You may define an attribute set that will apply to all users of this policy. Use of an attribute set can make user profile maintenance simple by specifying attributes for all users.

Use the Attribute Set options below to specify the attributes to use for users in this Policy. To specify Attribute Set for the entire Policy, select an existing Attribute Set below or create a new Attribute Set.

Attribute Set to use for this Policy

Use Attribute Sets

template-blank
PPP
SLIP
CSLIP
TELNET

Attribute Set Lookup Failure

Select the action to take if the any Attribute Set Name cannot be found.

Reject the Request
 Discard the Request
 Continue without Attribute Set

Advanced

Advanced

< Back Next > Cancel

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

Policy Configuration - MyPolicy

You have completed the information to edit a Policy. Below is a summary of the Policy configuration. Click Finish to save your work or use the Back button to change the Policy.

User Profile Source

User Profile Source: RSA ACE/Server (SecurID...)
Get Template Name From Shell Field: No
RSA ACE/Server Directory: c:\AAA\run\ace

Accounting

Accounting Method: Detail File
Proxy Accounting?: No

Authentication

Authentication: None
Override Auth-Type: No
Allowed-Auth-Types:

Attribute Sets

If Attribute Set Not Found: Continue without Attribute Set
Use User Name for Lookup: No
Read Set from User Profile: Yes

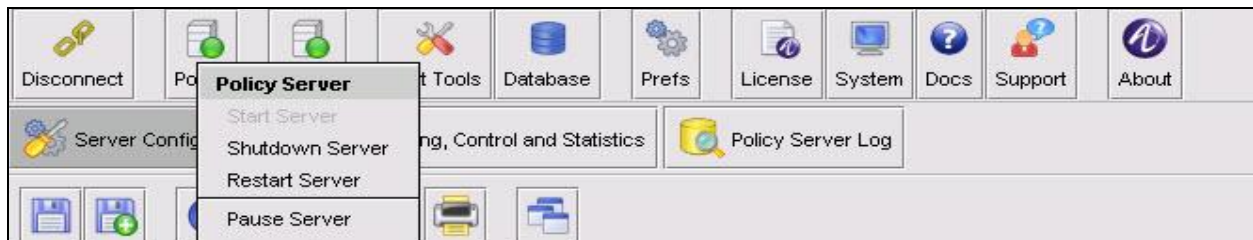
User and Session Limits

User Session Limit: No Limit
Total Policy Limit: No Limit

Note: If the Policy server is running, click Reload to update the PolicyAssistant configuration.

< Back Finish Cancel

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**.

Policy Configuration - MyPolicy

Source for User Profiles

Where are the user profiles for this policy stored?

Note: To see a description of an option, select the source name.

User Profile Source	Description
<input type="radio"/> RADIUS User File	Sends the user request to a remote RADIUS Server.
<input type="radio"/> Database	
<input type="radio"/> LDAP Directory	
<input type="radio"/> Microsoft Active Directory	
<input type="radio"/> Windows Security Access Manager	
<input type="radio"/> UNIX System	
<input type="radio"/> UNIX Password File	
<input type="radio"/> RSA ACE/Server (SecurID)	
<input type="radio"/> Secure Computing SafeWord Server	
<input checked="" type="radio"/> Radius Server (Proxy)	The PolicyAssistant assumes that the RADIUS Server has verified the password and any other authorization for the user request.
<input type="radio"/> None	

< Back Next > Cancel

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

Policy Configuration - MyPolicy

Accounting Configuration

RADIUS clients (NAS, RAS and other access points) send session accounting information to the Policy server in RADIUS accounting requests. The PolicyAssistant supports several options for processing these requests.

How do you want to process RADIUS accounting information?

Processing Accounting Requests

- Discard Accounting Information
- Save Accounting to a File
 - File Name:
 - Rollover Mode:
- Save Accounting to a Database

Proxying Accounting Records

- Proxy Accounting Information

Description

Does not save accounting information locally.

If you want to send the accounting information to a RADIUS Server (Proxy), select that option below and you will be prompted for the remote server information.

< Back Next > Cancel

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

Policy Configuration - MyPolicy

User and Session Limits

You can limit the total number of simultaneous sessions for this policy. You can also limit the number of sessions for each user authorized with this policy.

Setting a limit to 'No Limit' allows an unlimited number of sessions. Note: When a limit is set to 'No User Access' or the session limit is exceeded, access requests are rejected.

User Session Limits

Enter the maximum number of simultaneous network sessions a user may have.

- One Session
- No Limit
- No User Access
- Specific Limit (Enter limit below)

Policy Limits

Enter the maximum number of simultaneous network sessions available to all users in this Policy.

- No Limit
- No User Access
- Specific Limit (Enter limit below)

< Back Next > Cancel

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**.

Policy Configuration - MyPolicy

Radius Server (Proxy) Configuration

You need to enter the following information about the remote RADIUS server. The Servers are specified in format host:port. The shared secret is used for all the servers. This secret must match the shared secret on the remote servers.

Authentication Server Configuration

If the port is not specified, 1812 is used. At least one server and the secret are required.

Servers
10.100.50.32
10.100.50.33
10.100.50.34

Shared Secret: 12345678

Advanced

< Back Next > Cancel

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

Policy Configuration - MyPolicy

You have completed the information to edit a Policy. Below is a summary of the Policy configuration. Click Finish to save your work or use the Back button to change the Policy.

User Profile Source

User Profile Source: Radius Server (Proxy)

Servers: 10.100.50.32, 10.100.50.33, 10.100.50.34

Shared Secret: 12345678

Accounting

Accounting Method: None

Proxy Accounting?: No

User and Session Limits

User Session Limit: No Limit

Total Policy Limit: No Limit

Note: If the Policy server is running, click Reload to update the PolicyAssistant configuration.

< Back Finish Cancel

- Follow the steps in the section **Create a Policy Rule**.
- 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.

Policy Server PolicyAssistant
The PolicyAssistant manages policies to control user's access to your network. A policy, defined in the top section, is a set of rules the Policy server uses to determine how users are authenticated, how access is authorized and configured, and how accounting data is stored.

Policy	User Profile Source	Authentication	User Limit	Policy Limit	Accounting
MyPolicy	SecurID	None	No Limit	No Limit	Detail File
DeviceBootRecords	None	Reject All Requests	No User Access	No User Access	Detail File

Policy Selection Rules Limits USS Settings Cisco PEAP

The Policy Rules manages how a Policy is selected from information in a request.

Name	Condition	Policy or Reject	Max Connections
BootRecords	Acct-Status-Type <equals> Accounting-On OR	DeviceBootRecords	No User Access
MyRule	<Match All Requests>	MyPolicy	No Limit

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

Rule Configuration

Name: MyRule
Policy: MyPolicy
Reject Requests:

Conditions Max Connections Request Map

Simple Advanced

Match ALL Conditions
 Match ANY Conditions

OK Cancel Revert

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.

Radius Client Properties

Radius Client Properties | Client Classes & Attributes | Comment

◆ Client IP Address or Host: 10.100.129.34

◆ Shared Secret: 12345678

Dictionary: #default

TAOS Port Normalization: <unspecified>

Client Timeout: 5s

Authenticaton Timeout: 5s

Accounting Timeout:

Character Set for Encoding: <Server Default File Encoding>

Truncate Attributes at First NUL: Yes No <unspecified>

Add NUL to String Attributes: Yes No <unspecified>

Check Duplicates: Yes No <unspecified>

Check Authenticators: Off

OK Cancel Revert

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
CRYPTOCARD RADIUS Client	1.0	Windows XP

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 checked="" type="checkbox"/>
System Generated PIN	<input checked="" type="checkbox"/>	System Generated PIN	<input checked="" type="checkbox"/>
User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>	User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>
User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>	User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>
Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>	Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>
Deny Alphanumeric PIN	<input checked="" type="checkbox"/>	Deny Alphanumeric PIN	<input checked="" type="checkbox"/>
Deny Numeric PIN	<input checked="" type="checkbox"/>	Deny Numeric PIN	<input checked="" type="checkbox"/>
Deny PIN Reuse	<input checked="" type="checkbox"/>	Deny PIN Reuse	<input checked="" type="checkbox"/>
Passcode			
16-Digit Passcode	<input checked="" type="checkbox"/>	16-Digit Passcode	<input checked="" type="checkbox"/>
4-Digit Fixed Passcode	<input checked="" type="checkbox"/>	4-Digit Fixed Passcode	<input checked="" type="checkbox"/>
Next Tokencode Mode			
Next Tokencode Mode	<input checked="" type="checkbox"/>	Next Tokencode Mode	<input checked="" type="checkbox"/>
On-Demand Authentication			
On-Demand Authentication	<input checked="" type="checkbox"/>	On-Demand Authentication	<input checked="" type="checkbox"/>
On-Demand New PIN	<input checked="" type="checkbox"/>	On-Demand New PIN	<input checked="" type="checkbox"/>
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	<input checked="" type="checkbox"/>	Failover	<input checked="" type="checkbox"/>
No RSA Authentication Manager	<input checked="" type="checkbox"/>	No RSA Authentication Manager	<input checked="" type="checkbox"/>

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.