



## External Authentication with Cisco Router with VPN and Cisco EZVpn client

### Authenticating Users Using SecurAccess Server by SecurEnvoy

Contact information		
SecurEnvoy	<a href="http://www.securenvoy.com">www.securenvoy.com</a>	0845 2600010
	1210 Parkview Arlington Business Park Theale Reading RG7 4TY	
Phil Underwood	<a href="mailto:Punderwood@securenvoy.com">Punderwood@securenvoy.com</a>	

This document describes how to integrate a Cisco Router with VPN capabilities with Cisco EZVpn Client and SecurEnvoy two-factor Authentication solution called 'SecurAccess'

Cisco Router with VPN Client provides - Secure Remote Access to the internal corporate network for all Client/Server applications.

SecurAccess provides two-factor, strong authentication for remote Access solutions (such as Cisco VPN), without the complication of deploying hardware tokens or smartcards.

Two-Factor authentication is provided by the use of (your PIN and your Phone to receive the one time passcode)

SecurAccess is designed as an easy to deploy and use technology. It integrates directly into Microsoft's Active Directory and negates the need for additional User Security databases. SecurAccess consists of two core elements: a Radius Server and Authentication server. The Authentication server is directly integrated with LDAP or Active Directory in real time.

Cisco Router can be configured in such a way that it can proxy the Authentication request of the users to an external directory (such as Radius). This is how the Cisco EZVpn client was configured. All authentication requests were forwarded to SecurEnvoy Authentication server. SecurEnvoy utilizes a web GUI for configuration, whereas the Router configuration is shown with command line through Cisco IOS. All notes within this integration guide refer to this type of approach.

The equipment used for the integration process is listed below

Cisco

2621XM router running Cisco IOS Software Release 12.2(15)T2

Cisco EZVpn client Version 4.0.3 (D)

Microsoft

Windows 2000 server SP4

IIS installed with SSL certificate (required for management and remote administration)

Active Directory installed

SecurEnvoy

SecurAccess software release v2.7 0100

The Router configuration is shown below, all relevant commands are highlighted in blue, additional text has been added to help explain the configuration, yet this is not to be entered into the actual configuration.

Connect by console cable, telnet to the Router, logon and carry out a display of the running config by entering "Sho run"

`#Enable authentication, authorization and accounting (AAA) for user authentication and group authorization.`

```
aaa new-model
```

```
#To enable extended authentication (Xauth) for user authentication,  
#enable the aaa authentication commands.  
#"Group radius" specifies RADIUS user authentication.
```

```
aaa authentication login userauthen group radius
```

```
#To enable group authorization,  
#enable the aaa authorization commands.
```

```
aaa authorization network groupauthor local
```

```
#Create an Internet Security Association and Key Management  
Protocol (ISAKMP) policy for Phase 1 negotiations.
```

```
crypto isakmp policy 3  
encr 3des  
authentication pre-share  
group 2
```

```
#Create a group that will be used to specify the Windows Internet  
Naming Service (WINS) and Domain Naming Service (DNS) server addresses  
to the client, along with the pre-shared key for authentication.
```

```
crypto isakmp client configuration group 3000client  
key cisco123  
dns 14.1.1.10  
wins 14.1.1.20  
domain cisco.com  
pool ippool
```

```
#Create the Phase 2 policy for actual data encryption.
```

```
crypto ipsec transform-set myset esp-3des esp-sha-hmac
```

#Create a dynamic map and !--- apply the transform set that was created above.

```
crypto dynamic-map dynmap 10
set transform-set myset
```

#Create the actual crypto map, and apply the AAA lists that were created earlier.

```
crypto map clientmap client authentication list userauthen
crypto map clientmap isakmp authorization list groupauthor
crypto map clientmap client configuration address respond
crypto map clientmap 10 ipsec-isakmp dynamic dynmap
```

#Apply the crypto map on the outside interface.

```
interface Ethernet0/0
ip address 172.18.124.159 255.255.255.0
half-duplex
crypto map clientmap
interface Ethernet0/1
ip address 1.1.1.1 255.255.255.0
half-duplex
```

# Create a pool of addresses to be assigned to the VPN Clients.

```
ip local pool ippool 14.1.1.100 14.1.1.200
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.124.1
ip http server
ip pim bidir-enable
```

# Specify the IP address of the RADIUS server,  
#along with the RADIUS shared secret key.

```
radius-server host 10.48.66.102 auth-port 1645 acct-port 1646 key
"SharedSecret"
radius-server retransmit 10
```

**To set up Radius on SecurEnvoy SecurAccess,**

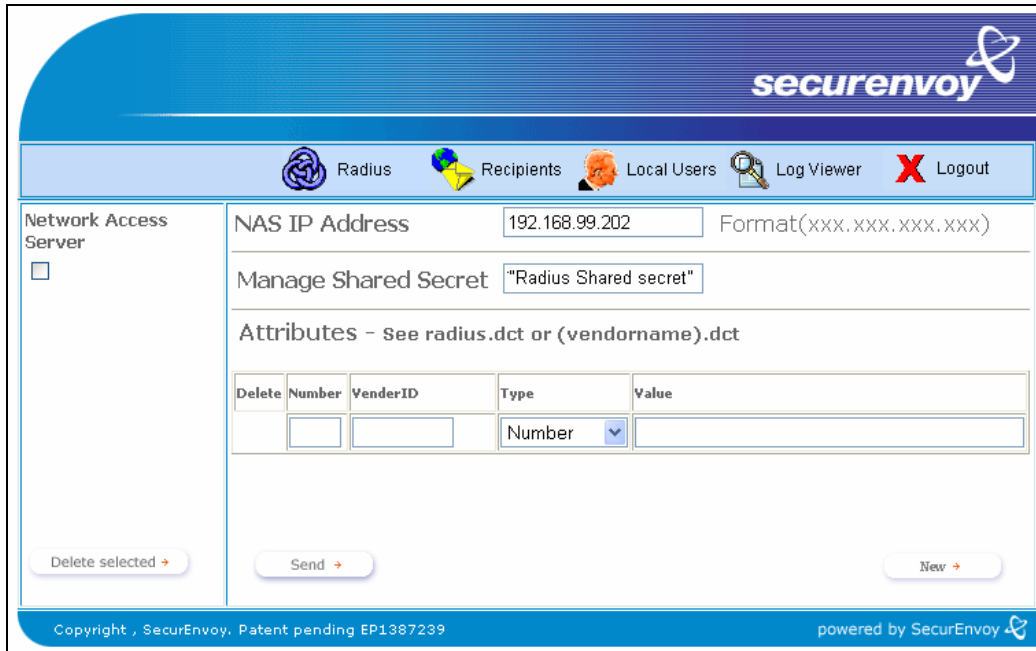
Launch Local Security Server Administration

Select Radius

Enter NAS IP address, this will be the internal address of the Router firewall

Enter "Radius Shared Secret", this must match what was entered within the Pix config.

Click Send



The screenshot shows the SecurEnvoy SecurAccess web interface. The top navigation bar includes links for Radius, Recipients, Local Users, Log Viewer, and Logout. The main content area is titled "Network Access Server" and contains a checkbox. Below this, there are input fields for "NAS IP Address" (192.168.99.202) and "Manage Shared Secret" ("Radius Shared secret"). A section for "Attributes" includes a table with columns for Delete, Number, VendorID, Type, and Value. The table is currently empty. At the bottom of the form, there are buttons for "Delete selected", "Send", and "New". The footer contains copyright information and the SecurEnvoy logo.

Network Access Server

NAS IP Address: 192.168.99.202 Format(xxx.xxx.xxx.xxx)

Manage Shared Secret: "Radius Shared secret"

Attributes - See radius.dct or (vendorname).dct

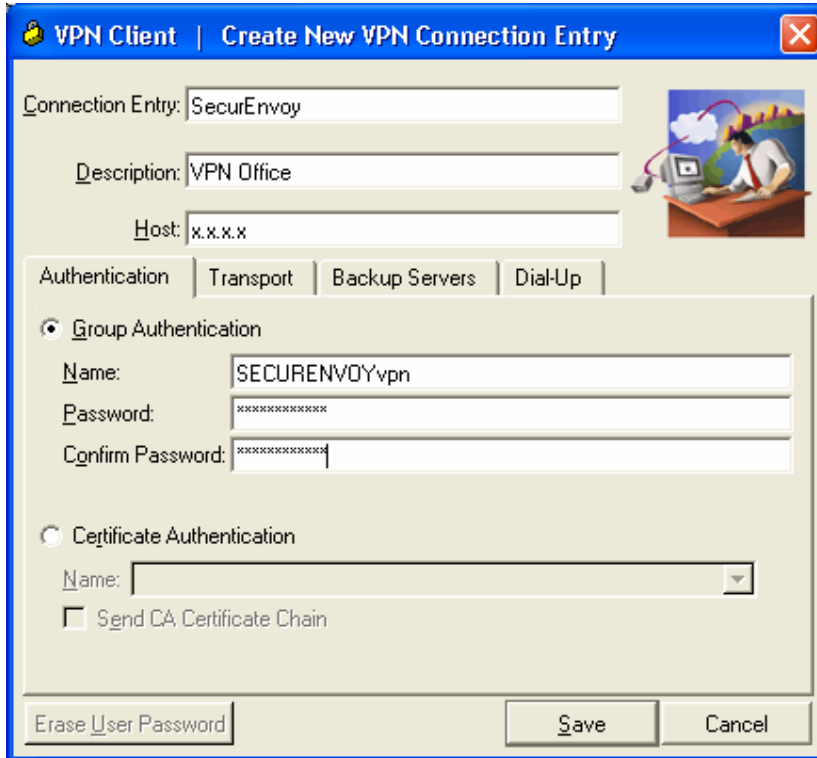
Delete	Number	VendorID	Type	Value
	<input type="text"/>	<input type="text"/>	Number	<input type="text"/>

Delete selected → Send → New →

Copyright , SecurEnvoy. Patent pending EP1387239 powered by SecurEnvoy

Click "logout"

The VPN client requires minimal configuration, enter details for the entry and a description. Designate what the Router public IP address is. Finally set the VPN group name and password. Click "Save"



The screenshot shows the 'VPN Client | Create New VPN Connection Entry' dialog box. It has a blue title bar with a close button. The main area is light beige and contains several input fields and tabs. The 'Connection Entry' field is filled with 'SecurEnvoy'. The 'Description' field is filled with 'VPN Office'. The 'Host' field is filled with 'x.x.x.x'. There are four tabs: 'Authentication' (selected), 'Transport', 'Backup Servers', and 'Dial-Up'. Under the 'Authentication' tab, there are two radio buttons: 'Group Authentication' (selected) and 'Certificate Authentication'. Under 'Group Authentication', there are three input fields: 'Name' (filled with 'SECURENVOYvpn'), 'Password' (filled with '\*\*\*\*\*'), and 'Confirm Password' (filled with '\*\*\*\*\*'). Under 'Certificate Authentication', there is a 'Name' dropdown menu and a 'Send CA Certificate Chain' checkbox. At the bottom, there are three buttons: 'Erase User Password', 'Save', and 'Cancel'.

Once the configuration has been saved, the connection can be initiated by selecting the VPN profile for SecurEnvoy and click "connect"



The screenshot shows the 'VPN Client | User Authentication for "SecurEnvoy"' dialog box. It has a blue title bar with a close button. The main area is light beige and contains the Cisco Systems logo on the left. To the right of the logo are two input fields: 'Username' and 'Password'. At the bottom, there are two buttons: 'OK' and 'Cancel'.

Enter your NT Username in the username field and PIN Passcode in the password field. Click "OK" to complete the logon process.