Konfigurieren eines Cisco VPN 500 Concentrator mit externer Authentifizierung für einen Microsoft Windows 2000 IAS RADIUS Server

Inhalt

Einführung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Konventionen
Konfiguration des Cisco VPN 5000 Concentrator
Konfigurieren des Microsoft Windows 2000 IAS RADIUS-Servers
Überprüfen des Ergebnisses
Konfigurieren des VPN-Clients
Concentrator-Protokolle
Fehlerbehebung
Zugehörige Informationen

Einführung

In diesem Dokument werden die Verfahren beschrieben, die zum Konfigurieren eines Cisco VPN 500 Concentrator mit externer Authentifizierung für einen Microsoft Windows 2000 Internet Authentication Server (IAS) mit RADIUS verwendet werden.

Hinweis: CHAP (Challenge Handshake Authentication Protocol) funktioniert nicht. Verwenden Sie ausschließlich das Password Authentication Protocol (PAP). Weitere Informationen finden Sie unter Cisco Bug ID CSCdt96941 (nur registrierte Kunden).

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf dieser Softwareversion:

- Cisco VPN 5000 Concentrator Software Version 6.0.16.0001

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten

Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

Konfiguration des Cisco VPN 5000 Concentrator

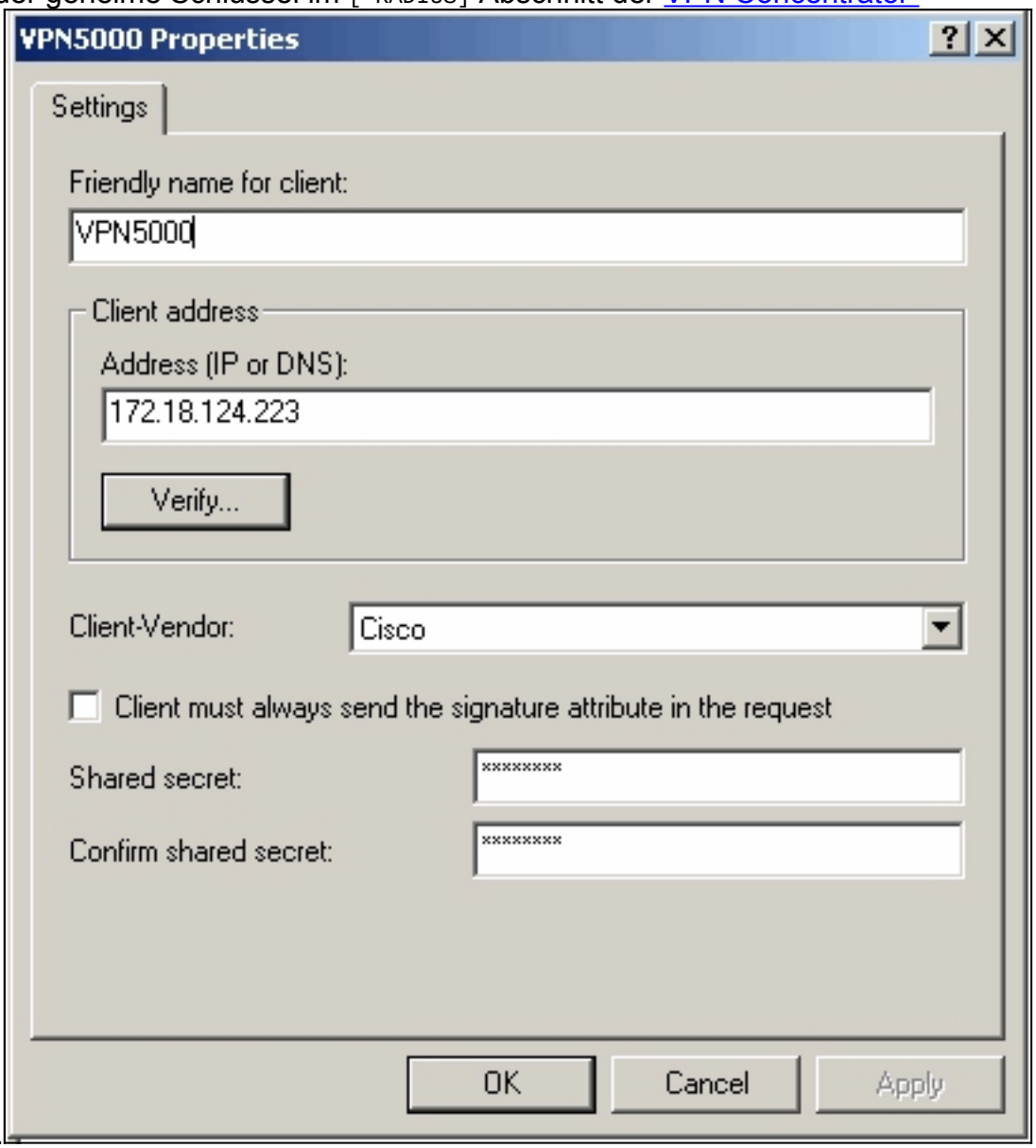
VPN5001_4B9CBA80

```
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#
```

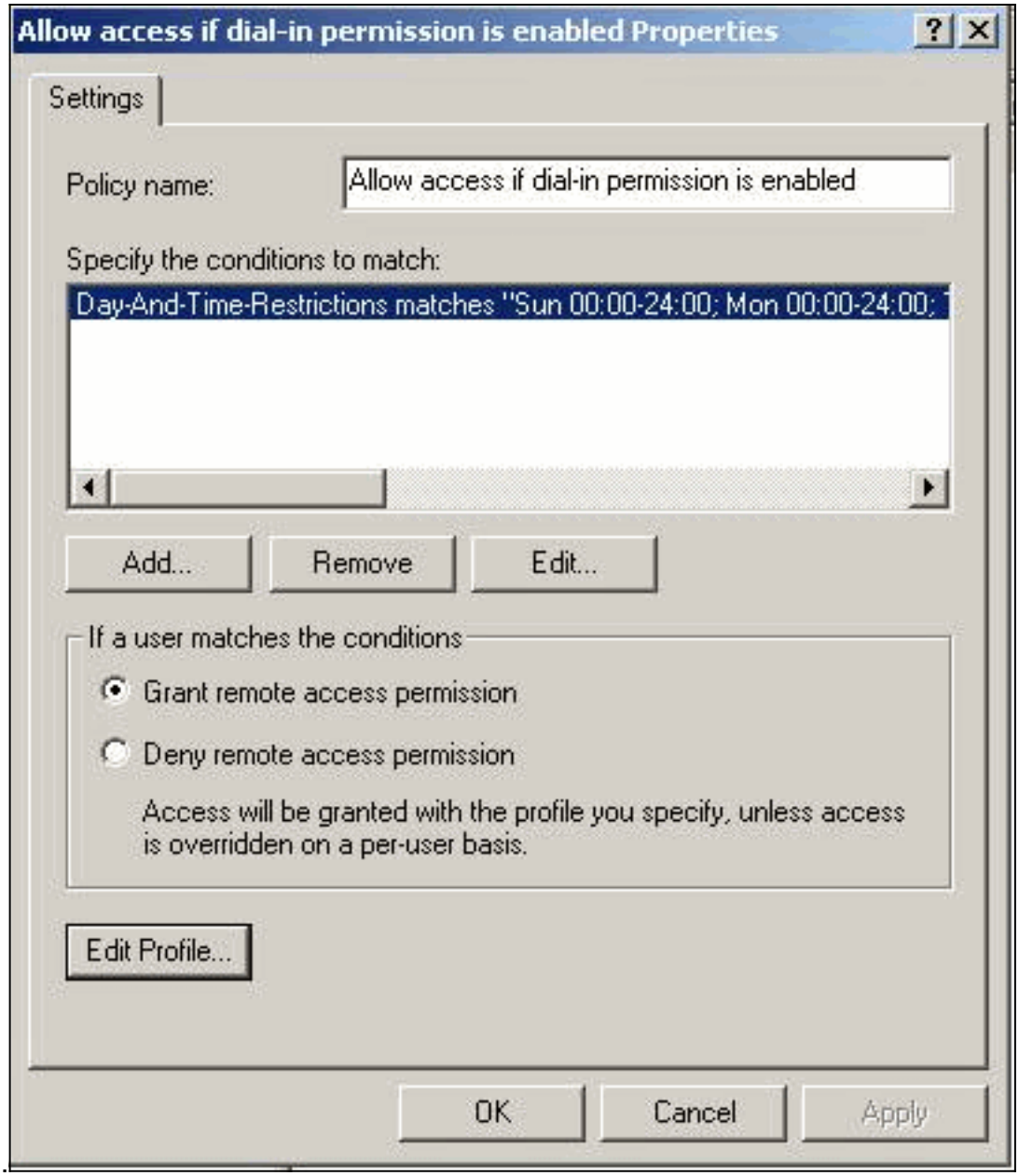
Konfigurieren des Microsoft Windows 2000 IAS RADIUS-Servers

Diese Schritte führen Sie durch eine einfache RADIUS-Serverkonfiguration in Microsoft Windows 2000 IAS.

1. Wählen Sie unter den Microsoft Windows 2000 IAS-Eigenschaften **Clients aus**, und erstellen Sie einen neuen Client.In diesem Beispiel wird ein Eintrag mit dem Namen VPN5000 erstellt. Die IP-Adresse des Cisco VPN 500 Concentrator lautet 172.18.124.223. Wählen Sie im Dropdown-Feld Client-Anbieter die Option **Cisco aus**. Der gemeinsam genutzte geheime Schlüssel ist der geheime Schlüssel im `[ RADIUS]` Abschnitt der VPN Concentrator-Konfiguration.

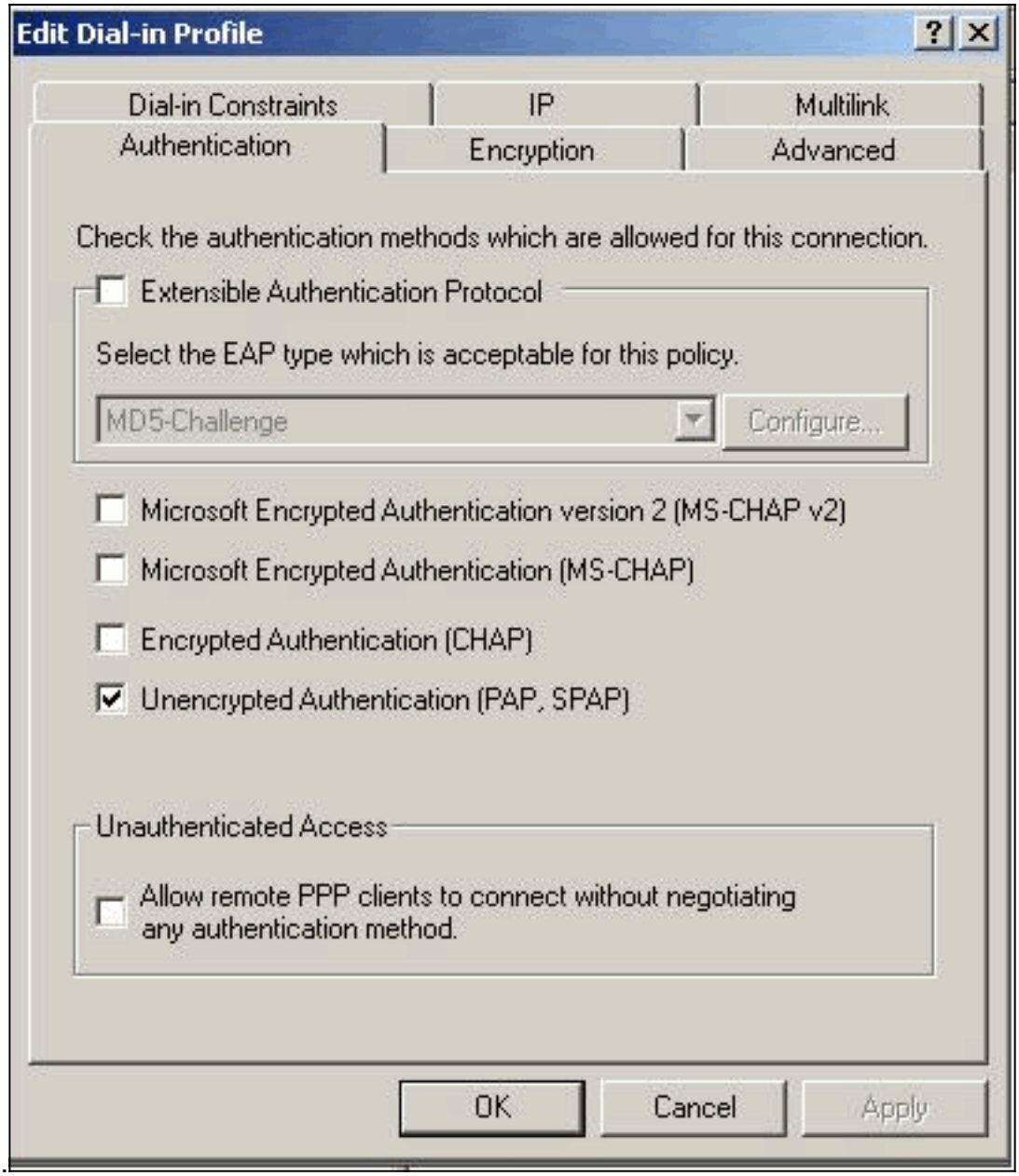


2. Wählen Sie unter den Eigenschaften der Remote-Zugriffsrichtlinie im Abschnitt "Wenn ein Benutzer die Bedingungen erfüllt" die Option **Remotezugriffsberechtigung erteilen aus**, und klicken Sie dann auf **Profil**



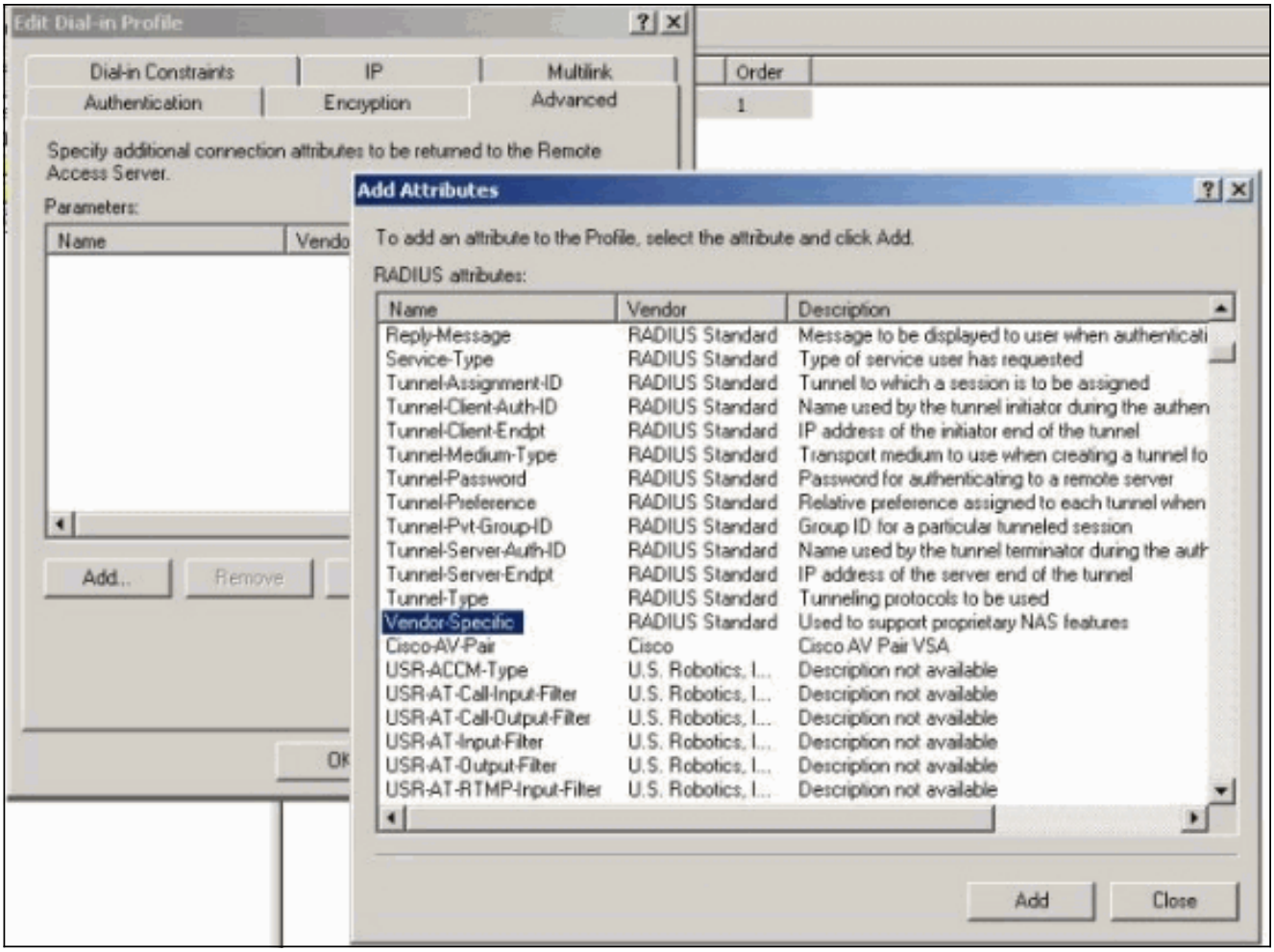
bearbeiten.

3. Klicken Sie auf die Registerkarte Authentifizierung, und stellen Sie sicher, dass nur **unverschlüsselte Authentifizierung (PAP, SPAP)** ausgewählt

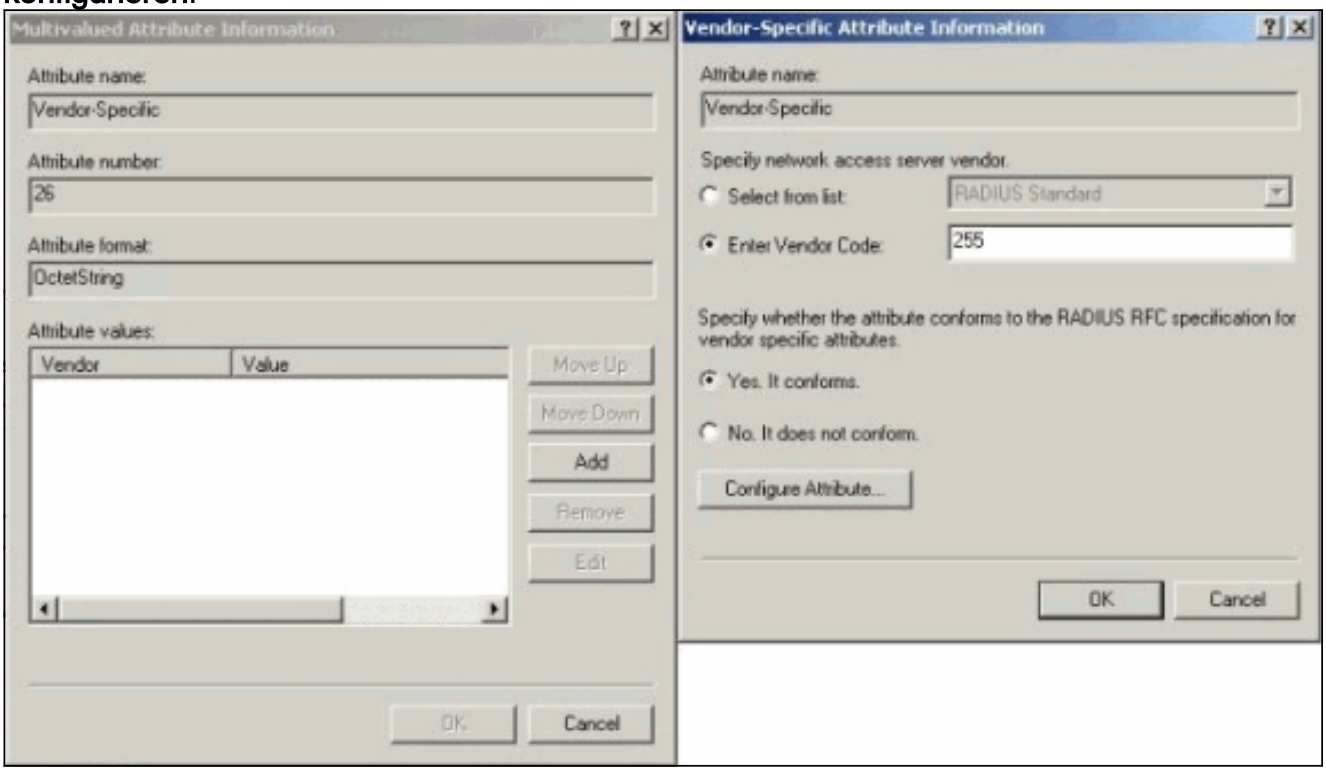


ist.

4. Wählen Sie die Registerkarte Erweitert aus, klicken Sie auf **Hinzufügen**, und wählen Sie **Anbieterspezifisch aus**.



5. Klicken Sie im Dialogfeld Mehrwertige Attributinformationen für das anbieterspezifische Attribut auf **Hinzufügen**, um zum Dialogfeld Herstellerspezifische Attributinformationen zu gelangen. Wählen Sie **Anbietercode eingeben** und geben Sie **255** in das angrenzende Feld ein. Wählen Sie anschließend **Ja aus. Es entspricht** und klickt auf **Attribut konfigurieren**.



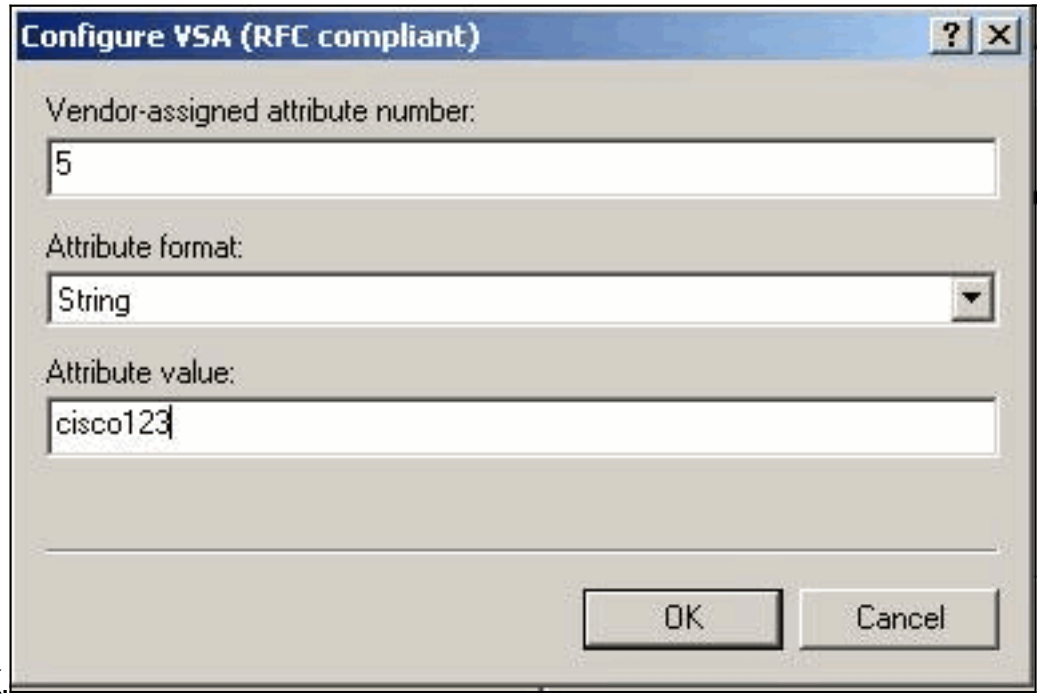
6. Geben Sie im Dialogfeld Configure VSA (RFC-konform) (VSA konfigurieren) **4** für die vom Anbieter zugewiesene Attributnummer ein, geben Sie **String** für das Attributformat ein, und

geben Sie **rtp-group** (Name der VPN-Gruppe im Cisco VPN 5000 Concentrator) für den Attributwert ein. Klicken Sie auf **OK**, und wiederholen Sie Schritt

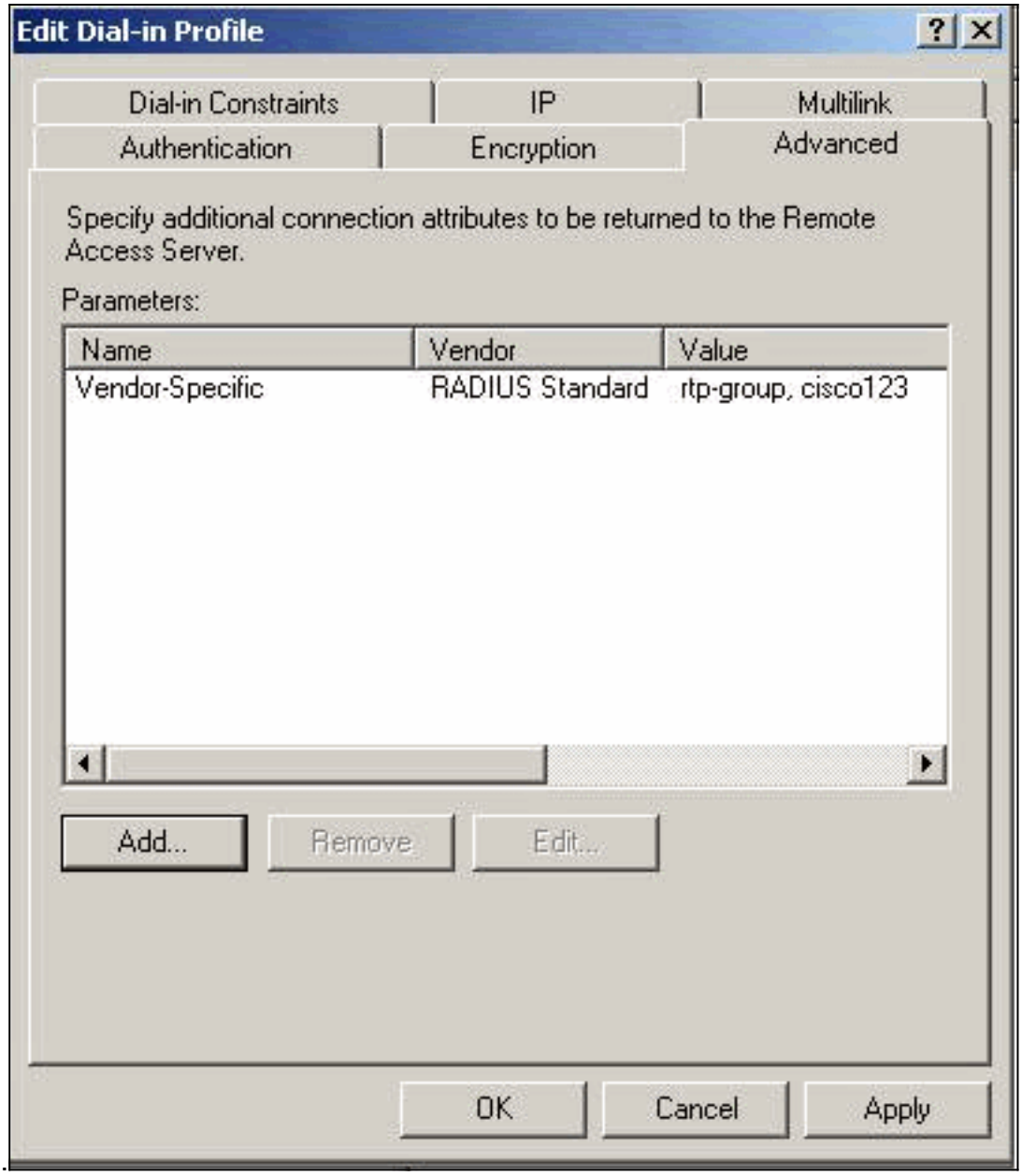
5.

7. Geben Sie im Dialogfeld Configure VSA (RFC-kompatibel) (VSA konfigurieren) (RFC-kompatibel) **4** für die vom Anbieter zugewiesene Attributnummer ein, geben Sie **String** für das Attributformat ein, und geben Sie **cisco123** (den Client Shared geheim) für den Attributwert ein. Klicken Sie auf

OK.

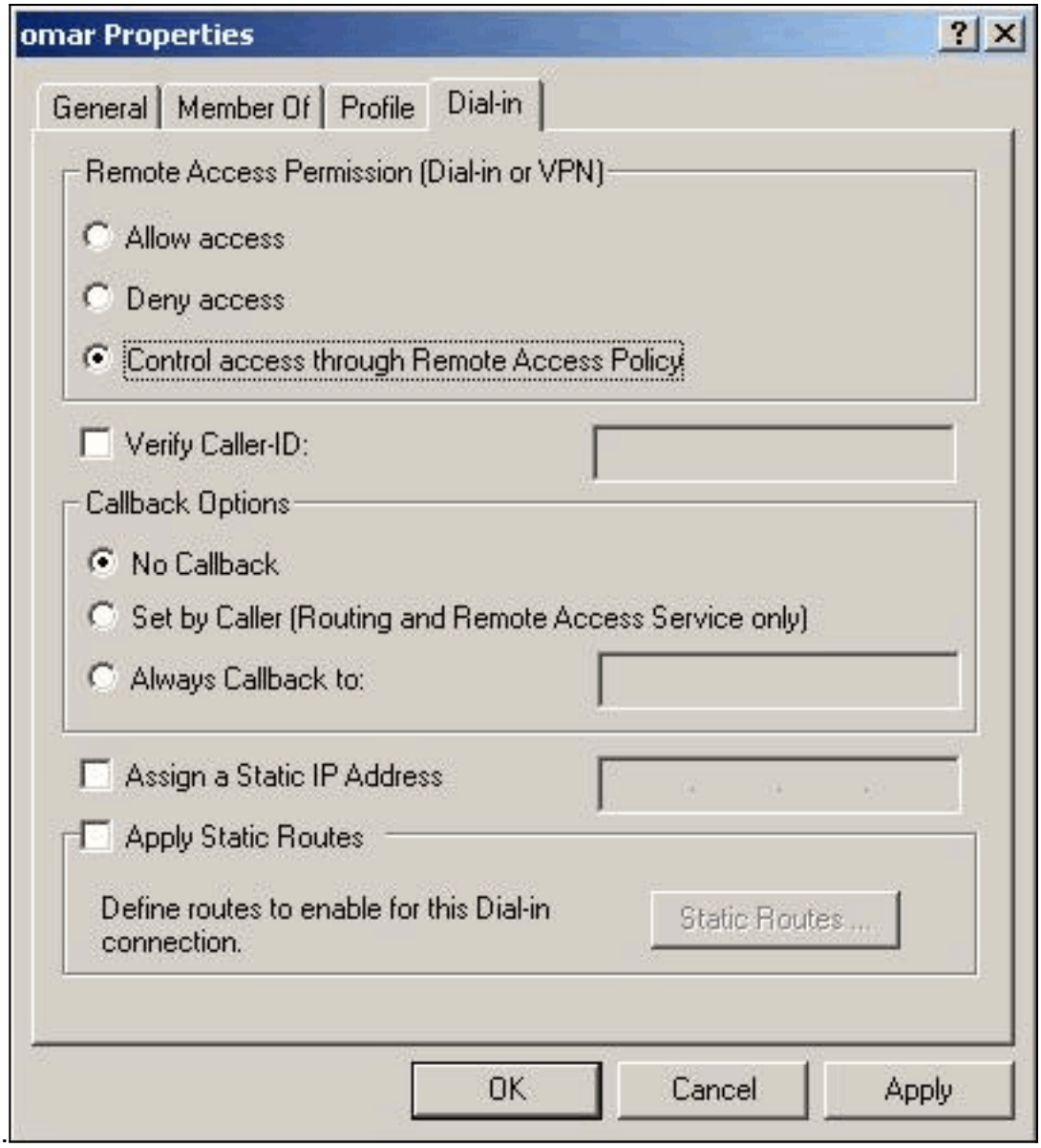


8. Sie sehen, dass das anbieterspezifische Attribut zwei Werte enthält (Gruppen- und VPN-



Kennwort).

9. Klicken Sie unter den Benutzereigenschaften auf die Registerkarte Einwählen, und stellen Sie sicher, dass die Option **Zugriffssteuerung über Remote-Zugriffsrichtlinie** ausgewählt



ist.

Überprüfen des Ergebnisses

Dieser Abschnitt enthält Informationen, die Sie verwenden können, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Bestimmte **show**-Befehle werden vom Output Interpreter Tool unterstützt (nur registrierte Kunden), mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

- **show radius statistics** - Zeigt Paketstatistiken für die Kommunikation zwischen dem VPN Concentrator und dem im RADIUS-Abschnitt identifizierten RADIUS-Standardserver an.
- **show radius config** - Zeigt die aktuellen Einstellungen für RADIUS-Parameter an.

Dies ist die Ausgabe des Befehls **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>
```

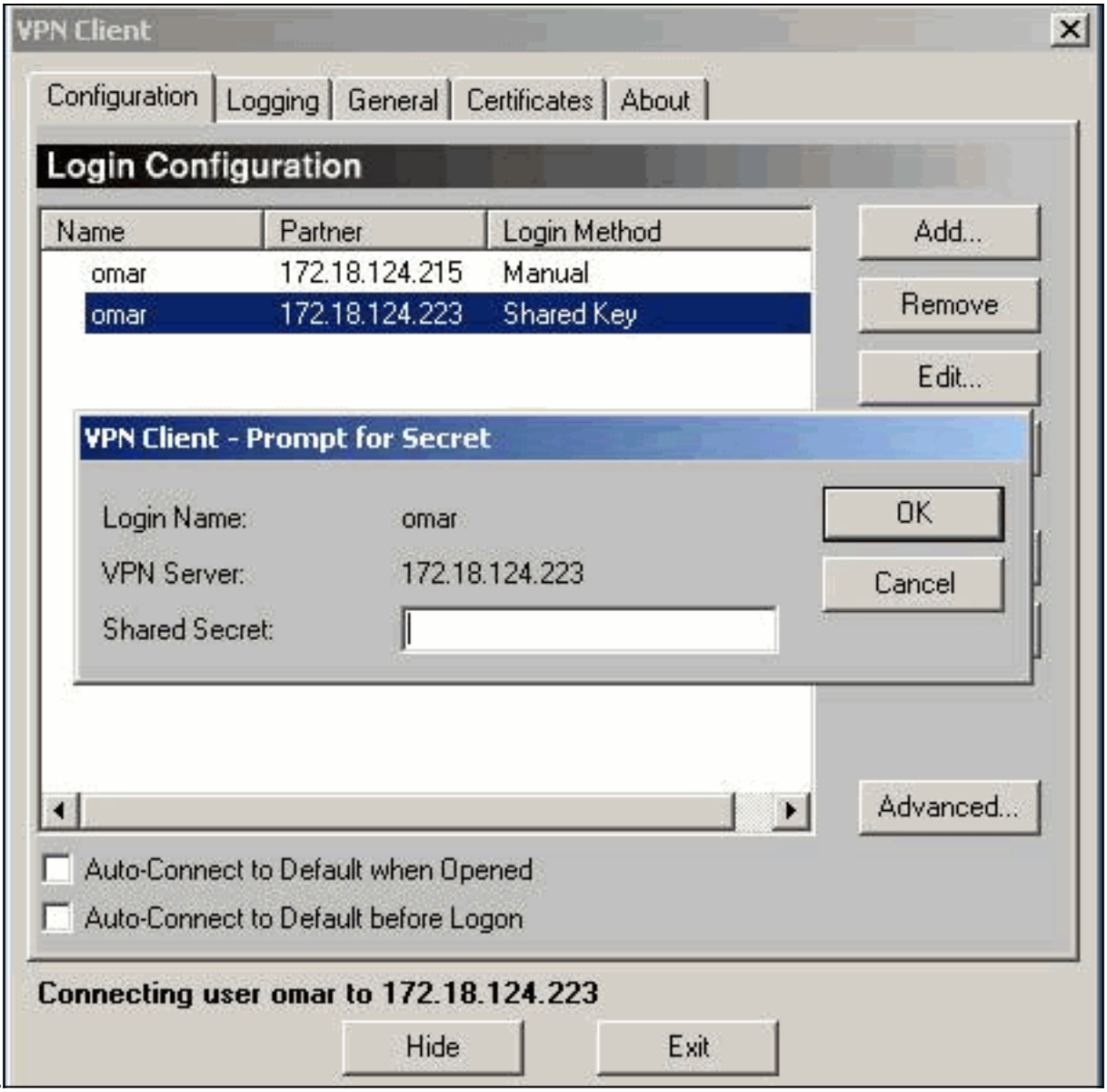
Dies ist die Ausgabe des Befehls **show radius config**.

```
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
```

Konfigurieren des VPN-Clients

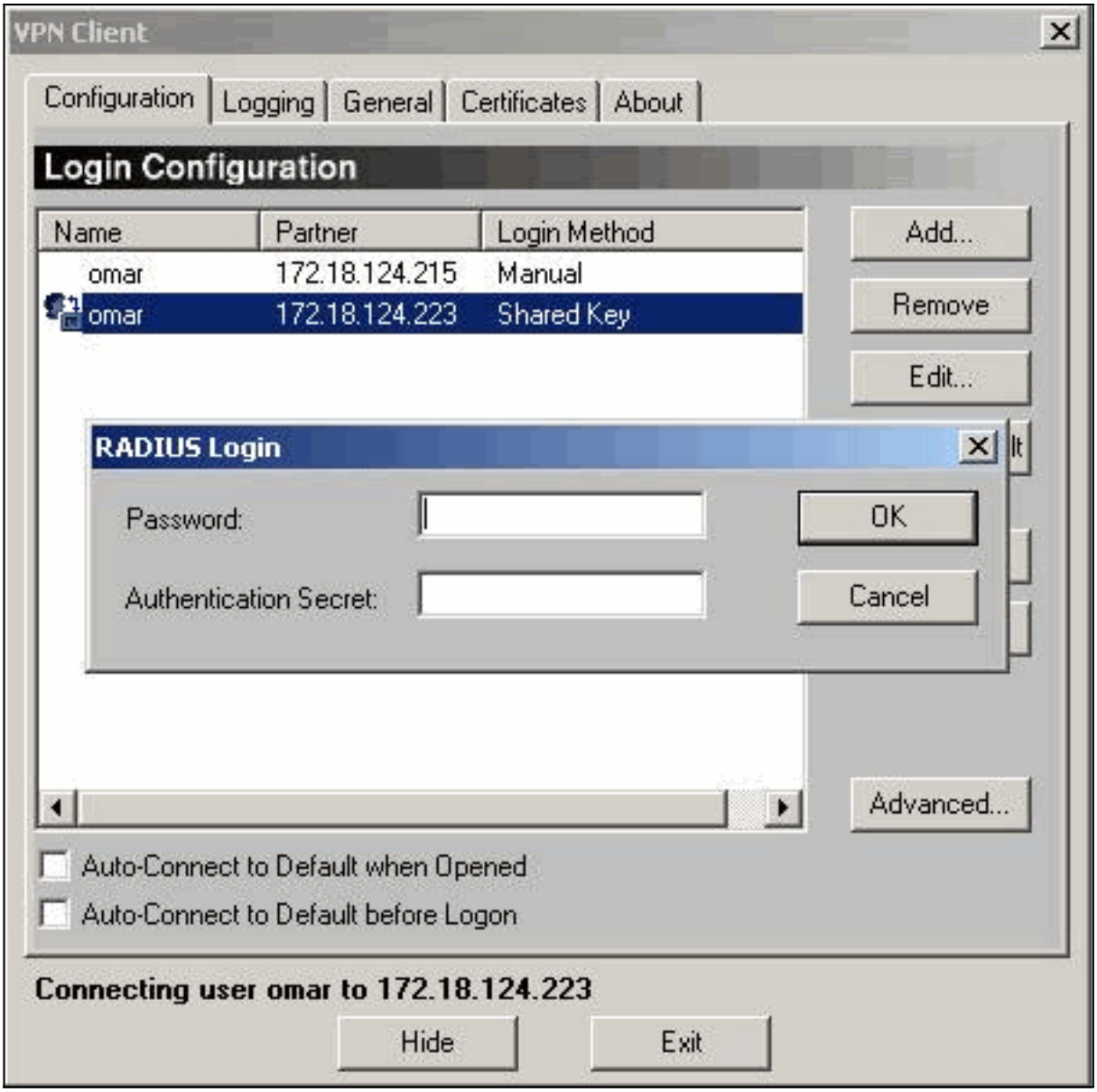
Dieses Verfahren führt Sie durch die Konfiguration des VPN-Clients.

1. Wählen Sie im Dialogfeld VPN-Client die Registerkarte Konfiguration aus. Geben Sie anschließend im Dialogfeld VPN Client-Prompt for Secret (VPN-Client-Aufforderung zur Geheimhaltung) den gemeinsamen geheimen Schlüssel unter dem VPN-Server ein. Der gemeinsame geheime Schlüssel des VPN-Clients ist der Wert, der für das VPN-Kennwort des Attributs 5 im VPN-Konzentrator eingegeben



wurde.

2. Nachdem Sie den freigegebenen geheimen Schlüssel eingegeben haben, werden Sie zur Eingabe eines Kennworts und eines Authentifizierungsgeheimnisses aufgefordert. Das Kennwort ist Ihr RADIUS-Kennwort für diesen Benutzer, und der Authentifizierungsgeheimnis ist der geheime PAP-Authentifizierungsschlüssel im `[ RADIUS]` Abschnitt des VPN Concentrator.



Concentrator-Protokolle

```
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
```

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Cisco VPN Concentrators der Serie 5000 - Ankündigung des Vertriebsendes

- Support-Seite für Cisco VPN 500 Concentrator
- Support-Seite für Cisco VPN 5000-Client
- IPSec-Support-Seite
- Technischer Support - Cisco Systems