Exemplo de Configuração de VSAs Cisco Airespace no Microsoft IAS Radius Server

Contents

Introduction

Este documento mostra como configurar um servidor do Microsoft Internet Authentication Service (IAS) para oferecer suporte a Cisco Airespace VSAs (Vendor Specific Attributes). O código de fornecedor do VSA do Cisco Airespace é 14179.

Prerequisites

Requirements

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Conhecimento de como configurar um servidor IAS
- Conhecimento da configuração de LAPs (Lightweight Access Points) e WLCs (Wireless LAN Controllers, Controladores de LAN sem Fio) da Cisco
- Conhecimento das soluções Cisco Unified Wireless Security

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Servidor Microsoft Windows 2000 com IAS

- Cisco 4400 WLC que executa a versão de software 4.0.206.0
- Cisco 1000 Series LAPs
- Adaptador cliente sem fio 802.11 a/b/g com firmware 2.5
- Aironet Desktop Utility (ADU) versão 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.

Observação: este documento destina-se a dar ao leitor um exemplo da configuração necessária no servidor IAS para suportar VSAs do Cisco Airespace. A configuração do servidor IAS apresentada neste documento foi testada no laboratório e funciona como esperado. Se você tiver problemas para configurar o servidor IAS, entre em contato com a Microsoft para obter ajuda. O Cisco TAC não oferece suporte à configuração do servidor Microsoft Windows.

Este documento pressupõe que o WLC foi configurado para operação básica e que os LAPs foram registrados no WLC. Se você for um novo usuário tentando configurar a WLC para a operação básica com LAPs, consulte Lightweight AP (LAP) Registration to a Wireless LAN Controller (WLC).

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

Na maioria dos sistemas de LAN sem fio (WLAN), cada WLAN tem uma política estática que se aplica a todos os clientes associados a um SSID (Service Set Identifier). Embora poderoso, este método tem limitações porque exige que os clientes se associem com os diferentes SSID para herdar diferentes QoS e políticas de segurança.

No entanto, a Cisco Wireless LAN Solution suporta redes de identidade, o que permite que a rede anuncie um único SSID e usuários específicos para herdar diferentes políticas de QoS ou segurança com base em seus perfis de usuário. As políticas específicas que você pode controlar usando a rede de identidade incluem:

- **Qualidade de Serviço** —Quando presente em uma Aceitação de Acesso RADIUS, o valor de Nível de QoS substitui o valor de QoS especificado no perfil de WLAN.
- **ACL** —Quando o atributo Access Control List (ACL) está presente na Aceitação de Acesso RADIUS, o sistema aplica o ACL-Name à estação cliente depois de autenticar. Isso substitui qualquer ACL atribuída à interface.
- **VLAN** —Quando um VLAN Interface-Name ou VLAN-Tag está presente em um RADIUS Access Accept, o sistema coloca o cliente em uma interface específica.
- **WLAN ID** —Quando o atributo WLAN-ID está presente na Aceitação de Acesso RADIUS, o sistema aplica a WLAN-ID (SSID) à estação cliente depois de se autenticar. O ID da WLAN é enviado pela WLC em todas as instâncias de autenticação, exceto IPSec. No caso da autenticação da Web, se a WLC receber um atributo WLAN-ID na resposta de autenticação do servidor AAA e não corresponder à ID da WLAN, a autenticação será rejeitada. Outros tipos de métodos de segurança não fazem isso.

- **Valor de DSCP** — Quando presente em uma Aceitação de Acesso RADIUS, o valor de DSCP substitui o valor de DSCP especificado no perfil de WLAN.
- **802.1p-Tag**—Quando presente em uma Aceitação de Acesso RADIUS, o valor 802.1p substitui o padrão especificado no perfil da WLAN.

Observação: o recurso de VLAN só suporta filtragem de MAC, 802.1X e Wi-Fi Protected Access (WPA). O recurso de VLAN não suporta autenticação da Web ou IPSec. O banco de dados de Filtro MAC local do sistema operacional foi estendido para incluir o nome da interface. Isso permite que os filtros MAC locais especifiquem qual interface o cliente deve receber. Um servidor RADIUS separado também pode ser usado, mas o servidor RADIUS deve ser definido usando os menus de segurança.

Consulte Configuração de Redes de Identidade para obter mais informações sobre redes de identidade.

Configurar o IAS para VSAs Airespace

Para configurar o IAS para VSAs do Airespace, você precisa concluir estas etapas:

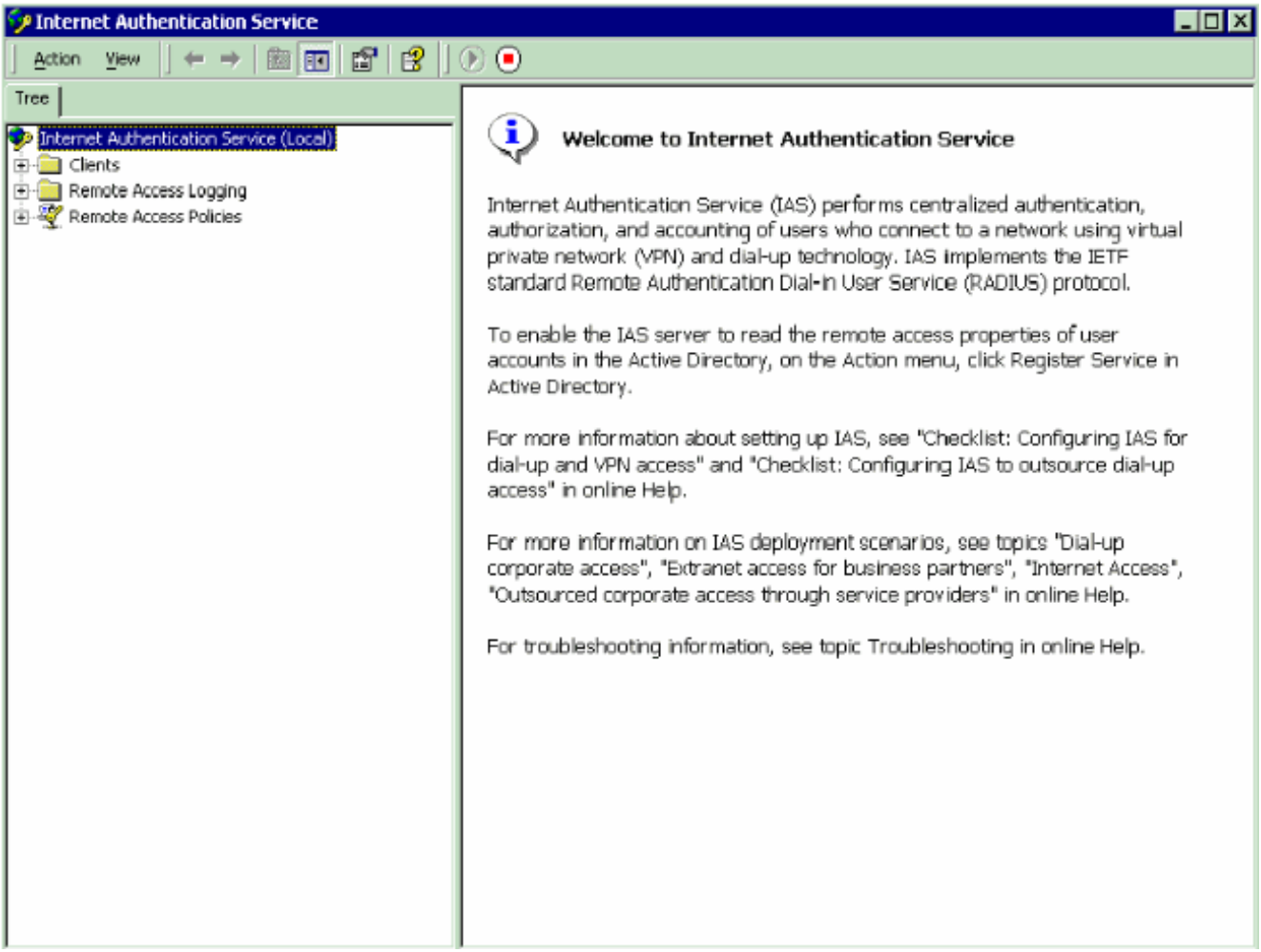
1. Configurar o WLC como um cliente AAA no IAS
2. Configurar a política de acesso remoto no IAS

Observação: os VSAs são configurados na Política de acesso remoto.

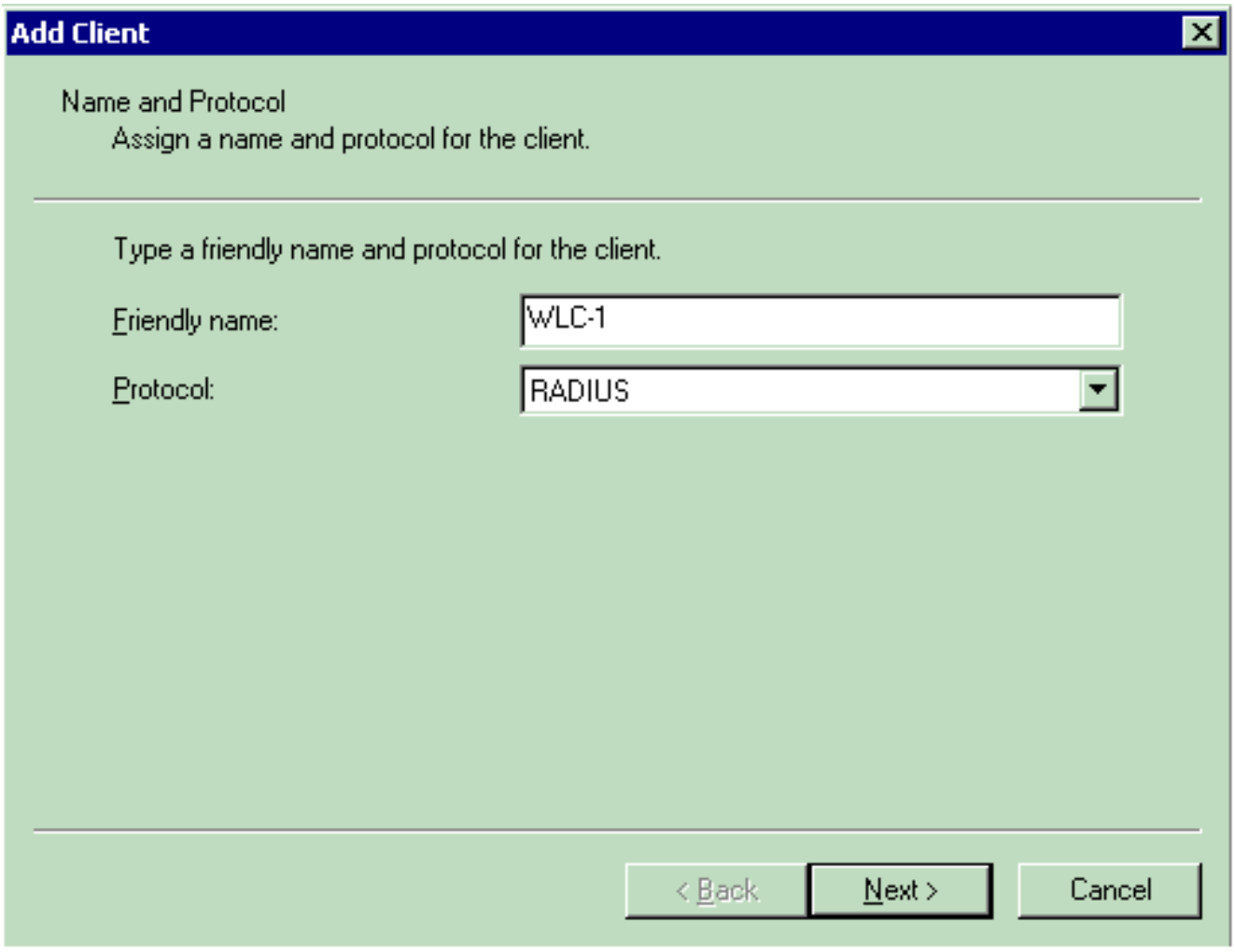
Configurar o WLC como um cliente AAA no IAS

Conclua estes passos para configurar a WLC como um cliente AAA no IAS:

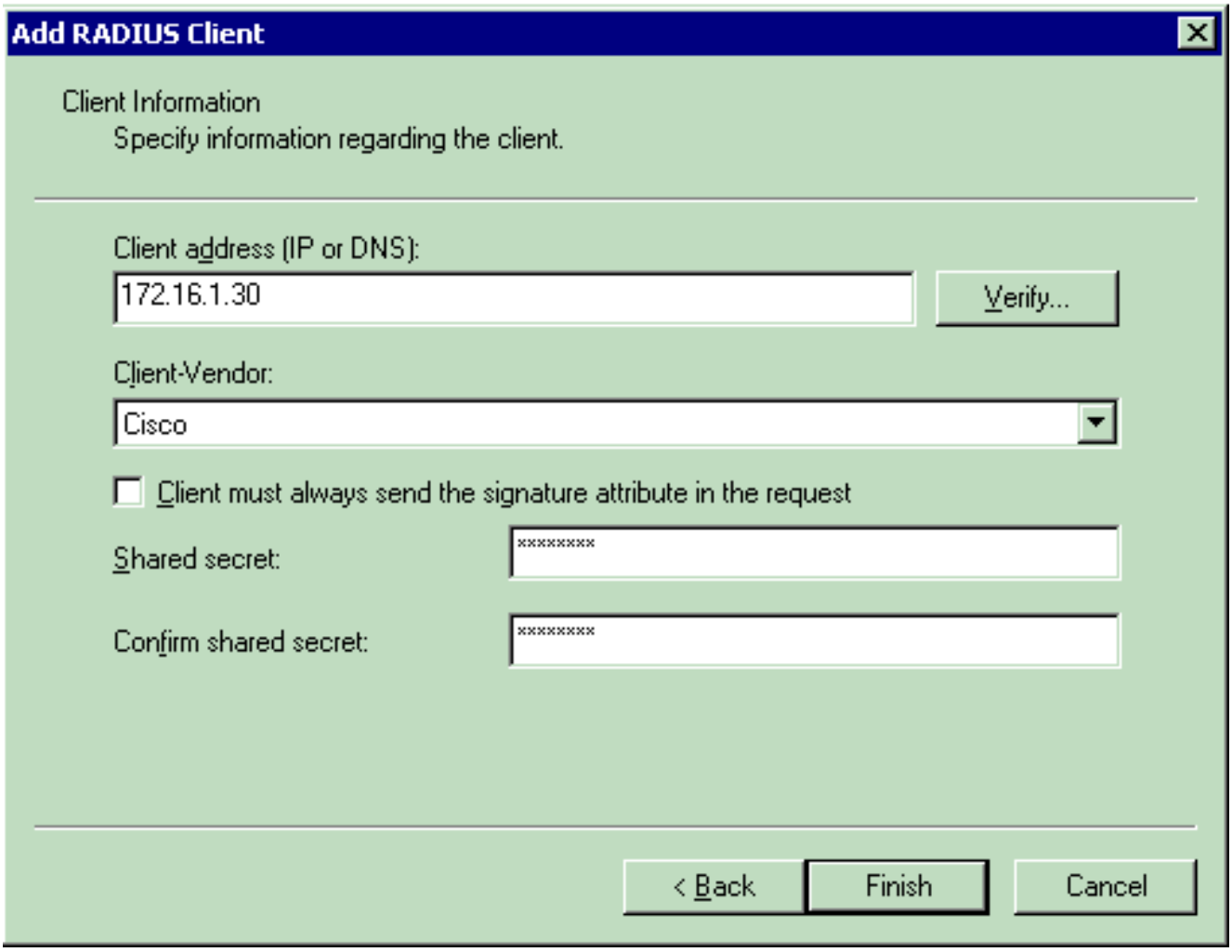
1. Clique em **Programas > Ferramentas Administrativas > Internet Authentication Service** para iniciar o IAS no servidor Microsoft
   2000.



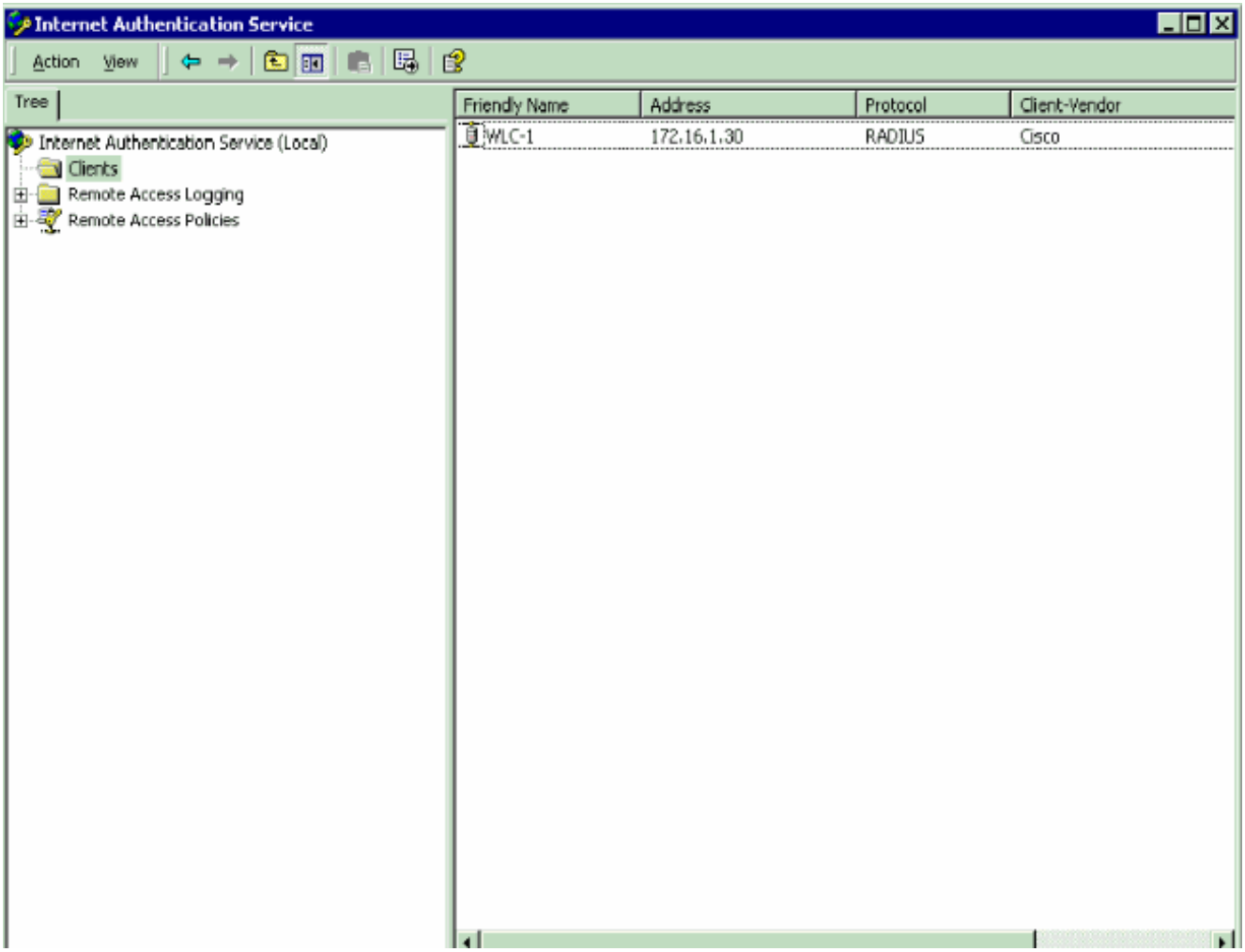
2. Clique com o botão direito do mouse na pasta **Clients** e escolha **New Client** para adicionar um novo cliente RADIUS.
3. Na janela Add Client (Adicionar cliente), digite o nome do cliente e escolha **RADIUS** como o Protocolo. Em seguida, clique em **Avançar**.Neste exemplo, o nome do cliente é *WLC-1*.**Observação:** por padrão, o protocolo é definido como RADIUS.



4. Na janela Add RADIUS Client (Adicionar cliente RADIUS), insira o **endereço IP do cliente**, **Client-Vendor** e **Shared secret**. Depois de inserir as informações do cliente, clique em **Concluir**.Este exemplo mostra um cliente chamado *WLC-1* com um endereço IP de *172.16.1.30*, o Client-Vendor está definido como *Cisco* e o segredo compartilhado é *cisco123*:



Com essas informações, a WLC chamada WLC-1 é adicionada como cliente AAA do servidor
IAS.

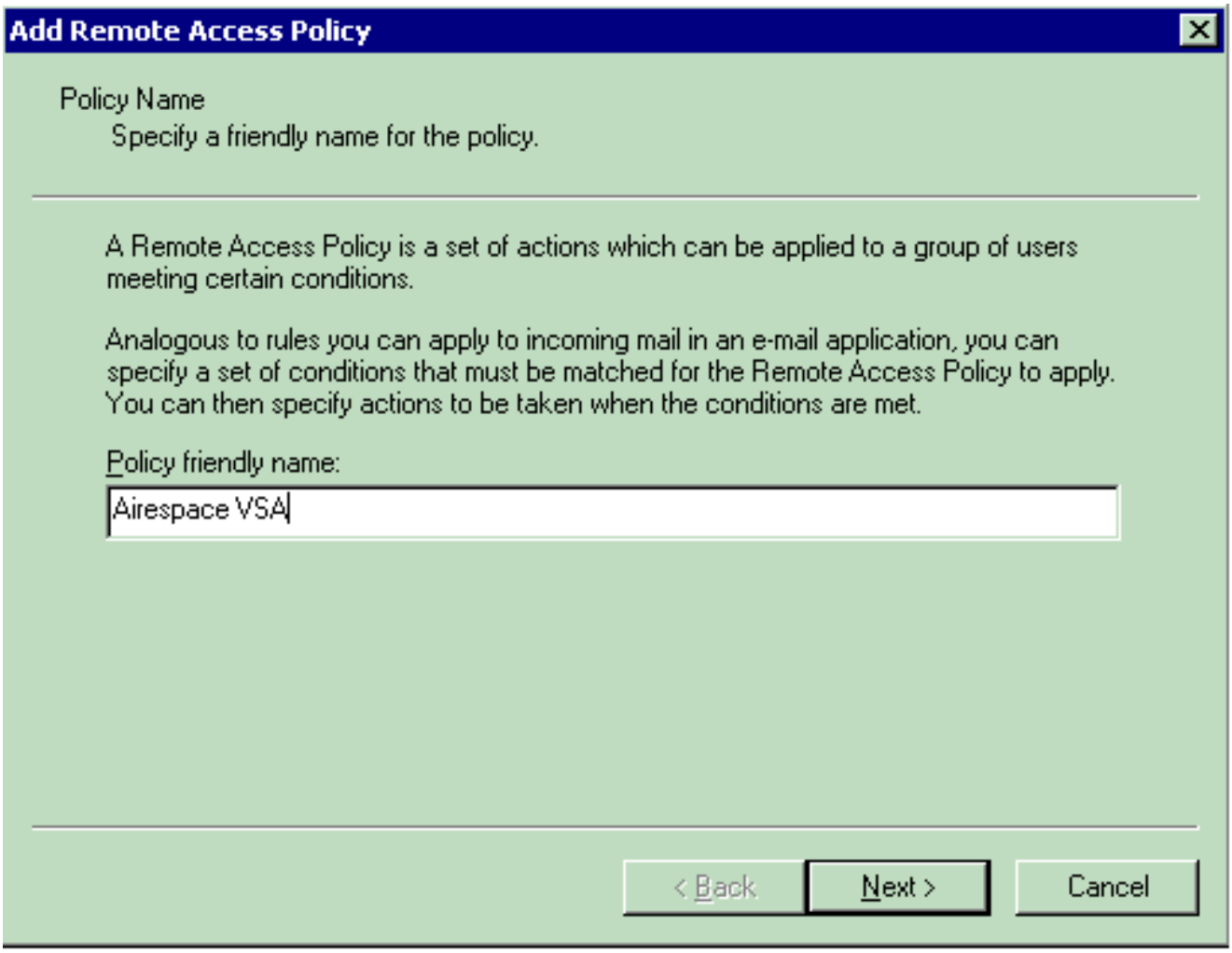


A próxima etapa é criar uma política de acesso remoto e configurar os VSAs.

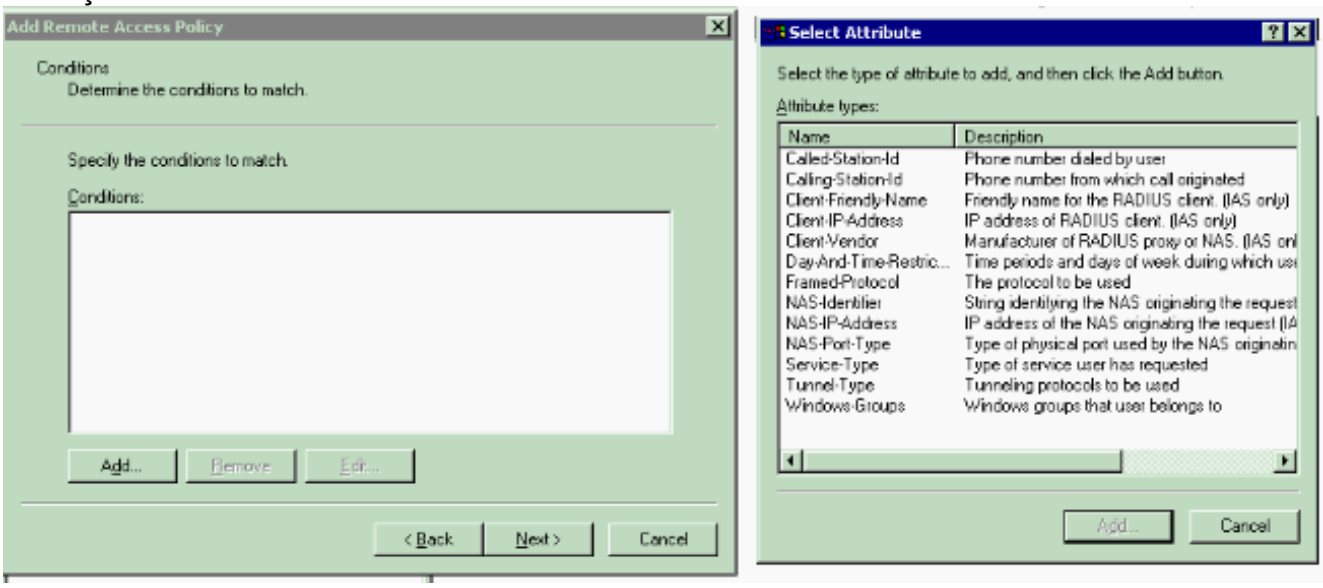
Configurar a política de acesso remoto no IAS

Conclua estes passos para configurar uma nova política de acesso remoto no IAS:

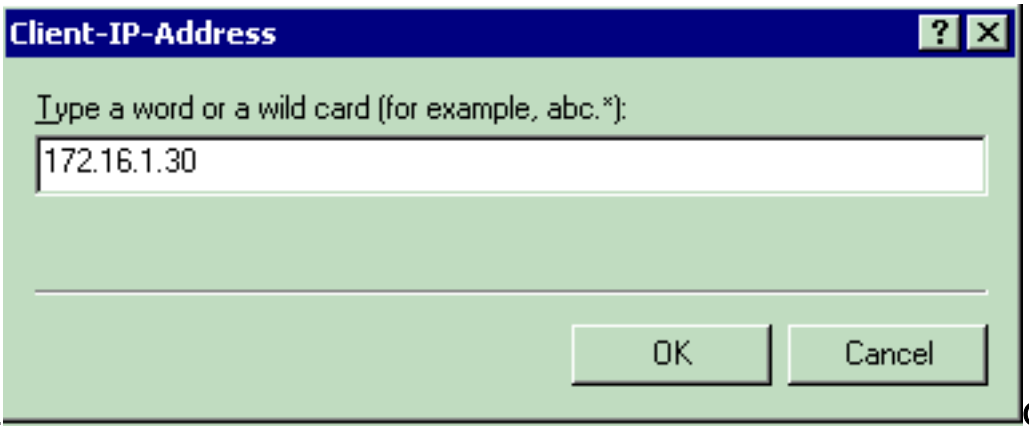
1. Clique com o botão direito do mouse em **Remote Access Policies** e escolha **New Remote AccessMS Policy**.A janela Nome da política é exibida.
2. Insira o nome da diretiva e clique em **Next (Avançar)**.



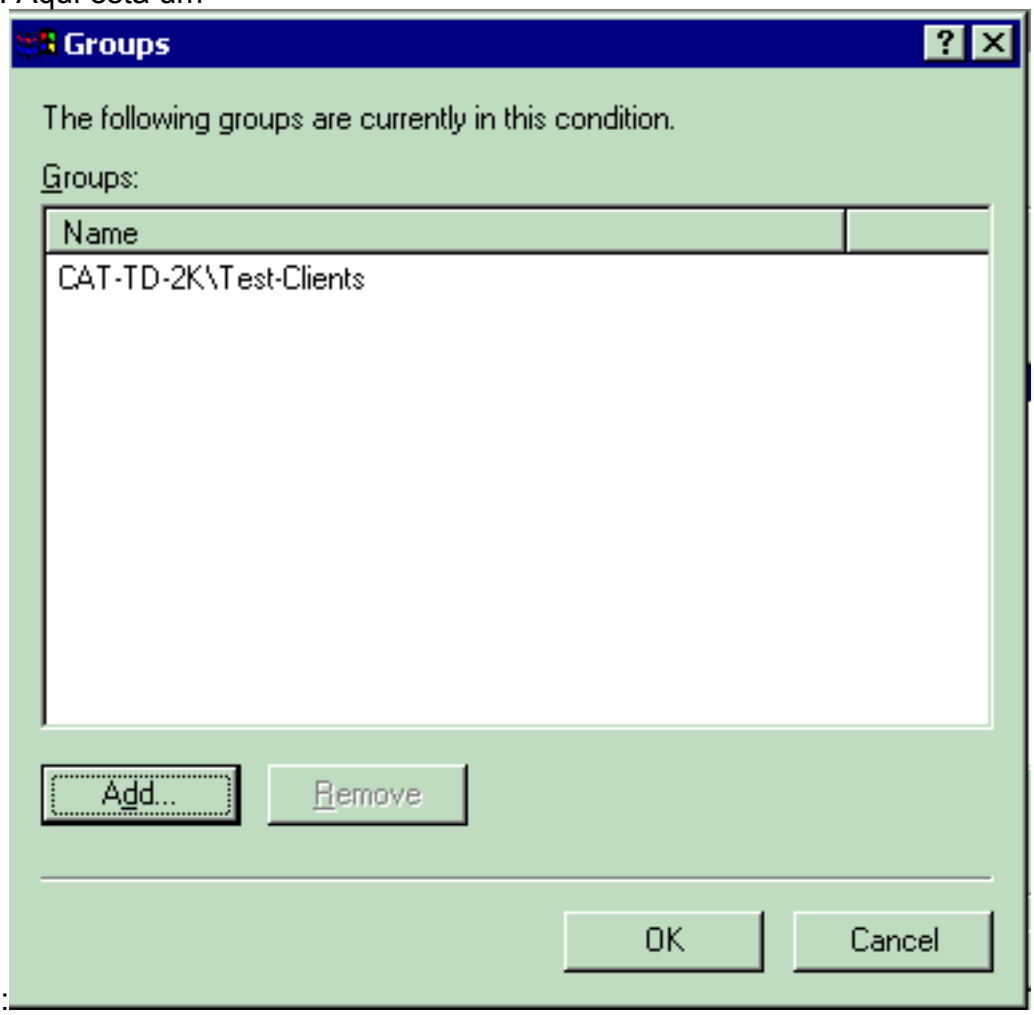
3. Na próxima janela, selecione as condições às quais a Diretiva de acesso remoto será aplicada. Clique em **Adicionar** para selecionar as condições.



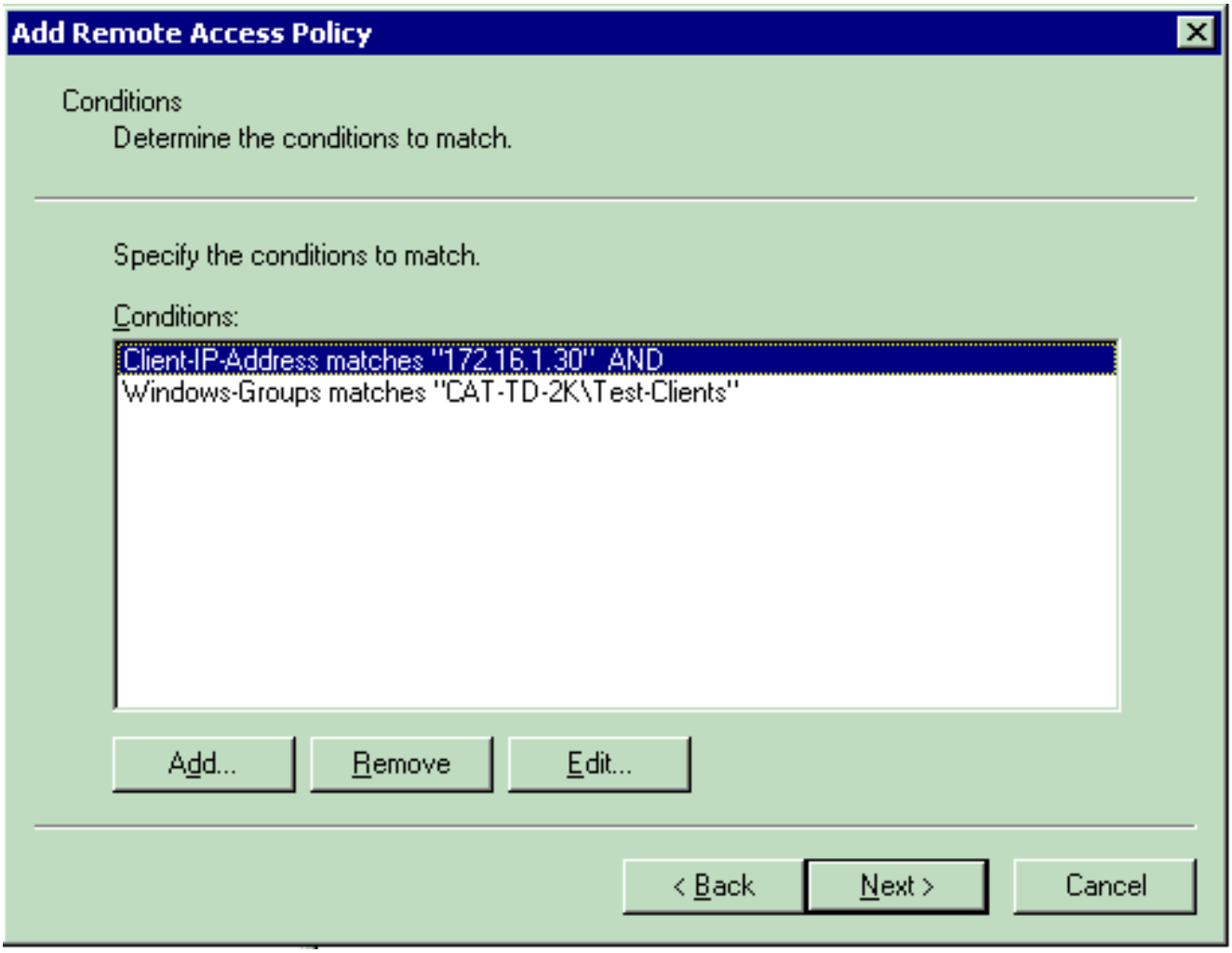
4. No menu Tipos de atributos, selecione estes atributos:**Client-IP-Address** — Insira o endereço IP do cliente AAA. Neste exemplo, o endereço IP das WLCs é inserido para que a política se aplique aos pacotes da



WLC. **Grupos do Windows** —Selecione o grupo do Windows (o grupo de usuários) ao qual a diretiva será aplicada. Aqui está um

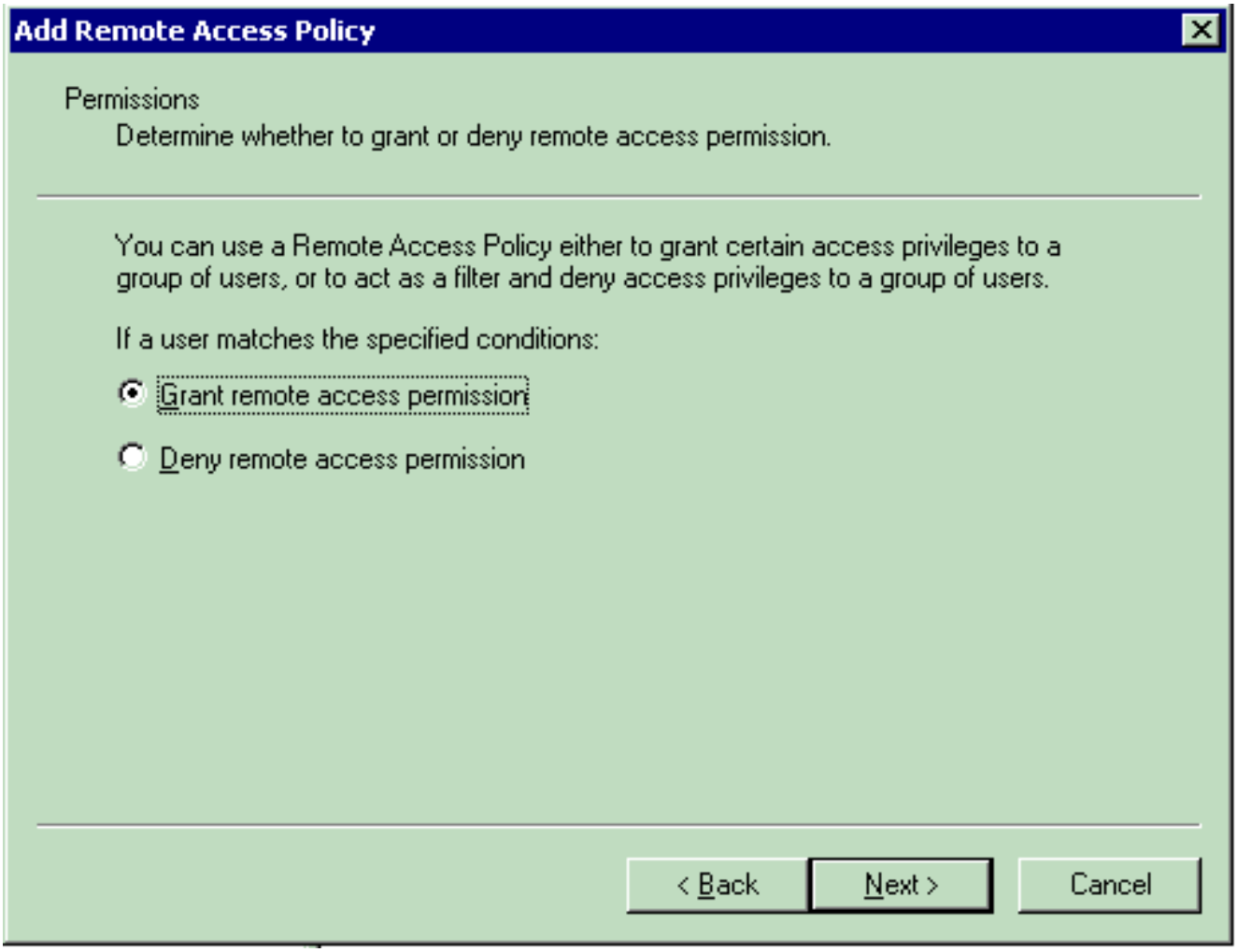


exemplo:

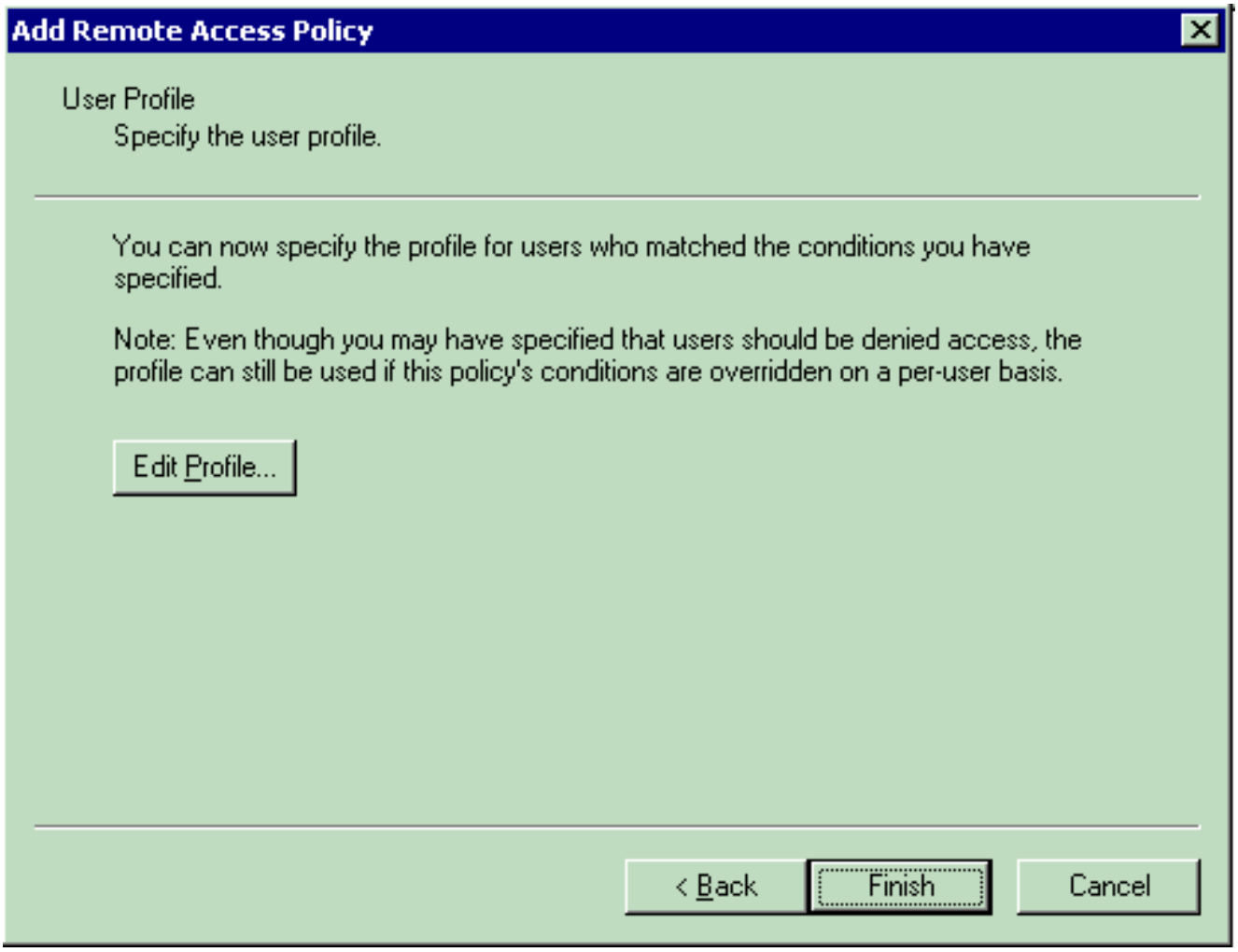


Este exemplo mostra apenas duas condições. Se houver mais condições, adicione essas condições também e clique em **Avançar**.A janela Permissões é exibida.

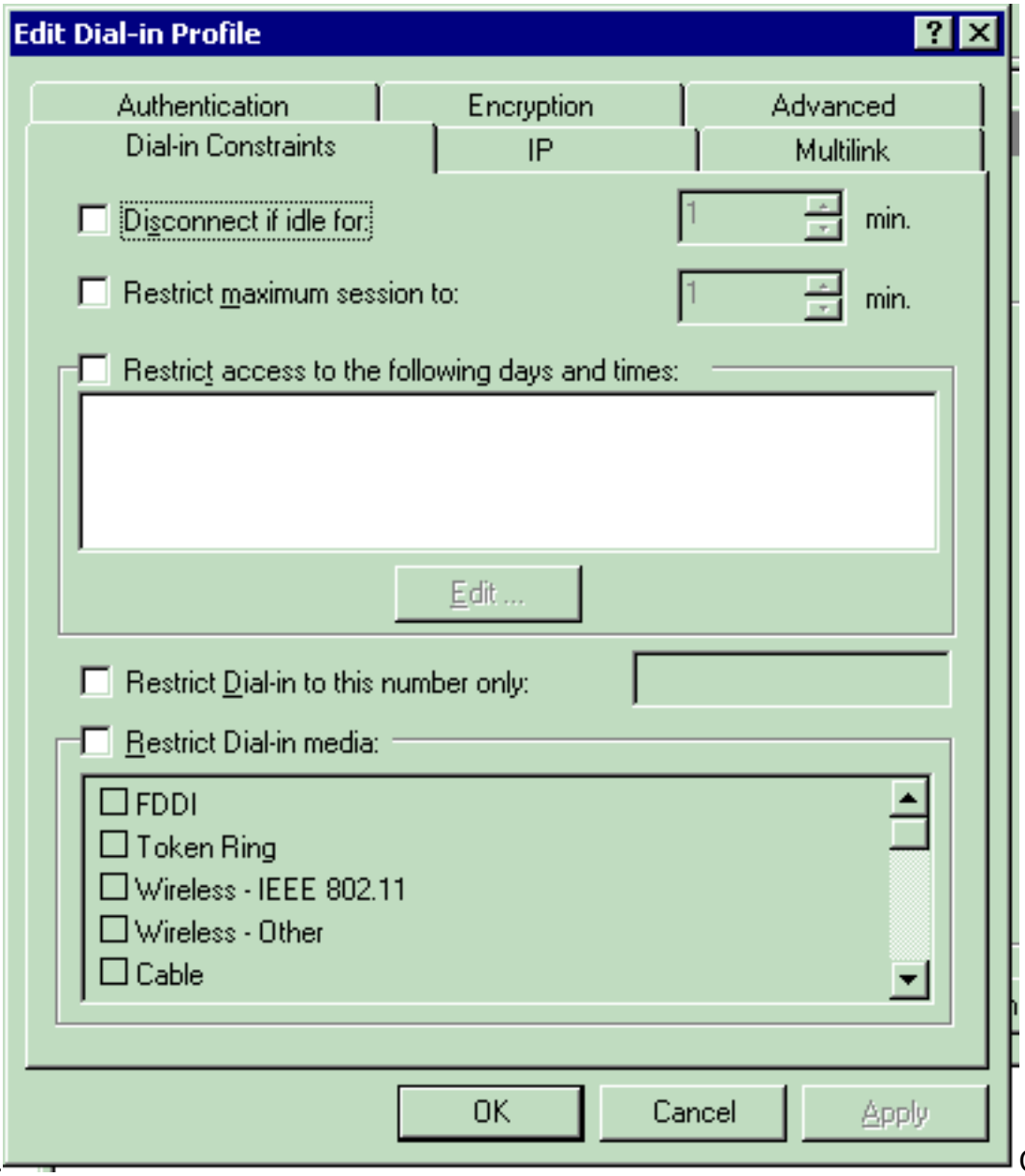
5. Na janela Permissões, escolha **Conceder permissão de acesso remoto**.Depois de escolher essa opção, o usuário recebe acesso, desde que corresponda às condições especificadas (da etapa
2).



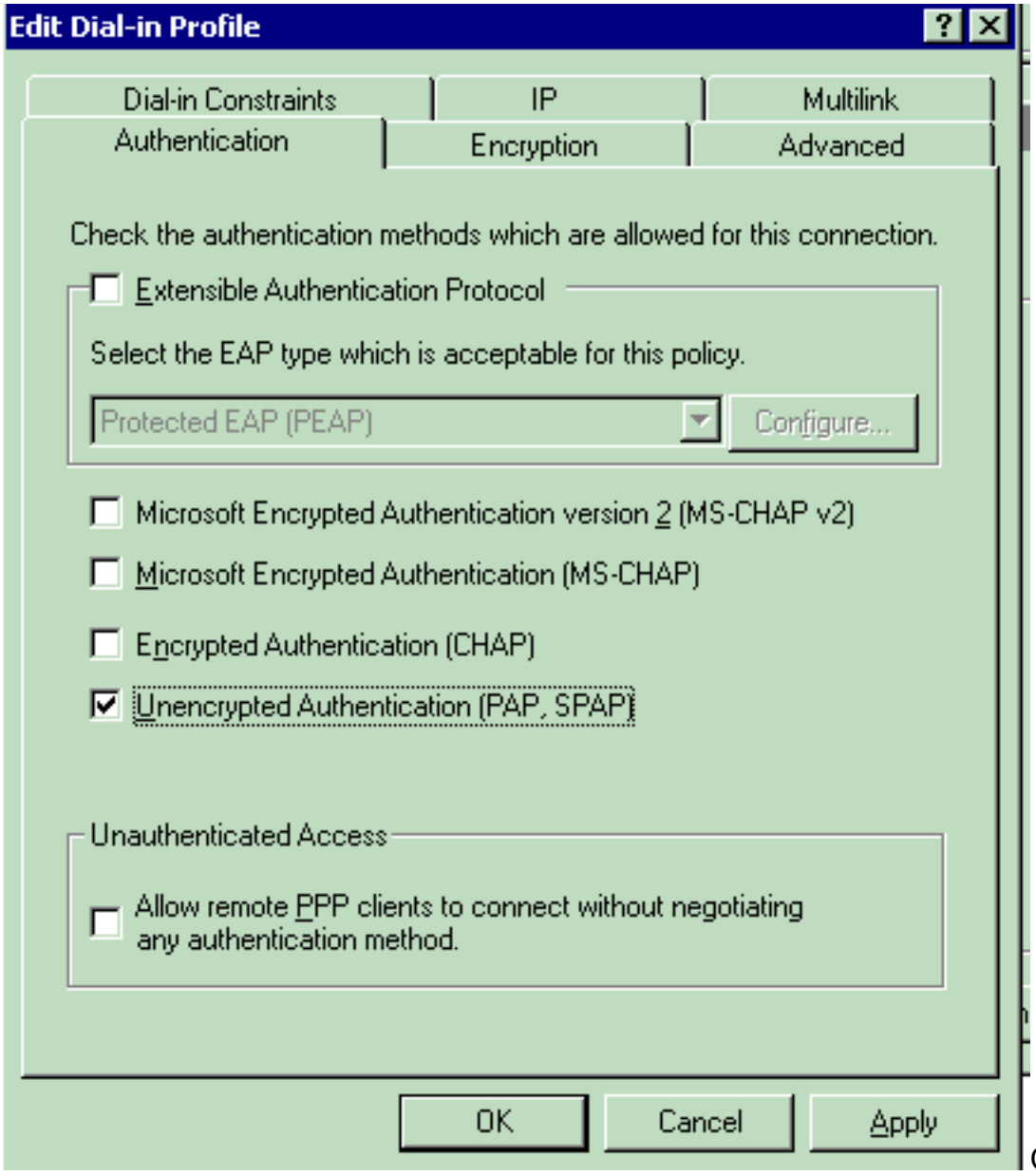
6. Clique em Next.
7. A próxima etapa é configurar o perfil do usuário.Mesmo que você tenha especificado que os usuários devem ter o acesso negado ou concedido com base nas condições, o perfil ainda poderá ser usado se as condições dessa política forem substituídas por usuários.



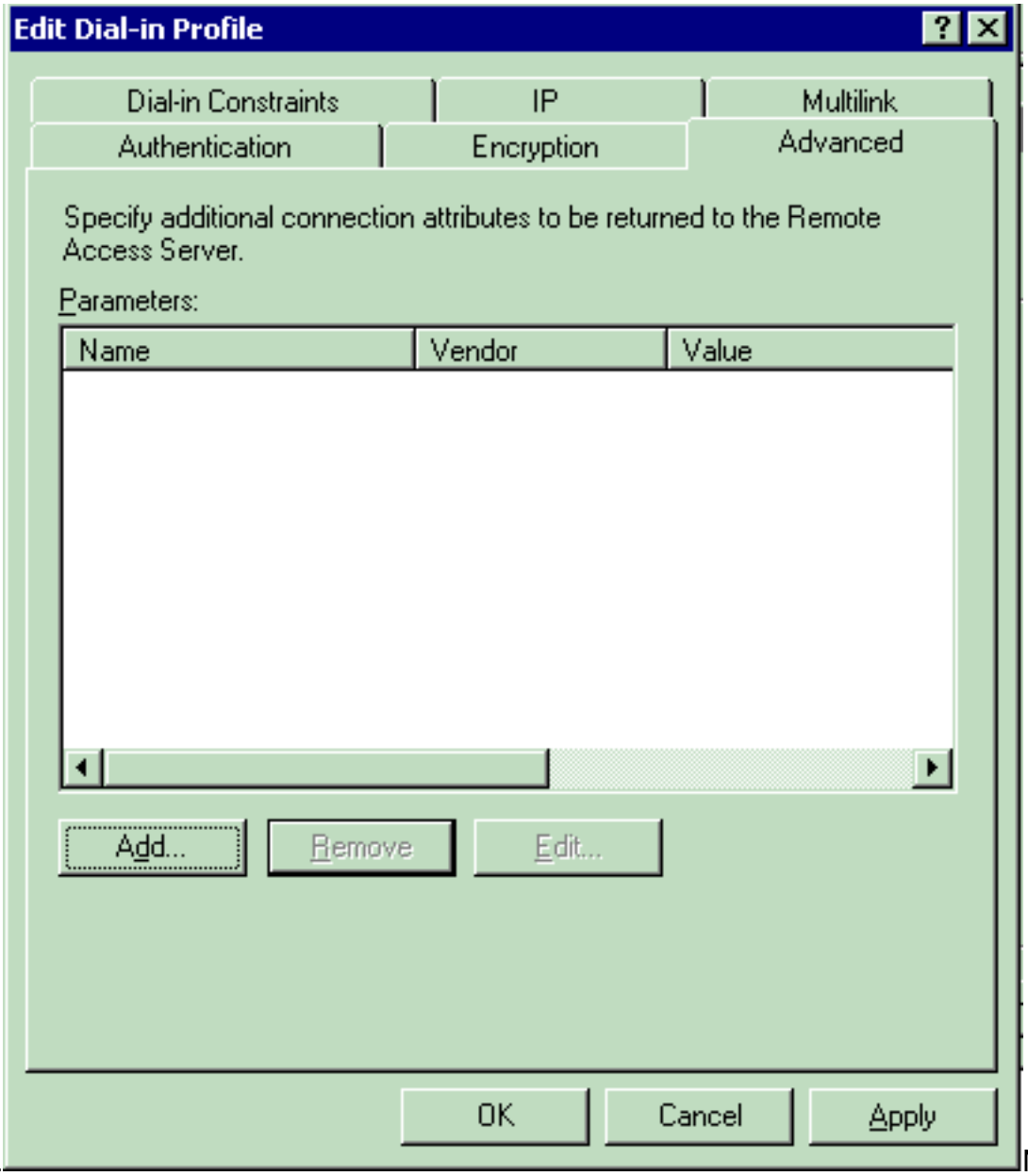
Para configurar o perfil de usuário, clique em **Editar perfil** na janela Perfil de usuário.A janela Editar perfil de discagem é



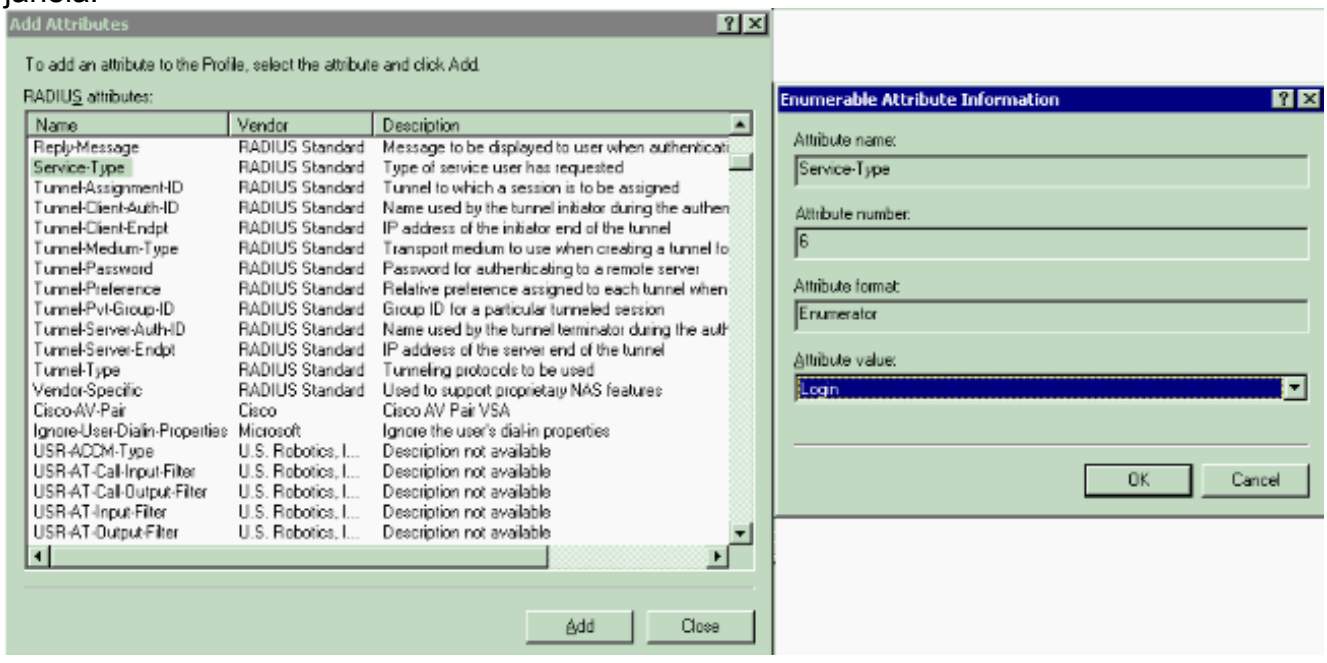
exibida. Clique na guia **Authentication** e escolha o método de autenticação usado na WLAN.Este exemplo usa autenticação não criptografada



(PAP,SPAP). Clique na guia Advanced. Remova todos os parâmetros padrão e clique em

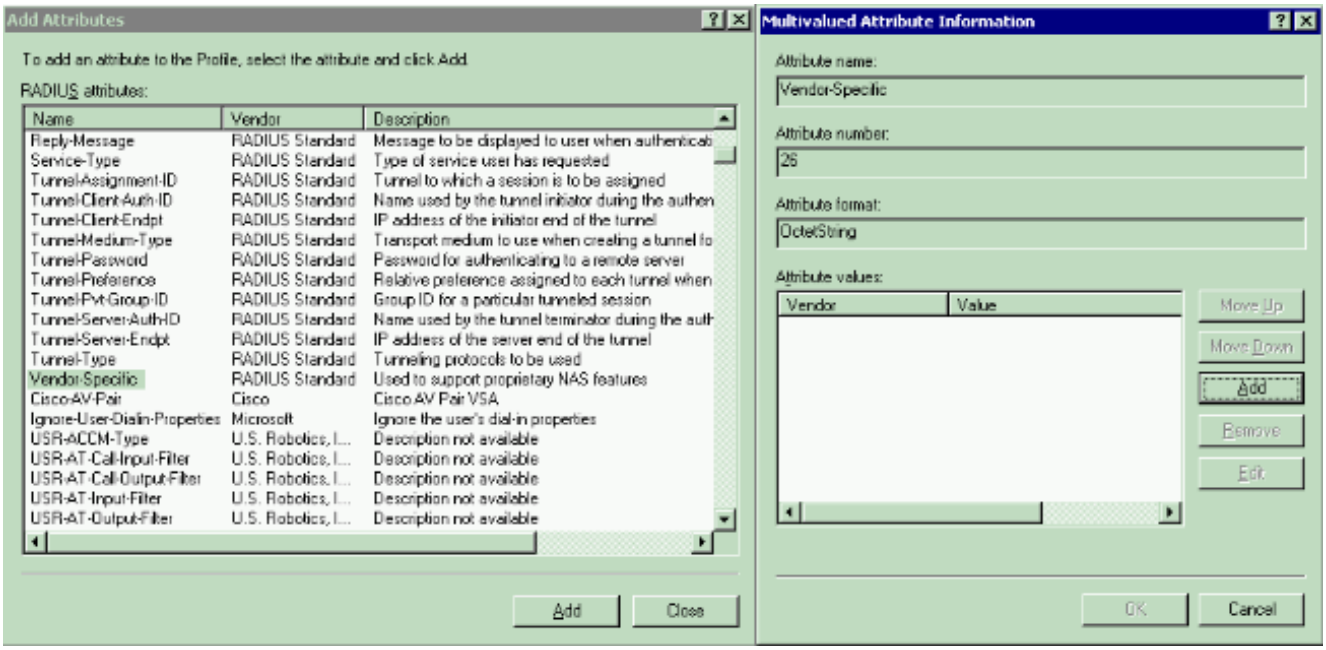


Adicionar.Na janela **Adicionar atributos**, selecione **Tipo de serviço** e escolha o valor de **logon** na próxima janela.

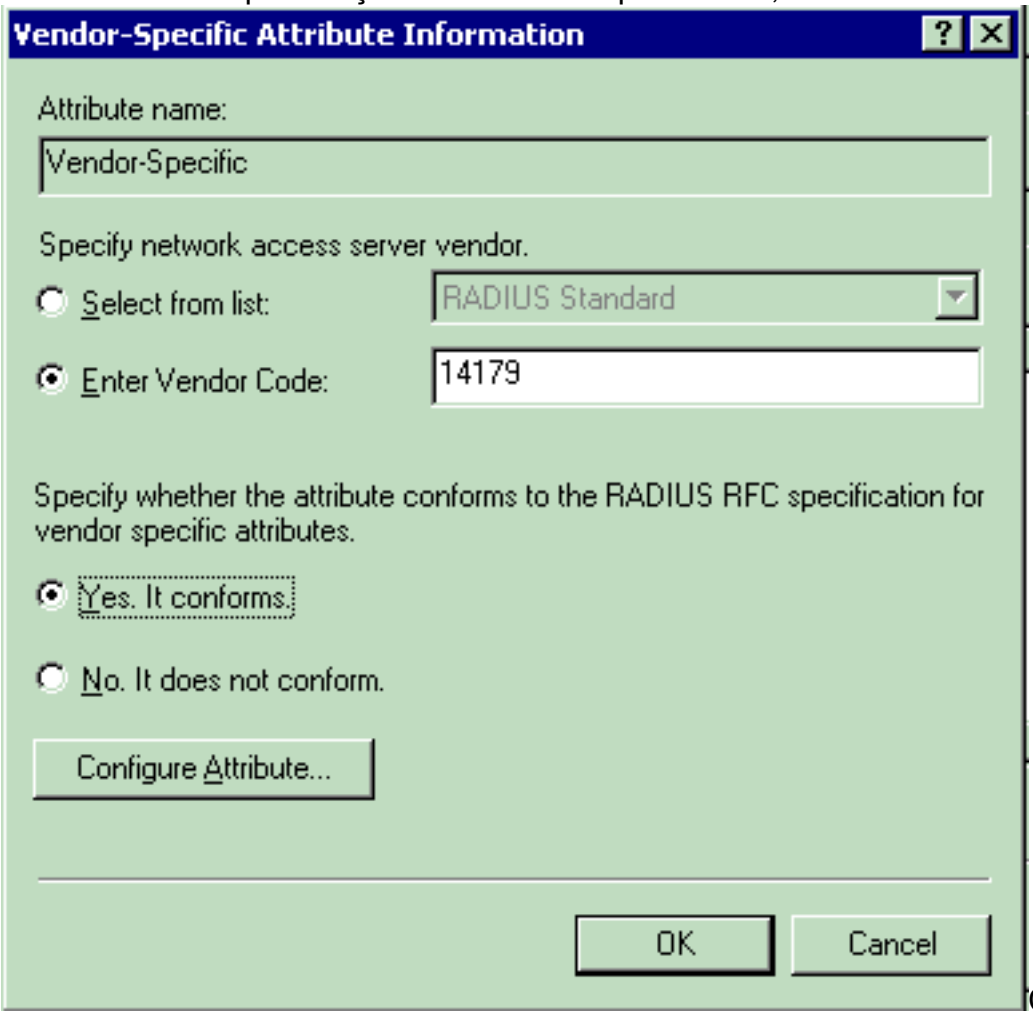


Em seguida, você precisa selecionar o atributo **específico do fornecedor** na lista de atributos

RADIUS.

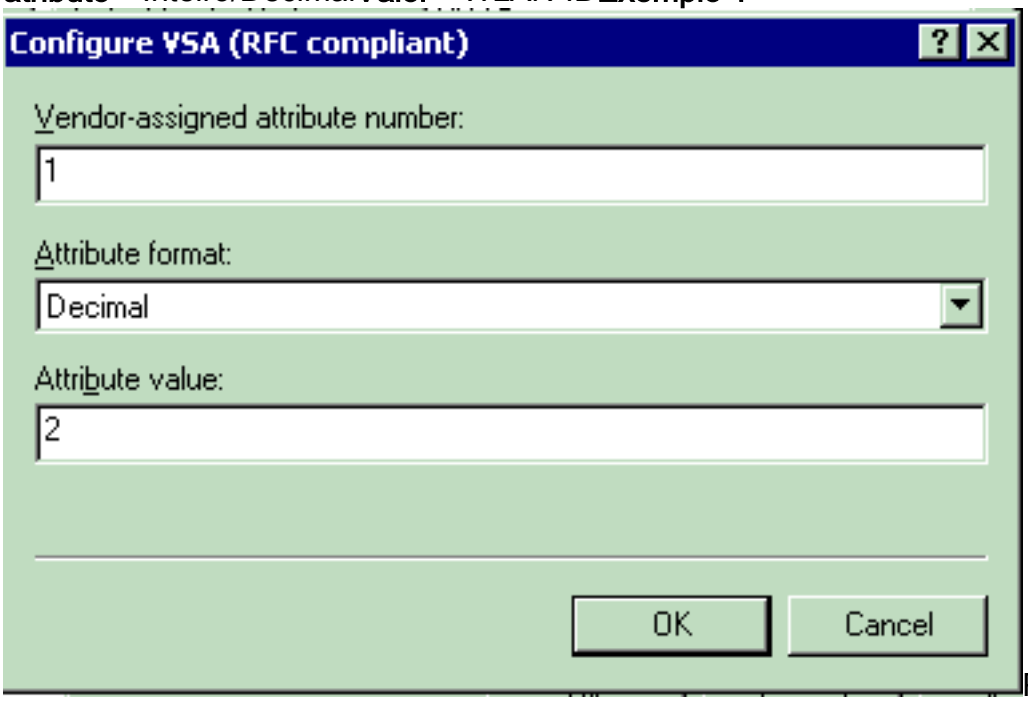


Na próxima janela, clique em **Adicionar** para selecionar um novo VSA.A janela Vendor-Specific Attribute Information é exibida.Em Especificar fornecedor do servidor de acesso à rede, escolha **Inserir código do fornecedor**.Insira o código do fornecedor para VSAs do Airespace. O código de fornecedor do VSA do Cisco Airespace é 14179.Como este atributo está em conformidade com a especificação RADIUS RFC para VSAs, escolha **Sim. Está em conformidade.**.

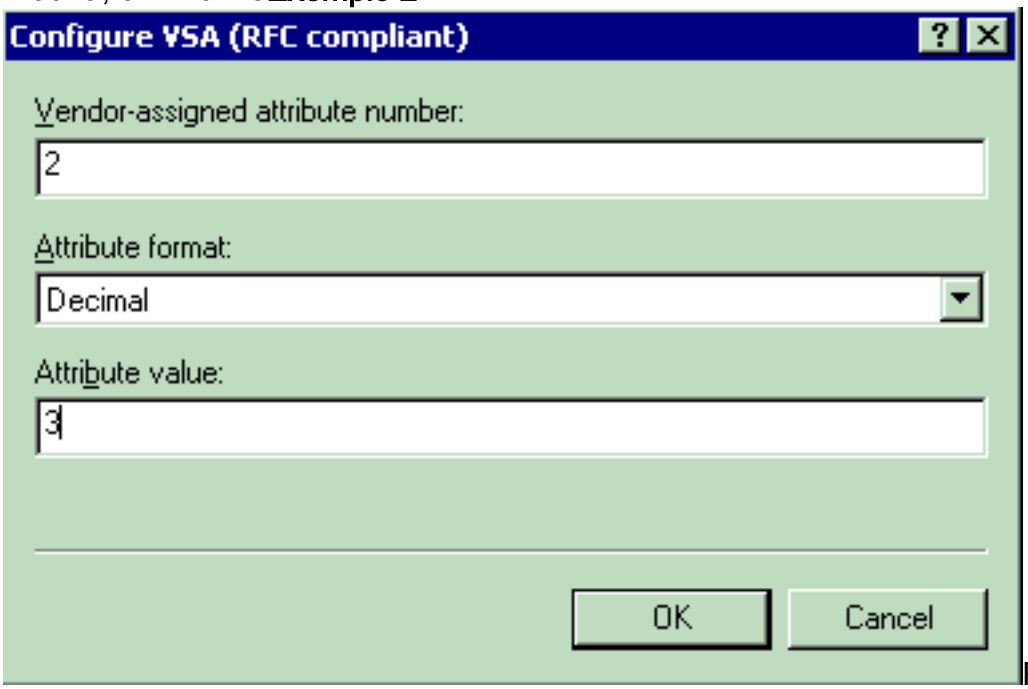


Cliqu e em **Configurar atributo**.Na janela Configurar VSA (compatível com RFC), insira o número do atributo atribuído pelo fornecedor, o formato do atributo e o valor do atributo, que dependem do VSA que você deseja usar.Para definir a ID da WLAN por usuário:**Nome do**

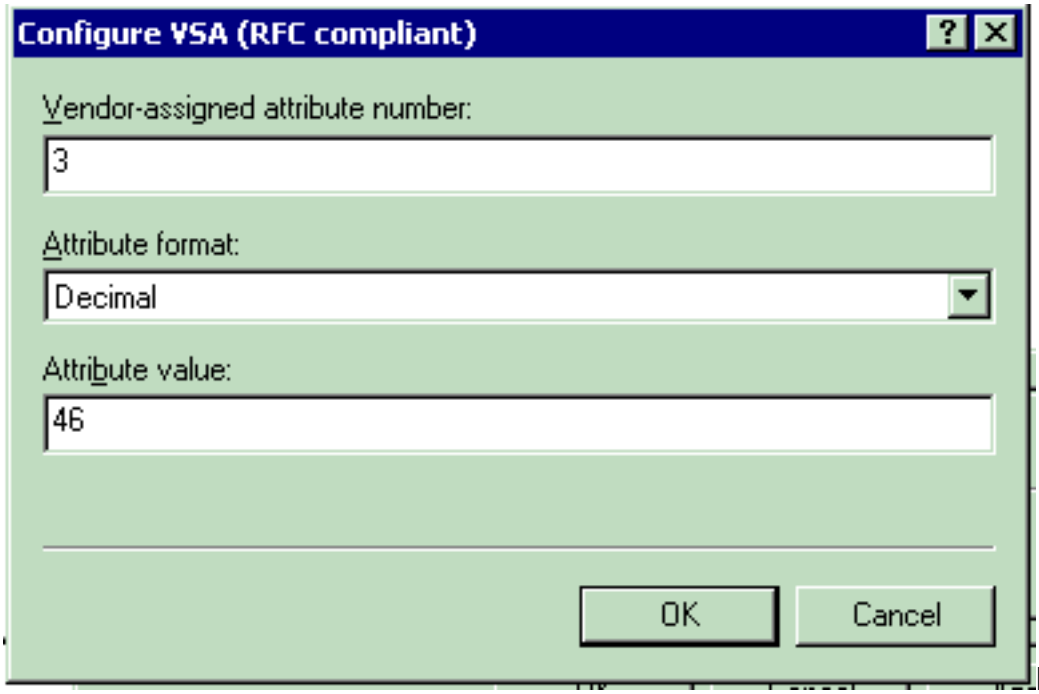
atributo —Airespace-WLAN-Id**Número de atributo atribuído pelo fornecedor**—1**Formato do atributo**—Inteiro/Decimal**Valor**—WLAN-ID**Exemplo 1**



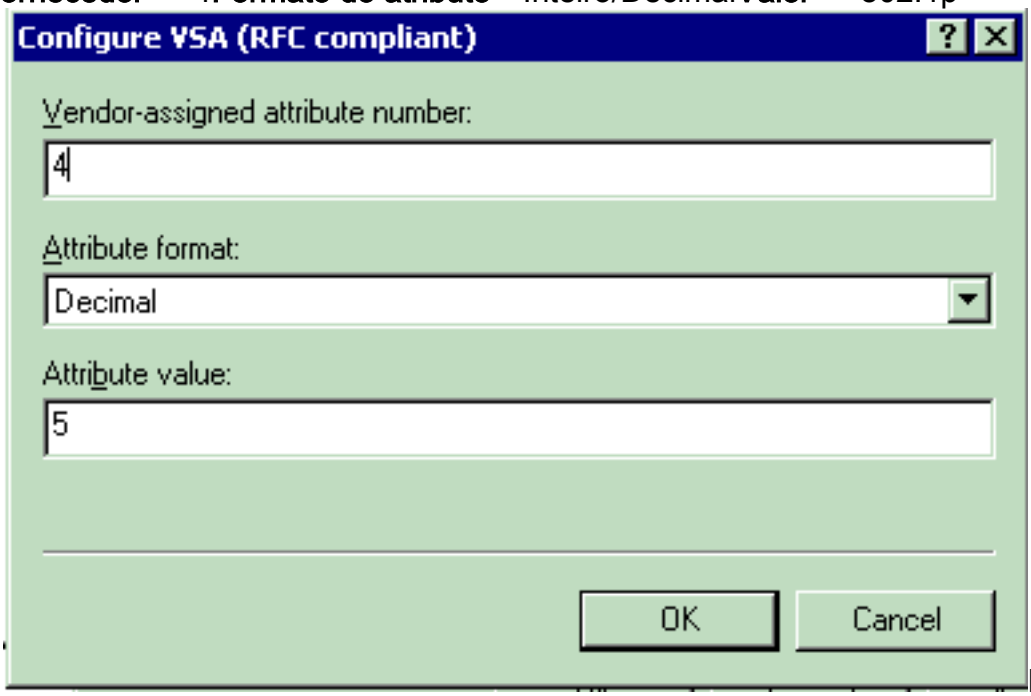
Para definir o perfil de QoS por usuário:**Nome do atributo**—Nível de QoS-Airespace**Número de atributo atribuído pelo fornecedor** — 2**Formato do atributo**—Inteiro/Decimal**Valor**—0 - Prata; 1 - Ouro; 2 - Platina; 3 - Bronze**Exemplo 2**



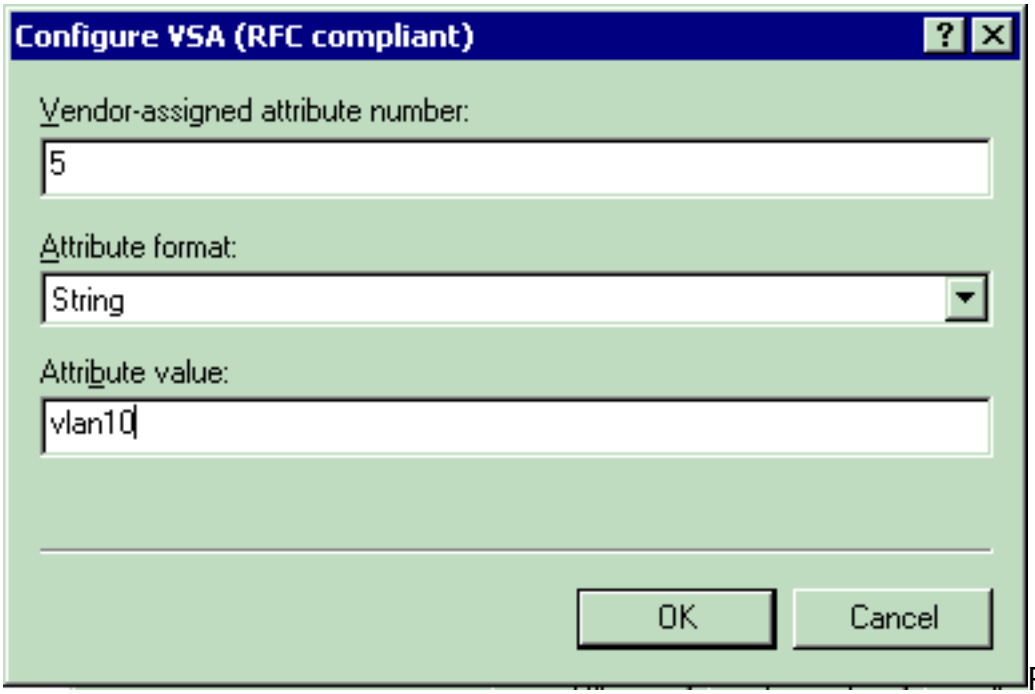
Para definir o valor de DSCP por usuário:**Nome do atributo** — Airespace-DSCP**Número de atributo atribuído pelo fornecedor** — 3**Formato do atributo**—Inteiro/Decimal**Valor** — Valor do DSCP**Exemplo 3**



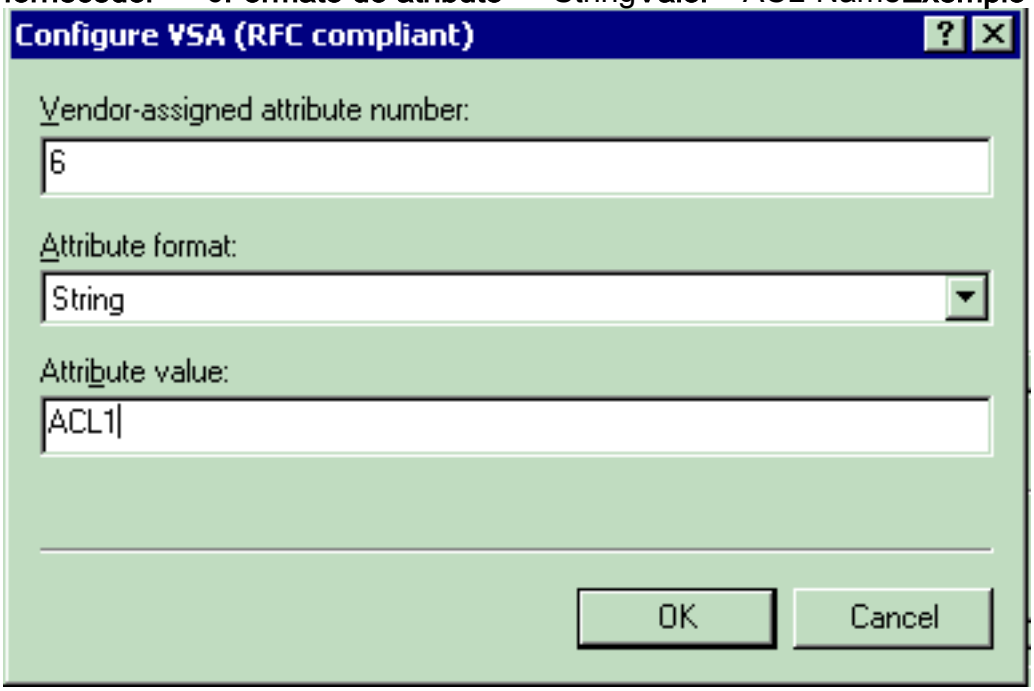
Para definir a etiqueta 802.1p por usuário:**Nome do atributo**—Airespace-802.1p-Tag**Número de atributo atribuído pelo fornecedor** — 4**Formato do atributo**—Inteiro/Decimal**Valor** — 802.1p-Tag**Exemplo 4**



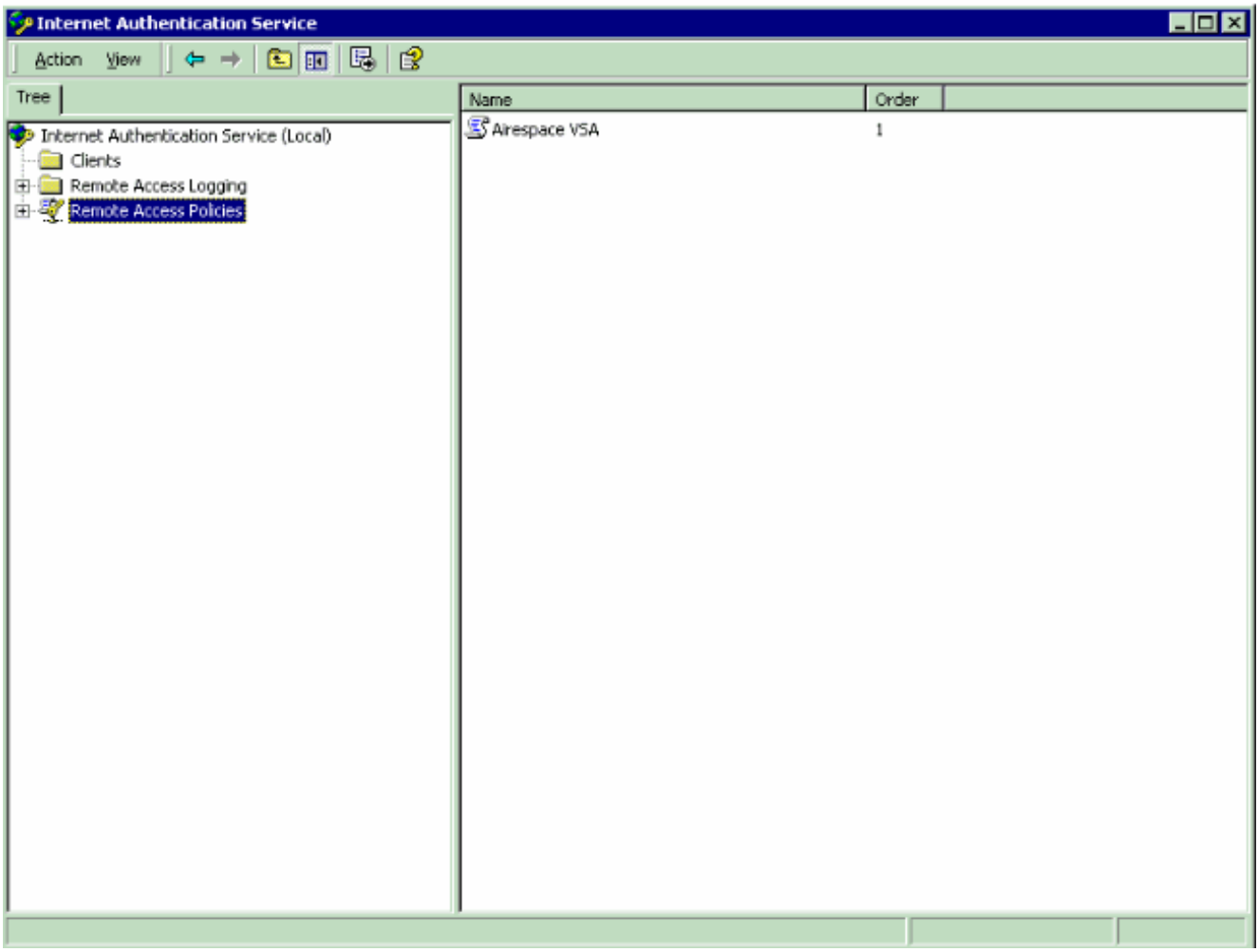
Para definir a Interface (VLAN) por usuário:**Nome do atributo**—Airespace-Interface-Name**Número de atributo atribuído pelo fornecedor** — 5**Formato do atributo** — String**Valor** — Nome da interface**Exemplo 5**



Para definir a ACL por usuário:**Nome do atributo** —Airespace-ACL-Name**Número de atributo atribuído pelo fornecedor** — 6**Formato do atributo** — String**Valor**—ACL-Name**Exemplo 6**

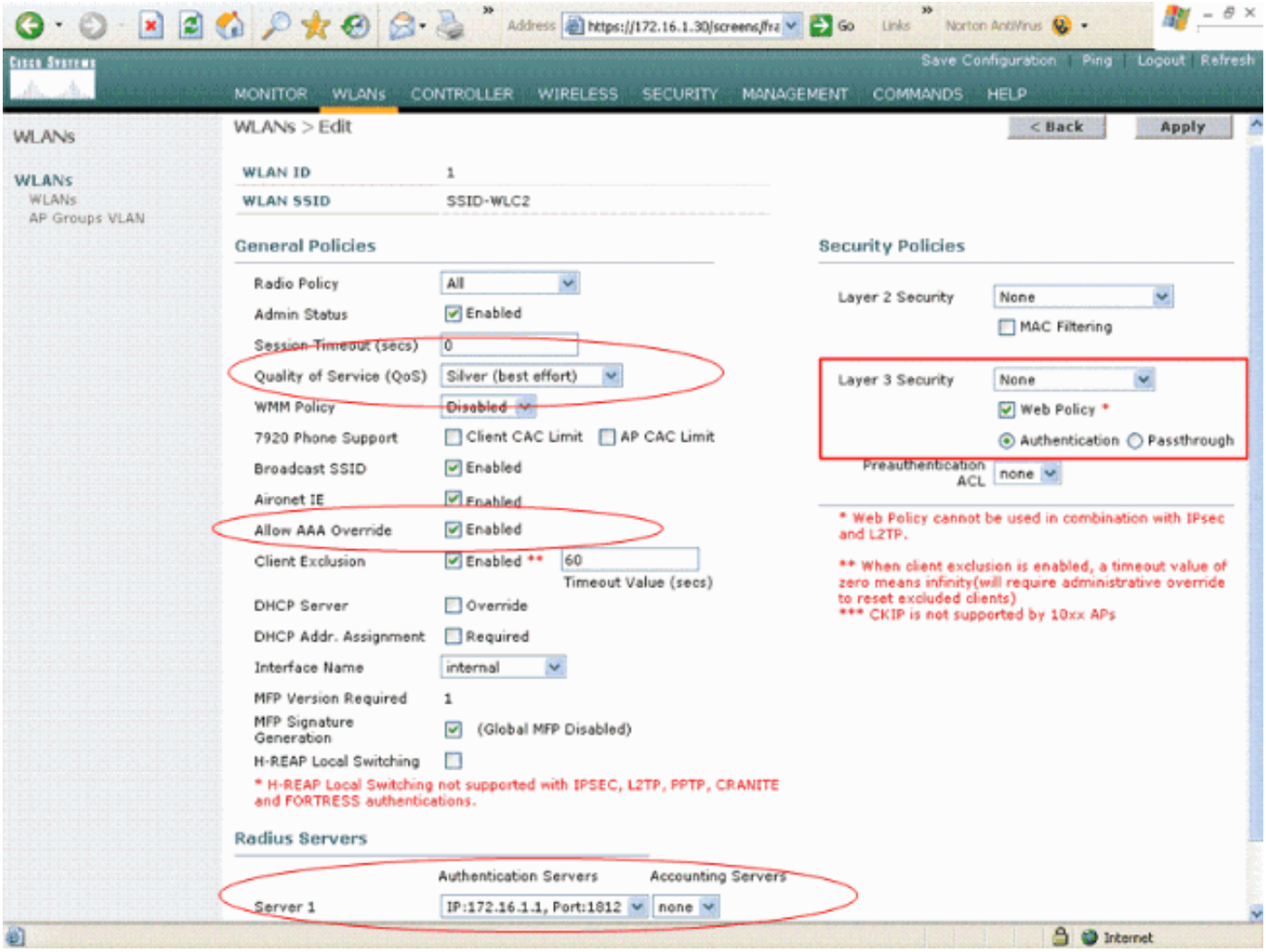


8. Depois de configurar os VSAs, clique em **OK** até ver a janela Perfil do usuário.
9. Em seguida, clique em **Finish** para concluir a configuração.Você pode ver a nova política em Políticas de acesso
   remoto.



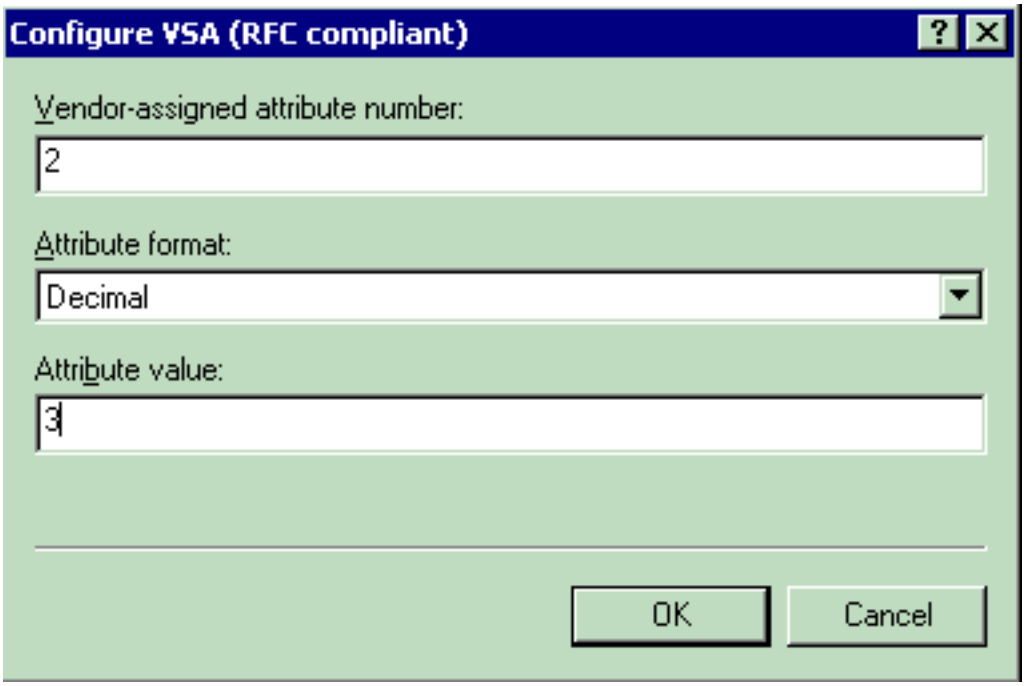
Exemplo de configuração

Neste exemplo, uma WLAN é configurada para autenticação da Web. Os usuários são autenticados pelo servidor IAS RADIUS e o servidor RADIUS é configurado para alocar políticas de QoS por usuário.



Como você pode ver nesta janela, a autenticação da Web está habilitada, o servidor de autenticação é 172.16.1.1 e a substituição de AAA também está habilitada na WLAN. A configuração de QoS padrão para esta WLAN é definida como Silver.

No servidor do IAS RADIUS, uma Política de Acesso Remoto é configurada que retorna o atributo de QoS Bronze na solicitação de aceitação do RADIUS. Isso é feito quando você configura o VSA específico para o atributo QoS.



Consulte a seção Configurar a Política de Acesso Remoto no IAS deste documento para obter informações detalhadas sobre como configurar uma Política de Acesso Remoto no servidor IAS.

Quando o servidor IAS, o WLC e o LAP estiverem configurados para essa configuração, os clientes sem fio poderão usar a autenticação da Web para se conectarem.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Quando o usuário se conecta à WLAN com um ID de usuário e uma senha, a WLC passa as credenciais para o servidor RADIUS IAS, que autentica o usuário em relação às condições e ao perfil de usuário configurado na Política de acesso remoto. Se a autenticação de usuário for bem-sucedida, o servidor RADIUS retornará uma solicitação de aceitação RADIUS que também contém os valores de substituição AAA. Nesse caso, a política de QoS do usuário é retornada.

Você pode emitir o comando **debug aaa all enable** para ver a sequência de eventos que ocorre durante a autenticação. Veja um exemplo de saída:

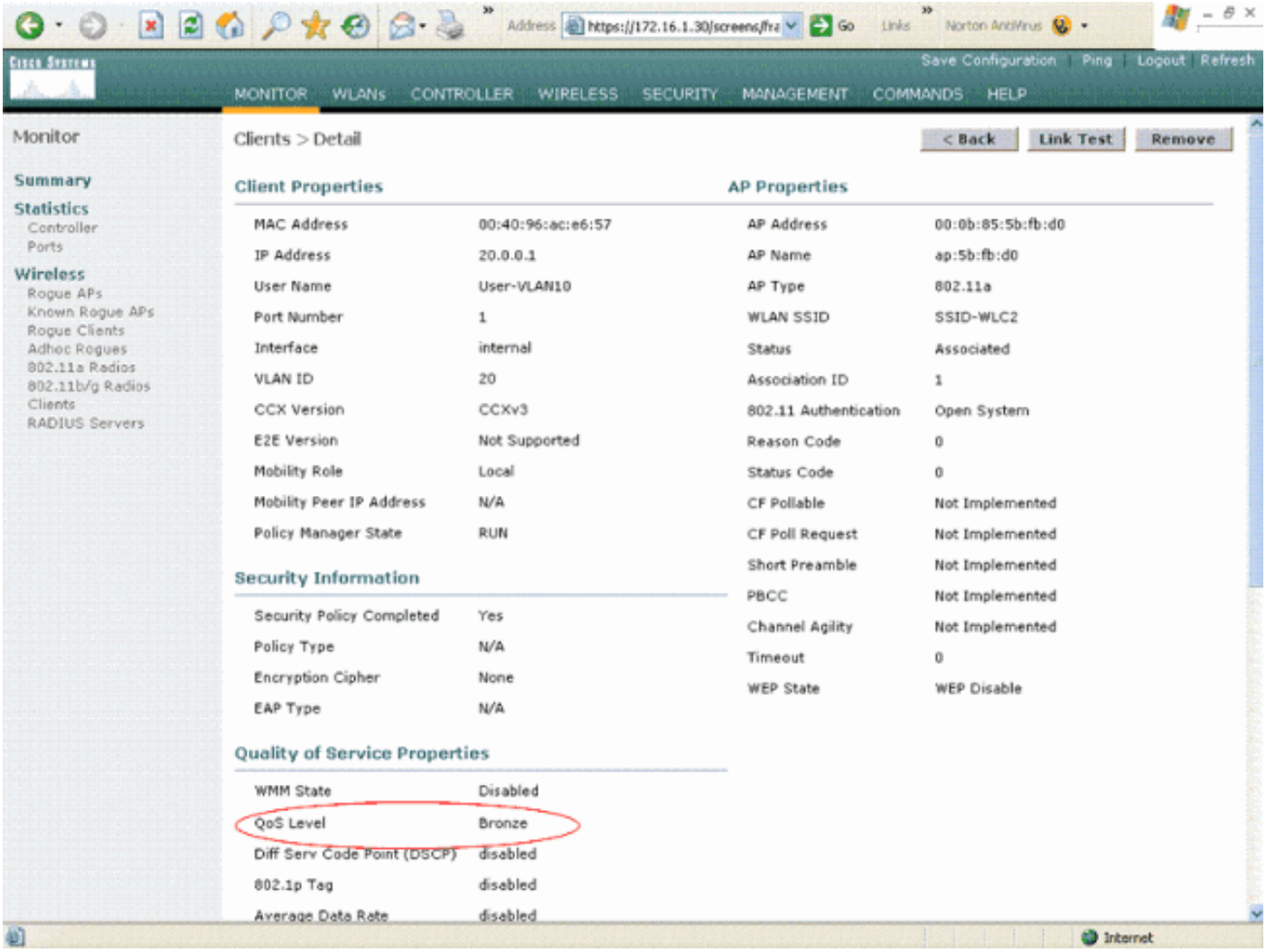
```
(Cisco Controller) > debug aaa all enable
Wed Apr 18 18:14:24 2007: User admin authenticated
Wed Apr 18 18:14:24 2007: 28:1f:00:00:00:00 Returning AAA Error 'Success' (0) for
                          mobile 28:1f:00:00:00:00
Wed Apr 18 18:14:24 2007: AuthorizationResponse: 0xbadff97c
Wed Apr 18 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 você pode ver na saída, o usuário é autenticado. Em seguida, os valores de substituição AAA são retornados com a mensagem de aceitação RADIUS. Nesse caso, o usuário recebe a política de QoS do Bronze.

Você também pode verificar isso na GUI da WLC. Aqui está um exemplo:



Observação: o perfil de QoS padrão para este SSID é Silver. No entanto, como a substituição de AAA é selecionada e o usuário é configurado com um perfil de QoS de Bronze no servidor IAS, o perfil de QoS padrão é substituído.

Troubleshoot

Você pode usar o comando **debug aaa all enable** na WLC para solucionar problemas de configuração. Um exemplo da saída dessa depuração em uma rede em funcionamento é mostrado na seção Verificar deste documento.

Nota:Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos debug.

Informações Relacionadas

- Guia de Configuração da Cisco Wireless LAN Controller Release 4.0
- Restringir o acesso à WLAN com base no SSID com WLC e o exemplo de configuração do Cisco Secure ACS
- Suporte de produtos Wireless
- Suporte Técnico e Documentação - Cisco Systems