RSA SecurID Ready Implementation Guide

Last Modified: October 18, 2007

Partner Information

Product Information	
Partner Name	A10 Networks
Web Site	www.a10networks.com
Product Name	IDsentrie
Version & Platform	Release 2.1.1 build 17; IDsentrie 1U
Product Description	IDsentrie is the network identity management appliance with instant user identity resolution, which helps organizations of all sizes save time and minimizes risk by resolving security issues faster. IDsentrie is built on a flexible, virtual directory model for rapid integration with existing network infrastructure and support for a variety of popular data stores to simplify complex user resource management, and authentication and access issues.
Product Category	RADIUS Servers

Solution Summary

Partner Integration Overview	
Authentication Methods Supported	Both Native RSA SecurID Authentication and RADIUS
List Library Version Used	Version #5.3.1
RSA Authentication Manager name Locking	Yes
RSA Authentication Manager Replica Support	Full Replica Support
Secondary RADIUS Server Support	Yes, 4
Location of Node Secret on Agent	In Registry
RSA Authentication Agent Host Type	Communication Server, UNIX Agent
RSA SecurID User Specification	Designated Users, All uses, Default Method
RSA SecurID Protection of Administrative Users	Yes
RSA Software Token and RSA SecurID 800 Automation	No
Use of Cached Domain Credentials	No

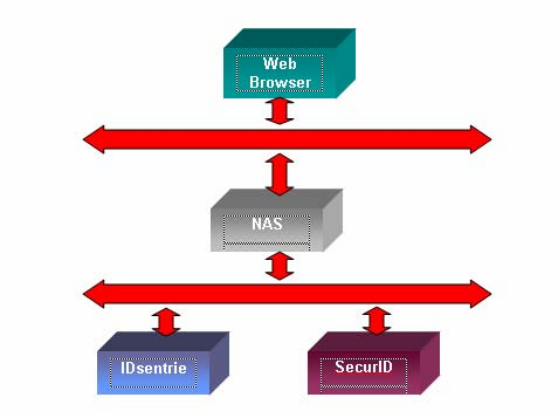
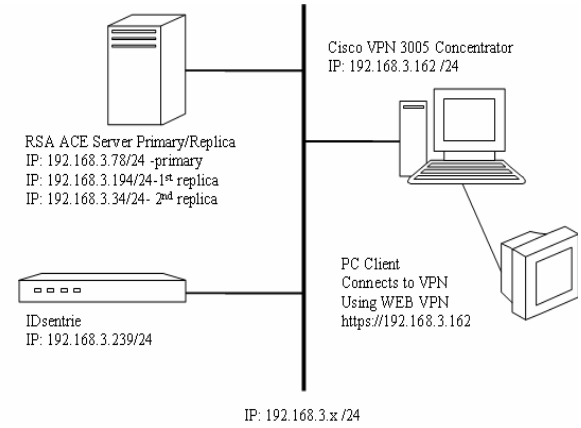


Diagram Network Flow



Network Topology

Product Requirements

Partner Product Requirements: IDsentrie	
Hardware Version	IDsentrie 1U
Software Version	Release 2.1.1 Build 17

Note: The A10 IDsentrie and IDaccess appliance runs a customized operating system. RSA SecurID authentication is completely supported from Release 1.0 without RADIUS failover. The RADIUS failover feature was added at Release 2.1.1 and 2.2.

Additional Software Requirements:

Additional Software Requirements	
Application	**Additional Patches**
IE 5.0 or above version	All Patch Levels Supported
Firefox 2.0 or above version	All Patch Levels Supported

Agent Host Configuration

To facilitate communication between IDsentrie and the RSA Authentication Manager / RSA SecurID Appliance, an Agent Host record must be added to the RSA Authentication Manager database and RADIUS server database. The Agent Host record identifies IDsentrie 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 IDsentrie as Communication Server. This setting is used by the RSA Authentication Manager to determine how communication with IDsentrie 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.

RSA SecurID files

RSA SecurID Authentication Files	
Files	**Location**
sdconf.rec	sdconf.rec File imported to preconfigured file path
Node Secret	In Registry
sdstatus.12	stored in the same file path
sdopts.rec	Optional, stored in the same file path

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.

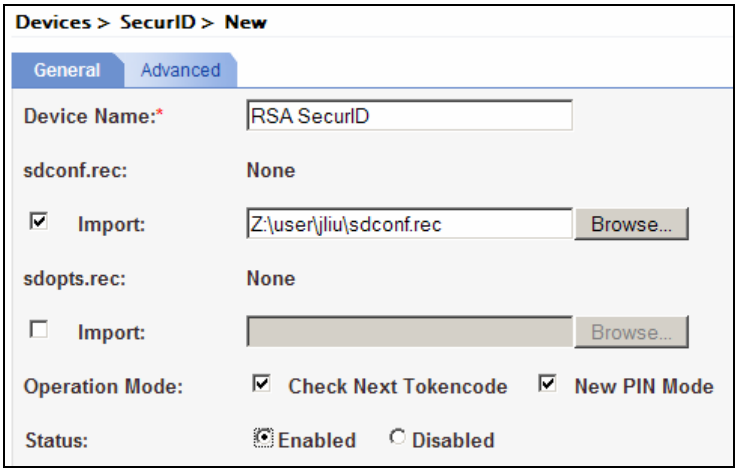
Documenting the Solution

IDsentrie supports both Native RSA SecurID and RADIUS Protocols. RSA SecurID could be added into IDsentrie either as a SecurID or a RADIUS Server device depends on which protocol to be used.

Configuring Native SecurID

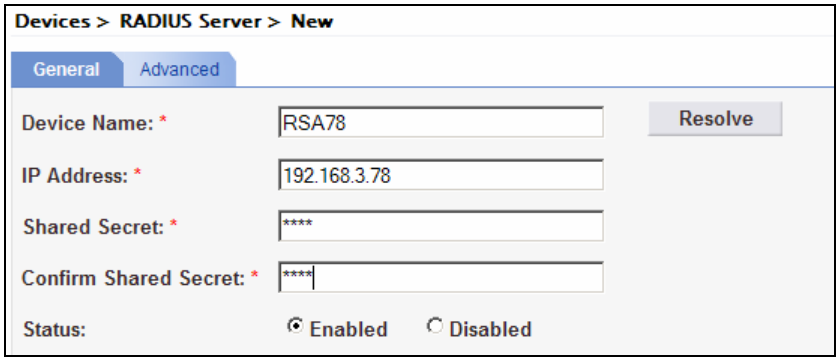
On IDsentrie, navigate to **Device > New > SecurID**, select the files and check both **"Check Next Tokencode"** and **"New PIN Mode"** in order to support these modes using RSA Native Protocol.

Also, make sure the Status is set to **"Enabled"**.

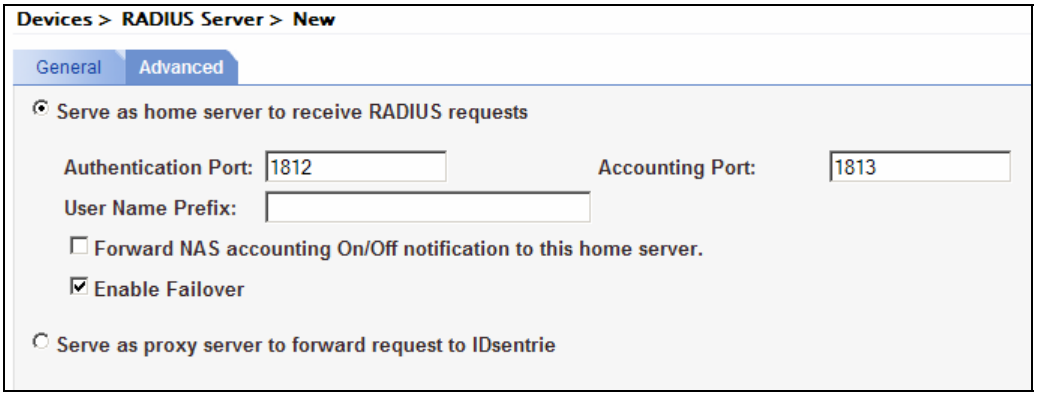


Configuring RADIUS SecurID

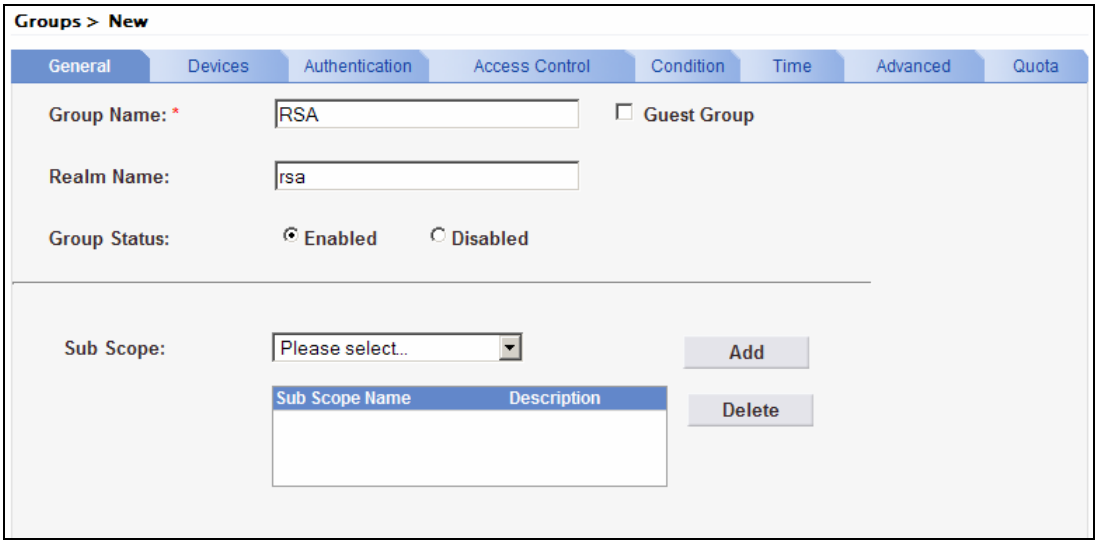
On IDsentrie WEB GUI, Navigate to **Device > RADIUS Server >New** and fill in the **General** tab, use the same encryption key set on RSA Server as shared secret.



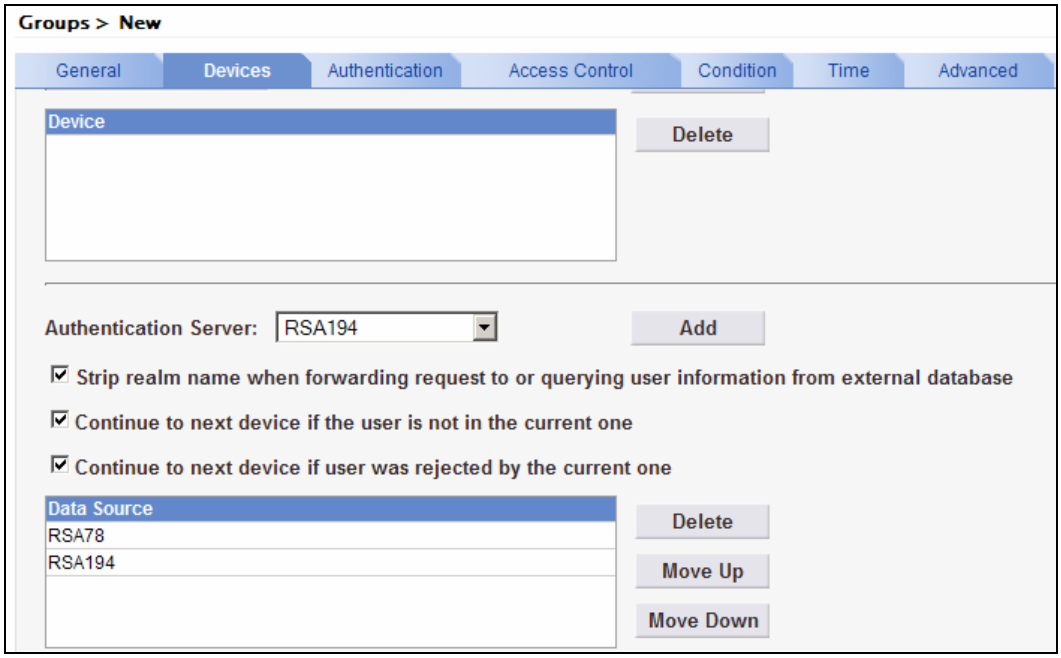
On **Advanced** tab, configure the authentication and/or accounting ports of RSA Radius Daemon. Remember to check **"Enable Failover"** if RADIUS failover is needed.



Navigate to **RADIUS > Action > New > Group**, create a **Group** and a realm name (if necessary) for this group on **General** tab:



On **Devices** tab, choose the previous RSA RADIUS server as the authentication servers. Check **"Strip realm"** if realm name need to be stripped when proxy user authentication. Check the next two options when failover is needed.



Certification Checklist For RSA Authentication Manager

Date Tested: August 3, 2007

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	6.0	Windows Server 2003
A10 IDsentrie	R2.1.1	Proprietary

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)	✓
User Selectable	✓	User Selectable	✓
Deny 4 and 8 Digit PIN	✓	Deny 4 and 8 Digit PIN	✓
Deny Alphanumeric PIN	✓	Deny Alphanumeric PIN	✓
Passcode			
16 Digit Passcode	✓	16 Digit Passcode	✓
4 Digit Password	✓	4 Digit Password	✓
Next Tokencode Mode			
Next Tokencode Mode	✓	Next Tokencode Mode	✓
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	✓	Failover	✓
Name Locking Enabled	✓	Name Locking Enabled	
No RSA Authentication Manager	✓	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 SecurID 800 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
Credential Functionality			
Determine Cached Credential State	N/A	Determine Cached Credential State	
Set Credential	N/A	Set Credential	
Retrieve Credential	N/A	Retrieve Credential	

BSD / PAR

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