

# Configuración de un Concentrador VPN 5000 de Cisco con autenticación externa en un servidor IAS RADIUS de Microsoft Windows 2000.

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configuración del concentrador VPN 5000 de Cisco](#)

[Configuración del servidor RADIUS IAS de Microsoft Windows 2000](#)

[Verificar el resultado](#)

[Configure el cliente VPN](#)

["Registros del concentrador"](#)

[Troubleshoot](#)

[Información Relacionada](#)

## Introducción

Este documento describe los procedimientos utilizados para configurar un Cisco VPN 5000 Concentrator con autenticación externa a un Microsoft Windows 2000 Internet Authentication Server (IAS) con RADIUS.

**Nota:** El protocolo de autenticación por desafío mutuo (CHAP) no funciona. Utilice solamente el protocolo de autenticación de contraseña (PAP). Consulte Cisco bug ID [CSCdt96941](#) ([sólo](#) clientes registrados) para obtener más detalles.

## Prerequisites

### Requirements

No hay requisitos específicos para este documento.

### Componentes Utilizados

La información de este documento se basa en esta versión del software:

- Software del concentrador VPN 5000 de Cisco versión 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.

## Convenciones

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

## Configuración del concentrador VPN 5000 de Cisco

```
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

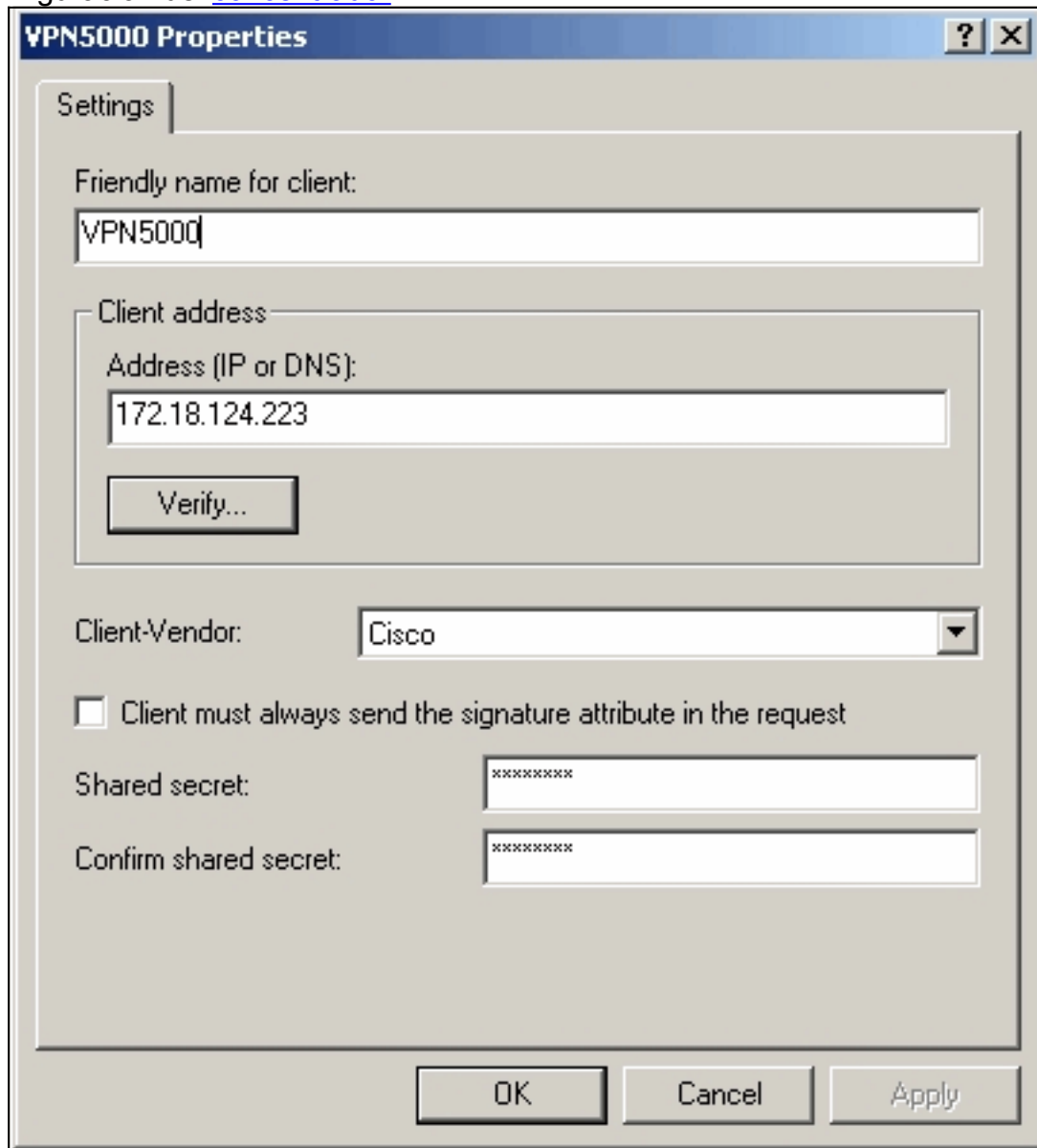
[ Logging ]
Level                = 7
Enabled              = On

Configuration size is 1065 out of 65500 bytes.
VPN5001_4B9CBA80#
```

# Configuración del servidor RADIUS IAS de Microsoft Windows 2000

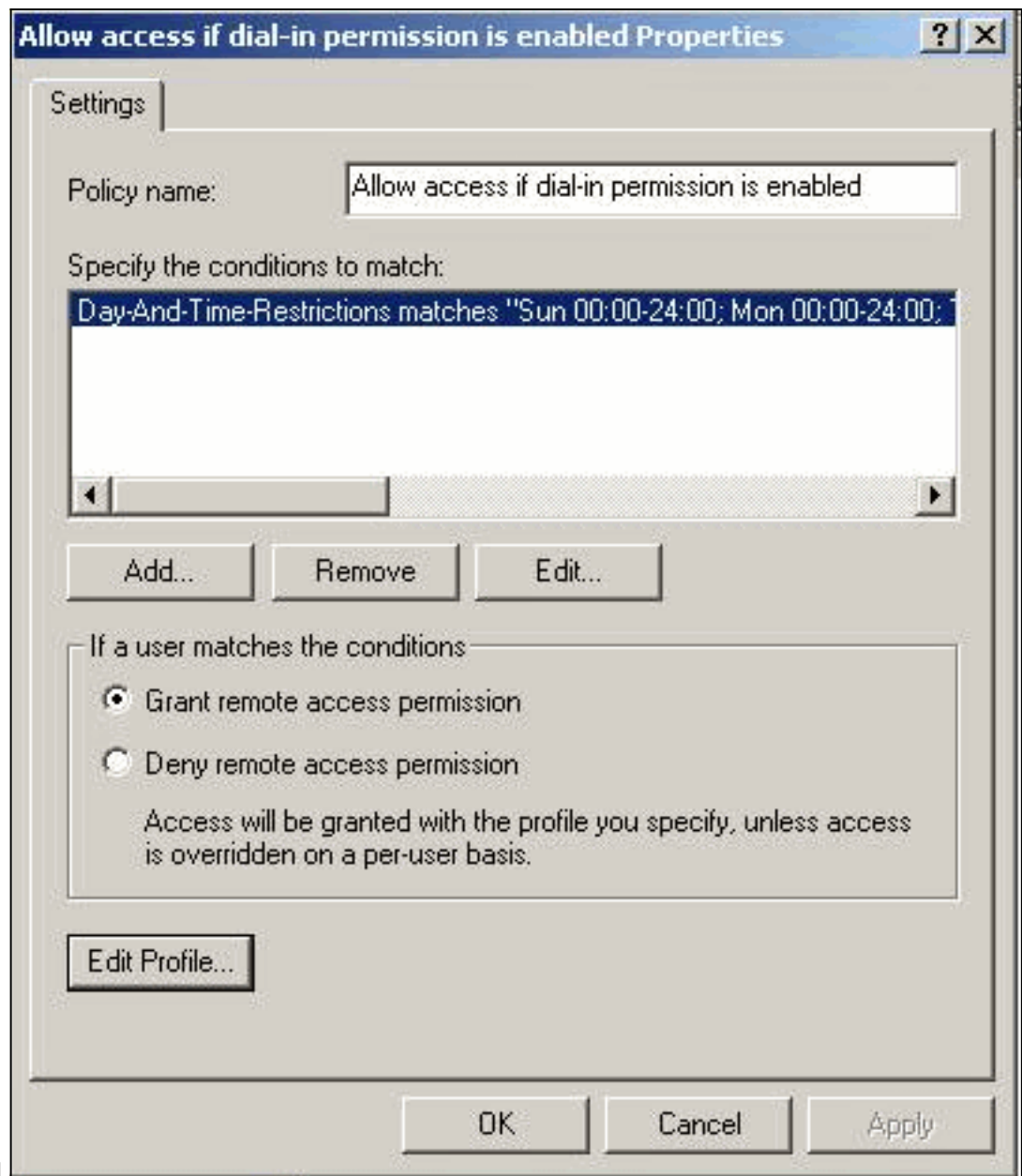
Estos pasos le guiarán a través de una simple configuración del servidor IAS RADIUS de Microsoft Windows 2000.

1. En las propiedades de Microsoft Windows 2000 IAS, seleccione **Clientes** y cree un nuevo cliente. En este ejemplo, se crea una entrada denominada VPN5000. La dirección IP del Cisco VPN 5000 Concentrator es 172.18.124.223. En el cuadro desplegable Cliente-Proveedor, seleccione **Cisco**. El secreto compartido es el secreto en la sección [ RADIUS ] de la configuración del [concentrador](#)



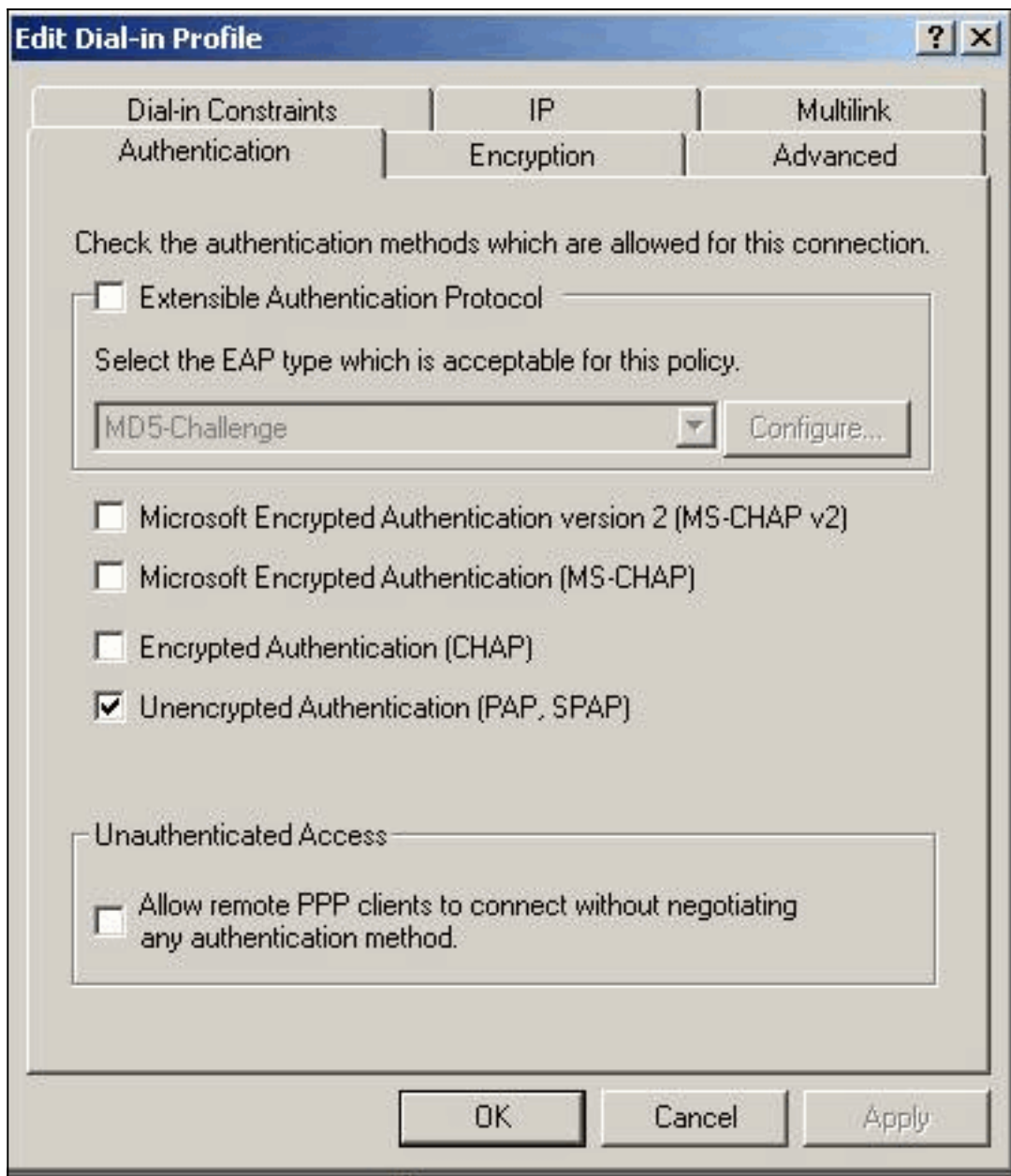
[VPN](#).

2. Bajo las propiedades de la política de acceso remoto, seleccione **Conceder permiso de acceso remoto** en la sección "Si un usuario coincide con las condiciones" y luego haga clic



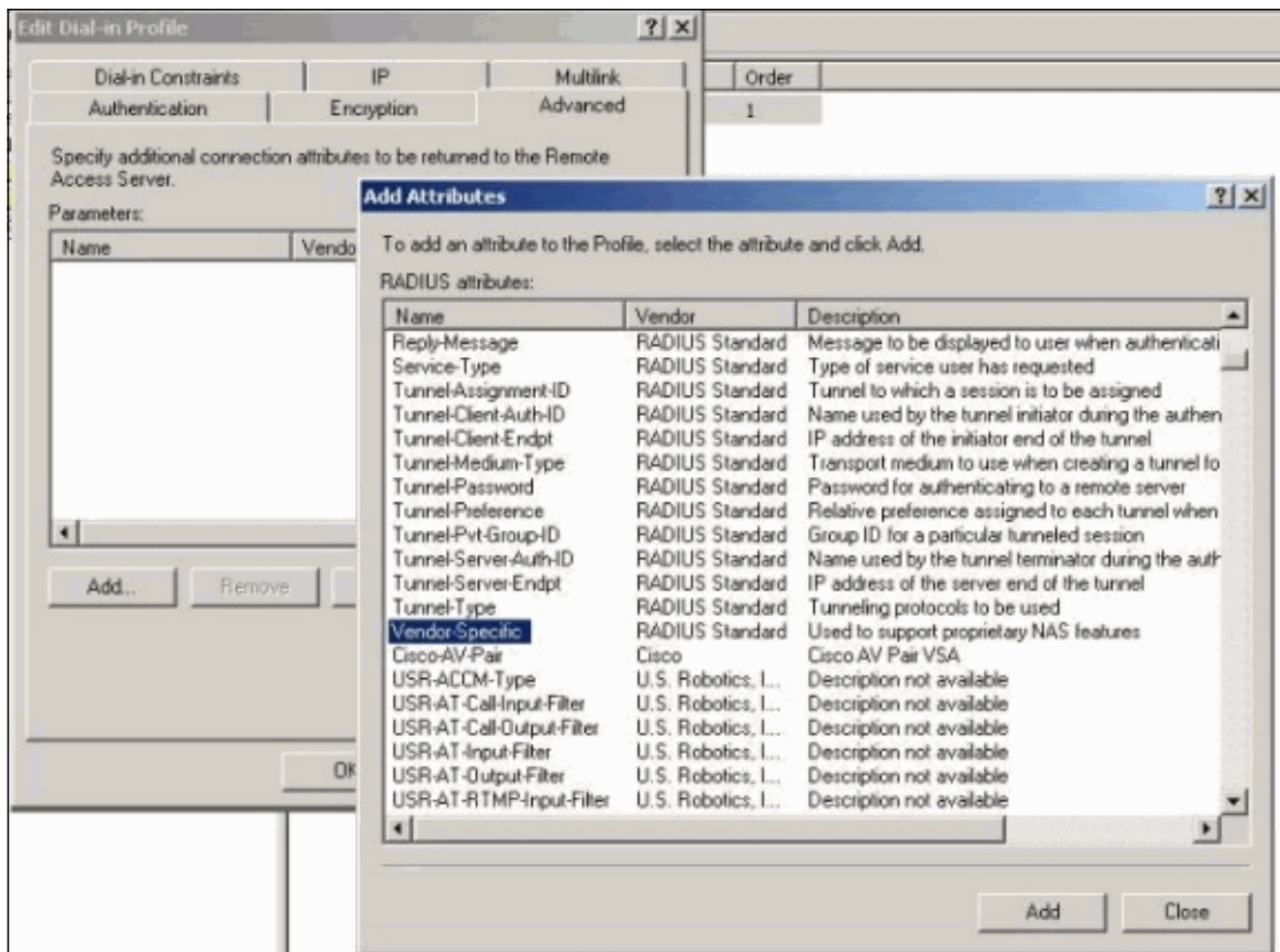
en **Editar perfil.**

3. Haga clic en la ficha Authentication (Autenticación) y asegúrese de que sólo **esté** seleccionada la autenticación no cifrada (PAP,

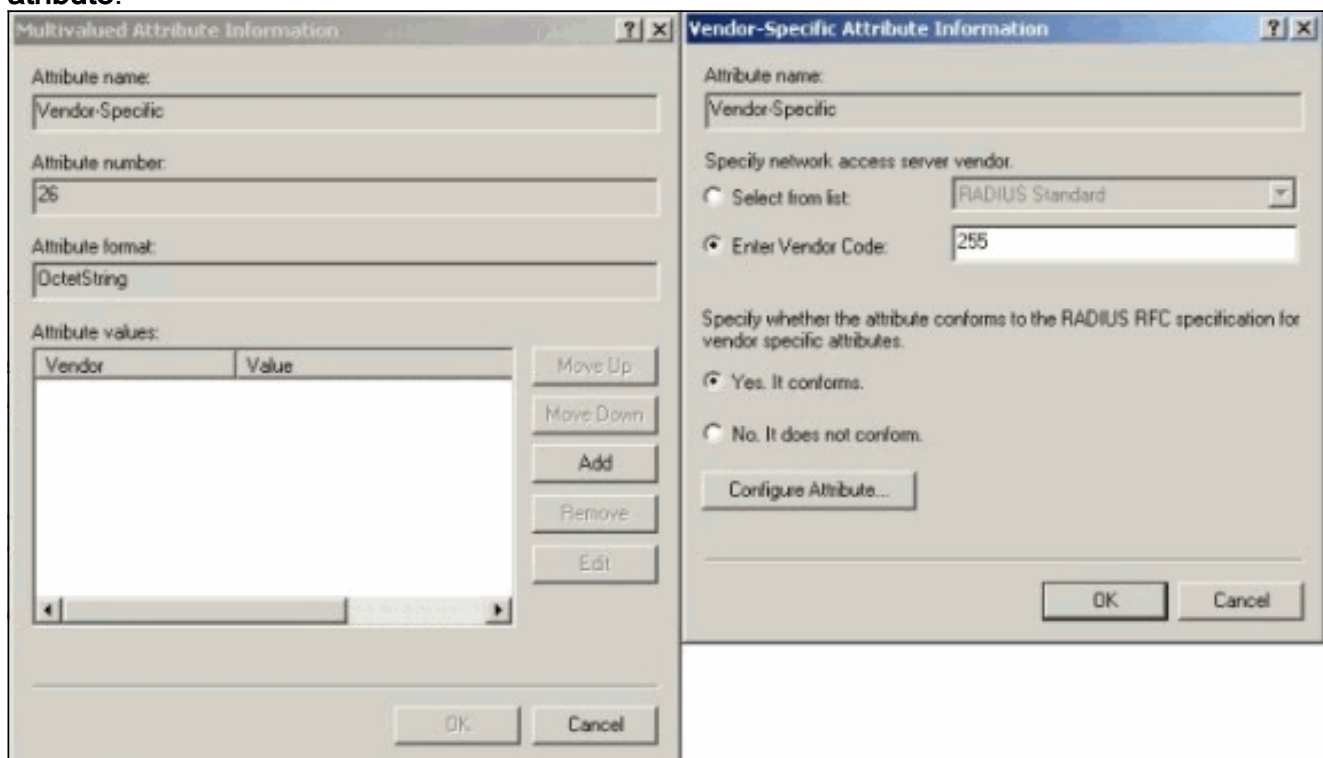


SPAP).

4. Seleccione la pestaña Advanced, haga clic en **Add** y seleccione **Vendor-Specific**.



5. En el cuadro de diálogo Información de atributo multivalor para el atributo específico del proveedor, haga clic en **Agregar** para ir al cuadro de diálogo Información de atributo específico del proveedor. Seleccione **Introducir código del proveedor** e introduzca **255** en el cuadro adyacente. A continuación, seleccione **Yes (Sí)**. **Se ajusta** y hace clic en **Configurar atributo**.



6. En el cuadro de diálogo Configurar VSA (compatible con RFC), escriba **4** para el número de atributo asignado por el proveedor, escriba **String** para el formato de atributo e introduzca

**rtp-group** (nombre del grupo de VPN en el concentrador Cisco VPN 5000) para el valor de atributo. Haga clic en **Aceptar** y repita el paso



Configure VSA (RFC compliant)

Vendor-assigned attribute number:  
4

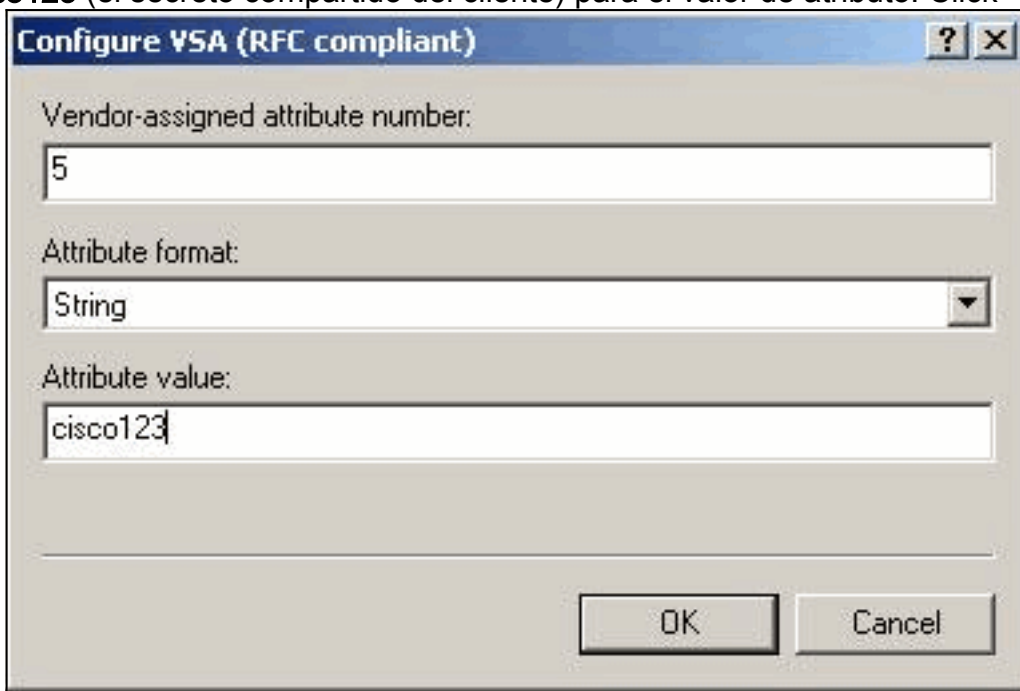
Attribute format:  
String

Attribute value:  
rtp-group

OK Cancel

5.

7. En el cuadro de diálogo Configurar VSA (compatible con RFC), escriba **4** para el número de atributo asignado por el proveedor, escriba **String** para el formato de atributo e introduzca **cisco123** (el secreto compartido del cliente) para el valor de atributo. Click



Configure VSA (RFC compliant)

Vendor-assigned attribute number:  
5

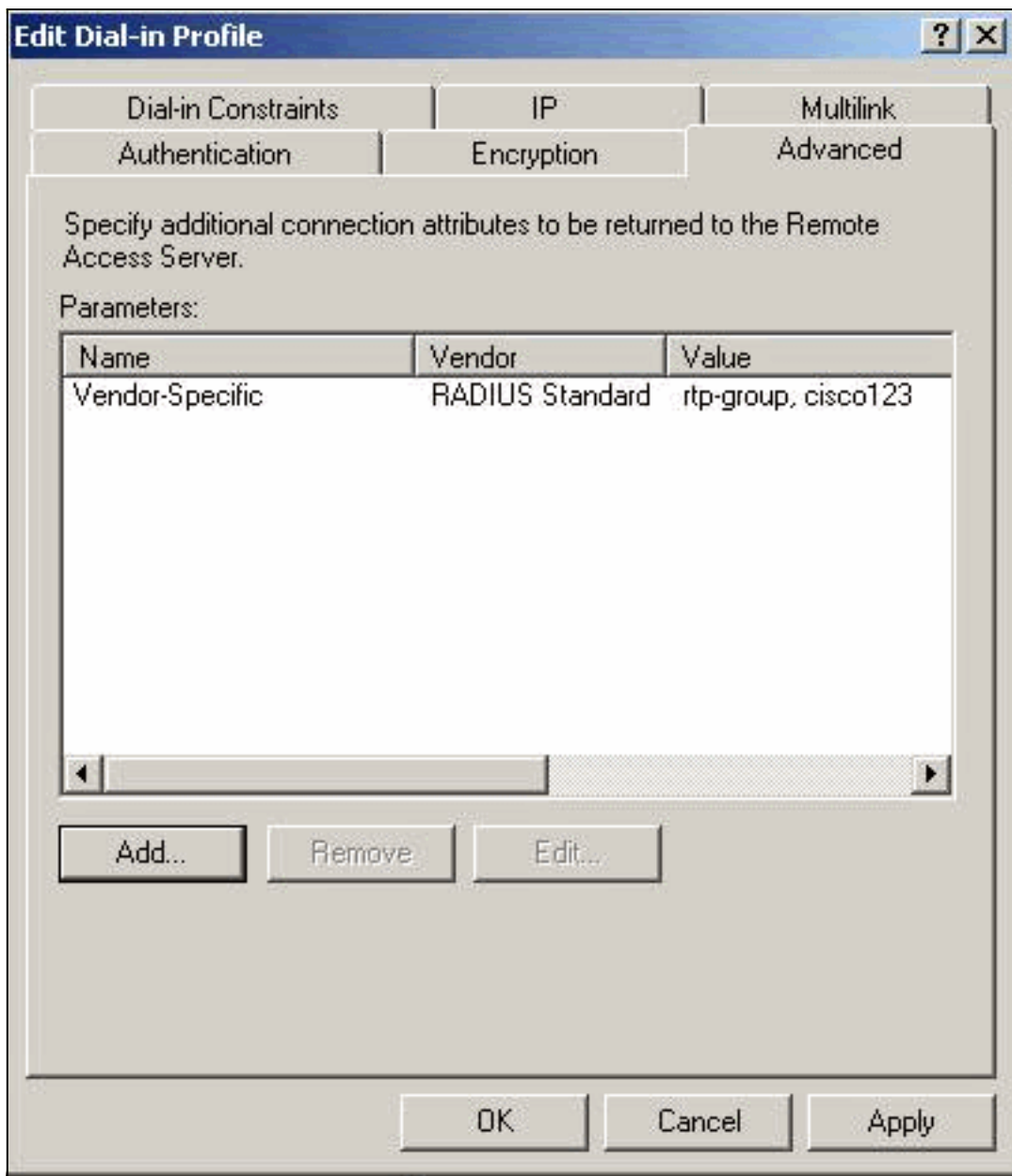
Attribute format:  
String

Attribute value:  
cisco123

OK Cancel

OK.

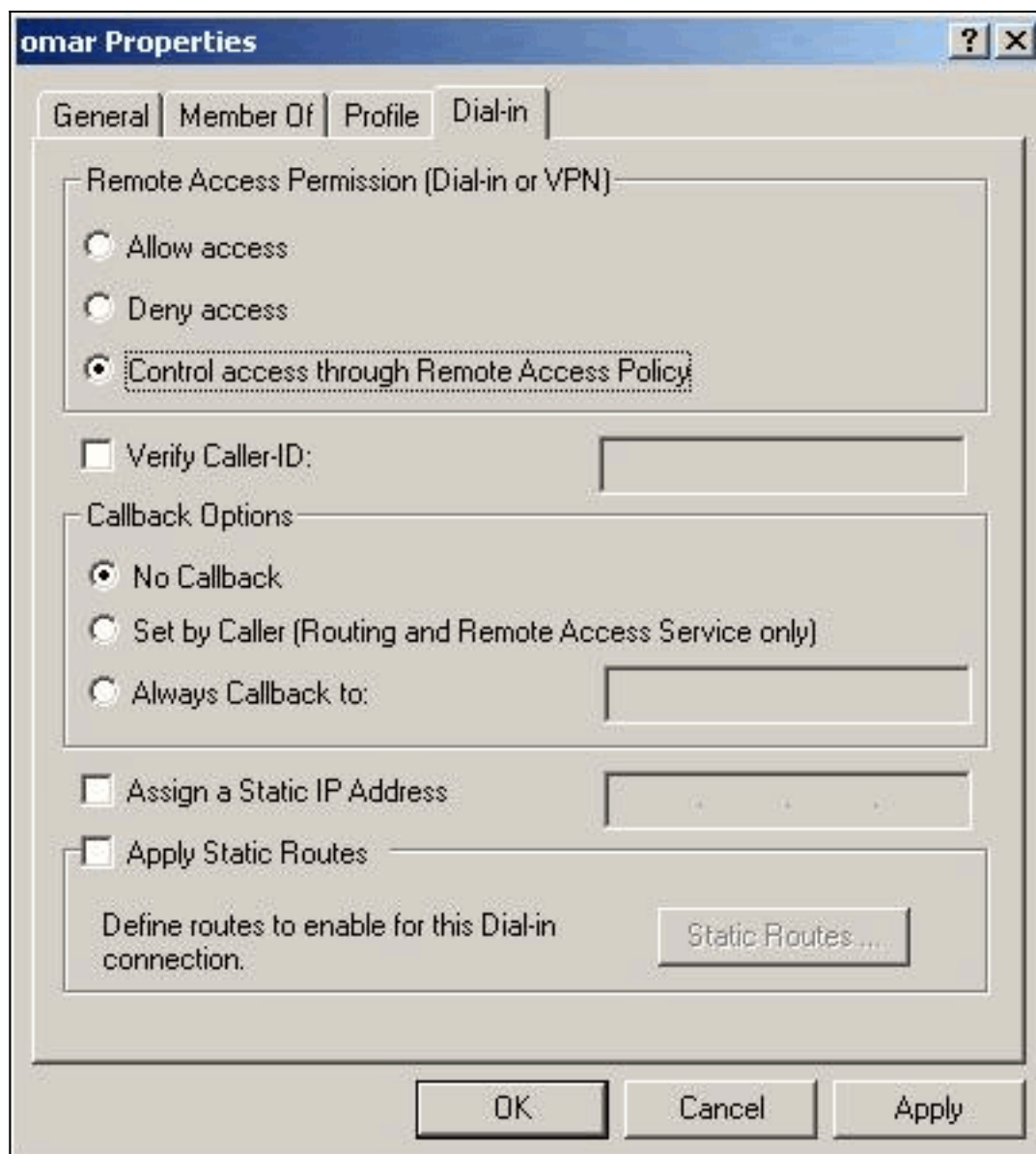
8. El atributo Específico del proveedor contiene dos valores (grupo y contraseña de



VPN).

9. En las propiedades de usuario, haga clic en la ficha Marcar y asegúrese de que está seleccionado **Control access through Remote Access Policy**





## Verificar el resultado

Esta sección proporciona información que puede utilizar para confirmar que su configuración funciona correctamente.

La herramienta [Output Interpreter](#) (sólo para clientes registrados) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

- **show radius statistics**—Muestra las estadísticas de paquetes para la comunicación entre el VPN Concentrator y el servidor RADIUS predeterminado identificado por la sección RADIUS.
- **show radius config**: muestra la configuración actual para los parámetros RADIUS.

Este es el resultado 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>

Este es el resultado del comando **show radius config**.

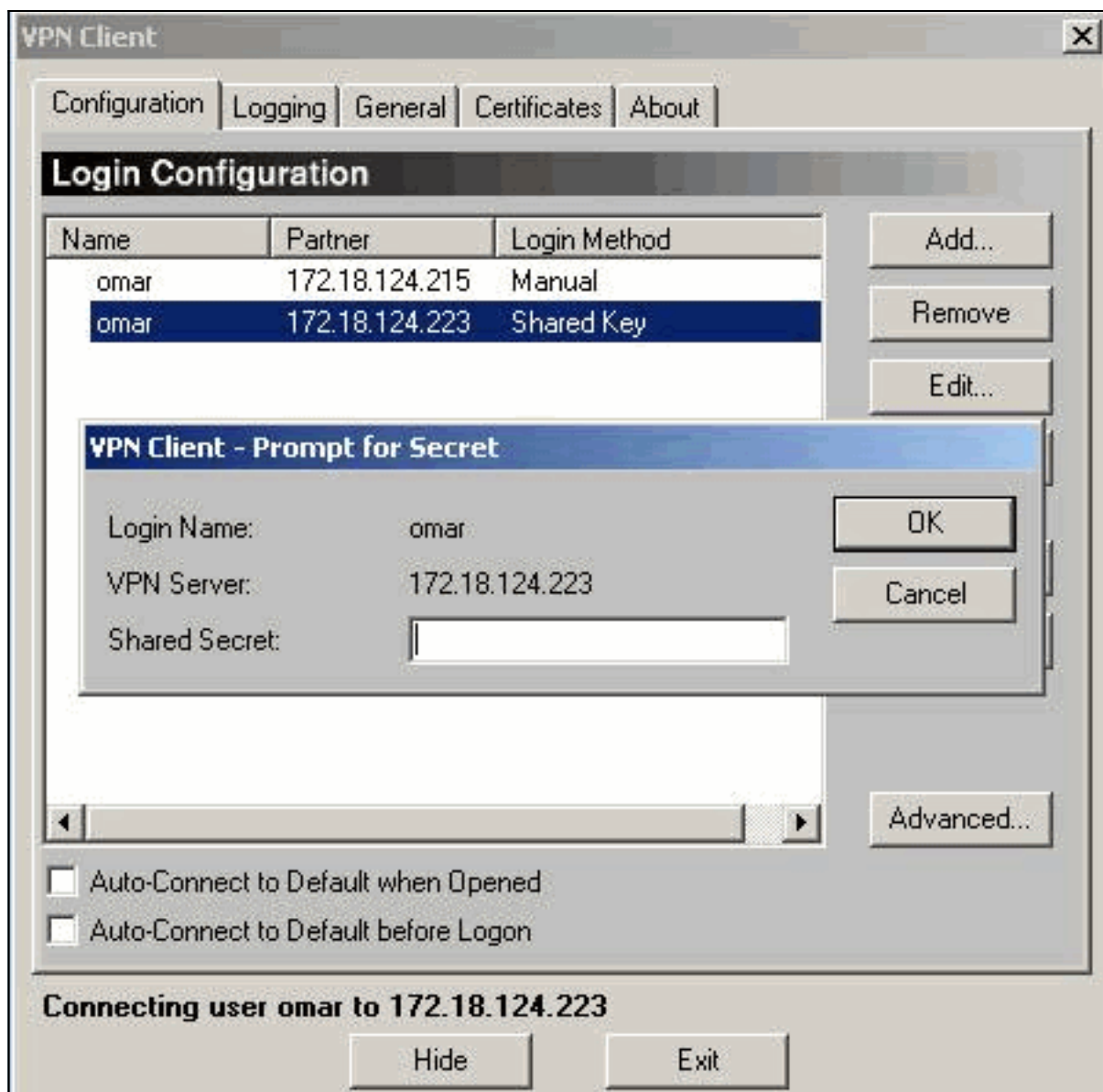
RADIUS	State	UDP	CHAP16
Authentication	On	1812	No
Accounting	Off	1813	n/a
Secret	'radiuspassword'		

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

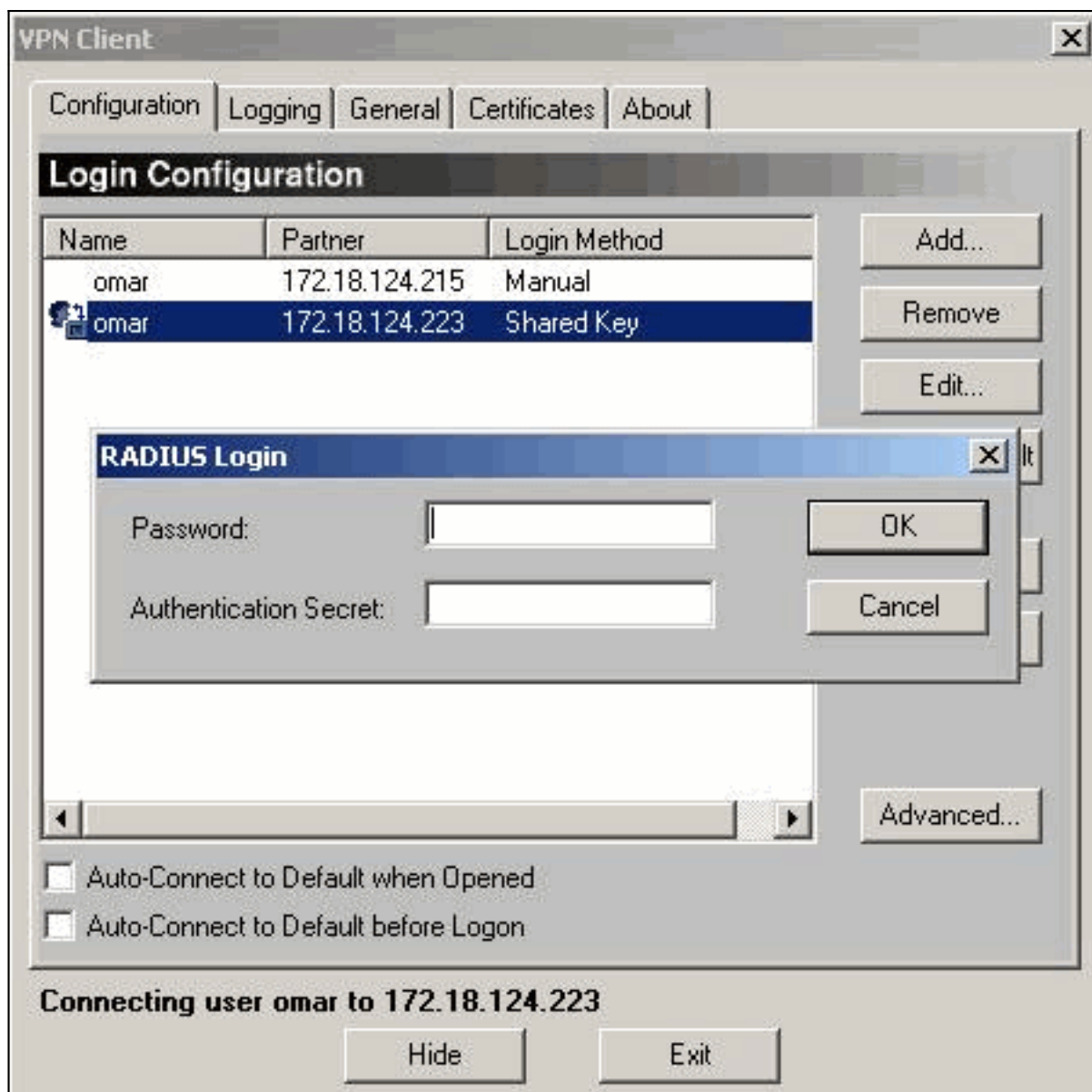
## [Configure el cliente VPN](#)

Este procedimiento le guía a través de la configuración del VPN Client.

1. En el cuadro de diálogo VPN Client, seleccione la ficha Configuration . A continuación, en el cuadro de diálogo Solicitud de cliente VPN para secreto, introduzca el secreto compartido en el servidor VPN. El secreto compartido de VPN Client es el valor ingresado para la contraseña VPN del atributo 5 en el VPN Concentrator.



2. Después de introducir el secreto compartido, se le solicitará una contraseña y un secreto de autenticación. La contraseña es su contraseña RADIUS para ese usuario, y el secreto de autenticación es el secreto de autenticación PAP en la sección [ RADIUS ] de [VPN Concentrator](#).



## [“Registros del concentrador”](#)

```
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
```

## [Troubleshoot](#)

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

## [Información Relacionada](#)

- [Anuncio de fin de venta de los concentradores Serie VPN 5000 de Cisco](#)
- [Página de soporte del concentrador VPN 5000 de Cisco](#)

- [Página de soporte para Cisco VPN 5000 Client](#)
- [Página de soporte de IPSec](#)
- [Soporte Técnico - Cisco Systems](#)