Ejemplo de Configuración de VSA de Cisco Airespace en Microsoft IAS Radius Server

Contenido

Introducción

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

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento de cómo configurar un servidor IAS
- Conocimiento de la configuración de los puntos de acceso ligeros (LAP) y de los controladores de LAN inalámbrica (WLC) de Cisco
- Conocimiento de las soluciones Cisco Unified Wireless Security

Componentes Utilizados

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

- Servidor Microsoft Windows 2000 con IAS
- Cisco 4400 WLC que ejecuta la versión de software 4.0.206.0
- Cisco 1000 Series LAP
- Adaptador de cliente inalámbrico 802.11 a/b/g con firmware 2.5
- Aironet Desktop Utility (ADU) versión 2.5

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.

Nota: Este documento pretende dar al lector un ejemplo de la configuración requerida en el servidor IAS para soportar los VSA de Cisco Airespace. La configuración del servidor IAS que se presenta en este documento se ha probado en el laboratorio y funciona según lo esperado. Si tiene problemas para configurar el servidor IAS, póngase en contacto con Microsoft para obtener ayuda. Cisco TAC no admite la configuración del servidor de Microsoft Windows.

Este documento asume que el WLC está configurado para el funcionamiento básico y que los LAPs están registrados en el WLC. Si es un usuario nuevo que intenta configurar el WLC para el funcionamiento básico con los LAP, consulte Registro de Lightweight AP (LAP) en un controlador de LAN 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 inalámbricos (WLAN), cada WLAN tiene una política estática que se aplica a todos los clientes asociados a un identificador de conjunto de servicios (SSID). Aunque poderoso, este método tiene limitaciones porque requiere que los clientes se asocien con diferentes SSID para heredar diferentes QoS y políticas de seguridad.

Sin embargo, la solución Cisco Wireless LAN Solution admite redes de identidad, lo que permite a la red anunciar un solo SSID y a usuarios específicos heredar diferentes QoS o políticas de seguridad en función de sus perfiles de usuario. Entre las políticas específicas que puede controlar mediante las redes de identidad se incluyen las siguientes:

- **Calidad de Servicio**: cuando está presente en un RADIUS Access Accept, el valor de QoS-Level anula el valor de QoS especificado en el perfil WLAN.
- **ACL**: cuando el atributo de la lista de control de acceso (ACL) está presente en la aceptación de acceso RADIUS, el sistema aplica el nombre de ACL a la estación cliente después de que se autentica. Esto anula cualquier ACL que se asignen a la interfaz.
- **VLAN**: cuando hay un nombre de interfaz VLAN o una etiqueta VLAN en un acceso RADIUS Accept, el sistema coloca al cliente en una interfaz específica.
- **WLAN ID**: cuando el atributo WLAN-ID está presente en RADIUS Access Accept, el sistema aplica el WLAN-ID (SSID) a la estación cliente después de que se autentica. El WLC envía el ID de WLAN en todas las instancias de autenticación excepto IPSec. En caso de autenticación web, si el WLC recibe un atributo WLAN-ID en la respuesta de autenticación del servidor AAA y no coincide con el ID de la WLAN, la autenticación es rechazada. Otros tipos

de métodos de seguridad no hacen esto.

- **Valor DSCP**: cuando está presente en una aceptación de acceso RADIUS, el valor DSCP invalida el valor DSCP especificado en el perfil WLAN.
- **802.1p-Tag**: cuando está presente en un RADIUS Access Accept, el valor 802.1p invalida el valor predeterminado especificado en el perfil WLAN.

Nota: La función VLAN sólo admite filtrado de MAC, 802.1X y acceso Wi-Fi protegido (WPA). La función VLAN no admite autenticación web ni IPSec. La base de datos de filtro MAC local del sistema operativo se ha ampliado para incluir el nombre de la interfaz. Esto permite a los filtros MAC locales especificar qué interfaz se debe asignar al cliente. También se puede utilizar un servidor RADIUS independiente, pero el servidor RADIUS debe definirse mediante los menús de seguridad.

Refiérase a Configuración de las Redes de Identidad para obtener más información sobre las Redes de Identidad.

Configuración de IAS para VSA de Airespace

Para configurar el IAS para los VSA de Airespace, debe completar estos pasos:

1. Configure el WLC como un Cliente AAA en el IAS
2. Configure la Política de Acceso Remoto en el IAS

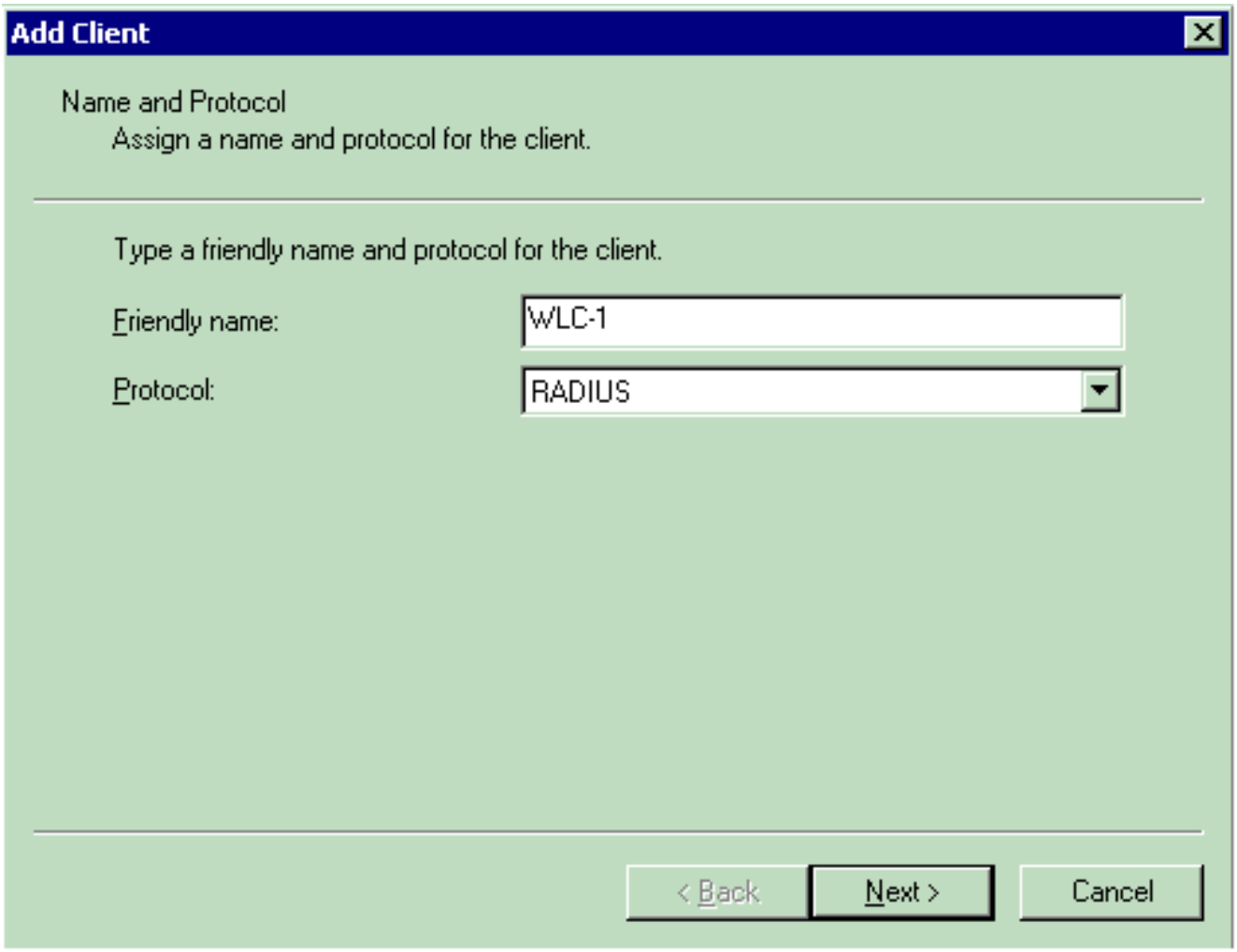
Nota: Los VSA se configuran en la Política de acceso remoto.

Configure el WLC como un Cliente AAA en el IAS

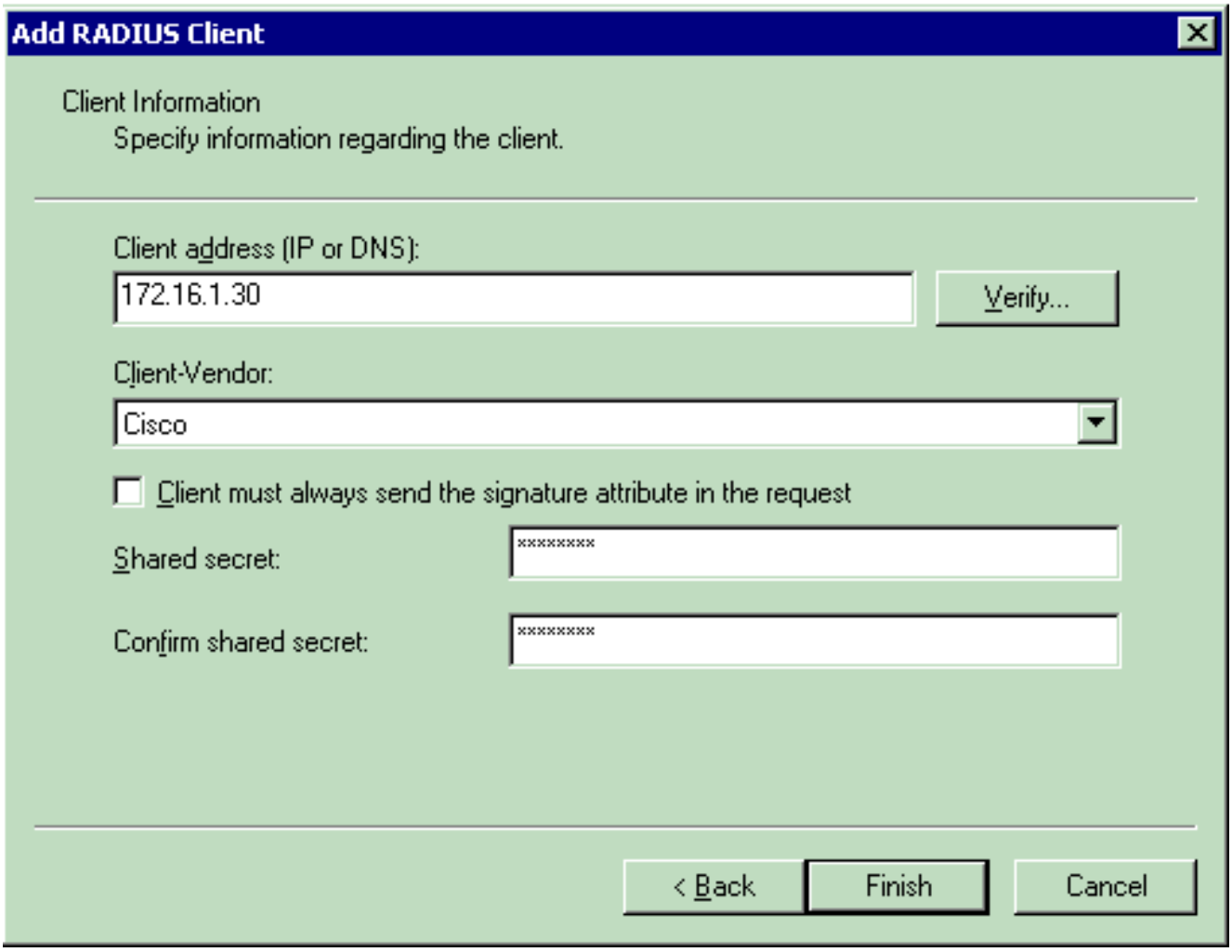
Complete estos pasos para configurar el WLC como un cliente AAA en el IAS:

1. Haga clic en **Programas > Herramientas administrativas > Servicio de autenticación de Internet** para iniciar IAS en el servidor Microsoft 2000.

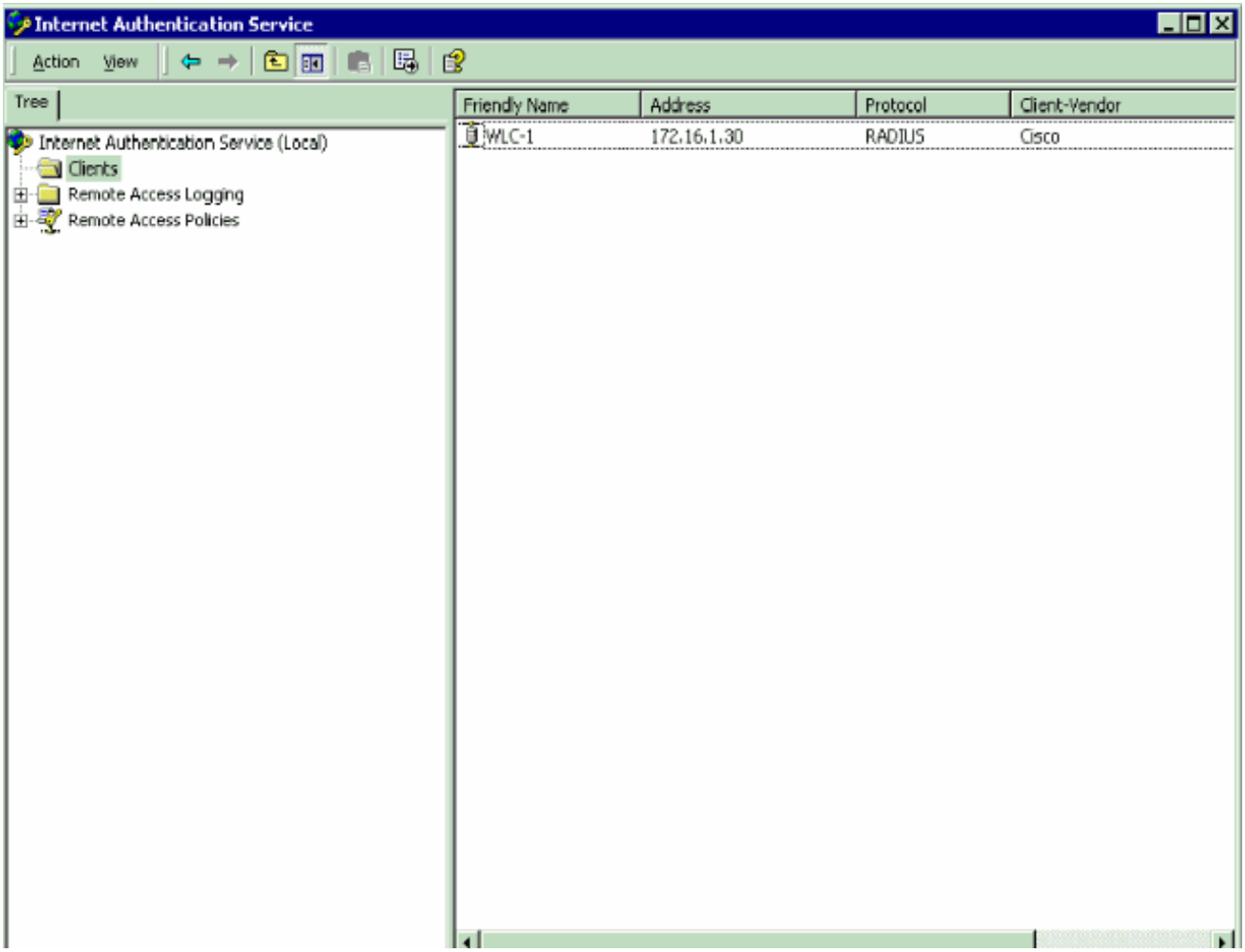
2. Haga clic con el botón derecho del mouse en la carpeta **Clientes** y elija **Nuevo Cliente** para agregar un nuevo cliente RADIUS.
3. En la ventana Add Client, ingrese el nombre del cliente y elija **RADIUS** como el Protocolo. A continuación, haga clic en **Siguiente**.En este ejemplo, el nombre del cliente es *WLC-1*.**Nota:** De forma predeterminada, el protocolo se establece en RADIUS.



4. En la ventana Add RADIUS Client, ingrese la **dirección IP del cliente**, **cliente-proveedor** y **secreto compartido**. Después de ingresar la información del cliente, haga clic en **Finalizar**.Este ejemplo muestra un cliente llamado *WLC-1* con una dirección IP de *172.16.1.30*, el Cliente-Proveedor está configurado en *Cisco* y el Secreto Compartido es *cisco123*:



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

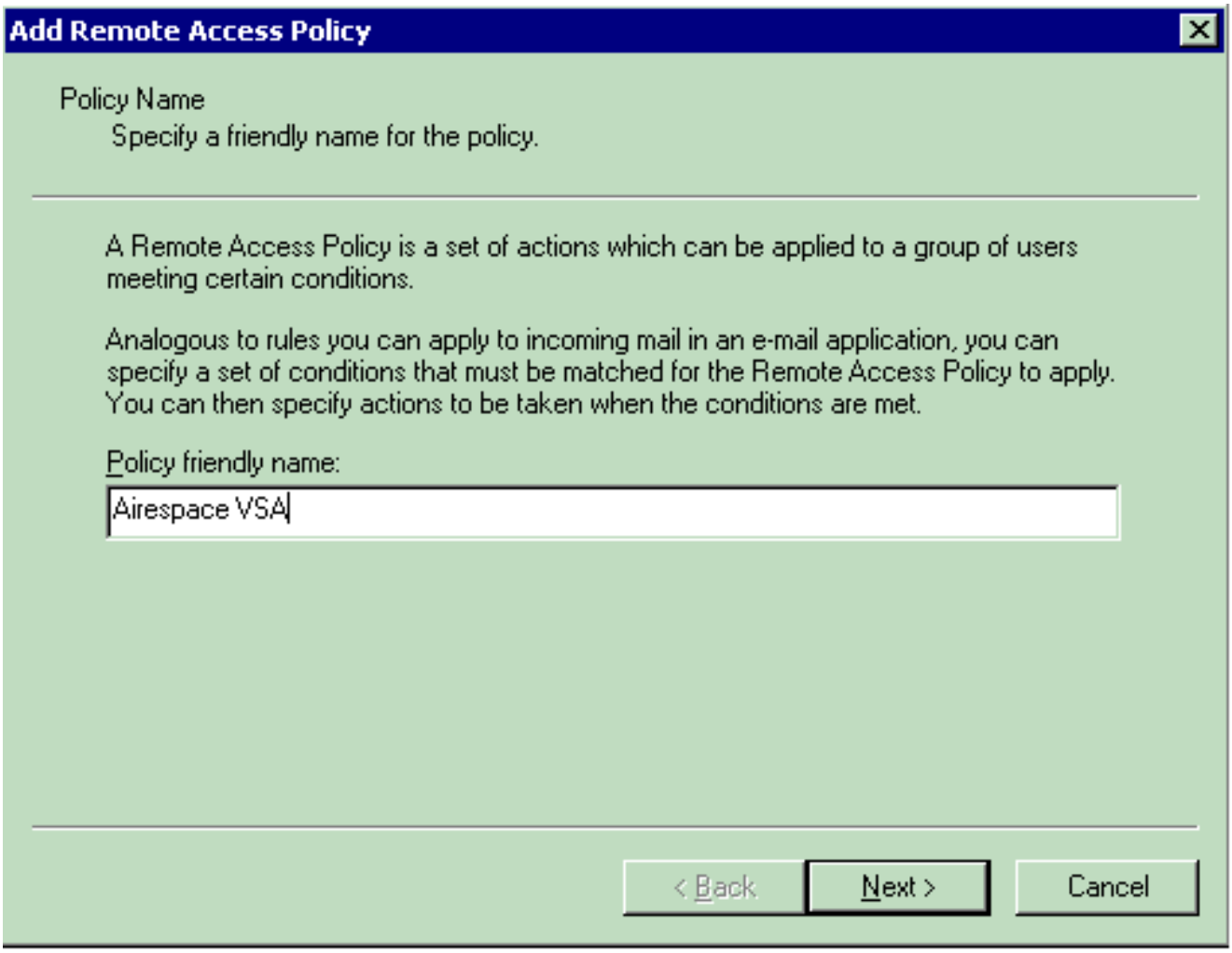


El siguiente paso es crear una política de acceso remoto y configurar los VSA.

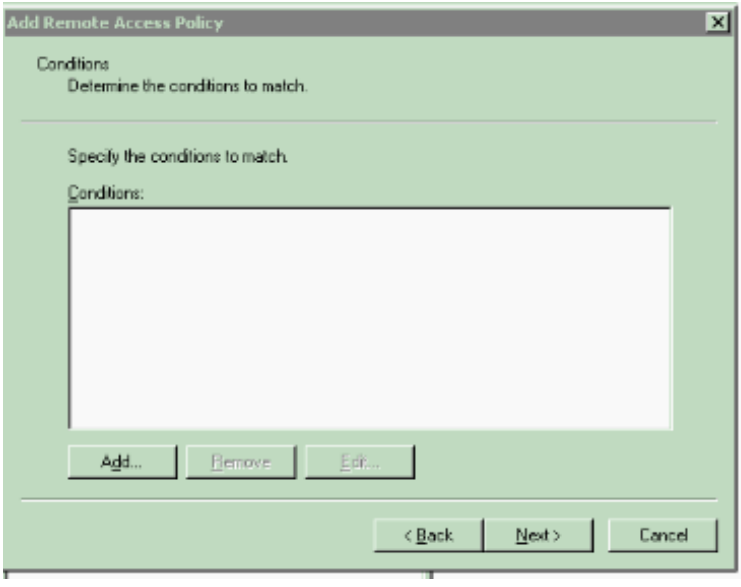
Configure la Política de Acceso Remoto en el IAS

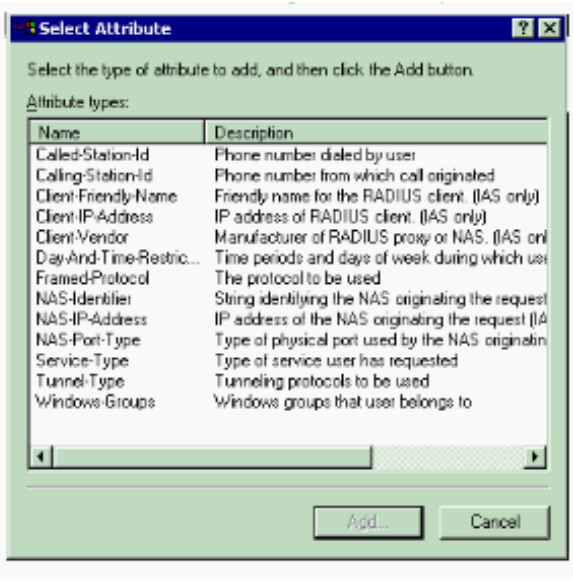
Complete estos pasos para configurar una nueva política de acceso remoto en el IAS:

1. Haga clic con el botón derecho del ratón en **Remote Access Policies** y elija **New Remote AccessMSss Policy**.Aparecerá la ventana Policy Name (Nombre de directiva).
2. Introduzca el nombre de la política y haga clic en **Siguiente**.

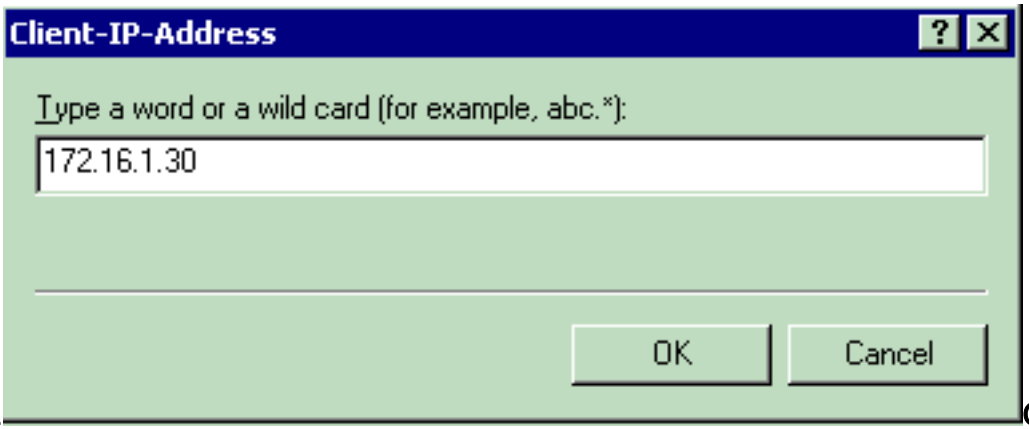


3. En la siguiente ventana, seleccione las condiciones para las que se aplicará la política de acceso remoto. Haga clic en **Agregar** para seleccionar las condiciones.

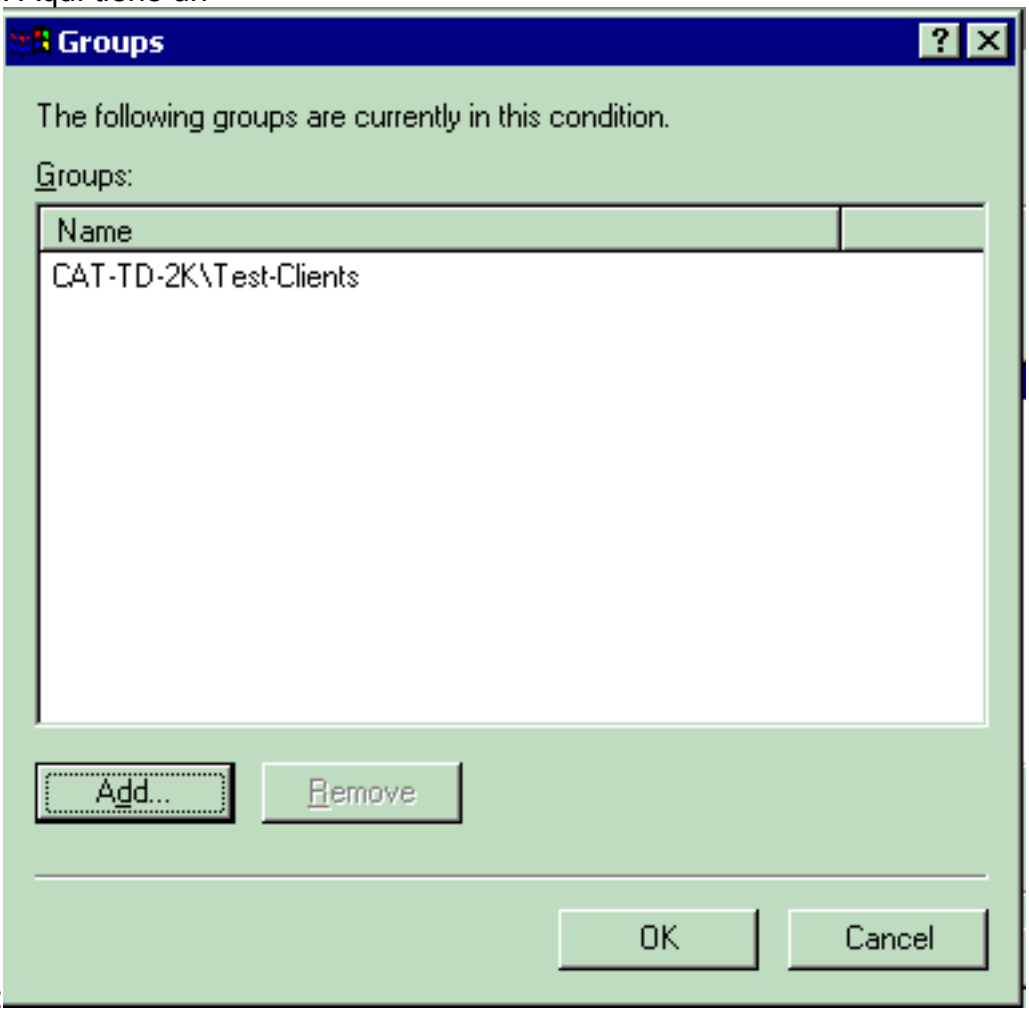




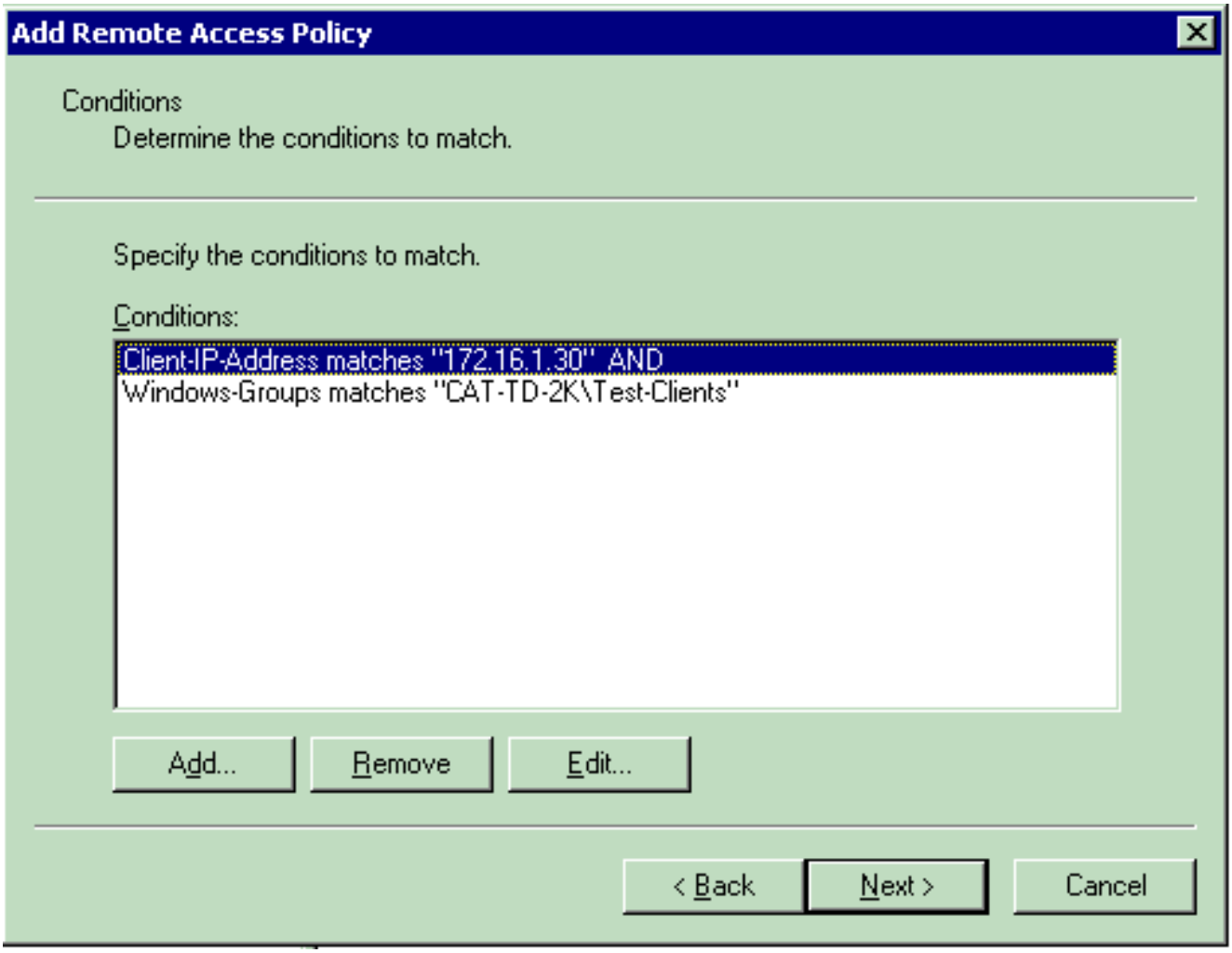
4. En el menú Tipos de atributos, seleccione estos atributos:**Client-IP-Address**: introduzca la dirección IP del cliente AAA. En este ejemplo, se ingresa la dirección IP del WLC para que la política se aplique a los paquetes del



WLC. **Grupos de Windows**: seleccione el grupo de Windows (el grupo de usuarios) para el que se aplicará la directiva. Aquí tiene un

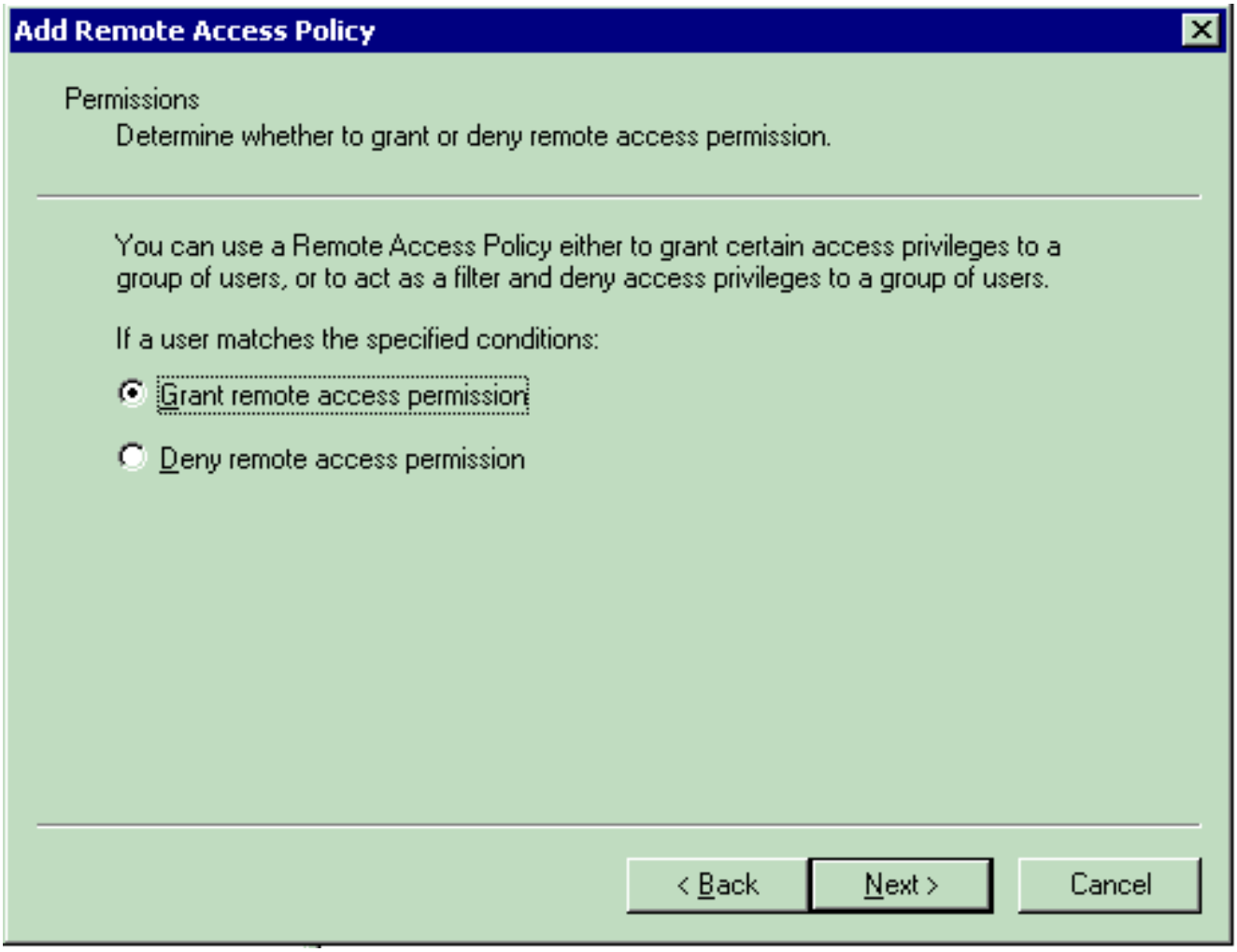


ejemplo:

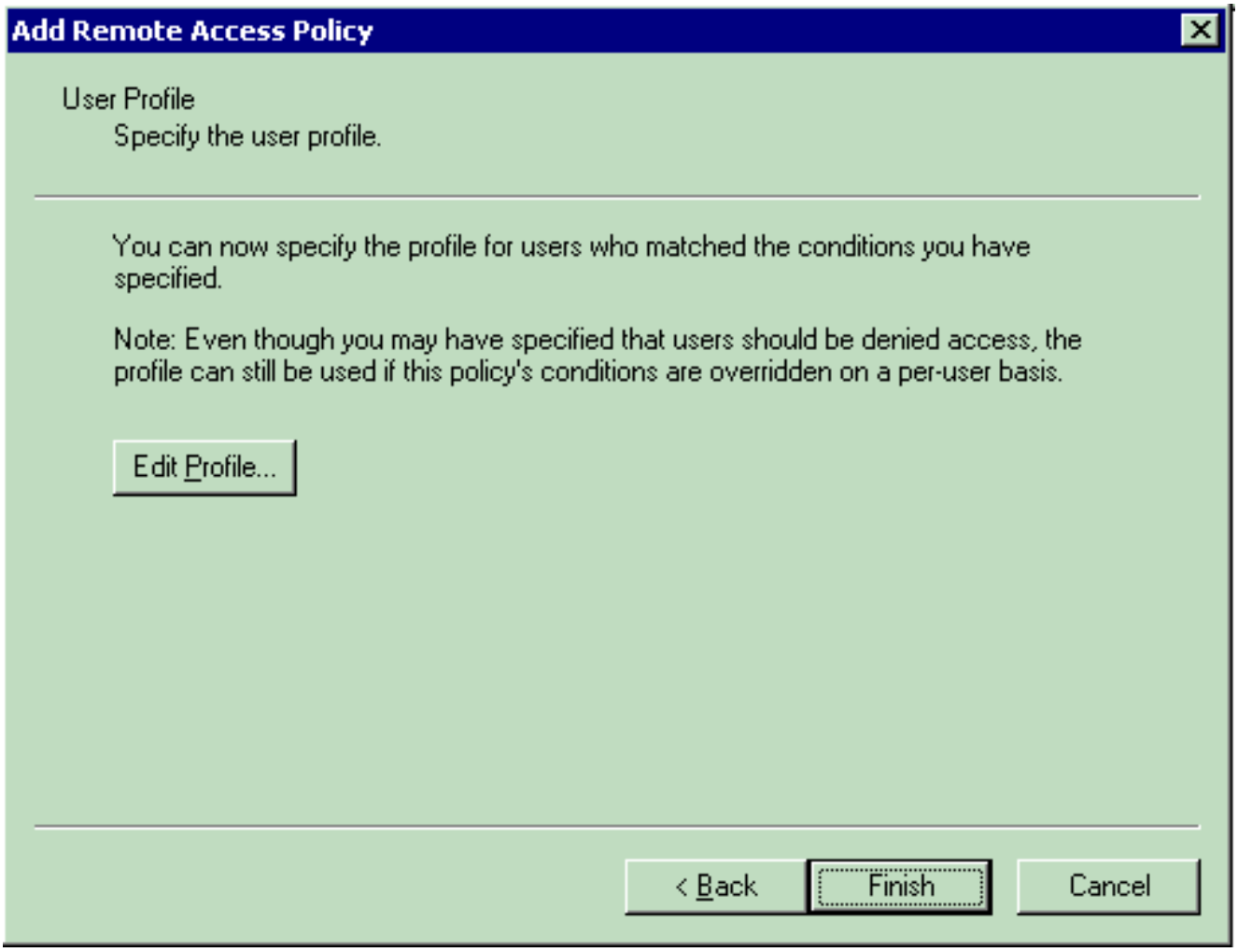


Este ejemplo muestra sólo dos condiciones. Si hay más condiciones, agregue también esas condiciones y haga clic en **Siguiente**.Aparecerá la ventana Permisos.

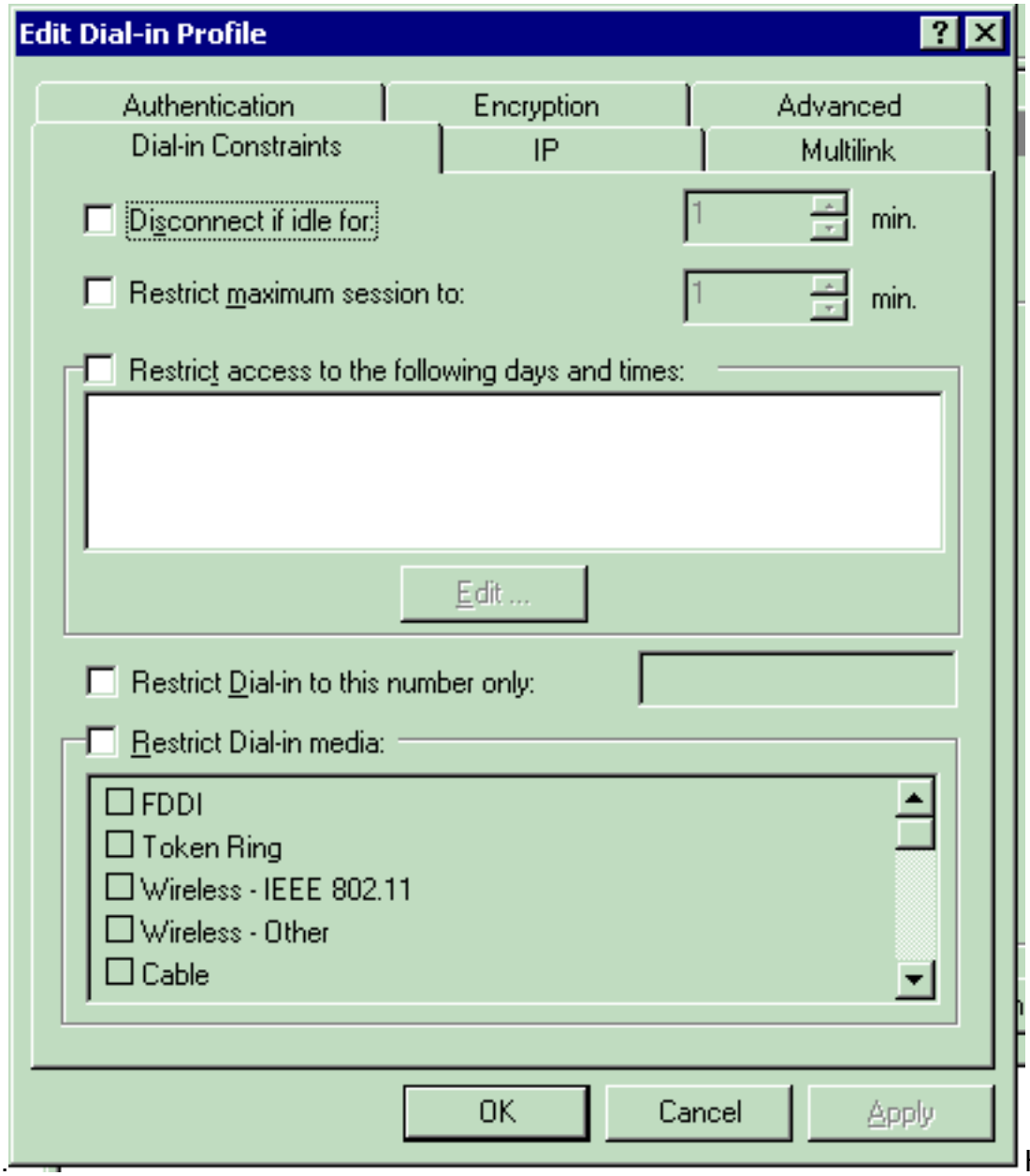
5. En la ventana Permisos, elija **Conceder permiso de acceso remoto**.Después de elegir esta opción, se dará acceso al usuario, siempre que el usuario coincida con las condiciones especificadas (desde el paso
2).



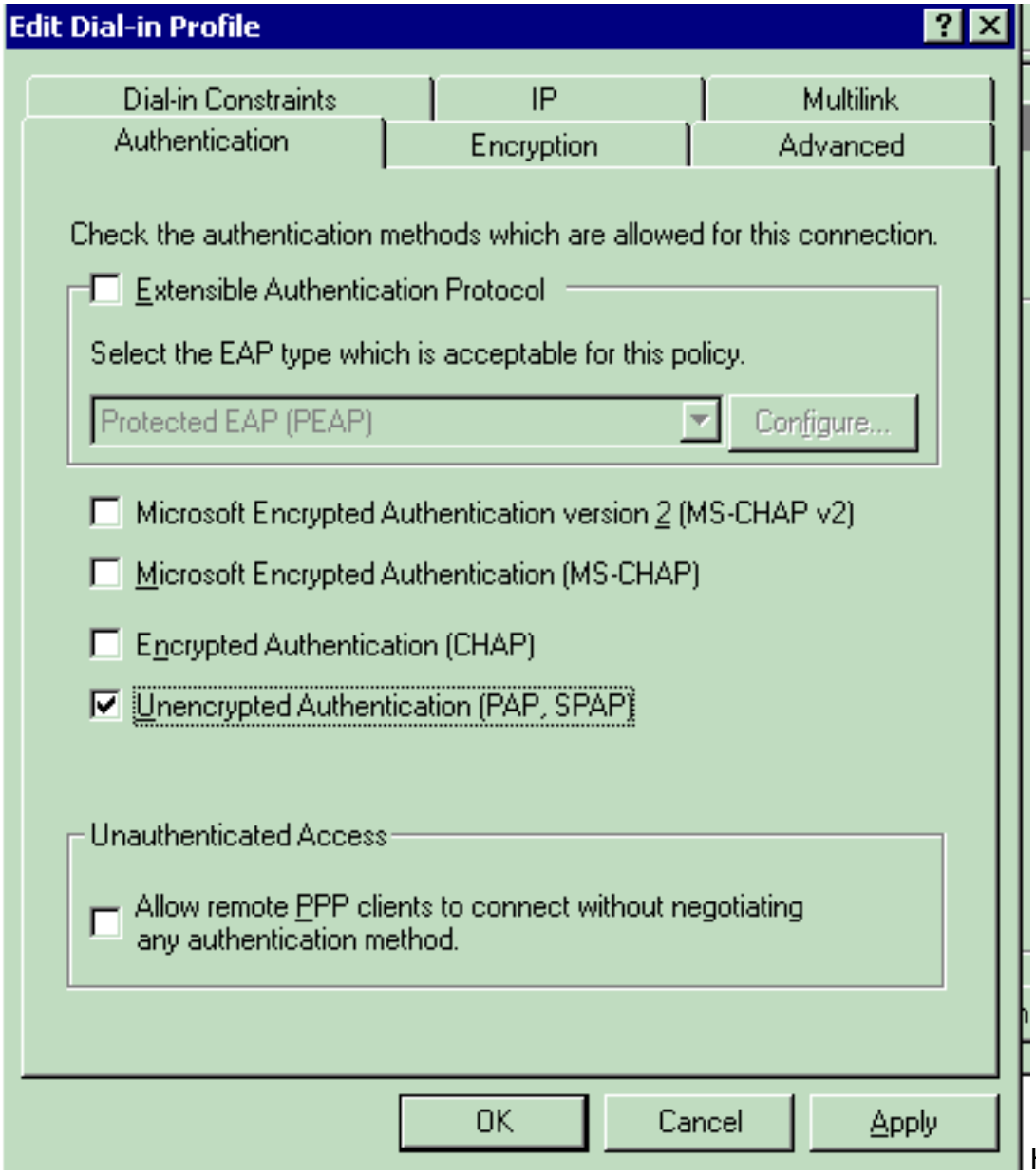
6. Haga clic en Next (Siguiente).
7. El siguiente paso es configurar el perfil de usuario.Aunque puede haber especificado que se debe denegar o conceder acceso a los usuarios en función de las condiciones, el perfil se puede seguir utilizando si se anulan las condiciones de esta política por usuario.



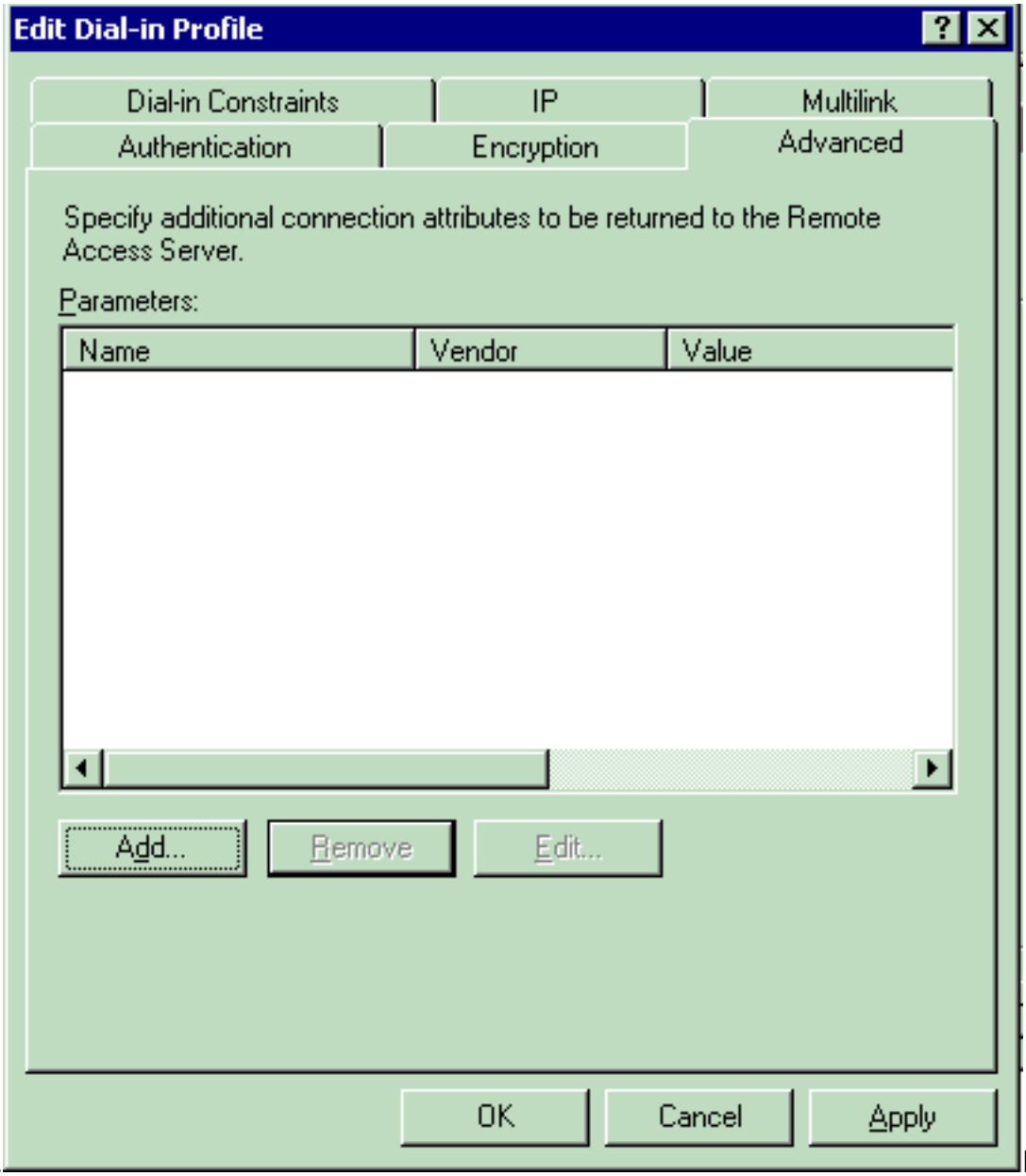
Para configurar el perfil de usuario, haga clic en **Editar perfil** en la ventana Perfil de usuario.Aparecerá la ventana Edit Dial-in Profile (Editar perfil de



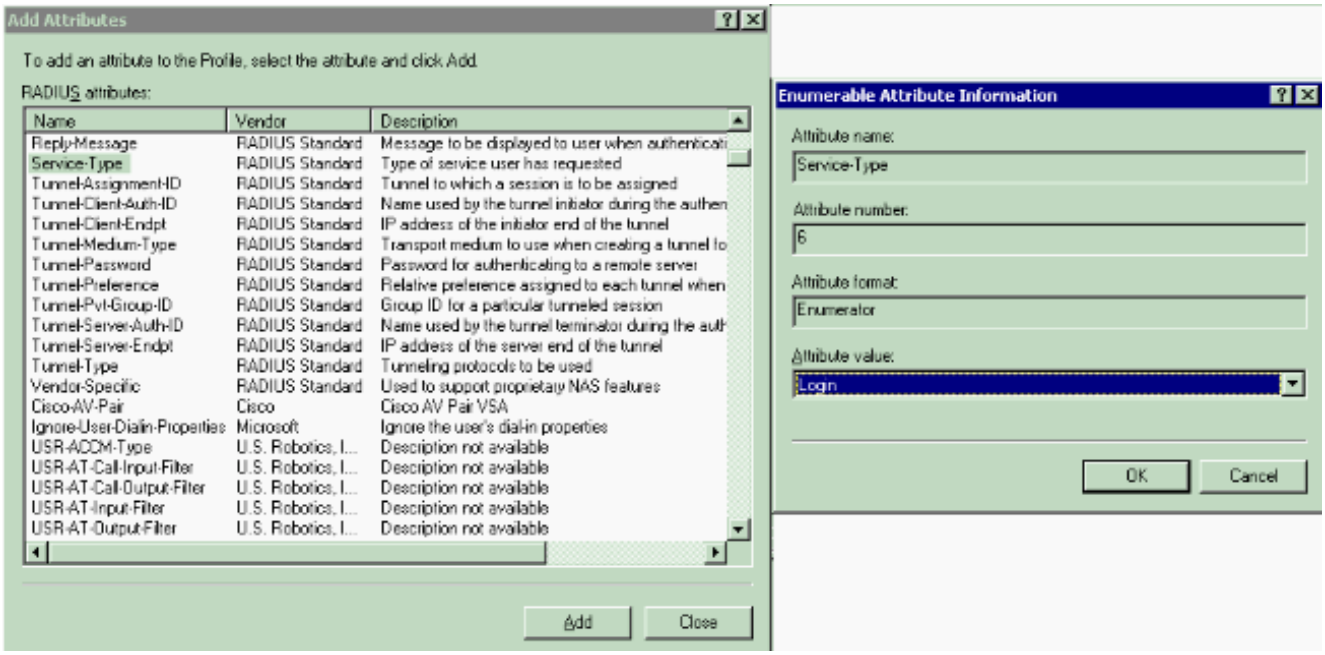
marcado). Haga clic en la ficha **Authentication** y luego elija el método de autenticación que se utiliza en la WLAN.Este ejemplo utiliza la autenticación no cifrada



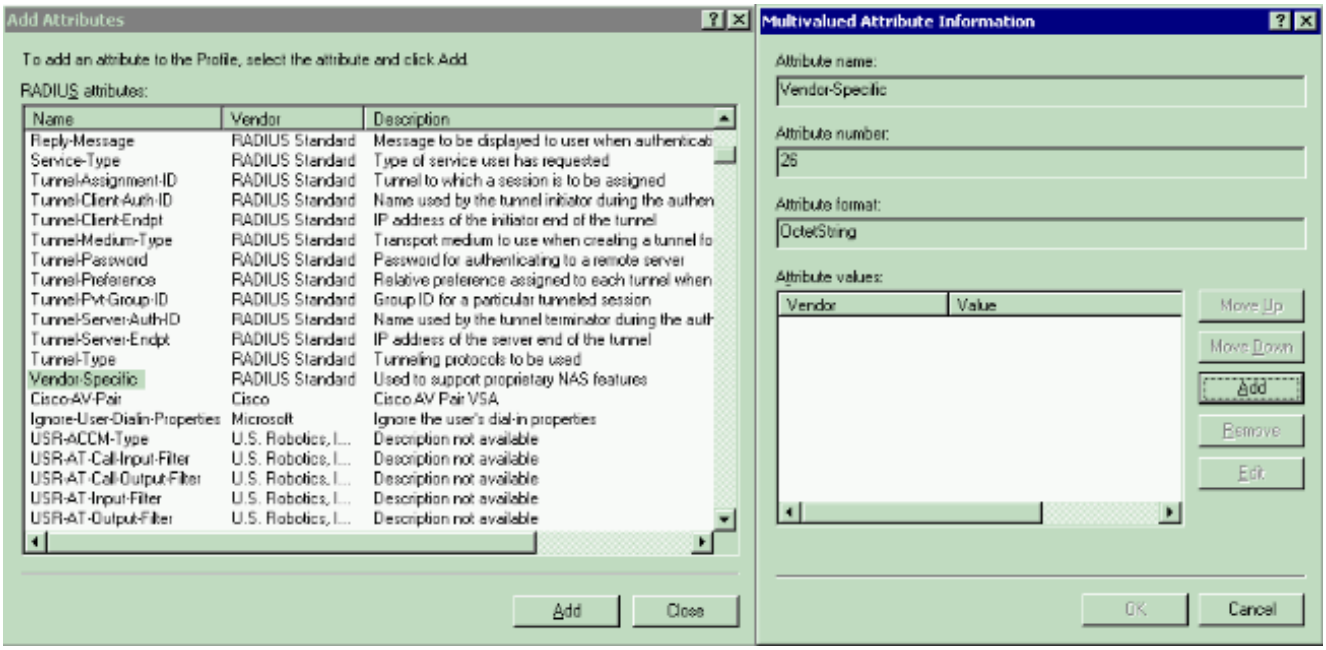
(PAP,SPAP). Haga clic en la ficha Advanced (Opciones avanzadas). Elimine todos los parámetros predeterminados y haga clic en



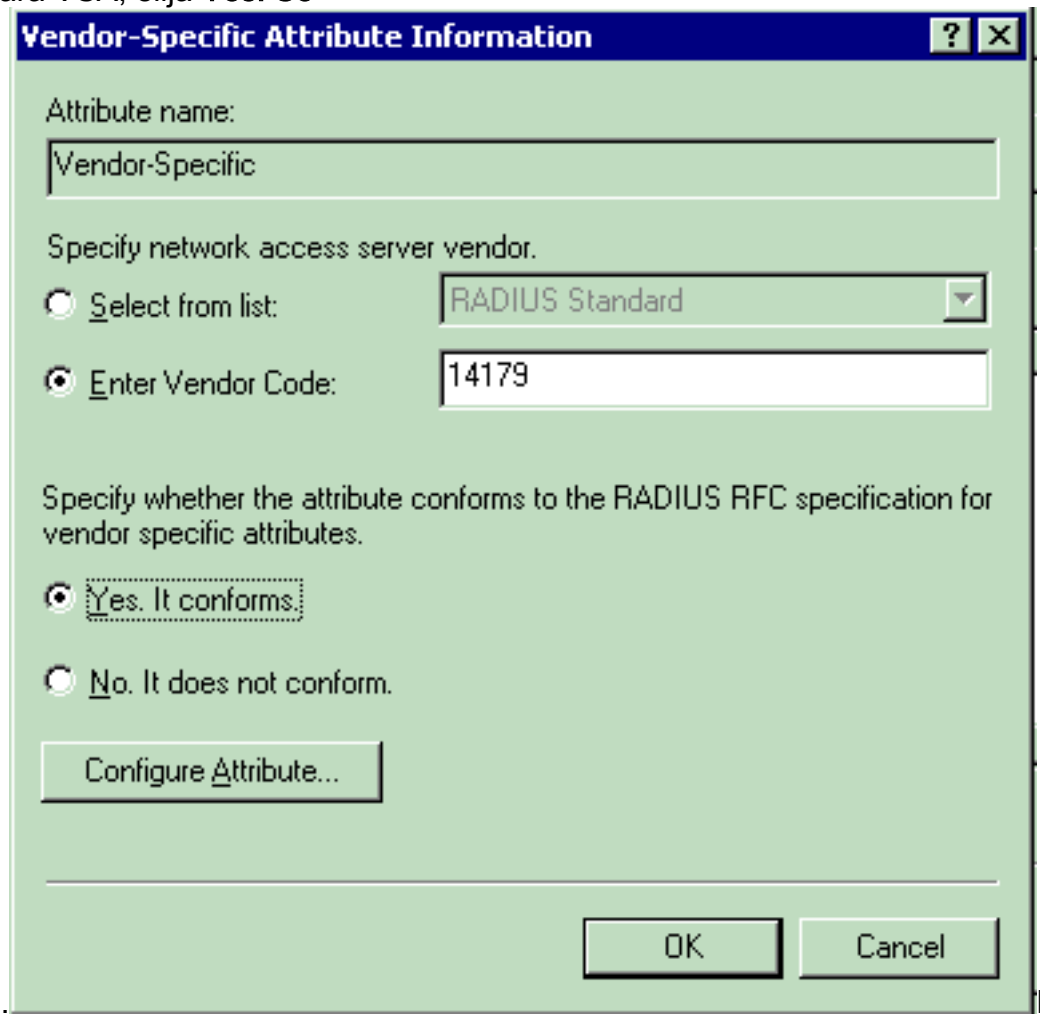
Agregar.En la ventana **Agregar atributos**, seleccione **Tipo de servicio** y, a continuación, elija el valor **Inicio de sesión** en la siguiente ventana.



A continuación, debe seleccionar el atributo **específico del proveedor** de la lista de atributos RADIUS.

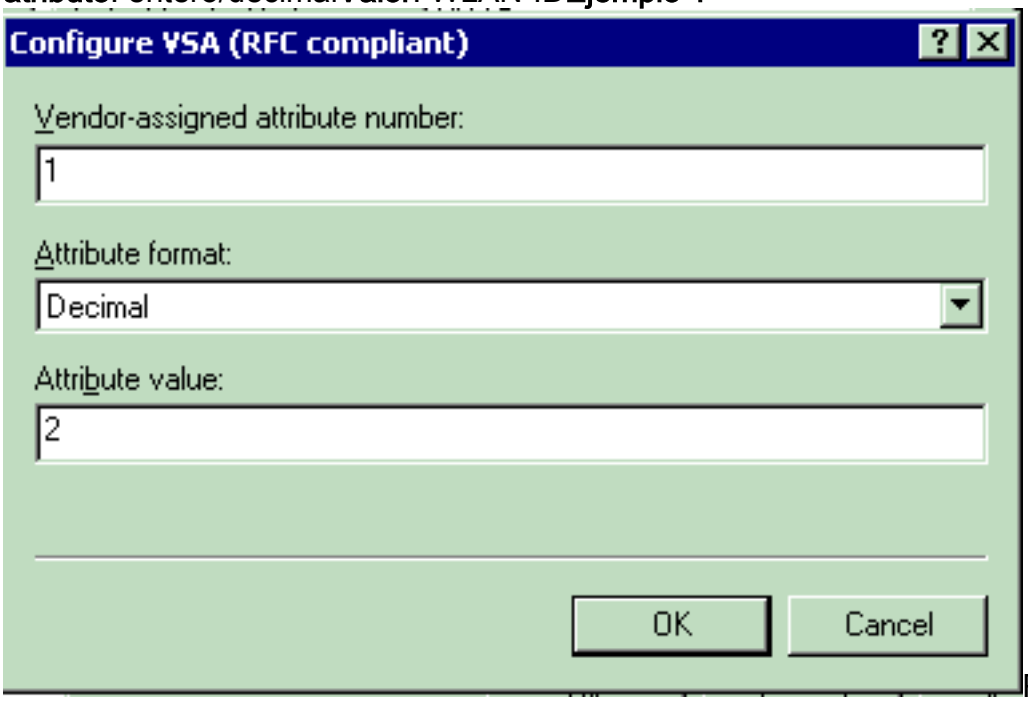


En la siguiente ventana, haga clic en **Agregar** para seleccionar un nuevo VSA.Aparecerá la ventana Información de atributo específica del proveedor.En Especificar proveedor de servidor de acceso a la red, elija **Introducir código del proveedor**.Introduzca el código del proveedor para VSA de Airespace. El Vendor Code (Código de proveedor) para los VSA de Cisco Airespace es 14179.Debido a que este atributo se ajusta a la especificación RADIUS RFC para VSA, elija **Yes. Se**

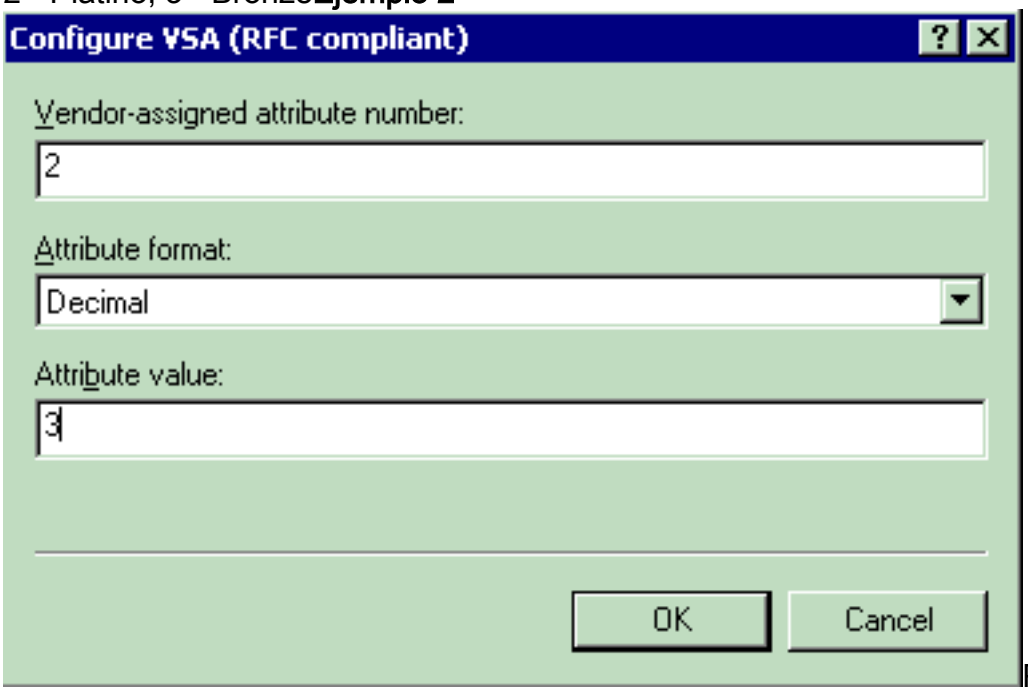


ajusta..Haga clic en **Configurar atributo**.En la ventana Configurar VSA (compatible con RFC), introduzca el

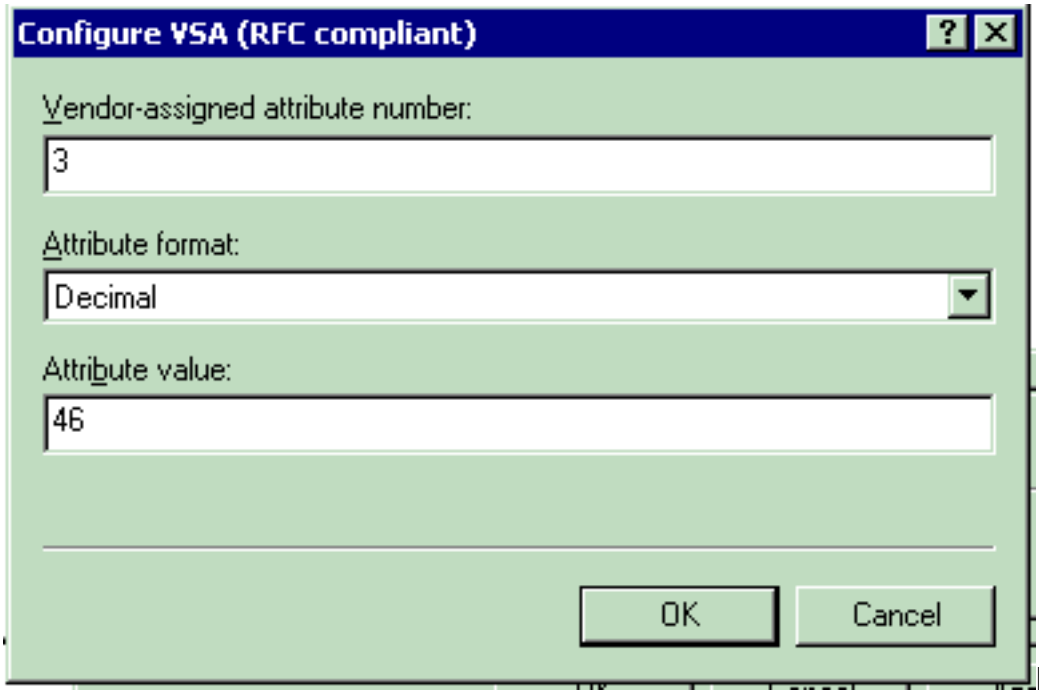
número de atributo asignado por el proveedor, el formato de atributo y el valor de atributo, que dependen del VSA que desea utilizar.Para configurar el WLAN-ID por usuario:**Nombre de atributo**: Airespace-WLAN-Id**Número de atributo asignado por el proveedor**: 1**Formato de atributo**: entero/decimal**Valor**: WLAN-ID**Ejemplo 1**



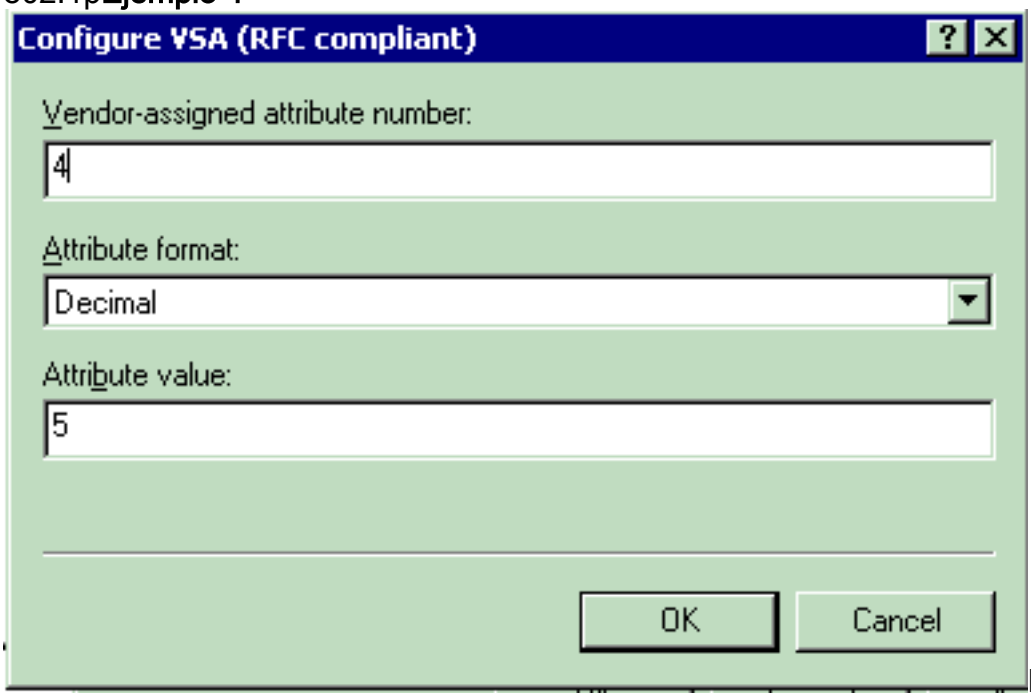
Para configurar el perfil de QoS por usuario:**Nombre de atributo**: Airespace-QoS-Level**Número de atributo asignado por el proveedor**: 2**Formato de atributo**: entero/decimal**Valor**: 0 - Plateado; 1 - Oro; 2 - Platino; 3 - Bronze**Ejemplo 2**



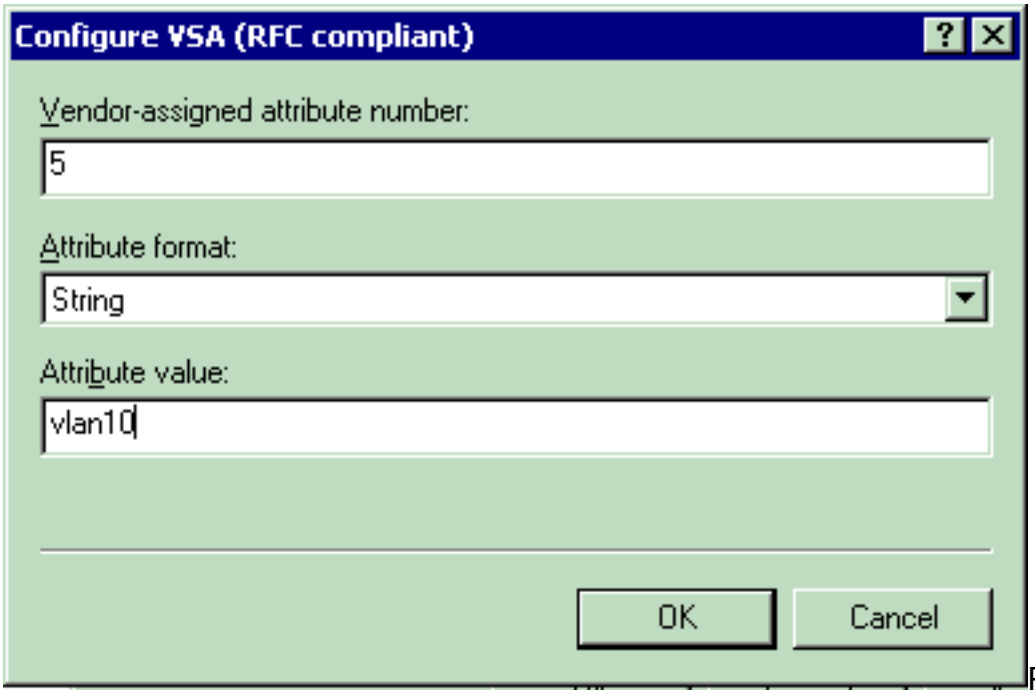
Para establecer el valor DSCP por usuario:**Nombre de atributo**: Airespace-DSCP**Número de atributo asignado por el proveedor**: 3**Formato de atributo**: entero/decimal**Valor**: valor DSCP**Ejemplo 3**



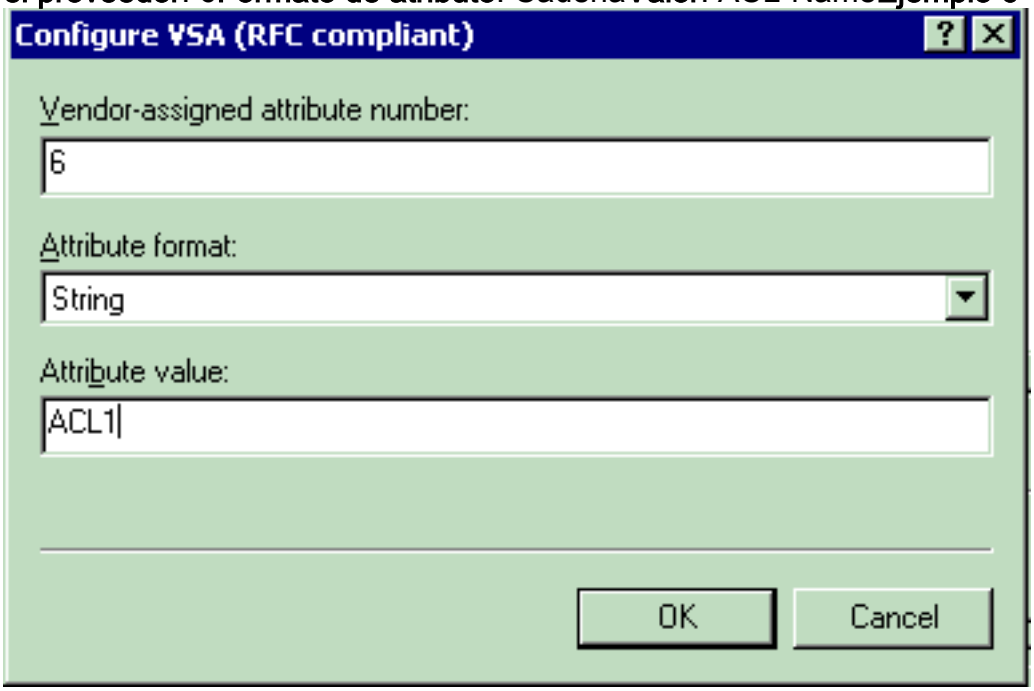
Para configurar la etiqueta 802.1p por usuario:**Nombre de atributo**: Airespace-802.1p-Tag**Número de atributo asignado por el proveedor**: 4**Formato de atributo**: entero/decimal**Valor**: etiqueta 802.1p**Ejemplo 4**



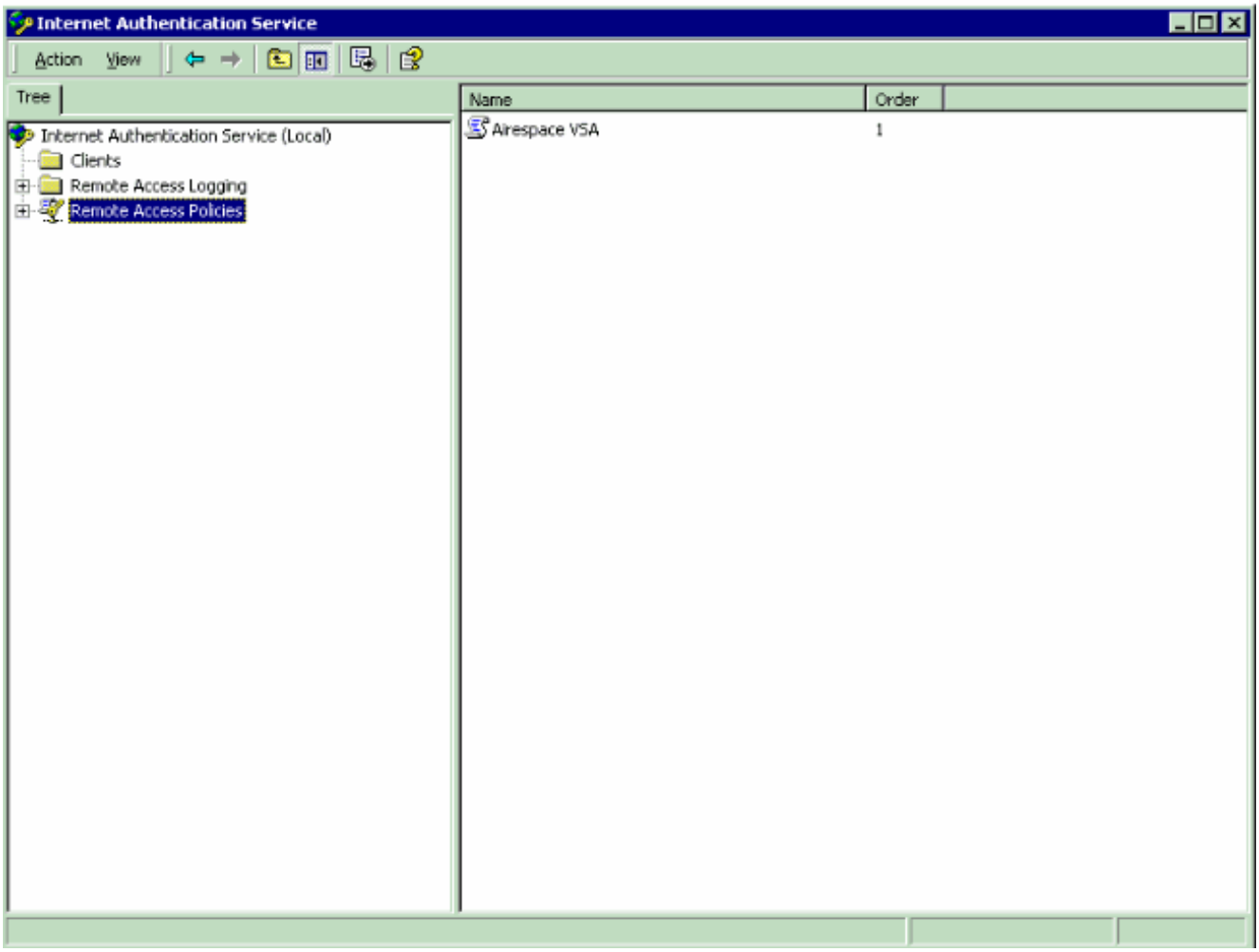
Para configurar la interfaz (VLAN) por usuario:**Nombre de atributo**: Airespace-Interface-Name**Número de atributo asignado por el proveedor**: 5**Formato de atributo**: Cadena**Valor**: Interface-Name**Ejemplo 5**



Para configurar la ACL por usuario:**Nombre de atributo**: Airespace-ACL-Name**Número de atributo asignado por el proveedor**: 6**Formato de atributo**: Cadena**Valor**: ACL-Name**Ejemplo 6**

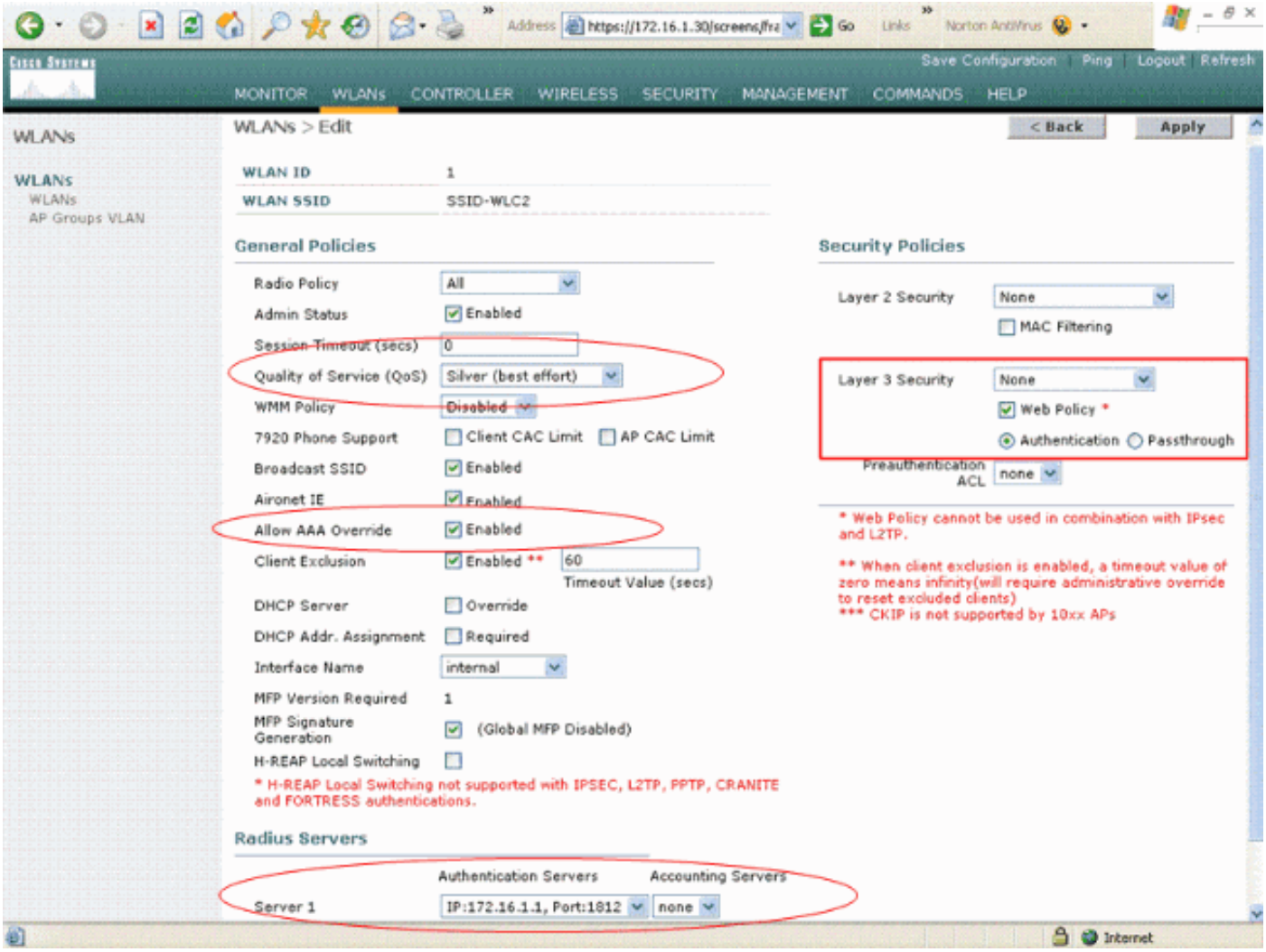


8. Una vez que haya configurado los VSA, haga clic en **Aceptar** hasta que vea la ventana Perfil de usuario.
9. A continuación, haga clic en **Finalizar** para completar la configuración.Puede ver la nueva política en Políticas de acceso
remoto.



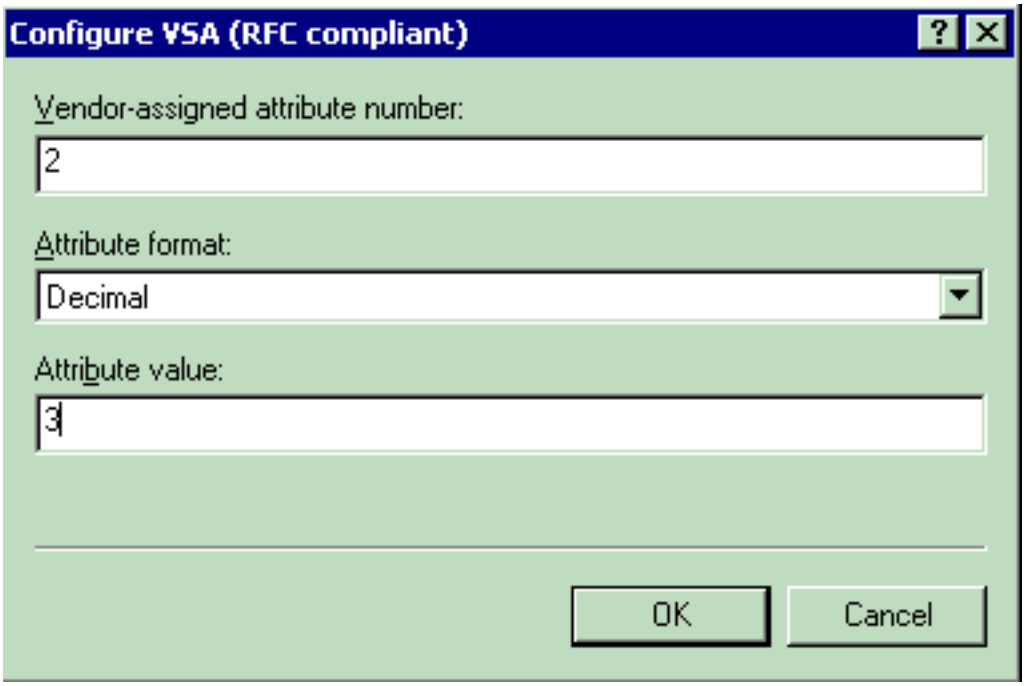
Ejemplo de configuración

En este ejemplo, se configura una WLAN para la autenticación web. El servidor IAS RADIUS autentica a los usuarios y el servidor RADIUS se configura para asignar políticas de QoS por usuario.



Como puede ver en esta ventana, la autenticación web está habilitada, el servidor de autenticación es 172.16.1.1, y el reemplazo AAA también está habilitado en la WLAN. La configuración de QoS predeterminada para esta WLAN está establecida en Silver.

En el servidor IAS RADIUS, se configura una política de acceso remoto que devuelve el atributo QoS Bronze en la solicitud de aceptación RADIUS. Esto se hace cuando configura el VSA específico para el atributo QoS.



Consulte la sección Configuración de la Política de Acceso Remoto en el IAS de este documento para obtener información detallada sobre cómo configurar una Política de Acceso Remoto en el servidor IAS.

Una vez que el servidor IAS, el WLC y el LAP se configuran para esta configuración, los clientes inalámbricos pueden utilizar la autenticación web para conectarse.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Cuando el usuario se conecta a la WLAN con un ID de usuario y una contraseña, el WLC pasa las credenciales al servidor IAS RADIUS que autentica al usuario con las condiciones y el perfil de usuario configurados en la política de acceso remoto. Si la autenticación de usuario es exitosa, el servidor RADIUS devuelve una solicitud de aceptación RADIUS que también contiene los valores de invalidación AAA. En este caso, se devuelve la política de QoS del usuario.

Puede ejecutar el comando **debug aaa all enable** para ver la secuencia de eventos que ocurre durante la autenticación. Éste es un ejemplo de salida:

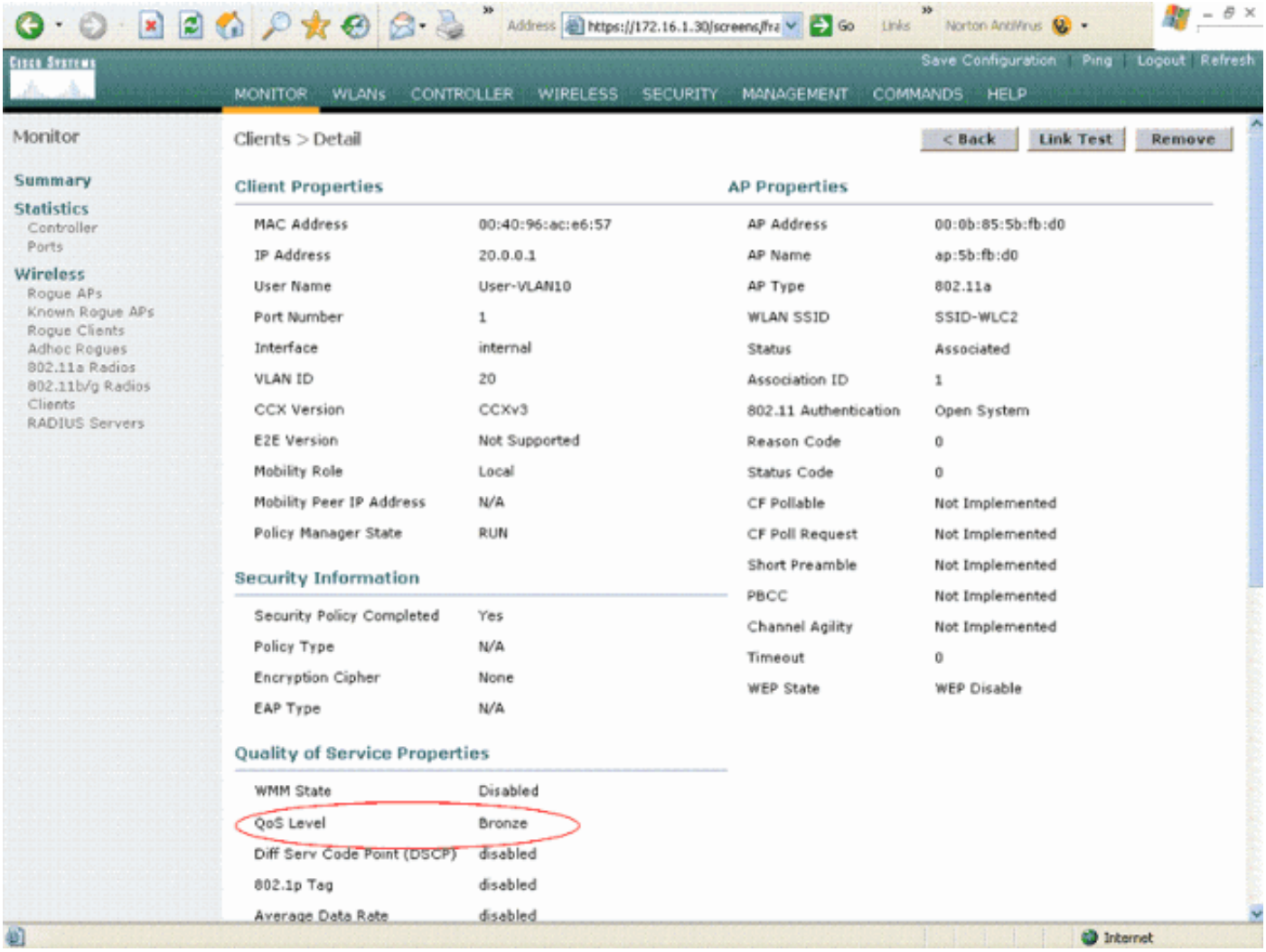
```
(Cisco Controller) > debug aaa all enable
Wed Apr 18 18:14:24 2007: User admin authenticated
Wed Apr 18 18:14:24 2007: 28:1f:00:00:00:00 Returning AAA Error 'Success' (0) for
                          mobile 28:1f:00:00:00:00
Wed Apr 18 18:14:24 2007: AuthorizationResponse: 0xbadff97c
Wed Apr 18 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 puede ver en el resultado, el usuario se autentica. Luego, los valores de invalidación AAA se devuelven con el mensaje RADIUS accept. En este caso, se da al usuario la política de QoS de Bronze.

También puede verificar esto en la GUI del WLC. Aquí tiene un ejemplo:



Nota: El perfil de QoS predeterminado para este SSID es Silver. Sin embargo, debido a que se selecciona la invalidación de AAA y el usuario se configura con un perfil de QoS de Bronze en el servidor IAS, se invalida el perfil de QoS predeterminado.

Troubleshoot

Puede utilizar el comando **debug aaa all enable** en el WLC para resolver problemas de la configuración. Un ejemplo del resultado de esta depuración en una red en funcionamiento se muestra en la sección Verificar de este documento.

Nota: Consulte Información Importante sobre Comandos Debug antes de utilizar los comandos **debug**.

Información Relacionada

- Guía de configuración del Controlador de LAN de la Red Inalámbrica Cisco, versión 4.0
- Ejemplo de Restringir Acceso WLAN Basado en SSID con WLC y Cisco Secure ACS Configuration
- Soporte de Productos de Red Inalámbrica
- Soporte Técnico y Documentación - Cisco Systems