Cisco Airespace VSA en el ejemplo de la configuración de servidor de RADIUS de Microsoft IAS

Contenido

Introducción
Prerequisites
Requisitos
Componentes usados
Convenciones
Antecedentes
Configure IAS para Airespace VSA
Configure el WLC como cliente AAA en IAS
Configure la política de acceso remoto en IAS
Ejemplo de configuración
Verifique
Troubleshooting
Información Relacionada

Introducción

Este documento le muestra cómo configurar un servidor del servicio de autenticación por Internet de Microsoft (IAS) para utilizar los atributos específicos del vendedor de Cisco Airespace (VSA). El Vendor Code (Código de proveedor) para los VSA de Cisco Airespace es 14179.

Prerequisites

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento de cómo configurar a un servidor IAS
- Conocimiento de la configuración reguladores inalámbricos del LAN de los Puntos de acceso ligeros (revestimientos) y de Cisco (WLCs)
- El conocimiento de Cisco unificó las soluciones de la seguridad de red inalámbrica

Componentes usados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Microsoft Windows 2000 Server con IAS
- Cisco 4400 WLC que funciona con la versión de software 4.0.206.0
- Cisco 1000 Series LAP
- adaptador de red inalámbrica de cliente del 802.11 a/b/g con los firmwares 2.5
- Aironet Desktop Utility (ADU) versión 2.5

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Note: Este documento se piensa para dar al programa de lectura un ejemplo en la configuración requerida en el servidor IAS para utilizar Cisco Airespace VSA. La configuración de servidor IAS presentada en este documento se ha probado en el laboratorio y trabaja como se esperaba. Si usted tiene problema que configura al servidor IAS, entre en contacto con Microsoft para la ayuda. El TAC de Cisco no utiliza la Configuración del servidor de Microsoft Windows.

Este documento asume que el WLC está configurado para la operación básica y que los revestimientos están registrados al WLC. Si usted es usuario nuevo que intenta poner el WLC para la operación básica con los revestimientos, refiera al registro ligero AP (REVESTIMIENTO) a un regulador LAN de la Tecnología inalámbrica (WLC).

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Antecedentes

En la mayoría de los sistemas LAN de la Tecnología inalámbrica (red inalámbrica (WLAN)), cada red inalámbrica (WLAN) tiene una directiva estática que se aplique a todos los clientes asociados a un Service Set Identifier (SSID). Aunque sea potente, este método tenga limitaciones porque requiere a los clientes asociarse a diversos SSID para heredar diverso QoS y las políticas de seguridad.

Sin embargo, la solución de LAN inalámbrica de Cisco utiliza el establecimiento de una red de la identidad, que permite que la red haga publicidad de un solo SSID y de los usuarios específicos para heredar diverso QoS o las políticas de seguridad basadas en sus perfiles de usuario. Las directivas específicas que usted puede controlar usando el establecimiento de una red de la identidad incluyen:

- **Calidad de servicio** — Cuando es presente en un acceso a RADIUS valide, el valor del QoS-nivel reemplaza el valor de QoS especificado en el perfil de la red inalámbrica (WLAN).
- **ACL** — Cuando el atributo de la lista de control de acceso (ACL) está presente en el acceso a RADIUS valide, el sistema aplica el ACL-nombre a la estación del cliente después de que autentique. Esto reemplaza cualquier ACL que se asigne al interfaz.
- **VLA N** — Cuando un Interfaz-nombre o una VLA N-etiqueta del VLA N está presente en un acceso a RADIUS valide, el sistema coloca al cliente en un interfaz específico.
- **Identificación de la red inalámbrica (WLAN)** — Cuando el atributo WLAN-ID está presente en el acceso a RADIUS valide, el sistema aplica el WLAN-ID (SSID) a la estación del cliente después de que autentique. La identificación de la red inalámbrica (WLAN) es enviada por el

WLC en todos los casos de la autenticación excepto IPSec. En caso de la autenticación Web, si el WLC recibe un atributo WLAN-ID en la respuesta de autenticación del servidor AAA, y de él no hace juego la identificación de la red inalámbrica (WLAN), autenticación se rechaza. Otros tipos de métodos de seguridad no hacen esto.

- **Valor DSCP** — Cuando es presente en un acceso a RADIUS valide, el valor DSCP reemplaza el valor DSCP especificado en el perfil de la red inalámbrica (WLAN).
- **802.1p-Tag** — Cuando es presente en un acceso a RADIUS valide, el valor 802.1p reemplaza el valor por defecto especificado en el perfil de la red inalámbrica (WLAN).

Note: La característica del VLA N utiliza solamente la filtración, el 802.1x, y el Acceso protegido de Wi-Fi (WPA) MAC. La característica del VLA N no utiliza la autenticación Web o IPSec. La base de datos del filtro del MAC local del sistema operativo se ha extendido para incluir el nombre del interfaz. Esto permite que los filtros del MAC local especifiquen qué interfaz debe ser asignado el cliente. Un servidor de RADIUS separado puede también ser utilizado, pero el servidor de RADIUS debe ser definido usando los menús de seguridad.

Refiera a configurar el establecimiento de una red de la identidad para más información sobre el establecimiento de una red de la identidad.

Configure IAS para Airespace VSA

Para configurar IAS para Airespace VSA, usted necesita completar estos pasos:

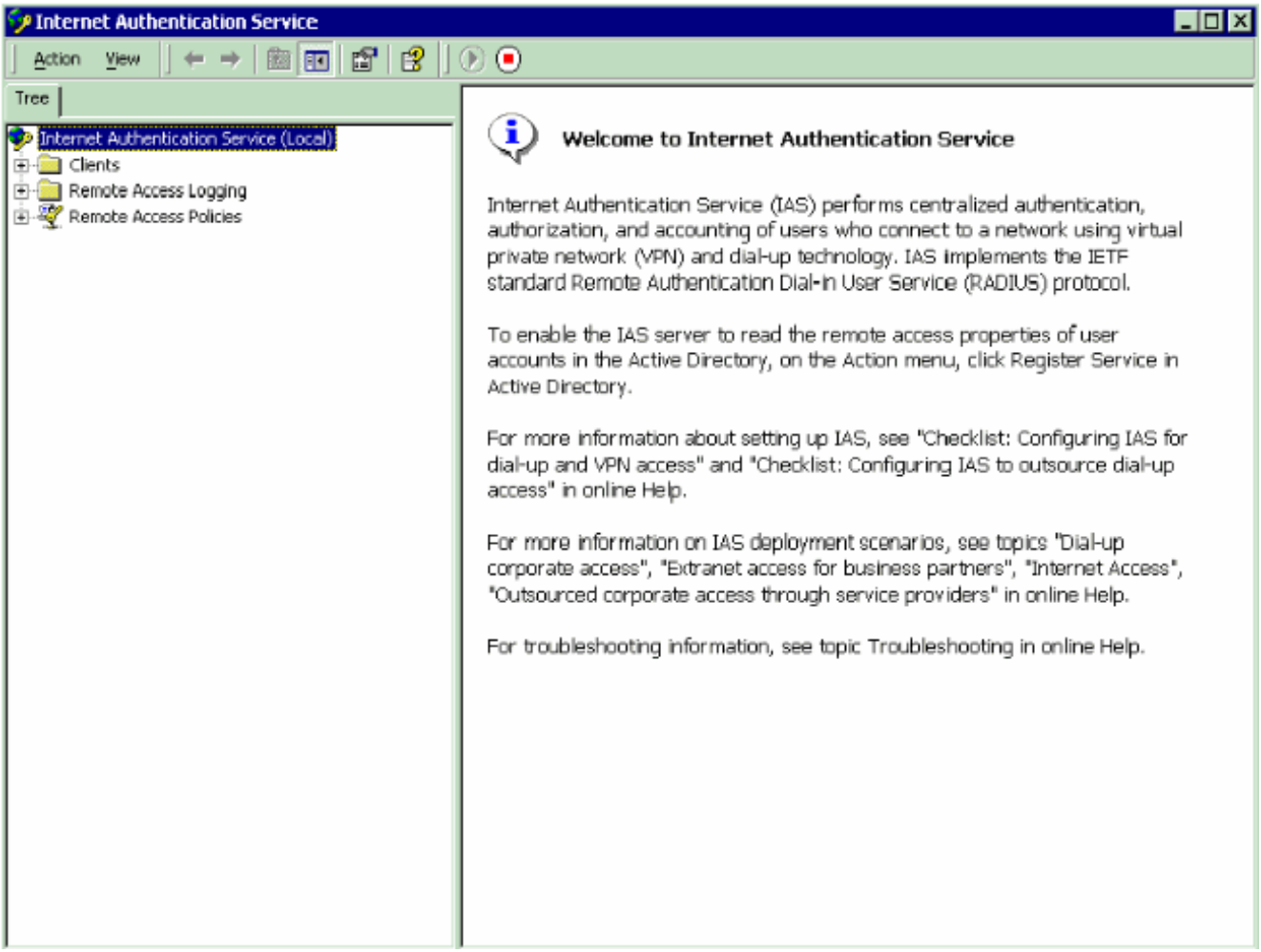
1. Configure el WLC como cliente AAA en IAS
2. Configure la política de acceso remoto en IAS

Note: Los VSA se configuran bajo política de acceso remoto.

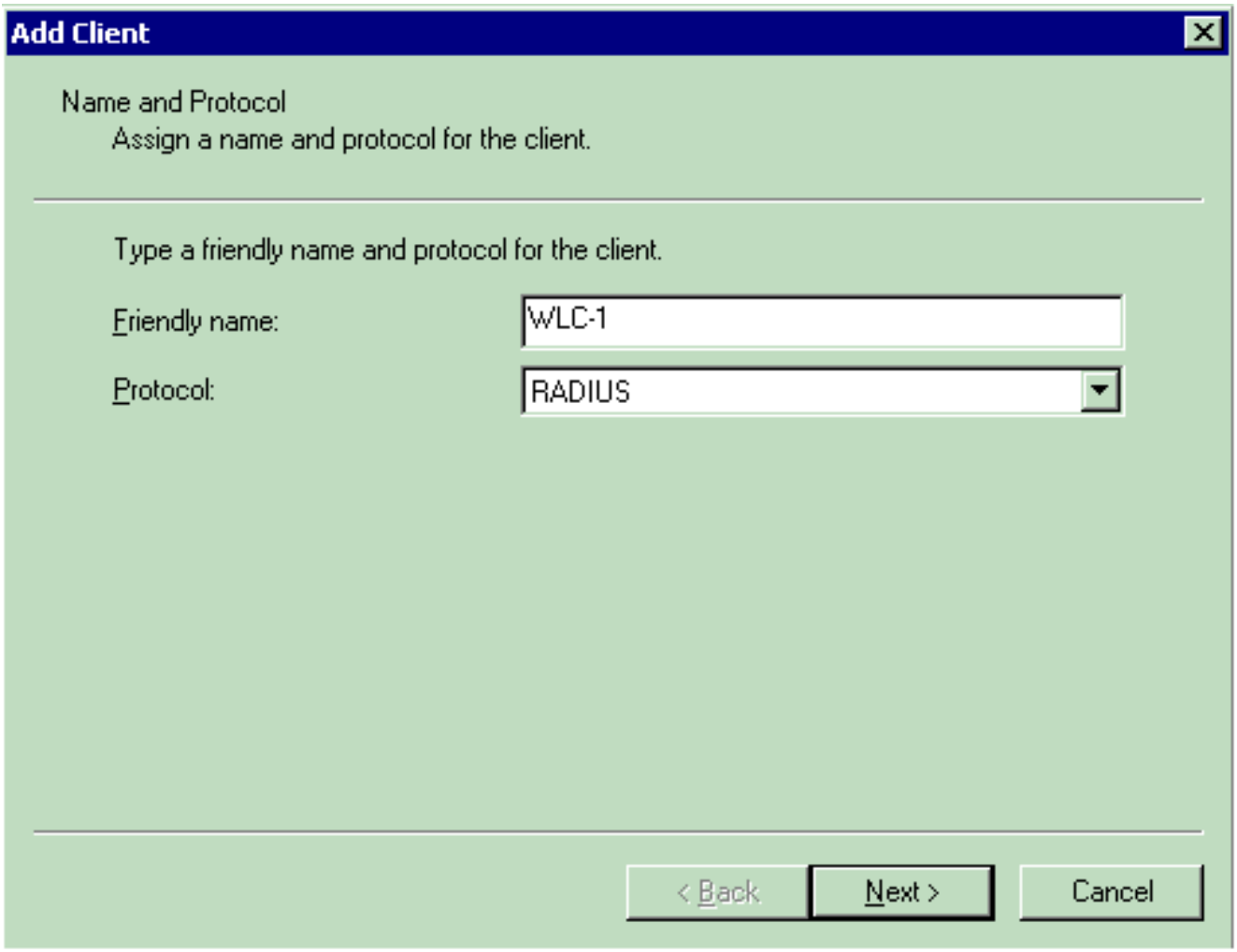
Configure el WLC como cliente AAA en IAS

Complete estos pasos para configurar el WLC como cliente AAA en IAS:

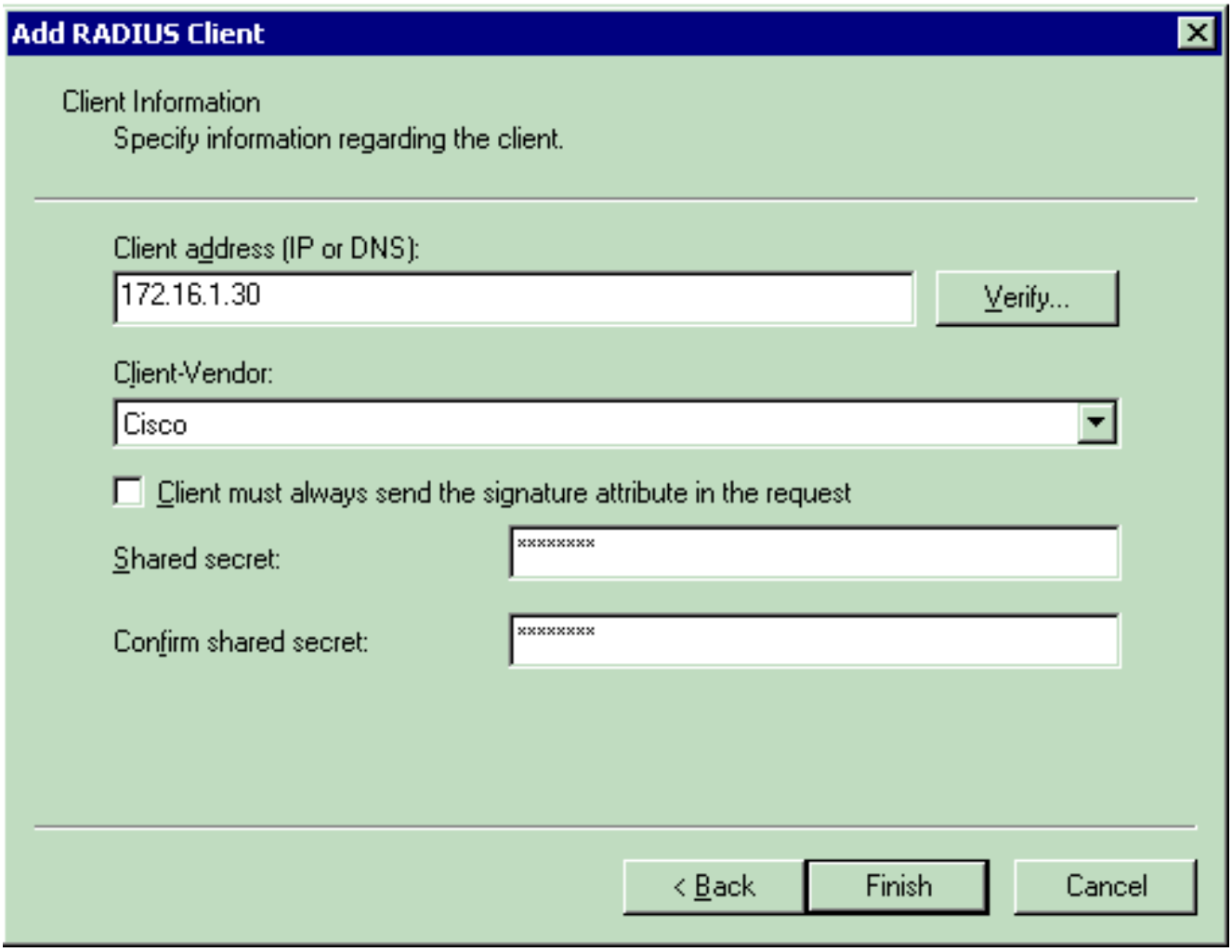
1. Haga clic los **programas > el Administrative Tools (Herramientas administrativas) > Internet Authentication Service (Servicio de autenticación de Internet)** para lanzar IAS en el servidor de Microsoft
   2000.



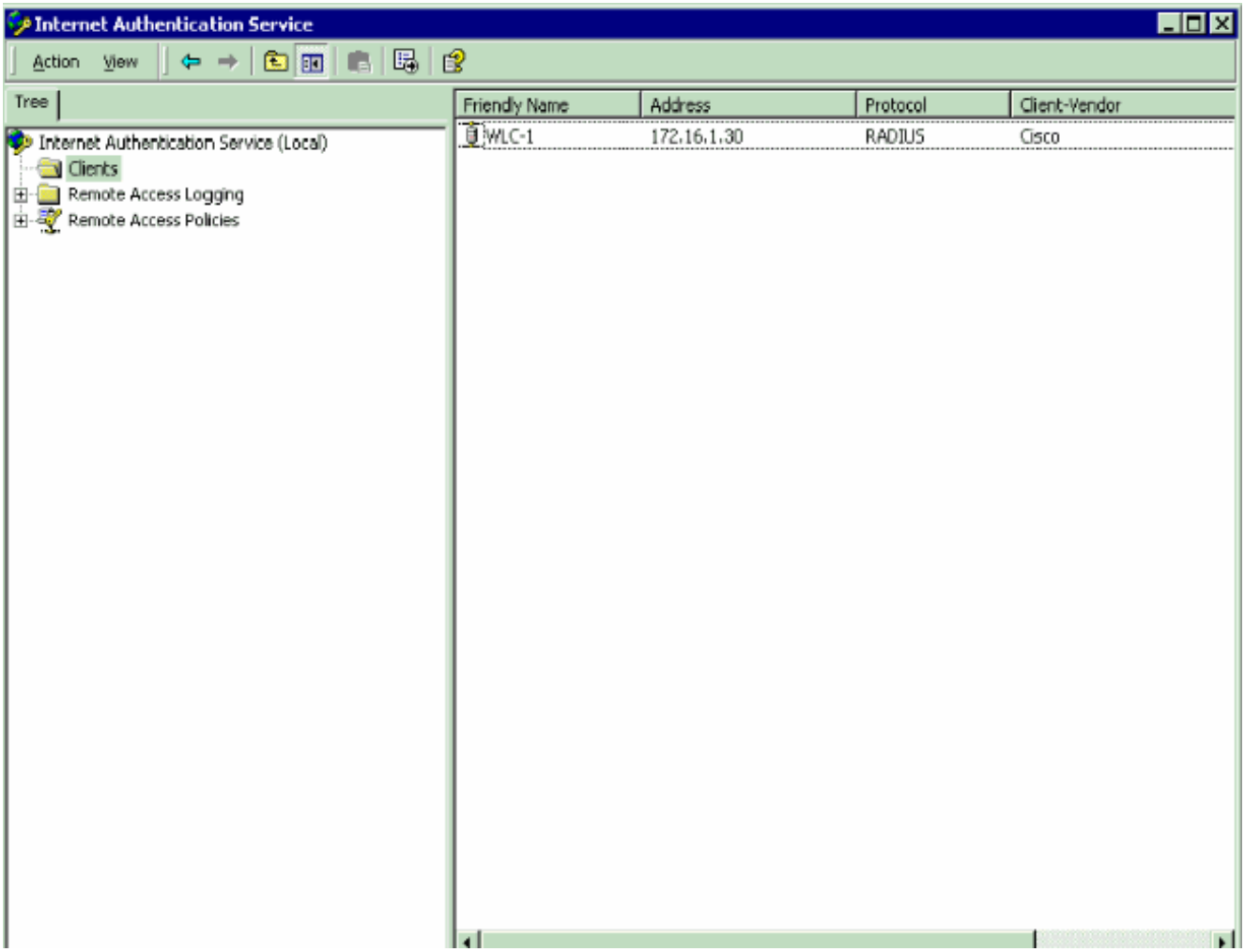
2. Haga clic derecho la carpeta de los **clientes** y elija al **nuevo cliente** para agregar a un nuevo cliente RADIUS.
3. En la ventana del cliente del agregar, ingrese el nombre del cliente y elija el **RADIO** como el protocolo. Entonces, haga clic **después**.En este ejemplo, el Nombre del cliente es *WLC-1*.**Note**: Por abandono, el protocolo se fija al RADIUS.



4. En la ventana del cliente del RADIO del agregar, ingrese el **IP address del cliente**, el Cliente-**vendedor**, y el **secreto compartido**. Después de que usted ingrese la información del cliente, haga clic el **final**.Este ejemplo muestra a un cliente nombrado *WLC-1* con una dirección IP de *172.16.1.30*, fijan al Cliente-vendedor a *Cisco*, y el secreto compartido es *cisco123*:



Con esta información, el WLC WLC-1 nombrado se agrega como cliente AAA del servidor IAS.

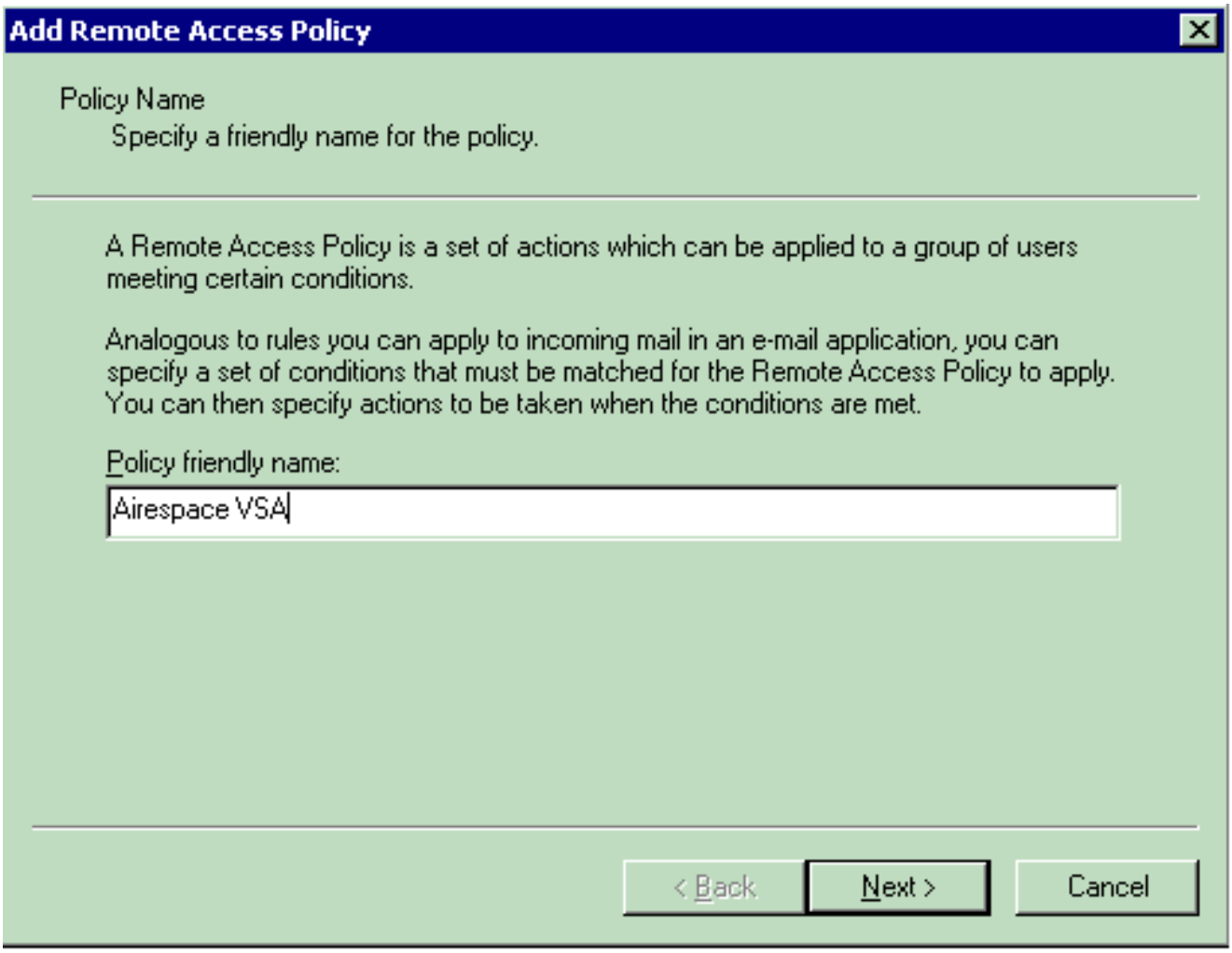


El siguiente paso es crear una política de acceso remoto y configurar los VSA.

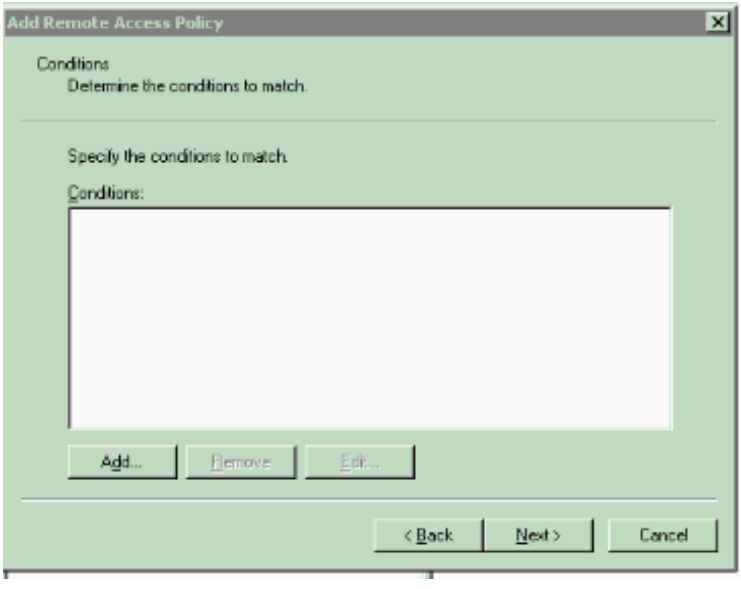
Configure la política de acceso remoto en IAS

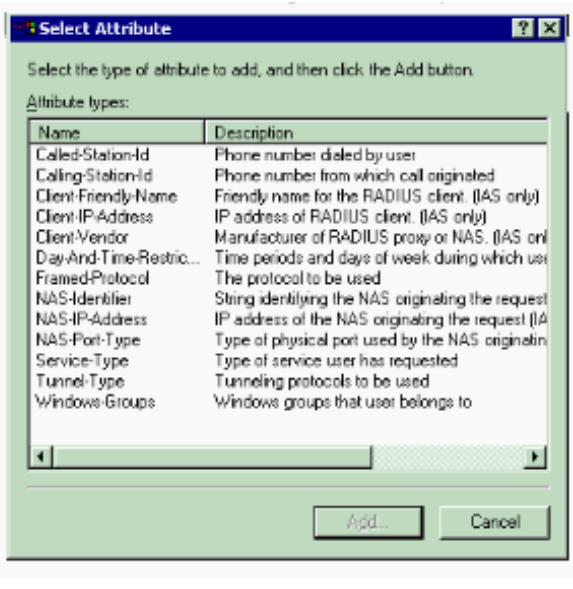
Complete estos pasos para configurar una nueva política de acceso remoto en IAS:

1. Haga clic derecho las **políticas de acceso remoto** y elija la **nueva directiva remota de AcceMSss**.La ventana Name de la directiva aparece.
2. Ingrese el nombre de la directiva y haga clic **después**.

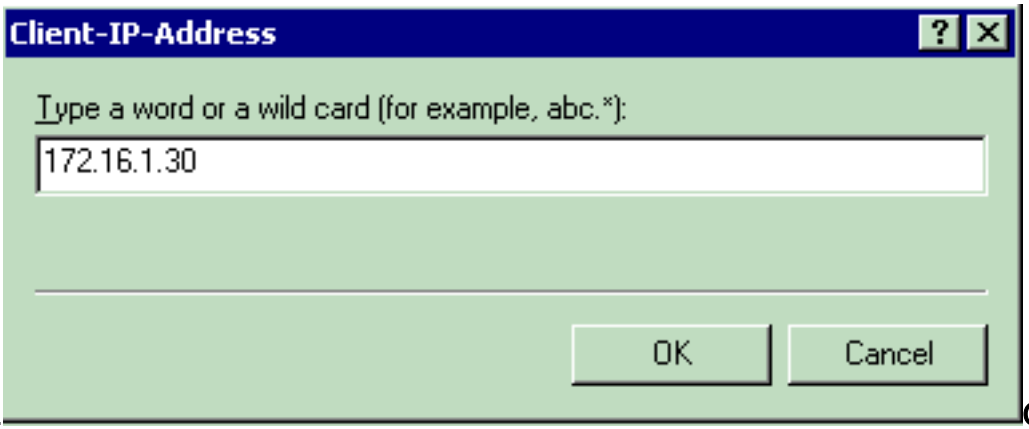


3. En la próxima ventana, seleccione las condiciones las cuales la política de acceso remoto solicitará. El tecleo **agrega** para seleccionar las condiciones.

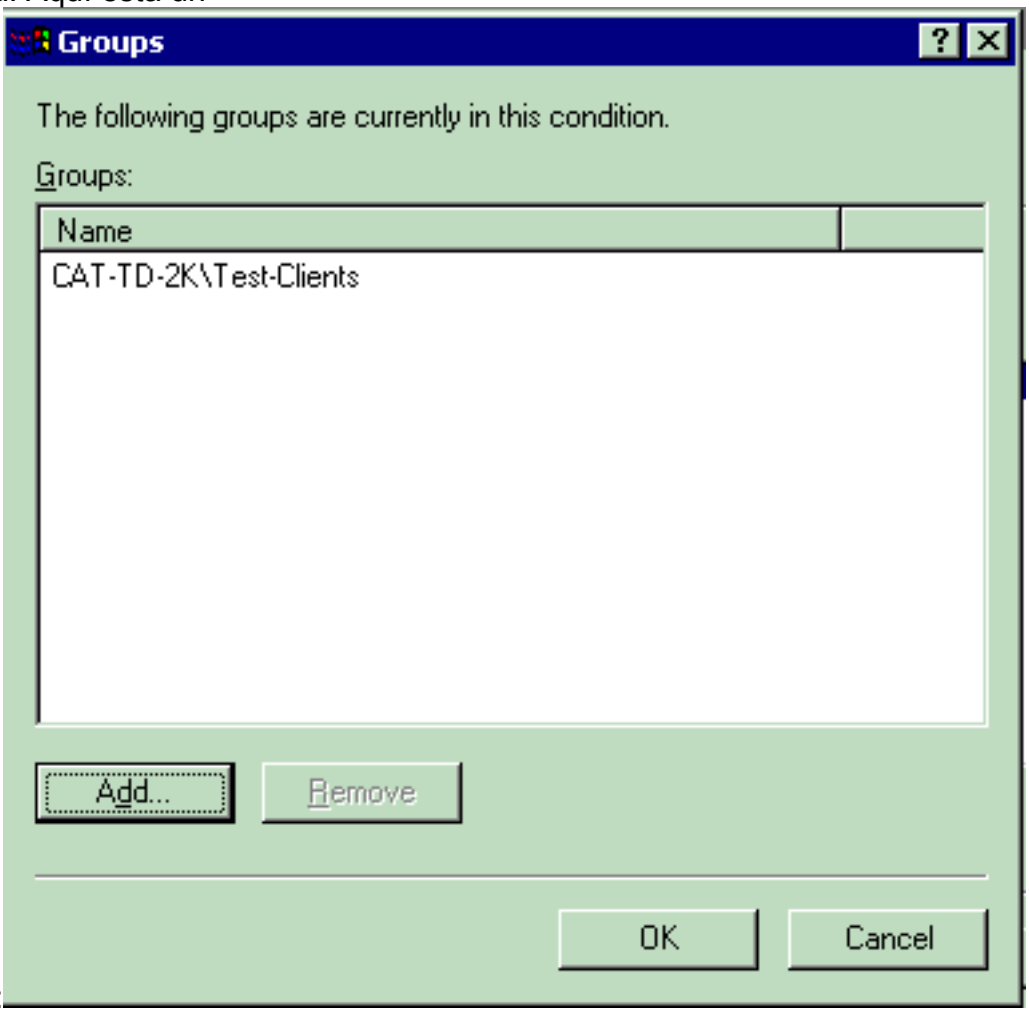




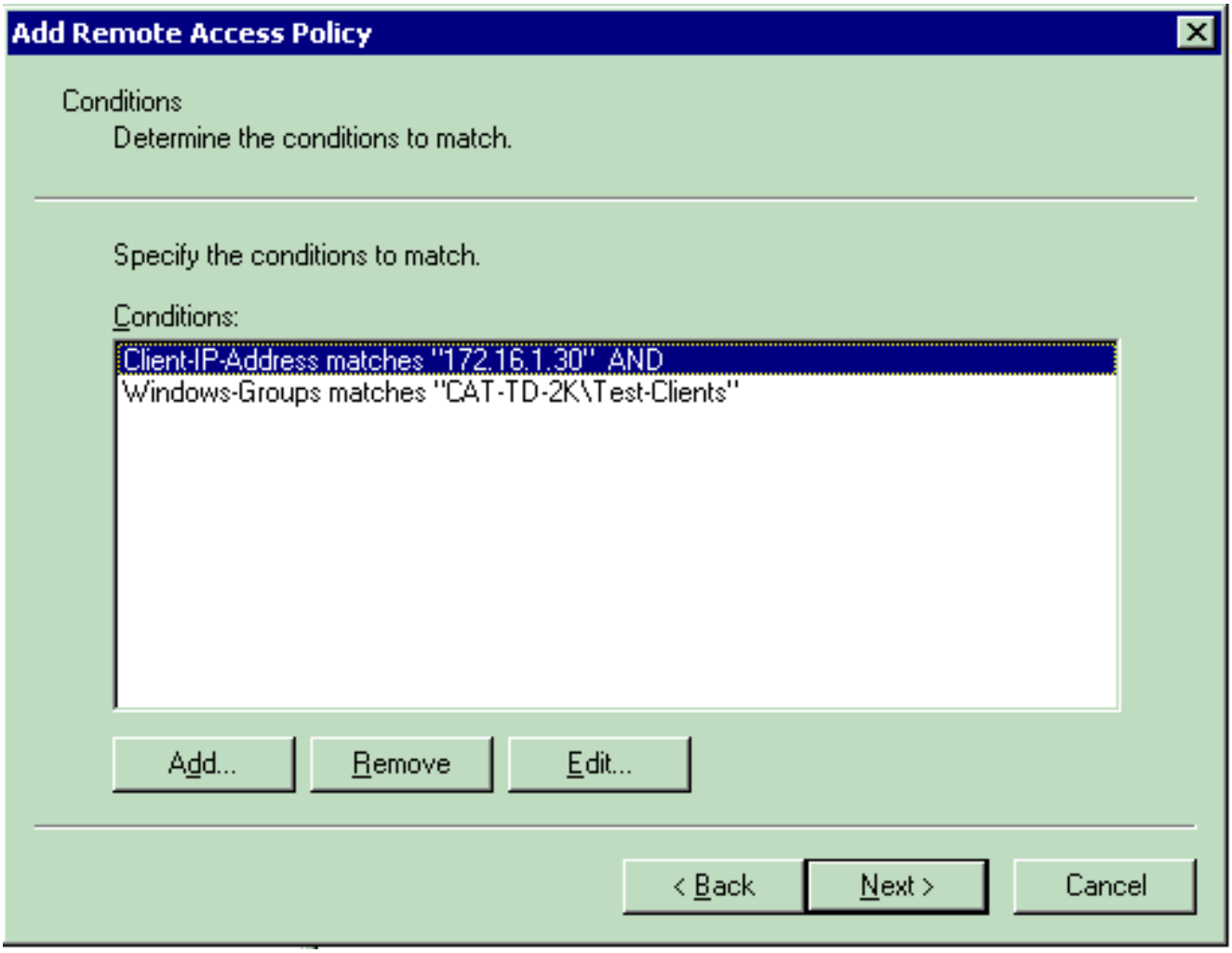
4. De los tipos menú del atributo, seleccione estos atributos:**Cliente-IP-direccionamiento** — Ingrese el IP address del cliente AAA. En este ejemplo, se ingresa el IP address de WLCs de modo que la directiva se aplique a los paquetes del



WLC. **Grupos de Windows** — Seleccione al grupo de Windows (el grupo de usuarios) quien la directiva solicitará. Aquí está un

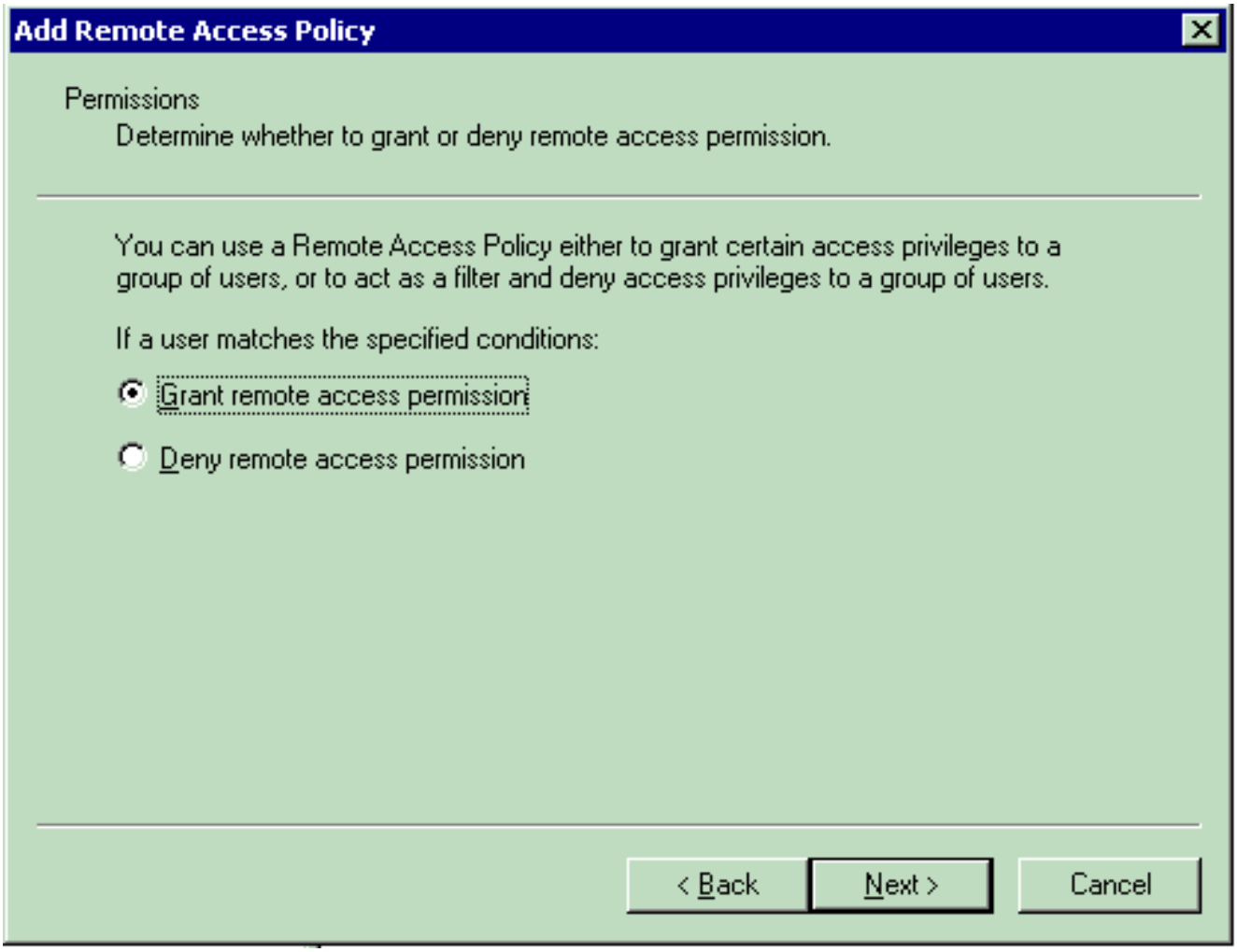


ejemplo:

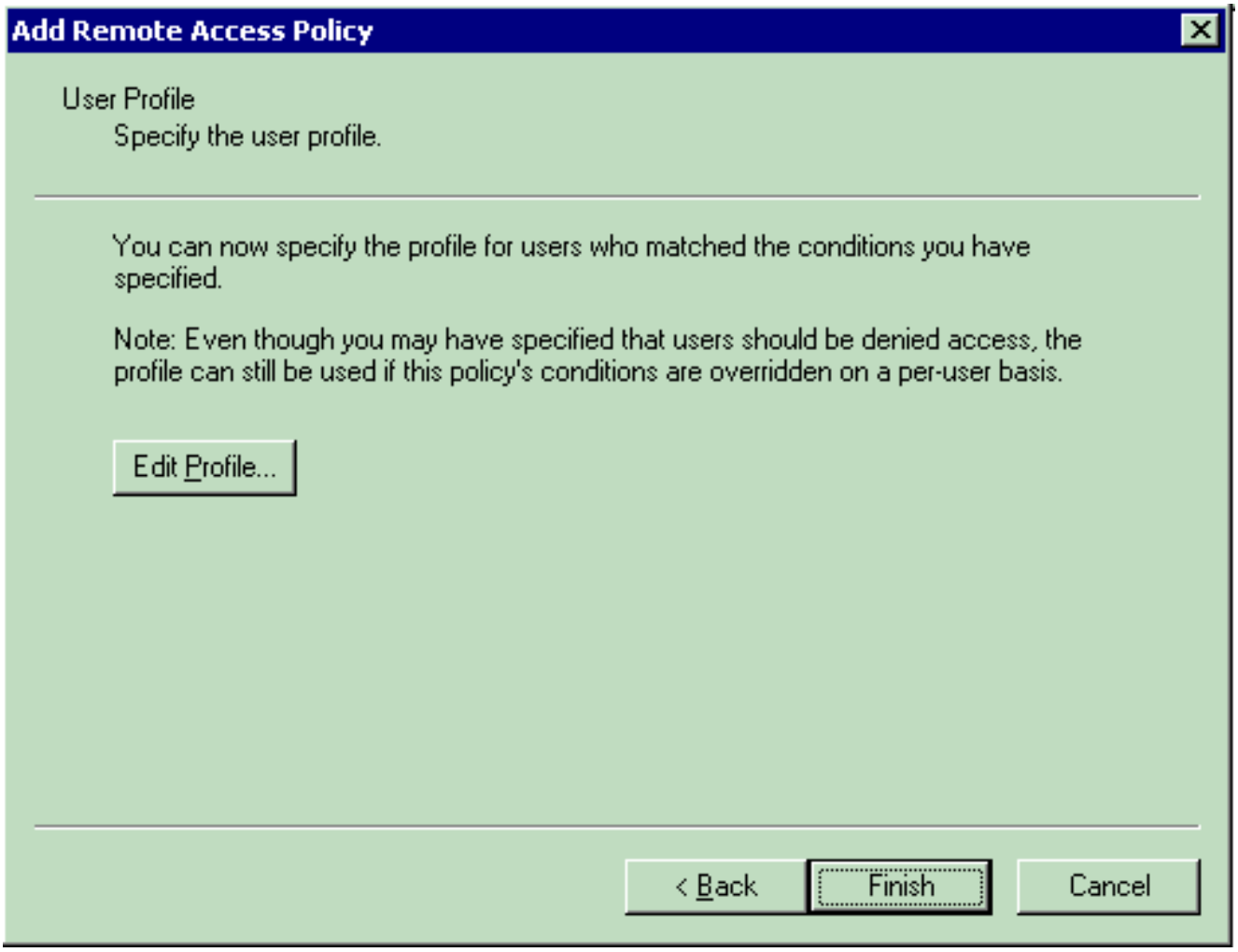


Este ejemplo muestra solamente dos condiciones. Si hay más condiciones, agregue esas condiciones también y haga clic **después**.La ventana de los permisos aparece.

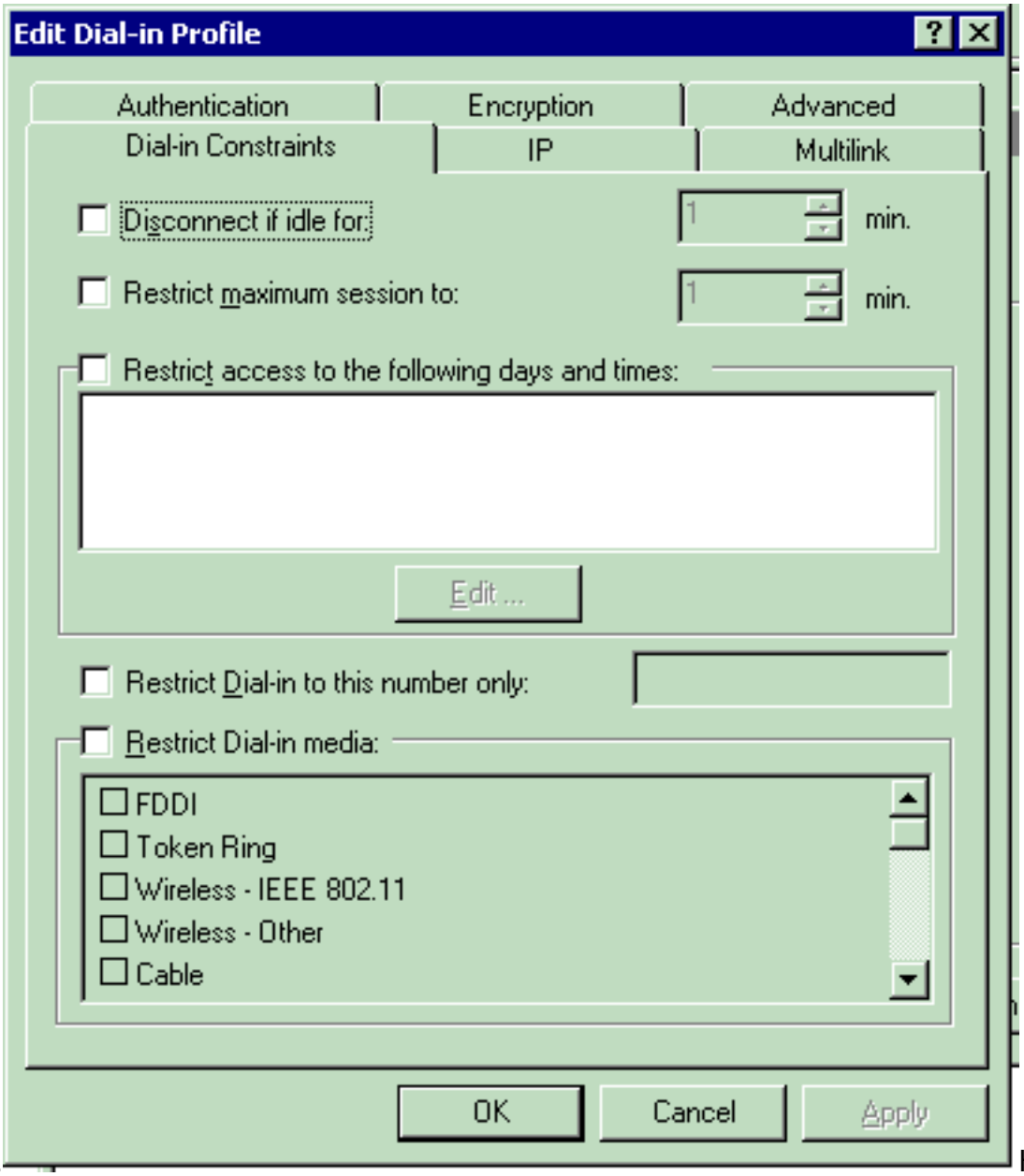
5. En la ventana de los permisos, elija el **Permiso de acceso remoto de Grant**.Después de que usted elija esta opción, dan el usuario el acceso, con tal que el usuario haga juego las condiciones especificadas (del paso
2).



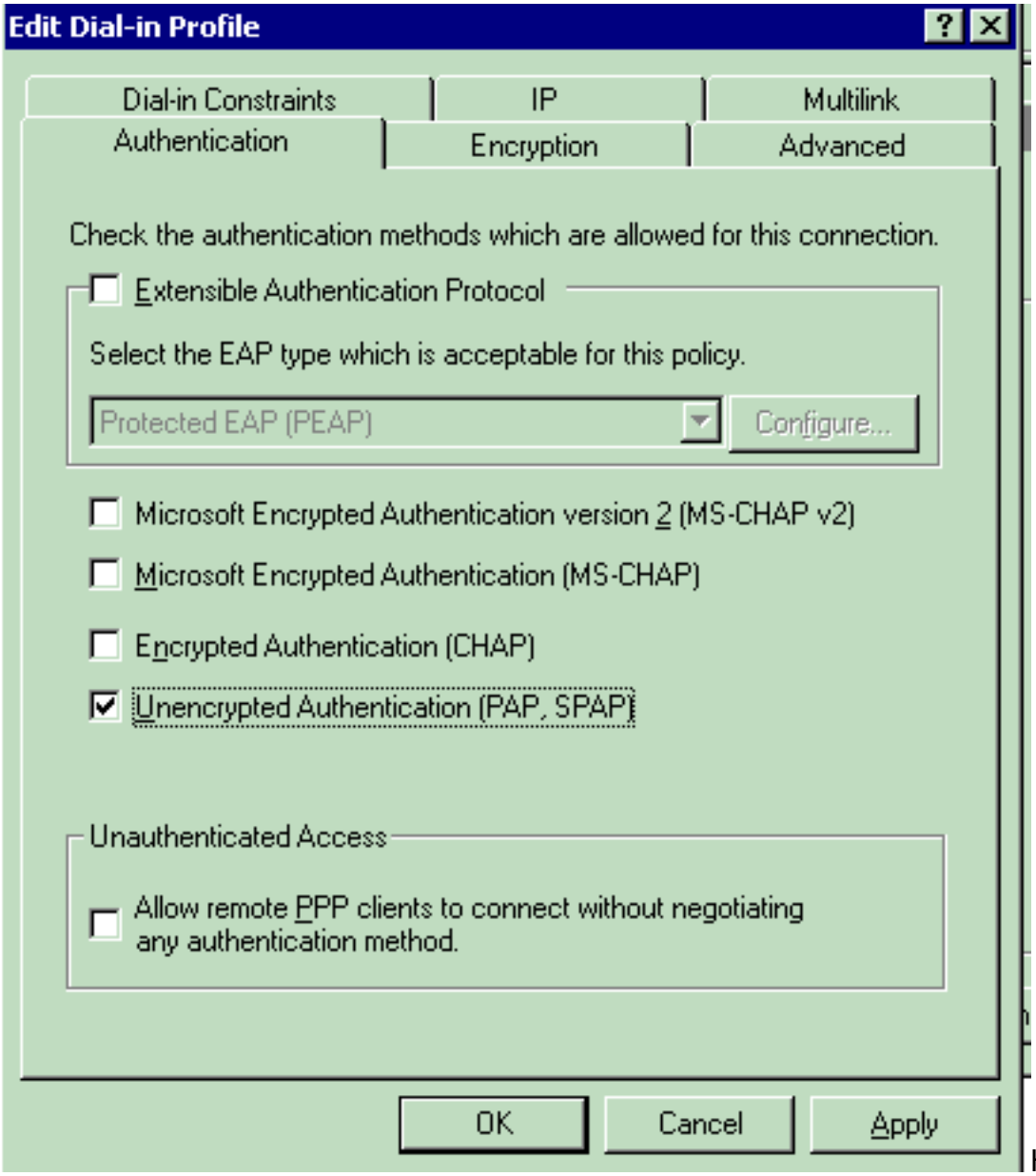
6. Haga clic en Next (Siguiente).
7. El siguiente paso es poner el perfil de usuario.Aunque usted puede ser que haya especificado que los usuarios deben ser negados o acceso concedido ser basados en las condiciones, el perfil puede todavía ser utilizado si las condiciones de esta directiva se reemplazan sobre una base del por-
usuario.



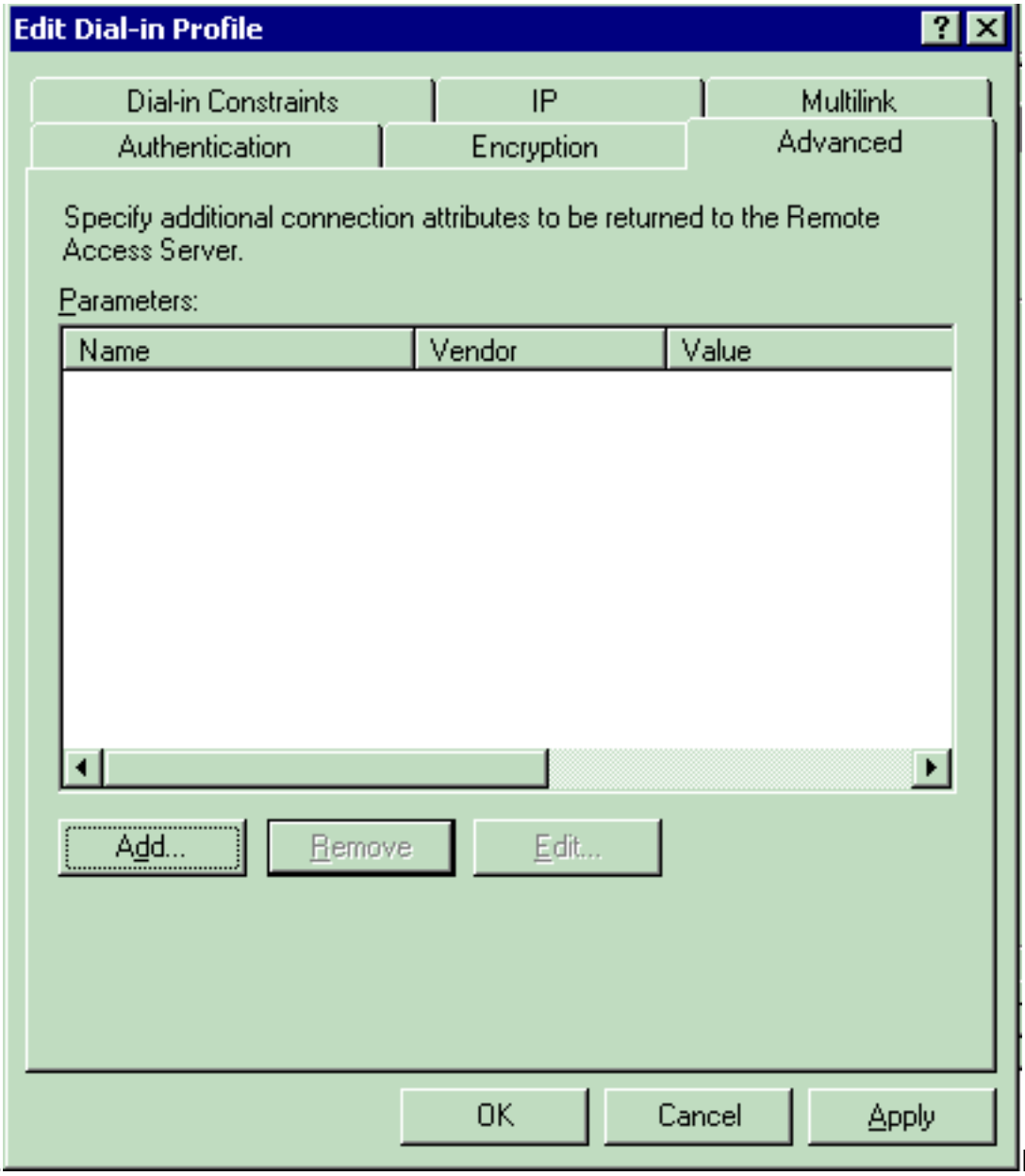
Para configurar el perfil de usuario, el tecleo **corrige el perfil** en la ventana del perfil de usuario.El corregir Dial-en la ventana del perfil



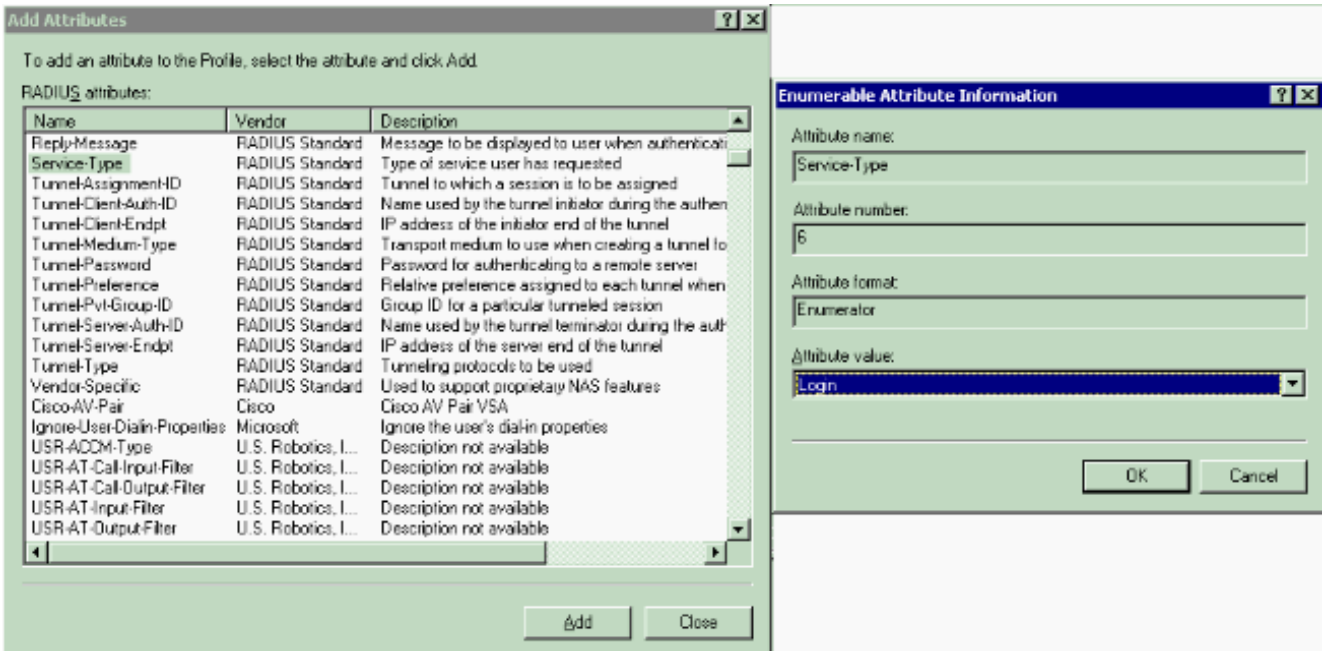
aparece. Haga clic la tabulación de la **autenticación**, después elija el método de autenticación que se utiliza en la red inalámbrica (WLAN).Este ejemplo utiliza la autenticación Unencrypted (PAP,



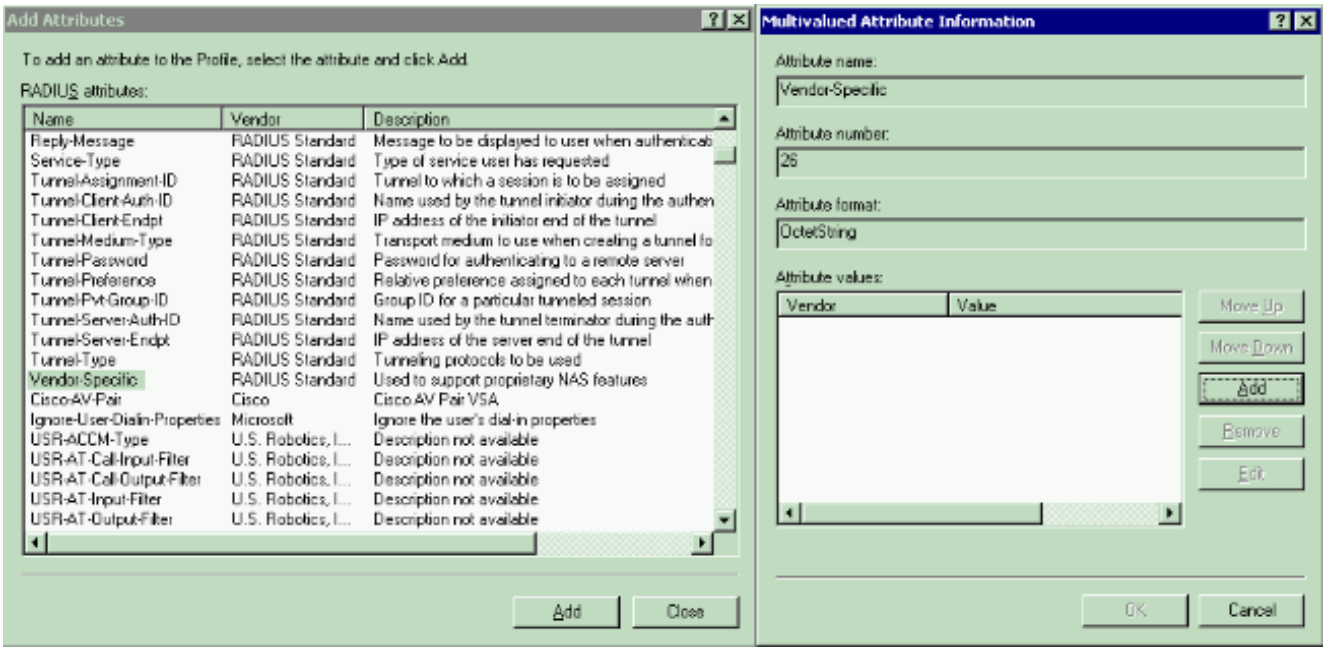
SPAP). Haga clic el cuadro **avanzado** quitan todos los parámetros de valor por defecto y el tecleo



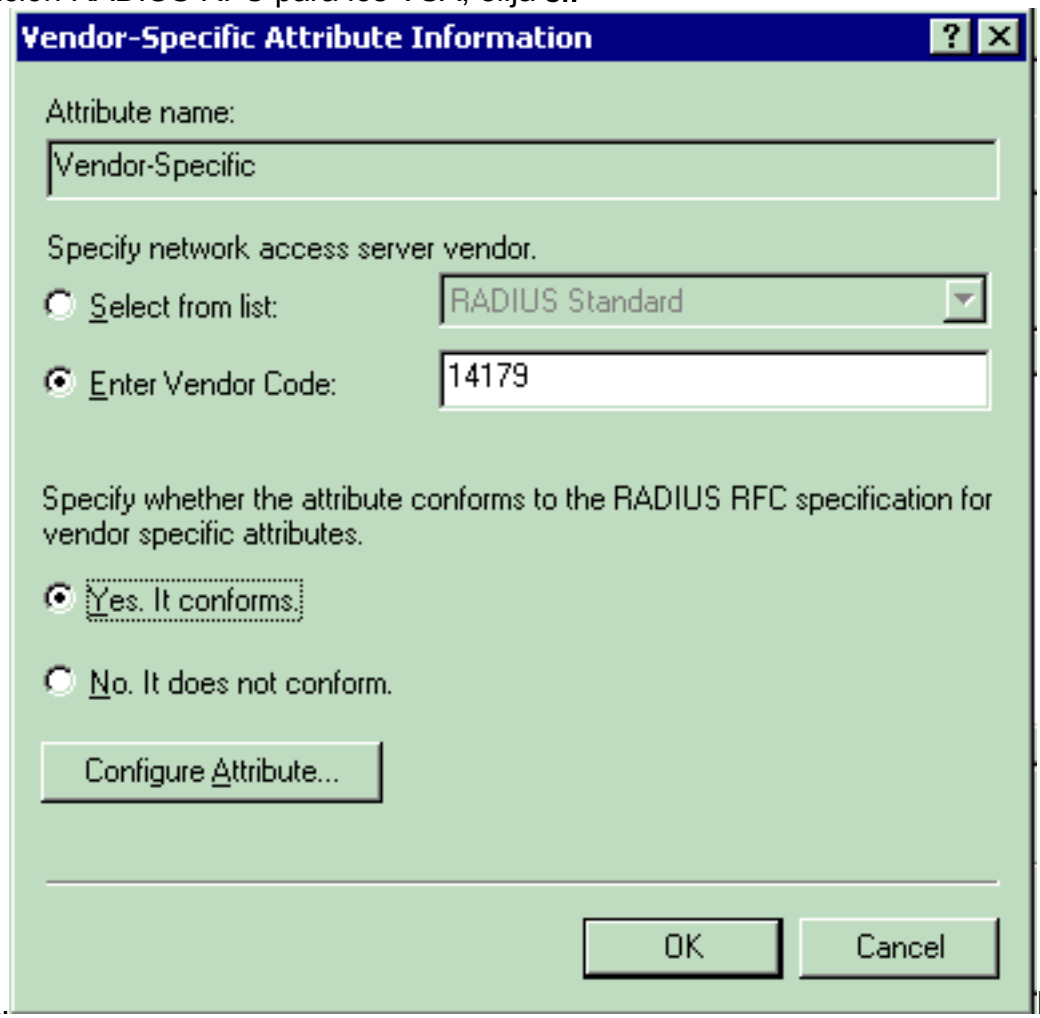
agrega.De la ventana de los **atributos del agregar**, el **tipo de servicio** selecto, entonces elige el valor de la **clave de la** próxima
ventana.



Después, usted necesita seleccionar el **atributo específico del proveedor de la** lista de atributos de
RADIUS.

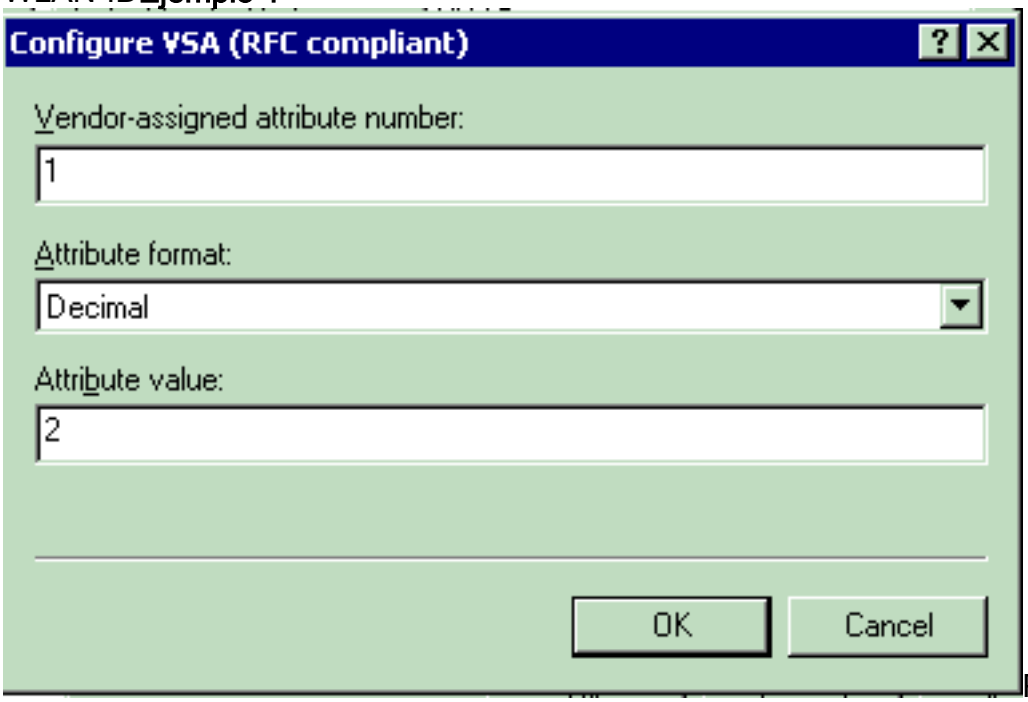


En la próxima ventana, el tecleo **agrega** para seleccionar un nuevo VSA.La ventana de la información de atributo específico del proveedor aparece.Bajo especifique al servidor del proveedor del acceso a la red, eligen **ingresan Vendor Code (Código de proveedor)**.Ingrese Vendor Code (Código de proveedor) para Airespace VSA. El Vendor Code (Código de proveedor) para los VSA de Cisco Airespace es 14179.Porque este atributo conforma con la especificación RADIUS RFC para los VSA, elija **sí.**

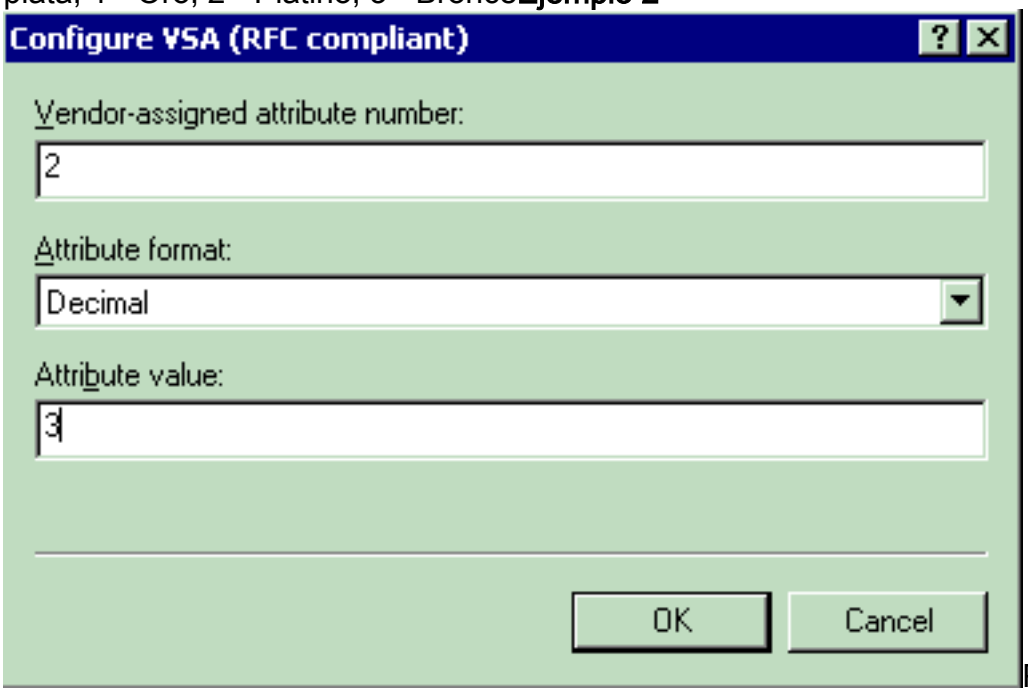


Conforma.El tecleo

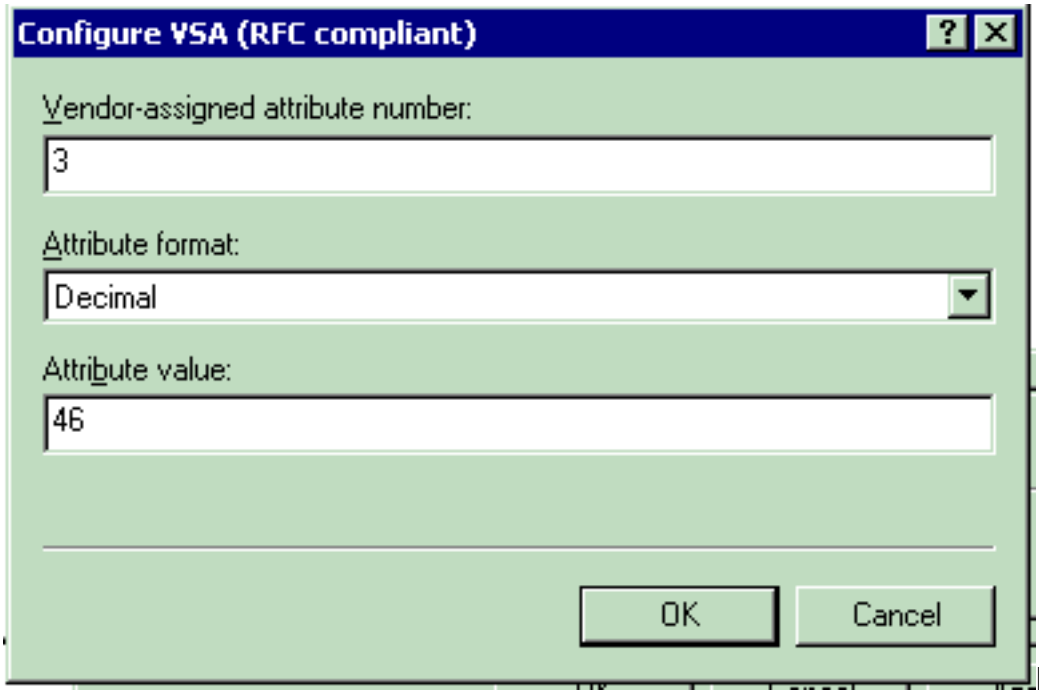
configura el atributo.En la ventana del configurar VSA (conforme a RFC), ingrese el número de atributo Vendedor-asignado, el formato de atributo y el valor de atributo, que dependen del VSA que usted quiere utilizar.Para fijar el WLAN-ID sobre una base del por-usuario:**Nombre del atributo** — Airespace-RED INALÁMBRICA (WLAN)-identificación**número de atributo Vendedor-asignado** — 1**Formato de atributo** — Número entero/decimal**Valor** — WLAN-ID**Ejemplo 1**



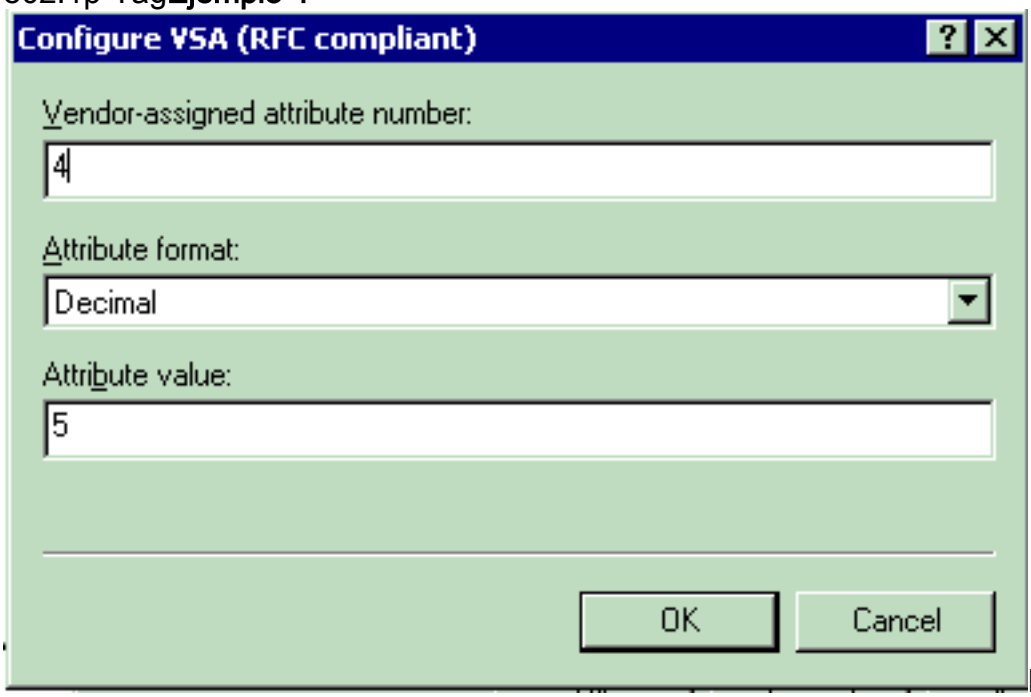
Para fijar el perfil de QoS sobre una base del por-usuario:**Nombre del atributo** — Airespace-QoS-nivel**número de atributo Vendedor-asignado** — 2**Formato de atributo** — Número entero/decimal**Valor** — 0 - plata; 1 - Oro; 2 - Platino; 3 - Bronce**Ejemplo 2**



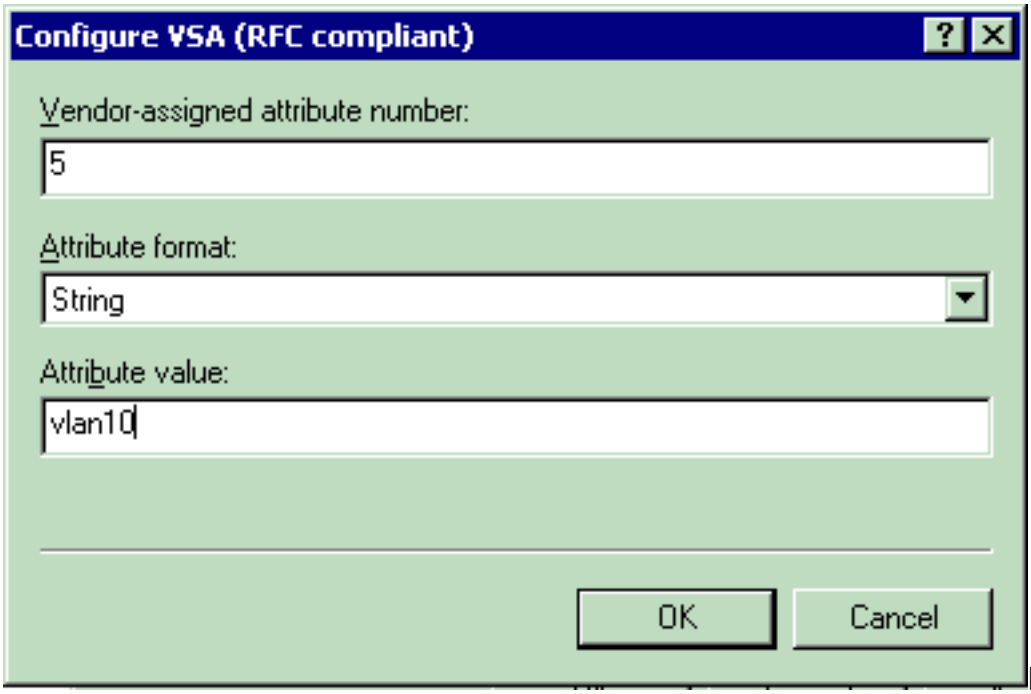
Para fijar el valor DSCP sobre una base del por-usuario:**Nombre del atributo** — Airespace-DSCP**aumber Vendedor-asignado del atributo** — 3**Formato de atributo** — Número entero/decimal**Valor** — Valor DSCP**Ejemplo 3**



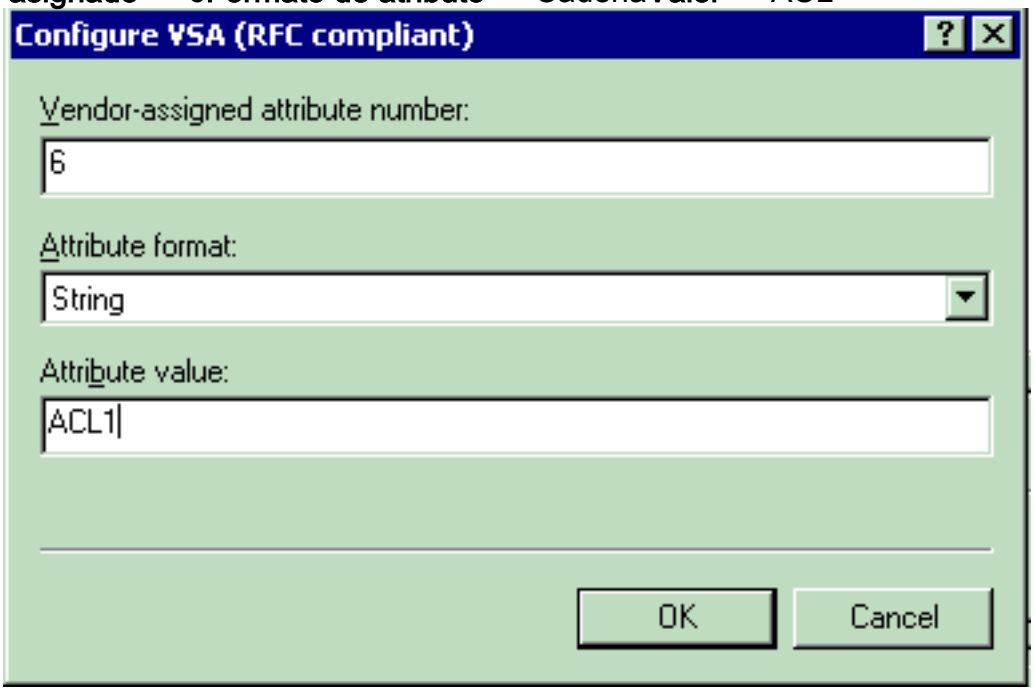
Para fijar el 802.1p-Tag sobre una base del por-usuario:**Nombre del atributo** — Airespace-802.1p-Tag**número de atributo Vendedor-asignado** — 4**Formato de atributo** — Número entero/decimal**Valor** — 802.1p-Tag**Ejemplo 4**



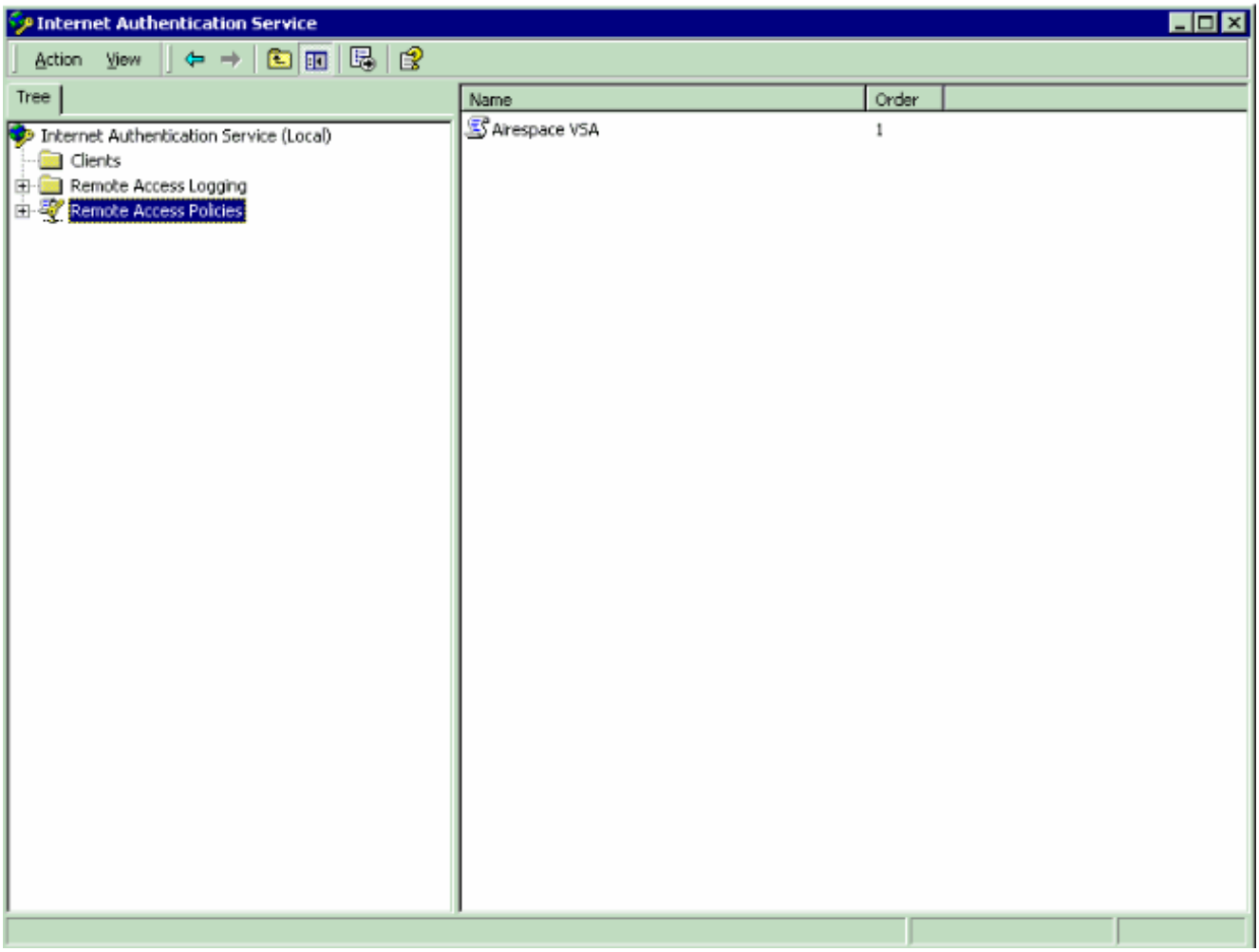
Para fijar el interfaz (VLA N) sobre una base del por-usuario:**Nombre del atributo** — Airespace-Interfaz-nombre**número de atributo Vendedor-asignado** — 5**Formato de atributo** — Cadena**Valor** — Interfaz-nombre**Ejemplo 5**



Para fijar el ACL sobre una base del por-usuario:**Nombre del atributo** — Airespace-ACL-nombre**número de atributo Vendedor-asignado** — 6**Formato de atributo** — Cadena**Valor** — ACL-nombre**Ejemplo 6**

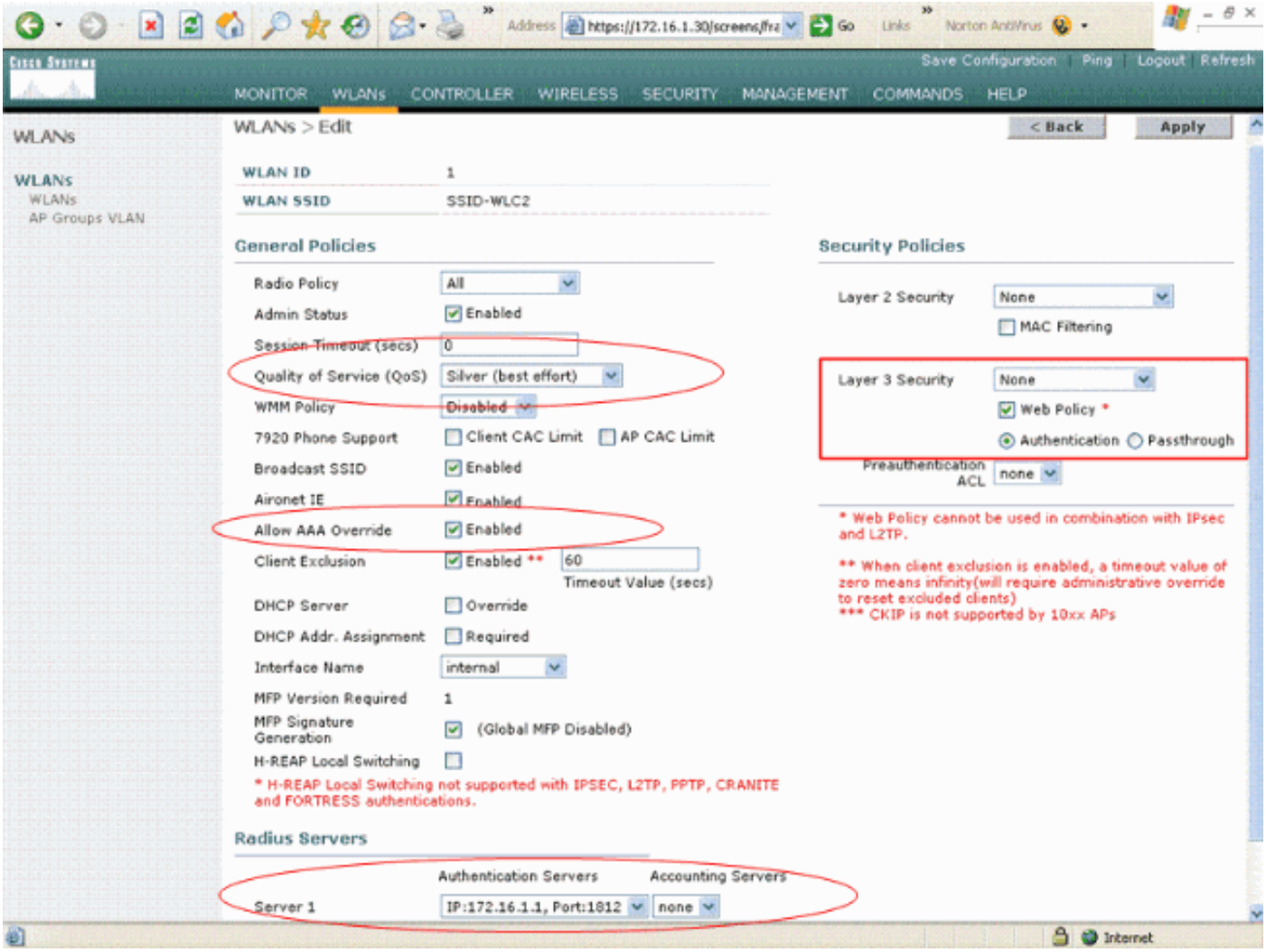


8. Una vez que usted ha configurado los VSA, haga clic la **AUTORIZACIÓN** hasta que usted vea la ventana del perfil de usuario.
9. Entonces, clic en Finalizar para completar la configuración.Usted puede ver la nueva directiva bajo políticas de acceso
   remoto.



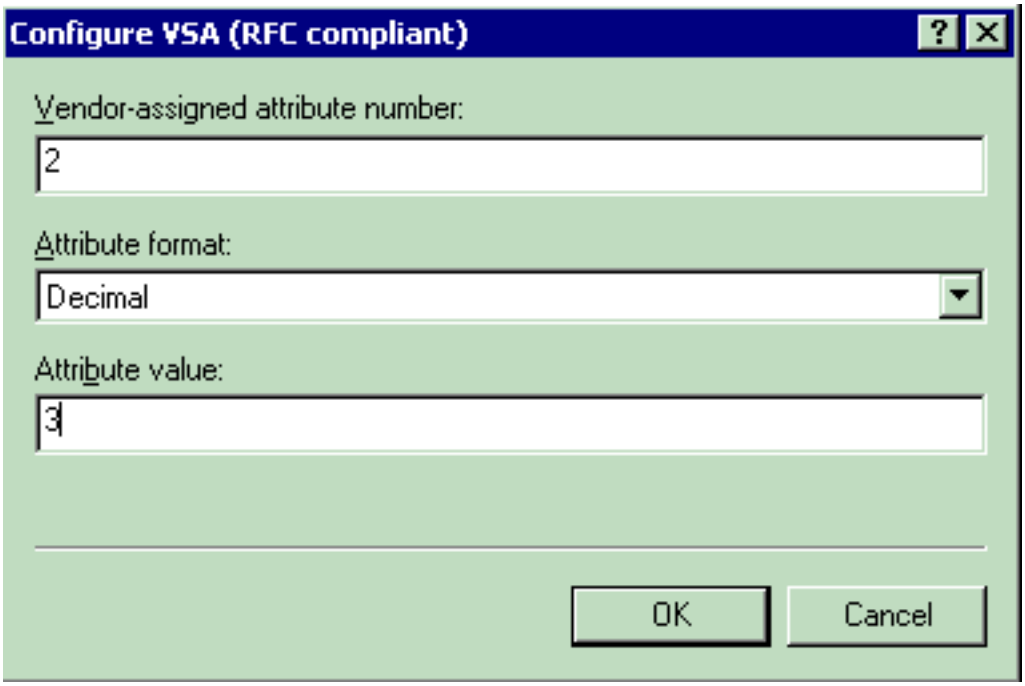
Ejemplo de configuración

En este ejemplo, una red inalámbrica (WLAN) se configura para la autenticación Web. Al servidor de RADIUS de IAS autentican a los usuarios, y configuran al servidor de RADIUS para asignar las directivas de QoS sobre una base del por-usuario.



Como usted puede ver de esta ventana, se activa la autenticación Web, el servidor de la autenticación es 172.16.1.1, y la invalidación AAA también se activa en la red inalámbrica (WLAN). La configuración de QoS del valor por defecto para esta red inalámbrica (WLAN) se fija para platearse.

En el servidor de RADIUS de IAS, se configura una política de acceso remoto que vuelve al QoS que bronce del atributo en el RADIUS valida la petición. Se hace esto cuando usted configura el específico VSA al atributo de QoS.



Vea el configurar la política de acceso remoto en la sección de IAS de este documento para información detallada sobre cómo configurar una política de acceso remoto en el servidor IAS.

Una vez el servidor IAS, el WLC, y el REVESTIMIENTO se configura para esta disposición, los clientes de red inalámbrica puede utilizar la autenticación Web para conectar.

Verifique

Use esta sección para confirmar que su configuración funciona correctamente.

Cuando el usuario conecta con la red inalámbrica (WLAN) con una identificación del usuario y contraseña, el WLC pasa las credenciales al servidor de RADIUS de IAS que autentica al usuario contra las condiciones y el perfil de usuario configuradas en la política de acceso remoto. Si la autenticación de usuario es acertada, el servidor de RADIUS vuelve un RADIUS valida la petición que también contiene los valores de la invalidación AAA. En este caso, política de calidad de servicio (QoS) del usuario se vuelve.

Usted puede publicar el **comando debug aaa all enable** para ver la Secuencia de eventos que ocurre durante la autenticación. Éste es un ejemplo de salida:

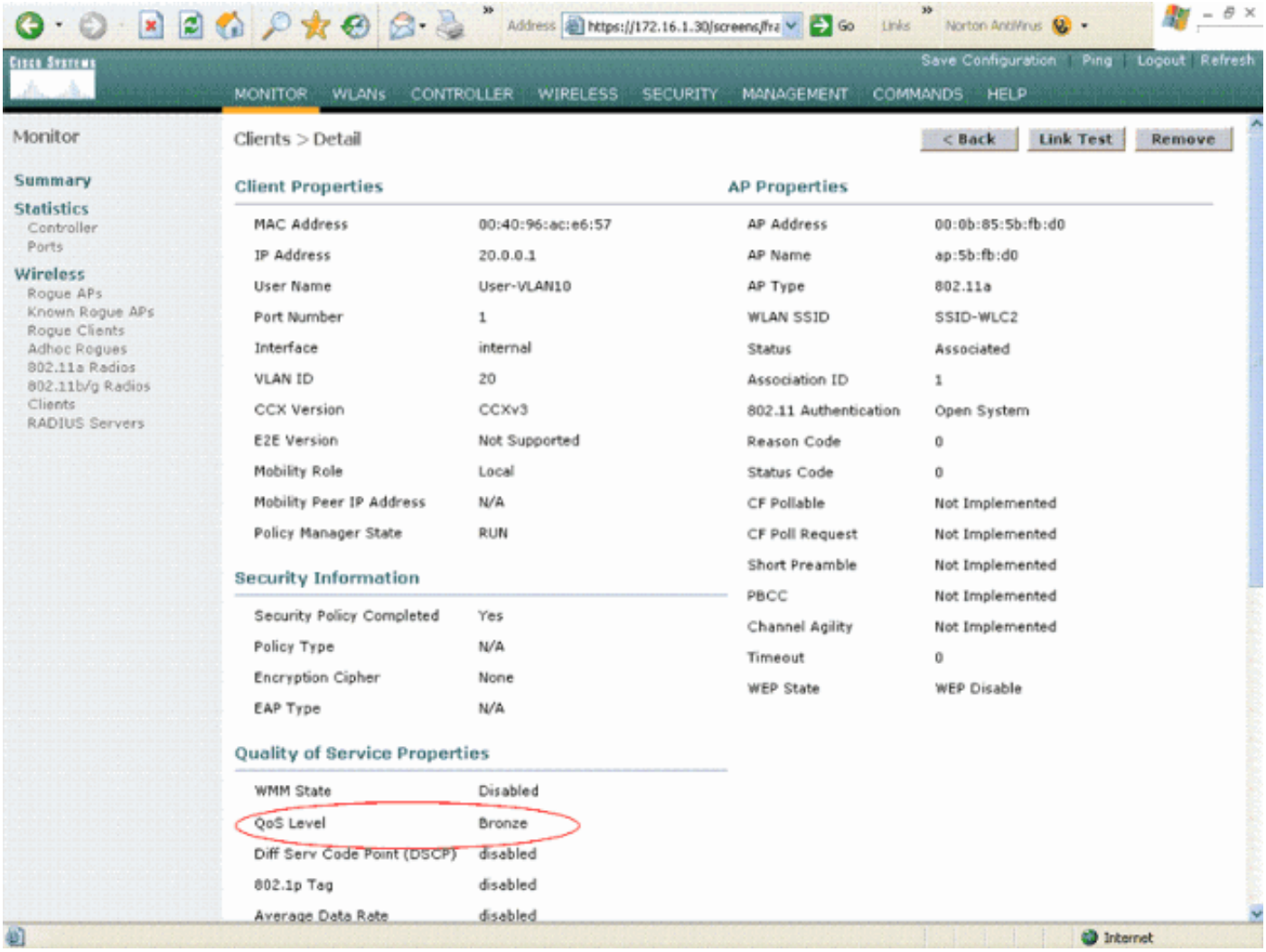
```
(Cisco Controller) > debug aaa all enable
Wed Apr 18 18:14:24 2007: User admin authenticated
Wed Apr 18 18:14:24 2007: 28:1f:00:00:00:00 Returning AAA Error 'Success' (0) for
                          mobile 28:1f:00:00:00:00
Wed Apr 18 18:14:24 2007: AuthorizationResponse: 0xbadff97c
Wed Apr 18 18:14:24 2007:       structureSize...............................70
Wed Apr 18 18:14:24 2007:       resultCode..................................0
Wed Apr 18 18:14:24 2007:       protocolUsed................................0x00000008
Wed Apr 18 18:14:24 2007:       proxyState..................................
                                28:1F:00:00:00:00-00:00
Wed Apr 18 18:14:24 2007:       Packet contains 2 AVPs:
Wed Apr 18 18:14:24 2007:           AVP[01] Service-Type.............................
                                    0x00000006 (6) (4 bytes)
Wed Apr 18 18:14:24 2007:           AVP[02] Airespace / WLAN-Identifier..............
                                    0x00000000 (0) (4 bytes)
```

```
Wed Apr 18 18:14:24 2007: User admin authenticated
Wed Apr 18 18:14:24 2007: 29:1f:00:00:00:00 Returning AAA Error 'Success' (0) for
                          mobile 29:1f:00:00:00:00
Wed Apr 18 18:14:24 2007: AuthorizationResponse: 0xbadff97c
Wed Apr 18 18:14:24 2007:       structureSize.............................70
Wed Apr 18 18:14:24 2007:       resultCode................................0
Wed Apr 18 18:14:24 2007:       protocolUsed..............................0x00000008
Wed Apr 18 18:14:24 2007:       proxyState................................
                                29:1F:00:00:00:00-00:00
Wed Apr 18 18:14:24 2007:       Packet contains 2 AVPs:
Wed Apr 18 18:14:24 2007:           AVP[01] Service-Type.....................
                                    0x00000006 (6) (4 bytes)
Wed Apr 18 18:14:24 2007:           AVP[02] Airespace / WLAN-Identifier......
                                    0x00000000 (0) (4 bytes)
Wed Apr 18 18:15:08 2007: Unable to find requested user entry for User-VLAN10
Wed Apr 18 18:15:08 2007: AuthenticationRequest: 0xa64c8bc
Wed Apr 18 18:15:08 2007:       Callback.................................0x8250c40
Wed Apr 18 18:15:08 2007:       protocolType.............................0x00000001
Wed Apr 18 18:15:08 2007:       proxyState................................
                                00:40:96:AC:E6:57-00:00
Wed Apr 18 18:15:08 2007:       Packet contains 8 AVPs (not shown)
Wed Apr 18 18:15:08 2007: 00:40:96:ac:e6:57 Successful transmission of Authentication Packet
                          (id 26) to 172.16.1.1:1812, proxy state 00:40:96:ac:e6:57-96:ac
Wed Apr 18 18:15:08 2007: 00000000: 01 1a 00 68 00 00 00 00  00 00 00 00 00 00 00 00
                          ...h............
Wed Apr 18 18:15:08 2007: 00000010: 00 00 00 00 01 0d 55 73  65 72 2d 56 4c 41 4e 31
                          ......User-VLAN1
Wed Apr 18 18:15:08 2007: 00000020: 30 02 12 fa 32 57 ba 2a  ba 57 38 11 bc 9a 5d 59
                          0...2W.*.W8...]Y
Wed Apr 18 18:15:08 2007: 00000030: ed ca 23 06 06 00 00 00  01 04 06 ac 10 01 1e 20
                          ..#.............
Wed Apr 18 18:15:08 2007: 00000040: 06 57 4c 43 32 1a 0c 00  00 37 63 01 06 00 00 00
                          .WLC2....7c.....
Wed Apr 18 18:15:08 2007: 00000050: 01 1f 0a 32 30 2e 30 2e  30 2e 31 1e 0d 31 37 32
                          ...20.0.0.1..172
Wed Apr 18 18:15:08 2007: 00000060: 2e 31 36 2e 31 2e 33 30 .16.1.30
Wed Apr 18 18:15:08 2007: 00000000: 02 1a 00 46 3f cf 1b cc  e4 ea 41 3e 28 7e cc bc
                          ...F?.....A>(~..
Wed Apr 18 18:15:08 2007: 00000010: 00 e1 61 ae 1a 0c 00 00  37 63 02 06 00 00 00 03
                          ..a.....7c......
Wed Apr 18 18:15:08 2007: 00000020: 06 06 00 00 00 01 19 20  37 d0 03 e6 00 00 01 37
                          ........7......7
Wed Apr 18 18:15:08 2007: 00000030: 00 01 ac 10 01 01 01 c7  7a 8b 35 20 31 80 00 00
                          ........z.5.1...
Wed Apr 18 18:15:08 2007: 00000040: 00 00 00 00 00 1b      ......
Wed Apr 18 18:15:08 2007: ****Enter processIncomingMessages: response code=2
Wed Apr 18 18:15:08 2007: ****Enter processRadiusResponse: response code=2
Wed Apr 18 18:15:08 2007: 00:40:96:ac:e6:57 Access-Accept received from RADIUS server
                          172.16.1.1 for mobile 00:40:96:ac:e6:57 receiveId = 0
Wed Apr 18 18:15:08 2007: AuthorizationResponse: 0x9802520
Wed Apr 18 18:15:08 2007:       structureSize.............................114
Wed Apr 18 18:15:08 2007:       resultCode................................0
Wed Apr 18 18:15:08 2007:       protocolUsed..............................0x00000001
Wed Apr 18 18:15:08 2007:       proxyState................................
                                00:40:96:AC:E6:57-00:00
Wed Apr 18 18:15:08 2007:       Packet contains 3 AVPs:
Wed Apr 18 18:15:08 2007:           AVP[01] Airespace / QOS-Level...........
                                    0x00000003 (3) (4 bytes)
Wed Apr 18 18:15:08 2007:           AVP[02] Service-Type.....................
                                    0x00000001 (1) (4 bytes)
Wed Apr 18 18:15:08 2007:           AVP[03] Class............................
                                    DATA (30 bytes)
Wed Apr 18 18:15:08 2007: 00:40:96:ac:e6:57 Applying new AAA override for station
                          00:40:96:ac:e6:57
```

```
Wed Apr 18 18:15:08 2007: 00:40:96:ac:e6:57 Override values for station 00:40:96:ac:e6:57
        source: 48, valid bits: 0x3
        qosLevel: 3, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1
        dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
        vlanIfName: '', aclName: '
Wed Apr 18 18:15:12 2007: AccountingMessage Accounting Start: 0xa64c8bc
Wed Apr 18 18:15:12 2007:       Packet contains 13 AVPs:
Wed Apr 18 18:15:12 2007:           AVP[01] User-Name..............................
                                    User-VLAN10 (11 bytes)
Wed Apr 18 18:15:12 2007:           AVP[02] Nas-Port...............................
                                    0x00000001 (1) (4 bytes)
Wed Apr 18 18:15:12 2007:           AVP[03] Nas-Ip-Address.........................
                                    0xac10011e (-1408237282) (4 bytes)
Wed Apr 18 18:15:12 2007:           AVP[04] NAS-Identifier.........................
                                    0x574c4332 (1464615730) (4 bytes)
Wed Apr 18 18:15:12 2007:           AVP[05] Airespace / WLAN-Identifier.............
                                    0x00000001 (1) (4 bytes)
Wed Apr 18 18:15:12 2007:           AVP[06] Acct-Session-Id........................
                                    4626602c/00:40:96:ac:e6:57/16 (29 bytes)
Wed Apr 18 18:15:12 2007:           AVP[07] Acct-Authentic.........................
                                    0x00000001 (1) (4 bytes)
Wed Apr 18 18:15:12 2007:           AVP[08] Tunnel-Type............................
                                    0x0000000d (13) (4 bytes)
Wed Apr 18 18:15:12 2007:           AVP[09] Tunnel-Medium-Type.....................
                                    0x00000006 (6) (4 bytes)
Wed Apr 18 18:15:12 2007:           AVP[10] Tunnel-Group-Id........................
                                    0x3230 (12848) (2 bytes)
Wed Apr 18 18:15:12 2007:           AVP[11] Acct-Status-Type.......................
                                    0x00000001 (1) (4 bytes)
Wed Apr 18 18:15:12 2007:           AVP[12] Calling-Station-Id.....................
                                    20.0.0.1 (8 bytes)
Wed Apr 18 18:15:12 2007:           AVP[13] Called-Station-Id......................
                                    172.16.1.30 (11 bytes)
```

Como usted puede ver de la salida, autentican al usuario. Entonces, los valores de la invalidación AAA se vuelven con el RADIUS validan el mensaje. En este caso, dan el usuario política de calidad de servicio (QoS) del bronce.

Usted puede verificar esto en el GUI WLC también. Aquí está un ejemplo:



Note: El perfil de QoS del valor por defecto para este SSID es plata. Sin embargo, porque se selecciona la invalidación AAA y configuran al usuario con un perfil de QoS del bronce en el servidor IAS, se reemplaza el perfil de QoS del valor por defecto.

Troubleshooting

Usted puede utilizar el **comando debug aaa all enable** en el WLC de resolver problemas la configuración. Un ejemplo de la salida de esta depuración en una red de trabajo se muestra en la sección del verificar de este documento.

Note: Refiera a la información importante en los comandos Debug antes de que usted utilice los **comandos debug**.

Información Relacionada

- Guía de configuración del Controlador de LAN de la Red Inalámbrica Cisco, versión 4.0
- Restrinja el acceso de la red inalámbrica (WLAN) basado en el SSID con el ejemplo seguro de la configuración WLC y de Cisco ACS
- Soporte de Productos de Red Inalámbrica
- Soporte técnico y documentación - Cisco Systems