RSA SecurID Ready Implementation Guide

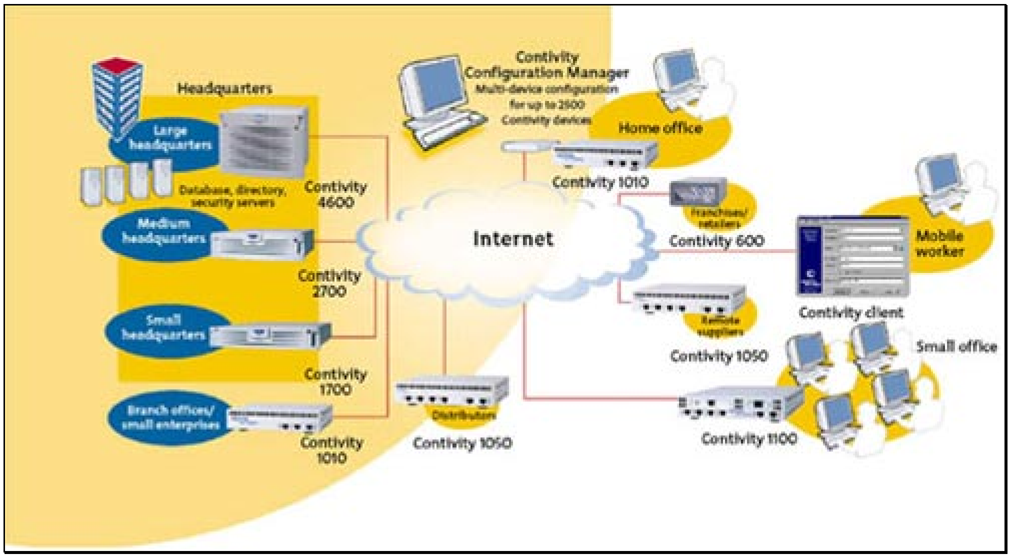
Last Modified: September 30, 2005

Partner Information

Product Information	
Partner Name	Nortel Networks
Web Site	www.nortelnetworks.com
Product Name	Nortel VPN Router
Version & Platform	1050, 1740, 2700, 5000 Series
Product Description	Each Nortel VPN Router is a single hardware device that provides routing, firewall, bandwidth management, encryption, authentication, and data integrity for secure tunneling across managed IP networks and the Internet. With Contivity VPN Switches, you can connect remote users, branch offices, suppliers, and customers with the cost and performance advantages of shared IP networks and the security and control you would expect from private networks.
Product Category	Virtual Private Networking

Solution Summary

Partner Integration Overview	
Authentication Methods Supported	RADIUS
List Library Version Used	N/A
RSA Authentication Manager Name Locking	No
RSA Authentication Manager Replica Support	No
Secondary RADIUS Server Support	Yes (3)
Location of Node Secret on Agent	‘None stored’
RSA Authentication Agent Host Type	Communication Server
RSA SecurID User Specification	Designated users
RSA SecurID Protection of Administrative Users	No
RSA Software Token API Integration	Yes
Use of Cached Domain Credentials	No



Product Requirements

Partner Product Requirements: Nortel VPN Router	
Firmware Version	V05_05.202

Partner Product Requirements: Nortel VPN Client	
Operating System	**Required Patches**
Windows XP	
Windows 2000	
Windows 98	
Windows ME	

Note: Nortel VPN Client Version 4.86 is the last release that provides support for the Windows NT operating system.

Version 4.91 will be the last release that provides support for Windows 98 and Windows ME operating systems.

Agent Host Configuration

To facilitate communication between the Nortel VPN Router and the RSA Authentication Manager / RSA SecurID Appliance, an Agent Host record must be added to the RSA Authentication Manager database. The Agent Host record identifies the Nortel VPN Router 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 using RADIUS Authentication Protocol)

When adding the Agent Host Record, you should configure the Nortel VPN Router as Communication Server. This setting is used by the RSA Authentication Manager to determine how communication with the Nortel VPN Router 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.

Partner Authentication Agent Configuration

Before You Begin

This section provides instructions for integrating the Nortel VPN Router with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

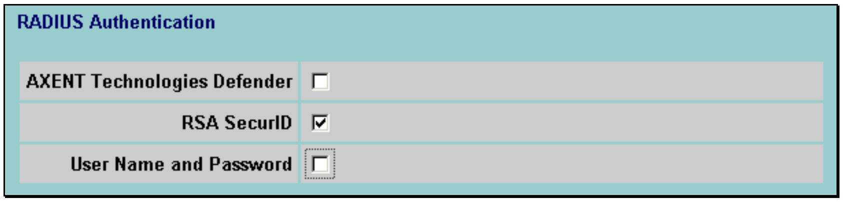
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

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.

Nortel VPN Router Configuration

Enabling Support for RSA SecurID Authentication

1. Using your Internet Browser, connect and login to your Nortel Contivity Switch Administration Console.
2. Enable RSA SecurID authentication via RADIUS
   (Services > IPSec > RADIUS Authentication).

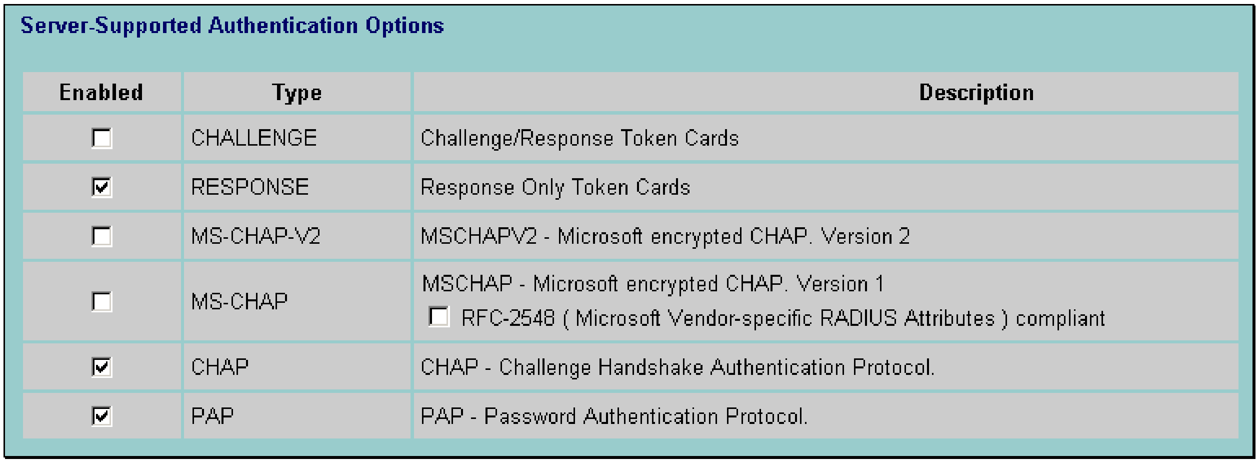


RADIUS Authentication

AXENT Technologies Defender	□
RSA SecurID	☑
User Name and Password	□

VPN Router Supported Authentication Types

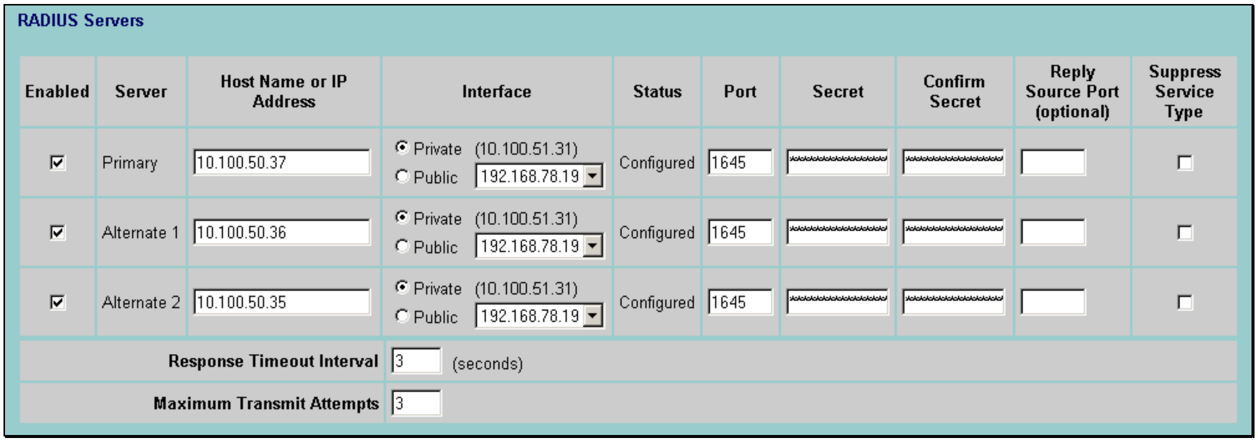
1. The Nortel VPN Router supports RSA ACE/Server authentication of users via Radius only. This is configured in the (Servers > Radius Auth) page of the CES Web management interface.
2. Check the box at the top of the screen that says ‘Enable Access to RADIUS Authentication’.
3. Under the ‘Server-Supported Authentication Options’ section, click the checkbox to enable support for Response Only authentication. This configuration is used for RSA SecurID Authentication.



Server-Supported Authentication Options

Enabled	Type	Description
□	CHALLENGE	Challenge/Response Token Cards
☑	RESPONSE	Response Only Token Cards
□	MS-CHAP-V2	MSCHAPV2 - Microsoft encrypted CHAP. Version 2
□	MS-CHAP	MSCHAP - Microsoft encrypted CHAP. Version 1 □ RFC-2548 (Microsoft Vendor-specific RADIUS Attributes) compliant
☑	CHAP	CHAP - Challenge Handshake Authentication Protocol.
☑	PAP	PAP - Password Authentication Protocol.

4. In the ‘RADIUS Servers’ section, fill out the info required. The Secret information for these servers should match the encryption key assigned in the Agent Host configuration.



RADIUS Servers

Enabled	Server	Host Name or IP Address	Interface	Status	Port	Secret	Confirm Secret	Reply Source Port (optional)	Suppress Service Type
☑	Primary	10.100.50.37	● Private (10.100.51.31) ○ Public 192.168.78.19 ▾	Configured	1645	***************	***************		☐
☑	Alternate 1	10.100.50.36	● Private (10.100.51.31) ○ Public 192.168.78.19 ▾	Configured	1645	***************	***************		☐
☑	Alternate 2	10.100.50.35	● Private (10.100.51.31) ○ Public 192.168.78.19 ▾	Configured	1645	***************	***************		☐

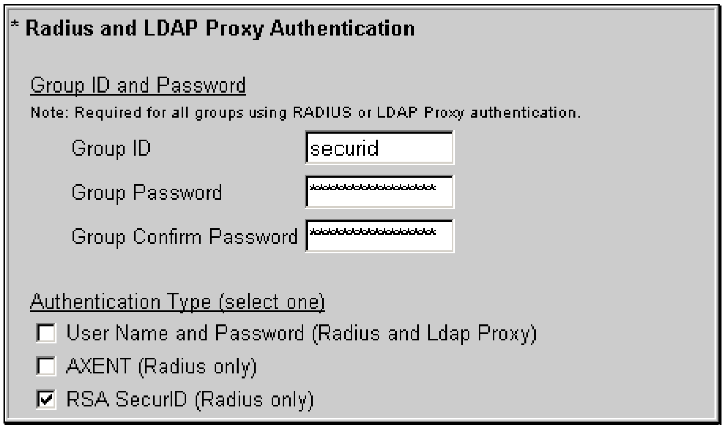
Response Timeout Interval 3 (seconds)

Maximum Transmit Attempts 3

RADIUS Group Configuration

Any user seeking RADIUS authentication must belong to a group specified by a group ID and password, configured in the Profiles > Groups > Edit > IPSec > Authentication > Configure page. This is a two-step process where (1) the Switch authenticates the remote user with RSA SecurID tokens, and (2) the client uses the Group ID and Group Password to authenticate the Switch's identity.

1. Click to enable the RSA SecurID token security authentication.
2. Enter the Group ID and Password, which provide access to the switch.



* Radius and LDAP Proxy Authentication

Group ID and Password

Note: Required for all groups using RADIUS or LDAP Proxy authentication.

Group ID: securid

Group Password: ****************

Group Confirm Password: ****************

Authentication Type (select one)

☐ User Name and Password (Radius and Ldap Proxy)

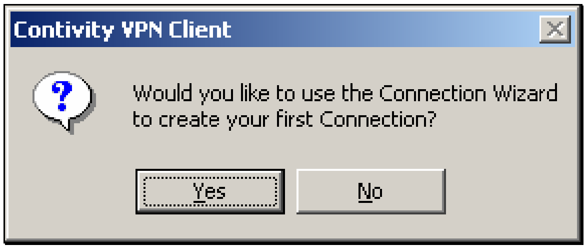
☐ AXENT (Radius only)

☑ RSA SecurID (Radius only)

IPSec Client configuration

Upon first run of the Contivity VPN Client, you will be prompted to create a connection profile via the Connection Wizard.

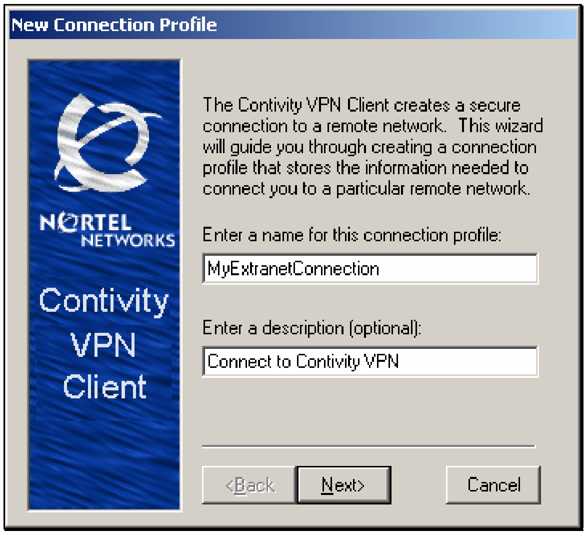
Use the screenshots below as a guide to setting up your connection for RSA SecurID authentication. For a detailed explanation of each configuration parameter, please reference the manuals from Nortel that comes with the client software.



Contivity VPN Client

Would you like to use the Connection Wizard to create your first Connection?

Connection Wizard



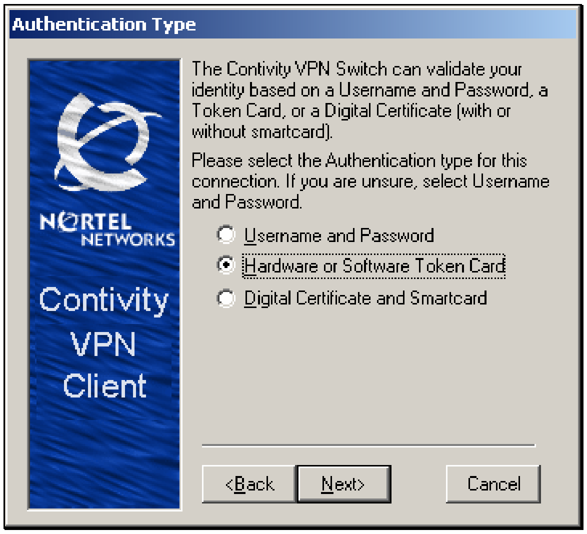
New Connection Profile

The Contivity VPN Client creates a secure connection to a remote network. This wizard will guide you through creating a connection profile that stores the information needed to connect you to a particular remote network.

Enter a name for this connection profile: MyExtranetConnection

Enter a description (optional): Connect to Contivity VPN

Connection Profile name and description



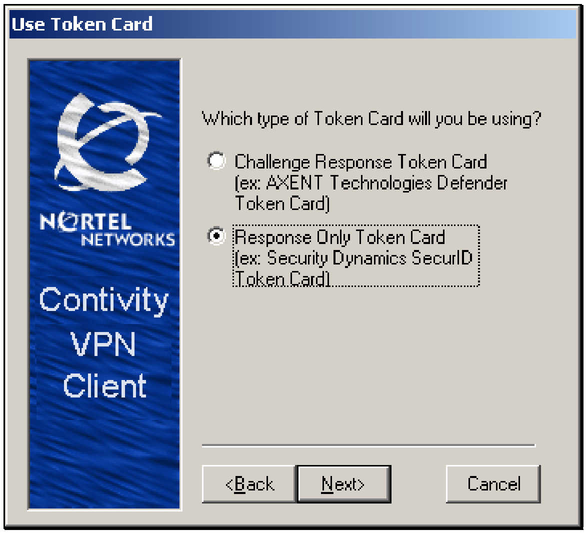
Authentication Type

The Contivity VPN Switch can validate your identity based on a Username and Password, a Token Card, or a Digital Certificate (with or without smartcard).

Please select the Authentication type for this connection. If you are unsure, select Username and Password.

- ○ Username and Password
- ● Hardware or Software Token Card
- ○ Digital Certificate and Smartcard

Authentication type

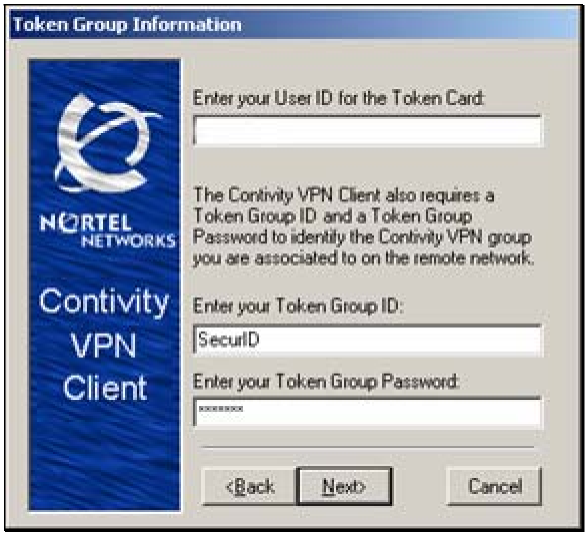


Use Token Card

Which type of Token Card will you be using?

- ○ Challenge Response Token Card (ex: AXENT Technologies Defender Token Card)
- ● Response Only Token Card (ex: Security Dynamics SecurID Token Card)

Token card type



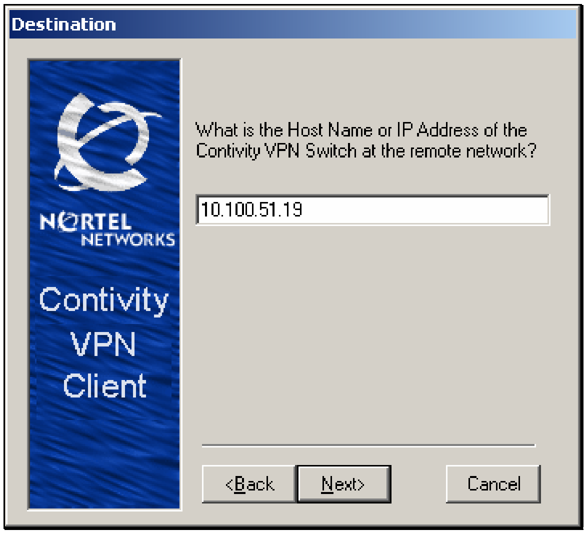
Enter your User ID for the Token Card:

The Contivity VPN Client also requires a Token Group ID and a Token Group Password to identify the Contivity VPN group you are associated to on the remote network.

Enter your Token Group ID: SecurID

Enter your Token Group Password: ********

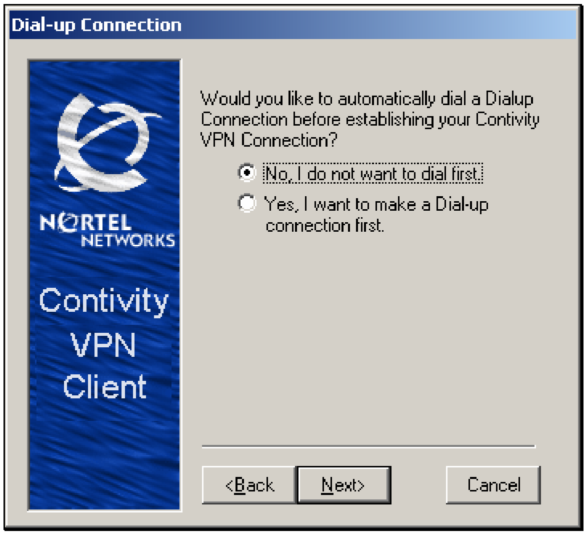
User ID for RSA SecurID Authentication



What is the Host Name or IP Address of the Contivity VPN Switch at the remote network?

10.100.51.19

Name/IP Address of switch

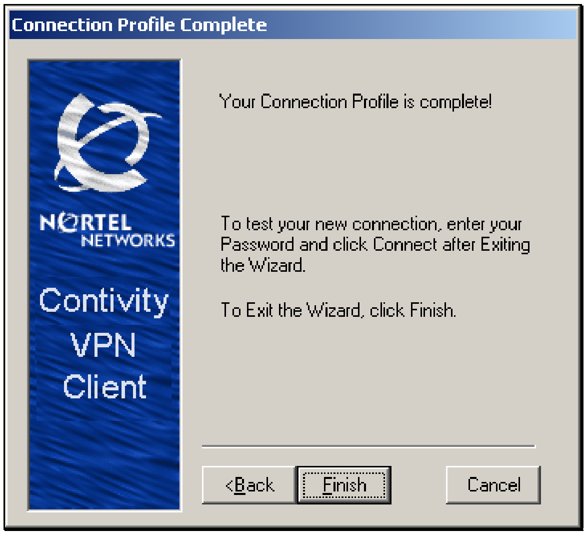


Would you like to automatically dial a Dialup Connection before establishing your Contivity VPN Connection?

● No, I do not want to dial first.

○ Yes, I want to make a Dial-up connection first.

Do you need to initiate a dial up connection first or are you already connected to the internet/network?

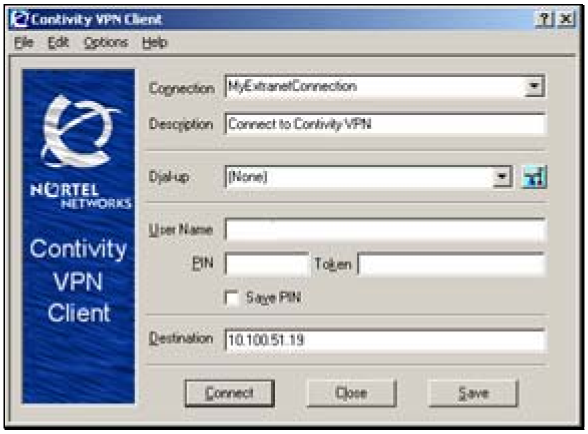


Your Connection Profile is complete!

To test your new connection, enter your Password and click Connect after Exiting the Wizard.

To Exit the Wizard, click Finish.

Setup complete!



Connection: MyExtranetConnection

Description: Connect to Contivity VPN

Dial-up: (None)

User Name:

PIN: Token:

□ Save PIN

Destination: 10.100.51.19

Login screen

Certification Checklist

Date Tested: September 30, 2005

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	6.1	Windows 2003 Server (SP1)
RSA Software Token	3.0.5	Windows XP Professional (SP2)
RSA Authentication Utility	1.0 Build 25	Windows XP Professional (SP2)
Nortel VPN Router	1050	Firmware V05_05.202

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 API Functionality			
System Generated PIN	✓	System Generated PIN	✓
User Defined (8 Digit Numeric)	✓	User Defined (8 Digit Numeric)	✓
User Selectable	✓	User Selectable	✓
Next Tokencode Mode	✓	Next Tokencode Mode	✓
Domain Credential Functionality			
Determine Cached Credential State	N/A	Determine Cached Credential State	
Set Domain Credential	N/A	Set Domain Credential	
Retrieve Domain Credential	N/A	Retrieve Domain Credential	

EF

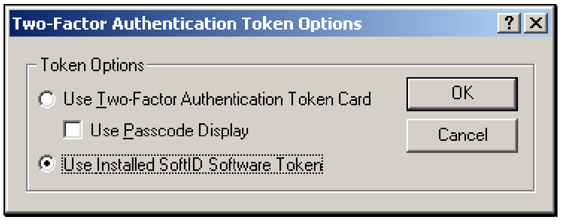
✓ = Pass ✗ = Fail N/A = Non-Available Function

Known Issues

RSA Software Token

The Contivity VPN Client can be configured to detect the installation of the RSA Software Token through the presence of stauto32.dll. Users will then be prompted for their Pin only. The Tokencode displayed on the Software Token is automatically coupled with the Pin and passed along to the RSA ACE/Server.

This functionality is configured within the Contivity VPN Client under (Options > Authentication Options > Response Only Token > Options > Use Installed SoftID Software Token)



Two-Factor Authentication Token Options

Token Options

○ Use Two-Factor Authentication Token Card

□ Use Passcode Display

● Use Installed SoftID Software Token

New Pin mode

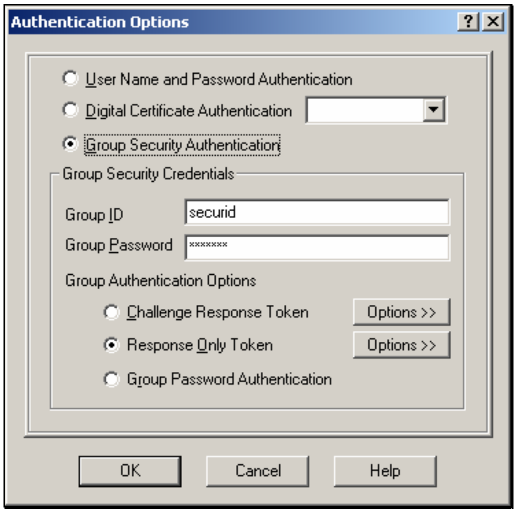
RSA SecurID Software Token integration with the Contivity VPN Client supports basic authentication functionality. When the user is in New Pin Mode, they need to enter ‘0000’ in the PIN window to initiate the authentication process. Also, once the PIN is created, they will have to wait for the “Tokencode to change” before successfully logging in.

Alphanumeric PINS

The Contivity VPN Client does not allow alphabetic characters to be entered in the Passcode field of the connection dialog box.

There is a workaround for instances where alphanumeric PINs are allowed for SecurID users, the Contivity VPN Client must be configured to display separate Tokencode and PIN fields.

This is achieved by clearing the Use Passcode Display checkbox in the Two-Factor Authentication Token Options dialog. The user can then enter an alphanumeric PIN in the separate PIN field.



Authentication Options

○ User Name and Password Authentication

○ Digital Certificate Authentication

● Group Security Authentication

Group Security Credentials

Group ID: securid

Group Password: *******

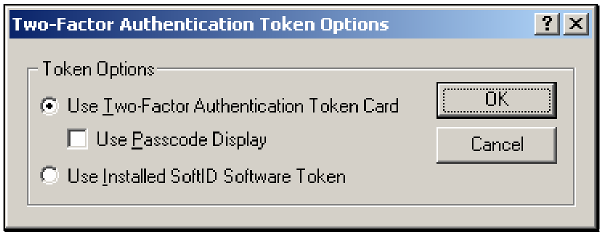
Group Authentication Options

○ Challenge Response Token

● Response Only Token

○ Group Password Authentication

Authentication Options



Two-Factor Authentication Token Options

Token Options

● Use Two-Factor Authentication Token Card

□ Use Passcode Display

○ Use Installed SoftID Software Token

Response Only Token Options

RSA Software Updates

RSA Software Token 3.0.5

Certification Testing was completed with a point release build of the RSA Software Token Application. In order to ensure a successful integration, please verify that the build of the utility is correct prior to beginning the integration.

For the updated build of the RSA Security Software Token, please contact RSA Security Customer Support or login to RSA SecureCare Online for download instructions.

RSA Authentication Utility 1.0 Build 25

Certification Testing was completed with a point release build of the RSA Authentication Utility. In order to ensure a successful integration, please verify that the build of the utility is correct prior to beginning the integration.

For the updated build of the RSA Authentication Utility, please contact RSA Security Customer Support or login to RSA SecureCare Online for download instructions.

RSA Authentication Utility (SID800 Integration)

Authentication fails if user enters 0000 as permanent SecurID PIN.

A user may not be able to authenticate when completing the New PIN procedure if the user enters four zeros (0000) as the permanent PIN. You cannot use 0000 as a permanent PIN.

System-generated RSA SecurID SID800 PIN with VPN Client

If your USB token is in New PIN mode during authentication to a VPN client, and the RSA Authentication Manager requires that you accept a system-generated SecurID PIN, a delay occurs once you accept the SecurID PIN. You then are prompted to enter the new SecurID PIN with the next Tokencode to complete authentication. This does not happen if the RSA Authentication Manager specifies a user-generated SecurID PIN.