為Microsoft Windows 2000 IAS RADIUS伺服器配置帶有外部身份驗證的Cisco VPN 5000集中器

目錄

簡介

本文檔介紹用於將帶有外部身份驗證的Cisco VPN 5000集中器配置為具有RADIUS的Microsoft Windows 2000 Internet身份驗證伺服器(IAS)的過程。

注意：質詢握手身份驗證協定(CHAP)不起作用。僅使用密碼驗證通訊協定(PAP)。 如需進一步的詳細資訊，請參閱Cisco錯誤ID CSCdt96941(僅限註冊客戶)。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據以下軟體版本：

- Cisco VPN 5000 Concentrator軟體版本6.0.16.0001

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

Cisco VPN 5000 Concentrator配置

VPN5001_4B9CBA80

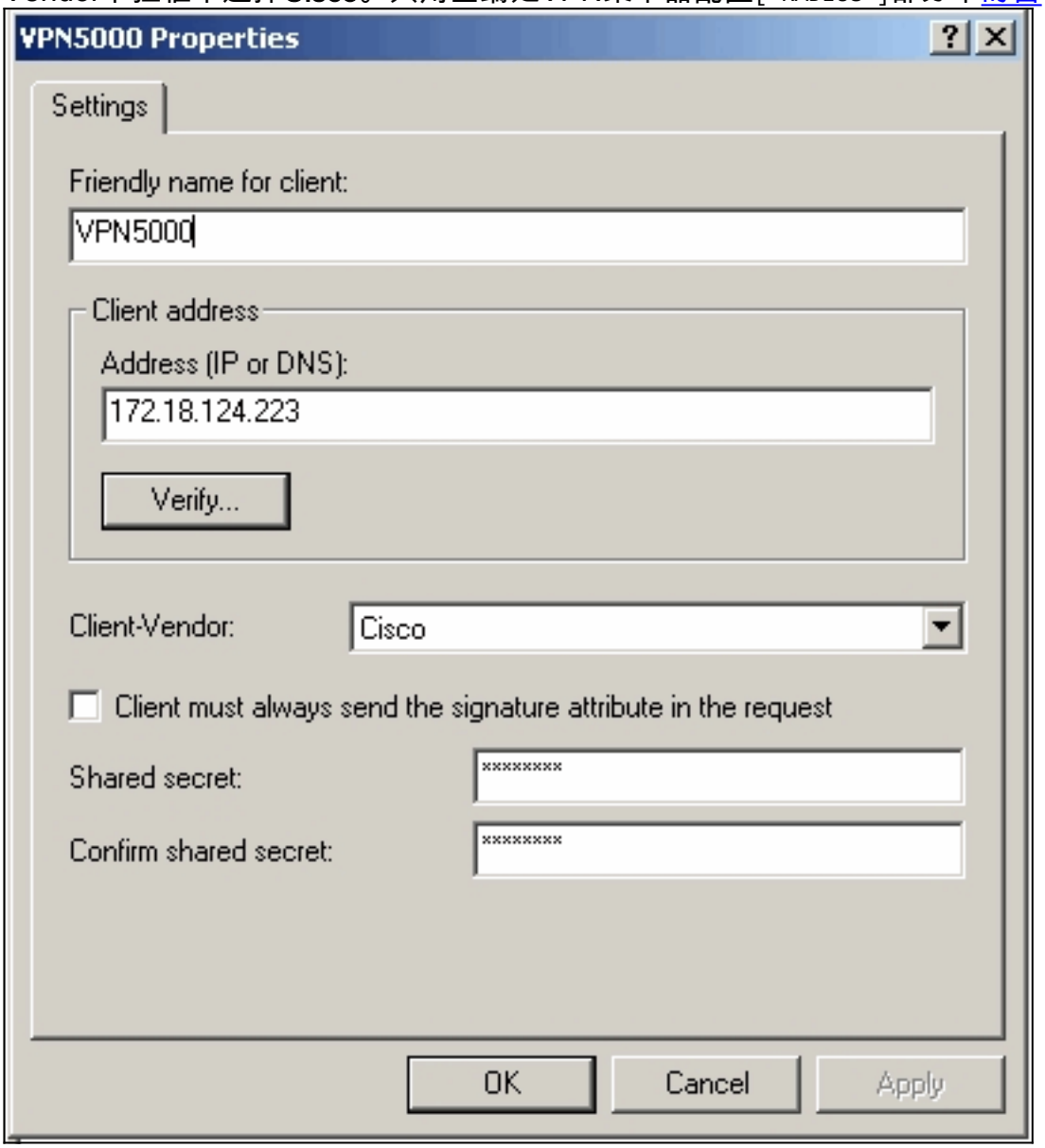
```
VPN5001_4B9CBA80> show config
Enter Password:

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伺服器

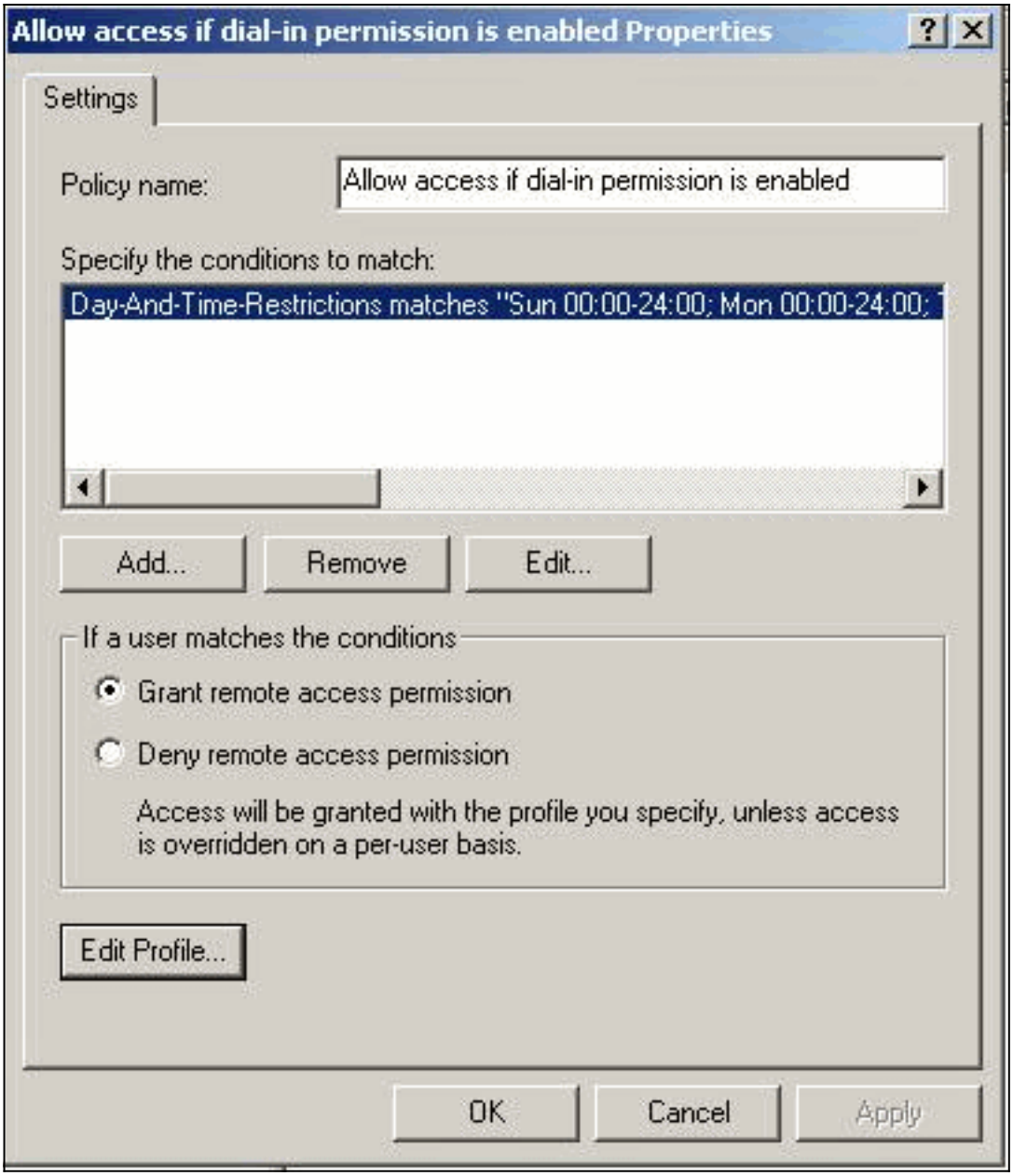
這些步驟將引導您完成簡單的Microsoft Windows 2000 IAS RADIUS伺服器配置。

1. 在Microsoft Windows 2000 IAS屬性下，選擇**Clients**並建立新客戶端。在此示例中，建立了一

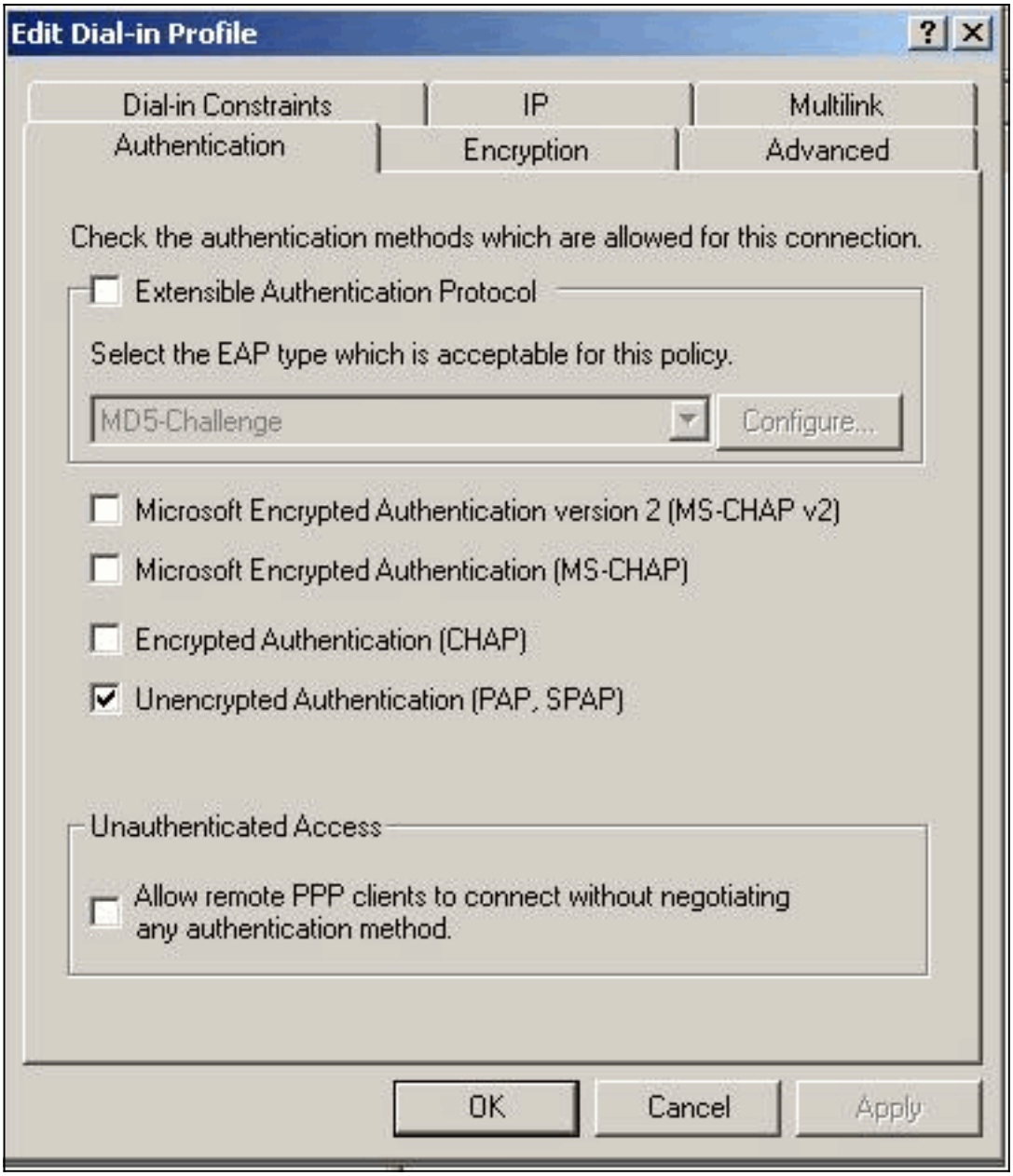
個名為VPN5000的條目。Cisco VPN 5000集中器的IP地址為172.18.124.223。在Client-Vendor下拉框中選擇**Cisco**。共用金鑰是VPN集中器配置[RADIUS]部分中的密碼。



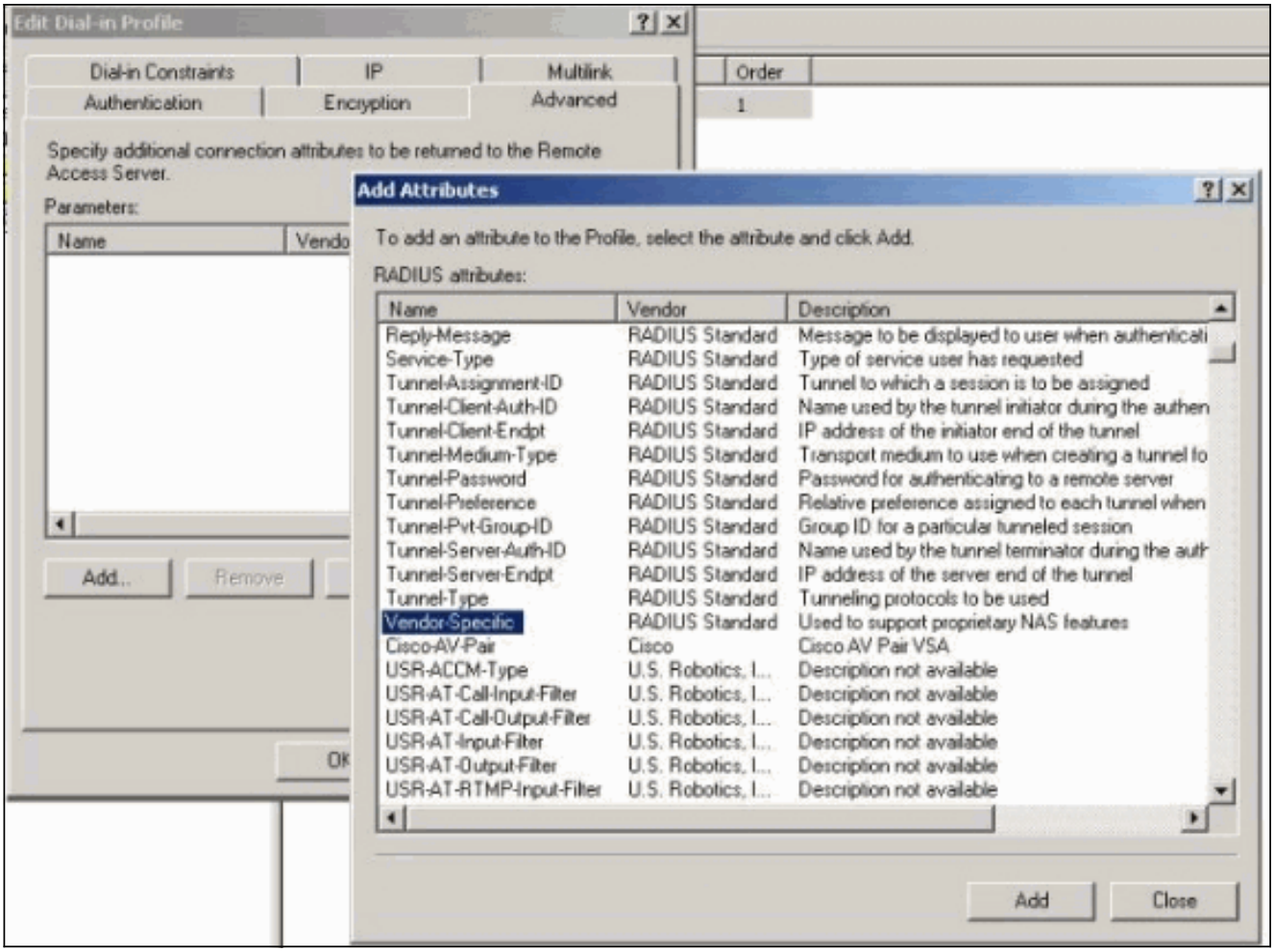
2. 在「遠端訪問策略」的屬性下，選擇「如果使用者匹配條件」部分下的**授予遠端訪問許可權**，然後按一下**編輯配置檔案**。



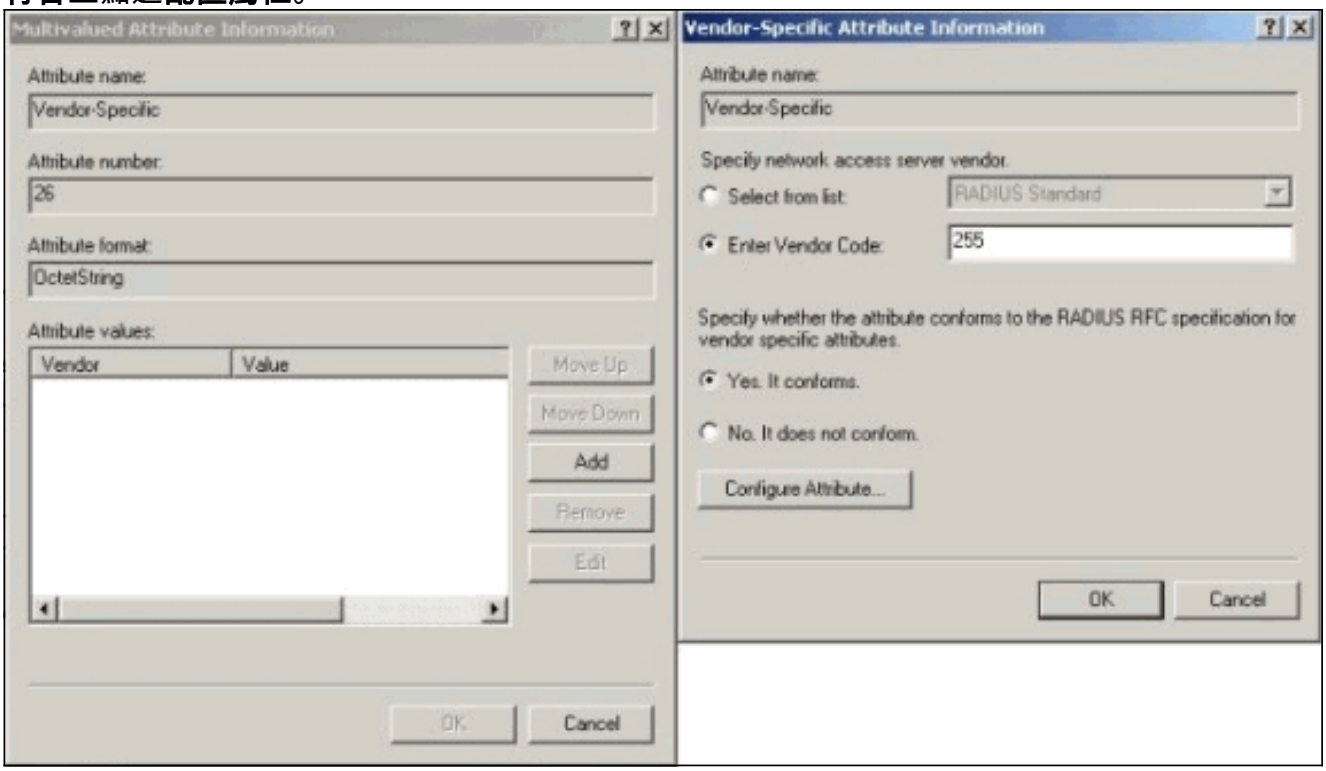
3. 按一下Authentication頁籤，並確保僅選中**Unencrypted Authentication(PAP， SPAP)**。



4. 選擇「高級」頁籤，按一下**Add**，然後選擇**Vendor-Specific**。

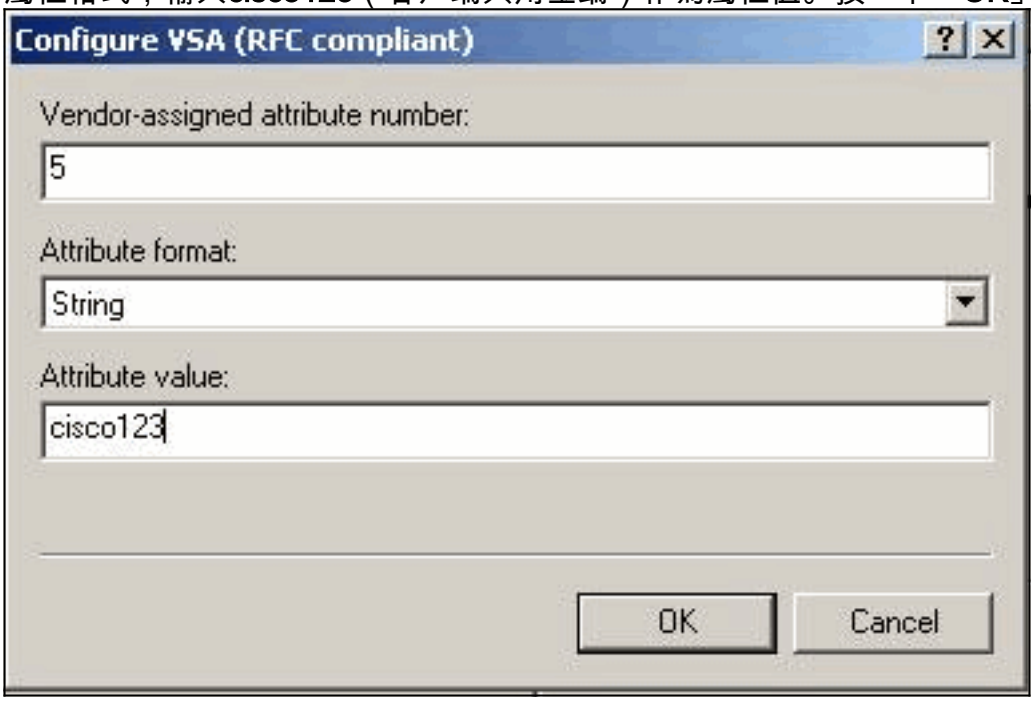


5. 在「供應商特定屬性」的「多值屬性資訊」對話方塊中，按一下**新增**以轉至「供應商特定屬性資訊」對話方塊。選擇**Enter Vendor Code**，然後在相鄰的框中輸入**255**。接下來，選擇**是。它符合**並點選**配置屬性**。

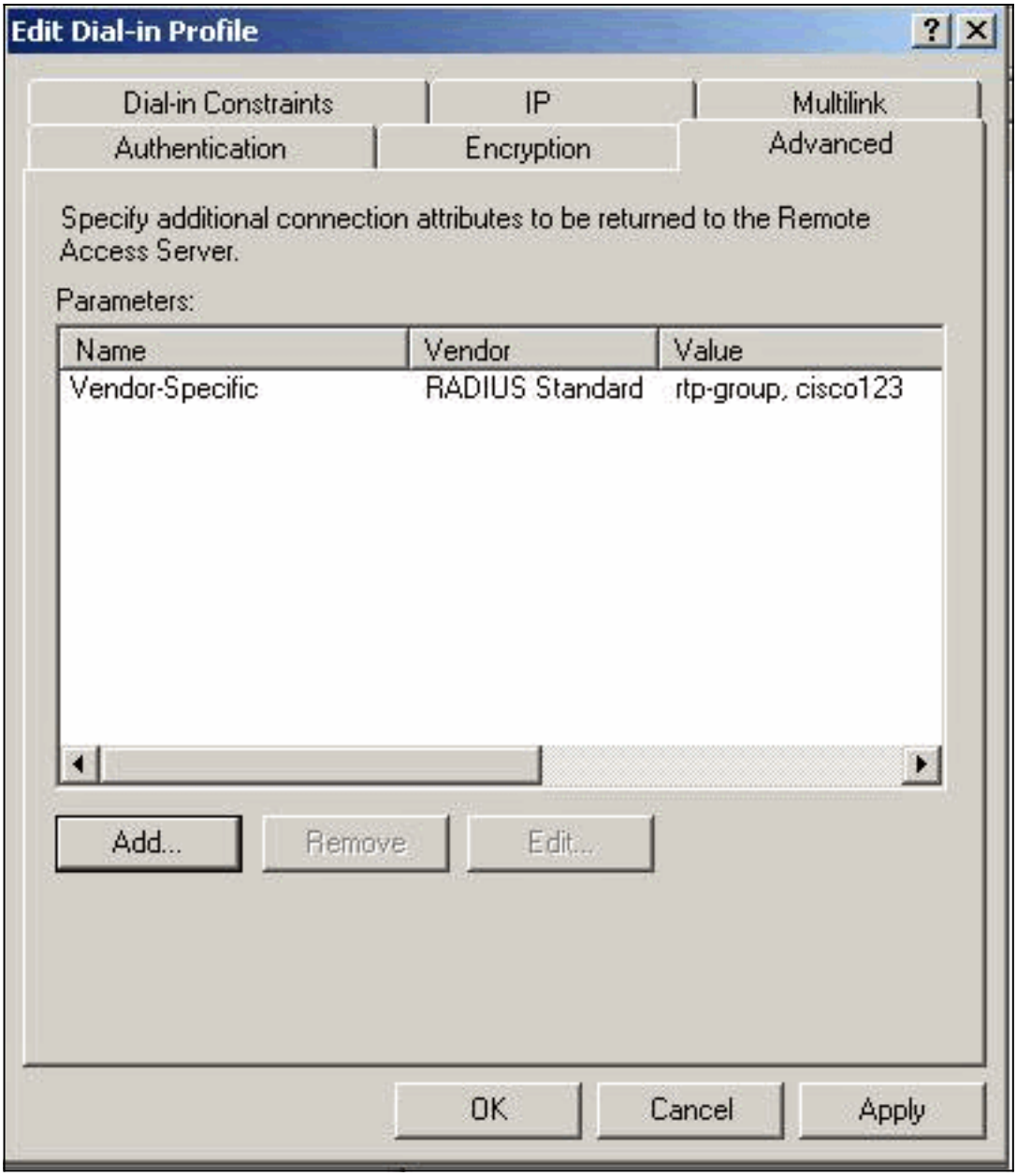


6. 在Configure VSA(RFC compliant)對話方塊中，輸入**4**作為供應商分配的屬性編號，輸入**String**作為屬性格式，輸入**rtp-group**（Cisco VPN 5000集中器中的VPN組的名稱）作為屬性值。按一下「**OK**」，然後重複步驟5。

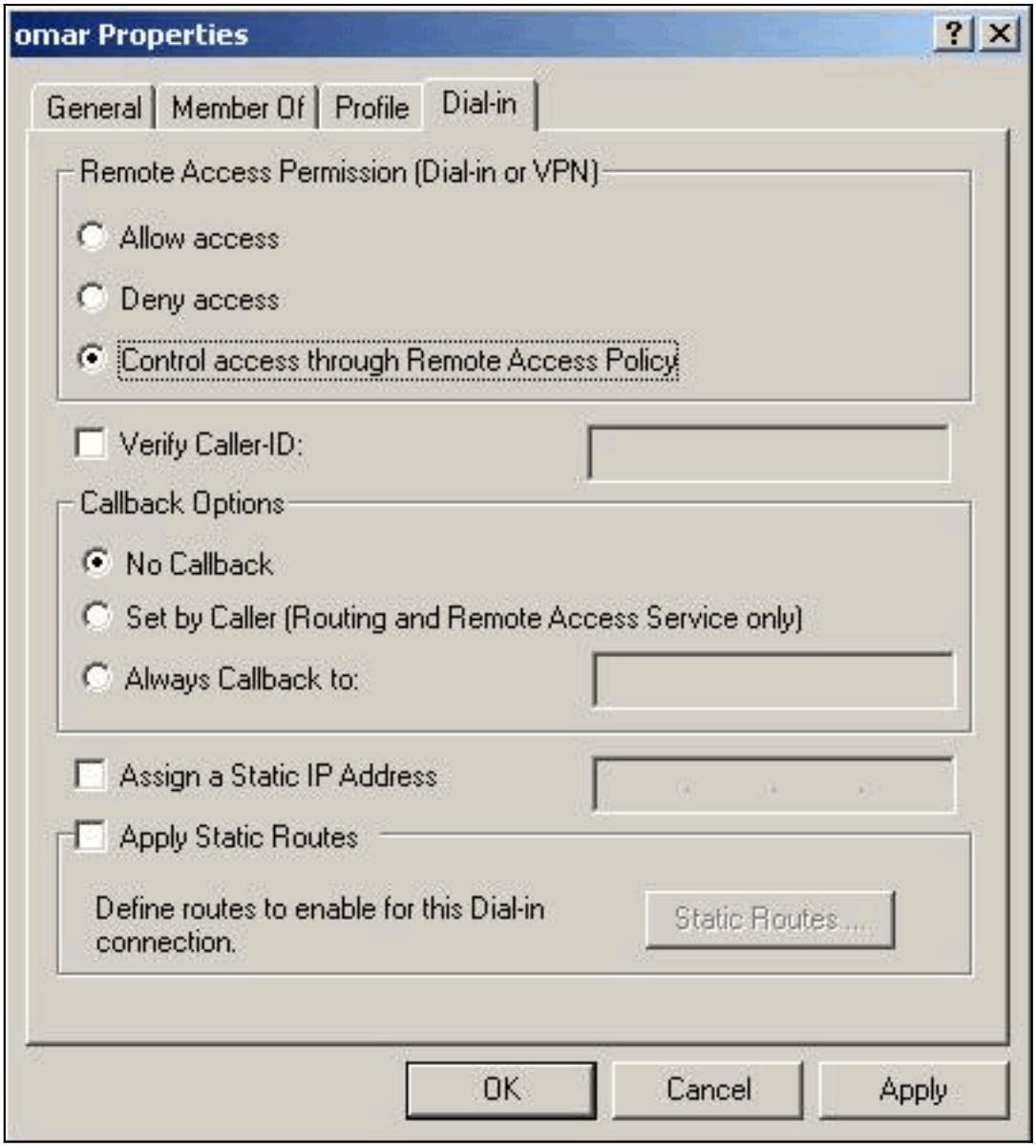
7. 在「配置VSA（符合RFC）」對話方塊中，輸入**4**作為供應商分配的屬性編號，輸入**String**作為屬性格式，輸入**cisco123**（客戶端共用金鑰）作為屬性值。按一下「**OK**」（確定）。



8. 您會看到「特定於供應商」屬性包含兩個值（組和VPN密碼）。



9. 在使用者屬性下，按一下「撥入」頁籤，並確保選中**Control access through Remote Access**



Policy。

驗證結果

本節提供的資訊可用於確認您的組態是否正常運作。

輸出直譯器工具(僅供註冊客戶使用)支援某些**show**命令，此工具可讓您檢視show命令輸出的分析。

- **show radius statistics** — 顯示VPN集中器與RADIUS部分識別的預設RADIUS伺服器之間通訊的資料包統計資訊。
- **show radius config** — 顯示RADIUS引數的當前設定。

以下是**show radius statistics**命令的輸出。

```
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>
```

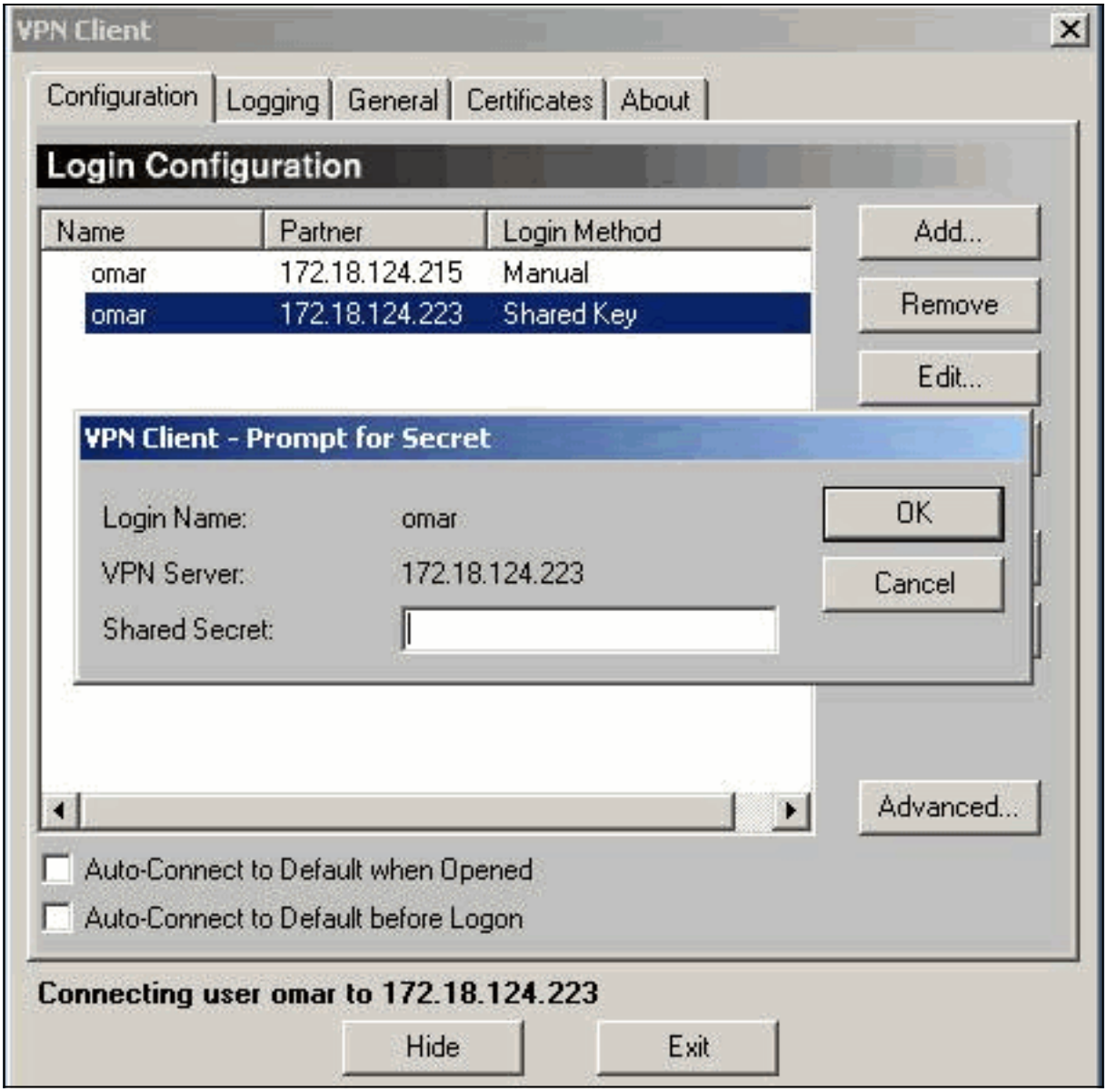
以下是**show radius config**命令的輸出。

```
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
```

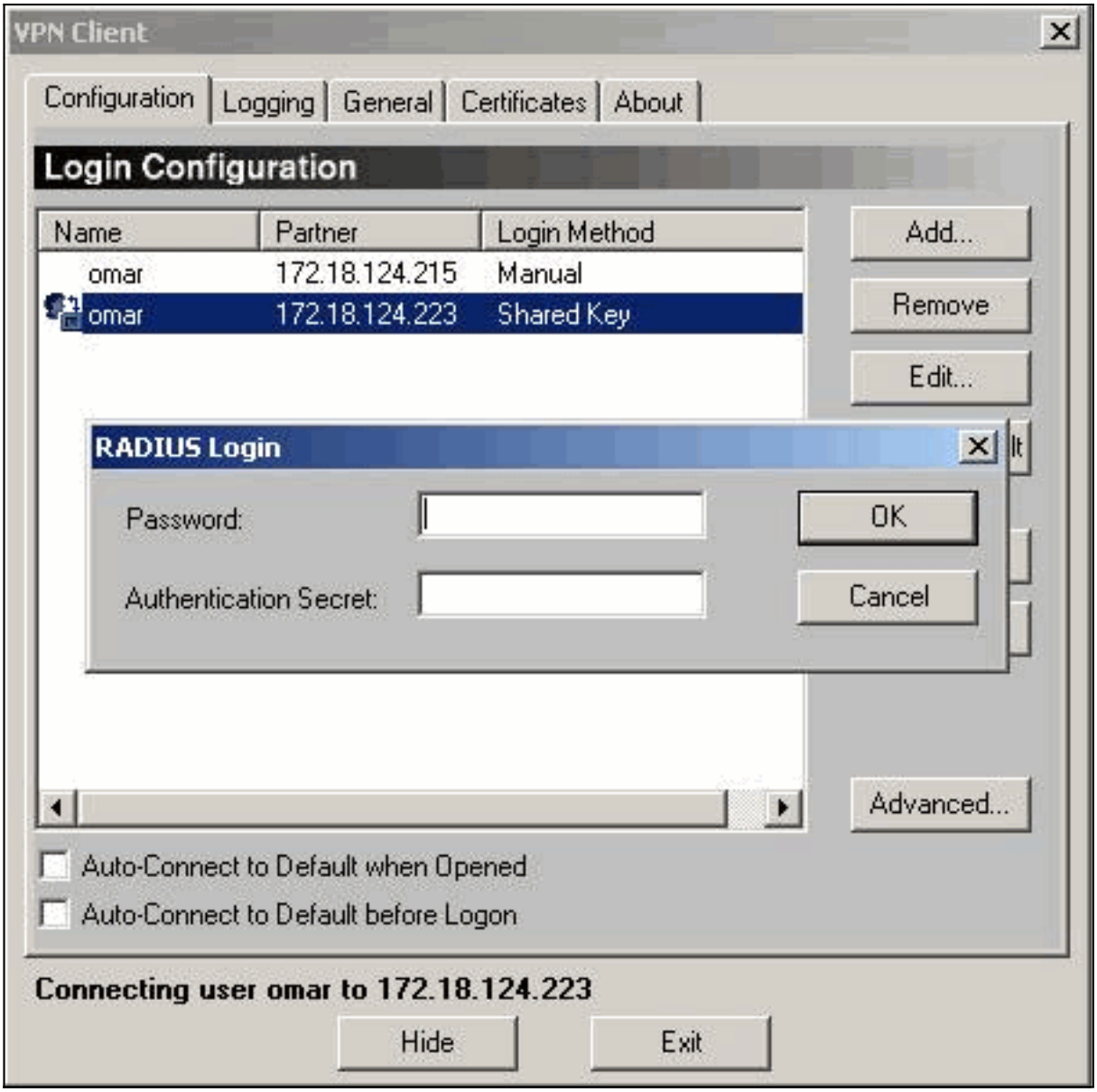
配置VPN客戶端

此過程將指導您完成VPN客戶端的配置。

1. 從VPN Client對話方塊中，選擇Configuration頁籤。接下來，在VPN Client-Prompt for Secret對話方塊中，在VPN Server下輸入共用金鑰。VPN客戶端共用金鑰是在VPN集中器中為屬性5的VPN密碼輸入的值。



2. 輸入共用金鑰後，系統將提示您輸入口令和身份驗證金鑰。密碼是該使用者的RADIUS密碼，而身份驗證金鑰是VPN集中器[RADIUS]的PAP身份驗證金鑰。



集中器日誌

```
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
```

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- Cisco VPN 5000系列集中器銷售終止公告
- Cisco VPN 5000集中器支援頁

- Cisco VPN 5000使用者端支援頁面
- IPSec支援頁面
- 技術支援 - Cisco Systems