

Cisco Airespace VSA no exemplo da configuração de servidor RADIUS do Microsoft IAS

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Informações de Apoio](#)

[Configurar IAS para Airespace VSA](#)

[Configurar o WLC como um cliente de AAA em IAS](#)

[Configurar a política de acesso remoto em IAS](#)

[Exemplo de configuração](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

[Introdução](#)

Este documento mostra-lhe como configurar um server do Internet Authentication Service de Microsoft (IAS) para apoiar os atributos específicos do vendedor de Cisco Airespace (VSA). O código de fornecedor do VSA do Cisco Airespace é 14179.

[Pré-requisitos](#)

[Requisitos](#)

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

- Conhecimento de como configurar um servidor de IAS
- Conhecimento da configuração do Lightweight Access Points (regações) e dos controladores de LAN do Cisco Wireless (WLC)
- Conhecimento de soluções da Segurança do Cisco Unified Wireless

[Componentes Utilizados](#)

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

- Servidor do Microsoft Windows 2000 com IAS
- Cisco 4400 WLC que executa a versão de software 4.0.206.0
- Cisco 1000 Series LAPs
- adaptador de cliente Wireless do a/b/g do 802.11 com firmware 2.5
- Versão 2.5 do utilitário de Desktop de Aironet (ADU)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Note: Este documento é pretendido dar ao leitor um exemplo na configuração exigida no servidor de IAS para apoiar Cisco Airespace VSA. A configuração de servidor de IAS apresentada neste documento foi testada no laboratório e trabalha como esperado. Se você tem o problema que configura o servidor de IAS, contacte Microsoft para a ajuda. O tac Cisco não apoia a configuração do Microsoft Windows server.

Este documento supõe que o WLC está configurado para a operação básica e que os regaços estão registrados ao WLC. Se você é um novo usuário que tenta setup o WLC para a operação básica com regaços, refira o [registro de pouco peso AP \(REGAÇO\) a um controlador do Wireless LAN \(WLC\)](#).

Convenções

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

Informações de Apoio

Na maioria de sistemas do Wireless LAN (WLAN), cada WLAN tem uma política estática que se aplique a todos os clientes associados com um Service Set Identifier (SSID). 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.

Contudo, a solução de LAN do Cisco Wireless apoia os trabalhos em rede da identidade, que permitem que a rede anuncie um único SSID e uns usuários específicos para herdar QoS diferente ou políticas de segurança baseado em seus perfis de usuário. As políticas específicas que você pode controlar usando trabalhos em rede da identidade incluem:

- **Qualidade de Serviço** — Quando atual em um acesso radius aceite, o valor do QoS-nível cancela o valor do QoS especificado no perfil WLAN.
- **ACL** — Quando o atributo do Access Control List (ACL) esta presente no acesso radius aceite, o sistema aplica o ACL-nome à estação do cliente depois que autentica. Isto cancela todos os ACL que forem atribuídos à relação.
- **VLAN** — Quando um nome da interface ou a VLAN-etiqueta VLAN estam presente em um acesso radius aceite, o sistema coloca o cliente em uma relação específica.
- **ID de WLAN** — Quando o atributo do ID de WLAN esta presente no acesso radius aceite, o sistema aplica o ID de WLAN (SSID) à estação do cliente depois que autentica. O ID de WLAN é enviado pelo WLC em todos os exemplos da autenticação exceto o IPsec. Em caso da autenticação da Web, se o WLC recebe um atributo do ID de WLAN na resposta de

autenticação do servidor AAA, e dele não combina o ID do WLAN, autenticação é rejeitado. Outros tipos de métodos de segurança não fazem este.

- **Valor DSCP** — Quando atual em um acesso radius aceite, o valor DSCP cancela o valor DSCP especificado no perfil WLAN.
- **802.1p-Tag** — Quando atual em um acesso radius aceite, o valor 802.1p cancela o padrão especificado no perfil WLAN.

Note: A característica VLAN apoia somente a filtração, o 802.1X, e o Wi-Fi Protected Access (WPA) MAC. A característica VLAN não apoia a autenticação da Web ou o IPsec. O base de dados do filtro do MAC local do sistema operacional foi estendido para incluir o nome da relação. Isto permite que os filtros do MAC local especifiquem que relação o cliente deve ser atribuído. Um servidor Radius separado pode igualmente ser usado, mas o servidor Radius deve ser definido usando os menus Segurança.

Refira [configurar trabalhos em rede da identidade](#) para obter mais informações sobre dos trabalhos em rede da identidade.

[Configurar IAS para Airespace VSA](#)

A fim configurar IAS para Airespace VSA, você precisa de terminar estas etapas:

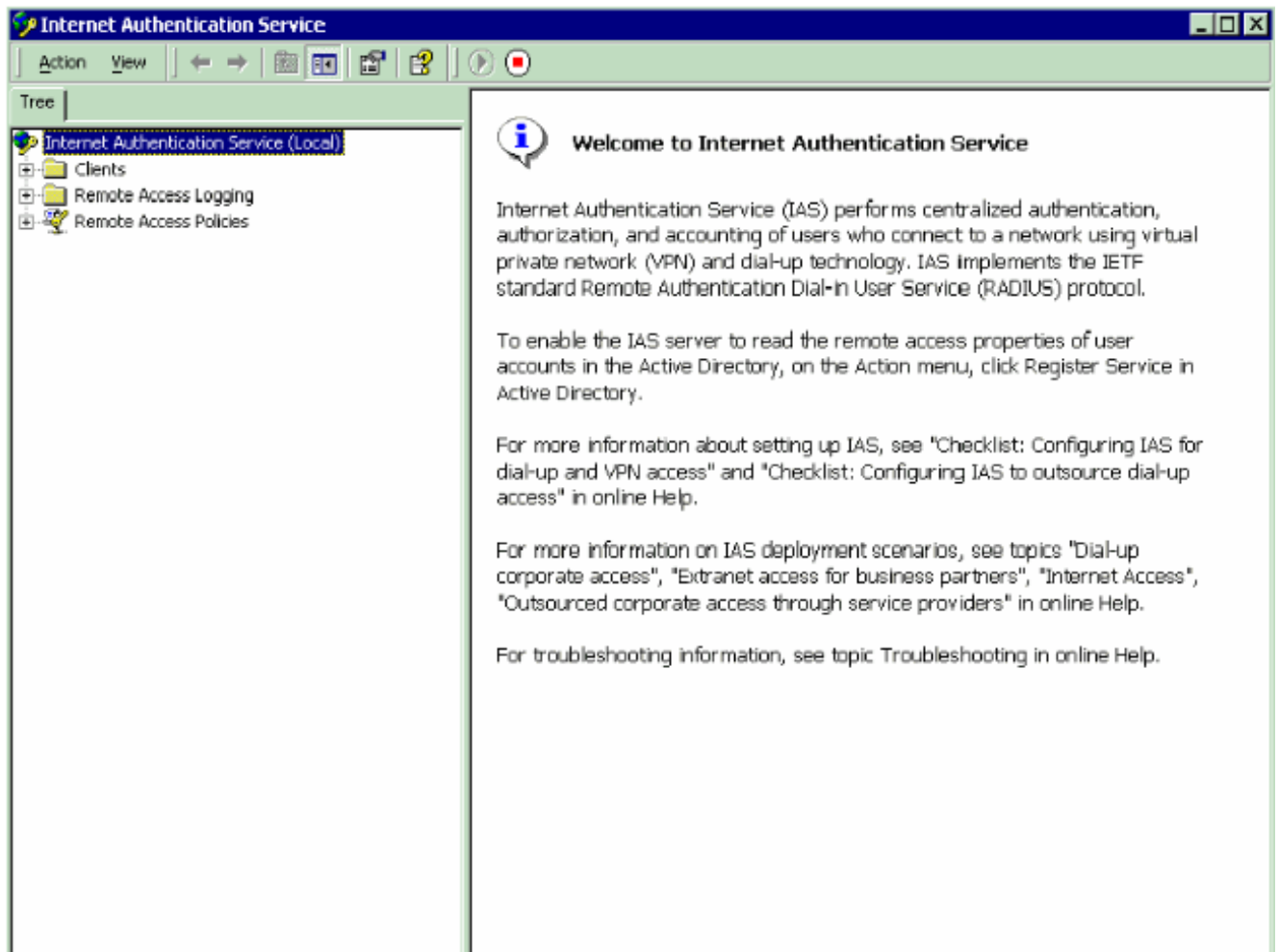
1. [Configurar o WLC como um cliente de AAA em IAS](#)
2. [Configurar a política de acesso remoto em IAS](#)

Note: Os VSA são configurados sob a política de acesso remoto.

[Configurar o WLC como um cliente de AAA em IAS](#)

Termine estas etapas a fim configurar o WLC como um cliente de AAA em IAS:

1. Clique **programas > Ferramentas Administrativas > Serviço de Autenticação de Internet** a fim lançar IAS no Microsoft 2000 server.



2. Clicar com o botão direito o dobrador dos **clientes** e escolha o **cliente novo** a fim adicionar um cliente RADIUS novo.
3. Na janela de cliente adicionar, dê entrada com o nome do cliente e escolha o **RAIO** como o protocolo. Então, clique **em seguida**. Neste exemplo, o nome do cliente é *WLC-1*. **Note:** À revelia, o protocolo é ajustado ao RAIO.

Add Client [X]

Name and Protocol
Assign a name and protocol for the client.

Type a friendly name and protocol for the client.

Friendly name:

Protocol:

< Back Next > Cancel

4. No indicador do cliente RADIUS adicionar, incorpore o **endereço IP cliente**, o **Client-Vendor**, e o **segredo compartilhado**. Depois que você incorpora a informação cliente, clique o **revestimento**. Este exemplo mostra um cliente nomeado *WLC-1* com um endereço IP de Um ou Mais Servidores Cisco ICM NT de *172.16.1.30*, Client-Vendor é ajustado a *Cisco*, e o segredo compartilhado é *cisco123*:

Add RADIUS Client [X]

Client Information
Specify information regarding the client.

Client address (IP or DNS):
172.16.1.30 [Verify...]

Client-Vendor:
Cisco [v]

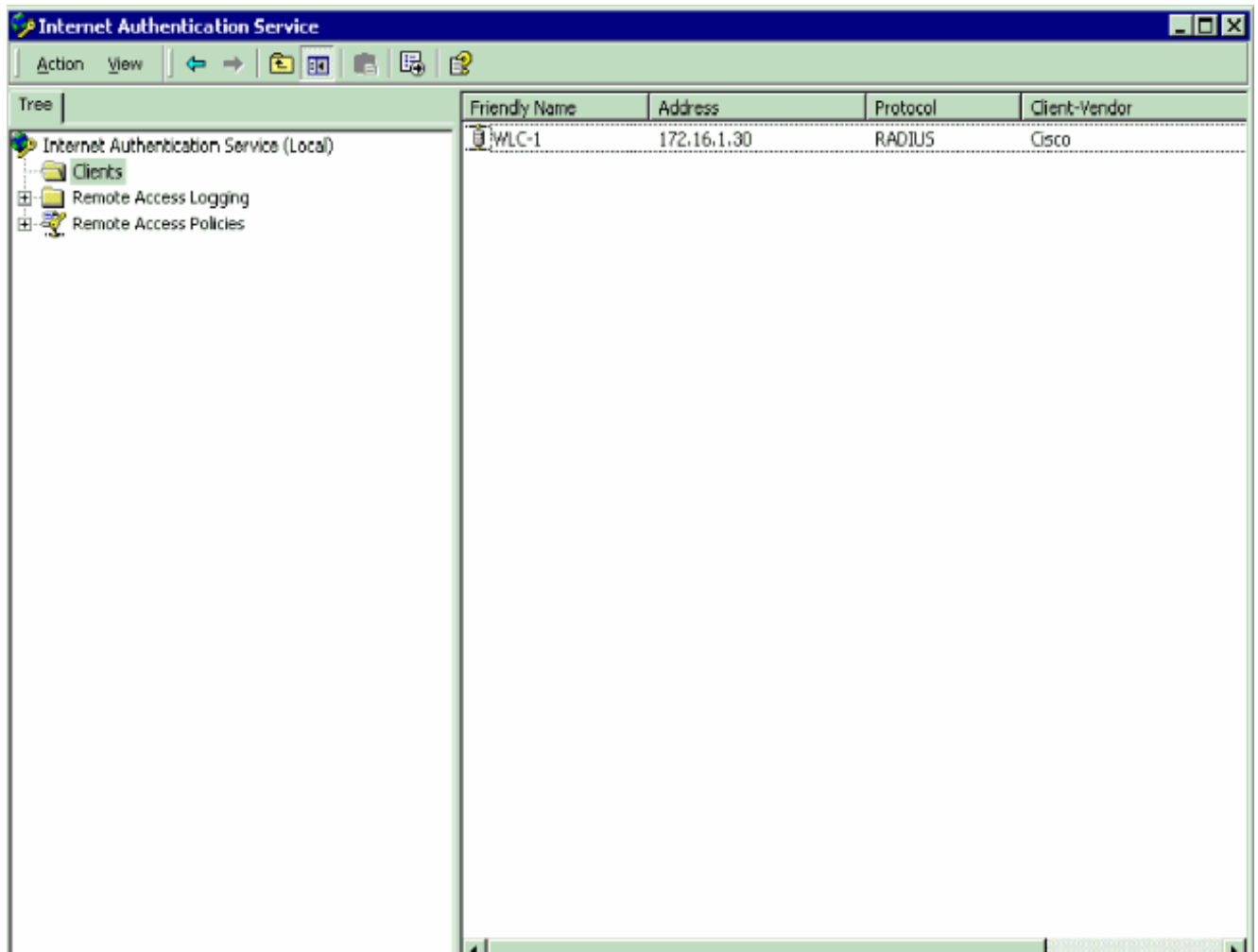
Client must always send the signature attribute in the request

Shared secret: [xxxxxxx]

Confirm shared secret: [xxxxxxx]

[< Back] [Finish] [Cancel]

Com esta informação, o WLC WLC-1 nomeado é adicionado como o cliente de AAA do servidor de IAS.

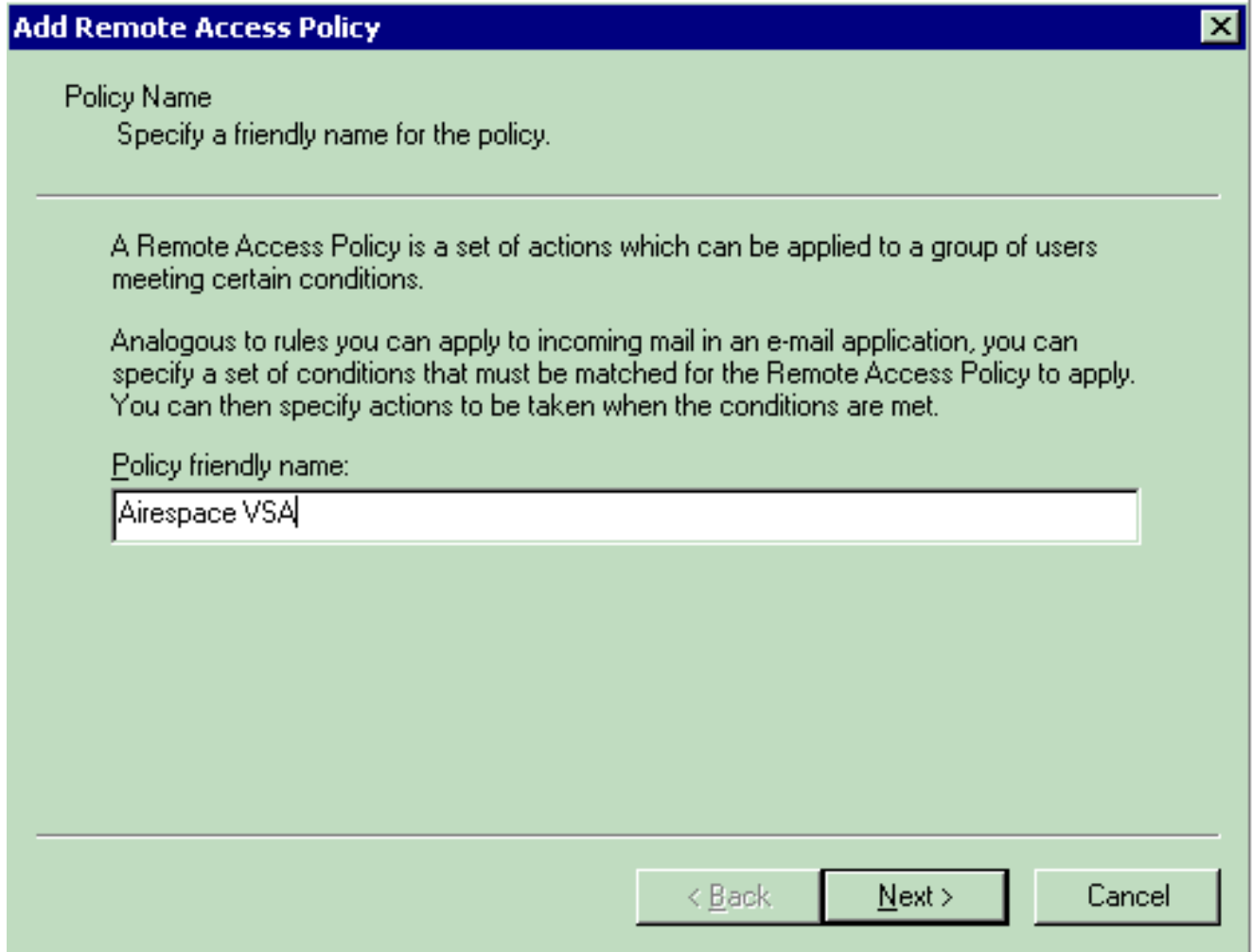


A próxima etapa é criar uma política de acesso remoto e configurar os VSA.

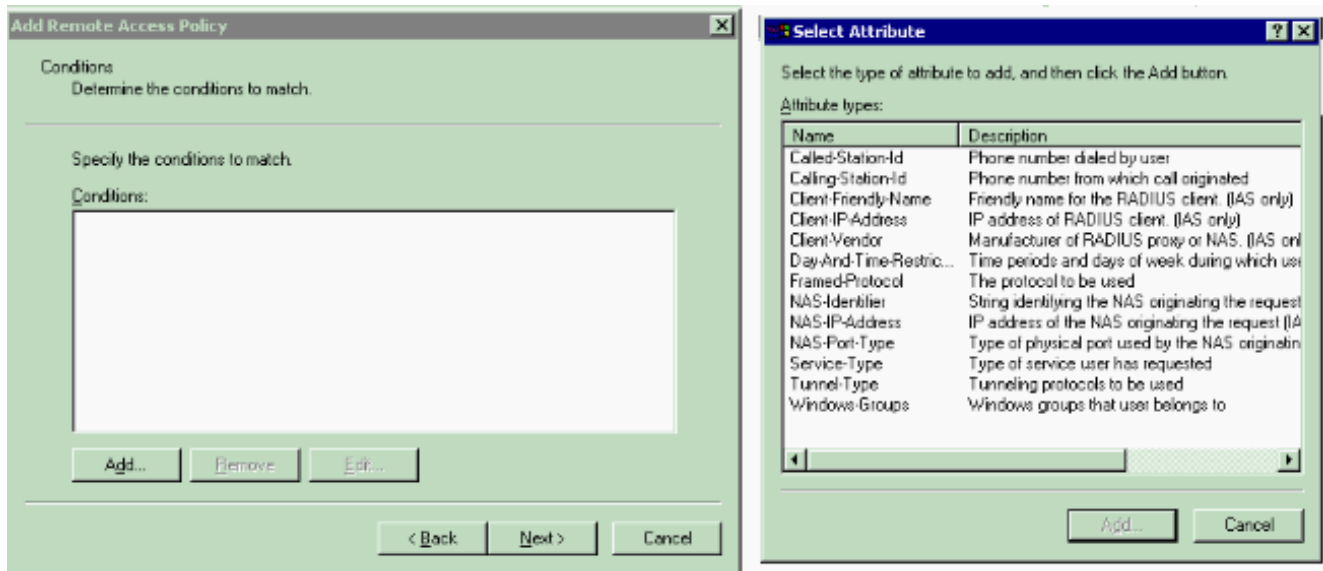
[Configurar a política de acesso remoto em IAS](#)

Termine estas etapas a fim configurar uma política de acesso remoto nova em IAS:

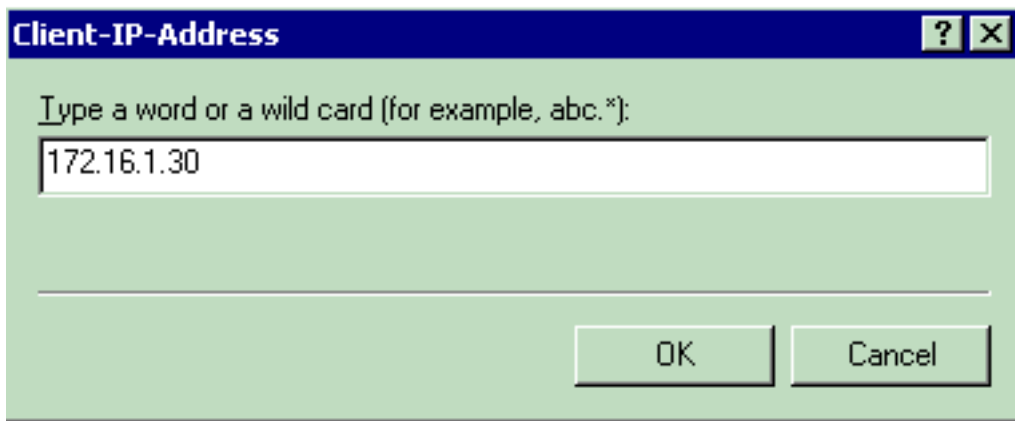
1. Clicar com o botão direito **políticas de acesso remoto** e escolha a **política remota nova de AcceMSss**. A janela de nome da política aparece.
2. Dê entrada com o nome da política e clique-o **em seguida**.



3. Na próxima janela, selecione as circunstâncias para que a política de acesso remoto se aplicará. O clique **adiciona** a fim selecionar as circunstâncias.



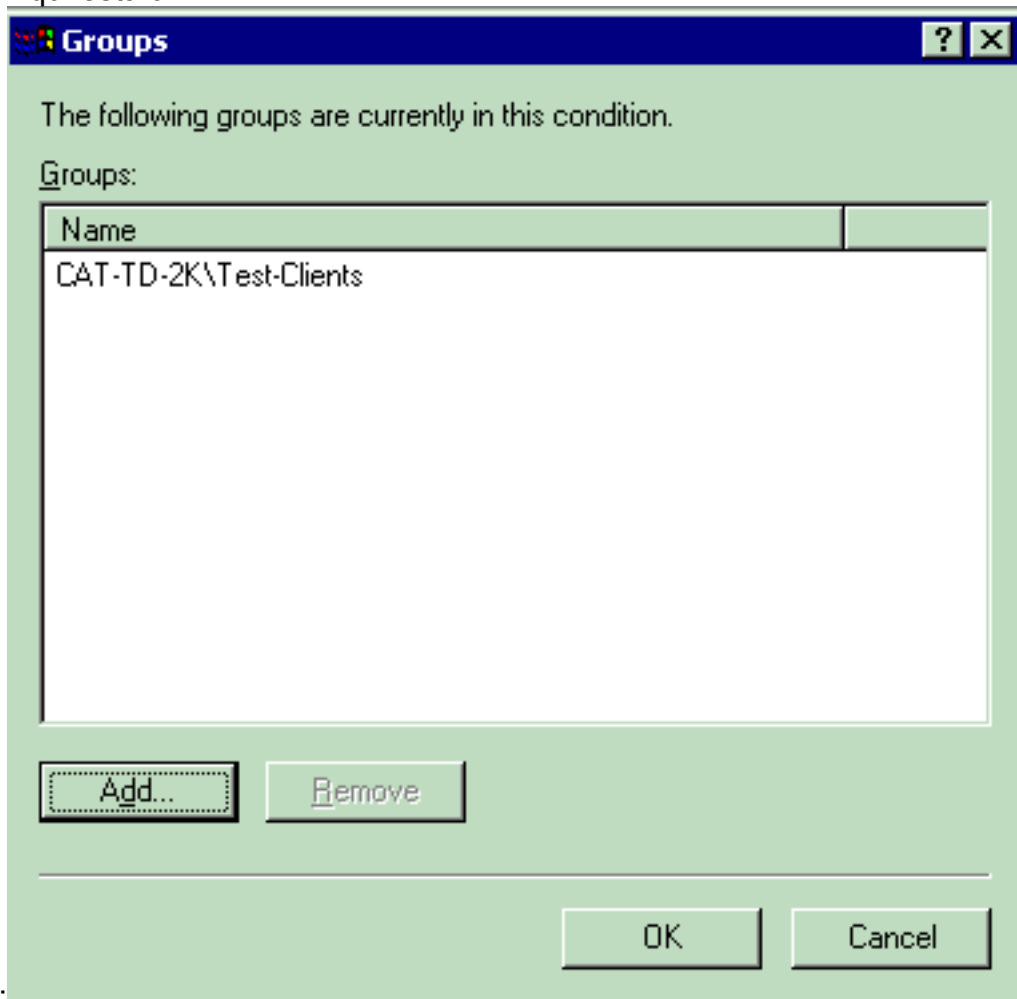
4. Dos tipos menu do atributo, selecione estes atributos: **Endereço de IP do cliente** — Incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT do cliente de AAA. Neste exemplo, o endereço IP de Um ou Mais Servidores Cisco ICM NT WLC é incorporado de modo que a política se aplique aos pacotes do



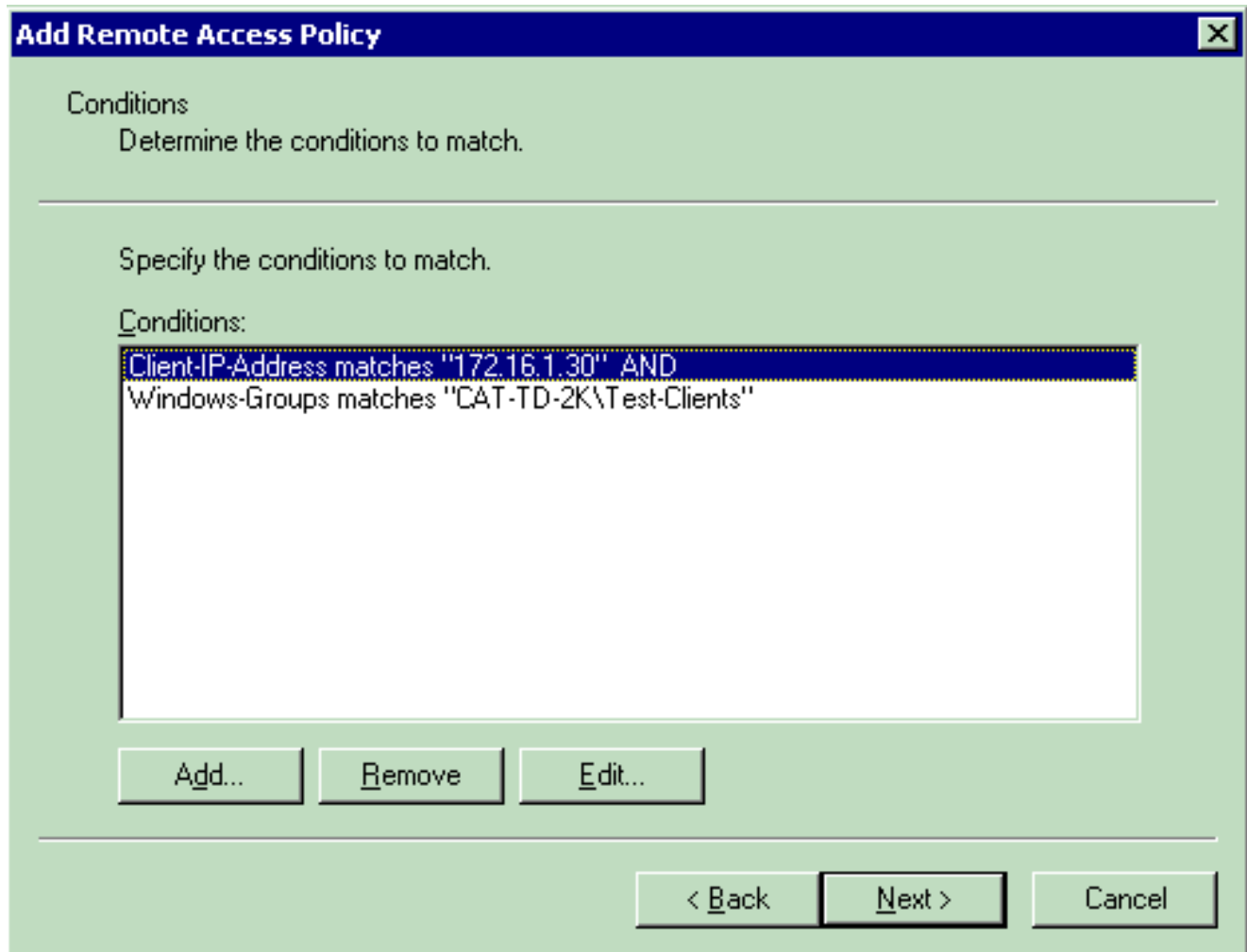
WLC.

Grupos de

Windows — Seleccione o grupo de Windows (grupo de usuário) para que a política se aplicará. Aqui está um

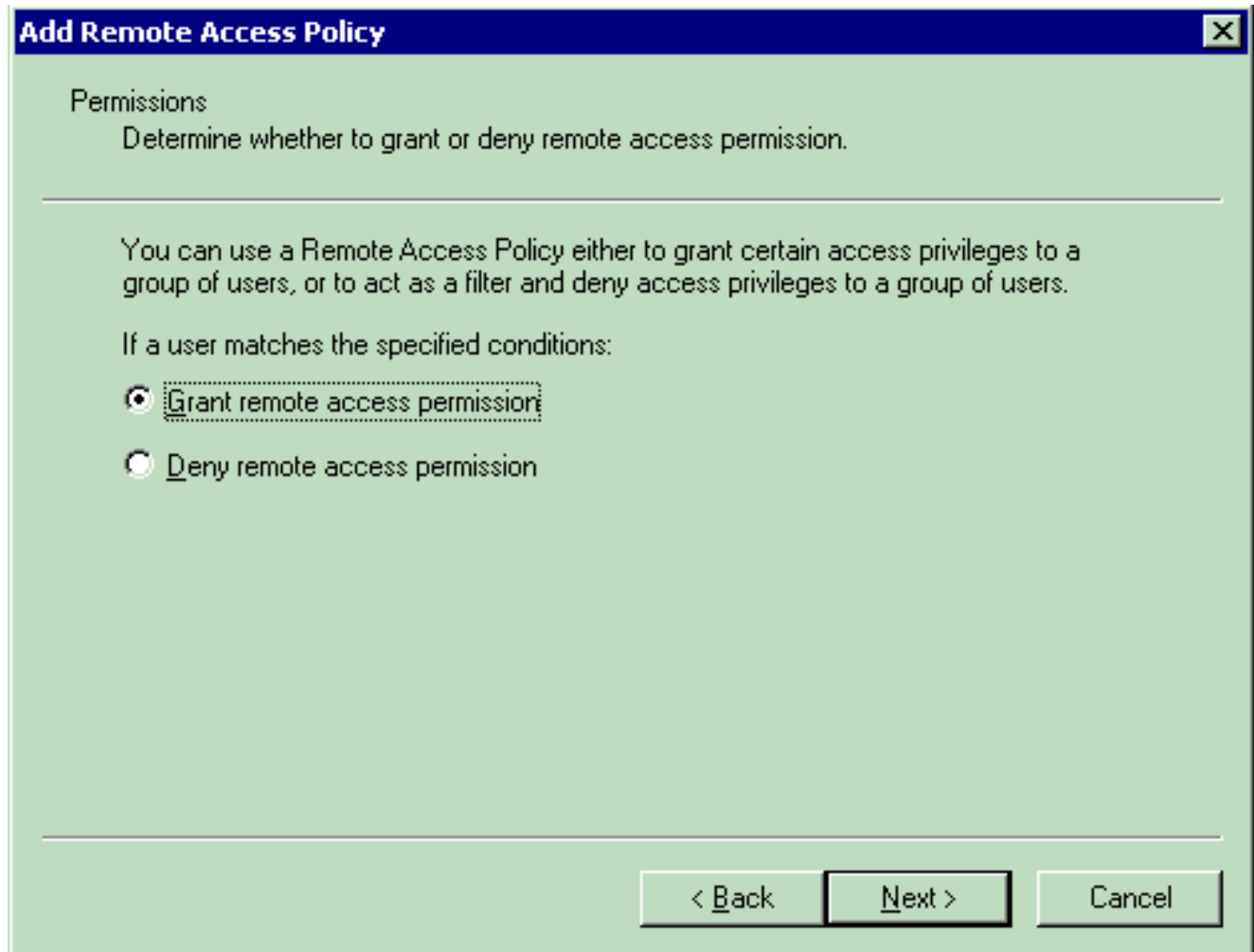


exemplo:



Este exemplo mostra somente duas circunstâncias. Se há mais circunstâncias, adicionar aquelas circunstâncias também e clique-as **em seguida**. O indicador das permissões aparece.

5. No indicador das permissões, escolha a **permissão de acesso remoto de Grant**. Depois que você escolhe esta opção, o usuário está dado o acesso, desde que o usuário combina as circunstâncias especificadas (de etapa 2).



6. Clique em Next.

7. A próxima etapa é estabelecer o perfil de usuário. Mesmo que você possa ter especificado que os usuários devem ser negados ou acesso concedido ser baseados nas circunstâncias, o perfil pode ainda ser usado se as condições desta política são canceladas em uma base do usuário per.

Add Remote Access Policy



User Profile

Specify the user profile.

You can now specify the profile for users who matched the conditions you have specified.

Note: Even though you may have specified that users should be denied access, the profile can still be used if this policy's conditions are overridden on a per-user basis.

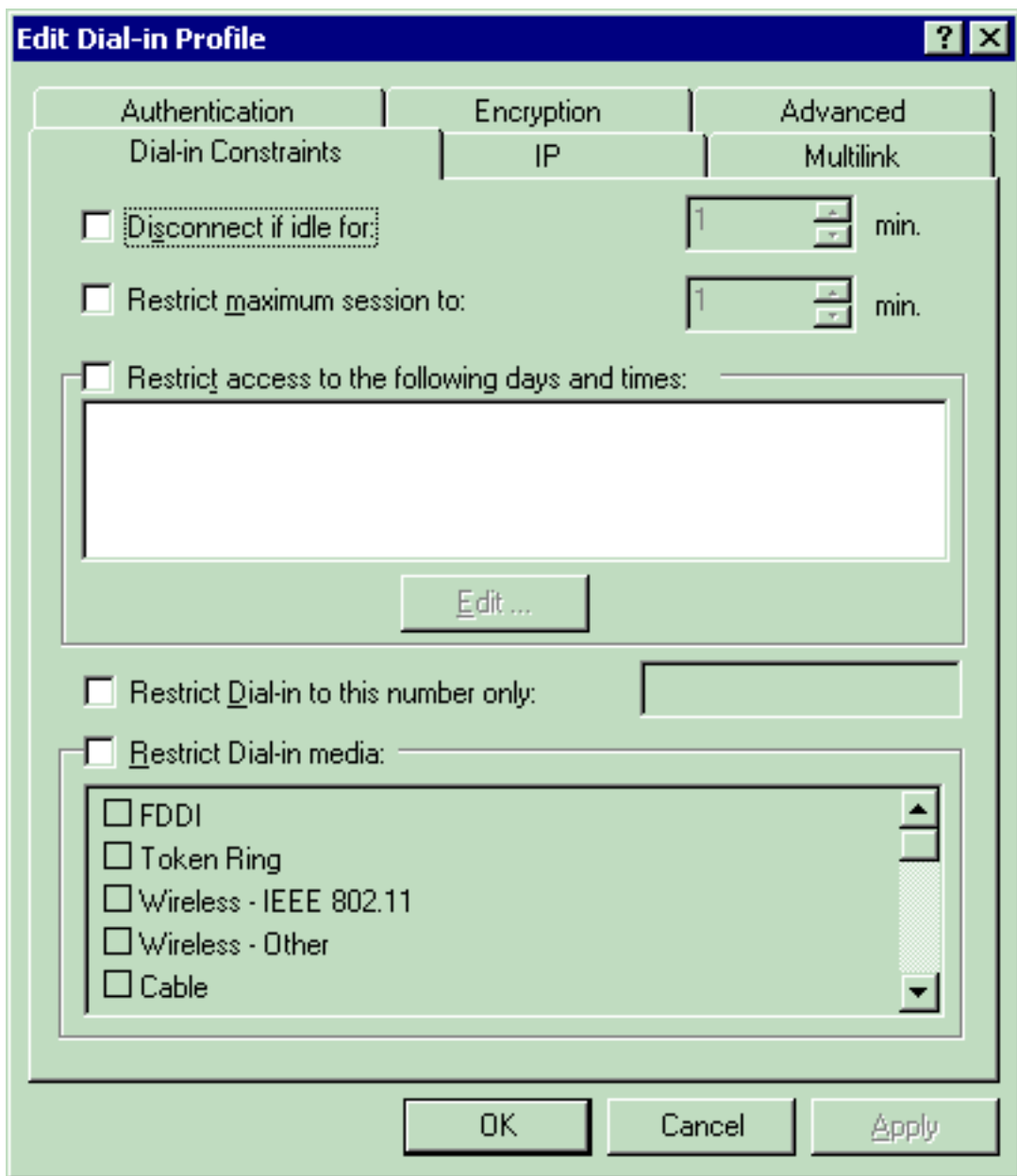
Edit Profile...

< Back

Finish

Cancel

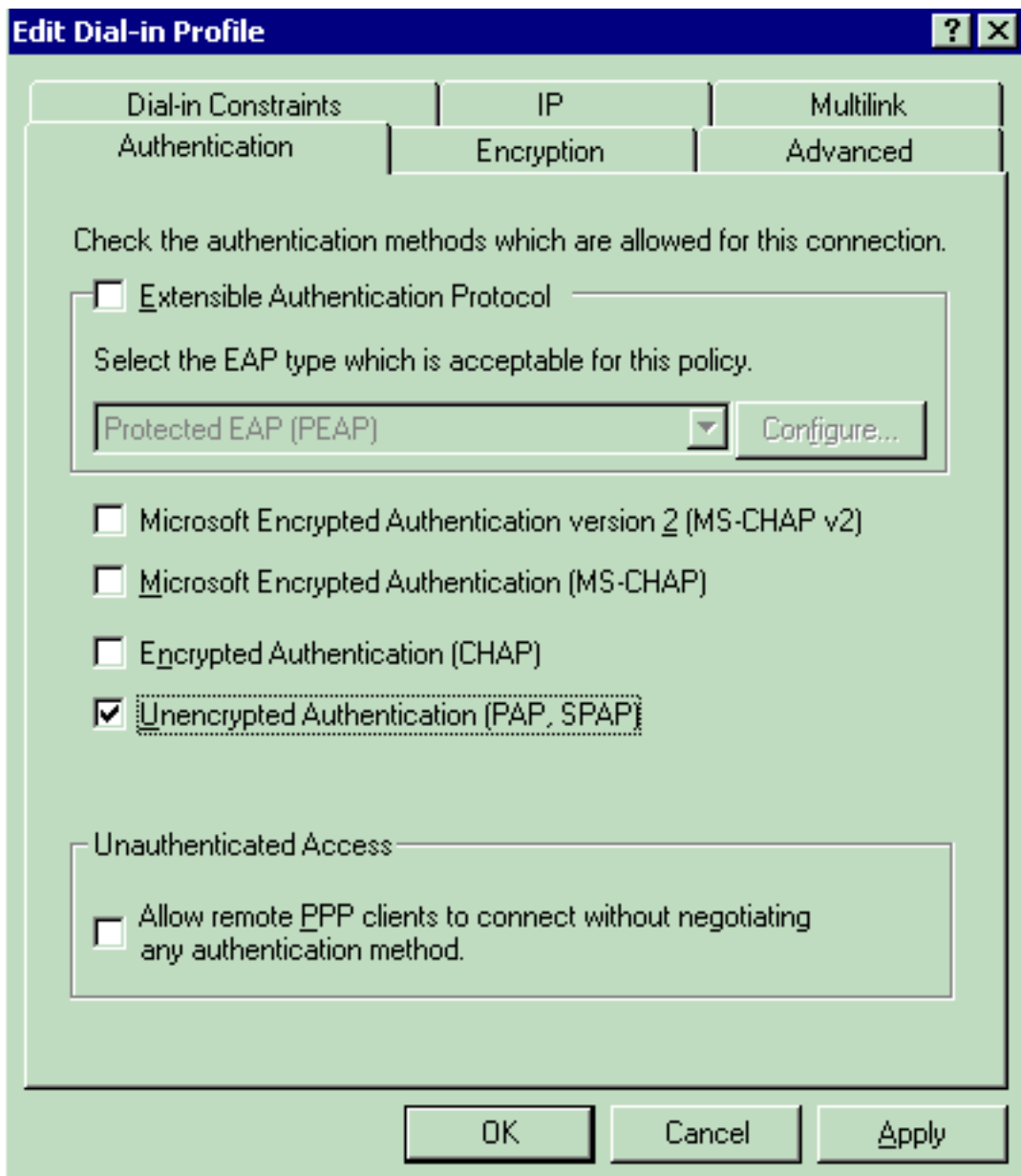
A fim configurar o perfil de usuário, o clique **edita o perfil no** indicador do perfil de usuário.O indicador do perfil do discado da edição



aparece.

a aba da **autenticação**, a seguir escolha o método de autenticação que é usado no WLAN. Este exemplo usa a autenticação não criptografada (PAP,

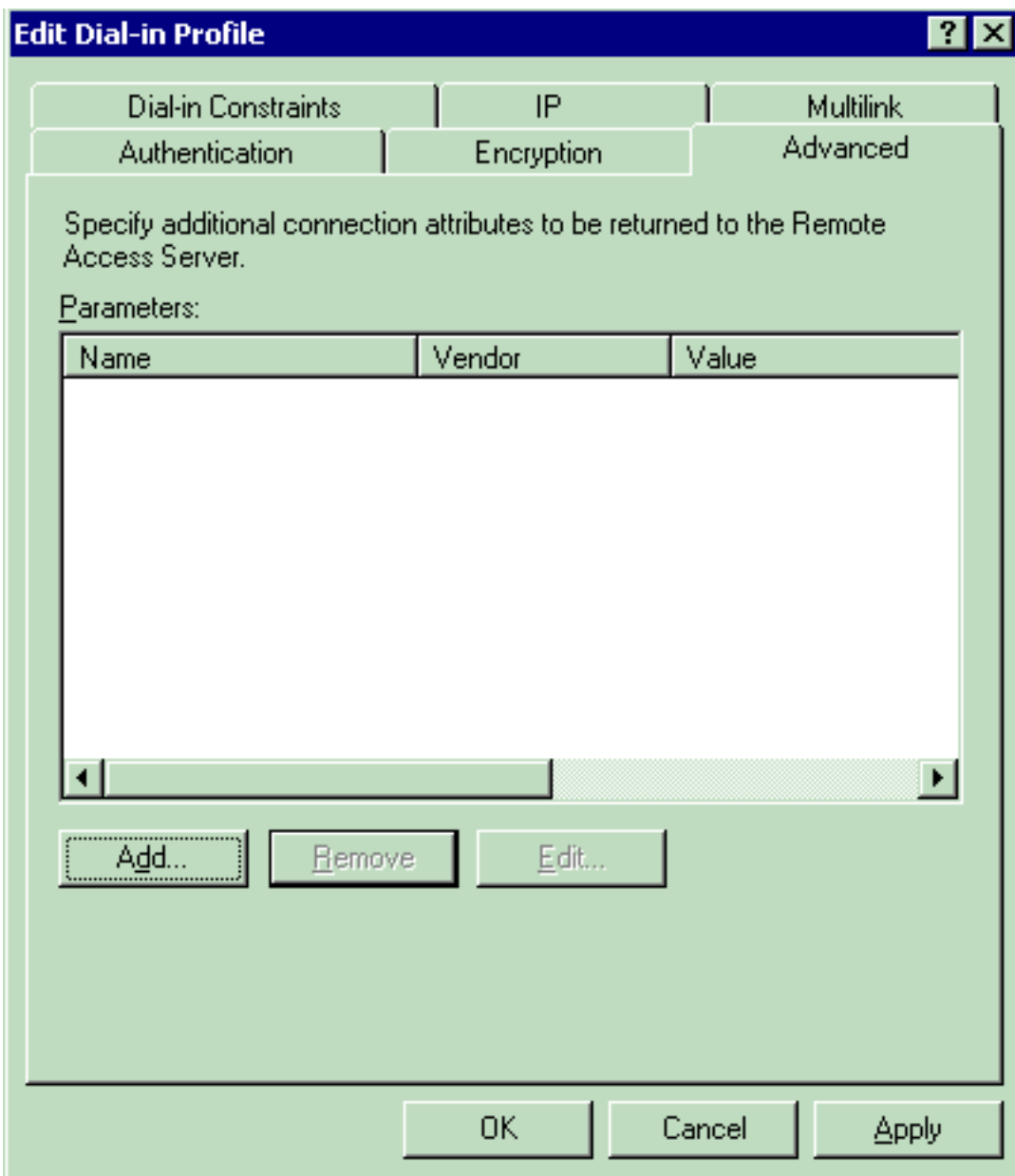
Clique



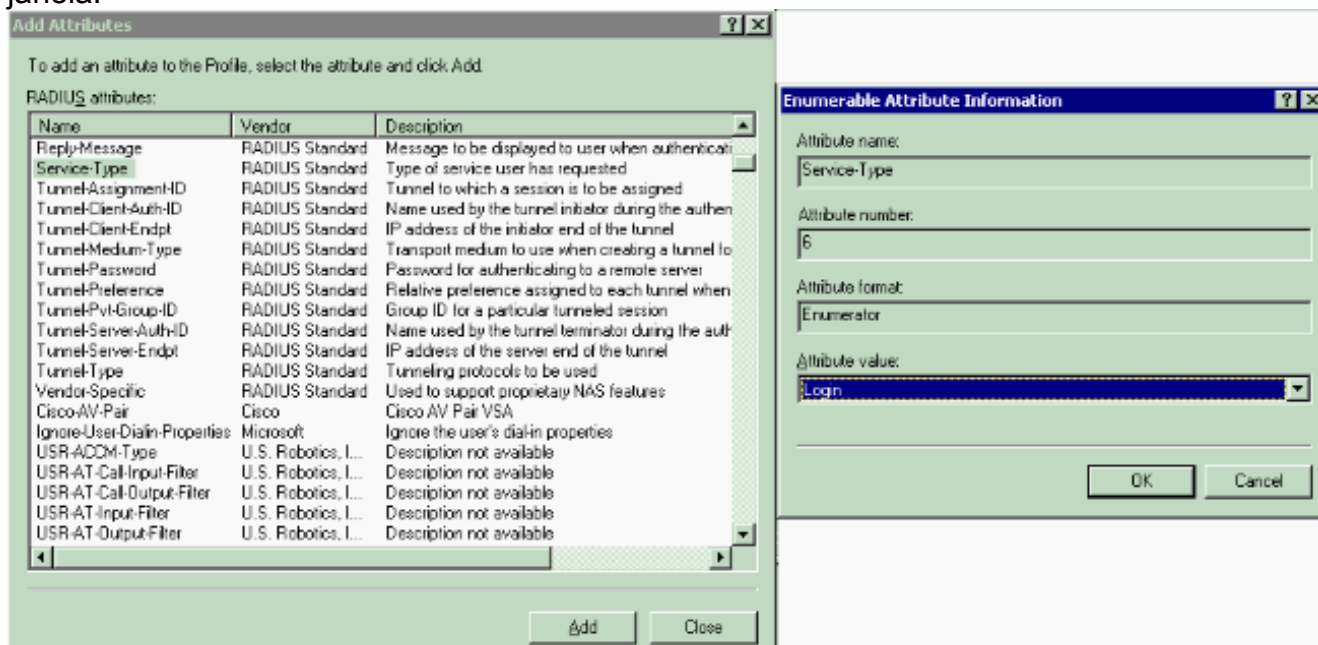
SPAP).

na guia Advanced. Remova todos os parâmetros padrão e o clique

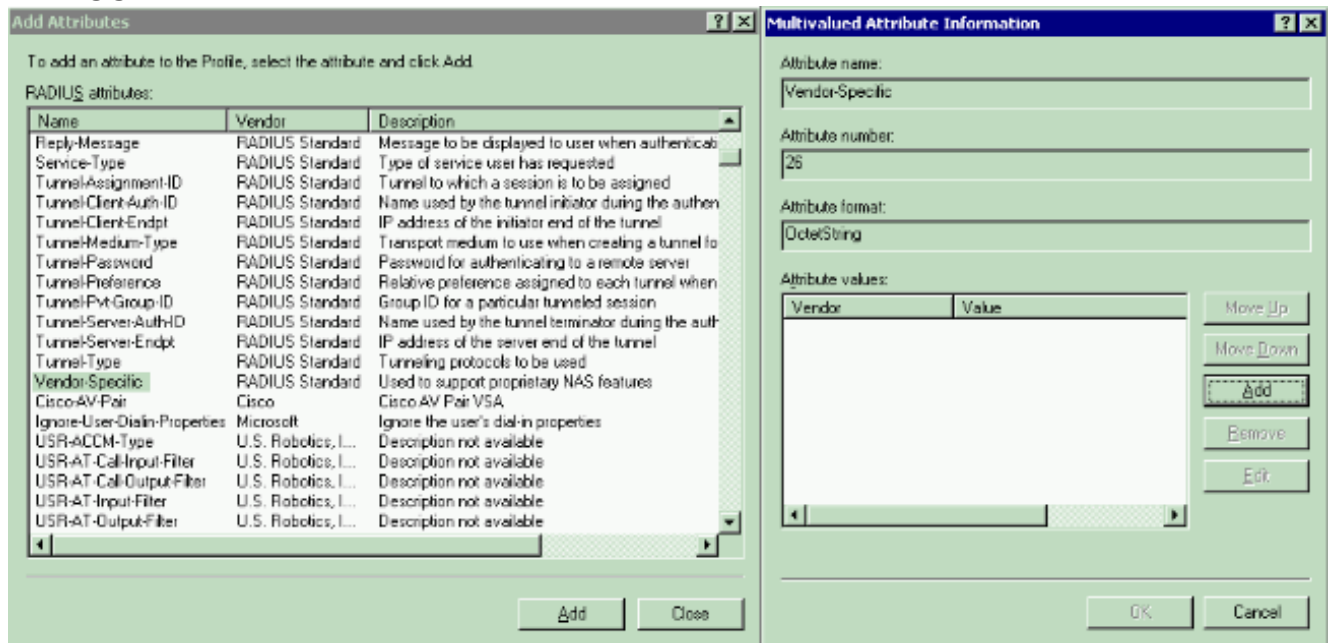
Clique



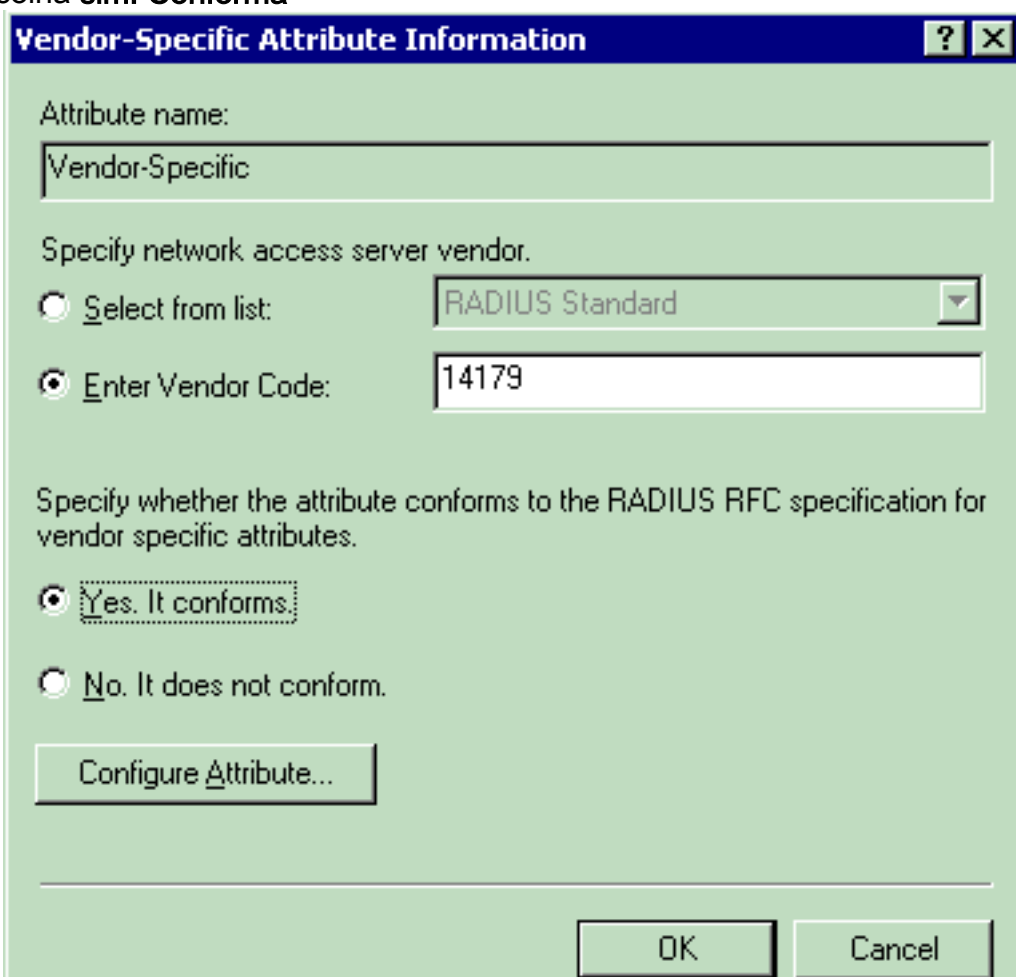
adiciona. Do indicador dos atributos adicionar, o tipo de serviço seletor, escolhe então o valor do início de uma sessão da próxima janela.



Em seguida, você precisa de selecionar o **atributo específico de fornecedor** da lista de atributos RADIUS.

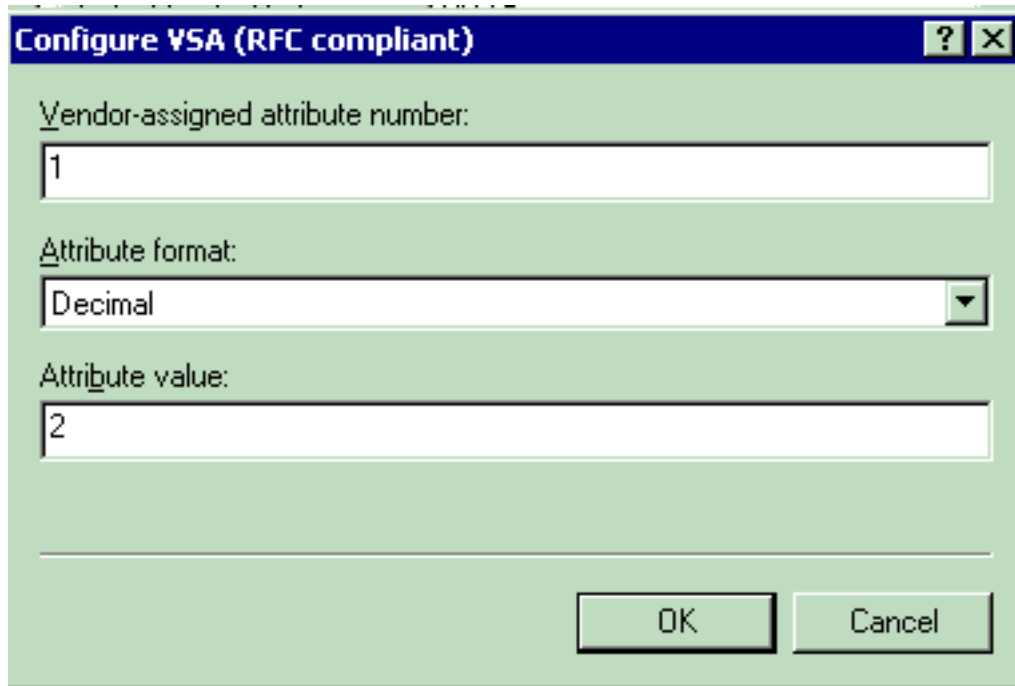


Na próxima janela, o clique **adiciona** a fim selecionar um VSA novo. A janela de informação do atributo específico de fornecedor aparece. Sob especificar o vendedor do servidor de acesso de rede, escolhem **dão entrada ao código de fornecedor**. Dê entrada ao código de fornecedor para Airespace VSA. O código de fornecedor do VSA do Cisco Airespace é 14179. Porque este atributo se conforma com a especificação do RADIUS RFC para VSA, escolha **sim**. **Conforma-**



se. O clique

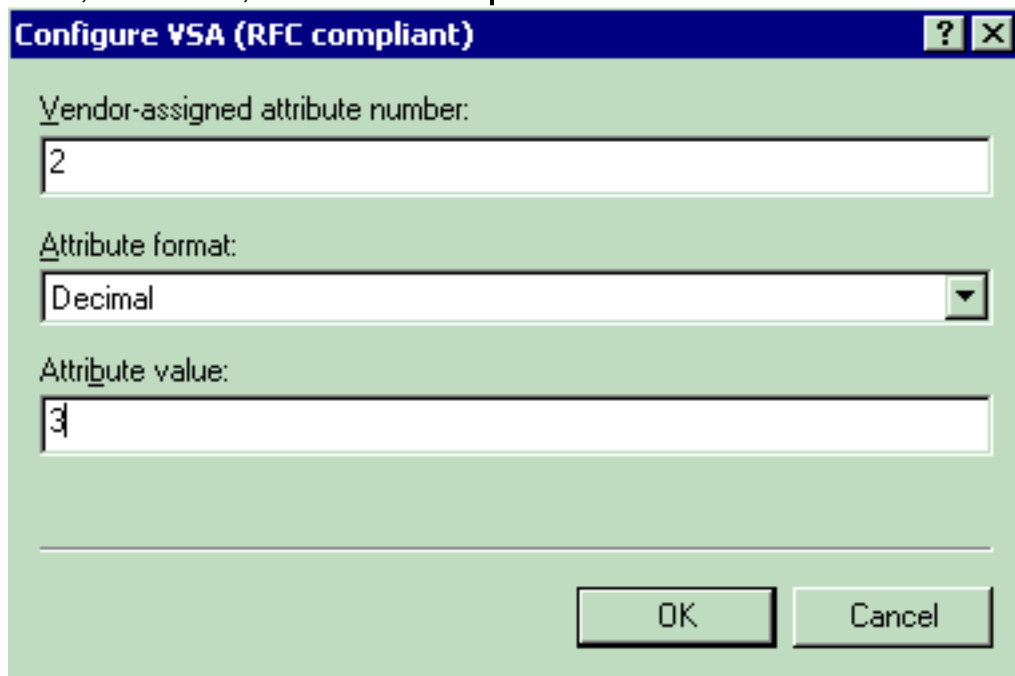
configura o atributo.No indicador configurar VSA (em conformidade com RFC), incorpore o número de atributo Vendedor-atribuído, o formato de atributo e o valor de atributo, que dependem do VSA que você quer usar.Para ajustar o ID de WLAN em uma base do usuário per.:**Nome do atributo** — Airespace-WLAN-identificação**número de atributo Vendedor-atribuído** — 1**Formato de atributo** — Inteiro/decimal**Valor** — ID de WLAN**Exemplo 1**



The screenshot shows a dialog box titled "Configure VSA (RFC compliant)". It has three input fields: "Vendor-assigned attribute number" with the value "1", "Attribute format" with a dropdown menu showing "Decimal", and "Attribute value" with the value "2". At the bottom, there are "OK" and "Cancel" buttons.

Para ajustar o perfil

de QoS em uma base do usuário per.:**Nome do atributo** — Airespace-QoS-nível**número de atributo Vendedor-atribuído** — 2**Formato de atributo** — Inteiro/decimal**Valor** — 0 - prata; 1 - Ouro; 2 - Platina; 3 - Bronze**Exemplo 2**



The screenshot shows a dialog box titled "Configure VSA (RFC compliant)". It has three input fields: "Vendor-assigned attribute number" with the value "2", "Attribute format" with a dropdown menu showing "Decimal", and "Attribute value" with the value "3". At the bottom, there are "OK" and "Cancel" buttons.

Para ajustar o valor

DSCP em uma base do usuário per.:**Nome do atributo** — Airespace-DSCP**number Vendedor-atribuído do atributo** — 3**Formato de atributo** — Inteiro/decimal**Valor** — Valor DSCP**Exemplo 3**

Configure VSA (RFC compliant)

Vendor-assigned attribute number:
3

Attribute format:
Decimal

Attribute value:
46

OK Cancel

Para ajustar o 802.1p-Tag em uma base do usuário per.: Nome do atributo — Airespace-802.1p-Tag número de atributo Vendedor-atribuído — 4 Formato de atributo — Inteiro/decimal Valor — 802.1p-

Configure VSA (RFC compliant)

Vendor-assigned attribute number:
4

Attribute format:
Decimal

Attribute value:
5

OK Cancel

Tag Exemplo 4 Para ajustar a relação (VLAN) em uma base do usuário per.: Nome do atributo — Airespace-Relação-nome número de atributo Vendedor-atribuído — 5 Formato de atributo — Corda Valor — Nome da interface Exemplo 5

Configure VSA (RFC compliant) [?] [X]

Vendor-assigned attribute number:

Attribute format:

Attribute value:

[OK] [Cancel]

Para ajustar o ACL

em uma base do usuário per.: Nome do atributo — Airespace-ACL-nome número de atributo
 Vendedor-atribuído — 6 Formato de atributo — Corda Valor — ACL-nome Exemplo 6

Configure VSA (RFC compliant) [?] [X]

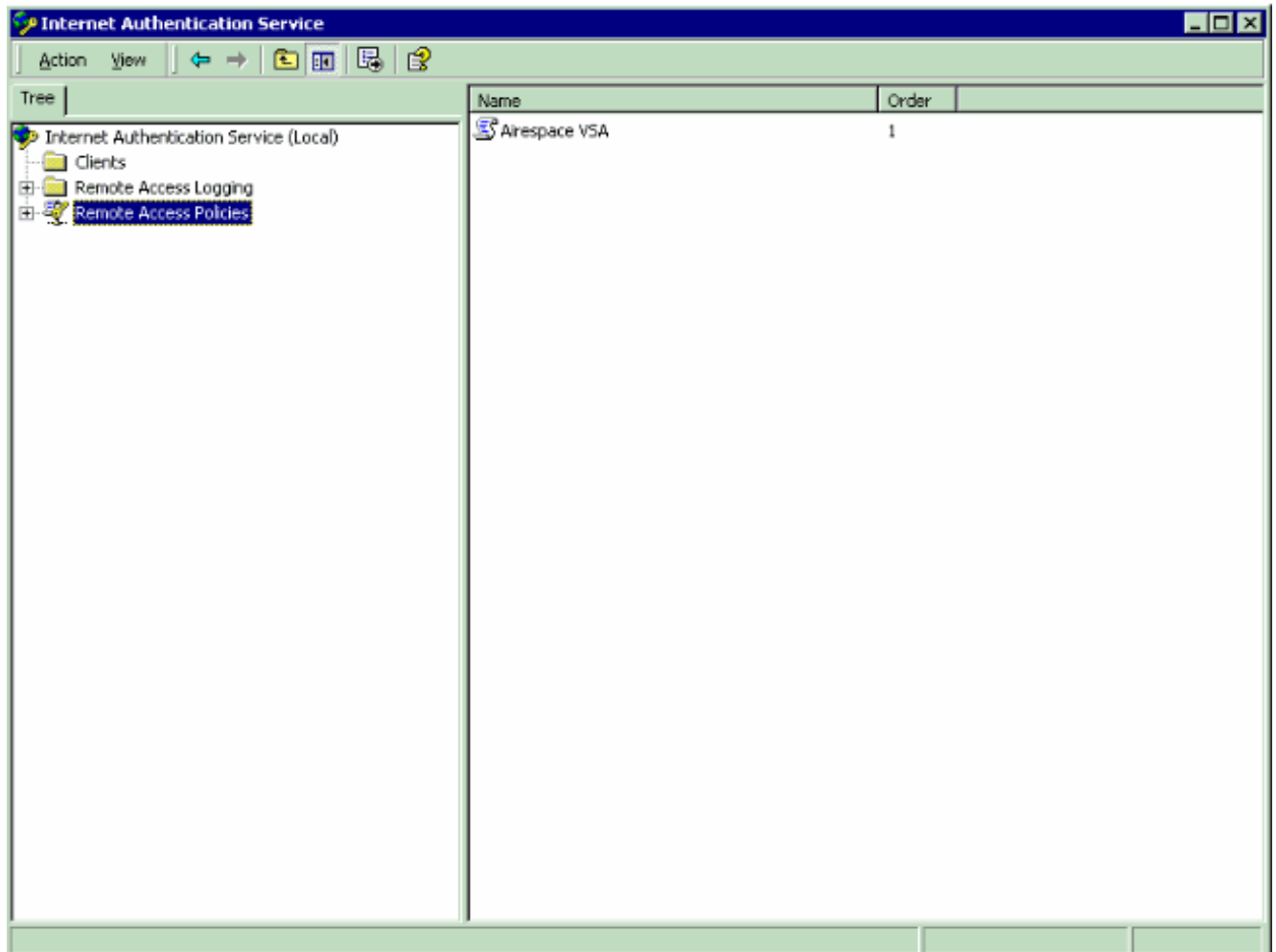
Vendor-assigned attribute number:

Attribute format:

Attribute value:

[OK] [Cancel]

8. Uma vez que você configurou os VSA, clique a **APROVAÇÃO** até que você ver o indicador do perfil de usuário.
9. Então, **revestimento do** clique a fim terminar a configuração. Você pode ver a política nova sob políticas de acesso remoto.



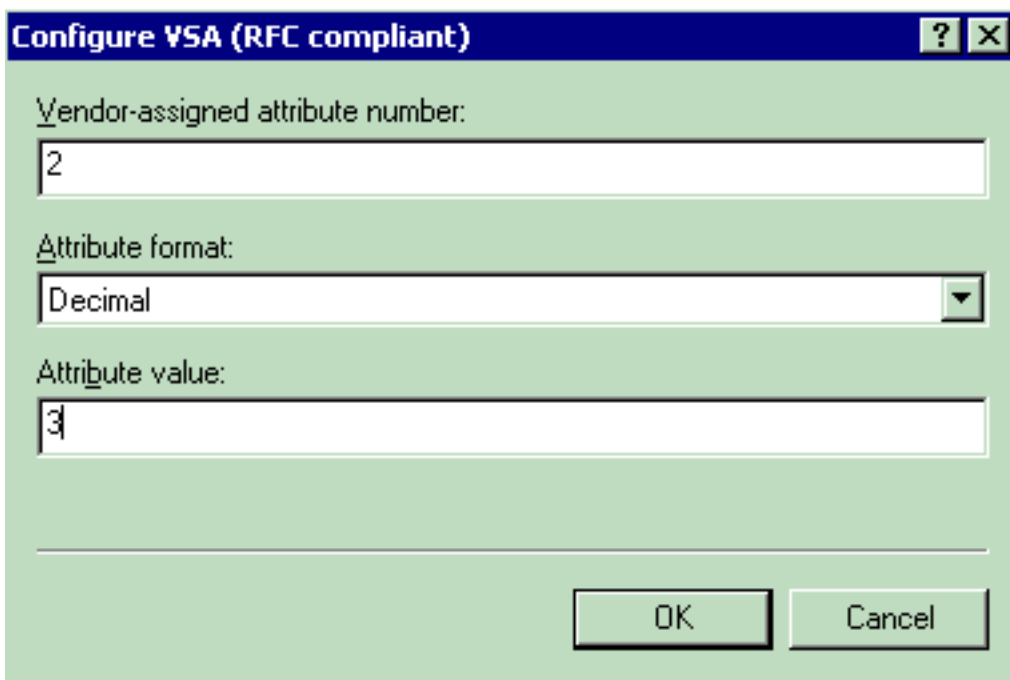
Exemplo de configuração

Neste exemplo, um WLAN é configurado para a autenticação da Web. Os usuários são autenticados pelo servidor Radius de IAS, e o servidor Radius é configurado para distribuir políticas de QoS em uma base do usuário per.

The screenshot displays the Cisco Systems WLANS configuration interface. The main content area is titled "WLANS > Edit" and shows the configuration for WLAN ID 1, SSID-WLC2. The "General Policies" section includes settings for Radio Policy (All), Admin Status (Enabled), Session Timeout (0), Quality of Service (QoS) (Silver (best effort)), WMM Policy (Disabled), 7920 Phone Support (Client CAC Limit and AP CAC Limit), Broadcast SSID (Enabled), Aironet IE (Enabled), Allow AAA Override (Enabled), Client Exclusion (Enabled with a 60-second timeout), DHCP Server (Override), DHCP Addr. Assignment (Required), Interface Name (internal), MFP Version Required (1), MFP Signature Generation (Enabled), and H-REAP Local Switching (Disabled). The "Security Policies" section shows Layer 2 Security (None) and Layer 3 Security (None) with Web Policy and Authentication enabled. The "Radius Servers" section shows a single server (Server 1) with IP 172.16.1.1 and Port 1812. Red circles highlight the QoS, AAA Override, and Radius Server settings. A red box highlights the Layer 3 Security settings. Red text at the bottom of the page provides warnings: "* Web Policy cannot be used in combination with IPsec and L2TP.", "** When client exclusion is enabled, a timeout value of zero means infinity (will require administrative override to reset excluded clients)", and "*** CKIP is not supported by 10xx APs".

Como você pode ver deste indicador, a autenticação da Web é permitida, o Authentication Server é 172.16.1.1, e a ultrapassagem AAA é permitida igualmente no WLAN. O ajuste de QoS do padrão para este WLAN é ajustado para pratear.

No servidor Radius de IAS, uma política de acesso remoto é configurada que retorne o QoS bronze do atributo que no RAIO aceita o pedido. Isto é feito quando você configura o específico VSA ao atributo de QoS.



Veja [configurar a política de acesso remoto na](#) seção de [IAS](#) deste documento para informações detalhadas sobre de como configurar uma política de acesso remoto no servidor de IAS.

Uma vez o servidor de IAS, o WLC, e o REGAÇO é configurado para esta instalação, os clientes Wireless pode usar a autenticação da Web a fim conectar.

Verificar

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

Quando o usuário conecta ao WLAN com um usuário - a identificação e a senha, o WLC passam as credenciais ao servidor Radius de IAS que autentica o usuário contra as circunstâncias e o perfil de usuário configurados na política de acesso remoto. Se a autenticação de usuário é bem sucedida, o servidor Radius retorna um RAIO aceita o pedido que igualmente contém os valores da ultrapassagem AAA. Neste caso, a política de QoS do usuário é retornada.

Você pode emitir o **comando debug aaa all enable** a fim ver a sequência de evento que ocorre durante a autenticação. Está aqui 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-Identifiaer.....
      0x574c4332 (1464615730) (4 bytes)
Wed Apr 18 18:15:12 2007:      AVP[05] Airespace / WLAN-Identifiaer.....
      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 da saída, o usuário é autenticado. Então, os valores da ultrapassagem AAA são retornados com o RAIO aceitam a mensagem. Neste caso, o usuário é dado a política de QoS do bronze.

Você pode verificar este no WLC GUI também. Aqui está um exemplo:

The screenshot shows the Cisco WLC GUI with the following data:

Client Properties		AP Properties	
MAC Address	00:40:96:ac:e6:57	AP Address	00:0b:85:5b:fb:d0
IP Address	20.0.0.1	AP Name	ap:5b:fb:d0
User Name	User-VLAN10	AP Type	802.11a
Port Number	1	WLAN SSID	SSID-WLC2
Interface	internal	Status	Associated
VLAN ID	20	Association ID	1
CCX Version	CCXv3	802.11 Authentication	Open System
E2E Version	Not Supported	Reason Code	0
Mobility Role	Local	Status Code	0
Mobility Peer IP Address	N/A	CF Pollable	Not Implemented
Policy Manager State	RUN	CF Poll Request	Not Implemented
Security Information		Short Preamble	Not Implemented
Security Policy Completed	Yes	PBCC	Not Implemented
Policy Type	N/A	Channel Agility	Not Implemented
Encryption Cipher	None	Timeout	0
EAP Type	N/A	WEP State	WEP Disable
Quality of Service Properties			
WMM State	Disabled		
QoS Level	Bronze		
Diff Serv Code Point (DSCP)	disabled		
802.1p Tag	disabled		
Average Data Rate	disabled		

Note: O perfil de QoS do padrão para este SSID é prata. Contudo, porque a ultrapassagem AAA é selecionada e o usuário é configurado com um perfil de QoS do bronze no servidor de IAS, o perfil de QoS do padrão é cancelado.

Troubleshooting

Você pode usar o comando **debug aaa all enable** no WLC pesquisar defeitos a configuração. Um exemplo da saída deste debuga em uma rede de trabalho é mostrado na seção da [verificação](#) deste documento.

Note: 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](#)
- [Restrinja o acesso WLAN baseado no SSID com WLC e exemplo de configuração do Cisco Secure ACS](#)
- [Suporte de produtos Wireless](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)