

Configurazione di un concentratore Cisco VPN 5000 con autenticazione esterna per un server Microsoft Windows 2000 IAS RADIUS

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Cisco VPN 5000 Concentrator Configuration](#)

[Configurazione di Microsoft Windows 2000 IAS RADIUS Server](#)

[Verifica del risultato](#)

[Configurare il client VPN](#)

[Registri concentratore](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

[Introduzione](#)

In questo documento vengono descritte le procedure utilizzate per configurare un concentratore Cisco VPN 5000 con autenticazione esterna per un server Microsoft Windows 2000 Internet Authentication Server (IAS) con RADIUS.

Nota: il protocollo CHAP (Challenge Handshake Authentication Protocol) non funziona. Utilizzare solo il protocollo PAP (Password Authentication Protocol). Per ulteriori informazioni, fare riferimento all'ID bug Cisco [CSCdt96941](#) (solo utenti [registrati](#)).

[Prerequisiti](#)

[Requisiti](#)

Nessun requisito specifico previsto per questo documento.

[Componenti usati](#)

Le informazioni di questo documento si basano sulla seguente versione del software:

- Cisco VPN 5000 Concentrator Software versione 6.0.16.0001

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico

ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

Cisco VPN 5000 Concentrator Configuration

```
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#
```

Configurazione di Microsoft Windows 2000 IAS RADIUS Server

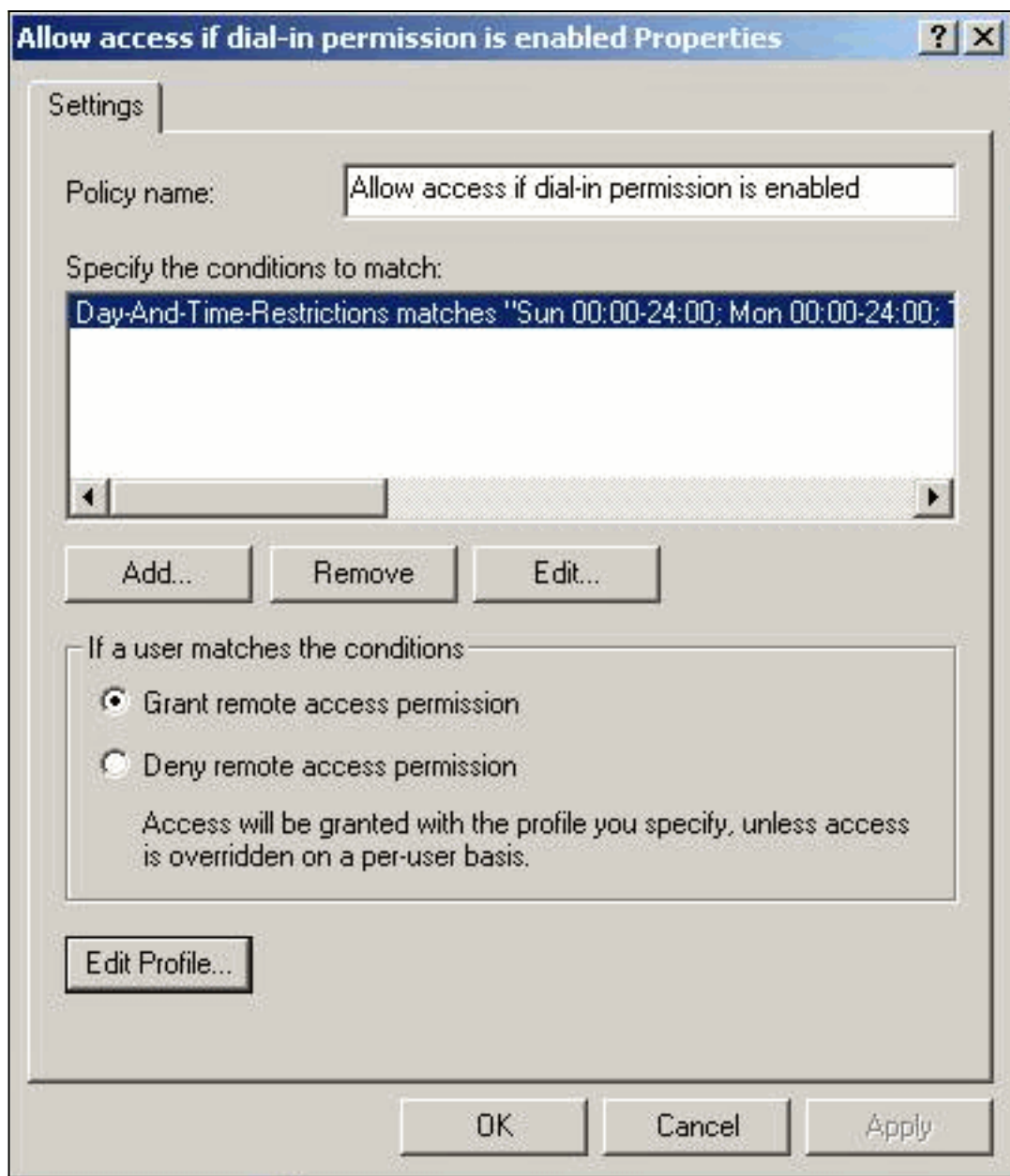
La procedura descritta di seguito consente di eseguire in modo semplificato la configurazione di un server RADIUS Microsoft Windows 2000 IAS.

1. Nelle proprietà IAS di Microsoft Windows 2000, selezionare **Client** e creare un nuovo client. Nell'esempio viene creata una voce denominata VPN5000. L'indirizzo IP di Cisco VPN 5000 Concentrator è 172.18.124.223. Nella casella a discesa Client-Vendor, selezionare **Cisco**. Il segreto condiviso è il segreto presente nella sezione [RADIUS] della configurazione di [VPN](#)

The screenshot shows the 'VPN5000 Properties' dialog box. The 'Settings' tab is active. The 'Friendly name for client' field contains 'VPN5000'. The 'Client address' section has a sub-field 'Address (IP or DNS):' with the value '172.18.124.223' and a 'Verify...' button. The 'Client-Vendor' dropdown 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 'xxxxxxx'. The dialog has 'OK', 'Cancel', and 'Apply' buttons at the bottom.

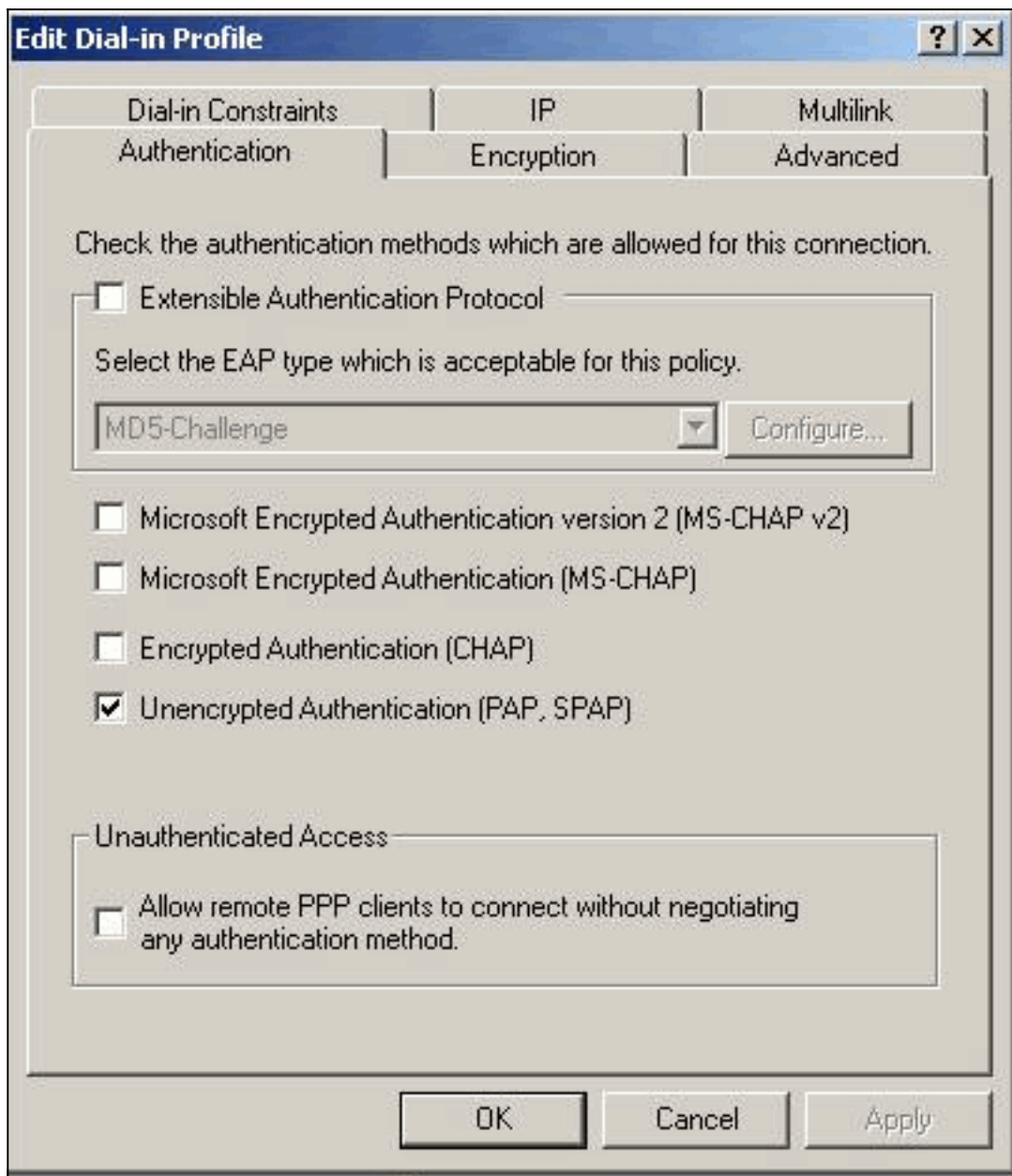
[Concentrator](#).

2. Nelle proprietà dei criteri di accesso remoto selezionare **Concedi autorizzazione di accesso remoto** nella sezione "Se un utente soddisfa le condizioni" e quindi fare clic su **Modifica**



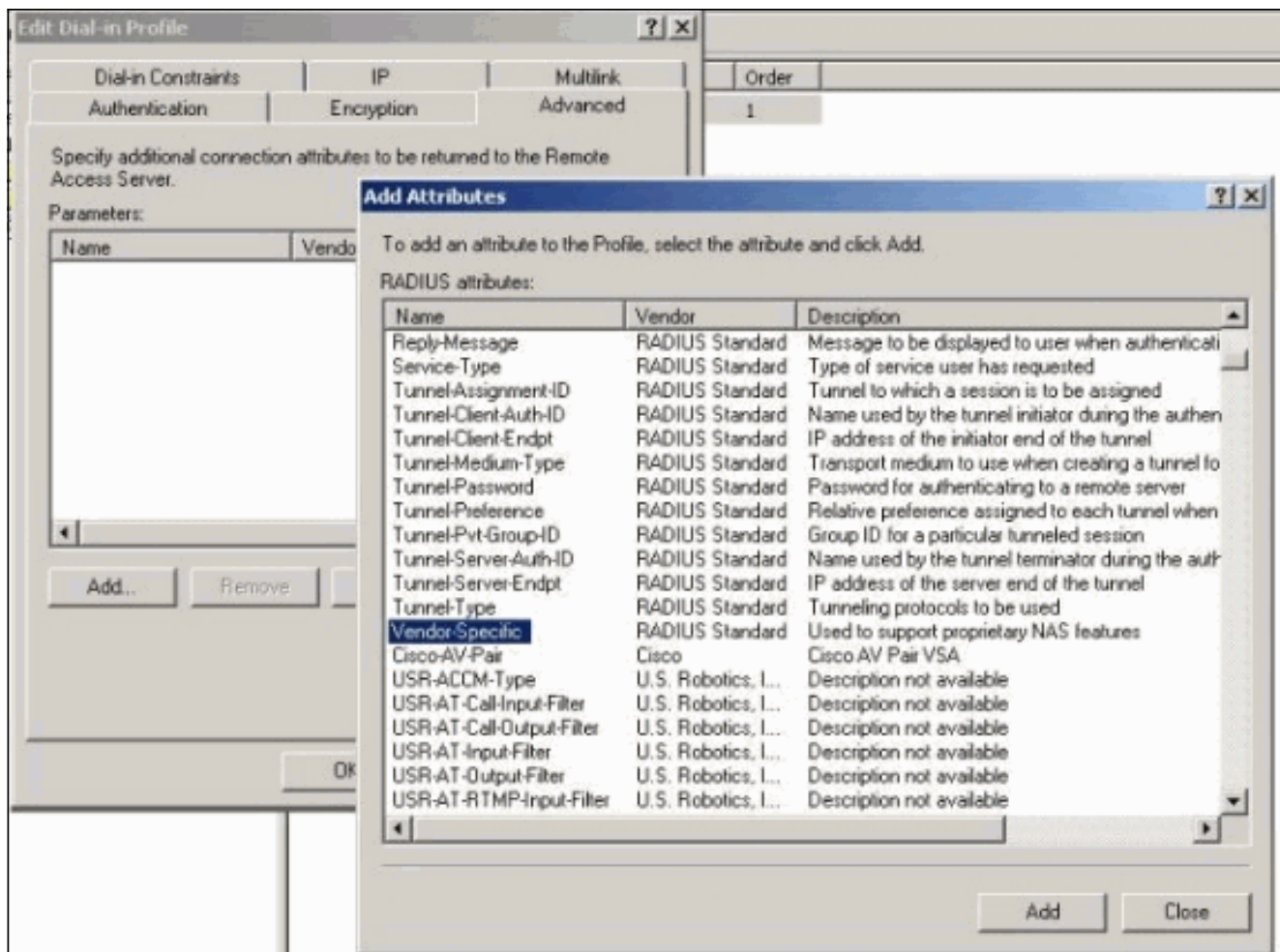
profilo.

3. Fare clic sulla scheda Autenticazione e verificare che sia selezionata solo l'opzione Autenticazione non crittografata (PAP,

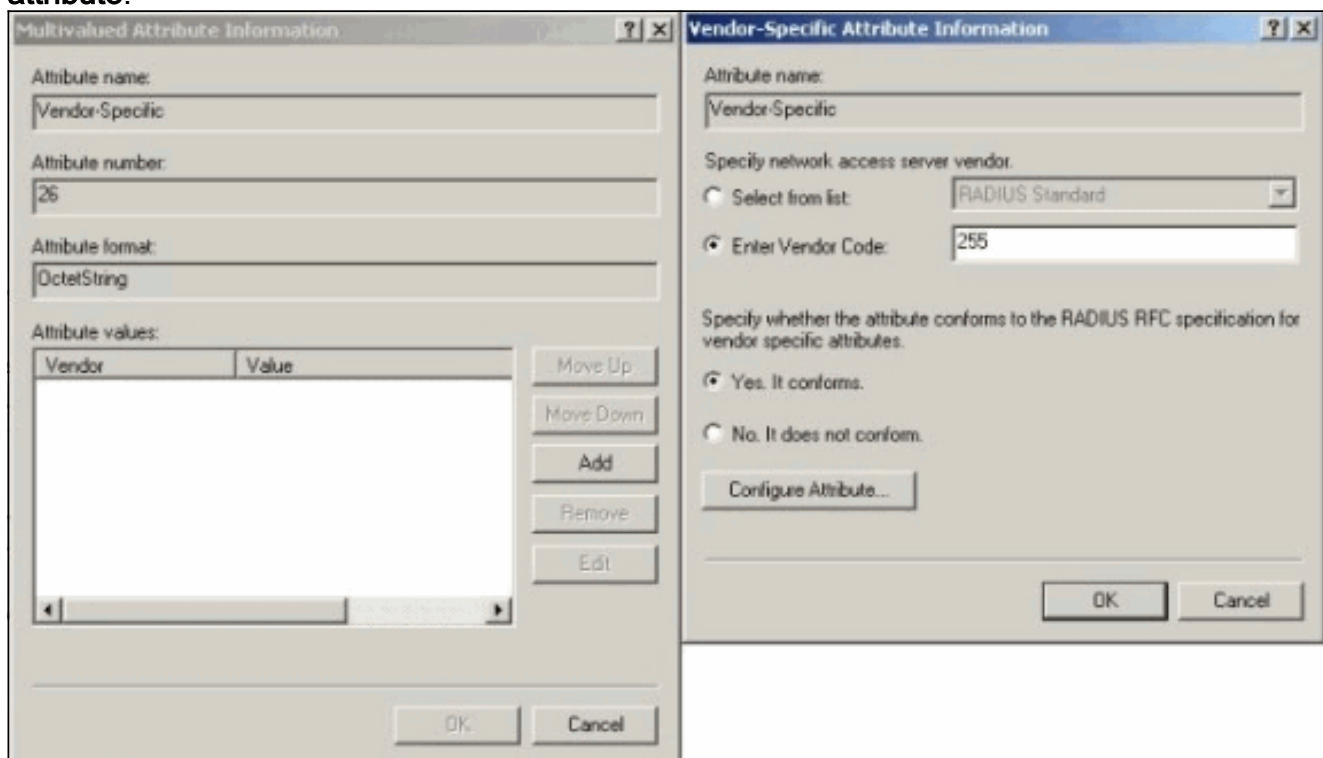


SPAP).

4. Selezionare la scheda Advanced (Avanzate), fare clic su **Add** (Aggiungi), quindi selezionare **Vendor-Specific** (Specifico del fornitore).

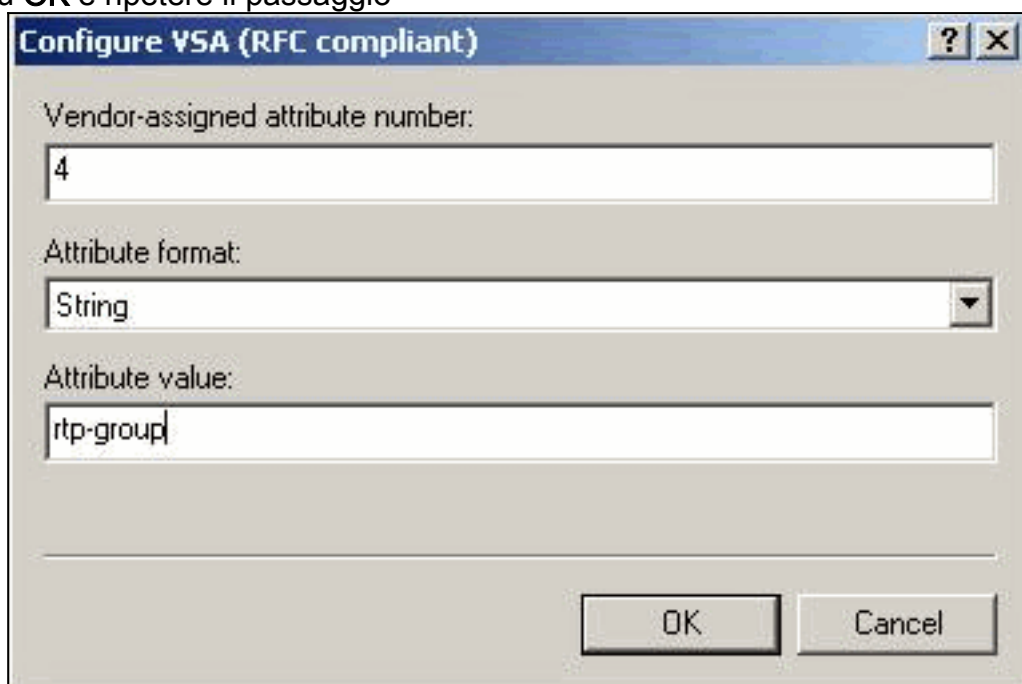


5. Nella finestra di dialogo Informazioni attributi multivalore relativa all'attributo specifico del fornitore, fare clic su **Add** per accedere alla finestra di dialogo Informazioni attributi specifici del fornitore. Selezionare **Enter Vendor Code** (Immetti codice fornitore) e immettere **255** nella casella adiacente. Quindi, selezionare **Sì. È conforme** e fare clic su **Configura attributo**.



6. Nella finestra di dialogo Configure VSA (RFC compliant), immettere **4** per il numero di attributo assegnato dal fornitore, **String** (Stringa) per il formato dell'attributo e **rtp-group**

(nome del gruppo VPN nel Cisco VPN 5000 Concentrator) per il valore dell'attributo. Fare clic su **OK** e ripetere il passaggio



Configure VSA (RFC compliant)

Vendor-assigned attribute number:
4

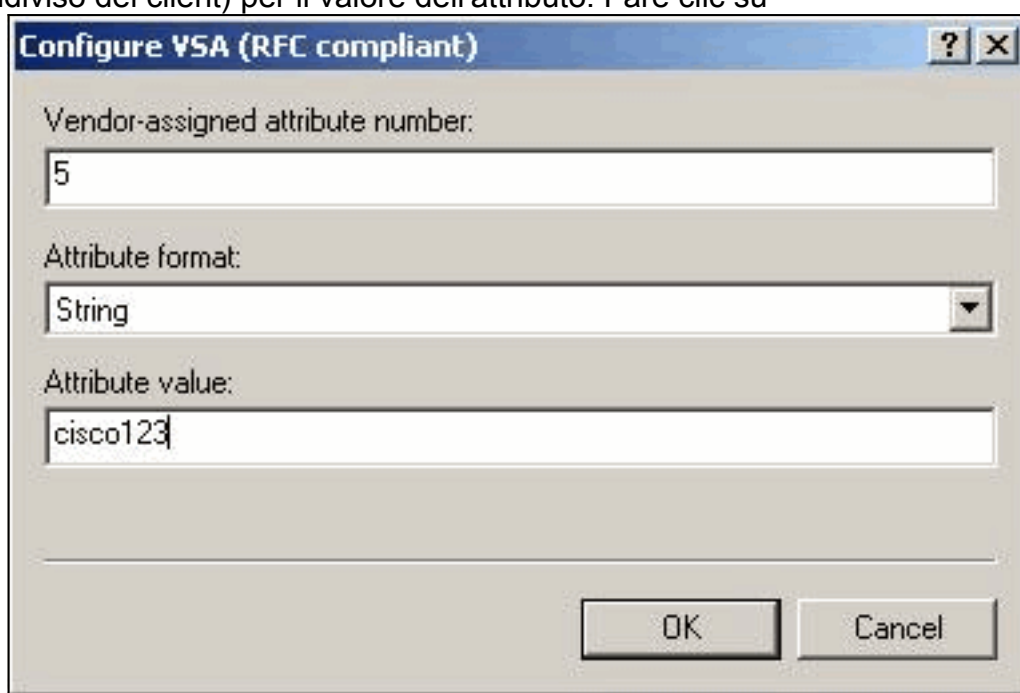
Attribute format:
String

Attribute value:
rtp-group

OK Cancel

5.

7. Nella finestra di dialogo **Configure VSA (RFC compliant)**, immettere **4** per il numero di attributo assegnato dal fornitore, **String** per il formato dell'attributo e **cisco123** (il segreto condiviso del client) per il valore dell'attributo. Fare clic su



Configure VSA (RFC compliant)

Vendor-assigned attribute number:
5

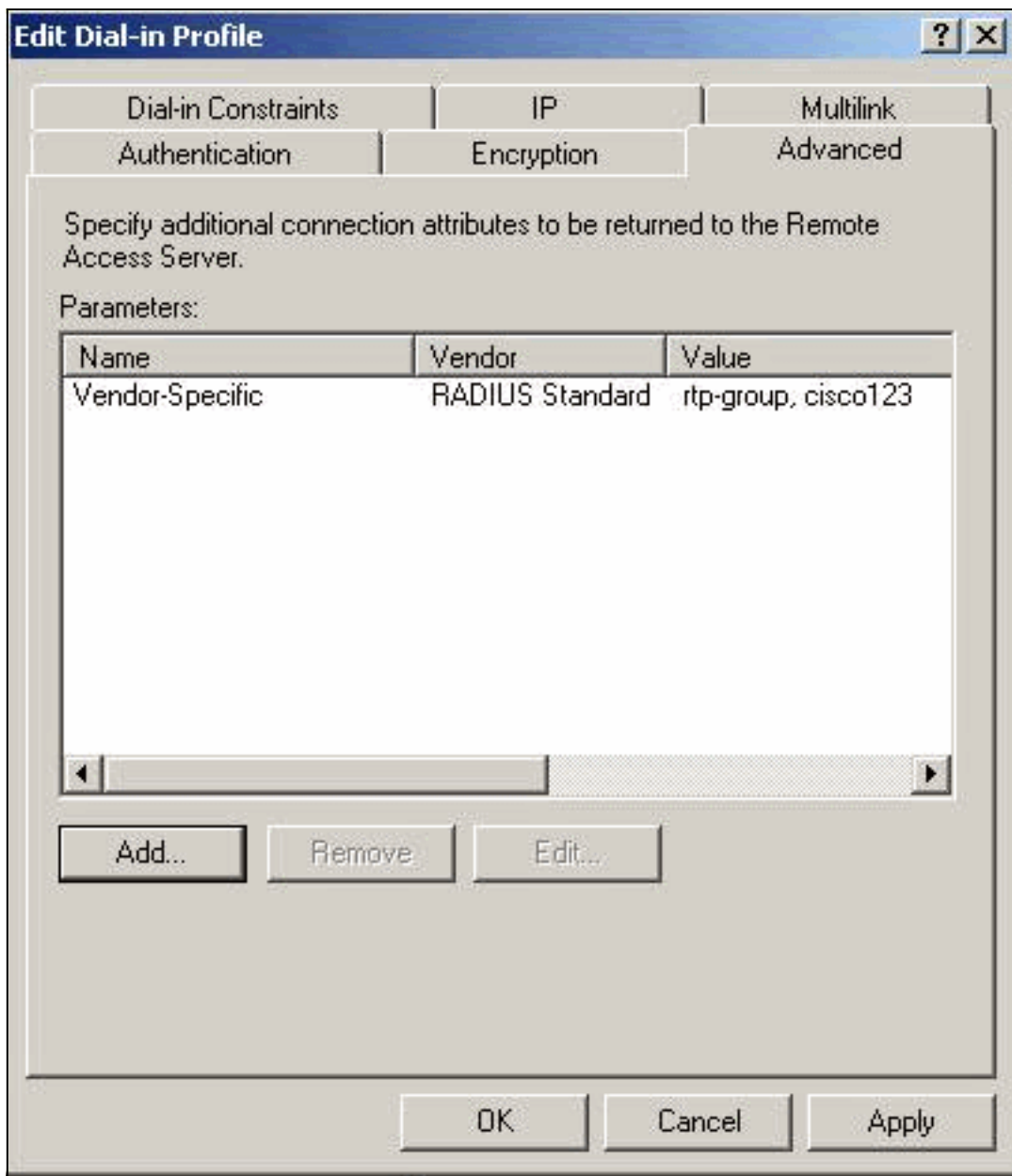
Attribute format:
String

Attribute value:
cisco123

OK Cancel

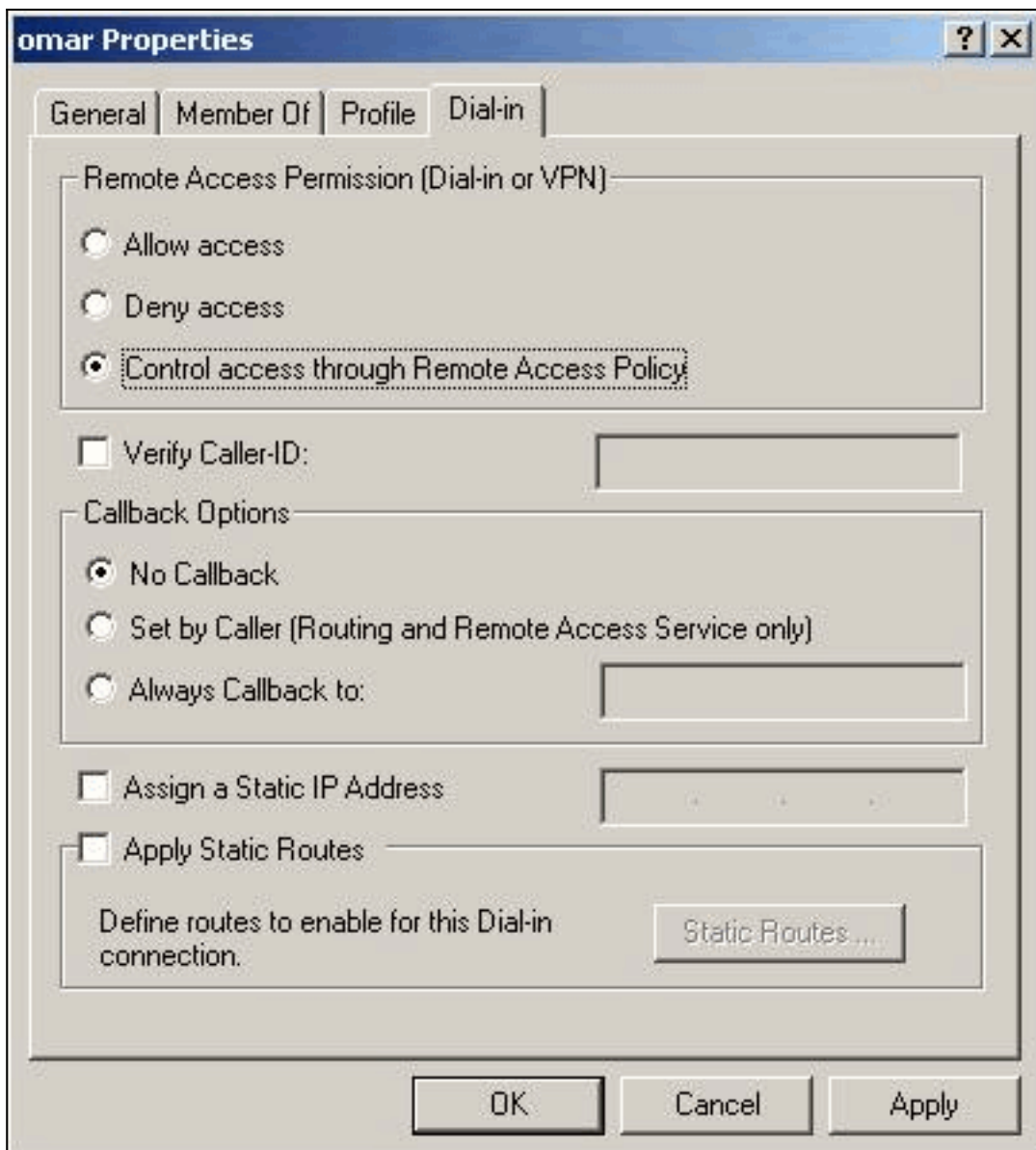
OK.

8. L'attributo Specifico del fornitore contiene due valori (gruppo e password



VPN).

9. In Proprietà utente fare clic sulla scheda Connessione remota e verificare che l'opzione **Controlla accesso tramite Criteri di accesso remoto** sia



selezionata.

Verifica del risultato

Le informazioni contenute in questa sezione permettono di verificare che la configurazione funzioni correttamente.

Alcuni comandi **show** sono supportati dallo [strumento Output Interpreter \(solo utenti registrati\)](#); lo strumento permette di visualizzare un'analisi dell'output del comando **show**.

- **show radius statistics**: visualizza le statistiche dei pacchetti per la comunicazione tra il concentratore VPN e il server RADIUS predefinito identificato dalla sezione RADIUS.
- **show radius config** - Visualizza le impostazioni correnti per i parametri RADIUS.

Questo è l'output del 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>

Questo è l'output del comando **show radius config**.

```

RADIUS          State    UDP   CHAP16
Authentication  On      1812  No
Accounting      Off     1813  n/a
Secret          'radiuspassword'

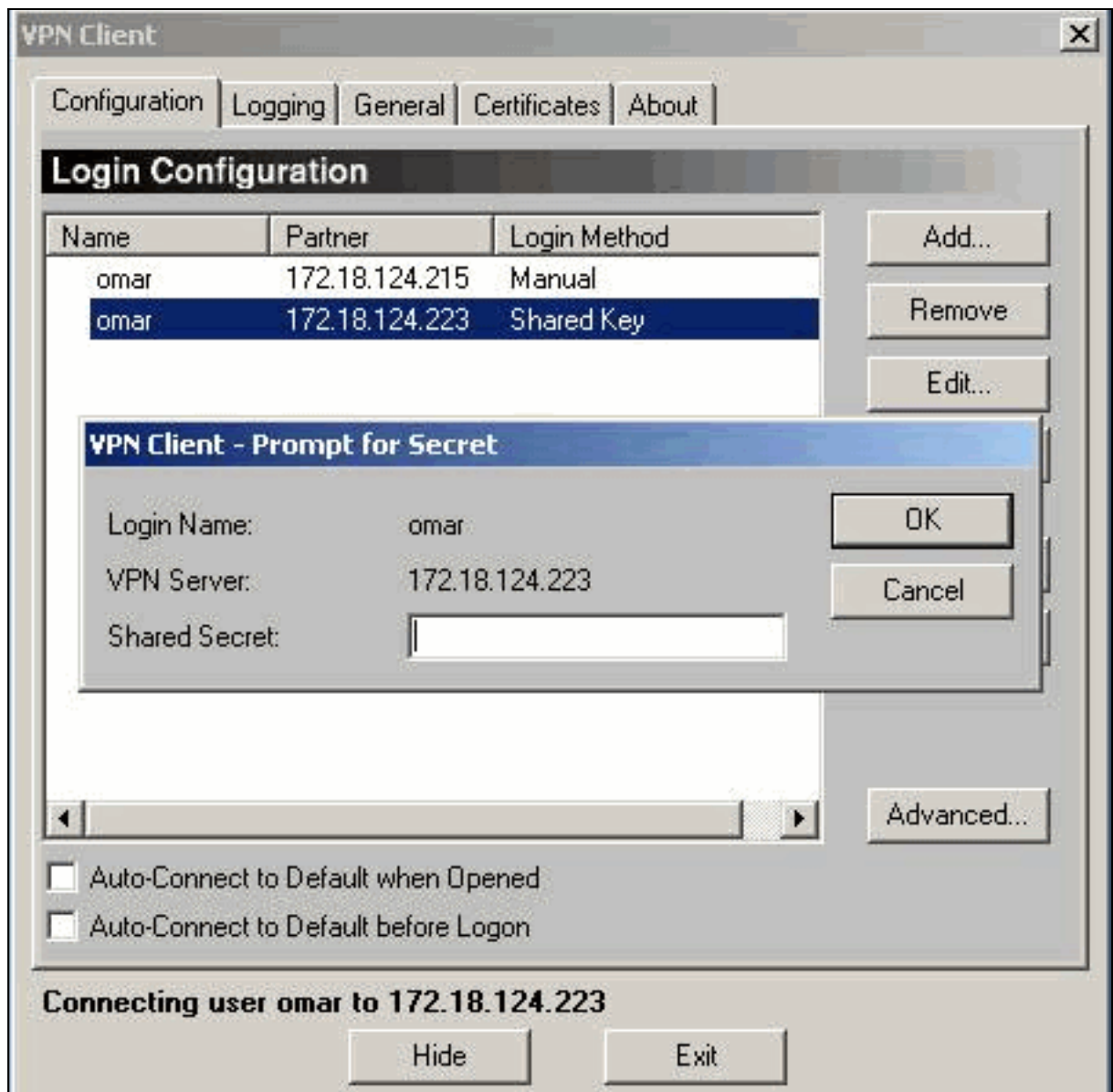
Server    IP address    Attempts  AcctSecret
Primary   172.18.124.108    5    n/a
Secondary Off

```

[Configurare il client VPN](#)

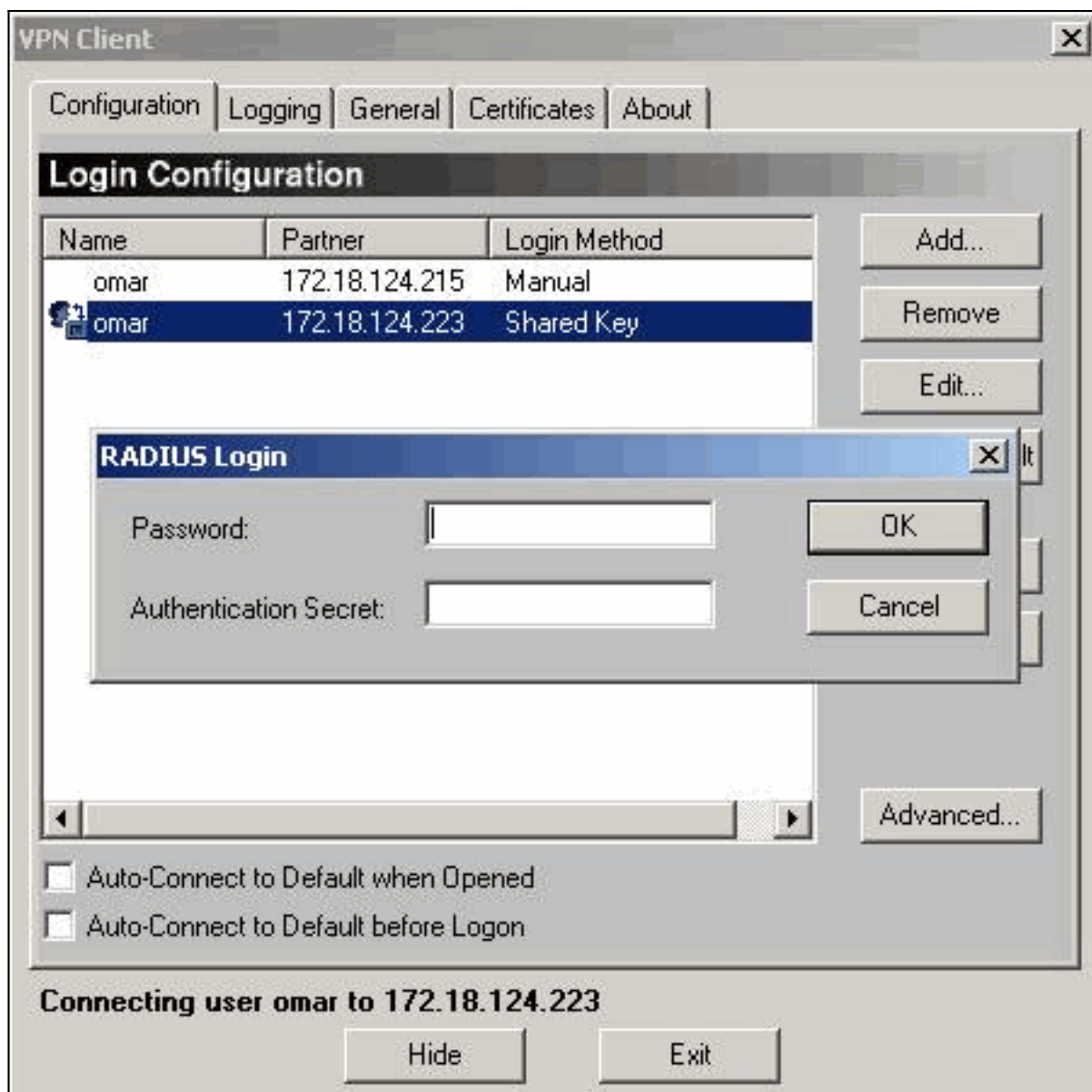
Questa procedura guida l'utente nella configurazione del client VPN.

1. Dalla finestra di dialogo VPN Client, selezionare la scheda Configurazione. Quindi, dalla finestra di dialogo VPN Client-Prompt for Secret, immettere il segreto condiviso nel server VPN. Il segreto condiviso del client VPN è il valore immesso per la password VPN dell'attributo 5 in Concentrator



VPN.

2. Dopo aver immesso il segreto condiviso, vengono richiesti una password e un segreto di autenticazione. La password è la password RADIUS per l'utente e il segreto di autenticazione è il segreto di autenticazione PAP nella sezione [RADIUS] di [VPN Concentrator](#).



[Registri concentratore](#)

```
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
```

[Risoluzione dei problemi](#)

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

[Informazioni correlate](#)

- [Cisco VPN serie 5000 concentrator: annuncio di fine vendita](#)

- [Pagina di supporto per Cisco VPN 5000 Concentrator](#)
- [Pagina di supporto per i client Cisco VPN 5000](#)
- [Pagina di supporto per IPSec](#)
- [Supporto tecnico – Cisco Systems](#)