RSA SecurID Ready Implementation Guide

Last Modified: November 18, 2004

1. Partner Information

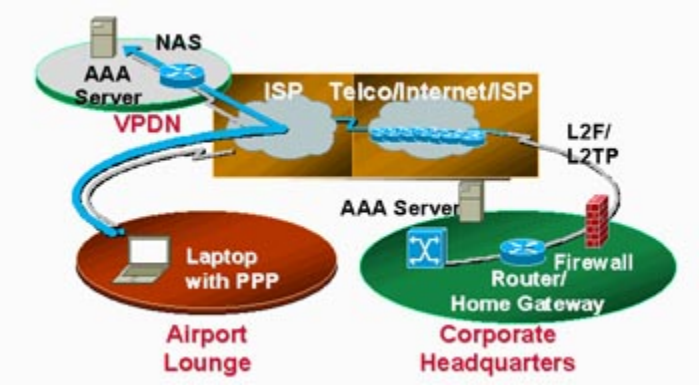
Partner Name	Cisco Systems
Web Site	www.cisco.com
Product Name	Cisco VPN 3000 Concentrator Series
Version & Platform	VPN 30xx
Product Description	Cisco VPN 3000 Series Concentrators is a family of purpose-built, remote access Virtual Private Network (VPN) platforms and client software that incorporates high availability, high performance and scalability with the most advanced encryption and authentication techniques available today. Supported connectivity mechanisms include IPSec and WebVPN (Clientless SSL Web browser-based connectivity).
Product Category	Perimeter Defense (Firewalls, VPNs & Intrusion Detection)

2. Contact Information

	Pre-Sales	Post-Sales
E-mail	sales@cisco.com	tac@cisco.com
Phone	1 800 553 6387	1 800 553 2447
Web	www.cisco.com	www.cisco.com/public/support/tac/home.shtml

3. Solution Summary

Feature	Details
Authentication Methods Supported	Native RSA SecurID and RADIUS
RSA Authentication Agent Library Version	Version # 5.02
RSA Authentication Manager Name Locking	Yes
RSA Authentication Manager Replica Support	Full Replica Support
Secondary RADIUS Server Support	Yes
Location of Node Secret on Client	Stored internally: Administration – File Mangement - *.SDI
RSA Authentication Agent Host Type	Communication server
RSA SecurID User Specification	Designated users for VPN client, all users for WEB VPN
Support for Download of Offline Day Files	No
RSA SecurID Protection of Partner Product Administrators	No
RSA Software Token API Integration	Yes



4. Product Requirements

- **VPN Concentrator**

  Hardware Supported:

  - Cisco VPN 3000 Series Concentrators, Models 3005 through 3080
  - Altiga Networks VPN Concentrators, Models C10 through C60

  Platform Files

  - Files beginning with vpn3000- support the VPN Concentrator 3015 through 3080 platforms.
  - Files beginning with vpn3005- support the VPN Concentrator 3005 platform only.

- **VPN Client**

  Operating Systems supported:

  - Microsoft® Windows® 95 (OSR2), Windows 98, or Windows 98 (second edition)
  - Windows ME
  - Windows NT® 4.0 (with Service Pack 6, or higher)
  - Windows 2000
  - Windows XP
  - Sun UltraSPARC, 32-bit or 64-bit Solaris kernel OS Version 2.6 or later
  - RedHat Version 6.2 or later Linux (Intel), or compatible libraries with glibc Version 2.1.1-6 or later, using kernel Versions 2.2.12 or later
  - Macintosh, OS X, Version 10.1.0 or later

  Hardware Supported:

  - 50 MB hard disk space.
  - RAM:
    - 32 MB for Windows 95/98
    - 64 MB for Windows
    - 64 MB for Unix, Linux

  To install the VPN Client on *any* system, you need:

  - CD-ROM drive (if you are installing from CD-ROM)
  - Administrator privileges

  The Cisco VPN Client supports the following Cisco VPN devices:

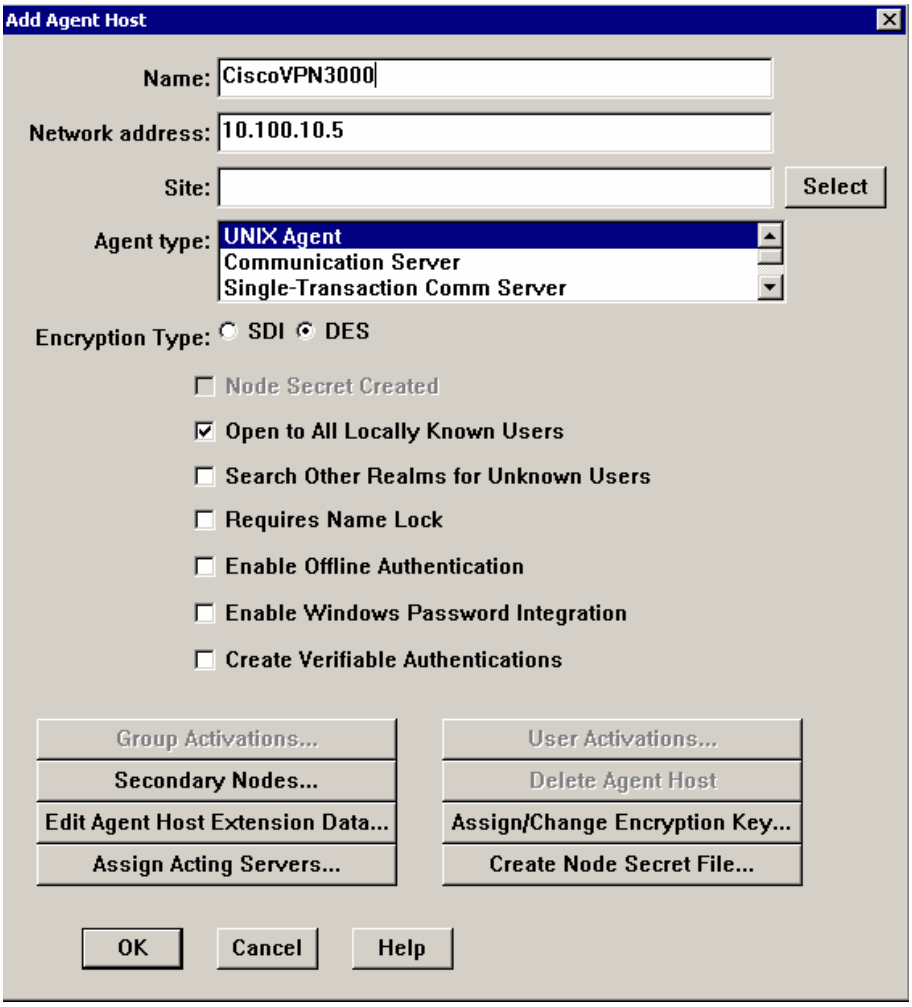
  - Cisco VPN 3000 Concentrator Series, Version 3.0 and later
  - Cisco PIX Firewall, Version 6.2.2 (122) or Version 6.3(1).
  - Cisco IOS Routers Version 12.2(8)T and later

5. RSA Authentication Manager configuration

Perform the following steps to set up the Cisco VPN 3000 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 VPN 3000.
   - In **Network address**, type the IP address of the Cisco VPN 3000.
   - For **Agent Type**, select Communication Server.
   - Under **Secondary Nodes**, define all hostname/IP addresses that resolve to the Cisco VPN 3000. (IF NEEDED)
   - (IF using RADIUS) Under Assign/Change Encryption Key…, enter the encryption key. This must match the encryption key you enter on the Cisco VPN 3000.

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 Cisco VPN 3000 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.

The VPN 3000 Concentrator Series appliance is configurable using a standard browser (Netscape or Internet Explorer). User must have authenticated using an authorized administrator username/password. If using SSL, user must first install the SSL certificate from the VPN3000.

Native RSA SecurID configuration

- The Cisco VPN 3000 has native support for SecurID authentication and does not require a RADIUS proxy/server to authenticate. In the Configuration > System > Servers > Authentication Screen, Add the following:

  Server Type: SDI
  Authentication Server: hostname or IP address of RSA ACE/Server
  SDI Server Version 5.0 or Pre-5.0
  Server Port: 5500

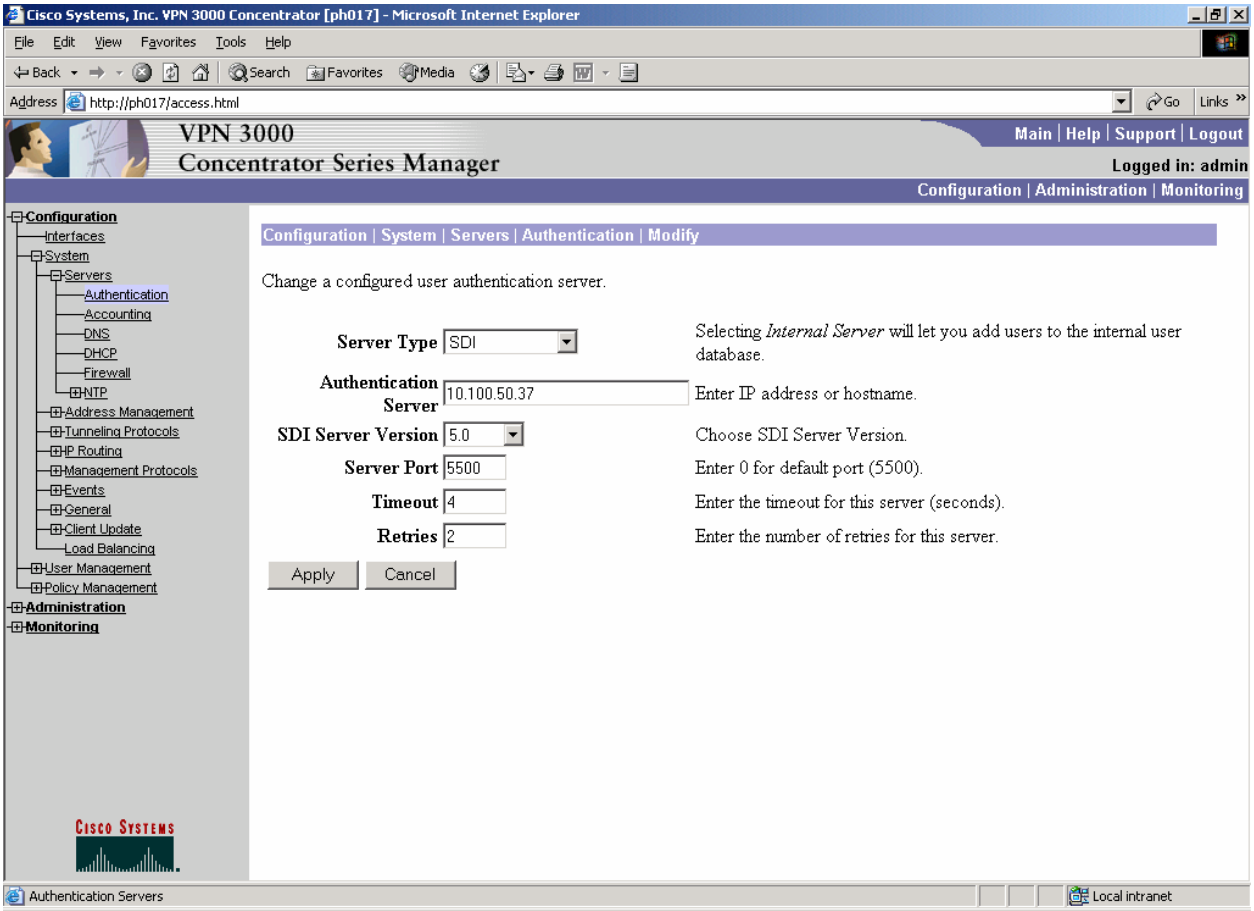


Figure 1 – SecurID Authentication configuration

SDI Version pre-5.0 - SDI versions prior to 5.0 use the concept of a master and a slave server, which share a single node secret file (SECURID). On the VPN Concentrator you can configure one pre-5.0 SDI master server and one SDI slave server globally, and one SDI master and one SDI slave server per each group.

SDI Version 5.0 - SDI version 5.0 uses the concepts of a primary and replica server. A version 5.0 SDI server that you configure on the VPN Concentrator can be either the primary or any one of the replicas. You can have one primary server, and up to 10 replicas; use the SDI documentation for configuration instructions. The primary and all the replicas can authenticate users. Each primary and its replicas share a single node secret file. The node secret file has its name based on the hexadecimal value of the ACE/Server IP address with .SDI appended. The VPN Concentrator obtains the server list when the first user authenticates to the configured server, which can be either a primary or a replica. The VPN Concentrator then assigns priorities to each of the servers on the list, and subsequent server selection derives at random from those assigned priorities. The highest priority servers have a higher likelihood of being selected.

- To configure a Slave server for use with versions of ACE/Server prior to 5.0, simply add an additional "SDI" authentication server:

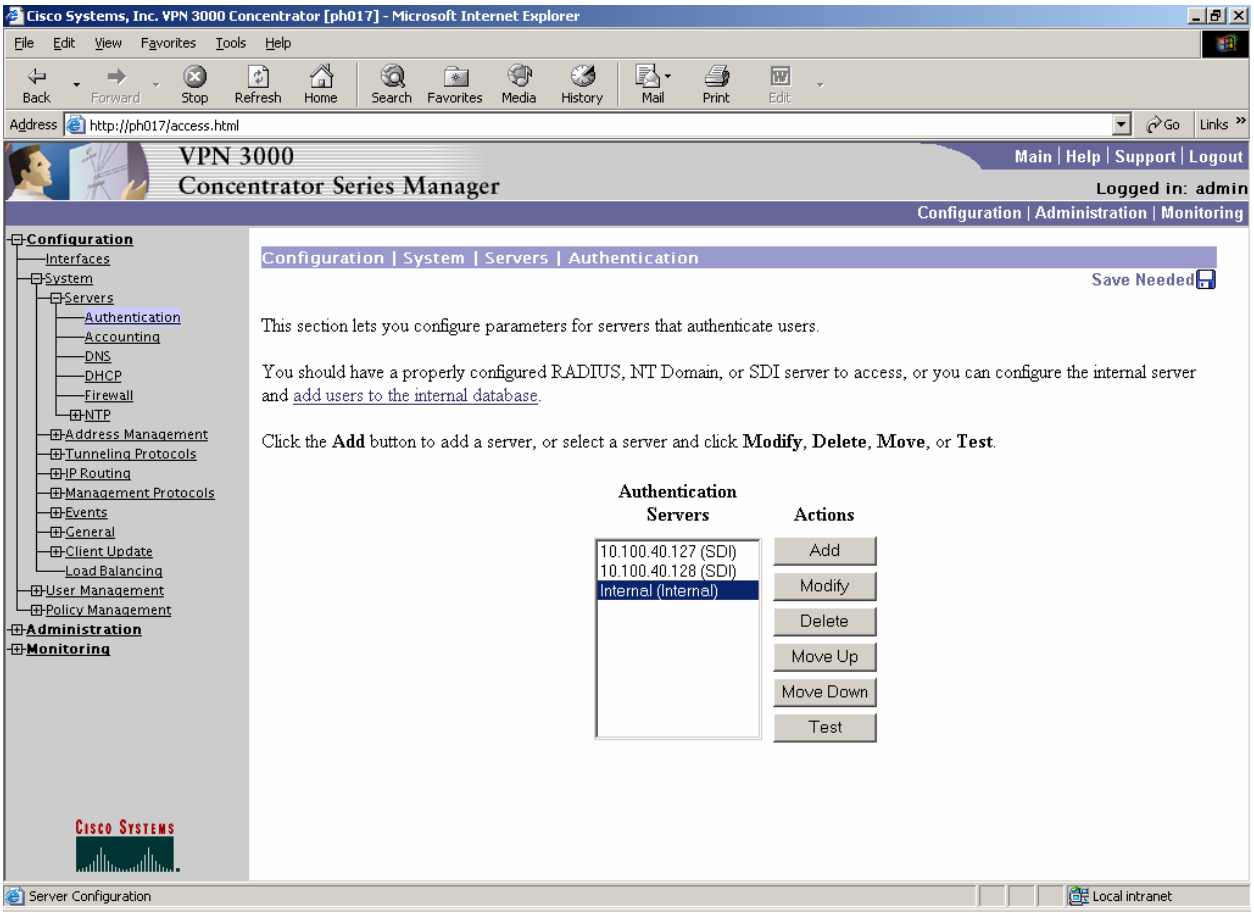


Figure 2 - Authentication Server List Menu

RADIUS Server Configuration:

- The Cisco VPN 3000 can also support RADIUS authentication to authenticate. In the Configuration > System > Servers > Authentication click add. Then add the following:

  Server Type: RADIUS
  Authentication Server: Hostname or IP address of RADIUS Server
  Server Port: *Usually 1645 or 1812 by default*
  Server Secret: Server secret set in the RADIUS server.

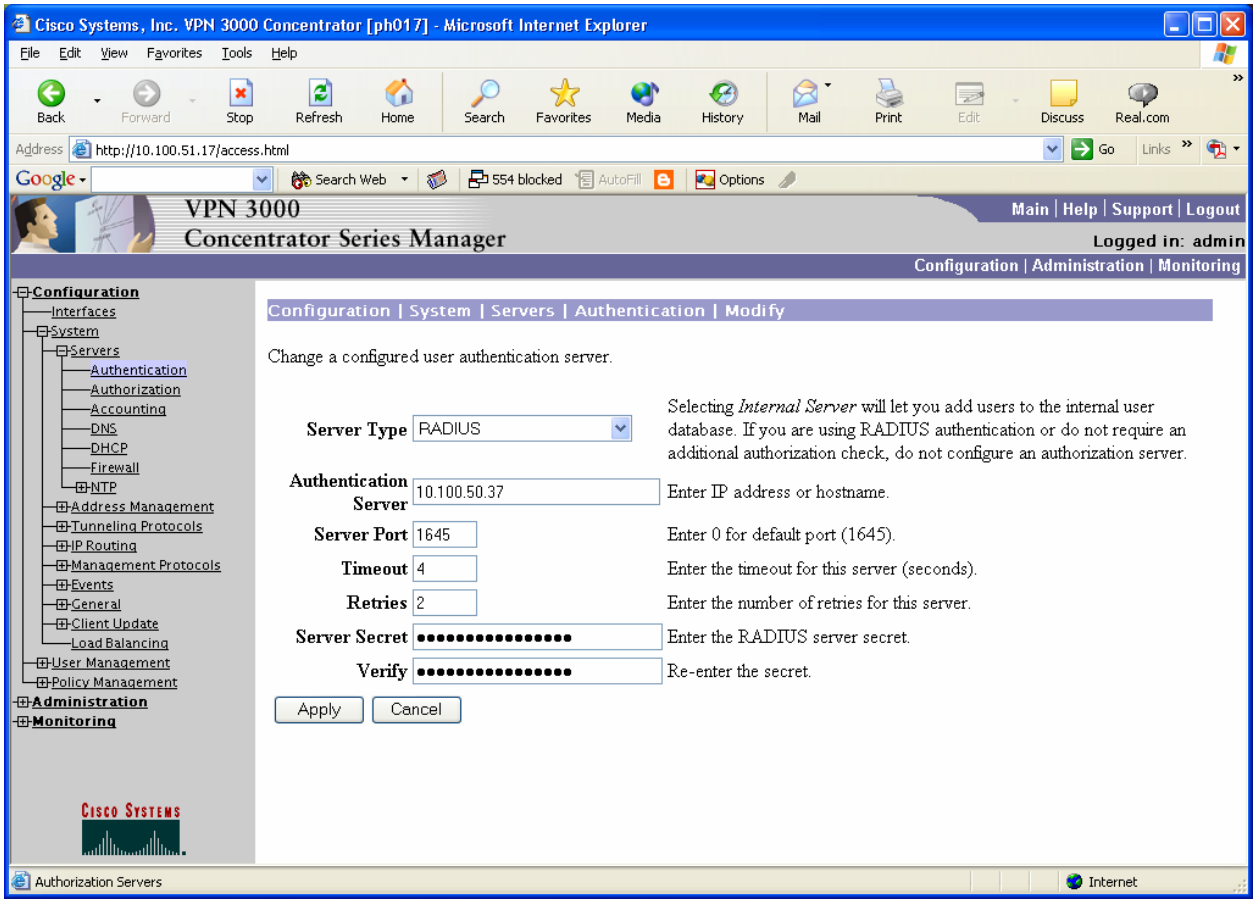


Figure 3 – RADIUS Authentication configuration

Group Configuration:

- In order for SecurID or RADIUS authentication to work properly, you need to create a group and set its authentication type to SDI for SecurID or RADIUS for RADIUS. This is done under Configuration > User Management > Groups: Click add to add a new group of users to be SecurID-challenged:

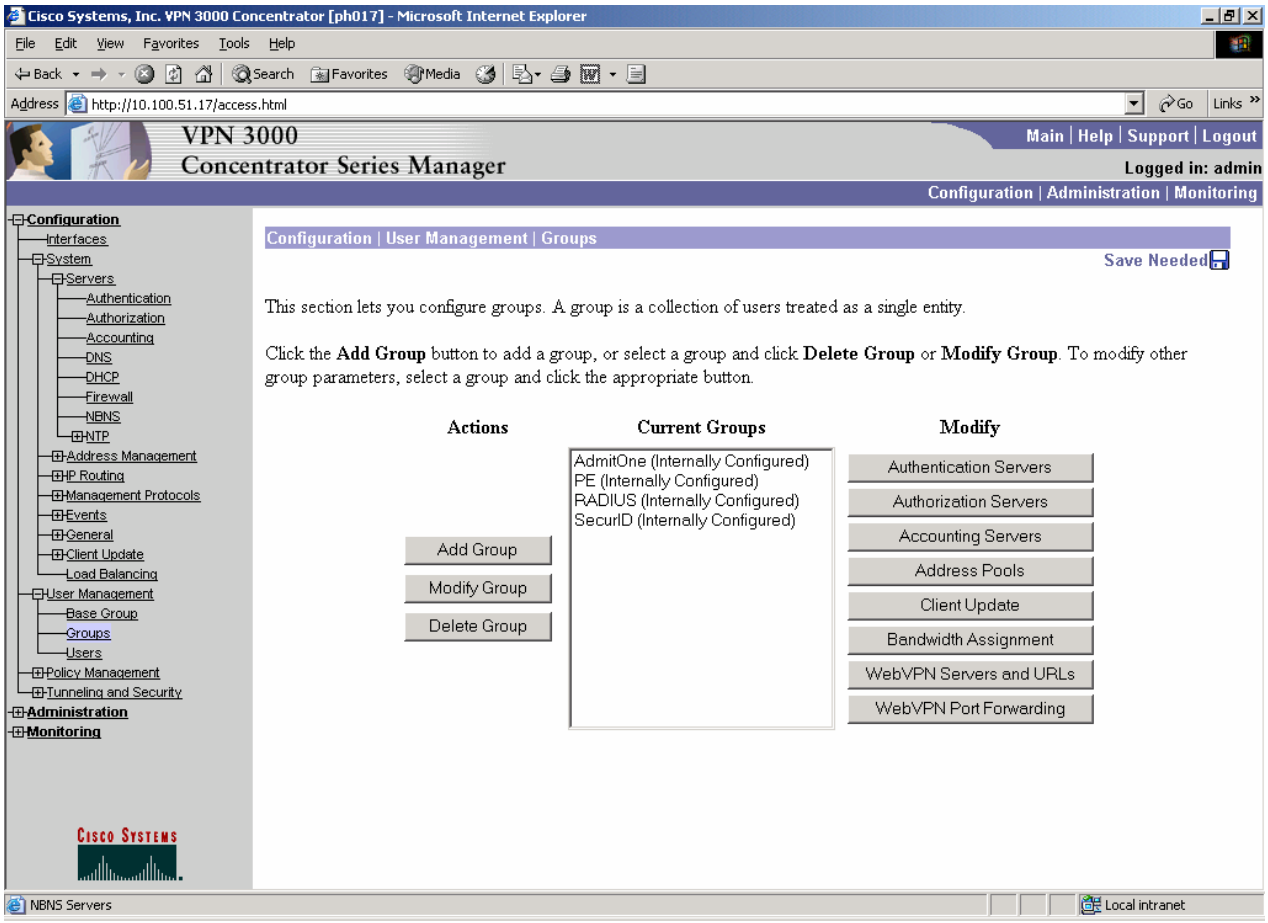


Figure 4 – Adding a Group

- Give the group a name and a password. Since you are configuring this group on the VPN3000 then choose the “Type” to be “Internal”.

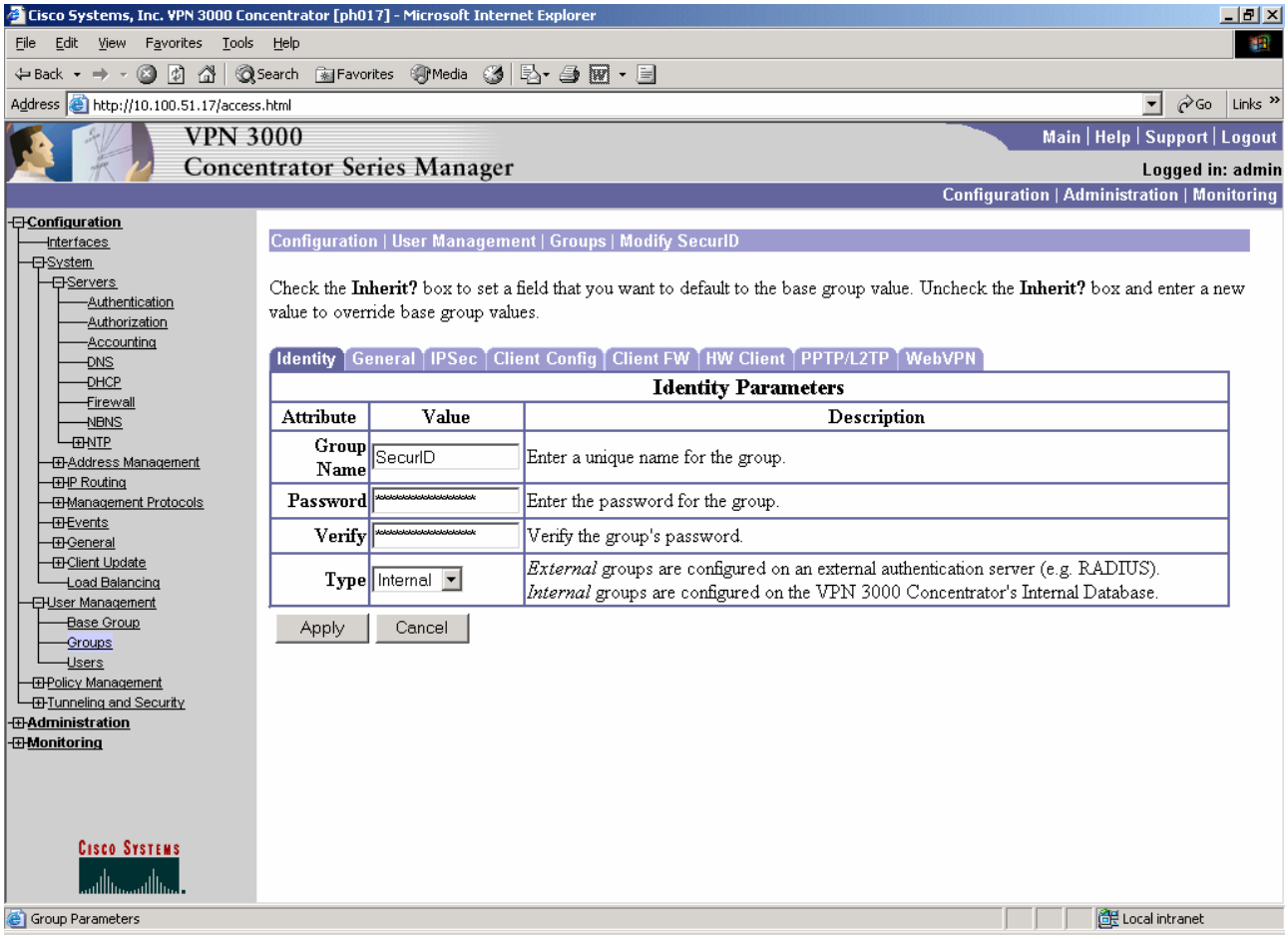


Figure 5 – Group Identity Configuration

- Then click the “IPSec” tab. Set the Tunnel Type to “Remote Access” and the Authentication type to “SDI” for SecurID or RADIUS for RADIUS. SecurID is shown in this example.

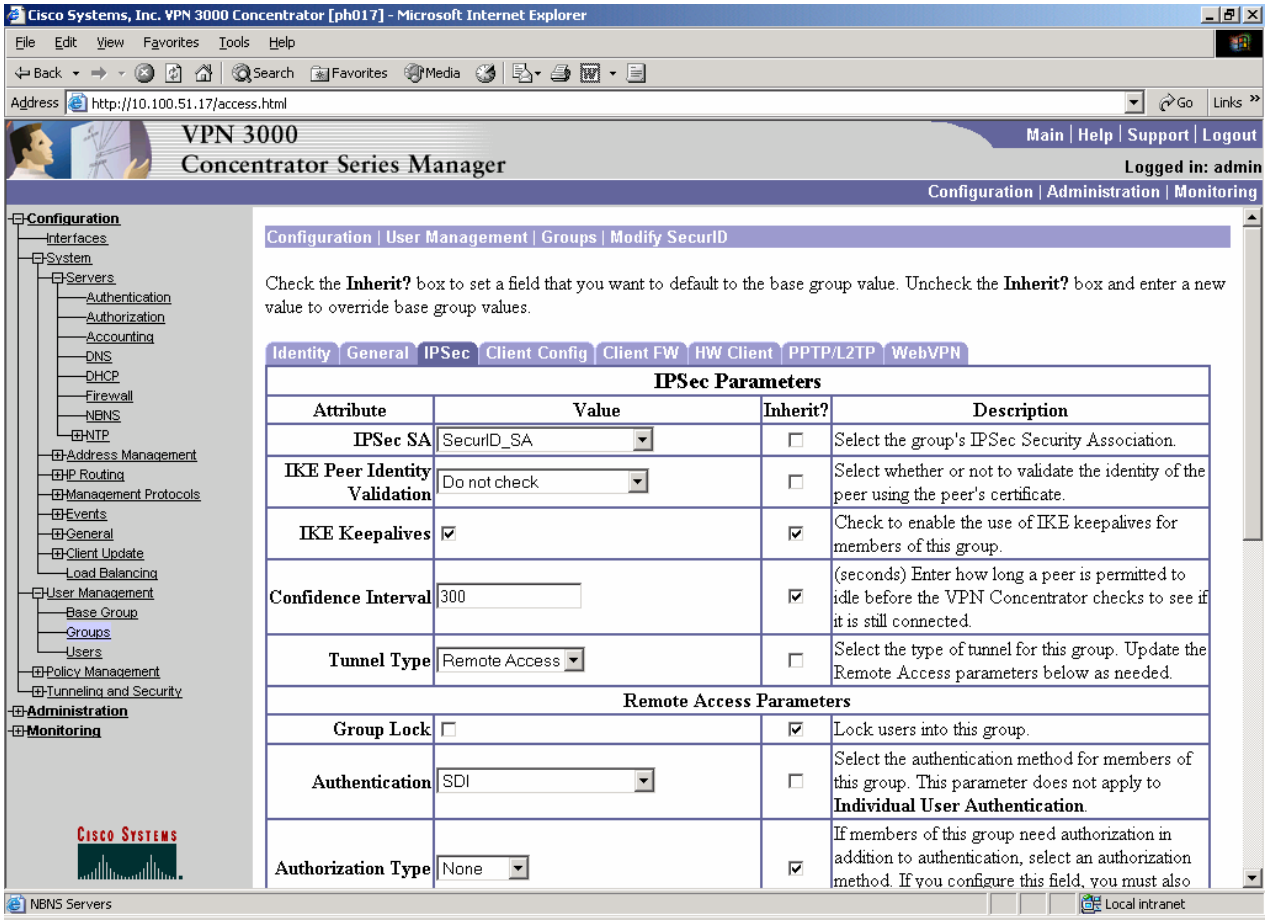


Figure 6 – IPSec Configuration

Note: When the VPN 3000 authenticates using native SecurID, against the ACE/Server for the first time, a secret key is exchanged which is called the node secret. This file can be viewed/deleted/copied from within the VPN3000 Series Concentrator Manager by browsing to Administration >File Management. The file is a HEX number followed by .SDI.

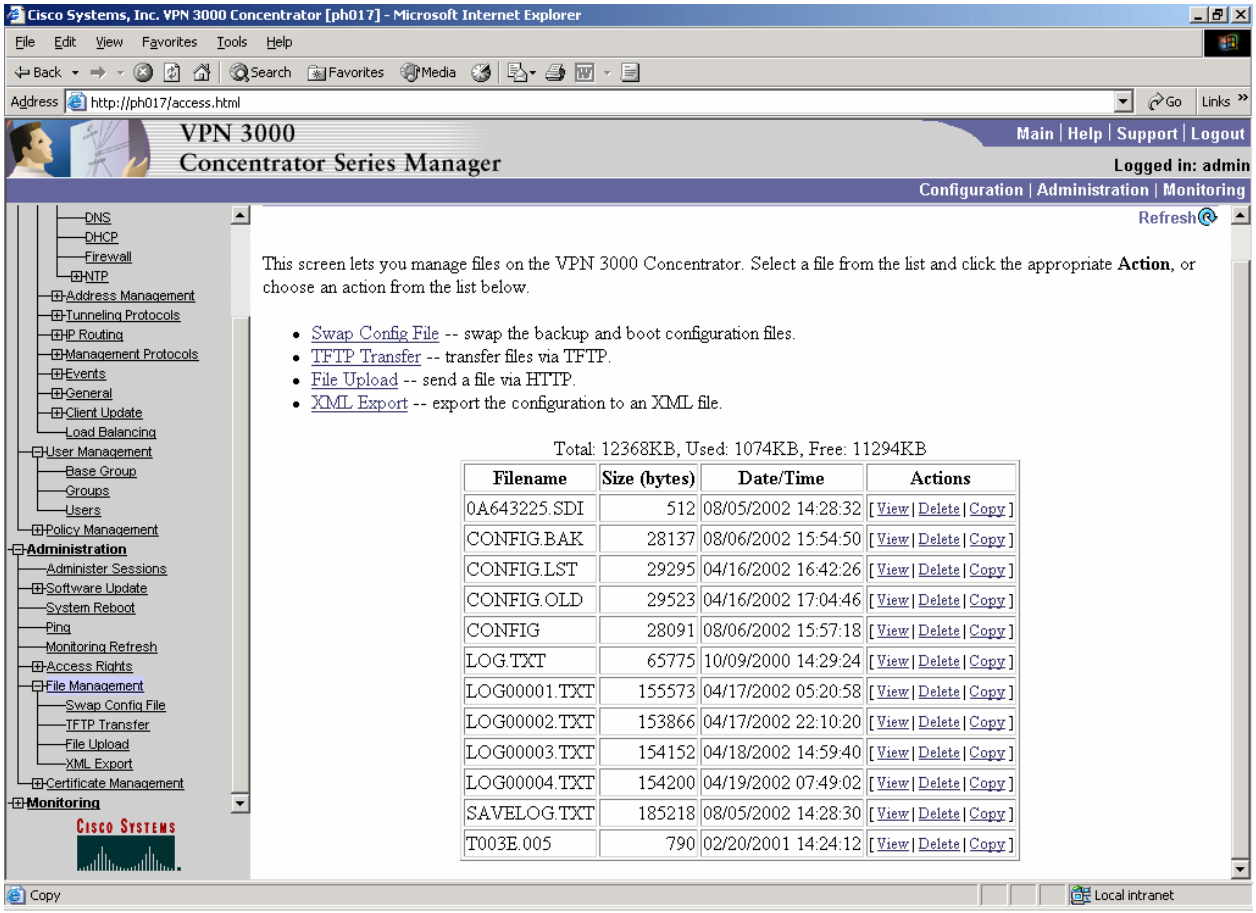


Figure 7 – Location of Node Secret File

Web VPN Configuration

The Web VPN uses the first authentication server listed to authenticate **all users**. Go to Configuration > System > Servers > Authentication and move the authentication server that should be used for authentication to the top of the list. See figure2 at the beginning of this section.

Note: You can change the Login Message displayed to the user by going to Configuration > Tunnel and Security > WebVPN > Home Page. Then enter the Login Message.

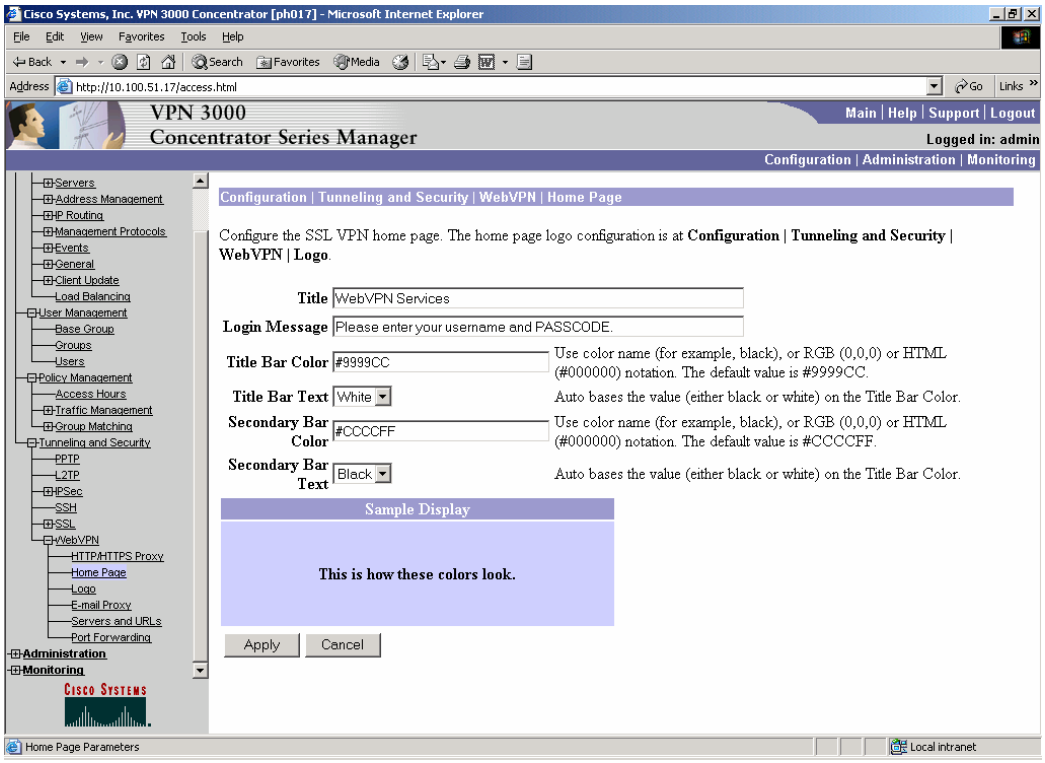


Figure 8 –Web VPN logon page configuration

In this example we have changed the Login Message to “Please enter your username and PASSCODE.”

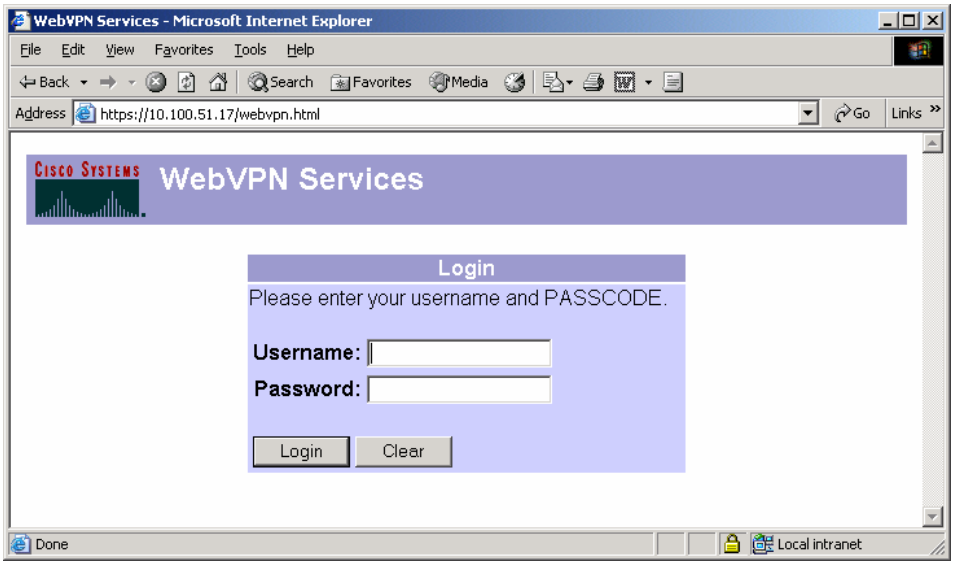
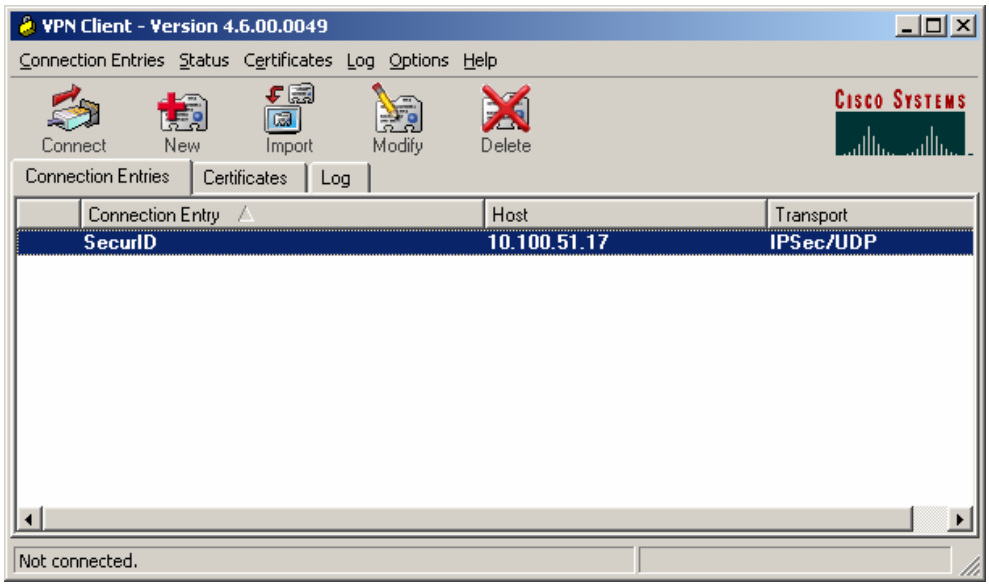


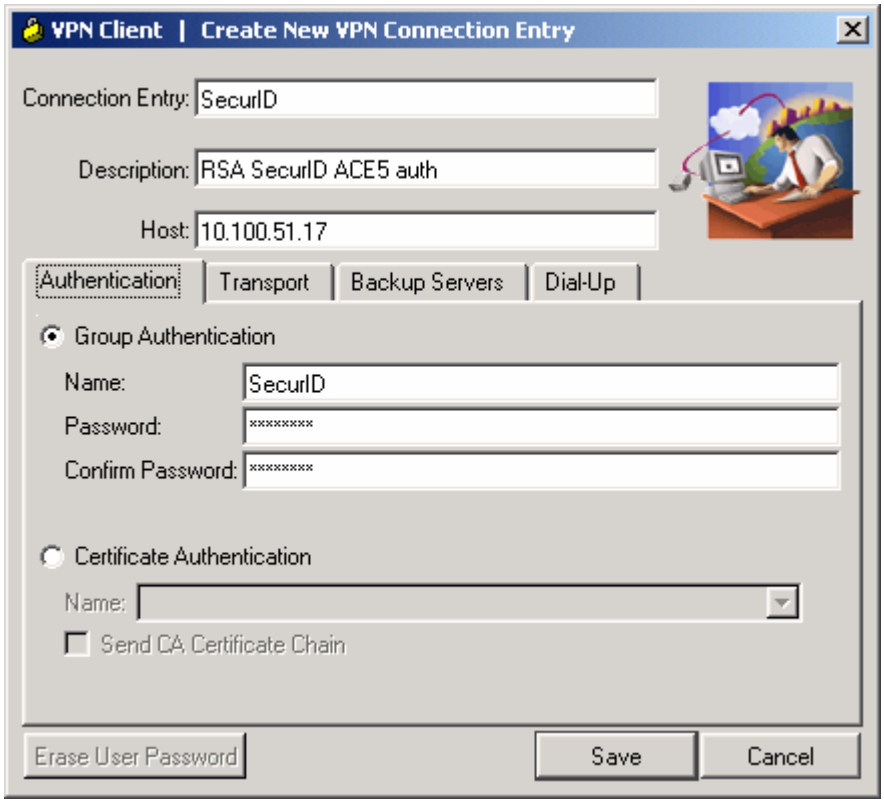
Figure 9 –Web VPN logon page

VPN Client Configuration

- Install the Cisco VPN client.



- Click the **New** button to create a RSA SecurID connection entry. Fill in the appropriate information for the connection. The group name and password must match the entry you create on the VPN server.



- Click Save.

- Highlight the connection created and click connect.
- The user will now be prompted for authentication information.

RSA Software Token note: If the Cisco VPN client detects that the RSA Software Token is installed (through the presence of stauto32.dll), users will be prompted for their PIN only. The tokencode displayed on the RSA Software Token is automatically coupled with the PIN and passed along to the RSA ACE/Server. VPN Client software should be upgraded to version 2.5 if using RSA Software Token. You can turn on and off the option for the PIN only prompt when using the Cisco VPN client 4.x. See the VPN client profile configuration parameters section for more information.

VPN client profile configuration parameters:

You can enable and disable the ability of the VPN client to only prompt the user for their PIN when using the RSA Software Token adding the following setting in your profile file. This file is located by default in Program Files\Cisco Systems\VPN Client\Profiles. The file name is the name of the connection entry with a .pcf extension.

SDIUseHardwareToken = 0 or 1
0 = Yes use RSA Software Token (default)
1 = No, ignore RSA Software Token installed on the PC.

You can also change the prompts displayed to a user that is authenticating using RADIUS to better resemble a SecurID authentication by setting the following parameter in the profile file.

RadiusSDI
0 = No (default)
1 = Yes

See the VPN client documentation for more information on these and other settings that can be used.

7. Certification Checklist

Date Tested: November 18, 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]
RSA Sign-On Manager	WIN2K SP4	4.0
Cisco VPN 3000 Concentrator	4.1.6.Rel-k9.bin	4.1.6.Rel-k9.bin
Cisco VPN Client	WIN2K SP4	4.6

Test	ACE Web	ACE VPN	RADIUS Web	RADIUS VPN Client
1st time auth. (node secret creation)	P	P		
New PIN mode:				
System-generated				
Non-PINPAD token	P	P	P	P
PINPAD token	P	P	P	P
User-defined (4-8 alphanumeric)				
Non-PINPAD token	P	P	P	P
Password	P	P	P	P
User-defined (5-7 numeric)				
Non-PINPAD token	P	P	P	P
PINPAD token	P	P	P	P
Software token	P	P	P	P
Deny 4 digit PIN	P(1)	P	P	P(2)
Deny Alphanumeric	P(1)	P	P	P(2)
User-selectable				
Non-PINPAD token	P	P	P	P
PINPAD token	P	P	P	P
PASSCODE				
16 Digit PASSCODE	P	P	P	P
4 Digit Password	P	P	P	P
"Pin-less" TokenCode	P	P	P	P
Next Tokencode mode				
Non-PINPAD token	P	P	P	P
PINPAD token	P	P	P	P
Software Token API Authentication				
New PIN mode	N/A	P(3)	N/A	N/A
8 Digit PIN with 8 Digit TokenCode	N/A	P	N/A	N/A
Failover	P	P	P	P
User Lock Test (RSA ACE Lock Function)	P	P		
No RSA ACE/Server	P	P	P	P

MPR / SWA *P=Pass or Yes F=Fail N/A=Non-available function (#)=See Known Issue

8. Known Issues

1) **Failed PIN creation via SecurID with Web authentication.**
When a user fails to enter a PIN that matches the PIN criteria the first time they will be prompted again to create a PIN but it will not work. The user will then be asked to authenticate again, which will then prompt them to create a PIN.

2) **Failed PIN creation via RADIUS with VPN Client.**
When a user fails to enter a PIN that matches the PIN criteria they will need to disconnect and reconnect before they can attempt to create the PIN again.

3) **Failed authentication after Cisco VPN 3000 is restarted.**
The Cisco VPN 3000 will be unable to authenticate to the RSA Authentication Manager Servers if the RSA Authentication Manger is stopped and the Cisco VPN 3000 is restarted during this time. The reason for this is that the Cisco VPN 3000 stores the RSA Authentication Manger Server list in memory and thus the server list is lost during a restart If the Primary RSA Authentication Manger Server is not running when the Cisco VPN 3000 starts backup it will not be able to authenticate because the only server defined on the Cisco VPN 3000 is the Primary RSA Authentication Manger Server. To correct this issue the Primary RSA Authentication Manger Server needs to be restarted or the Primary RSA Authentication Manger Server needs to be removed as the authentication server on the Cisco VPN 3000 and one of the Replica RSA Authentication Manger Server is define as the authentication server.