Configuring a Cisco VPN 5000 Concentrator with External Authentication to a Microsoft Windows 2000 IAS RADIUS Server

Document ID: 12491

Cisco has announced the end of sales for the Cisco VPN 5000 Series Concentrators. For more information, refer to the End−of−Sales Announcement.

Contents

Introduction

This document describes the procedures used to configure a Cisco VPN 5000 Concentrator with external authentication to a Microsoft Windows 2000 Internet Authentication Server (IAS) with RADIUS.

Note: Challenge Handshake Authentication Protocol (CHAP) does not work. Use only Password Authentication Protocol (PAP). Refer to Cisco bug ID CSCdt96941 (registered customers only) for further details.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on this software version:

- Cisco VPN 5000 Concentrator Software Version 6.0.16.0001

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Cisco VPN 5000 Concentrator Configuration

VPN5001_4B9CBA80

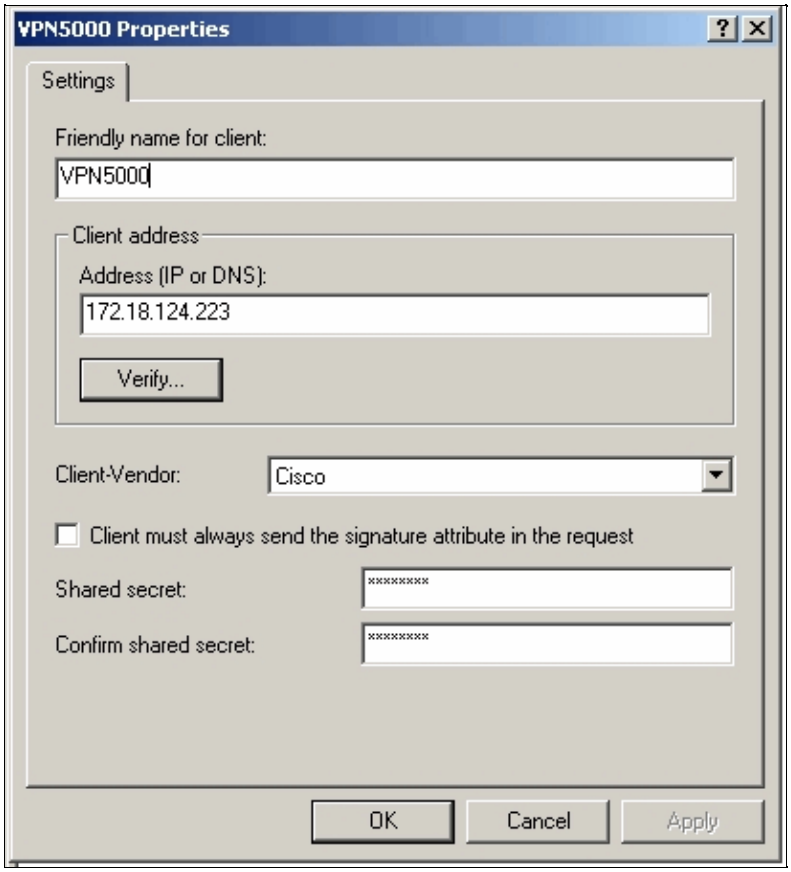
```
VPN5001_4B9CBA80> show config
Enter Password:

Edited Configuration not Present, using Running

[ General ]
EthernetAddress          = 00:02:4b:9c:ba:80
DeviceType               = VPN 5001 Concentrator
ConfiguredOn             = Timeserver not configured
ConfiguredFrom           = Command Line, from Console
EnablePassword           =
Password                 =

[ IP Ethernet 0 ]
Mode                     = Routed
SubnetMask               = 255.255.255.0
IPAddress                = 172.18.124.223

[ IP Ethernet 1 ]
Mode                     = Off

[ IKE Policy ]
Protection               = MD5_DES_G1

[ VPN Group "rtp-group" ]
BindTo                   = "ethernet0"
Transform                = esp(md5,des)
LocalIPNet               = 10.1.1.0/24
MaxConnections           = 10
IPNet                    = 0.0.0.0/0

[ RADIUS ]
BindTo                   = "ethernet0"
ChallengeType            = PAP
PAPAuthSecret            = "pappassword"
PrimAddress              = "172.18.124.108"
Secret                   = "radiuspassword"
UseChap16                = Off
Authentication           = On

[ Logging ]
Level                    = 7
Enabled                  = On

Configuration size is 1065 out of 65500 bytes.
VPN5001_4B9CBA80#
```

Configure the Microsoft Windows 2000 IAS RADIUS Server

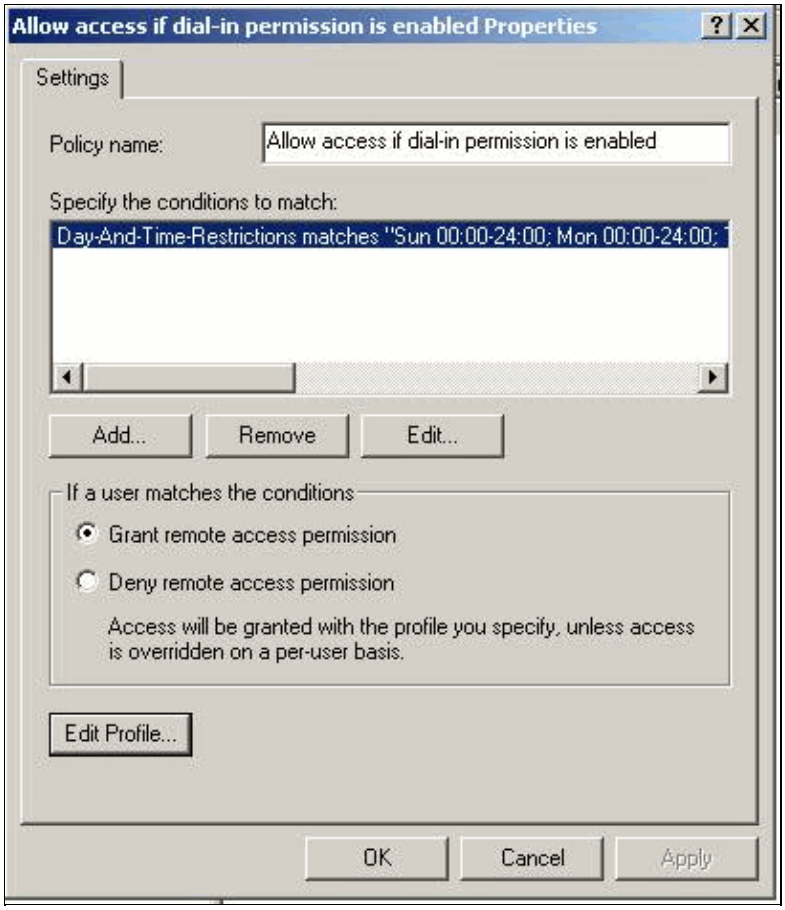
These steps guide you through a simple Microsoft Windows 2000 IAS RADIUS server configuration.

1. Under the Microsoft Windows 2000 IAS properties, select **Clients** and create a new client.

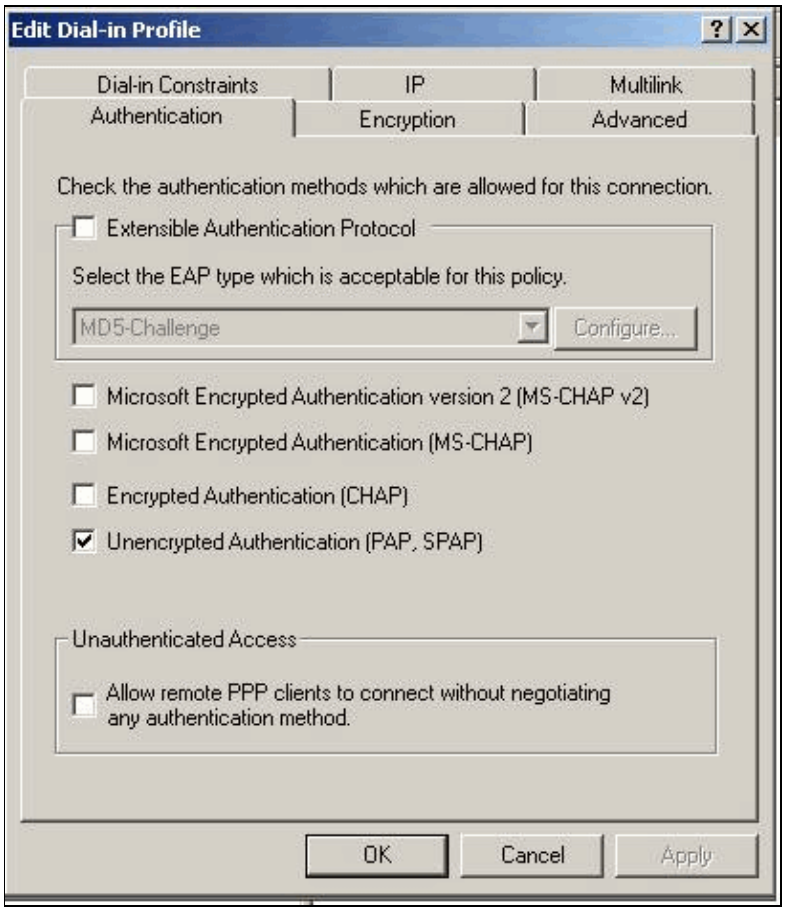
In this example, an entry named VPN5000 is created. The IP address of the Cisco VPN 5000 Concentrator is 172.18.124.223. Under the Client−Vendor drop−down box, select **Cisco**. The shared secret is the secret in the `[ RADIUS ]` section of the VPN Concentrator configuration.



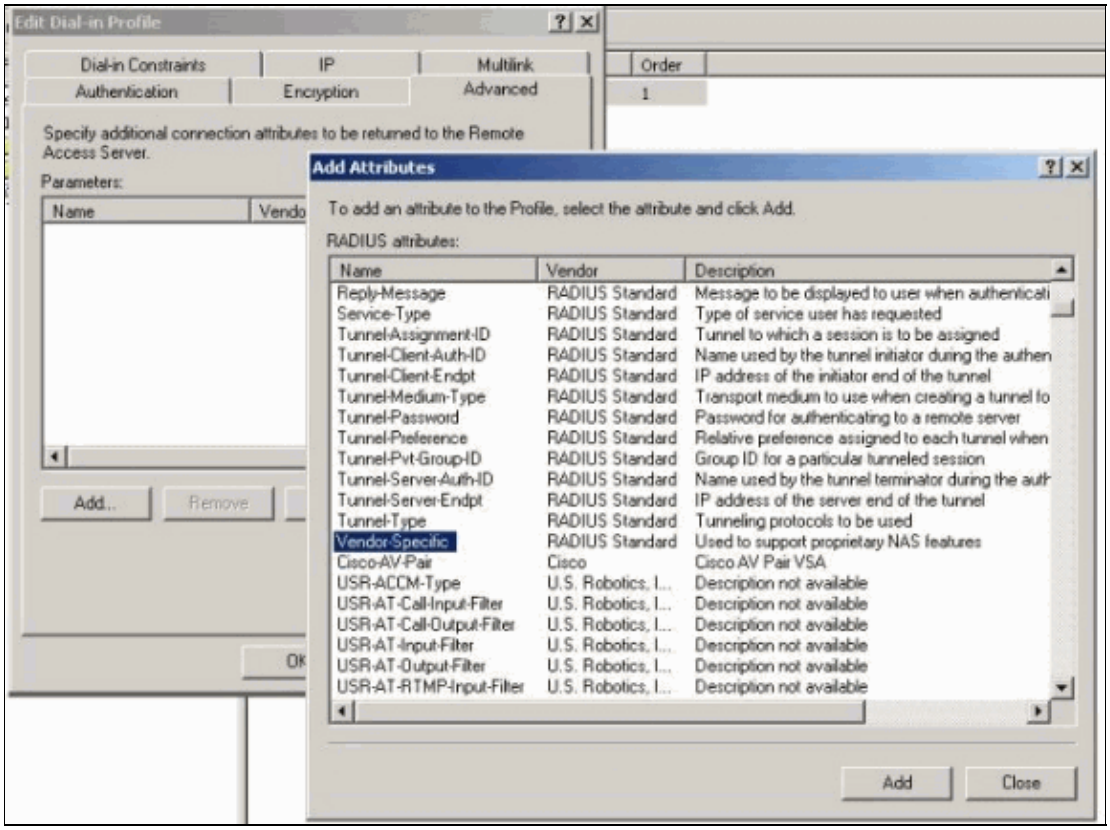
2. Under the properties of the Remote Access Policy, select **Grant remote access permission** under the "If a user matches the conditions" section and then click **Edit Profile**.



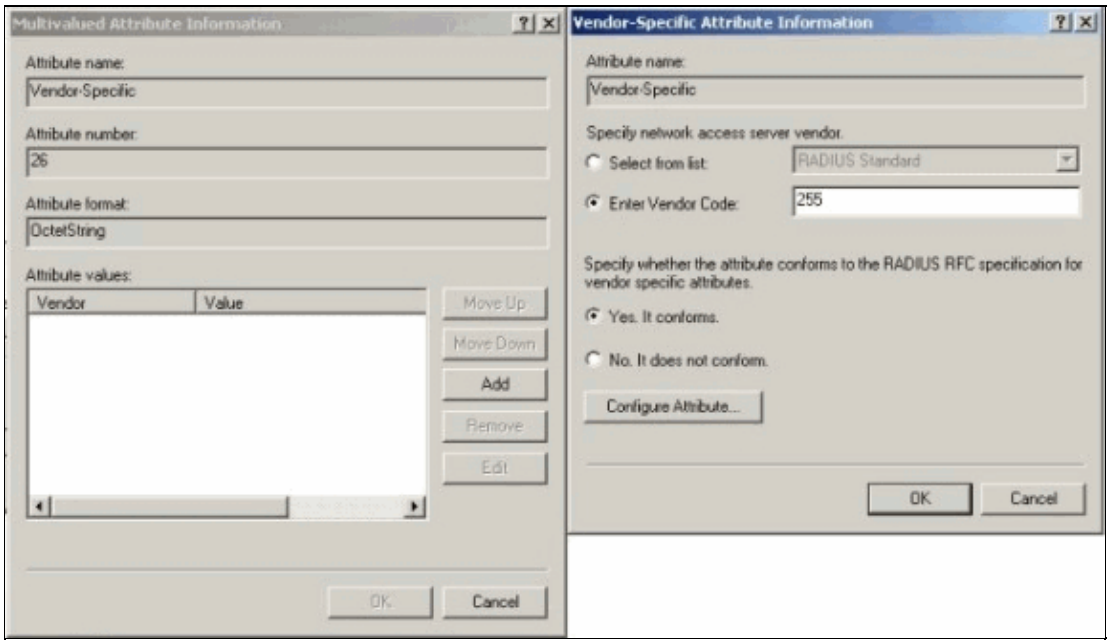
3. Click the Authentication tab and ensure that only **Unencrypted Authentication (PAP, SPAP)** is selected.



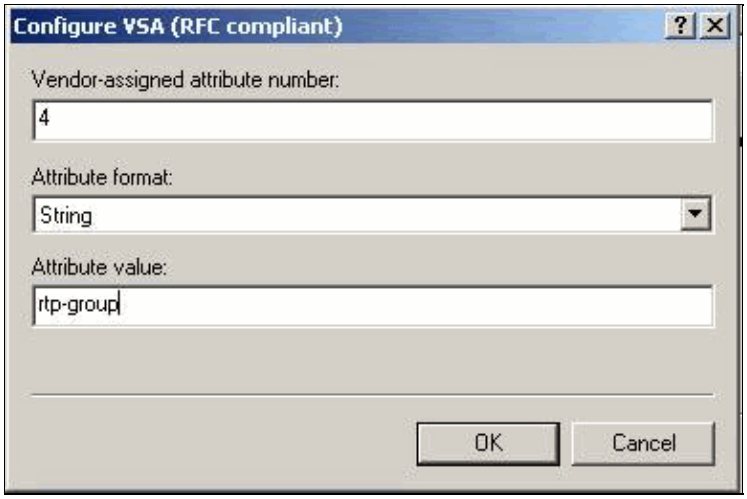
4. Select the Advanced tab, click **Add** and select **Vendor−Specific**.



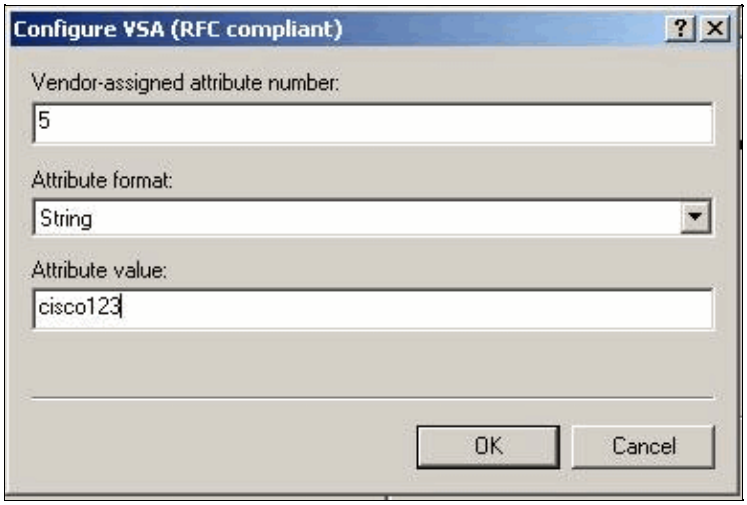
5. Under the Multivalued Attribute Information dialog box for the Vendor−Specific attribute, click **Add** in order to go to the Vendor−Specific Attribute Information dialog box. Select **Enter Vendor Code** and enter **255** in the adjacent box. Next, select **Yes. It conforms** and click **Configure Attribute**.



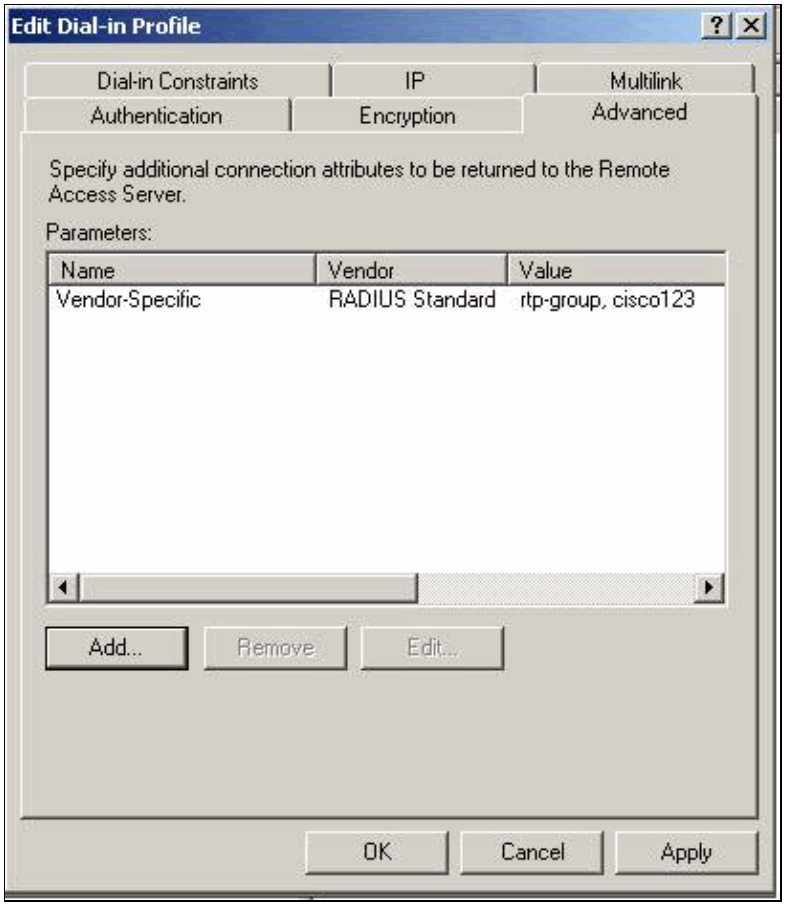
6. Under the Configure VSA (RFC compliant) dialog box, enter **4** for the Vendor−assigned attribute number, enter **String** for the Attribute format, and enter **rtp−group** (name of the VPN Group in the Cisco VPN 5000 Concentrator) for the Attribute value. Click **OK** and repeat step 5.



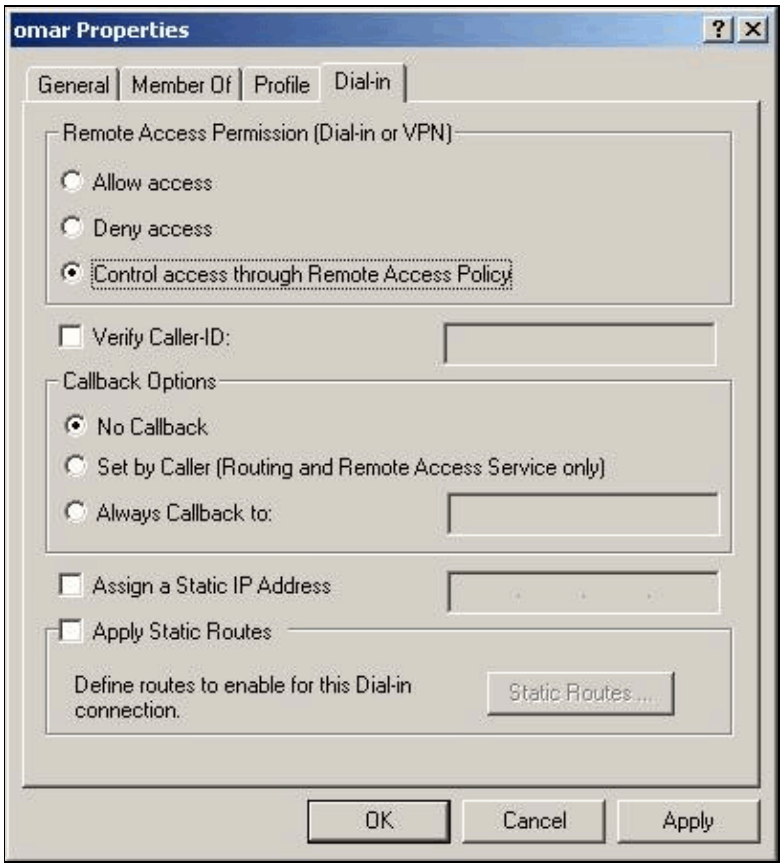
7. Under the Configure VSA (RFC compliant) dialog box, enter **4** for the Vendor−assigned attribute number, enter **String** for the Attribute format, and enter **cisco123** (the client shared secret) for the Attribute value. Click **OK**.



8. You see that the Vendor−Specific attribute contains two values (group and VPN password).



9. Under your user properties, click the Dial−in tab and ensure that **Control access through Remote Access Policy** is selected.



Verify the Result

This section provides information you can use in order to confirm your configuration works properly.

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

- **show radius statistics** Displays packet statistics for communication between the VPN Concentrator and the default RADIUS server identified by the RADIUS section.
- **show radius config** Shows the current settings for RADIUS parameters.

This is the output of the **show radius statistics** command.

```
VPN5001_4B9CBA80>show radius statistics

RADIUS Stats

Accounting            Primary       Secondary
Requests                 0             na
Responses                0             na
Retransmissions          0             na
Bad Authenticators       0             na
Malformed Responses      0             na
Packets Dropped          0             na
Pending Requests         0             na
Timeouts                 0             na
Unknown Types            0             na


Authentication        Primary       Secondary
Requests                 3             na
Accepts                  3             na
Rejects                  0             na
Challenges               0             na
Retransmissions          0             na
Bad Authenticators       0             na
Malformed Responses      0             na
Packets Dropped          0             na
Pending Requests         0             na
Timeouts                 0             na
Unknown Types            0             na



VPN5001_4B9CBA80>
```

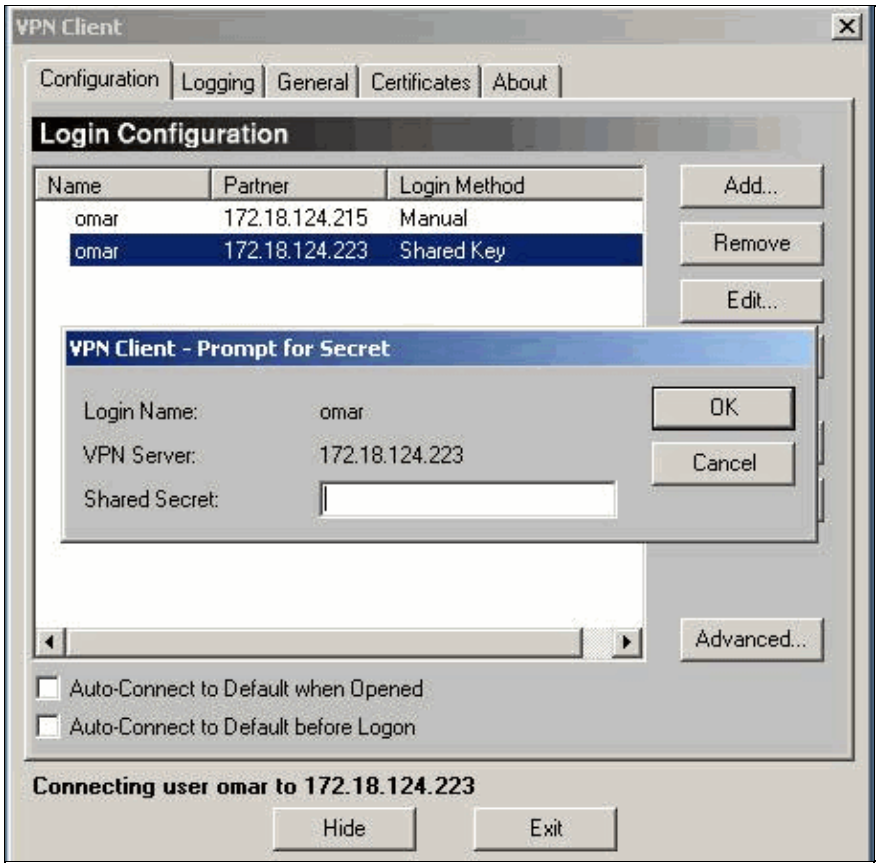
This is the output of the **show radius config** command.

```
RADIUS           State    UDP  CHAP16
Authentication   On      1812  No
Accounting       Off     1813  n/a
Secret           'radiuspassword'

Server     IP address      Attempts  AcctSecret
Primary    172.18.124.108         5  n/a
Secondary  Off
```

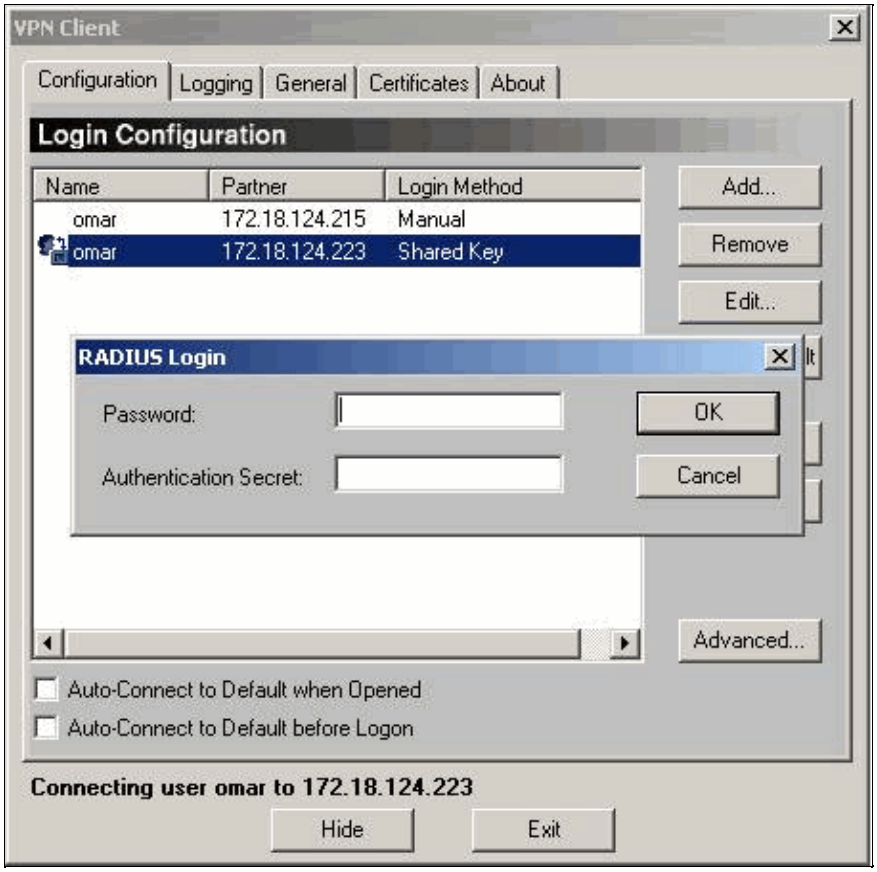
Configure the VPN Client

This procedure guides you through the configuration of the VPN Client.

1. From the VPN Client dialog box, select the Configuration tab. Next, from the VPN Client−Prompt for Secret dialog box, enter the shared secret under the VPN Server. The VPN Client shared secret is the value entered for the VPN password of attribute 5 in the VPN Concentrator.



2. After you enter the shared secret, you are prompted for a password and authentication secret. The password is your RADIUS password for that user, and the authentication secret is the PAP authentication secret in the `[ RADIUS ]` section of the VPN Concentrator.



Concentrator Logs

```
Notice   4080.11 seconds New IKE connection: [172.18.124.108]:1195:omar
Debug    4080.15 seconds Sending RADIUS PAP challenge to omar at 172.18.124.108
Debug    4087.52 seconds Received RADIUS PAP response from omar at 172.18.124.108, contact
Notice   4088.8 seconds VPN 0:3 opened for omar from 172.18.124.108.
Debug    4088.8 seconds Client's local broadcast address = 172.18.124.255
Notice   4088.8 seconds User assigned IP address 10.1.1.1
Info     4094.49 seconds Command loop started from 10.1.1.1 on PTY2
```

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- **Cisco VPN 5000 Series Concentrators End−of−Sales Announcement**
- **Cisco VPN 5000 Concentrator Support Page**
- **Cisco VPN 5000 Client Support Page**
- **IPSec Support Page**
- **Technical Support − Cisco Systems**

Updated: May 02, 2008 Document ID: 12491