



RSA SecurID Ready Implementation Guide

Last Modified: August 1, 2009

Partner Information

Product Information	
Partner Name	Cisco Systems
Web Site	www.cisco.com
Product Name	Cisco AnyConnect VPN Client
Version & Platform	2.3.0254
Product Description	<p>The AnyConnect client provides remote end users running Microsoft Vista, Windows XP or Windows 2000, Linux, or Macintosh OS X, with the benefits of a Cisco SSL VPN client, and supports applications and functions unavailable to a clientless, browser-based SSL VPN connection. In addition, the AnyConnect client supports connecting to IPv6 resources over an IPv4 network tunnel. This release supports the SSL and DTLS protocol. This release does not include IPsec support.</p> <p>The client can be loaded on the security appliance and automatically downloaded to remote users when they log in, or it can be manually installed as an application on PCs by a network administrator. After downloading, it can automatically uninstall itself after the connection terminates, or it can remain on the remote PC for future SSL VPN connections. The client includes the ability to create user profiles that are displayed in the user interface and define the names and addresses of host computers.</p>
Product Category	Perimeter Defense (Firewalls, VPNs & Intrusion Detection)





Solution Summary

The Cisco AnyConnect VPN Client allows users to authenticate via RSA SecurID to establish end-to-end encrypted SSL VPN tunnels for secure connectivity for mobile employees or teleworkers. The RSA two-factor authentication can be done via either Native RSA SecurID authentication or using the RADIUS protocol. The end user running on a Windows platform can also take advantage of additional integration work by using the RSA Software Token. The Cisco AnyConnect VPN client can pull the tokencode from the RSA Software Token running on the same machine and couple the PIN and tokencode so that users only need to enter their PIN during an authentication.

Partner Integration Overview	
Authentication Methods Supported	Native RSA SecurID Authentication and RADIUS
RSA Authentication Manager Name Locking	Server Dependant
RSA Authentication Manager Replica Support	Yes (Authentication Manager v6.x and above)
RSA Software Token	Yes
Use of Cached Domain Credentials	No

Product Requirements

Partner Product Requirements: Cisco AnyConnect VPN Client	
Memory	34 MB
Storage	50 MB

Operating System	
Platform	Required Patches
Windows XP	SP2 or later
Windows 2000	SP2 or later
Windows Vista	All versions as of date listed above

Additional Hardware Requirements:

The Cisco AnyConnect VPN Client has been certified with the following Cisco products

RSA Compatibility Matrix		
Cisco Product	Native RSA SecurID Authentication	RADIUS Authentication
Cisco ASA 5500 series – software v7.0 or later	Yes	Yes

Additional Software Requirements:

The Cisco AnyConnect VPN Client when using RSA Software Token and/or SID 800

RSA Software Token Compatibility Matrix		
RSA Products	Native RSA SecurID Authentication	RADIUS Authentication
RSA Software Token v4.0.242 or later	Yes	Yes
RSA SmartCard Middleware v3.0 or later	Yes	Yes



Partner Authentication Agent 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.

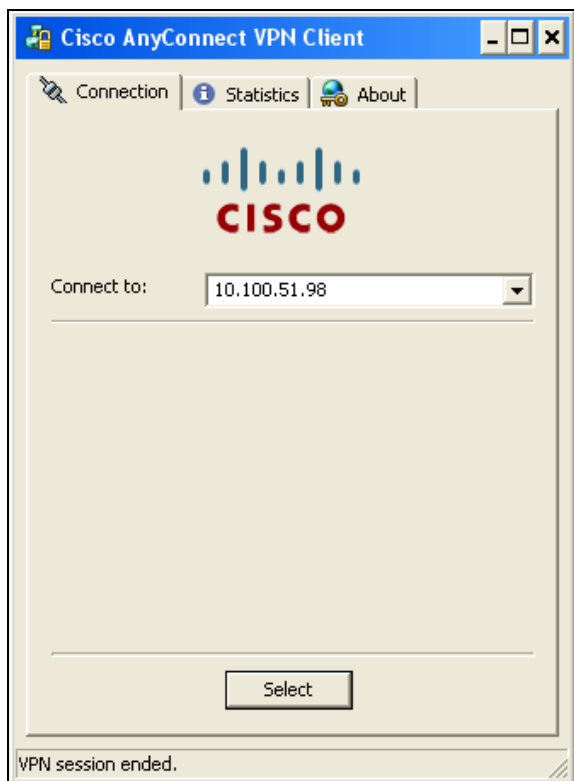
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

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

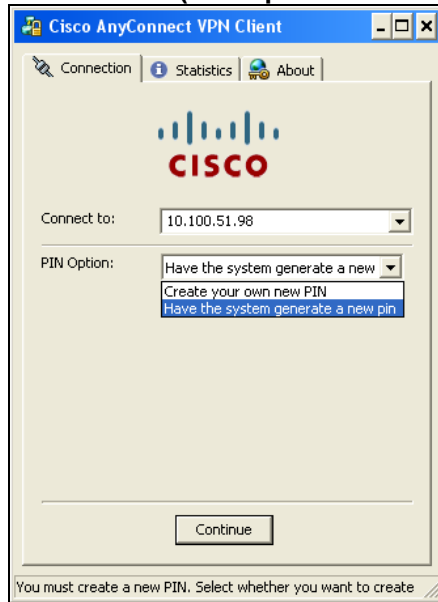
Cisco AnyConnect VPN Client Configuration

1. Install the Cisco AnyConnect VPN client and then start the application.
2. Enter the IP Address of the VPN Server in the **Connect to:** field.
3. Click **Select** and select the appropriate Group name from the **Group:** field (this attribute is provided from the connecting server).
4. Enter **Username:** and **Passcode:** and click **Connect**.





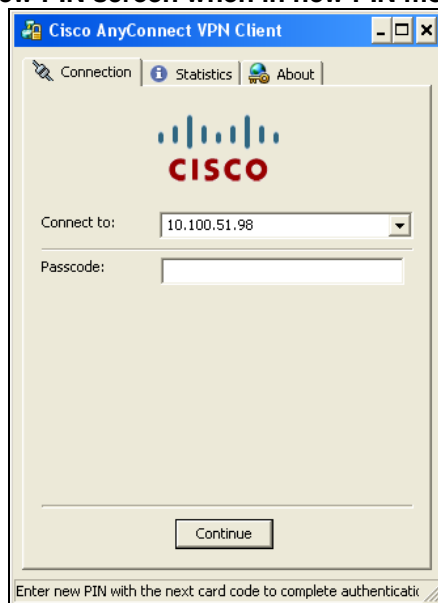
System Generated PIN (with option to create new PIN)



System Generated PIN displayed



New PIN screen when in new PIN mode





New PIN (User Defined)

Cisco AnyConnect VPN Client

Connection | Statistics | About



Connect to: 10.100.51.98

New PIN:

Verify PIN:


Continue

You must enter a new numeric PIN from 4 to 8 digits to continue

Next TokenCode Mode

Cisco AnyConnect VPN Client

Connection | Statistics | About



Connect to: 10.100.51.98

Token code:

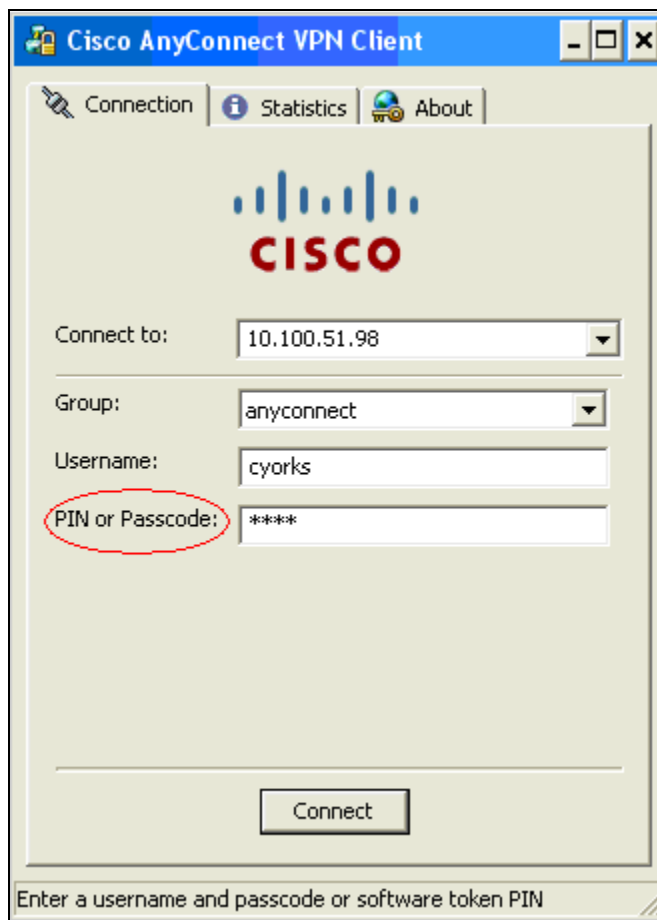
Continue

Enter the next card code to complete authentication.



RSA Software Token

RSA Software Token with the Cisco AnyConnect VPN client is dependent on the Cisco VPN server. See the compatibility matrix under the Product Requirements section for more details. If the Cisco AnyConnect VPN client detects that the RSA Software Token is installed (through the presence of stauto32.dll), users will be prompted for their **PIN** or **Passcode** as show below. The tokencode displayed on the RSA Software Token or SID 800 is automatically coupled with the PIN and passed along to the RSA Authentication Manager for validation.



! Important: The RSA Software Token is a Windows only solution.

Certification Checklist

See the RSA Security Implementation guide for each Cisco VPN server device for certification testing information.

http://www.rsa.com/rsasecured/guides/imp_pdfs/Cisco_ASA_AuthMan7.1.pdf