



## RSA SecurID Ready Implementation Guide

Last Modified: December 18, 2008

### Partner Information

---

Product Information	
Partner Name	Open System Consultants
Web Site	<a href="http://www.open.com.au">http://www.open.com.au</a>
Product Name	Radiator RADIUS Server, with AuthBY ACE
Version & Platform	4.3.1 on Windows, Linux, Solaris, AIX, HPUX
Product Description	A full featured, flexible, configurable, full source RADIUS server with native RSA SecurID support
Product Category	Radius Server





## Solution Summary

---

This document describes how the Radiator AuthBy ACE authentication module can be used to integrate with RSA Authentication Manager 6.1 and 7.1.

Radiator RADIUS Server integrates with RSA Authentication Manager as a:

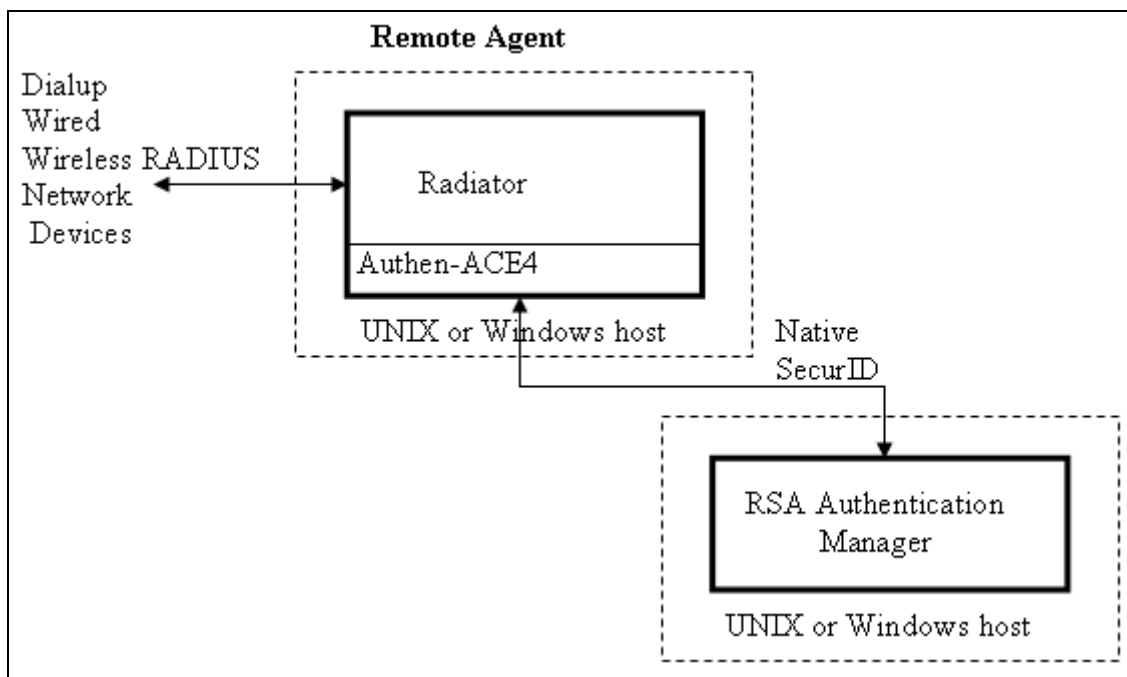
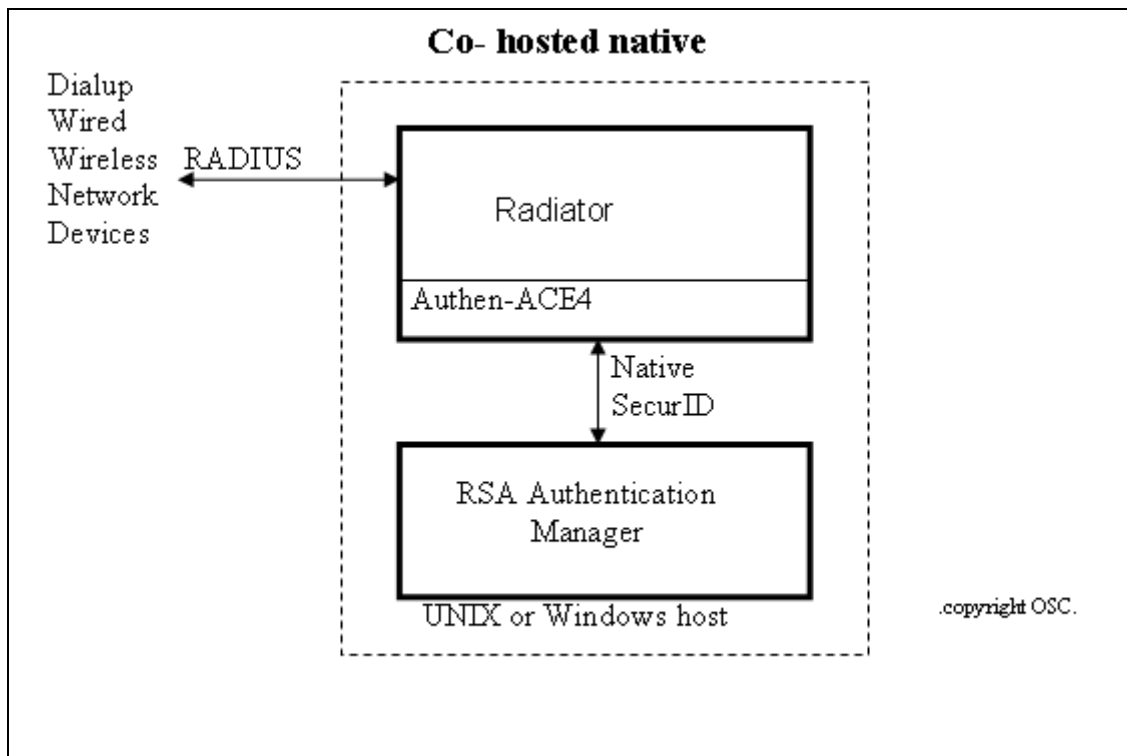
- native RSA Agent for direct authentication
- proxy by sending some or all RADIUS requests to RSA Authentication Manager RADIUS

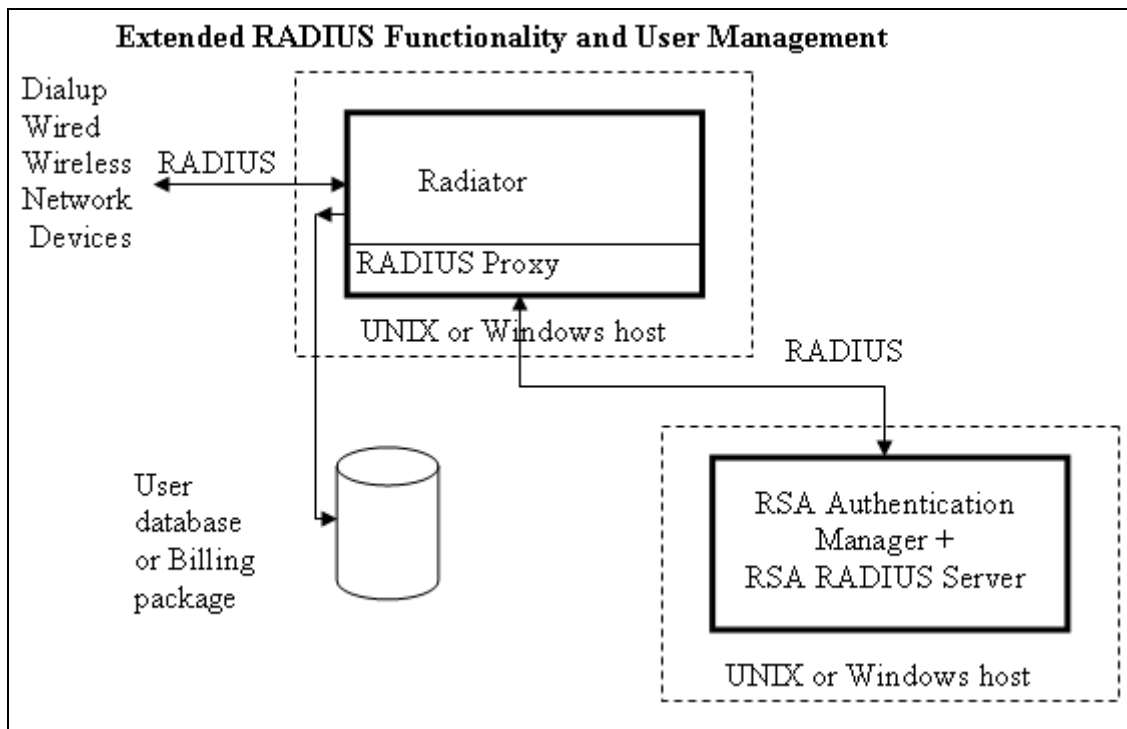
In either case, Radiator can be used to extend or enhance RSA authentication for added value or to add RSA authentication to existing RADIUS, TACACS+ or Diameter-based user management or billing systems, either custom or 3<sup>rd</sup> party. The use of Radiator with RSA Authentication Manager enables authentication solutions and flexibility that is not possible with either product alone.

Radiator is a highly flexible, full source, multi-platform RADIUS server that integrates with RSA Authentication Manager. The Radiator AuthBy ACE module uses the RSA Authentication Agent 6.1 to authenticate RSA tokens or static passwords against Authentication Manager 6.1/7.1.

Partner Integration Overview	
Authentication Methods Supported	Native RSA SecurID Authentication and RADIUS
List Library Version Used	6.1
RSA Authentication Manager Replica Support *	Full Replica Support
Secondary RADIUS Server Support	Yes (unlimited)
RSA Authentication Agent Host Type for 6.1	UNIX
RSA Authentication Agent Host Type for 7.1	Standard Agent
RSA SecurID User Specification	Designated Users, All Users (configurable)
RSA SecurID Protection of Administrative Users	Yes
RSA Software Token and RSA SecurID 800 Automation	Yes

Radiator can be deployed with RSA Authentication Manager in a number of ways, depending on exact requirements. Radiator can be deployed on one or more hosts (UNIX or Windows), on the same or different hosts as the ones where RSA Authentication Manager is deployed. This permits maximum flexibility and scalability. Some example architectures are shown below. Radiator's flexibility also permits many other types of deployment.







## Product Requirements

---

<b>Partner Product Requirements: Radiator RADIUS Server</b>	
<b>Version</b>	4.3.1
<b>CPU</b>	Intel, SPARC, PPC etc
<b>Memory</b>	512MB
<b>Hard Disk</b>	100MB

<b>Operating System</b>	
<b>Platform</b>	<b>Required Patches</b>
Windows NT, Server 2003, 2008, XP	All Patch Levels Supported
Linux	All Patch Levels Supported
Solaris 8, 9, 10	All Patch Levels Supported
HP-UX 10	All Patch Levels Supported
AIX	All Patch Levels Supported

<b>Additional Software Requirements</b>	
<b>Application</b>	<b>Additional Patches</b>
Perl 5.6 or 5.8	All Patch Levels Supported
Authen-ACE4 1.3	All Patch Levels Supported

# Agent Host Configuration

---

**!> Important: “Agent Host” and “Authentication Agent” are synonymous. “Agent Host” is a term used with the RSA Authentication Manager 6.x servers and below. RSA Authentication Manager 7.1 uses the term “Authentication Agent”.**

**!> Important: All “Authentication Agent” types for 7.1 should be set to “Standard Agent”.**

---

To facilitate communication between the Radiator 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 Radiator within its database and contains information about communication and encryption. You will also need to configure a RADIUS client.

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 the Radiator as UNIX Agent. This setting is used by the RSA Authentication Manager to determine how communication with the Radiator will occur.

To create the RADIUS client record, you will need the following information.

- Hostname
- IP Addresses for all 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 Security documentation for additional information about Creating, Modifying and Managing Agent Host, and RADIUS client records.


## RSA SecurID files

---

The location of the RSA Authentication Agent configuration files depends on the platform. On Windows, it is C:\Windows\System32. On UNIX, it defaults to /var/ace, but it is configurable, either through the Radiator configuration file, or with the VAR\_ ACE environment variable.

RSA SecurID Authentication Files	
Files	Location
sdconf.rec	VAR_ ACE/sdconf.rec
Node Secret	VAR_ ACE/securid
sdstatus.12	VAR_ ACE/sdstatus.12
sdopts.rec	VAR_ ACE/sdopts.rec

---

 **Note: Go to the appendix of this document to get detailed information regarding these files.**

---



## Partner Product 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.

### ***Installation***

In order for Radiator to be able to authenticate against an RSA Server, the Radiator host must have Perl, Radiator and the Authen-ACE4 Perl module installed. The instructions below describe how to install and configure the Radiator hosts(s), which may not be on the same as the RSA Server host.

The basic steps to install Radiator with RSA Authentication Manager support on the Radiator host are shown below. More detailed instructions are provided in `goodies/ace.txt` in the Radiator distribution.

### **Integration Overview: Windows**

1. Install ActivePerl 5.8 or later from <http://www.activestate.com>
2. Download and install the Radiator distribution. On Windows the self-extracting executable is easiest and preferred.
3. Install the Authen-ACE4 Perl module with the command shell command:  
`ppm install c:\Radiator\Radiator-4.3..1\ppm\Authen-ACE4.ppd`
4. Copy the `sdconf.rec` file from the RSA Server to `C:\Windows\System32` on the Radiator host.
5. Configure Radiator as described below.

### **Integration Overview: UNIX**

1. Ensure Perl is installed. On Solaris Perl from <http://www.sunfreeware.com> is recommended.
2. Ensure that GCC is installed. You will need this to build the Authen-ACE4 module for your platform.
3. Download and install the Radiator distribution. The full source distribution is preferred.
4. Obtain the RSA ACE/Agent SDK package for your platform from RSA.
5. Download, compile and install the Authen-ACE4 Perl module from <http://www.cpan.com> or from <http://www.open.com.au/radiator/free-downloads>.
6. Copy the `sdconf.rec` file from the RSA Server to `\opt\ace\data` on the Radiator host.
7. Configure Radiator as described below.

### **Configuring Radiator**

1. Ensure that basic RSA authentication works from the Radiator host to the RSA Server host. Use the tools provided by RSA in the ACE Agent or Authentication Agent software to confirm this. Unless native RSA Authentication works, Radiator will not be able to authenticate to RSA Server.
2. Create a Radiator configuration file with an `<AuthBy ACE>` clause. Use the sample configuration file in `goodies/ace.cfg` as a starting point.
3. Start Radiator with the configuration file.
4. Test basic Radiator authentication. Use the `radpwtst` program to send sample RADIUS authentication requests to Radiator which will then authenticate them against the RSA Server whose details are in the `sdconf.rec` file installed previously.
5. Complete configuration of Radiator, based on your specific requirements.
6. Arrange for Radiator to start automatically when the Radiator Host is booted.



## ***Testing Radiator with radpwstst***

The Radiator distribution contains the radpwstst program which can be used to test the complete Radiator/RSA Server installation.

In order to use radpwstst, you need a shell (on UNIX) or a Command Prompt (on Windows) on the Radiator host. Use a command something like:

```
perl radpwstst -noacct -interactive -user username -password 1111222222
```

Where username is the username of user to authenticate, and where 1111 is the user's PIN and 222222 is the user's current Tokencode.

# Certification Checklist For RSA Authentication Manager v6.x

Date Tested: December 17, 2008

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	6.1	Windows Server 2003
RSA Authentication Agent	6.1	Windows Server 2003
Radiator	4.3.1	Windows Server 2003

Mandatory Functionality			
RSA Native Protocol		RADIUS Protocol	
<b>New PIN Mode</b>			
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"/>
User Selectable	<input checked="" type="checkbox"/>	User Selectable	<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"/>
<b>Passcode</b>			
16 Digit Passcode	<input checked="" type="checkbox"/>	16 Digit Passcode	<input checked="" type="checkbox"/>
4 Digit Password	<input checked="" type="checkbox"/>	4 Digit Password	<input checked="" type="checkbox"/>
<b>Next Tokencode Mode</b>			
Next Tokencode Mode	<input checked="" type="checkbox"/>	Next Tokencode Mode	<input checked="" type="checkbox"/>
<b>Load Balancing / Reliability Testing</b>			
Failover (3-10 Replicas)	<input checked="" type="checkbox"/>	Failover	<input checked="" type="checkbox"/>
Name Locking Enabled	<input checked="" type="checkbox"/>	Name Locking Enabled	<input type="checkbox"/>
No RSA Authentication Manager	<input checked="" type="checkbox"/>	No RSA Authentication Manager	<input checked="" type="checkbox"/>
<b>Additional Functionality</b>			
<b>RSA Software Token Automation</b>			
System Generated PIN	<input type="checkbox"/> N/A	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
User Selectable	<input type="checkbox"/> N/A	User Selectable	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A
<b>RSA SecurID 800 Token Automation</b>			
System Generated PIN	<input type="checkbox"/> N/A	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
User Selectable	<input type="checkbox"/> N/A	User Selectable	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A
<b>Credential Functionality</b>			
Determine Cached Credential State	<input type="checkbox"/> N/A	Determine Cached Credential State	<input type="checkbox"/>
Set Credential	<input type="checkbox"/> N/A	Set Credential	<input type="checkbox"/>
Retrieve Credential	<input type="checkbox"/> N/A	Retrieve Credential	<input type="checkbox"/>

BSD / PAR

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

# Certification Checklist For RSA Authentication Manager 7.x

Date Tested: December 17, 2008

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	7.1	Windows Server 2003
RSA Authentication Agent	6.1	Windows Server 2003
Radiator	4.3.1	Windows Server 2003

Mandatory Functionality			
RSA Native Protocol		RADIUS Protocol	
<b>New PIN Mode</b>			
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"/>
PIN Reuse	<input checked="" type="checkbox"/>	PIN Reuse	<input checked="" type="checkbox"/>
<b>Passcode</b>			
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"/>
<b>Next Tokencode Mode</b>			
Next Tokencode Mode	<input checked="" type="checkbox"/>	Next Tokencode Mode	<input checked="" type="checkbox"/>
<b>Load Balancing / Reliability Testing</b>			
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"/>
<b>Additional Functionality</b>			
<b>RSA Software Token Automation</b>			
System Generated PIN	<input type="checkbox"/> N/A	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A
<b>RSA SecurID 800 Token Automation</b>			
System Generated PIN	<input type="checkbox"/> N/A	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A

BSD / PAR

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