使用外部认证配置 Cisco VPN 5000 集中器到 Microsoft Windows 2000 IAS RADIUS 服务器的连接

目录

简介
先决条件
要求
使用的组件
规则
Cisco VPN 5000 集中器配置
配置Microsoft Windows 2000 IAS RADIUS服务器
验证结果
配置 VPN 客户端
集中器日志
故障排除
相关信息

简介

本文档介绍用于配置Cisco VPN 5000集中器的过程，该集中器使用外部身份验证到带有RADIUS的Microsoft Windows 2000 Internet身份验证服务器(IAS)。

注意：质询握手身份验证协议(CHAP)不起作用。仅使用密码身份验证协议(PAP)。 有关详细信息，请参阅Cisco Bug ID CSCdt96941(仅限注册客户)。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件版本：

- Cisco VPN 5000 集中器软件版本 6.0.16.0001

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文件规则的更多信息请参见“ Cisco技术提示规则”。

Cisco VPN 5000 集中器配置

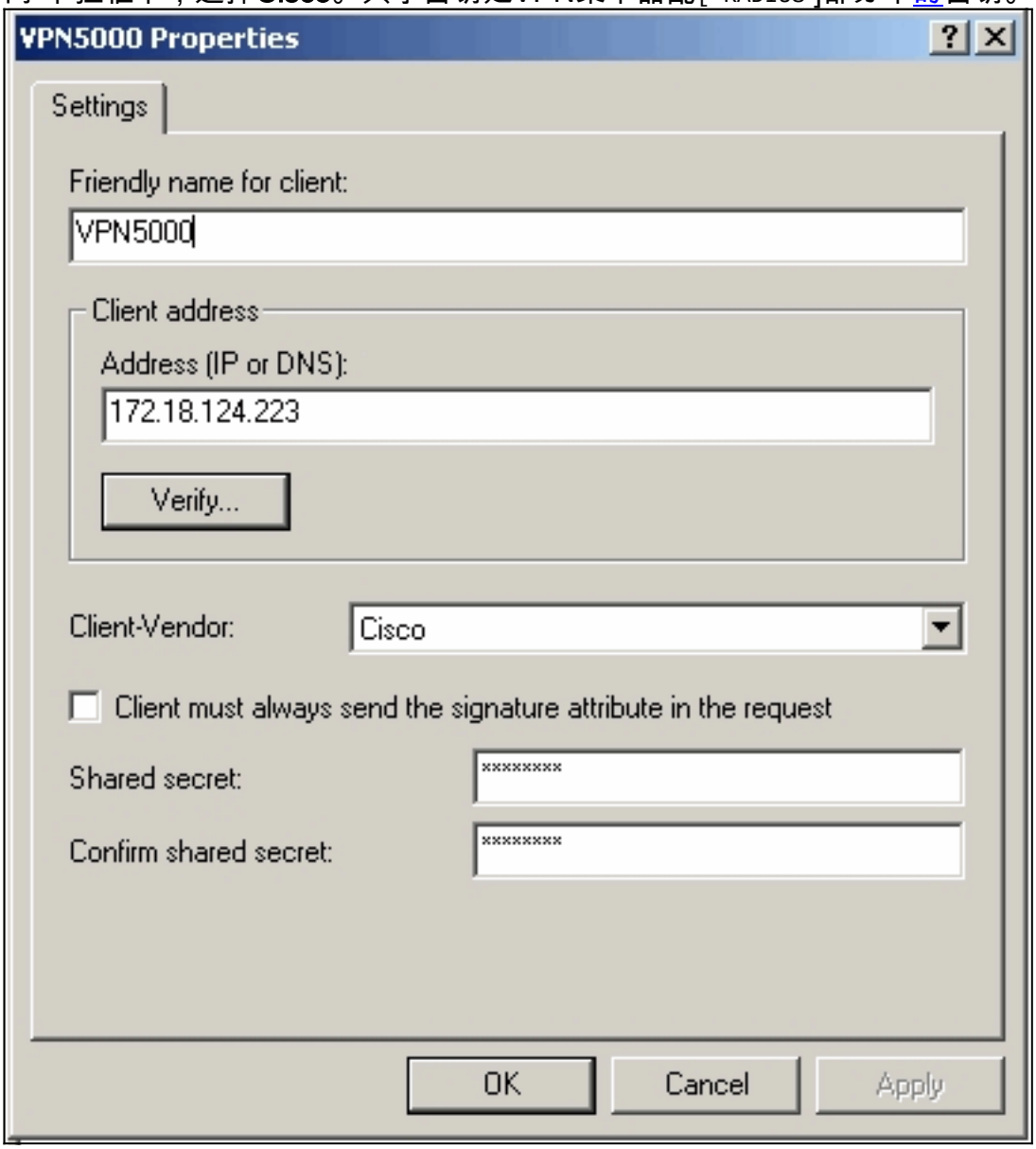
VPN5001_4B9CBA80

```
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#
```

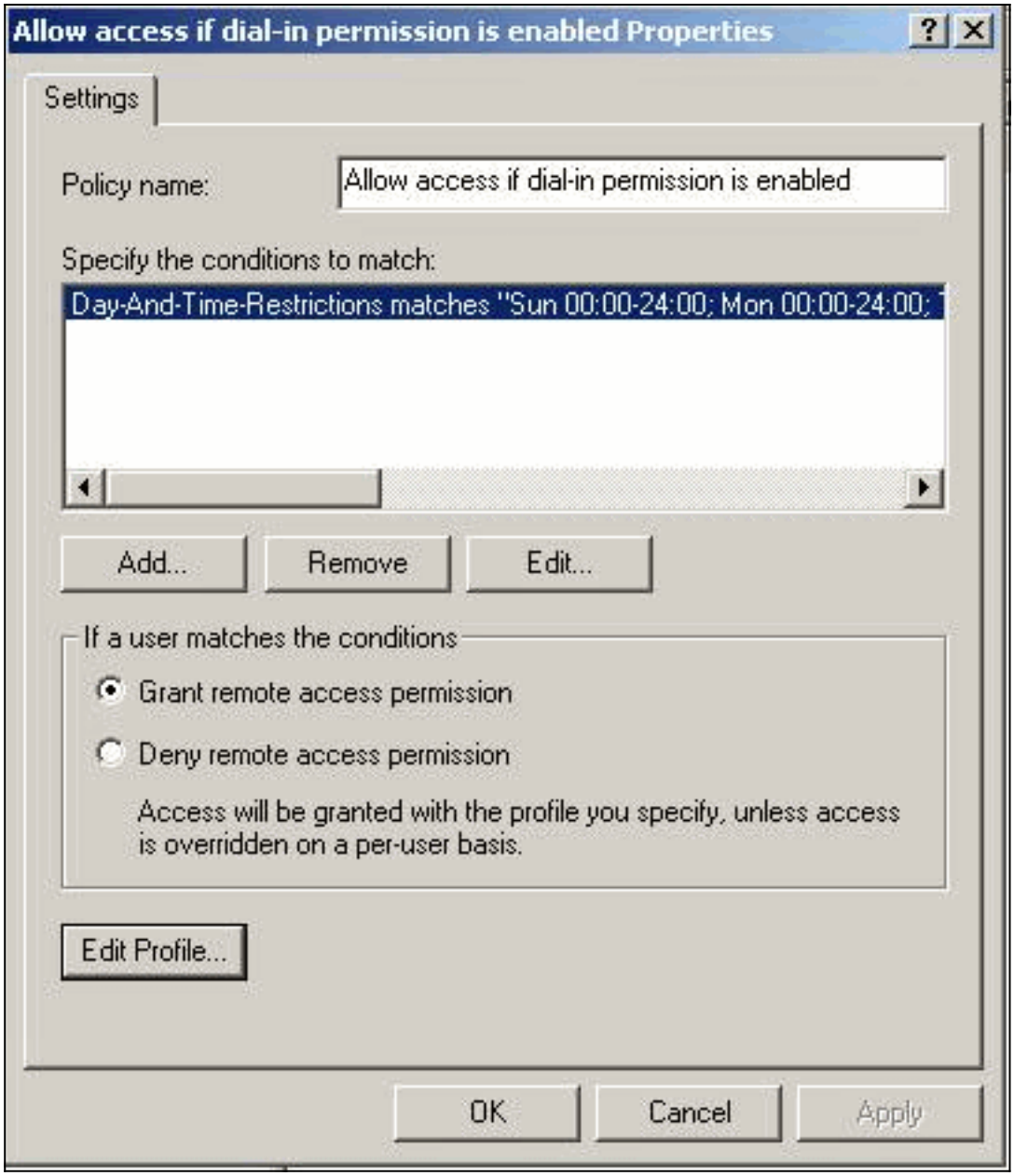
配置Microsoft Windows 2000 IAS RADIUS服务器

这些步骤将指导您完成简单的Microsoft Windows 2000 IAS RADIUS服务器配置。

1. 在Microsoft Windows 2000 IAS属性下，选择“客户**端”**并创建新客户端。在本示例中，创建名为VPN5000的条目。Cisco VPN 5000集中器的IP地址是172.18.124.223。在“客户端 — 供应商”下拉框下，选择**Cisco**。共享密钥是VPN集中器配[RADIUS]部分中的密钥。

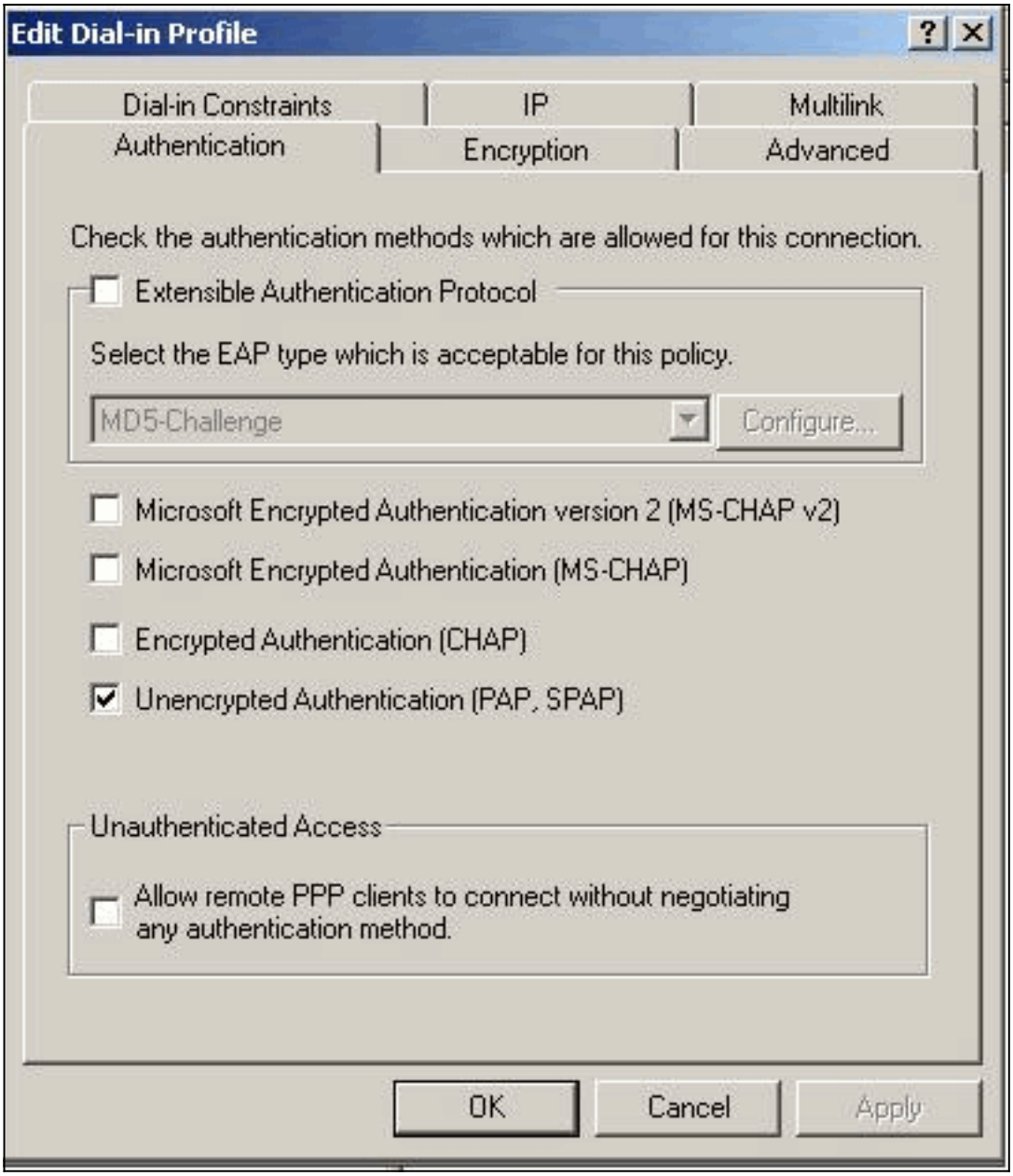


2. 在远程访问策略的属性下，在“If a user matches the conditions”（如果用户匹配条件）部分选择**Grant remote access permission**（授予远程访问权限），然后单击**Edit Profile(编辑配置文**

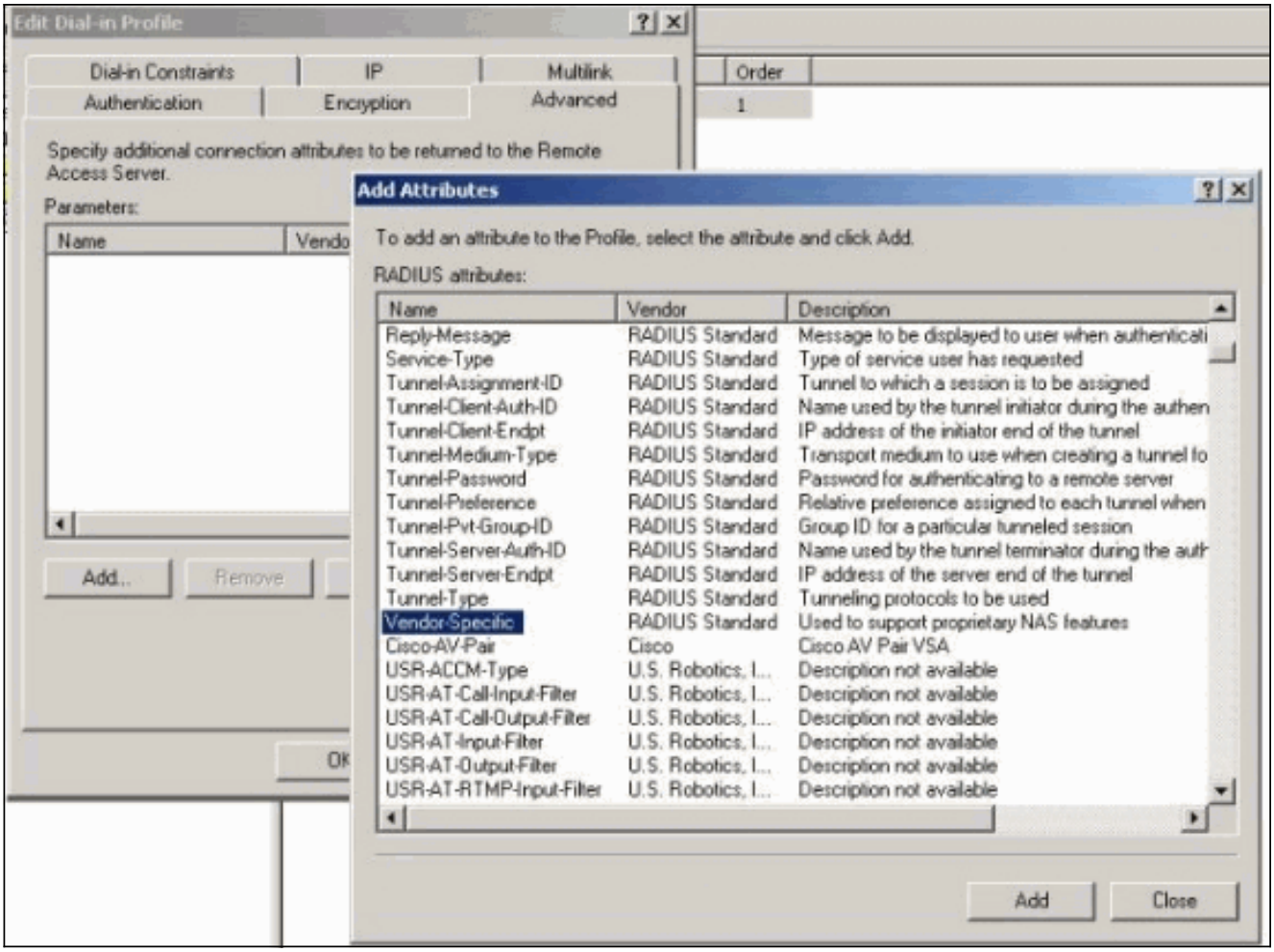


件)。

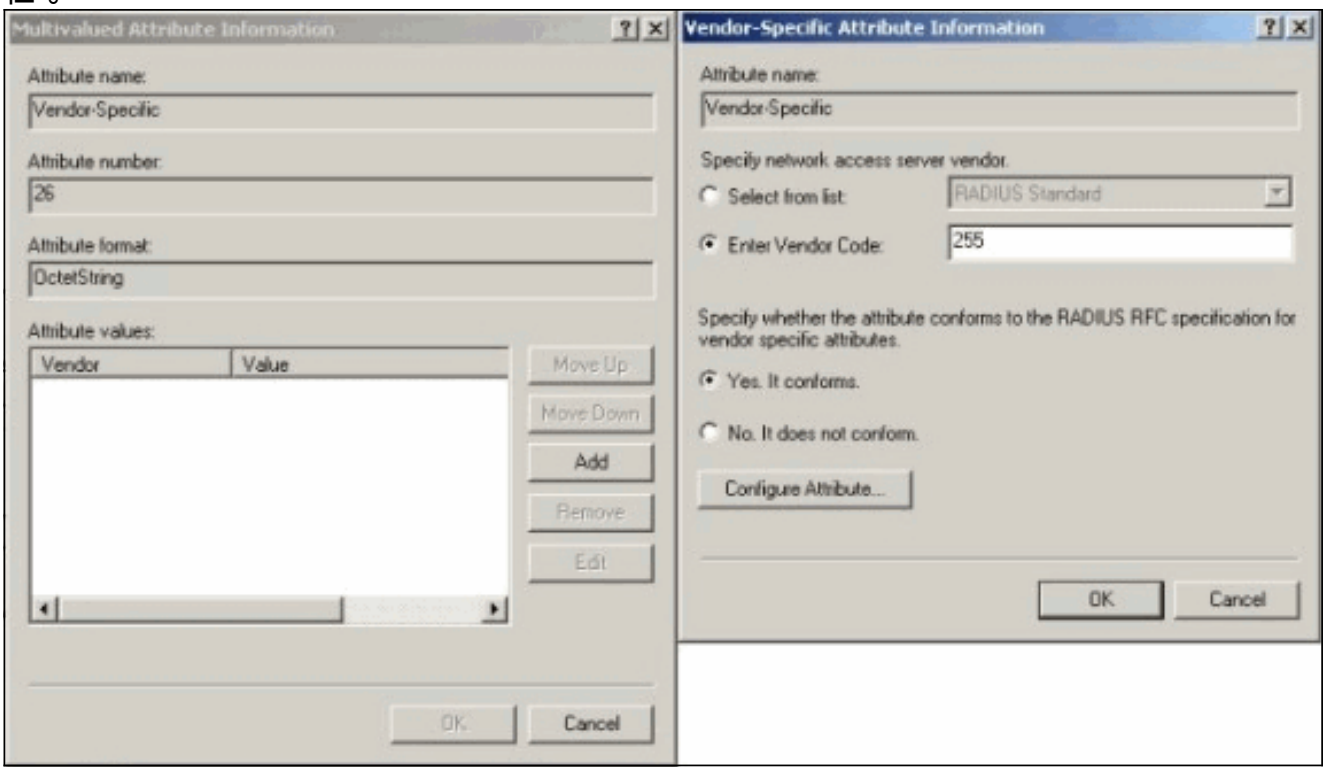
3. 单击Authentication选项卡，确保仅选择**Unencrypted Authentication(PAP， SPAP)**。



4. 选择“高级”选项卡，单**击“添**加”并**选择供应商特定**。



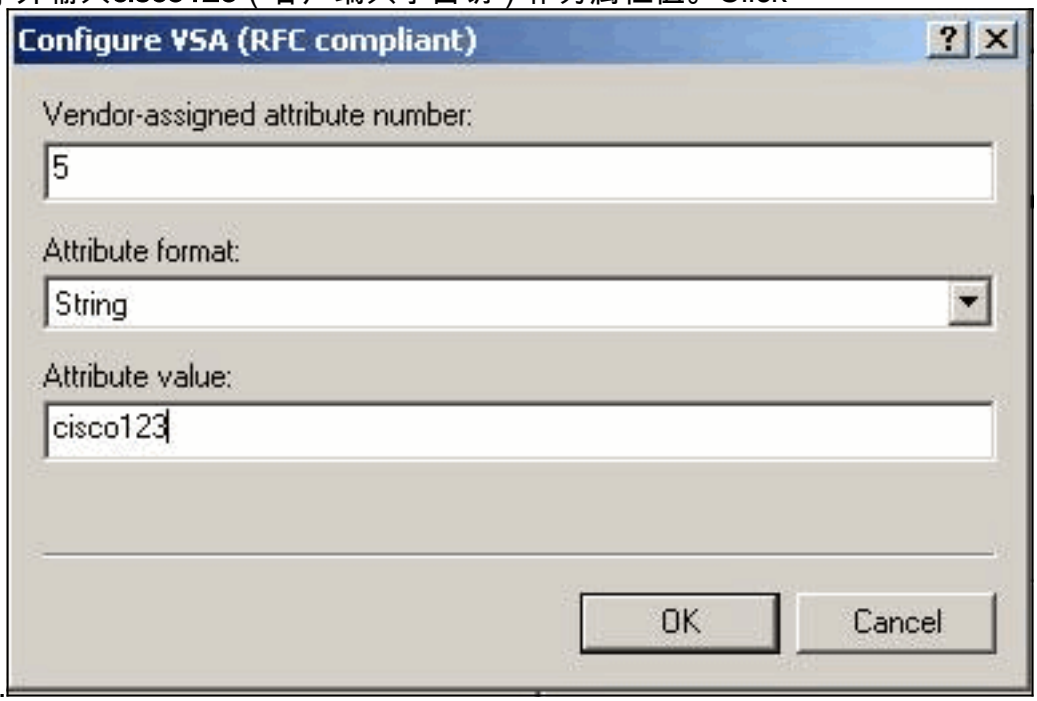
5. 在供应商特定属性的多值属性信息对话框下，单击**添加**以转到供应商特定属性信息对话框。选择**输入供应商**代码，**然后在**相邻框中输入255。然后，选择**是。它符合要求**，然后单**击"配置属性"**。



6. 在配置VSA（符合RFC）对话框下，输入**4**作为供应商分配的属性编号，输入**String**作为属性格式，并输入**rtp-group**（Cisco VPN 5000集中器中VPN组的名称）作为属性值。单击**OK**并重**复**

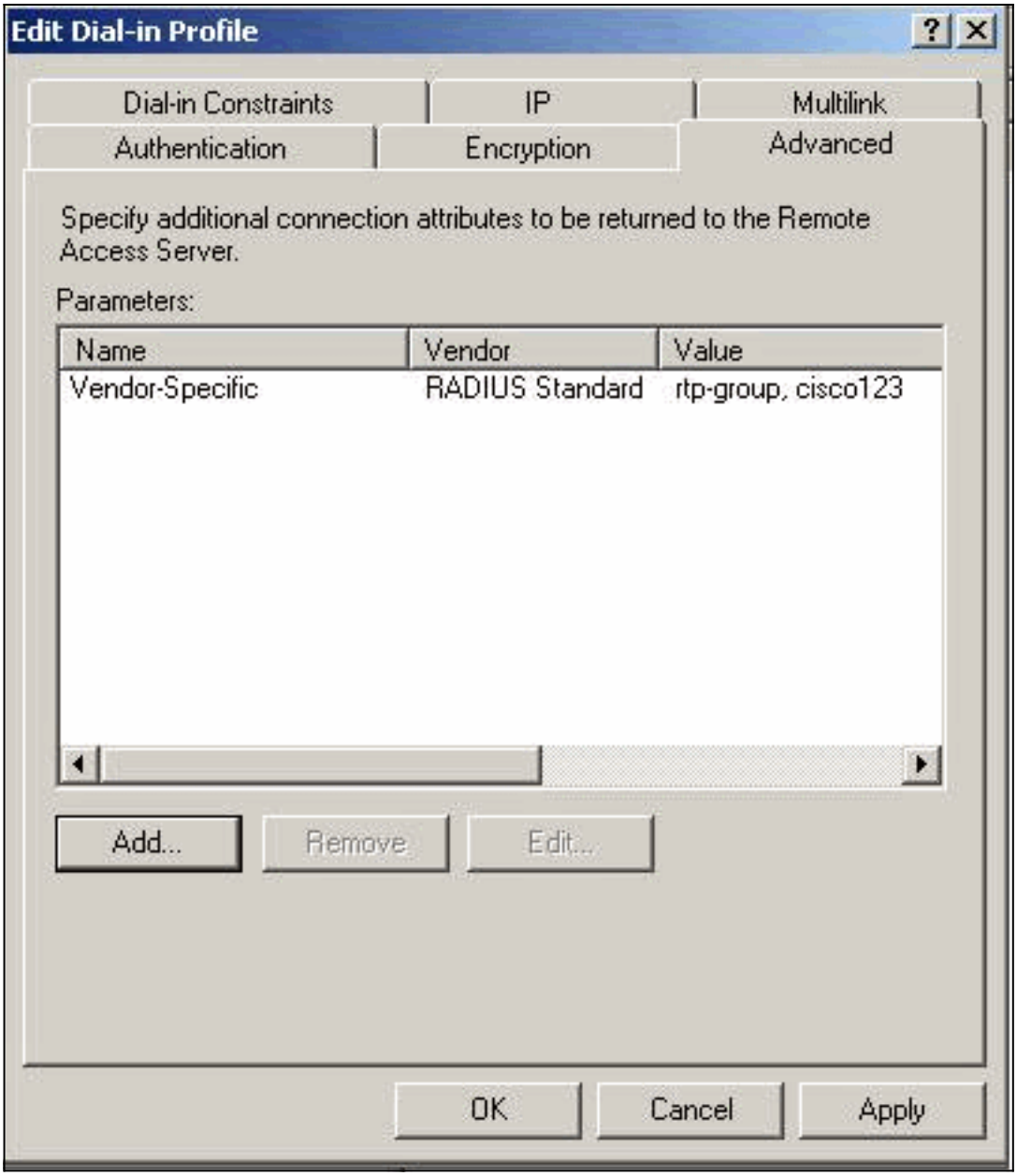
步骤5。

7. 在配置VSA（符合RFC）对话框下，输入**4**作为供应商分配的属性编号，输入**String**作为属性格式，并输入**cisco123**（客户端共享密钥）作为属性值。Click

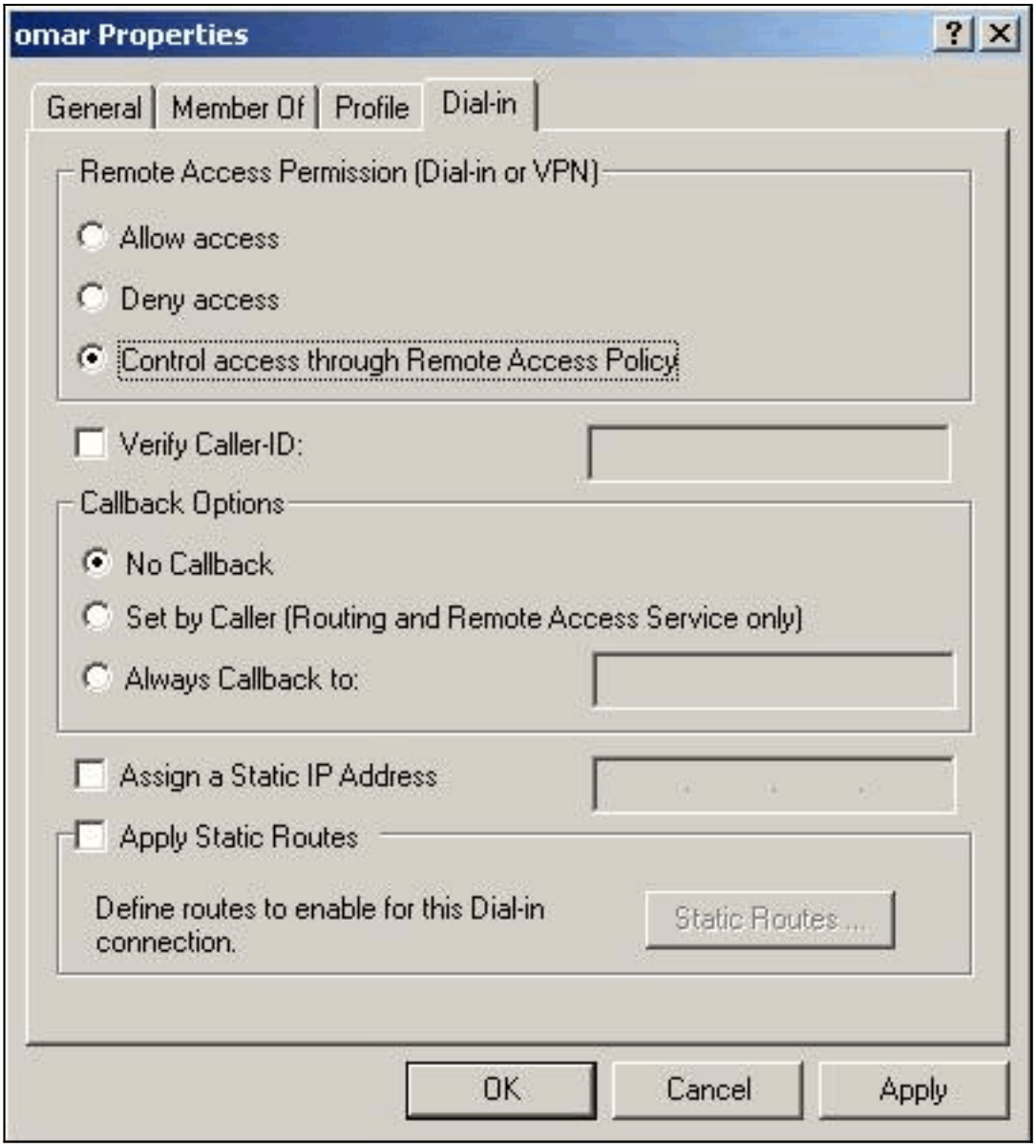


OK.

8. 您会看到供应商特定属性包含两个值（组和VPN密码）。



9. 在用户属性下，单击“拨入”选项卡，并确保已选**择“通过远程访问策略控制**访问”。



验证结果

本部分提供了可用于确认您的配置是否正常运行的信息。

命令输出解释程序工具（仅限注册用户）支持某些 **show 命令，使用此工具可以查看对 show 命令输出的分析。**

- **show radius statistics** — 显示VPN集中器与RADIUS部分标识的默认RADIUS服务器之间通信的数据包统计信息。
- **show radius config** — 显示RADIUS参数的当前设置。

这是show radius statistics命**令的输**出。

```
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>
```

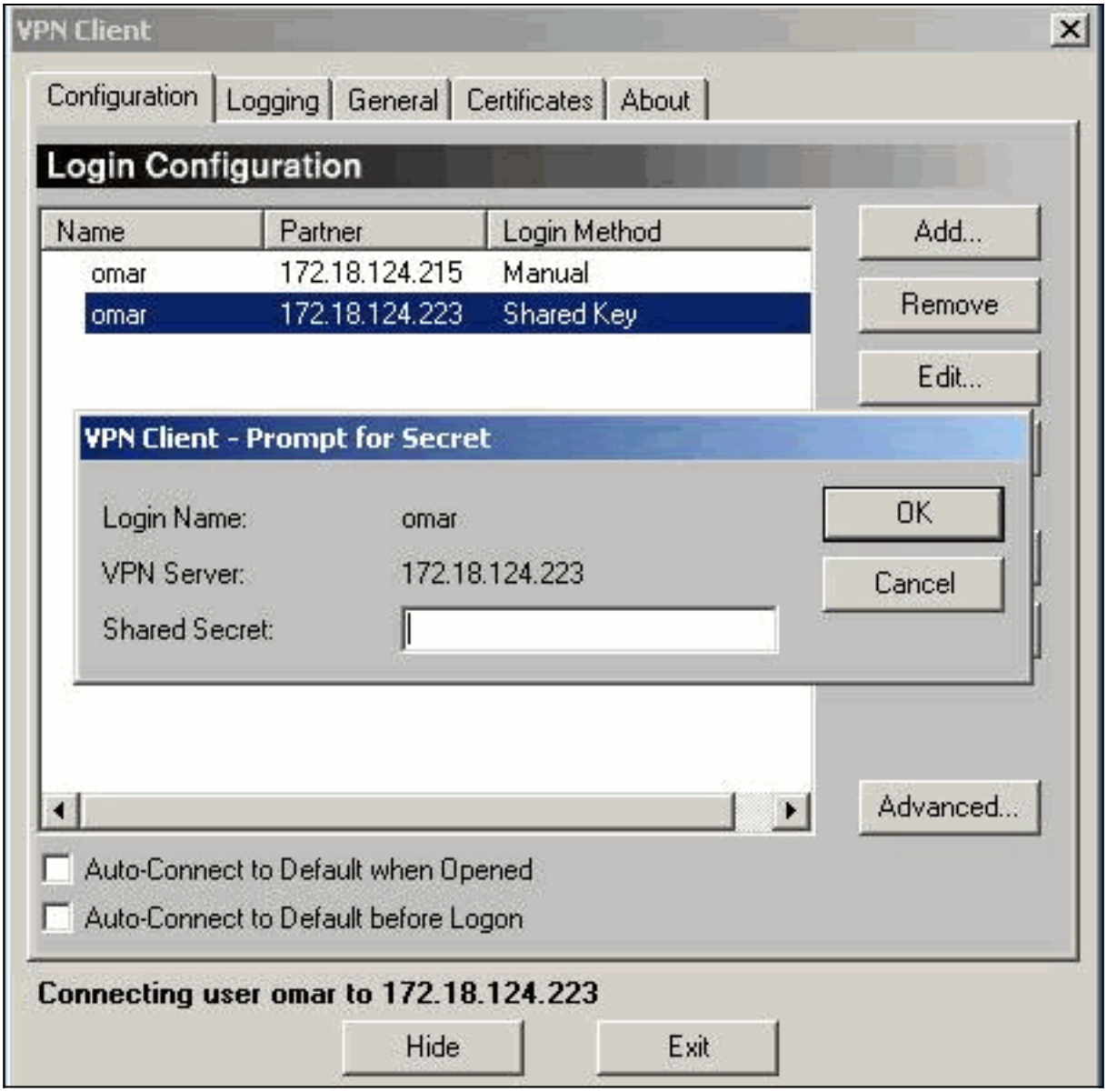
这是show radius config命令的输出。

```
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
```

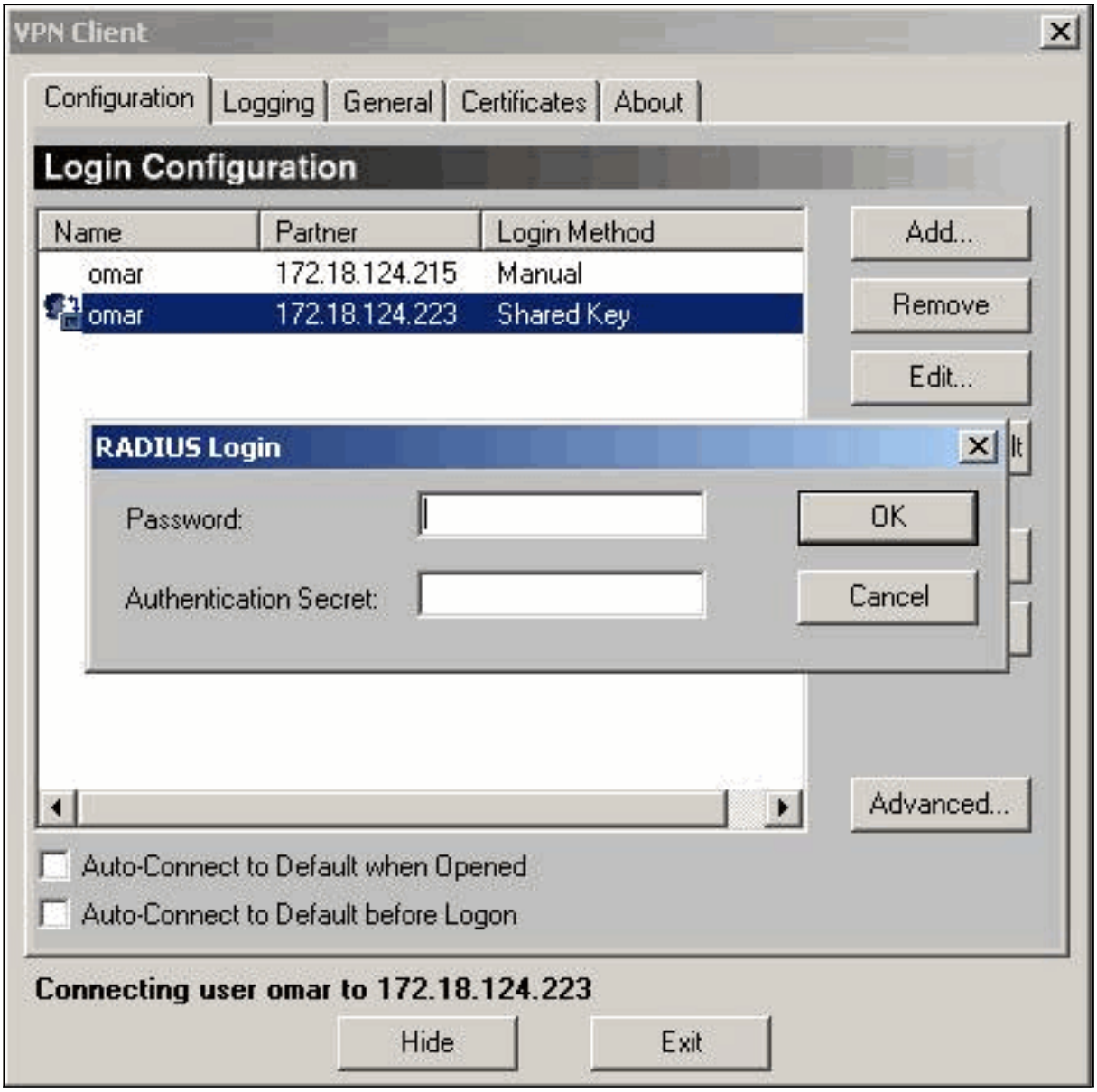
配置 VPN 客户端

此过程将指导您完成VPN客户端的配置。

1. 从VPN Client对话框中，选择Configuration选项卡。然后，在VPN Client-Prompt for Secret对话框中，在VPN Server下输入共享密钥。VPN Client shared secret是为VPN集中器中属性5的VPN密码输入的值。



2. 输入共享密钥后，系统会提示您输入密码和身份验证密钥。密码是该用户的RADIUS密码，身份验证密钥是VPN集中器[RADIUS]部PAP身份验证密钥。



集中器日志

```
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
```

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- Cisco VPN 5000 系列集中器终止销售公告
- Cisco VPN 5000 集中器支持页

- Cisco VPN 5000 客户端支持页
- IPSec 支持页面
- 技术支持 - Cisco Systems