

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

本文描述使用的步骤配置有外部验证的一台Cisco VPN 5000集中器到一个Microsoft Windows 2000互联网认证服务器(IAS)与RADIUS。

注意：质询握手验证协议(CHAP)不工作。请使用只密码认证协议。参考Cisco Bug ID [CSCdt96941](#) (仅限注册用户)关于更详细的资料。

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

有关文档规则的详细信息，请参阅 [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#
```

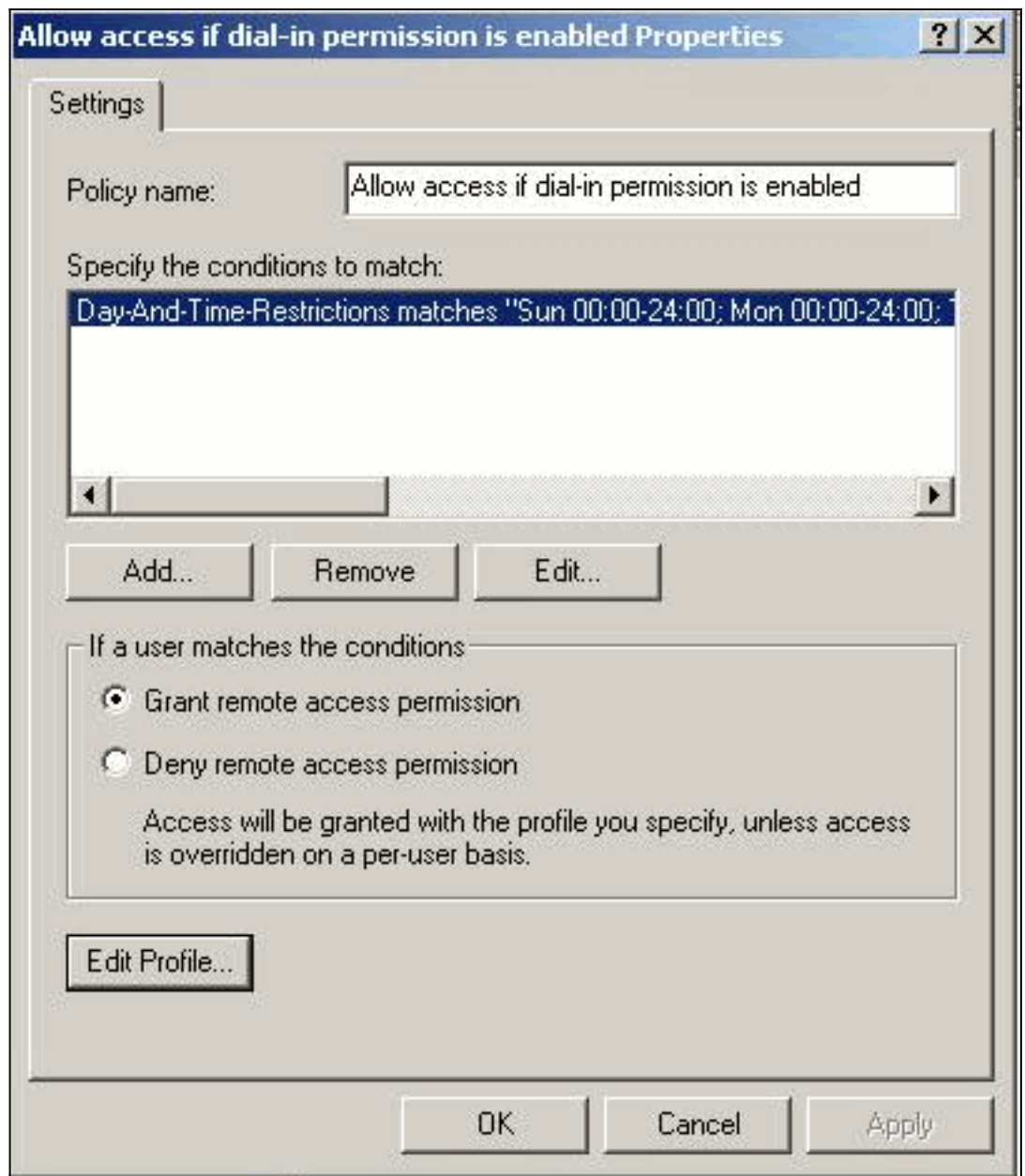
配置Microsoft Windows 2000 IAS RADIUS服务器

这些步骤通过一个简单Microsoft Windows 2000 IAS RADIUS服务器配置指导您。

1. 在Microsoft Windows 2000 IAS属性下，请选择**客户端**并且创建一个新的客户端。在本例中，名为VPN5000的条目创建。Cisco VPN 5000集中器的IP地址是172.18.124.223。在Client-Vendor下拉框下，请选择**思科**。共享机密是在**VPN集中器**配置的[RADIUS]部分的机密。

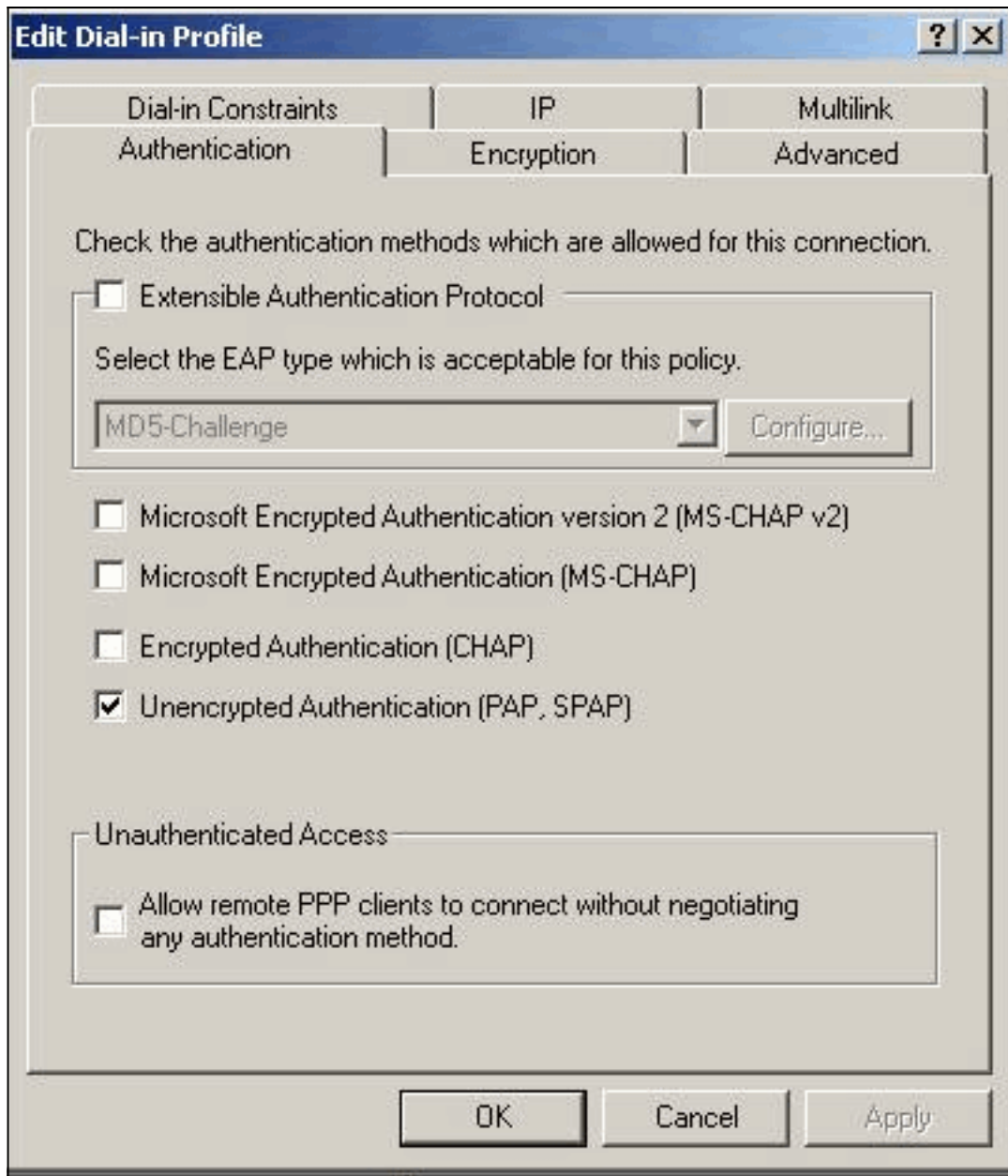
The image shows a screenshot of the 'VPN5000 Properties' dialog box. The 'Settings' tab is active. The 'Friendly name for client' field contains 'VPN5000'. The 'Client address' section has 'Address (IP or DNS):' set to '172.18.124.223' and a 'Verify...' button below it. The 'Client-Vendor' dropdown menu is set to 'Cisco'. There is an unchecked checkbox for 'Client must always send the signature attribute in the request'. The 'Shared secret' and 'Confirm shared secret' fields are both masked with asterisks. At the bottom, there are 'OK', 'Cancel', and 'Apply' buttons.

2. 在Remote access Policy的属性下，请选择**批准远程接入**在如果用户匹配条件部分下然后单击

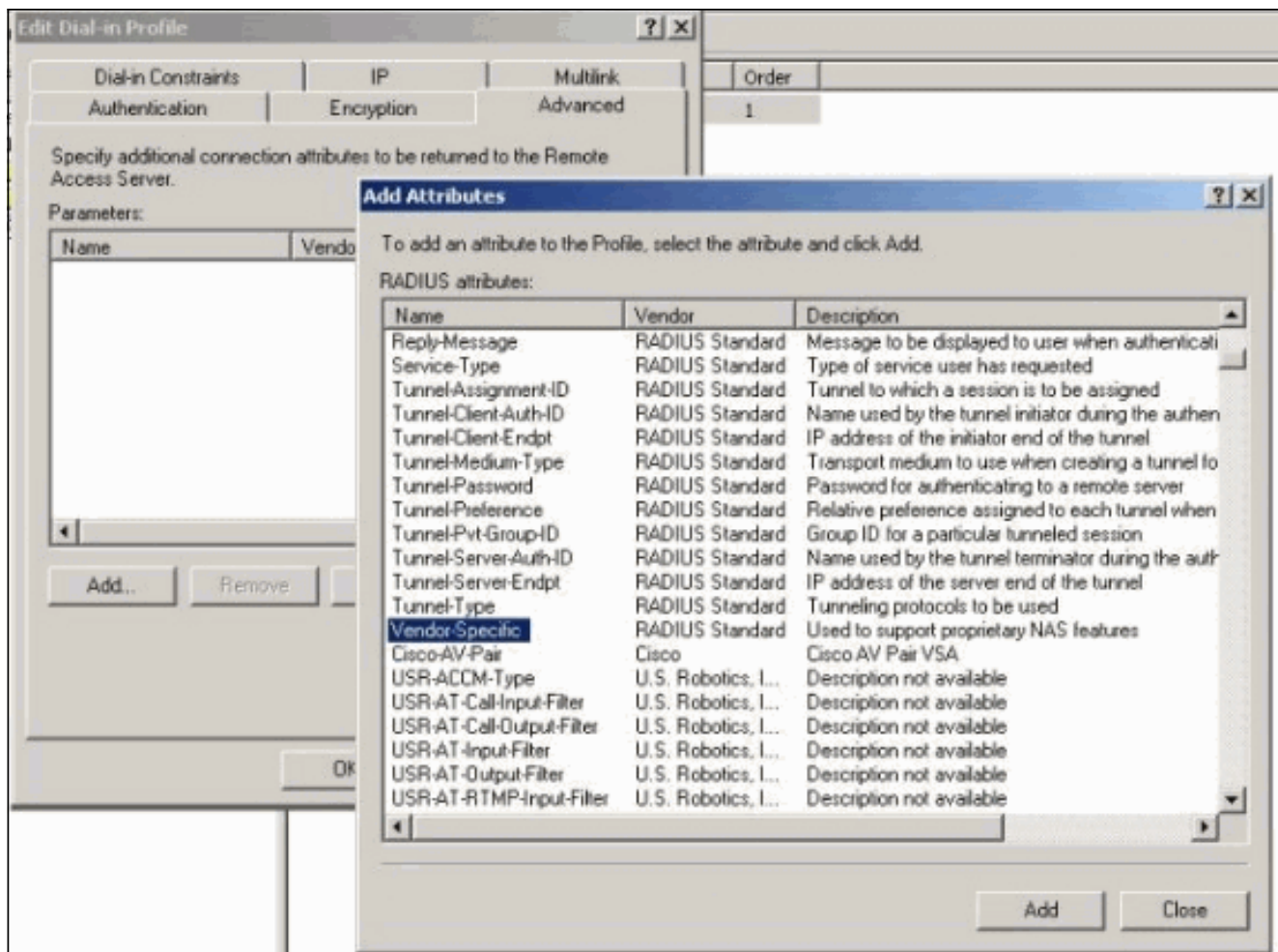


编辑配置文件。

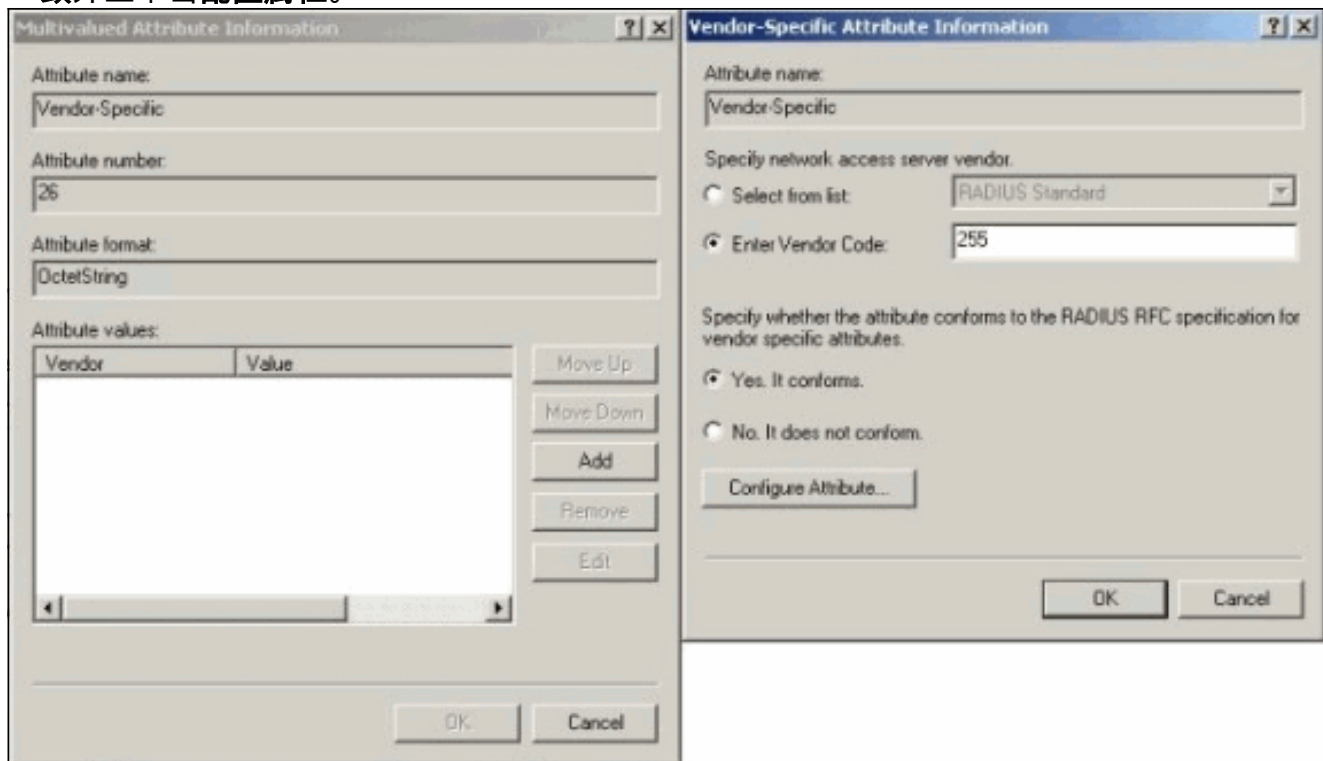
3. 点击Authentication选项并且保证仅该未加密的认证(PAP , SPAP)选择。



4. 选择高级选项卡。 ，单击添加并且选择根据厂商的。



5. 在供应商专用属性的Multivalued Attribute Information对话框下，请单击**添加**为了去供应商专用属性Information对话框。选择回车厂商代码并且输入**255**在相邻方框。其次，请选择**是**。它一致并且单击**配置属性**。



6. 在配置VSA (兼容的RFC)对话框下，为供应商赋值的属性编号请输入**4**，输入属性格式的字符串，并且进入**rtp-group** (VPN组的名称Cisco VPN 5000集中器的)属性值的。点击OK键并且重

Configure VSA (RFC compliant)

Vendor-assigned attribute number:
4

Attribute format:
String

Attribute value:
rtp-group

OK Cancel

复步骤5。

7. 在配置VSA (兼容的RFC)对话框下，为供应商赋值的属性编号请输入4，输入属性格式的字符串，并且进入cisco123 (客户端共享机密)属性值的。单击 Ok。

Configure VSA (RFC compliant)

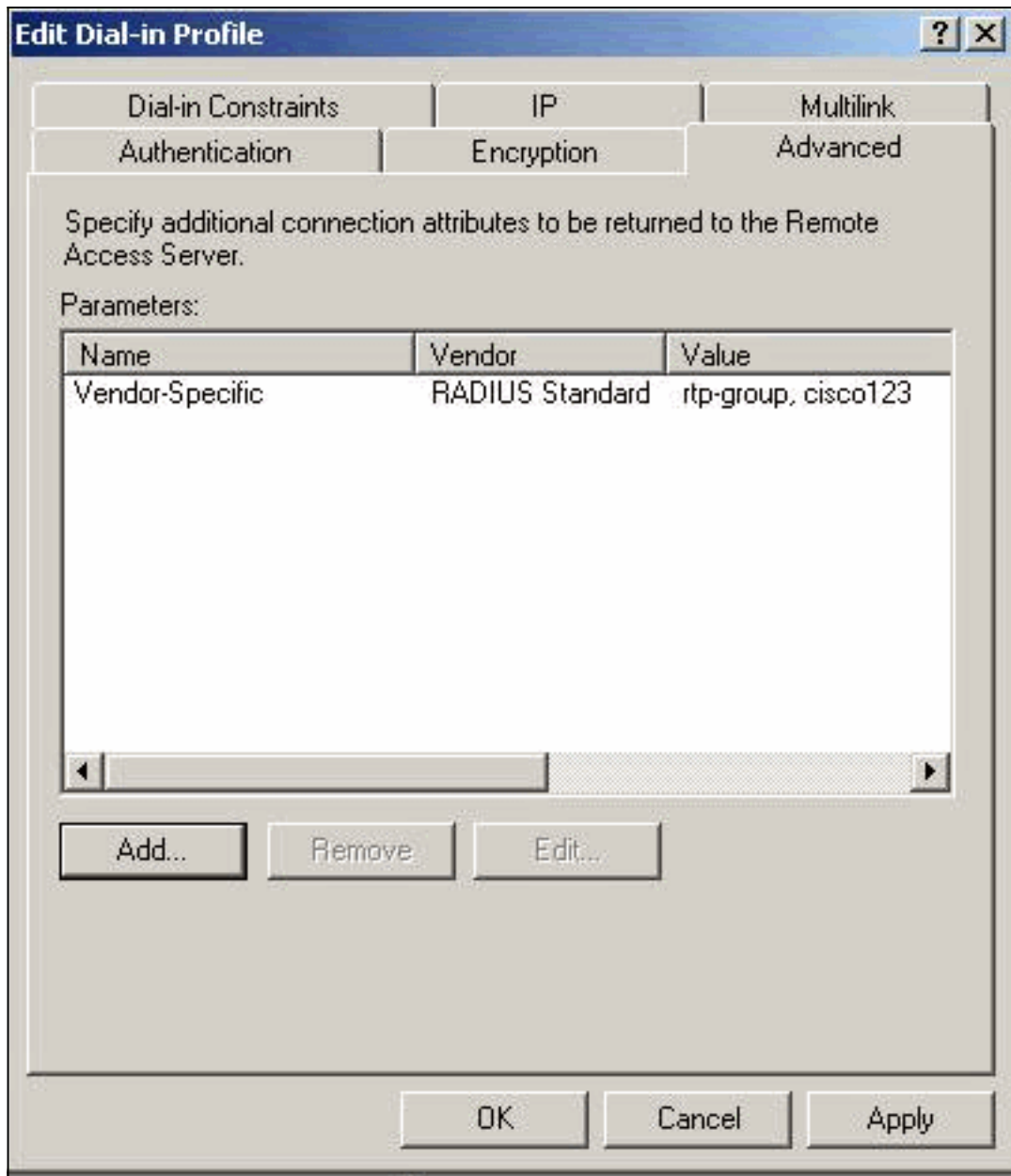
Vendor-assigned attribute number:
5

Attribute format:
String

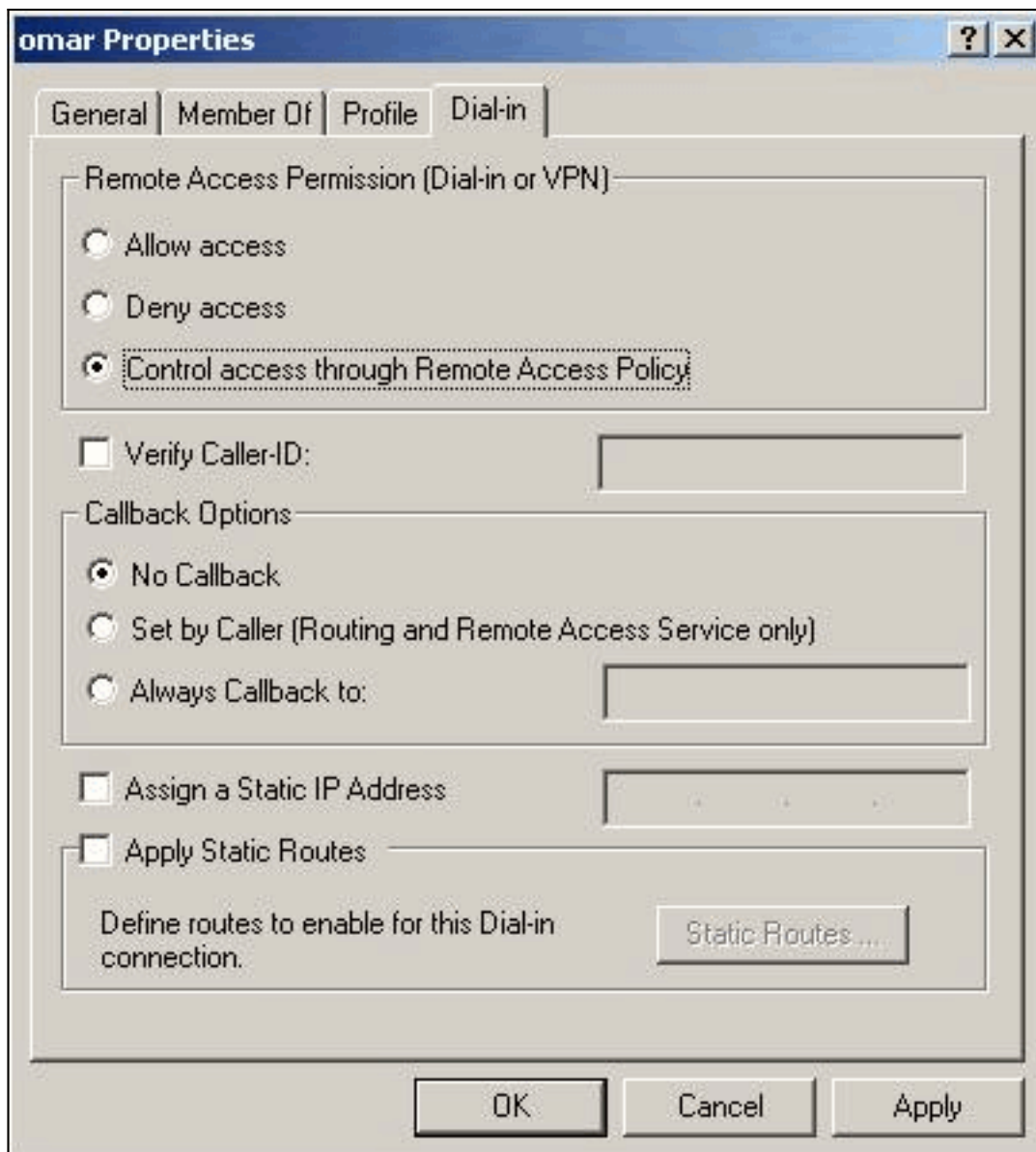
Attribute value:
cisco123

OK Cancel

8. 您看到供应商专用属性包含两个值(组和VPN密码)。



9. 在您的用户属性下，请点击Dial-in选项并且保证控制访问通过Remote access Policy选择。



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** 通信的统计显示信息包统计数据RADIUS部分和默认RADIUS服务器之间识别的VPN集中器。
- **show radius config** —显示RADIUS参数的当前设置。

这是输出**show radius statistics**命令。

```
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>

这是输出show radius config命令。

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

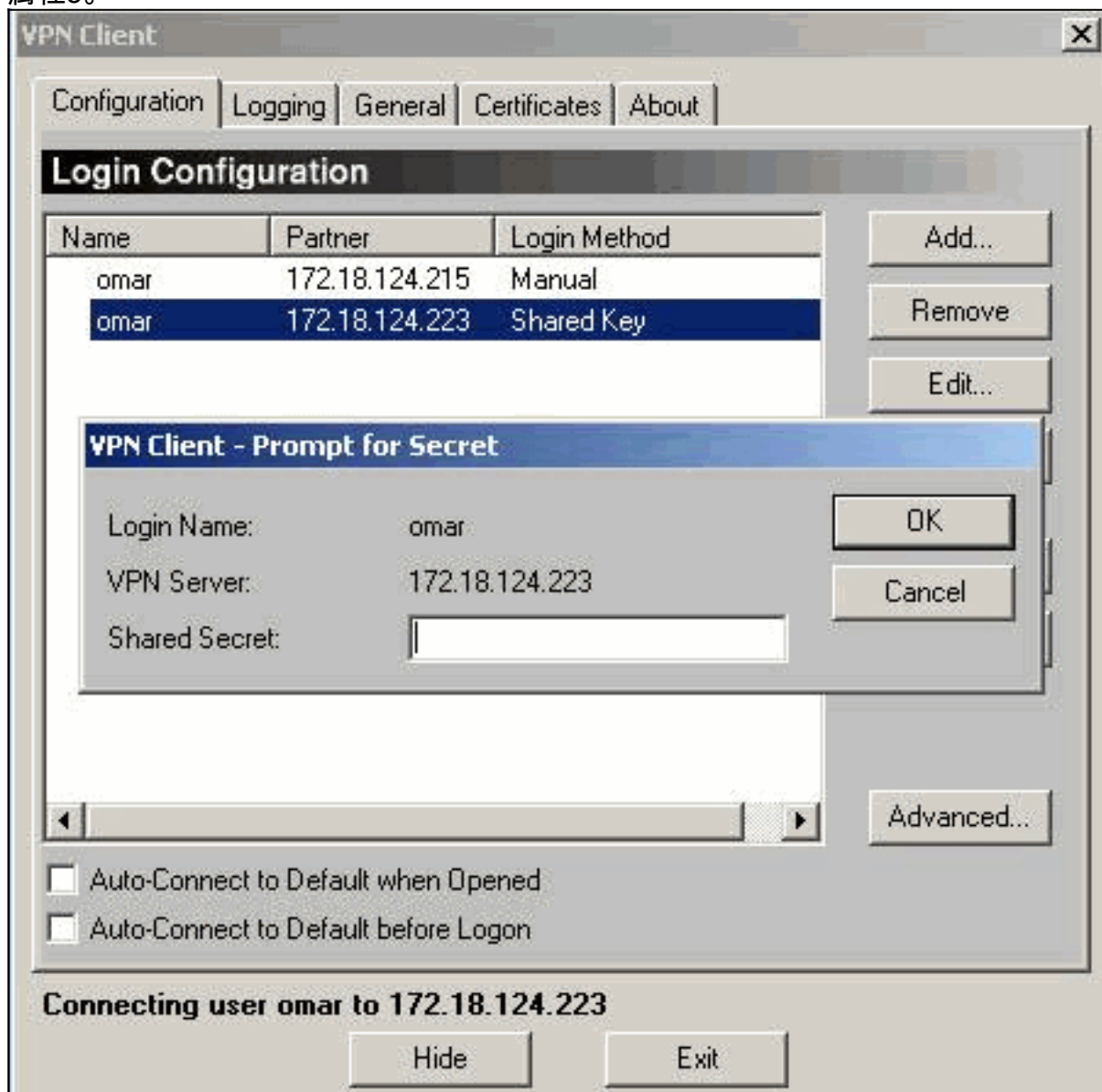
Authentication	Primary	Secondary
Requests	3	na
Accepts	3	na
Rejects	0	na
Challenges	0	na
Retransmissions	0	na
Bad Authenticators	0	na
Malformed Responses	0	na
Packets Dropped	0	na
Pending Requests	0	na
Timeouts	0	na
Unknown Types	0	na

VPN5001_4B9CBA80>

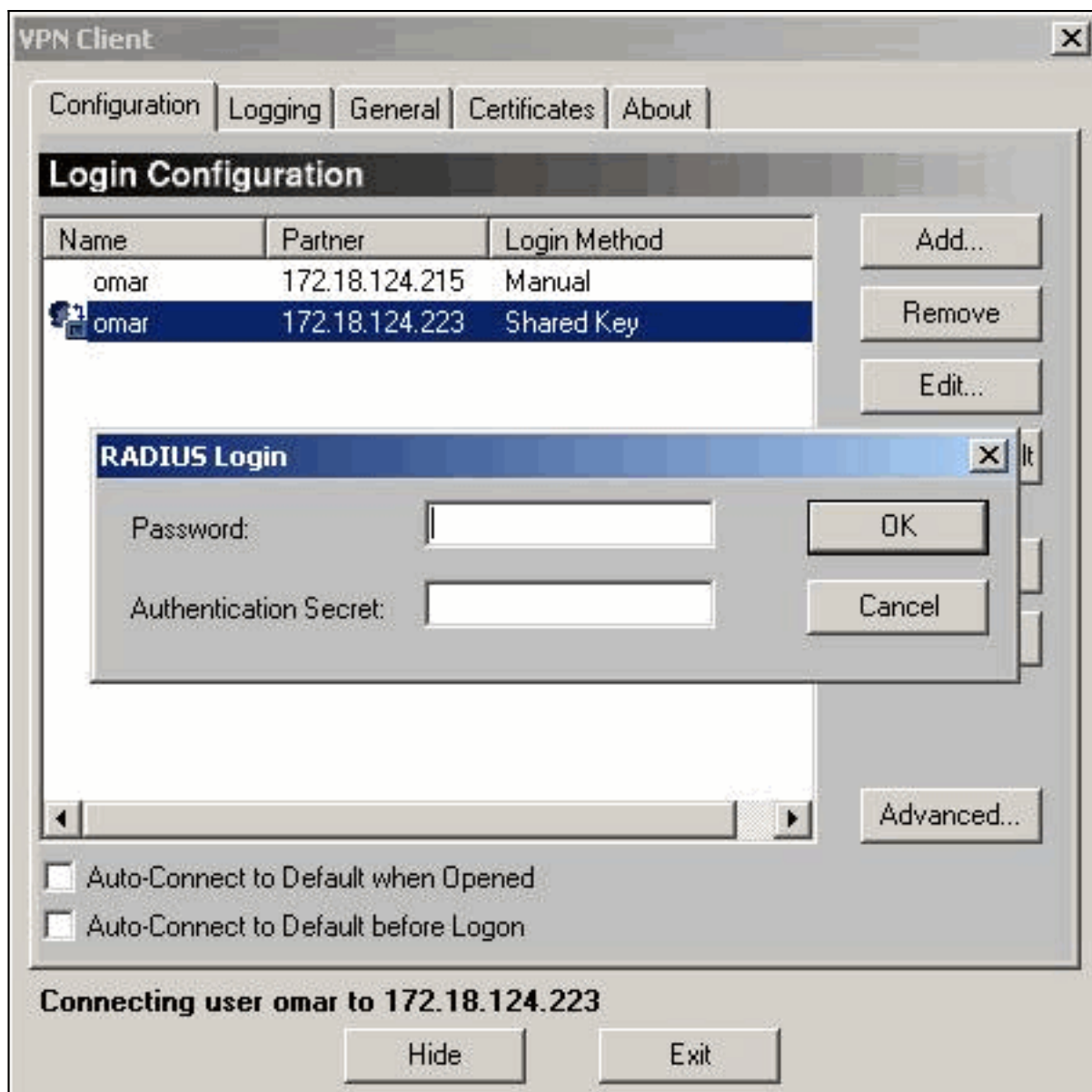
[配置 VPN 客户端](#)

此步骤指南您通过VPN客户端的配置。

1. 从VPN Client对话框，请选择Configuration选项。其次，从秘密对话框的VPN客户端提示，请输入共享机密在VPN服务器下。VPN客户端共享的机密是为VPN密码输入的值在VPN集中器的属性5。



2. 在您输入共享机密后，提示对于密码和验证密钥。密码是您的该用户的RADIUS密码，并且验证密钥是在VPN集中器的[RADIUS]部分的PAP认证机密。



[集中器日志](#)

```
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>

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](#)