

Configuration d'un concentrateur Cisco VPN 5000 avec authentification externe sur un serveur RADIUS IAS Microsoft Windows 2000

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Configuration du concentrateur Cisco VPN 5000](#)

[Configurer le serveur RADIUS IAS Microsoft Windows 2000](#)

[Vérifier le résultat](#)

[Configurer le client VPN](#)

[Journaux du concentrateur](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit les procédures utilisées pour configurer un concentrateur Cisco VPN 5000 avec authentification externe sur un serveur d'authentification Internet (IAS) Microsoft Windows 2000 avec RADIUS.

Remarque : le protocole CHAP (Challenge Handshake Authentication Protocol) ne fonctionne pas. Utilisez uniquement le protocole PAP (Password Authentication Protocol). Référez-vous à l'ID de bogue Cisco [CSCdt96941](#) (clients [enregistrés](#) uniquement) pour plus de détails.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

L'information contenue dans le présent document est fondée sur cette version logicielle:

- Logiciel du concentrateur Cisco VPN 5000 version 6.0.16.0001

The information in this document was created from the devices in a specific lab environment. All of

the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the [Cisco Technical Tips Conventions](#).

Configuration du concentrateur Cisco VPN 5000

```
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#
```

Configurer le serveur RADIUS IAS Microsoft Windows 2000

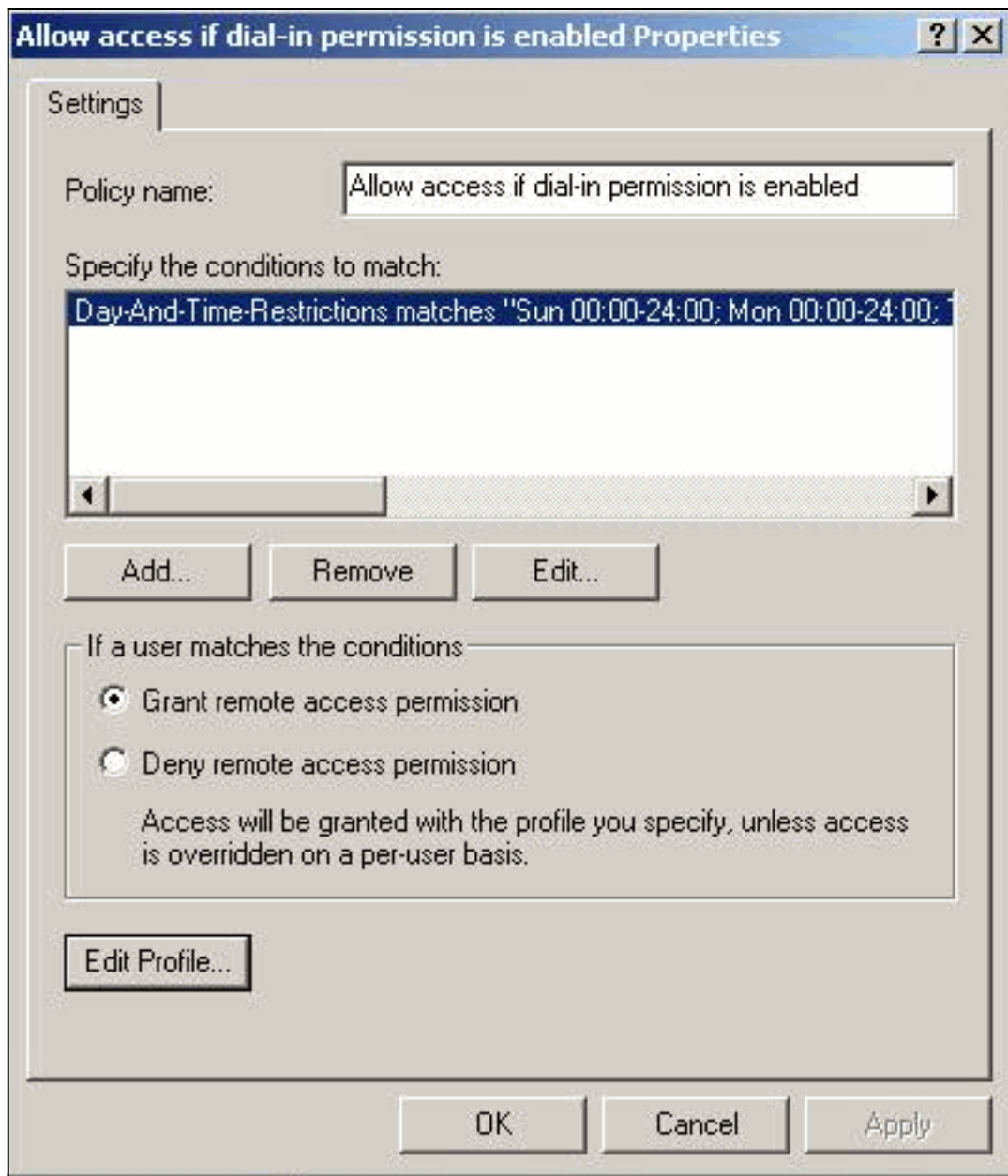
Ces étapes vous guident dans une configuration de serveur RADIUS Microsoft Windows 2000 IAS simple.

1. Sous les propriétés IAS de Microsoft Windows 2000, sélectionnez **Clients** et créez un nouveau client. Dans cet exemple, une entrée nommée VPN5000 est créée. L'adresse IP du concentrateur Cisco VPN 5000 est 172.18.124.223. Dans la liste déroulante Client-Vendor, sélectionnez **Cisco**. Le secret partagé est le secret de la configuration [RADIUS] de [concentrateur](#)

The screenshot shows the 'VPN5000 Properties' dialog box. The 'Settings' tab is active. The 'Friendly name for client' field is filled with 'VPN5000'. The 'Client address' section has an 'Address (IP or DNS)' field containing '172.18.124.223' and a 'Verify...' button. 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 'xxxxxxx'. At the bottom, there are 'OK', 'Cancel', and 'Apply' buttons.

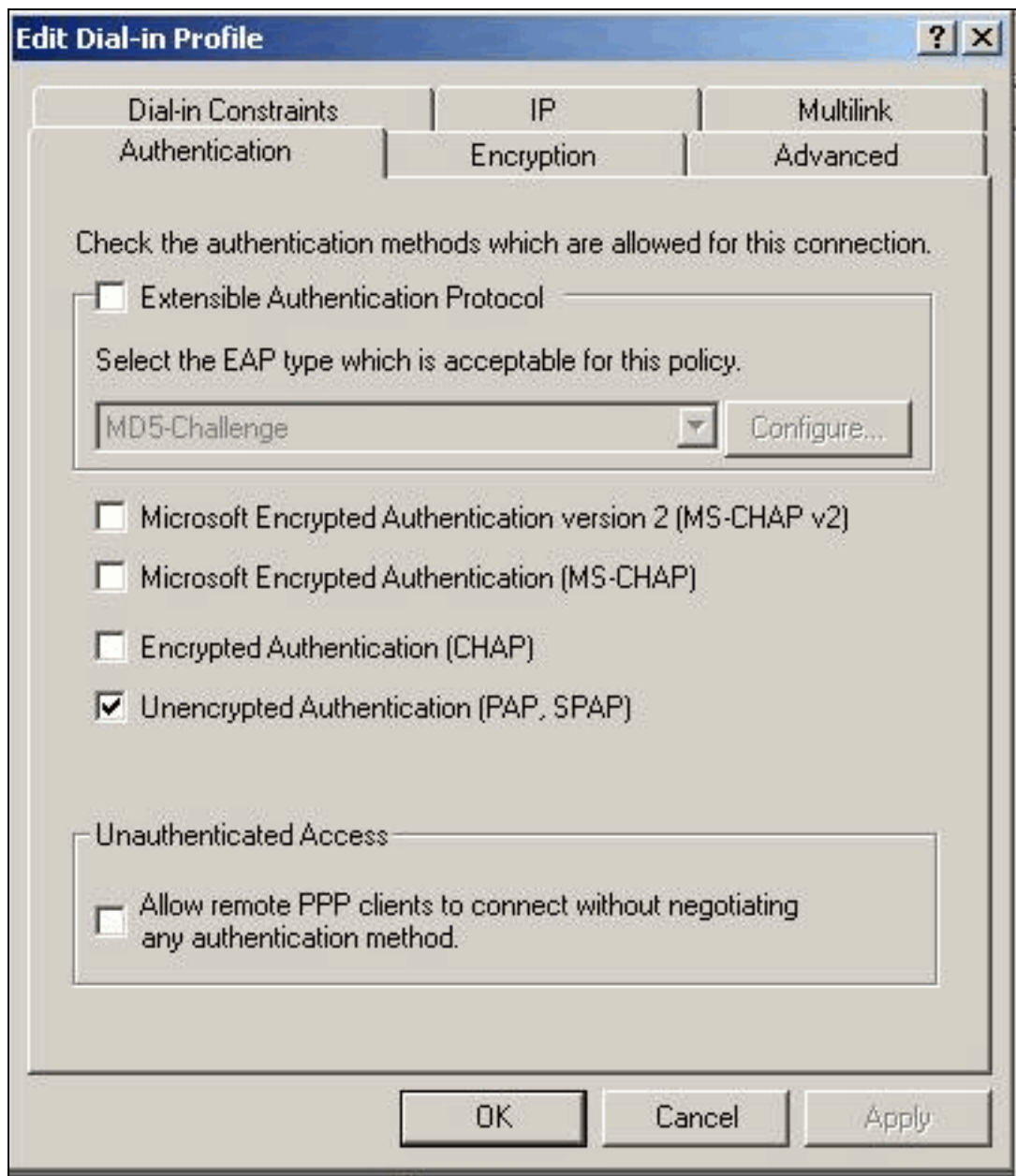
[VPN](#)

2. Sous les propriétés de la stratégie d'accès à distance, sélectionnez **Accorder l'autorisation d'accès à distance** dans la section « Si un utilisateur correspond aux conditions », puis cliquez sur **Modifier le**



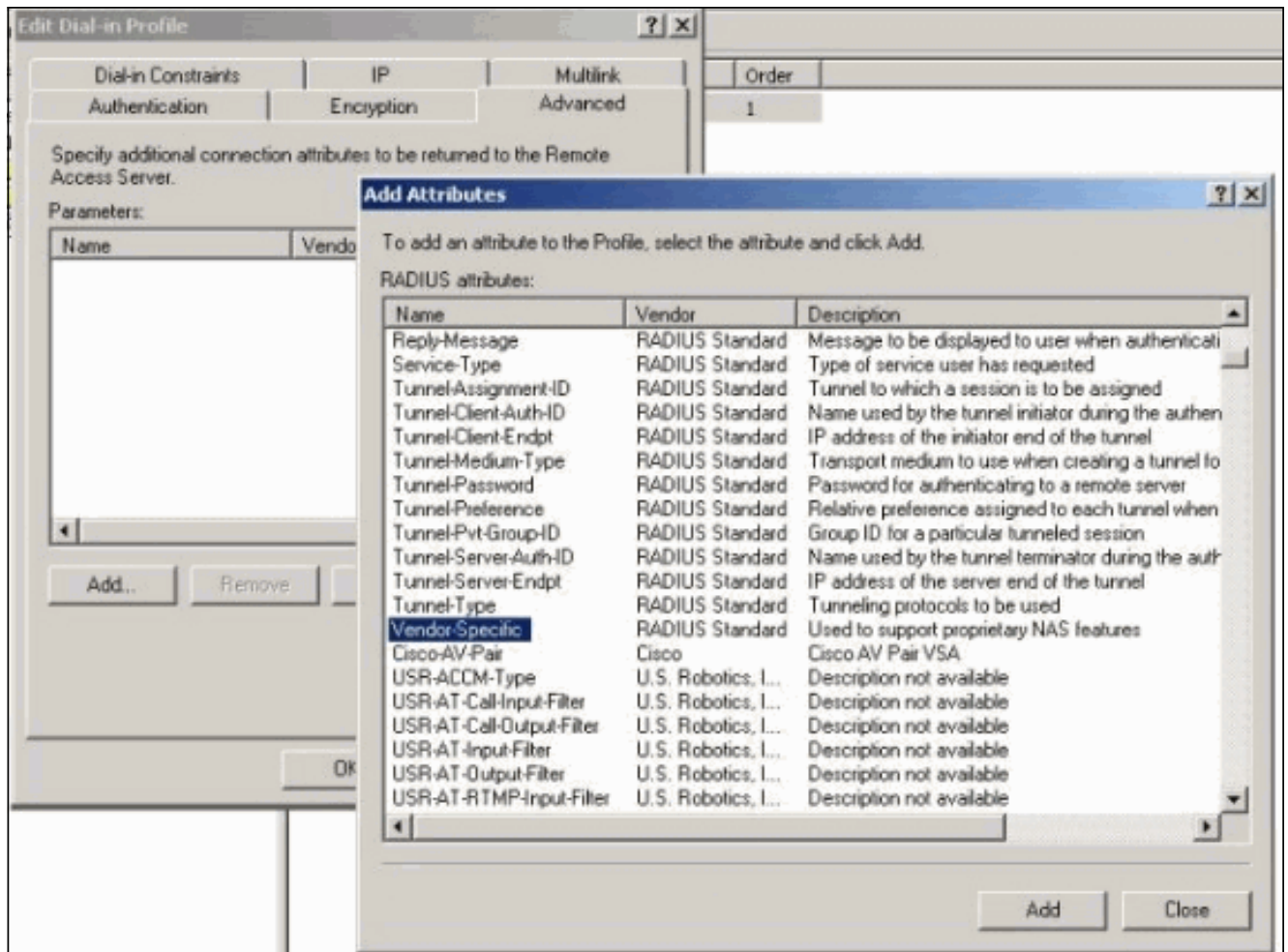
profil.

3. Cliquez sur l'onglet Authentication (Authentification) et assurez-vous que seule l'authentification non chiffrée (PAP, SPAP) est

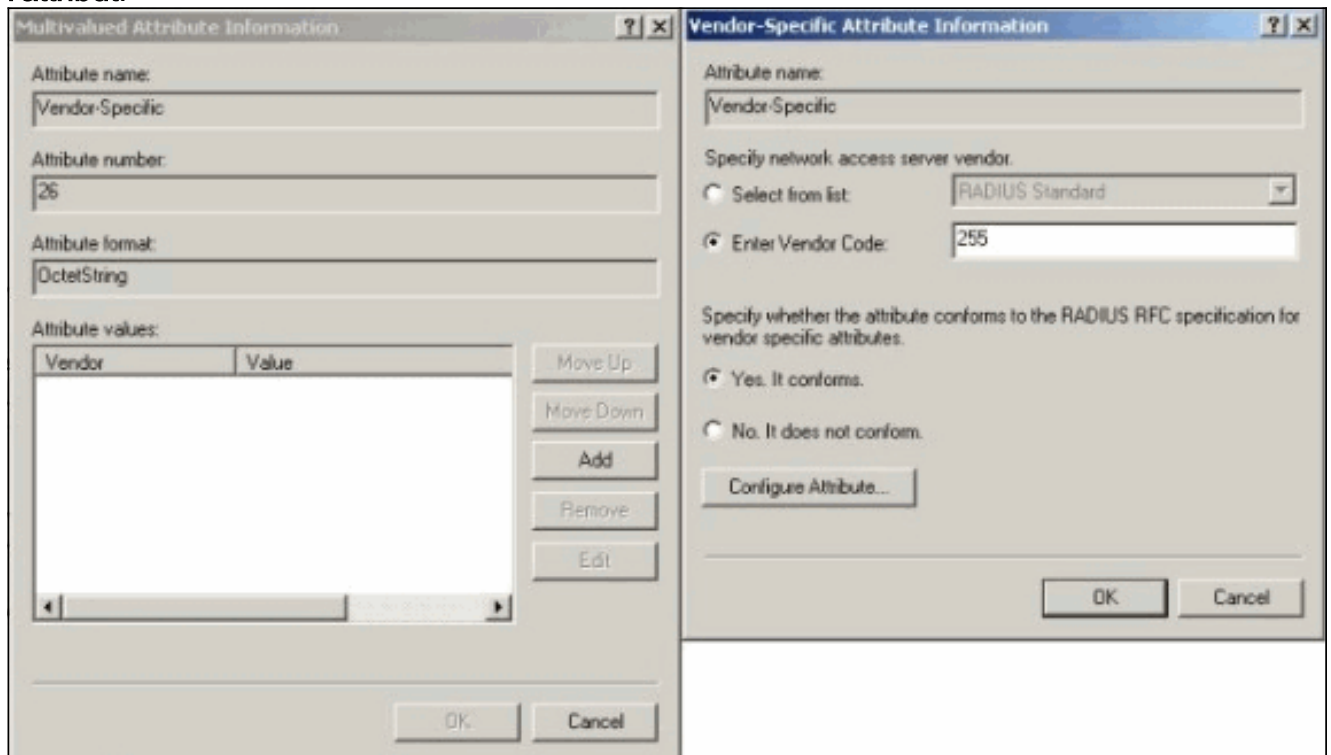


sélectionnée.

4. Sélectionnez l'onglet Avancé, cliquez sur **Ajouter** et sélectionnez **Spécifique au fournisseur**.



5. Sous la boîte de dialogue Informations d'attribut multivaleurs de l'attribut Spécifique au fournisseur, cliquez sur **Ajouter** afin d'accéder à la boîte de dialogue Informations d'attribut spécifique au fournisseur. Sélectionnez **Enter Vendor Code** et saisissez **255** dans la zone adjacente. Ensuite, sélectionnez **Oui. Il est conforme** et cliquez sur **Configurer l'attribut**.



6. Dans la boîte de dialogue Configurer VSA (conforme RFC), saisissez **4** pour le numéro d'attribut attribué par le fournisseur, saisissez **String** pour le format d'attribut et saisissez **rtp-**

group (nom du groupe VPN dans le concentrateur Cisco VPN 5000) pour la valeur d'attribut. Cliquez sur **OK** et répétez l'étape



Configure VSA (RFC compliant)

Vendor-assigned attribute number:
4

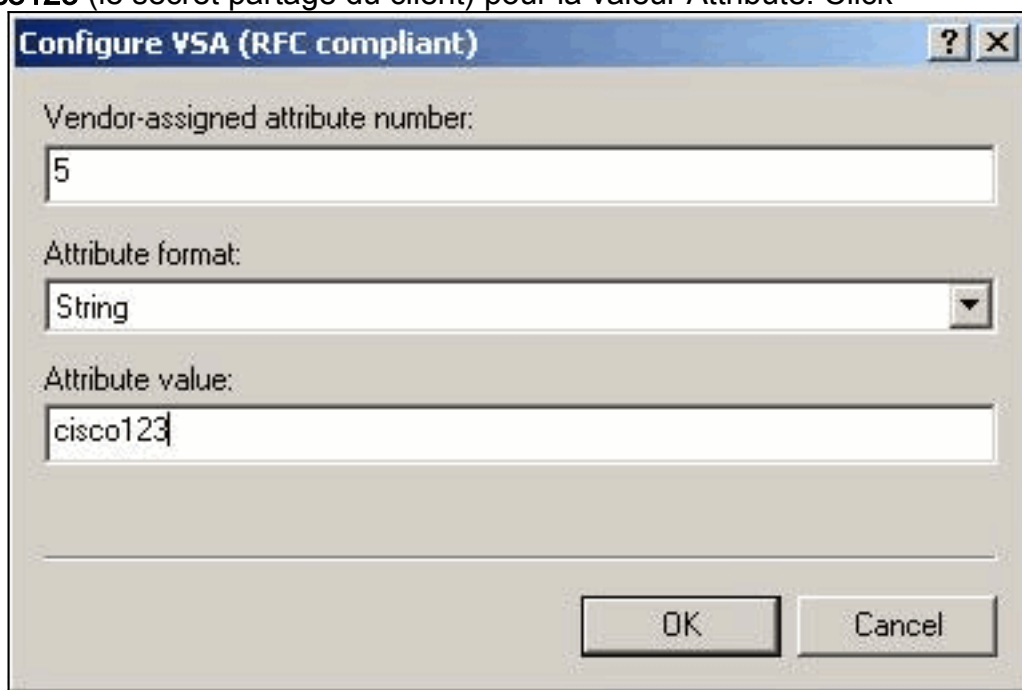
Attribute format:
String

Attribute value:
rtp-group

OK Cancel

5.

7. Dans la boîte de dialogue Configurer VSA (conforme RFC), saisissez **4** pour le numéro d'attribut attribué par le fournisseur, saisissez **String** pour le format d'attribut et saisissez **cisco123** (le secret partagé du client) pour la valeur Attribut. Cliquez



Configure VSA (RFC compliant)

Vendor-assigned attribute number:
5

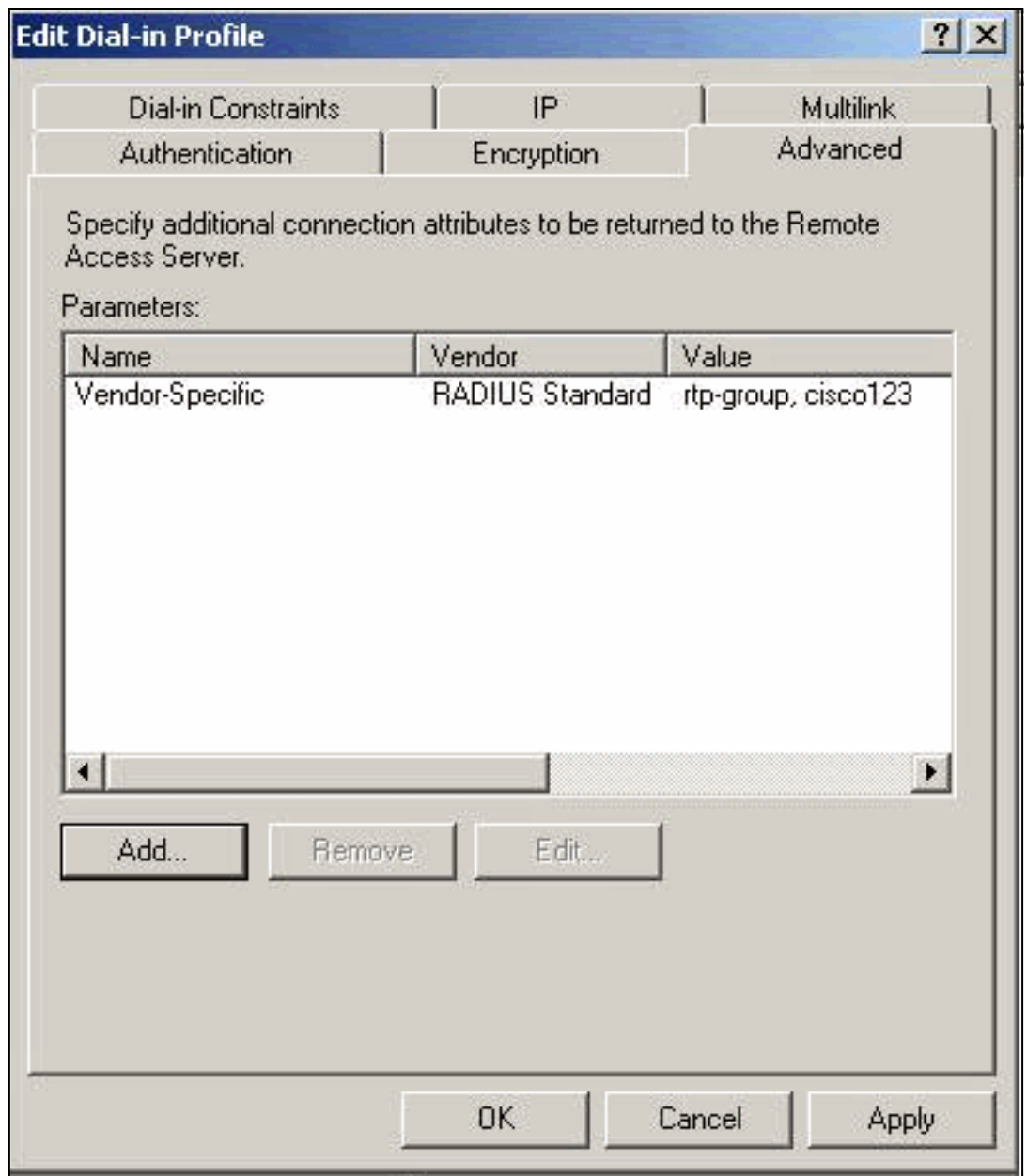
Attribute format:
String

Attribute value:
cisco123

OK Cancel

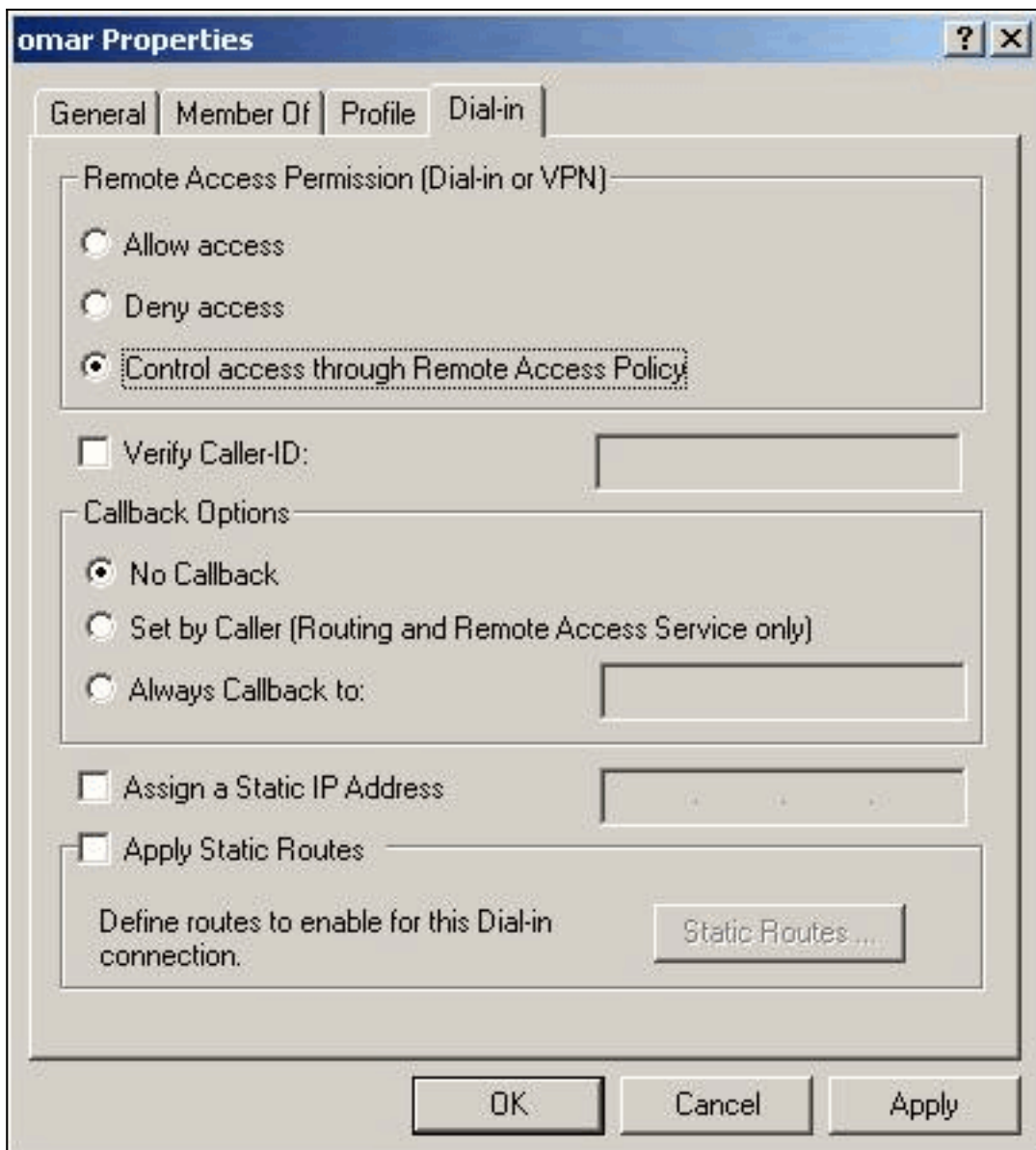
OK.

8. Vous voyez que l'attribut Spécifique au Fournisseur contient deux valeurs (mot de passe de



groupe et VPN).

9. Sous vos propriétés utilisateur, cliquez sur l'onglet Composer et assurez-vous que **Contrôle de l'accès via la stratégie d'accès à distance** est



sélectionné.

Vérifier le résultat

Cette section fournit des informations qui vous permettront de vérifier que votre configuration fonctionne correctement.

Certaines commandes **show** sont prises en charge par l'[Output Interpreter Tool](#) (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

- **show radius statistics** - Affiche les statistiques de paquets pour la communication entre le concentrateur VPN et le serveur RADIUS par défaut identifié par la section RADIUS.
- **show radius config** : affiche les paramètres actuels des paramètres RADIUS.

Il s'agit de la sortie de la commande **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>

Ceci est le résultat de la commande **show radius config**.

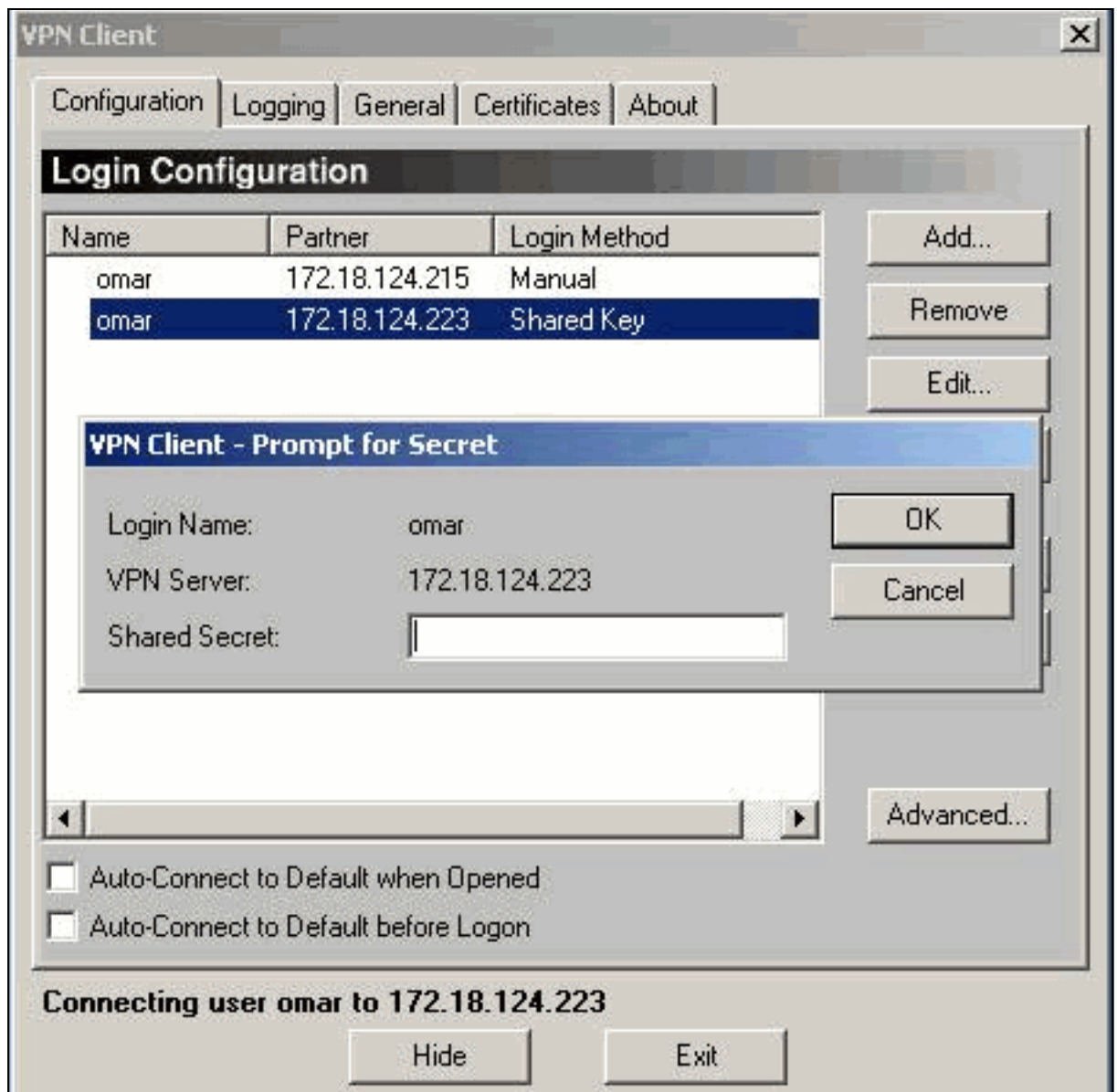
RADIUS	State	UDP	CHAP16
Authentication	On	1812	No
Accounting	Off	1813	n/a
Secret	'radiuspassword'		

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

[Configurer le client VPN](#)

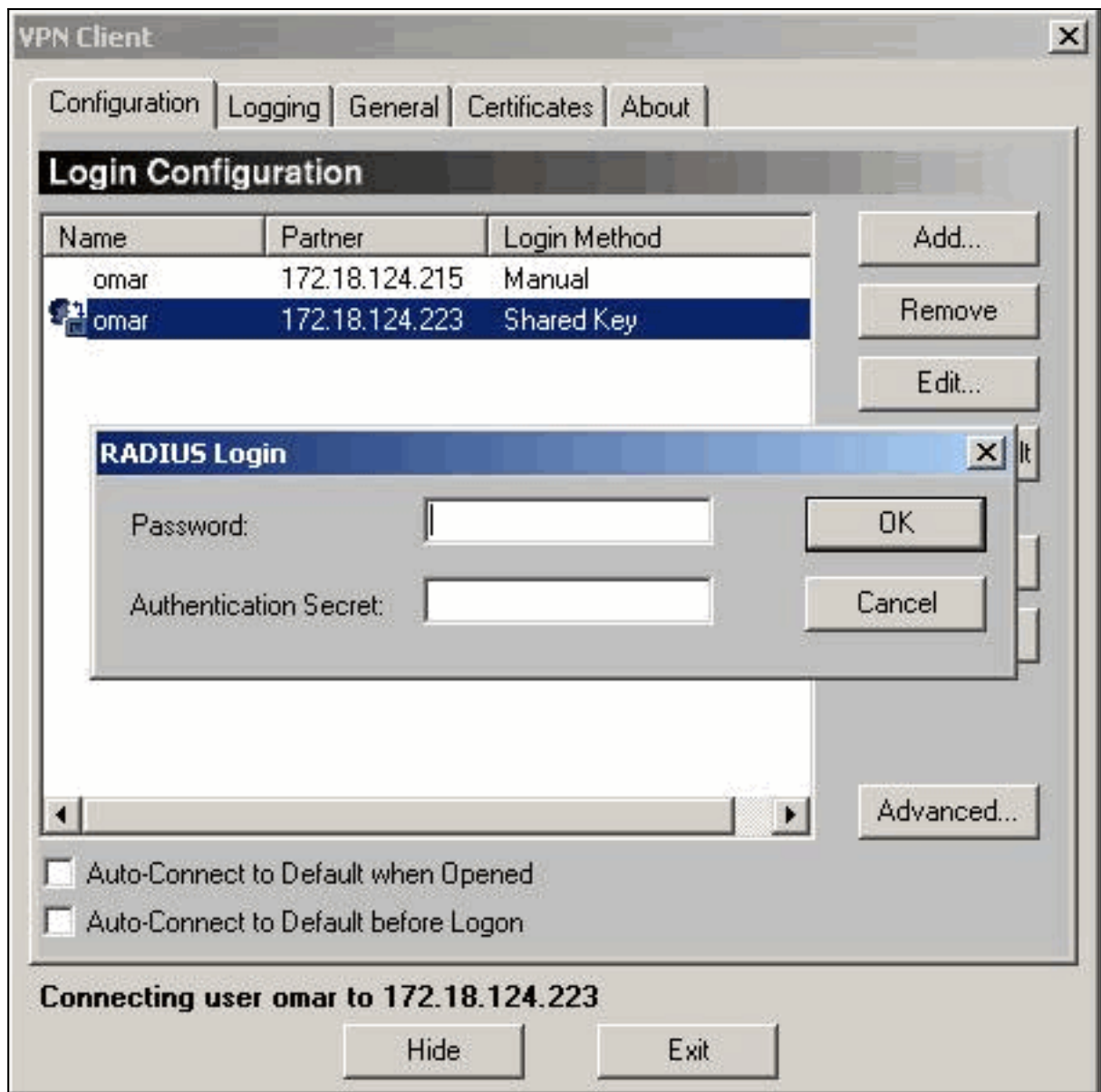
Cette procédure vous guide tout au long de la configuration du client VPN.

1. Dans la boîte de dialogue Client VPN, sélectionnez l'onglet Configuration. Ensuite, dans la boîte de dialogue VPN Client-Prompt for Secret, saisissez le secret partagé sous VPN Server. Le secret partagé du client VPN est la valeur entrée pour le mot de passe VPN de l'attribut 5 dans le concentrateur



VPN.

2. Après avoir entré le secret partagé, vous êtes invité à entrer un mot de passe et un secret d'authentification. Le mot de passe est votre mot de passe RADIUS pour cet utilisateur, et le secret d'authentification est le secret d'authentification PAP dans la section [RADIUS] du [concentrateur](#)



[VPN](#)

[Journaux du concentrateur](#)

```
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
```

[Dépannage](#)

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

[Informations connexes](#)

- [Annonce de fin de commercialisation des concentrateurs Cisco VPN 5000](#)
- [Page d'assistance du concentrateur VPN Cisco 5000](#)

- [Page d'assistance du client VPN 5000 de Cisco](#)
- [Page d'assistance IPsec](#)
- [Support technique - Cisco Systems](#)