RSA SecurID Ready Implementation Guide

Last Modified: July 14, 2003

1. Partner Information

Partner Name	Enterasys Networks
Web Site	http://www.enterasys.com/
Product Name	Aurorean Network Gateway
Version & Platform	Version 3.5 build 183 (3.5.2)
Product Description	The Aurorean VPN server is a universal platform consisting of the Aurorean Network Gateway and Policy Server for creating a global, virtual network that connects remote users and sites to corporate network resources. Each Aurorean server contains a high-speed processor that supports from hundreds to thousands of concurrent VPN connections. The Aurorean servers provide multiprotocol support and flexible configuration options that enable seamless integration into any environment. Strong encryption and enforcement of access controls provide maximum security. A redundant system design offers end-to-end high availability. Dedicated tunnel processing power and performance-enhancing compression algorithms optimize throughput and response time for all users on the network.
Product Category	Perimeter Defense (VPN)

ENTERASYS NETWORKS™

2. Contact Information

	Sales Contact	Support Contact
E-mail	sales@enterasys.com	support@enterasys.com
Web	http://www.enterasys.com/corporate/contact/contact-sales.html	www.enterasys.com/support

3. Solution Summary

Aurorean VPN servers along with SecurID enable VPN administrators to have a central database for effectively managing VPN clients for secure remote authentication. Administrators can use the VPN River Master management application for easy deployment and configuration of the ACE/Server authentication plug-in with practically no downtime with respect to VPN servers. The authentication mechanism built into RSA SecurID tokens combined with Enterasys Aurorean VPN ensures added security, simple management and peace of mind.

Feature	Details
Authentication Methods Supported	Native RSA SecurID, RADIUS
RSA ACE/Agent Library Version	5.03
RSA ACE 5 Locking	Yes
Replica RSA ACE/Server Support	Full Replica
Secondary RADIUS/TACACS+ Server Support	Yes
Location of Node Secret on Client	In Registry
RSA ACE/Server Agent Host Type	Communication server
RSA SecurID User Specification	Designated users
RSA SecurID Protection of Administrators	No

4. Product Requirements

- ***Hardware requirements***

Component Name: AVN 3000/7050 Appliances	
	Aurorean AVN 3000/7050 appliance

- ***Software requirements***

Component Name: AVN 3000/7050 Appliances	
Operating System	**Version (Patch-level)**
AVN 3000/7050	3.5 build 183 (3.5.2)

5. RSA ACE/Server configuration

For Native SecurID configuration the Aurorean Network Gateway needs to be configured as a Communication Server Agent Host on the RSA ACE/Server. For more information on configuring an Agent Host, please see the RSA ACE/Server Administrator's Guide.

For a RADIUS configuration, the Aurorean Network Gateway and the ACE/Server itself must be configured as Communication Server Agent Hosts on the RSA ACE/Server.

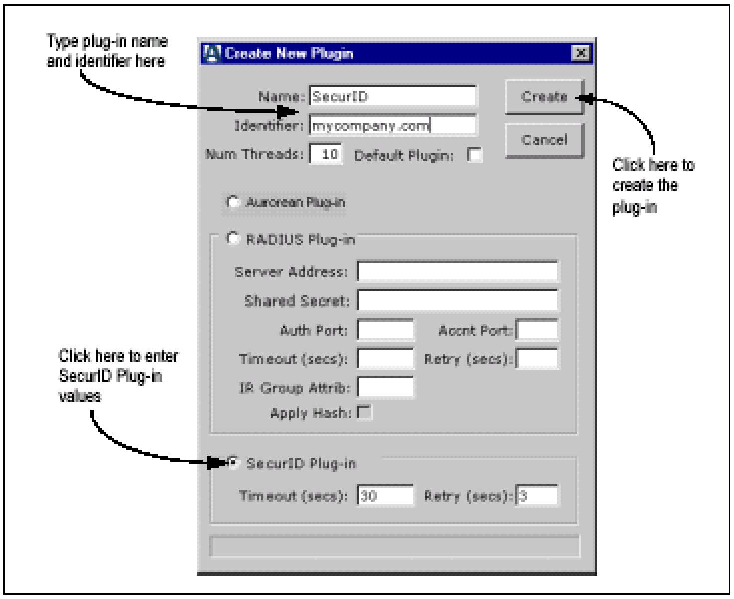
For more information on configuring an Agent Host, please see the RSA ACE/Server Administrator's Guide.

6. Partner RSA ACE/Agent configuration

A. Native SecurID Configuration

To configure the Aurorean Profile Server to forward authentication requests to the RSA ACE/Server via Native SecurID perform the following steps:

1. Open the Configuration pullout.
2. Choose Authorization Plug-ins from the Configure pull-down box in the top left corner of the pullout. Or, in the list of Aurorean devices, expand the tree list under the name of your APS (by clicking the + symbol), expand it again under Auth Service and click Make New Plug-in.
3. The Create New Plug-in window will appear



Type plug-in name and identifier here

Create New Plugin

Name: SecurID

Identifier: mycompany.com

Num Threads: 10 Default Plugin: □

○ Aurorean Plug-in

○ RADIUS Plug-in

Server Address:

Shared Secret:

Auth Port: Accnt Port:

Timeout (secs): Retry (secs):

IR Group Attrib:

Apply Hash: □

● SecurID Plug-in

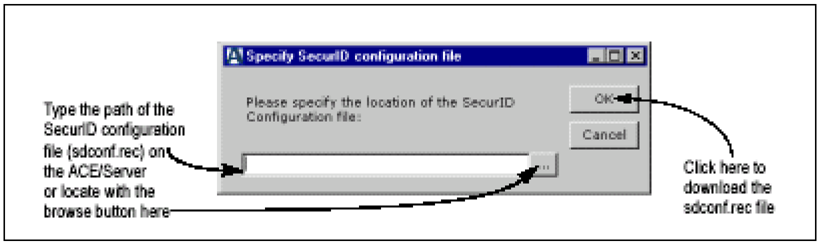
Timeout (secs): 30 Retry (secs): 3

Click here to create the plug-in

Click here to enter SecurID Plug-in values

4. In the Name field, type in a name to describe the plug-in. This name later appears in the plug-in tree list. For example, if you are adding a plug-in for a SecurID server, you can type **SecurID** as the name. If you plan to authenticate against more than one SecurID server, you can enter a specific server name in this field.

5. In the Identifier field, type a name that remote users will use to select this plug-in. Aurorean users can include this identifier as part of their VPN user names to override the default authorization plug-in. For example, if you enter **ACE** as the identifier for this plug-in, Aurorean users can specify a user name such as **Bob@ACE** to authenticate against the ACE/Server instead of the default plug-in.
6. Optionally, specify a value in the Num Threads field. This function allows the specified number of users to simultaneously log in without delay. The range of threads that can be set is 1 to 100, with a default value set to 10.
7. To make this plug-in the default authorization method, place a check next to Default Plug-In.
8. Click on SecurID Plug-in.
9. If desired, you can change the values for Timeout and Retry from the default values displayed. Timeout is the interval in seconds before another authorization attempt is made by the APS. Retry is the number of authorization attempts you will permit the APS to try.
10. Click Create.
11. The Specify SecurID configuration file window appears



Specify SecurID configuration file

Please specify the location of the SecurID Configuration file:

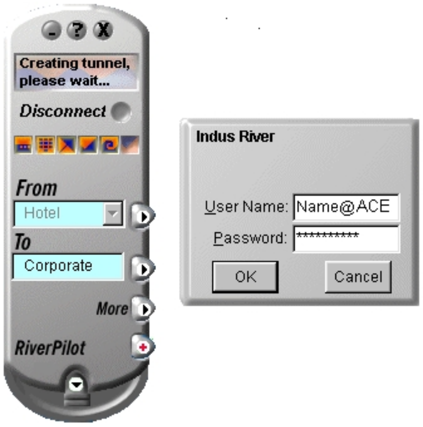
Type the path of the SecurID configuration file (sdconf.rec) on the ACE/Server or locate with the browse button here

Click here to download the sdconf.rec file

12. Type the path of the SecurID configuration file (SDCONF.rec) in the ACE/Server and click OK or find the file on the network by clicking the browse button to the right of the field.
13. If you typed the correct path of the configuration file, it is downloaded to its proper site on the APS and the plug-in saved. If you clicked the browse button, an Open window appears prompting you to locate the file.
14. When you find and select it, click Open and the Specify SecurID configuration file window will reappear. Then click OK and the process is complete.
15. Or you can copy the file off the ACE/Server to a floppy disk, load the disk in the RiverMaster floppy drive, and browse for the file on the a: drive.

Note - If a new SDCONF.rec becomes available, select the SecurID plug-in from the Auth Service list, click Properties and Update Configuration File, and repeat Step 12.

Users enter their username and PASSCODE to authenticate with SecurID.



Creating tunnel, please wait...

Indus River

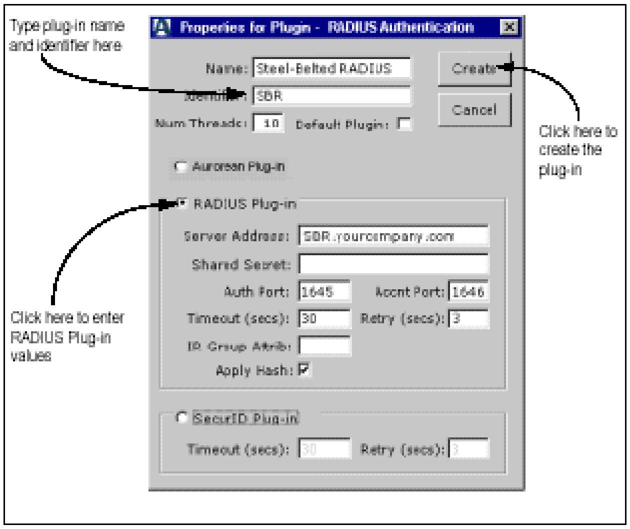
User Name: Name@ACE

Password: **********

B. RADIUS Configuration

To configure the Aurorean Profile Server to forward authentication requests to the RSA ACE/Server via RADIUS perform the following steps:

1. Open the Configuration pullout.
2. Choose Authorization Plug-ins from the Configure pull-down box in the top left corner of the pullout. Or, in the list of Aurorean devices, expand the tree list under the name of your APS (by clicking the + symbol), expand it again under Auth Service and click Make New Plug-in.
3. The Create New Plug-in window will appear



Type plug-in name and identifier here

Properties for Plugin - RADIUS Authentication

Name: Steel-Belted RADIUS

Identifier: SBR

Num Threads: 10 Default Plugin: □

○ Aurorean Plug-in

● RADIUS Plug-in

Server Address: SBR.yourcompany.com

Shared Secret:

Auth Port: 1645 Acont Port: 1646

Timeout (secs): 30 Retry (secs): 3

IP Group Attrib:

Apply Hash: ☑

○ SecurID Plug-in

Timeout (secs): 30 Retry (secs): 3

Click here to create the plug-in

Click here to enter RADIUS Plug-in values

4. In the Name field, type in a name to describe the plug-in. This name later appears in the plug-in tree list. For example, if you are adding a plug-in for a RADIUS server, you can type **RADIUS** as the name. If you plan to authenticate against more than one RADIUS server, you can enter a specific server name in this field.
5. In the Identifier field, type a name that remote users will use to select this plug-in. Aurorean users can include this identifier as part of their VPN user names to override the default authorization plug-in. For example, if you enter **RADIUS** as the identifier for this plug-in, Aurorean users can specify a user name such as **Bob@RADIUS** to authenticate against the RADIUS server instead of the default plug-in.
6. Optionally, specify a value in the Num Threads field. This function allows the specified number of users to simultaneously log in without delay. The range of threads that can be set is 1 to 100, with a default value set to 10.

   NOTE - Do not set Num Threads to a 0 (zero) value for a RADIUS plug-in. This will cause user login problems.
7. To make this plug-in the default authorization method, place a check next to Default Plug-In.
8. Click on Radius Plug-In.
9. In the Server Address field, enter the IP address or DNS name of the RADIUS server.
10. In the Shared Secret field, type the same shared secret password you entered on the RADIUS server. For more information on shared secrets, refer to the documentation supplied with your RADIUS server.

11. Leave the Authentication Port and Accounting Port fields set to their default values. These values specify UDP port numbers and match industry standards for RADIUS.
12. In the Timeout field, enter the number of seconds the APS should wait before resending an authentication request. If the RADIUS server fails to respond to an authentication request within the time specified, the APS automatically resends the request. For SecurID over RADIUS set this value to 30 seconds.
13. In the Retry field, enter the number of times the APS should resend an authentication request. For example, when this field is set to 2, the APS resends an authentication request twice before declaring the RADIUS server unreachable. For SecurID over RADIUS set this value to 1.
14. Click Commit to save the new plug-in. You will be prompted to re-type the Shared Secret.
15. Reboot the APS to enable the authorization changes.

7. Certification Checklist

Date Tested: July 14, 2003

Product	Tested Version
RSA ACE/Server	5.1
RSA ACE/Agent	5.03
Enterasys Networks Aurorean VPN servers	3.5 build 183 (3.5.2)

Test		ACE	RADIUS
1st time auth. (node secret creation)		P	P
New PIN mode:			
System-generated			
	Non-PINPAD token	P	P
	PINPAD token	P	P
User-defined (4-8 alphanumeric)			
	Non-PINPAD token	P	P
	Password	P	P
User-defined (5-7 numeric)			
	Non-PINPAD token	P	P
	PINPAD token	P	P
	SoftID token	P	P
	Deny 4 digit PIN	P	P
	Deny Alphanumeric	P	P
User-selectable			
	Non-PINPAD token	P	P
	PINPAD token	P	P
PASSCODE			
	16 Digit PASSCODE	P	P
	4 Digit Password	P	P
Next Tokencode mode			
	Non-PINPAD token	P	P
	PINPAD token	P	P
Failover		P	P
User Lock Test (RSA ACE Lock Function)		P	N/A
No RSA ACE/Server		P	P

PJV

Pass, Fail or N/A (N/A=Non-available function)

8. Known Issues

There are no known issues.