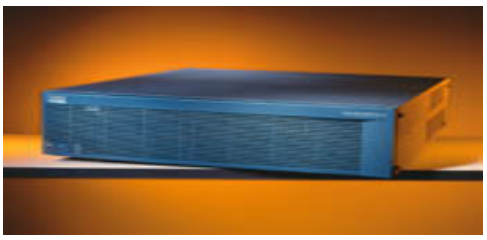
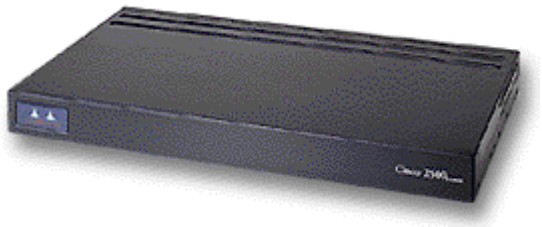
RSA SecurID Ready Implementation Guide

Last Modified: September 15, 2004

1. Partner Information

Partner Name	Cisco Systems
Web Site	www.cisco.com
Product Name	IOS Routers
Version & Platform	IOS 12.3.7T
Product Description	Cisco IOS® Software delivers a seamless integration of technology innovation, business-critical services, and hardware platform support. Currently operating on over ten million active systems, ranging from the small home office router to the core systems of the world's largest service provider networks.
Product Category	Remote Access





2. Contact Information

	Sales Contact	Support Contact
E-mail		cs-support-us@cisco.com
Phone	1-800-553-6387	1-800-553-6387
Web	www.cisco.com	www.cisco.com

3. Solution Summary

Feature	Details
Authentication Methods Supported	RADIUS
RSA Authentication Agent Library Version	N/A
RSA Authentication Manager Name Locking	N/A
RSA Authentication Manager Replica Support	N/A
Secondary RADIUS Server Support	Yes (Number is limited by hardware)
Location of Node Secret on Client	'None stored'
RSA Authentication Agent Host Type	Communication server
RSA SecurID User Specification	Designated users, all users
Support for Download of Offline Day Files	No
RSA SecurID Protection of Partner Product Administrators	Yes
RSA Software Token API Integration	No

4. Product Requirements

- ***Hardware requirements***

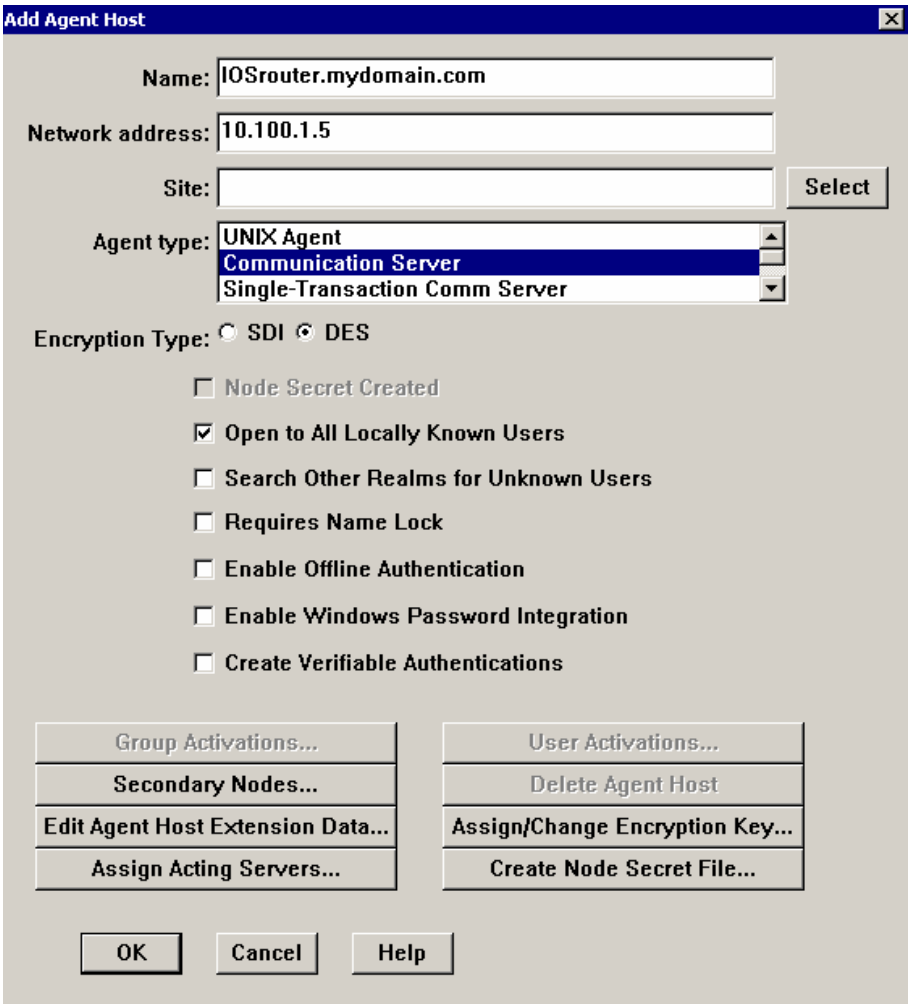
Component Name: Cisco IOS Router	
Firmware level	12.3.7T

5. RSA Authentication Manager configuration

Perform the following steps to set up the ***Cisco IOS Router*** as an Agent Host within the RSA Authentication Manager's database.

- On the RSA Authentication Manager computer, go to **Start > Programs > RSA ACE Server**, and then **Database Administration - Host Mode**.

1. On the **Agent Host** menu, choose **Add Agent Host…**.



   - In **Name**, type the hostname of the Cisco IOS Router.
   - In **Network address**, type the IP address of the Cisco IOS Router.
   - For **Agent Type**, select ***Communication Server***.
   - Under **Secondary Nodes**, define all hostname/IP addresses that resolve to the Cisco IOS Router. (IF NEEDED)
   - Under **Assign/Change Encryption Key**…, enter the encryption key. This must match the encryption key you enter on the Cisco IOS Router.

Note: It is important that all hostname and IP addresses resolve to each other. Please reference the RSA Authentication Manager documentation for detailed information on this and other configuration parameters within this screen. Subsequently, you can also select the 'Help' button at the bottom of the screen.

6. Partner RSA Authentication Agent configuration

This section provides instructions for integrating the partners' product with RSA SecurID. This document is not intended to suggest optimum installations or configurations. It is assumed that the reader has both working knowledge of the two products to perform the tasks outlined in this section and access to the documentation for both in order to install the required software components. All products/components need to be installed and working prior to this integration. Perform the necessary tests to confirm that this is true before proceeding.

Log onto the Cisco IOS Router and enter enable mode, by typing the word "enable" and giving the enable password. Then enter configuration mode by typing "config t". You are now able to enter the commands below to turn on authentication. Once you are done entering the commands hit <CTRL> Z. To turn off one of the commands put the word no in front of the command line and you will turn off that line.

The "aaa" command lines turn on authentication, tells the communication server what to authenticate and what protocol to use. The radius or tacacs commands inform the communication server what the IP address of the TACACS, or RADIUS server is, the time out value and what the encryption key is. The encryption key needs to be the same string on the TACACS or RADIUS server.

Note: CHAP authentication is not supported when using RSA SecurID authentication.

Cisco IOS Routers

1. Tacacs+ commands
aaa new-model
aaa authentication login default tacacs+ line enable
aaa authentication ppp default tacacs+
tacacs-server host xxx.xxx.xxx.xxx
tacacs-server timeout 120
tacacs-server key "your key"

2. RADIUS commands
aaa new-model
aaa authentication login default radius line enable
aaa authentication ppp default radius
radius-server host xxx.xxx.xxx.xxx auth-port 1645 acct-port 1646 key "your key"
radius-server timeout 120

7. Certification Checklist

Date Tested: September 16, 2004

Tested Certification Environment		
Product	**Platform (OS)**	**Product Version**
RSA Authentication Manager	WIN2K SP4	6.0
RSA Authentication Agent	N/A	N/A
RSA Software Token	WIN2K SP4	3.0.3 [008]
Cisco IOS Router	IOS	12.3.7T

Test	RSA Native Protocol	RADIUS Protocol
1st time auth. (node secret creation)	N/A	
New PIN mode:		
System-generated		
Non-PINPAD token	N/A	P
PINPAD token	N/A	P
User-defined (4-8 alphanumeric)		
Non-PINPAD token	N/A	P
Password	N/A	P
User-defined (5-7 numeric)		
Non-PINPAD token	N/A	P
PINPAD token	N/A	P
Software token	N/A	P
Deny 4 digit PIN	N/A	P
Deny Alphanumeric	N/A	P
User-selectable		
Non-PINPAD token	N/A	P
PINPAD token	N/A	P
PASSCODE		
16 Digit PASSCODE	N/A	P
4 Digit Password	N/A	P
"Pin-less" TokenCode	N/A	P
Next Tokencode mode		
Non-PINPAD token	N/A	P
PINPAD token	N/A	P
Software Token API Authentication		
New PIN mode	N/A	N/A
8 Digit PIN with 8 Digit TokenCode	N/A	N/A
Failover	N/A	P
User Lock Test (RSA Name Lock Function)	N/A	
No RSA Authentication Manager	N/A	P

SWA

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

8. Known Issues

- CHAP authentication is not supported when using RSA SecurID authentication.

Appendix

- .