# Configurando um Cisco VPN 5000 Concentrator com autenticação externa para um servidor RADIUS de IAS do Microsoft Windows 2000.

## Contents



## Introduction

Este documento descreve os procedimentos usados para configurar um Cisco VPN 5000 Concentrator com autenticação externa em um Microsoft Windows 2000 Internet Authentication Server (IAS) com RADIUS.

**Observação:** o Challenge Handshake Authentication Protocol (CHAP) não funciona. Use somente o PAP (Password Authentication Protocol Protocolo de Autenticação de Senha). Consulte o bug da Cisco ID CSCdt96941 (somente clientes registrados) para obter mais detalhes.

## Prerequisites

### Requirements

Não existem requisitos específicos para este documento.

### Componentes Utilizados

As informações aqui são baseadas nesta versão de software:

- Software Cisco VPN 5000 Concentrator versão 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.

# Configuração do concentrador Cisco VPN 5000

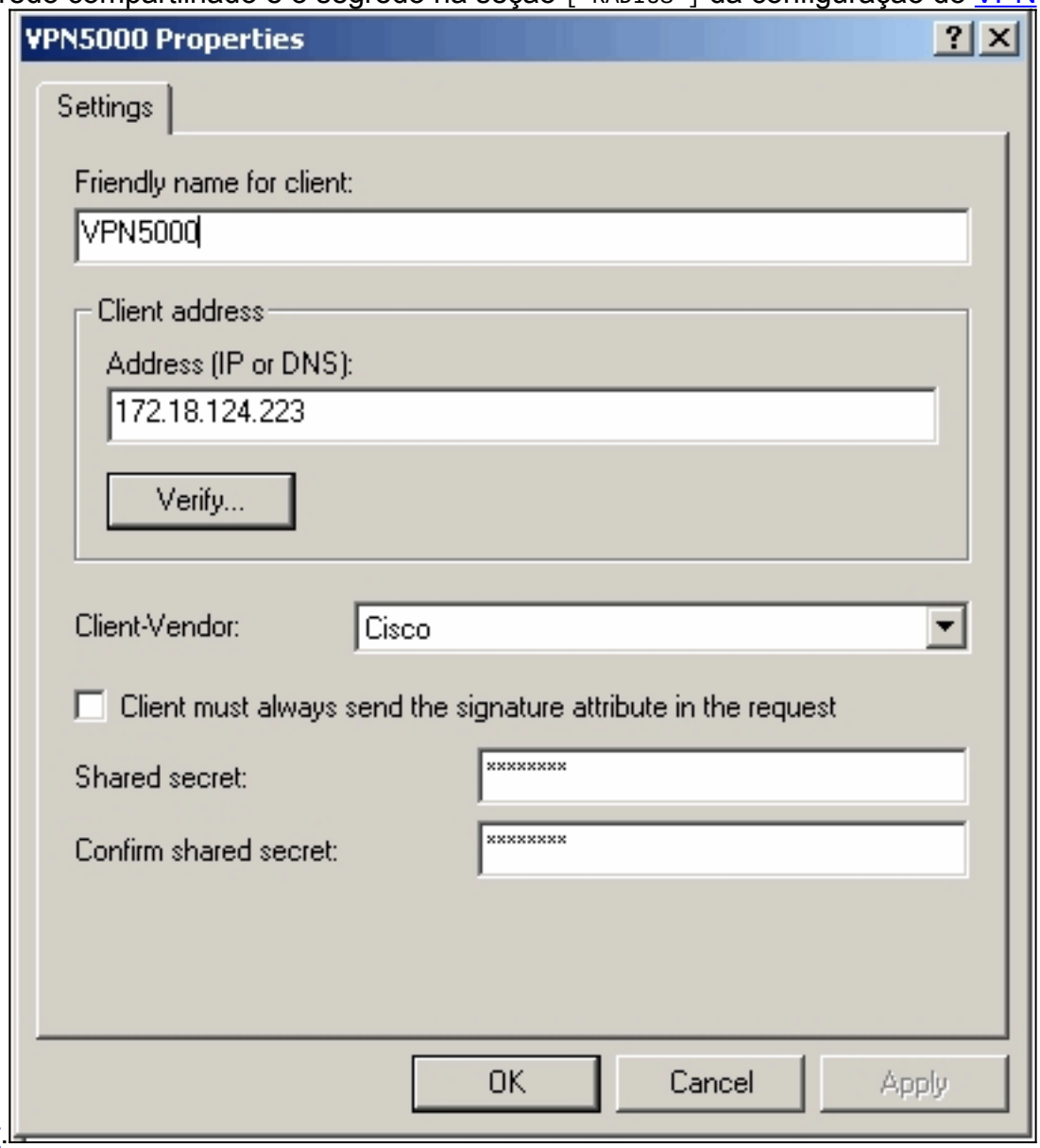
**VPN5001_4B9CBA80**

```
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#
```

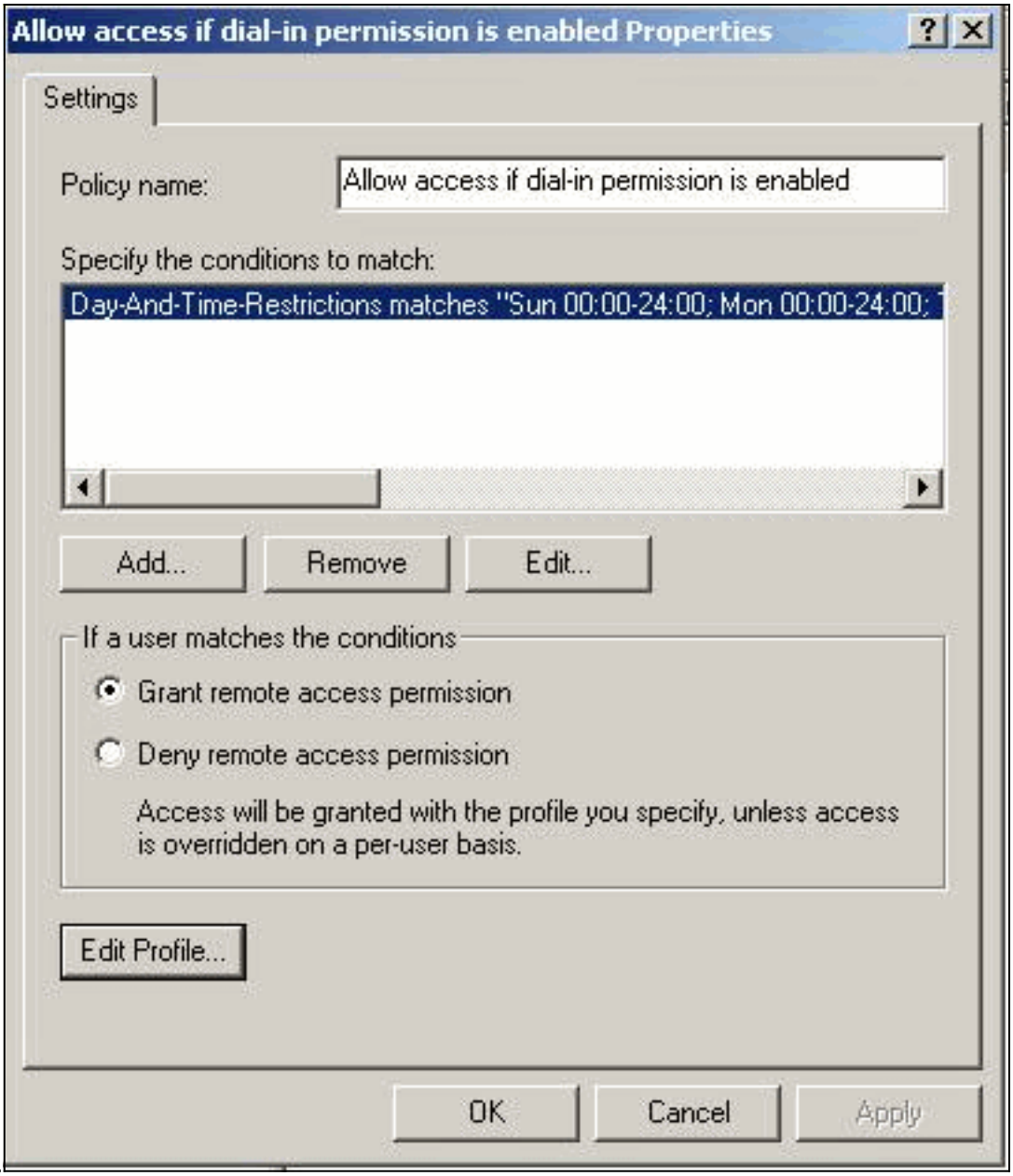
# Configurar o Microsoft Windows 2000 IAS RADIUS Server

Estas etapas o guiam por uma configuração simples do servidor Microsoft Windows 2000 IAS RADIUS.

1. Nas propriedades IAS do Microsoft Windows 2000, selecione **Clients** e crie um novo cliente.Neste exemplo, uma entrada chamada VPN5000 é criada. O endereço IP do Cisco VPN 5000 Concentrator é 172.18.124.223. Na caixa suspensa Client-Vendor, selecione **Cisco**. O segredo compartilhado é o segredo na seção `[ RADIUS ]` da configuração do VPN Concentrator.

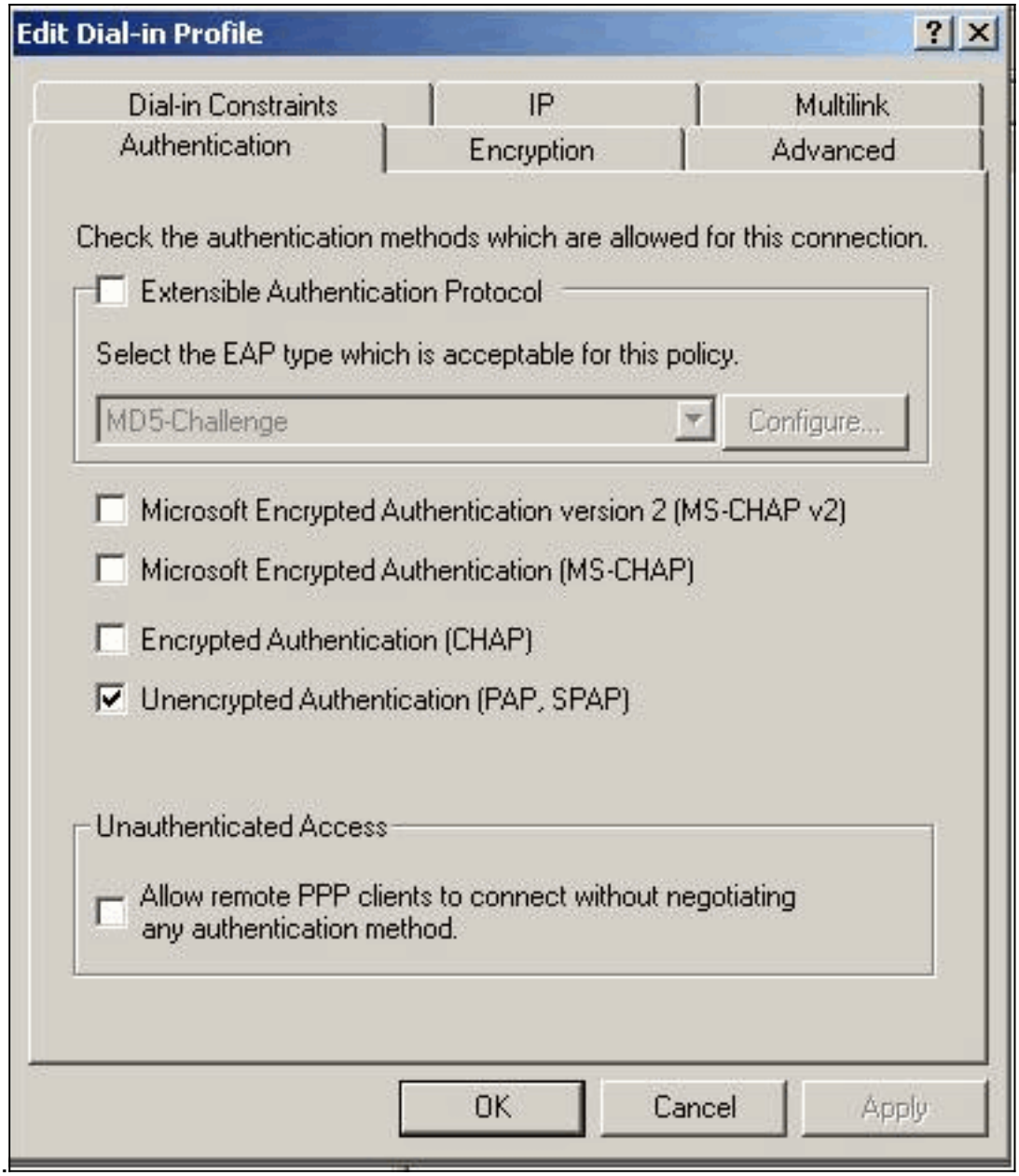



2. Nas propriedades da Política de acesso remoto, selecione **Conceder permissão de acesso remoto** na seção "Se um usuário corresponder às condições" e clique em **Editar**



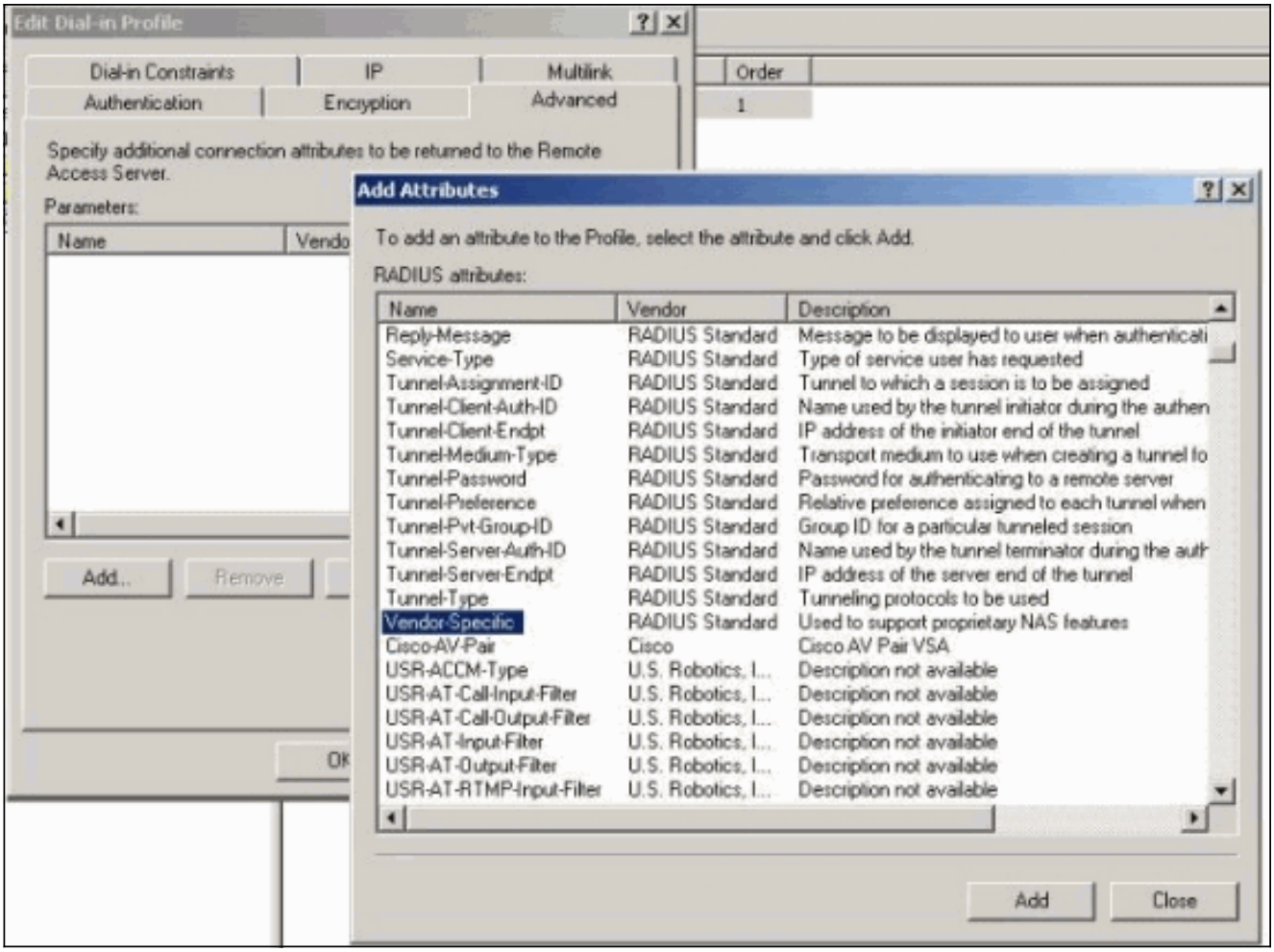

**perfil**.

3. Clique na guia Authentication (Autenticação) e verifique se **Unencrypted Authentication (PAP, SPAP)** está

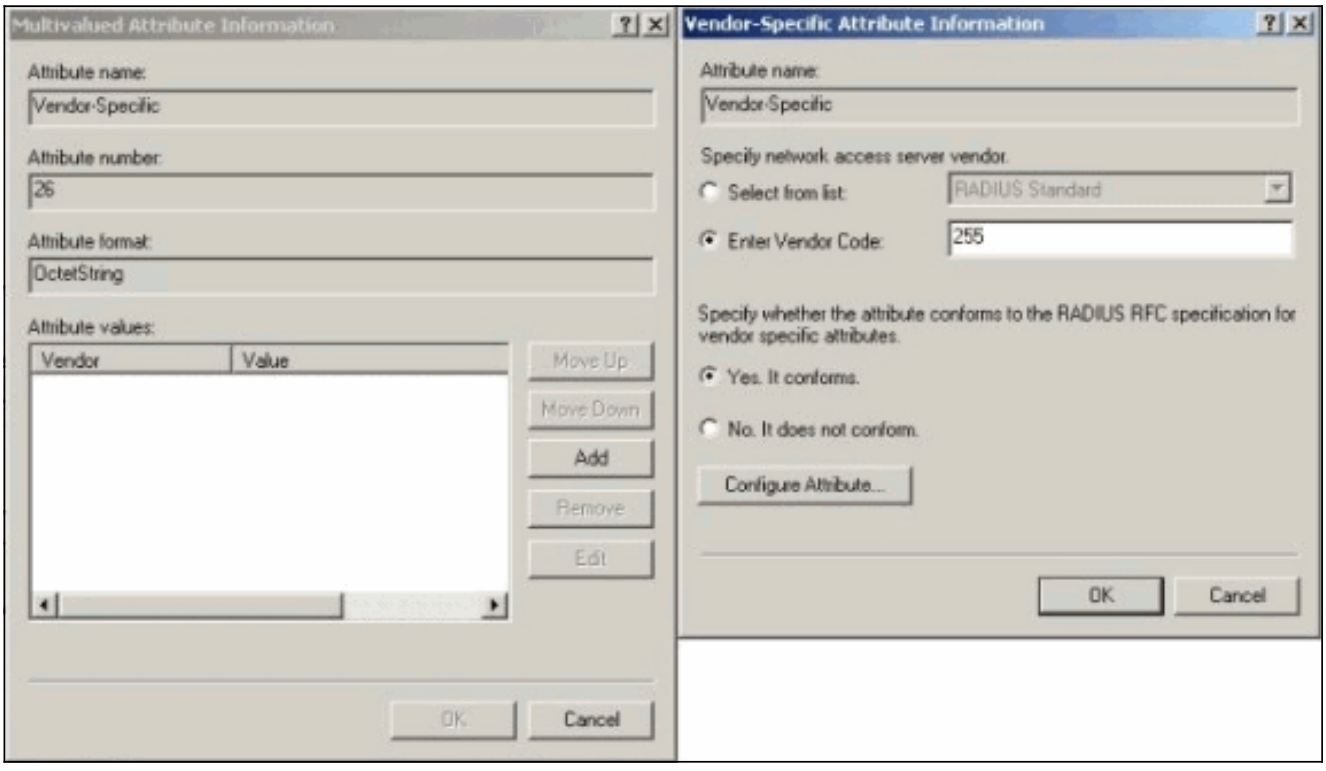



selecionado.

4. Selecione a guia Avançado, clique em **Adicionar** e selecione **Específico do fornecedor**.




5. Na caixa de diálogo Informações de atributo com vários valores para o atributo Específico do fornecedor, clique em **Adicionar** para ir para a caixa de diálogo Informações de atributo específicas do fornecedor. Selecione **Inserir código do fornecedor** e digite **255** na caixa adjacente. Em seguida, selecione **Sim. Ele está em conformidade** e clique em **Configurar atributo**.

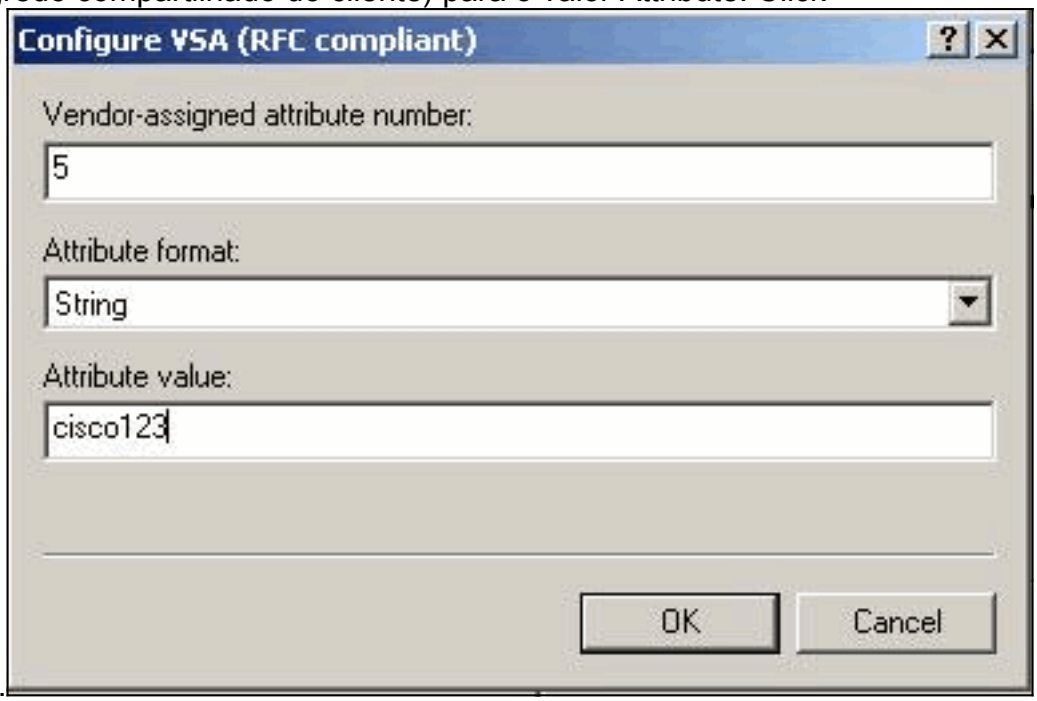



6. Na caixa de diálogo Configurar VSA (compatível com RFC), insira **4** para o número de atributo atribuído pelo Fornecedor, digite **String** para o formato do Atributo e digite **rtp-group**

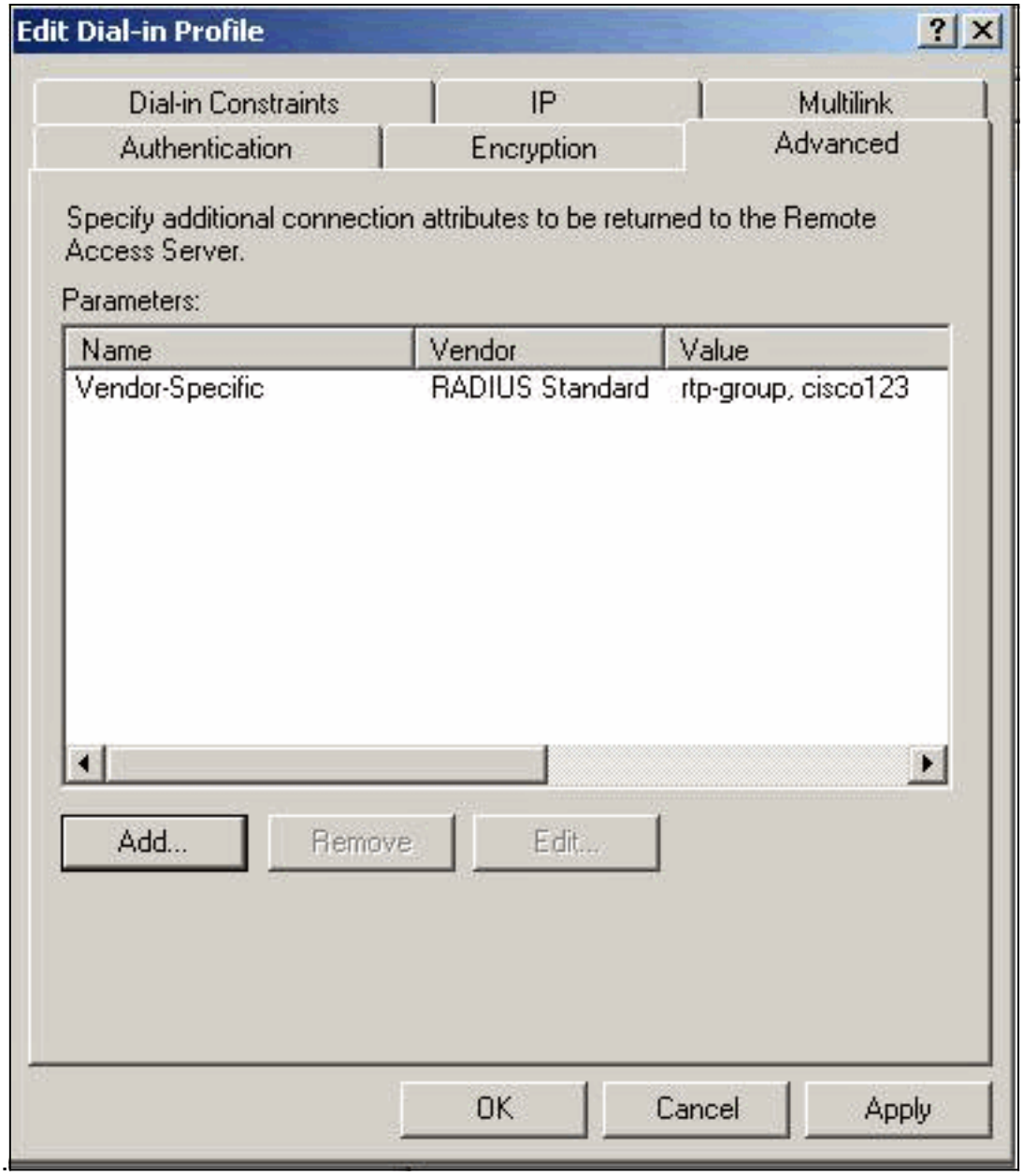
(nome do grupo VPN no Cisco VPN 5000 Concentrator) para o valor do Atributo. Clique em **OK** e repita a etapa

5. 


7. Na caixa de diálogo Configurar VSA (compatível com RFC), insira **4** para o número de atributo atribuído pelo fornecedor, digite **String** para o formato Attribute e digite **cisco123** (o segredo compartilhado do cliente) para o valor Attribute. Click **OK**.

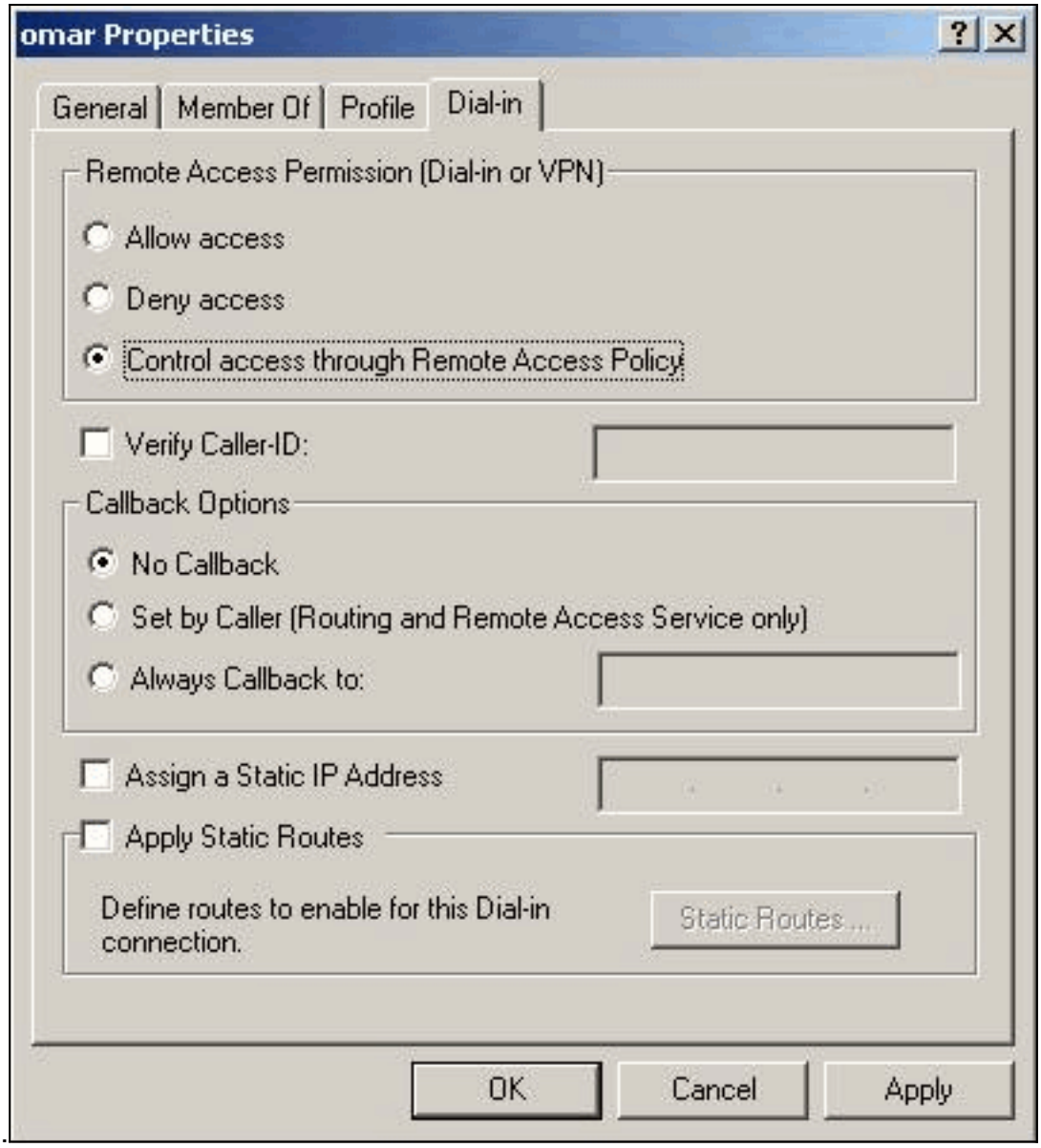



8. Você vê que o atributo Vendor-Specific contém dois valores (grupo e senha de




VPN).

9. Em suas propriedades de usuário, clique na guia Discar e verifique se o **acesso de controle por meio da Diretiva de acesso remoto** está



selecionado.

## Verificar o resultado

Esta seção fornece informações que você pode usar para confirmar se a sua configuração funciona corretamente.

A Output Interpreter Tool (somente clientes registrados) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

- **show radius statistics** —Exibe estatísticas de pacotes para comunicação entre o VPN Concentrator e o servidor RADIUS padrão identificado pela seção RADIUS.
- **show radius config** — Mostra as configurações atuais dos parâmetros RADIUS.

Esta é a saída do comando **show radius statistics**.

```
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>
```

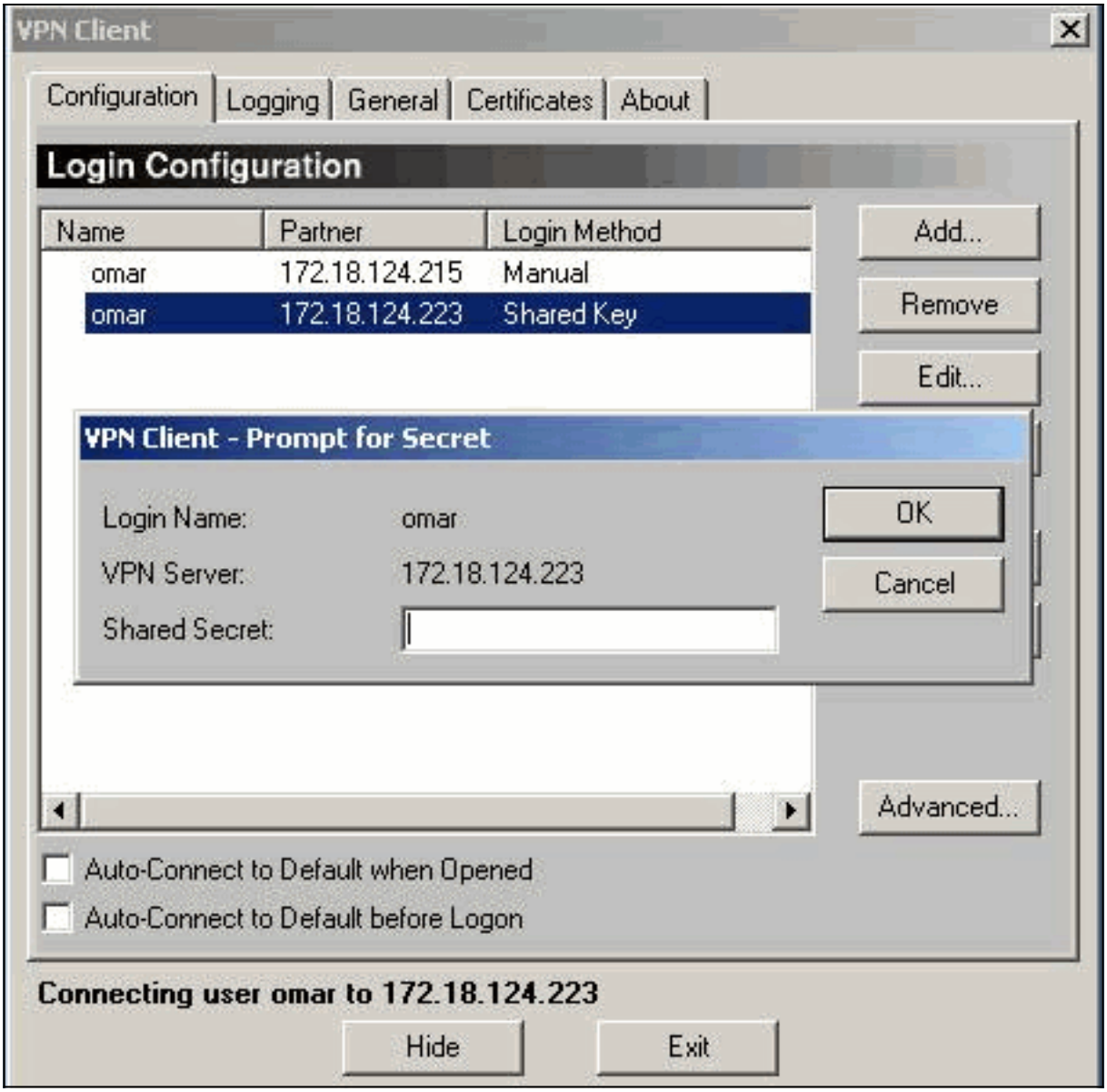
Esta é a saída do comando **show radius config**.

```
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
```

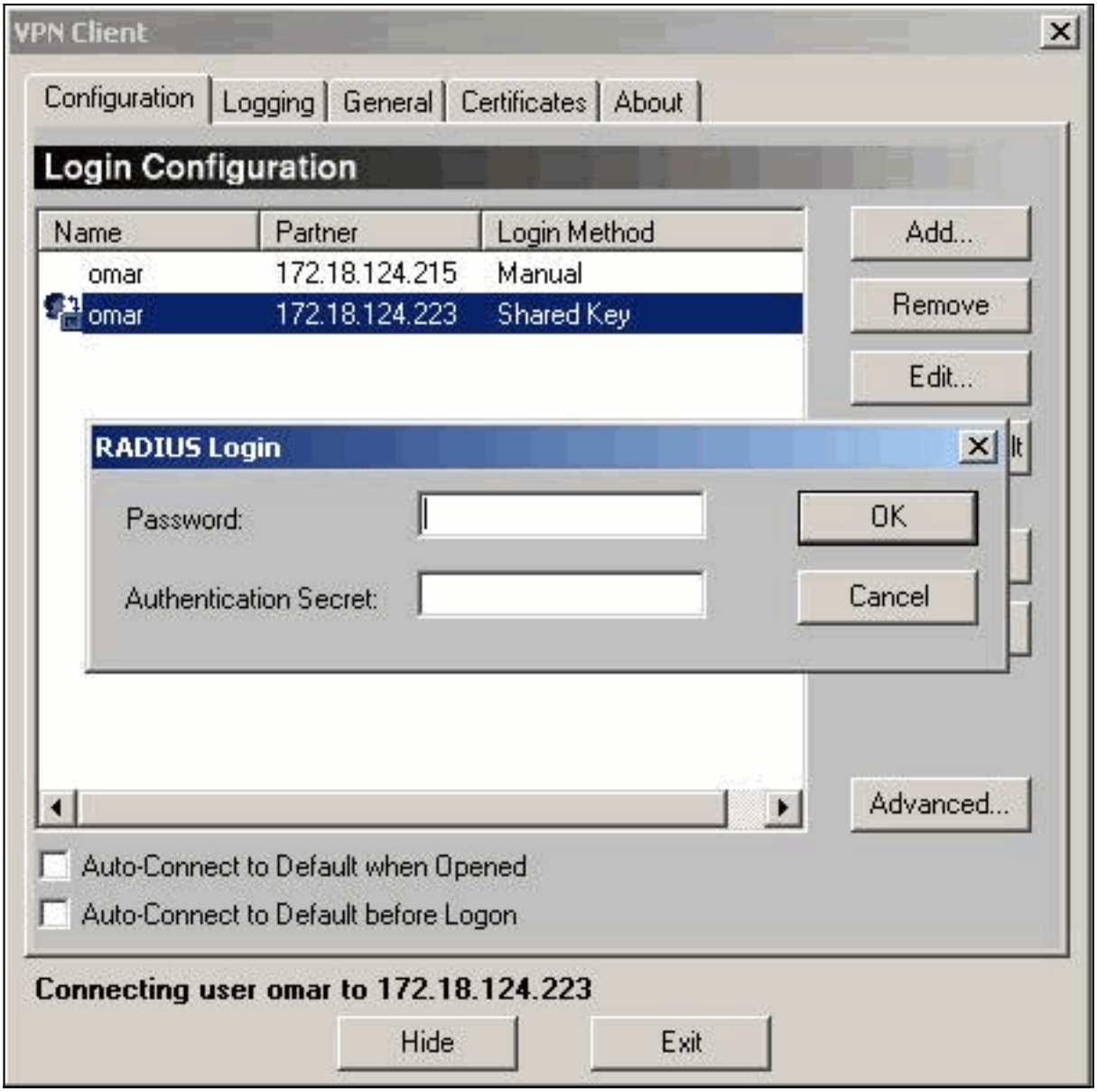
# Configurar o VPN Client

Este procedimento o orienta na configuração do VPN Client.

1. Na caixa de diálogo Cliente VPN, selecione a guia Configuração. Em seguida, na caixa de diálogo VPN Client-Prompt for Secret, digite o segredo compartilhado no VPN Server. O segredo compartilhado do VPN Client é o valor inserido para a senha VPN do atributo 5 no VPN
   Concentrator.




2. Depois de inserir o segredo compartilhado, você será solicitado a fornecer uma senha e um segredo de autenticação. A senha é sua senha RADIUS para esse usuário, e o segredo da autenticação é o segredo da autenticação PAP na seção `[ RADIUS]` do VPN Concentrator.




## Registros do concentrador

```
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, contacting
server
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

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

## Informações Relacionadas

- Anúncio do fim do ciclo de comercialização dos concentradores Cisco VPN 5000 Series

- Página de suporte do Cisco VPN 5000 Concentrator
- Página de suporte do Cisco VPN 5000 Client
- Página de suporte do IPSec
- Suporte Técnico - Cisco Systems