

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

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Configuration du concentrateur de Cisco VPN 5000](#)

[Configurez le serveur de RAYON d'IAS de Microsoft Windows 2000](#)

[Vérifiez le résultat](#)

[Configurer le client VPN](#)

[Logs de concentrateur](#)

[Dépannez](#)

[Informations connexes](#)

## [Introduction](#)

Ce document décrit les procédures utilisées pour configurer un concentrateur de Cisco VPN 5000 avec l'authentification externe à un Microsoft Windows 2000 Internet Authentication Server (IAS) avec le RAYON.

**Note:** Le protocole d'authentification CHAP (Challenge Handshake Authentication Protocol) ne fonctionne pas. Password Authentication Protocol (PAP) d'utilisation seulement. Référez-vous à l'ID de bogue Cisco [CSCdt96941](#) (clients [enregistrés](#) seulement) pour d'autres détails.

## [Conditions préalables](#)

### [Conditions requises](#)

Aucune spécification déterminée n'est requise pour ce document.

### [Composants utilisés](#)

Les informations dans ce document sont basées sur cette version de logiciel :

- Version 6.0.16.0001 de logiciel du concentrateur de Cisco VPN 5000

Les informations contenues dans ce document ont été créées à partir des périphériques d'un

environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

## Conventions

Pour plus d'informations sur les conventions de documents, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

## Configuration du concentrateur de 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#
```

## [Configurez le serveur de RAYON d'IAS de Microsoft Windows 2000](#)

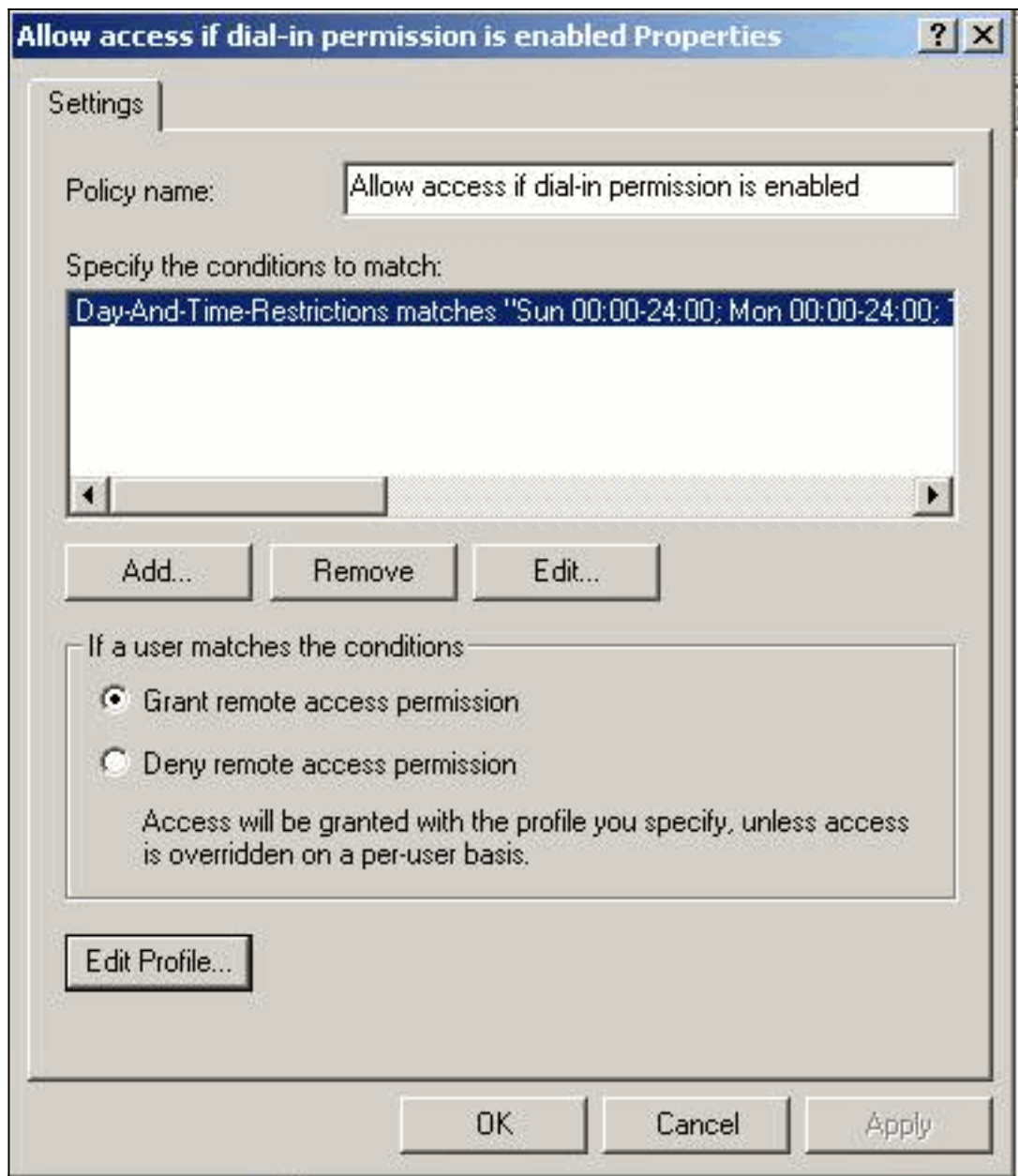
Ces étapes vous guident par une configuration du serveur RADIUS simple d'IAS de Microsoft Windows 2000.

1. Sous les propriétés d'IAS de Microsoft Windows 2000, les **clients** choisis et crée un nouveau client. Dans cet exemple, une entrée nommée VPN5000 est créée. L'adresse IP du concentrateur de Cisco VPN 5000 est 172.18.124.223. Sous la liste déroulante de Client-constructeur, **Cisco** choisi. Le secret partagé est le secret dans [la section de RAYON] de la [configuration du concentrateur](#)

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 'Address (IP or DNS):' set to '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.

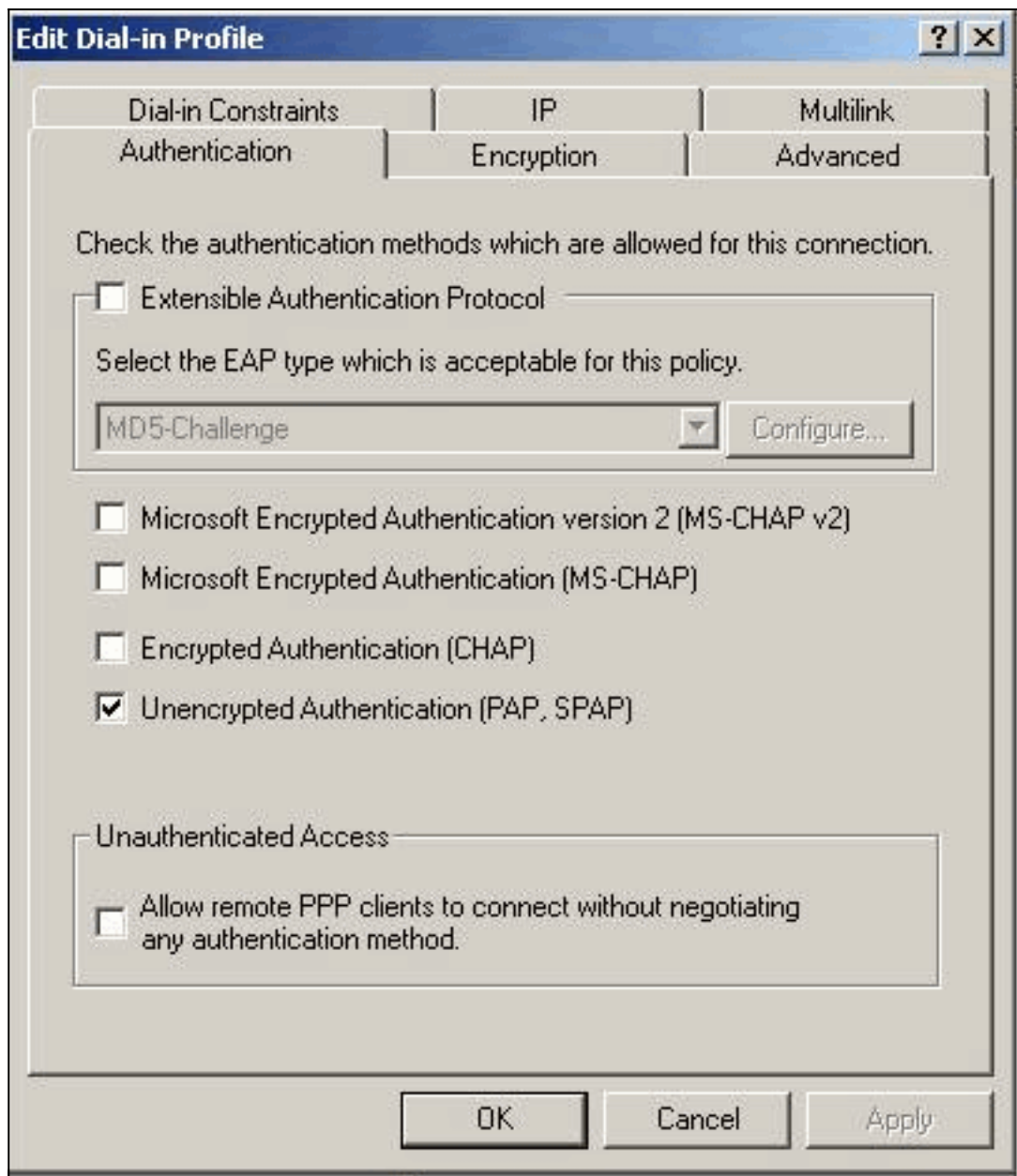
[VPN.](#)

2. Sous les propriétés de la stratégie d'accès à distance, l'**autorisation** choisie d'**Accès à distance de Grant** sous « si un utilisateur apparie les conditions » section et puis clique sur



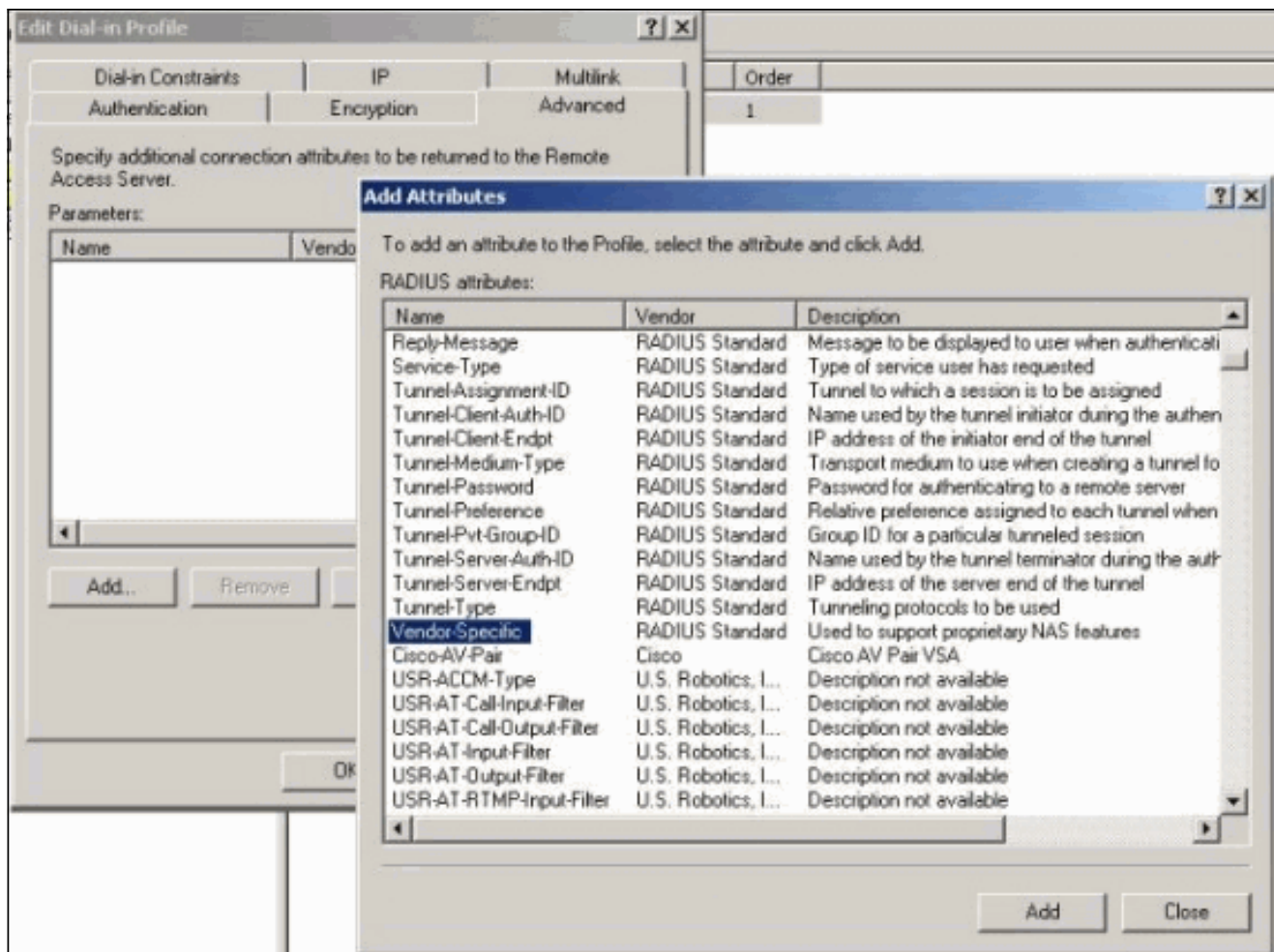
Edit le profil.

3. Cliquez sur l'onglet d'authentification et l'assurez que cette seulement **authentification décryptée (PAP, SPAP)** est

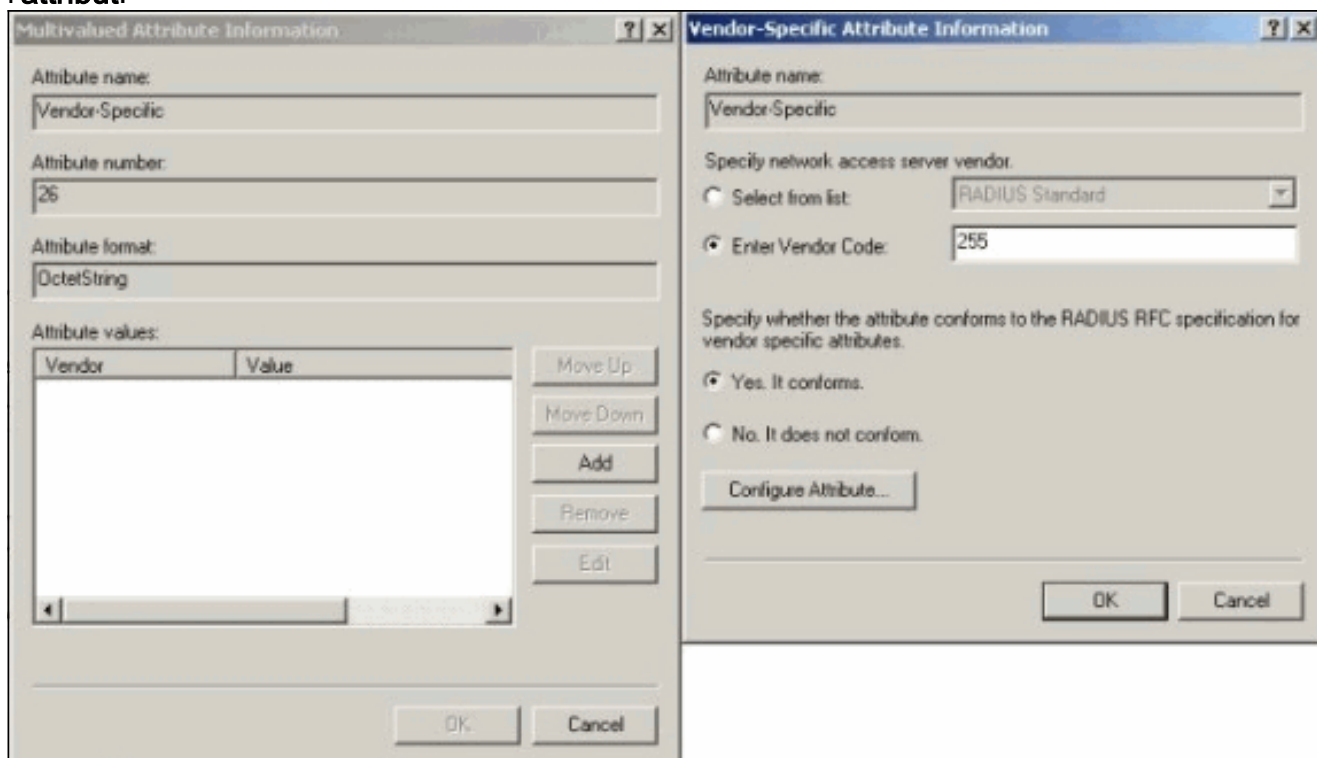


sélectionné.

4. Sélectionnez l'onglet Avancé, cliquez sur Add et sélectionnez la Constructeur-particularité.

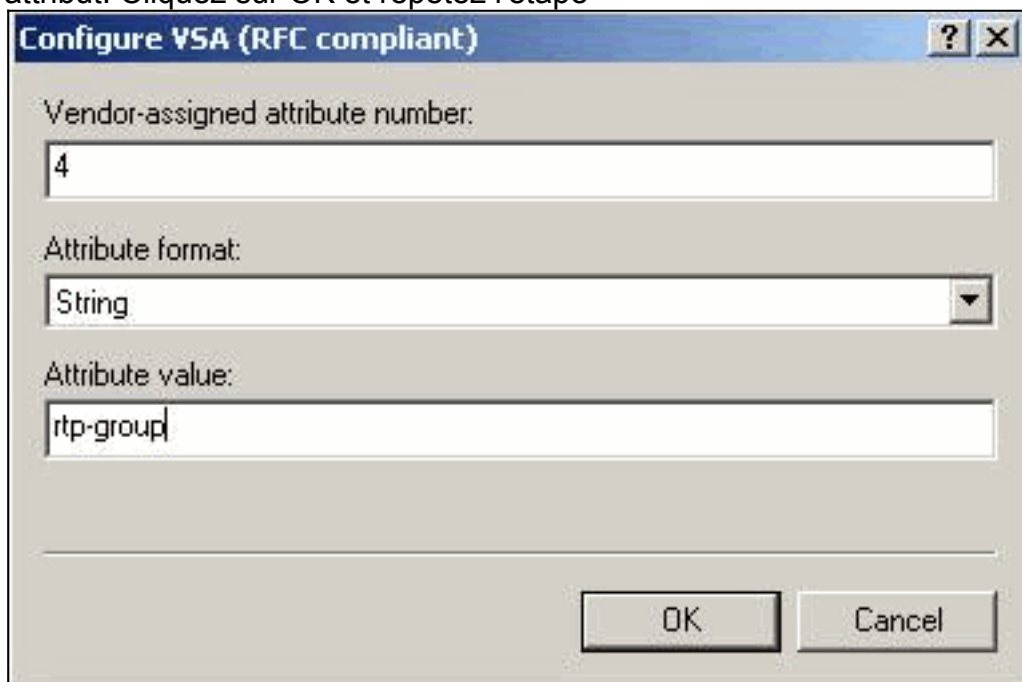


5. Sous la boîte de dialogue à valeurs multiples de l'information d'attribut pour l'attribut de Constructeur-particularité, cliquez sur Add afin d'aller dans la boîte de dialogue de l'information d'attribut de Constructeur-particularité. Choisissez **écrivez le code de constructeur** et écrivez **255** dans la case adjacente. Prochain, sélectionnez **oui**. Il se conforme et cliquez sur Configure l'attribut.



6. Sous la boîte de dialogue VSA de configurer (RFC conforme), écrivez **4** pour le nombre

Constructeur-assigné d'attribut, écrivez la **chaîne** pour le format d'attribut, et écrivez le **rtp-groupe** (nom du groupe VPN dans le concentrateur de Cisco VPN 5000) pour la valeur d'attribut. Cliquez sur OK et répétez l'étape



Configure VSA (RFC compliant)

Vendor-assigned attribute number:  
4

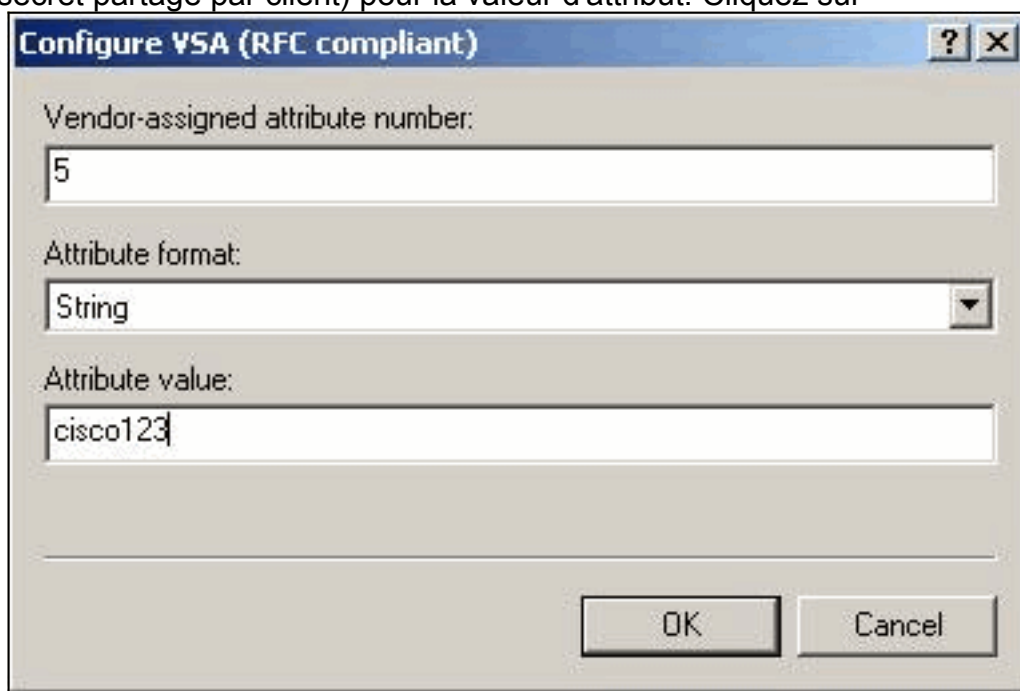
Attribute format:  
String

Attribute value:  
rtp-group

OK Cancel

5.

7. Sous la boîte de dialogue VSA de configurer (RFC conforme), écrivez **4** pour le nombre Constructeur-assigné d'attribut, écrivez la **chaîne** pour le format d'attribut, et écrivez **cisco123** (le secret partagé par client) pour la valeur d'attribut. Cliquez sur



Configure VSA (RFC compliant)

Vendor-assigned attribute number:  
5

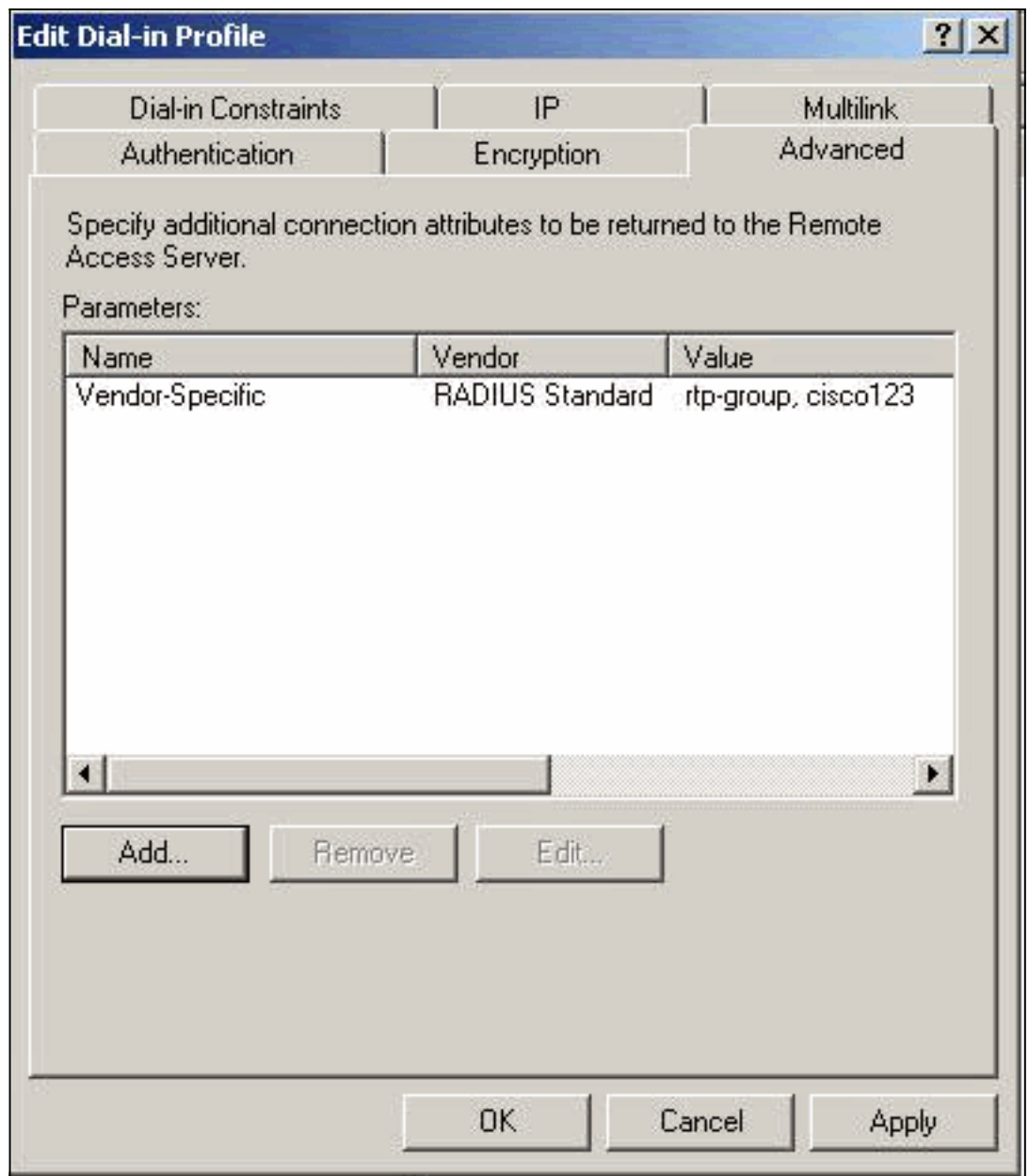
Attribute format:  
String

Attribute value:  
cisco123

OK Cancel

OK.

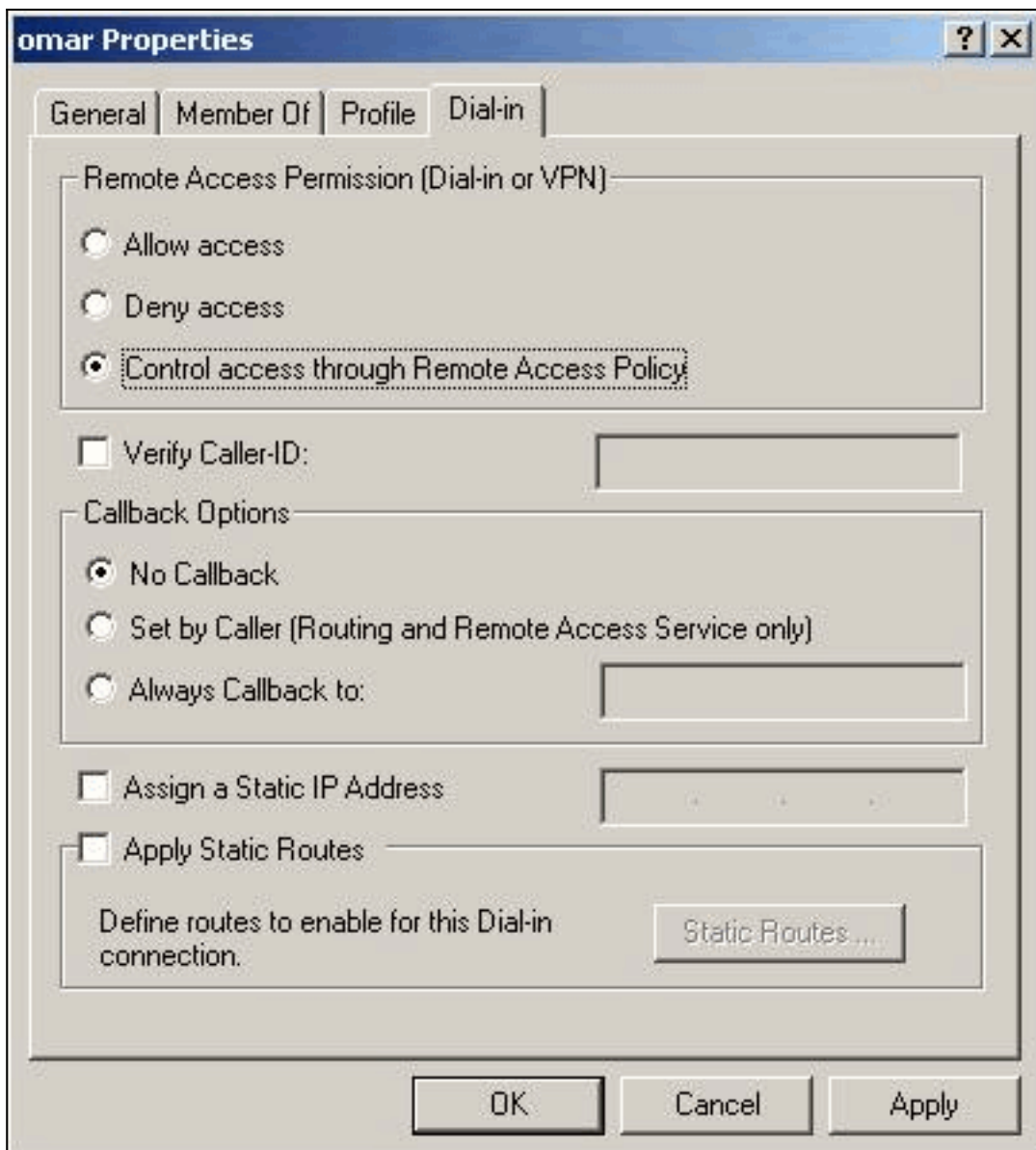
8. Vous voyez que l'attribut de Constructeur-particularité contient deux valeurs (groupe et mot



de passe VPN).

9. Sous vos propriétés d'utilisateur, cliquez sur l'onglet Numérotation et assurez-vous que l'accès de contrôle par la stratégie d'accès à distance est





sélectionné.

## Vérifiez 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** — Les statistiques de paquet d'affichages pour la transmission entre le concentrateur VPN et le serveur par défaut de RAYON les ont identifié par la section de RAYON.
- **config de show radius** — Affiche les configurations actuelles pour des paramètres de RAYON.

C'est la sortie de la commande de **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>

C'est la sortie de la commande de config de show radius.

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

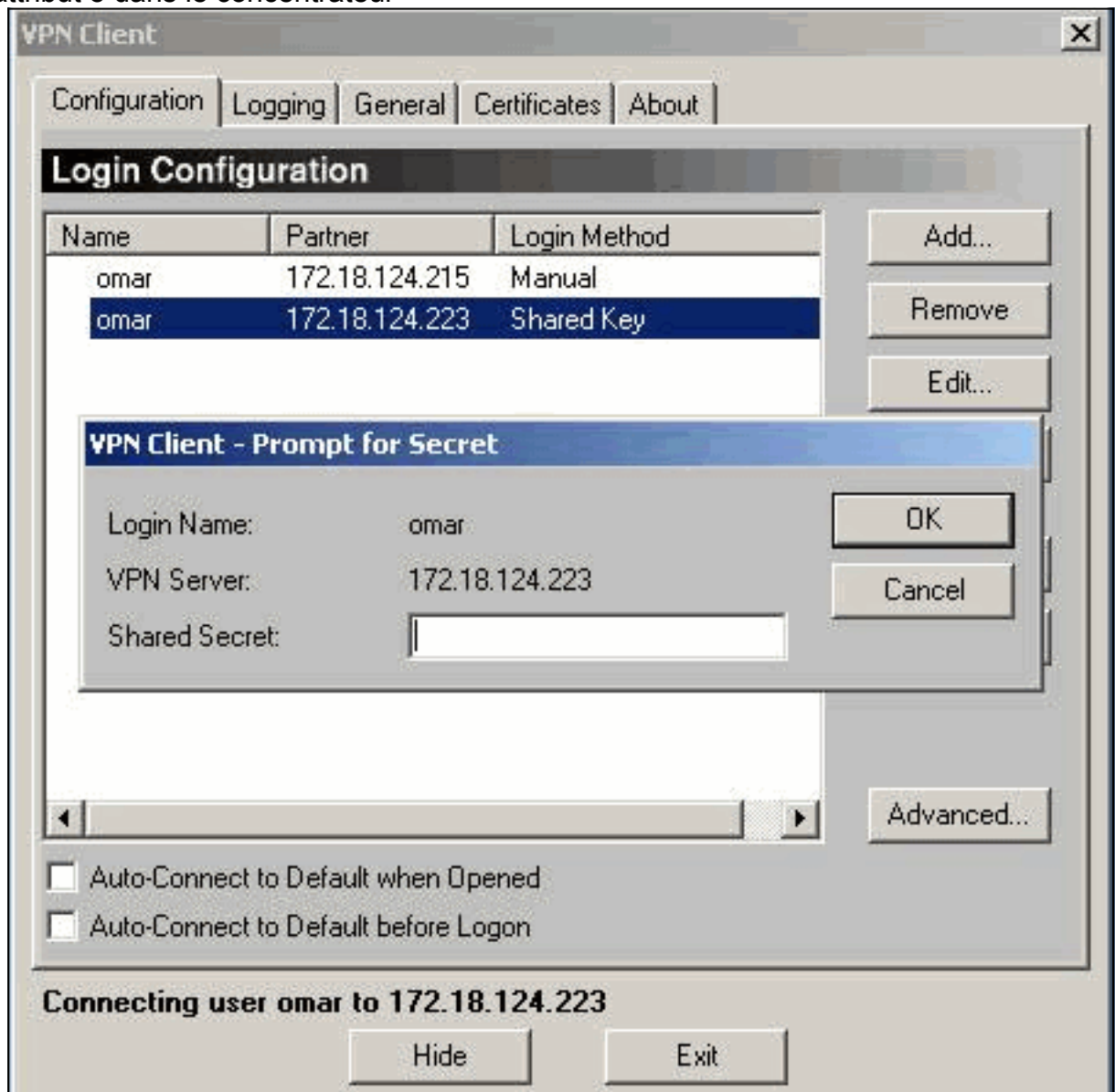
Authentication	Primary	Secondary
Requests	3	na
Accepts	3	na
Rejects	0	na
Challenges	0	na
Retransmissions	0	na
Bad Authenticators	0	na
Malformed Responses	0	na
Packets Dropped	0	na
Pending Requests	0	na
Timeouts	0	na
Unknown Types	0	na

VPN5001\_4B9CBA80>

[Configurer le client VPN](#)

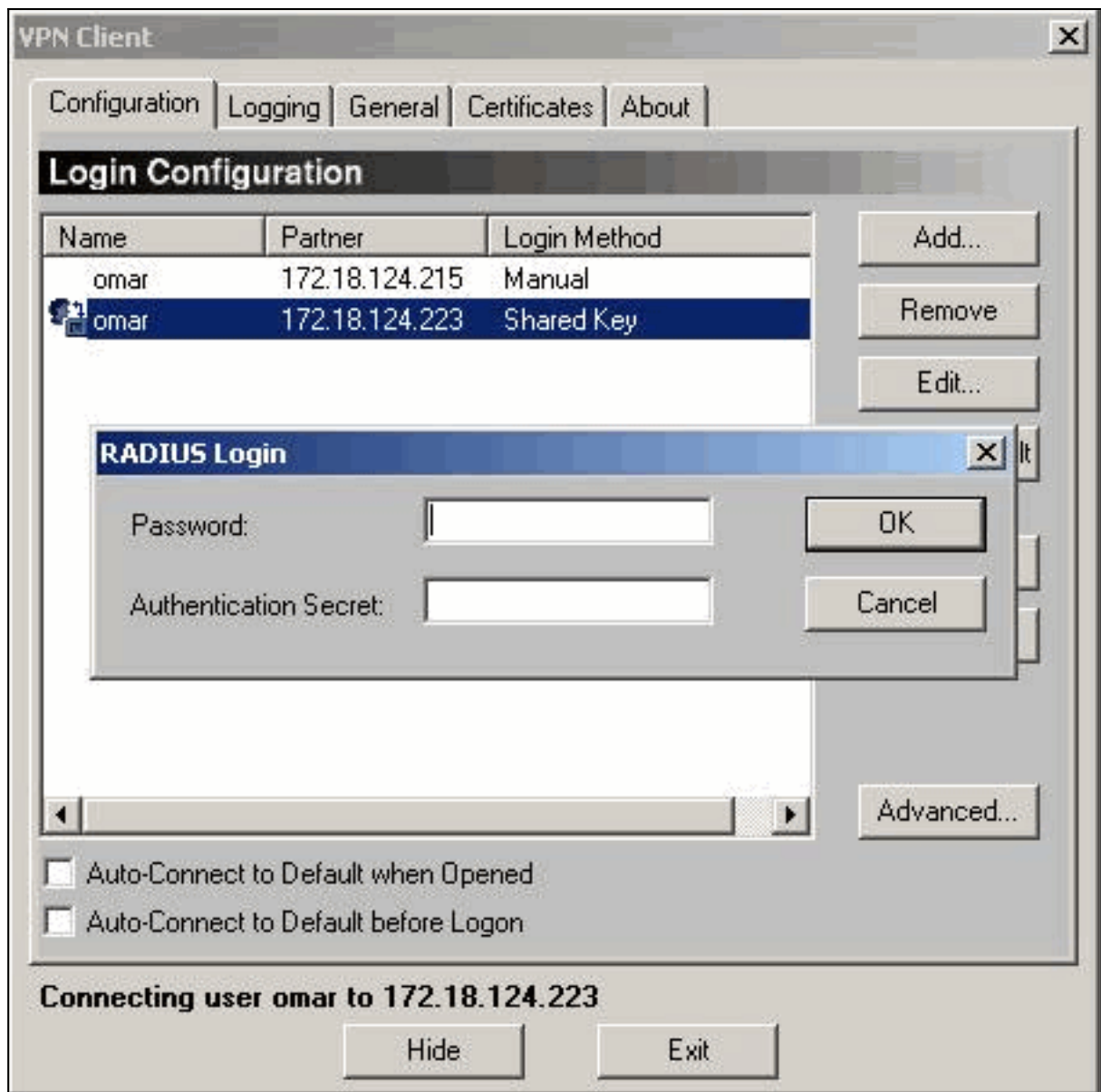
Cette procédure vous guide par la configuration du client vpn.

1. De la boîte de dialogue de client vpn, sélectionnez l'onglet de configuration. Ensuite, de la Client-demande VPN pour la boîte de dialogue secrète, écrivez le secret partagé sous le serveur VPN. Le secret partagé par client vpn est la valeur entrée pour le mot de passe VPN de l'attribut 5 dans le concentrateur



VPN.

2. Après que vous écrivez le secret partagé, vous êtes incité pour un mot de passe et un secret d'authentification. Le mot de passe est votre mot de passe de RAYON pour cet utilisateur, et le secret d'authentification est le secret d'authentification PAP dans [la section de RAYON] du [concentrateur](#)



[VPN](#)

## Logs de concentrateur

```
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>

## Dépannez

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

## Informations connexes

- [Annonce de fin de ventes de Concentrateur VPN de la gamme Cisco 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](#)