

Cisco Aironet VSA's op Microsoft IAS Radius Server Configuratievoorbeeld

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Achtergrondinformatie](#)

[De IAS voor Airespace VSA's configureren](#)

[De WLC configureren als een AAA-client in de IAS](#)

[Het externe toegangsbeleid op de IAS configureren](#)

[Configuratievoorbeeld](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

[Inleiding](#)

Dit document toont hoe u een Microsoft Internet Verification Service (IAS)-server kunt configureren ter ondersteuning van Cisco Aironet Vendor Specific Attributes (VSA's). De leveranciercode voor Cisco Airesponders is **14179**.

[Voorwaarden](#)

[Vereisten](#)

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

- Kennis van de wijze waarop u een IAS-server moet configureren
- Kennis van de configuratie van Lichtgewicht Access Point (LAP's) en Cisco draadloze LAN-controllers (WLC's)
- Kennis van Cisco Unified Wireless Security-oplossingen

[Gebruikte componenten](#)

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Microsoft Windows 2000-server met IAS

- Cisco 4400 WLC-software versie 4.0.206.0
- Cisco 1000 Series LAP's
- 802.11 a/b/g draadloze clientadapter met firmware 2.5
- Aironet Desktop Utility (ADU) versie 2.5

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Opmerking: Dit document is bedoeld om de lezer een voorbeeld te geven over de configuratie die op de IAS-server vereist is ter ondersteuning van VSA's van Cisco Airespo. De DIA-serverconfiguratie die in dit document wordt gepresenteerd, is in het laboratorium getest en werkt zoals verwacht. Als u de IAS-server niet kunt configureren, neemt u contact op met Microsoft voor ondersteuning. Cisco TAC ondersteunt Microsoft Windows-serverconfiguratie niet.

Dit document gaat ervan uit dat de WLC is ingesteld voor een eenvoudige bediening en dat de LAP's zijn geregistreerd op de WLC. Als u een nieuwe gebruiker bent die probeert om de WLC in te stellen voor basisbediening met LAN's, raadpleegt u [Lichtgewicht AP \(LAP\)-registratie naar een draadloze LAN-controller \(WLC\)](#).

Conventies

Raadpleeg [Cisco Technical Tips Conventions \(Conventies voor technische tips van Cisco\) voor meer informatie over documentconventies](#).

Achtergrondinformatie

In de meeste draadloze LAN-systemen (WLAN) heeft elk WLAN een statisch beleid dat van toepassing is op alle klanten die bij een serviceset ID (SSID) zijn gekoppeld. Hoewel krachtig, heeft deze methode beperkingen omdat het van cliënten vereist om met verschillende SSIDs te associëren om verschillend QoS en veiligheidsbeleid te erven.

Maar de Cisco draadloze LAN-oplossing ondersteunt identiteitsnetwerken, waardoor het netwerk kan adverteren met één SSID en bepaalde gebruikers om verschillende QoS- of beveiligingsbeleid te erven op basis van hun gebruikersprofielen. Het specifieke beleid dat u kunt controleren met behulp van identiteitsnetwerken is onder meer:

- **Quality-of-Service**—Wanneer deze in een RADIUS-toegangsaccepteren wordt aangeboden, heeft de QoS-Level-waarde te boven de QoS-waarde die in het WLAN-profiel is gespecificeerd.
- **ACL**-wanneer de eigenschap Toegangscontrolelijst (ACL) aanwezig is in de RADIUS-toegangscontrole Accept, past het systeem de ACL-naam op het clientstation toe nadat dit voor authentiek is verklaard. Dit heeft betrekking op ACL's die aan de interface zijn toegewezen.
- **VLAN**-Wanneer een VLAN-interface-naam of VLAN-tag in een RADIUS-toegangscontrole aanwezig is, plaatst het systeem de client op een specifieke interface.
- **WLAN-id** - Wanneer de WLAN-ID eigenschap in de RADIUS-toegangscontrole aanwezig is, past het systeem de WLAN-ID (SSID) op het clientstation toe nadat deze voor authentiek is verklaard. De WLAN-id wordt door de WLC verzonden in alle gevallen van verificatie behalve

IPSec. In het geval van web authenticatie, als de WLC een WLAN-ID eigenschap in de authenticatiereactie van de AAA-server ontvangt en deze niet overeenkomt met de ID van de WLAN, wordt verificatie verworpen. Andere beveiligingsmethoden doen dat niet.

- **DSCP-waarde** - Wanneer deze in een RADIUS-toegangsbestand aanwezig is, heeft de DSCP-waarde voorrang op de DSCP-waarde die in het WLAN-profiel is gespecificeerd.
- **802.1p-Tag** - Wanneer u een RADIUS-toegangsaccepteren hebt, heeft de 802.1p waarde te veel waarde dan gespecificeerd in het WLAN-profiel.

Opmerking: de functie VLAN ondersteunt alleen MAC-filtering, 802.1X en Wi-Fi Protected Access (WAP). De VLAN-functie ondersteunt geen webverificatie of IPSec. De lokale MAC Filter database van het besturingssysteem is uitgebreid om de interfacenaam op te nemen. Hiermee kunnen lokale MAC-filters specificeren welke interface de client moet worden toegewezen. Er kan ook een afzonderlijke RADIUS-server worden gebruikt, maar de RADIUS-server moet worden gedefinieerd met behulp van de Security menu's.

Raadpleeg [Identiteitsnetwerken configureren](#) voor meer informatie over identiteitsnetwerken.

[De IAS voor Airespace VSA's configureren](#)

Om de IAS voor VSA's te kunnen configureren moet u deze stappen voltooien:

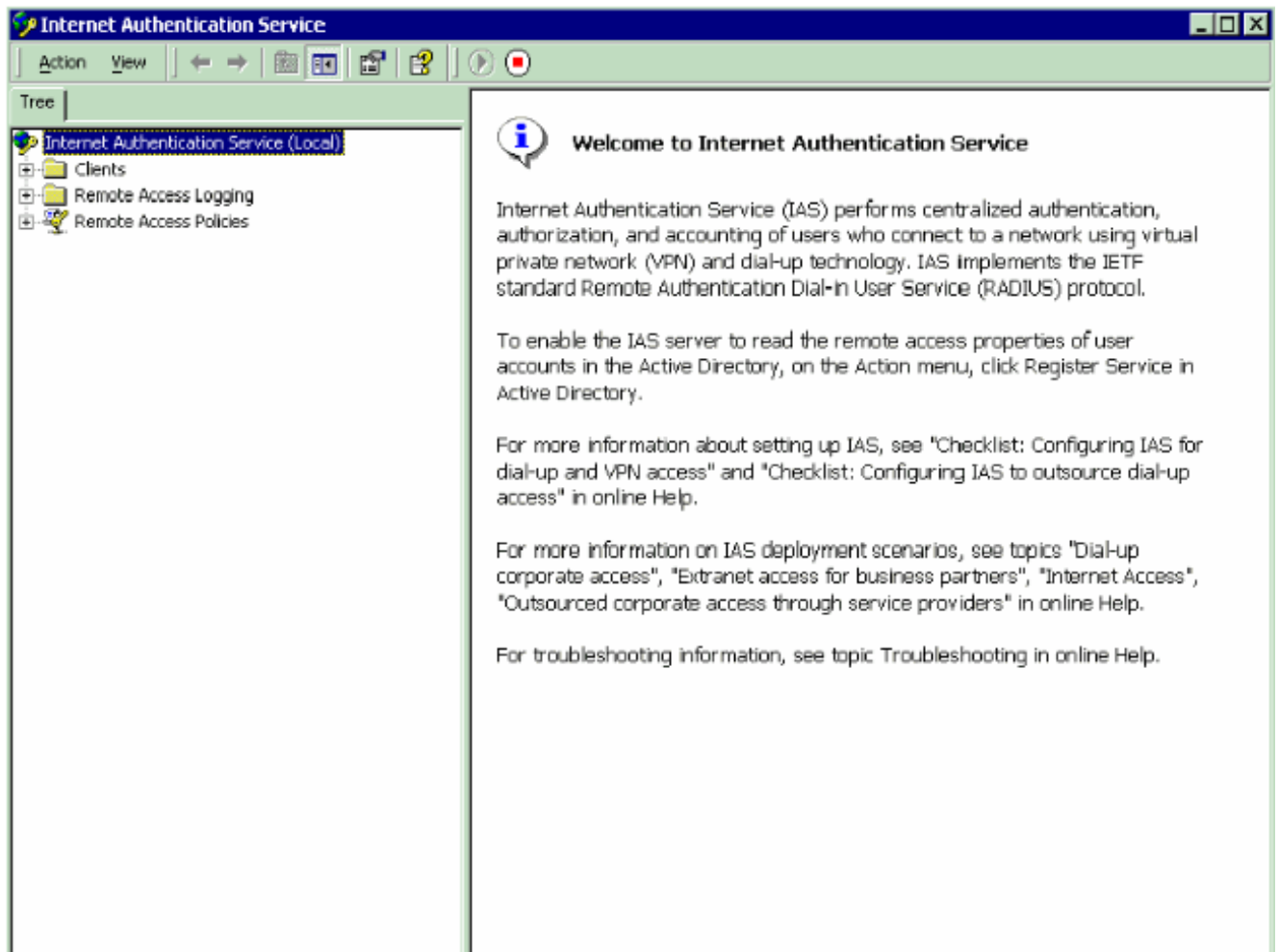
1. [De WLC configureren als een AAA-client in de IAS](#)
2. [Het externe toegangsbeleid op de IAS configureren](#)

Opmerking: de VSA's zijn ingesteld onder het beleid voor externe toegang.

[De WLC configureren als een AAA-client in de IAS](#)

Voltooi deze stappen om de WLC te configureren als een AAA-cliënt in de IAS:

1. Klik op **Programma's > Administratieve Gereedschappen > Internet Verificatieservice** om IAS te starten op de Microsoft 2000-server.



2. Klik met de rechtermuisknop op de map **Clients** en kies **Nieuwe client** om een nieuwe RADIUS-client toe te voegen.
3. Voer in het venster Add Client de naam van de client in en kies **RADIUS** als protocol. Klik vervolgens op **Volgende**. In dit voorbeeld is de naam van de client **WLC-1**. **Opmerking:** standaard is het protocol ingesteld op RADIUS.

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. Voer in het venster RADIUS-client toe het **IP-adres van de client, de client-verkoper** en het **gedeelde geheim** in. Klik op **Voltoeien** nadat u de clientinformatie hebt ingevoerd. Dit voorbeeld toont een client met de naam *WLC-1* met een IP-adres van *172.16.1.30*. De client-verkoper wordt op *Cisco* ingesteld en het gedeelde geheim is *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]

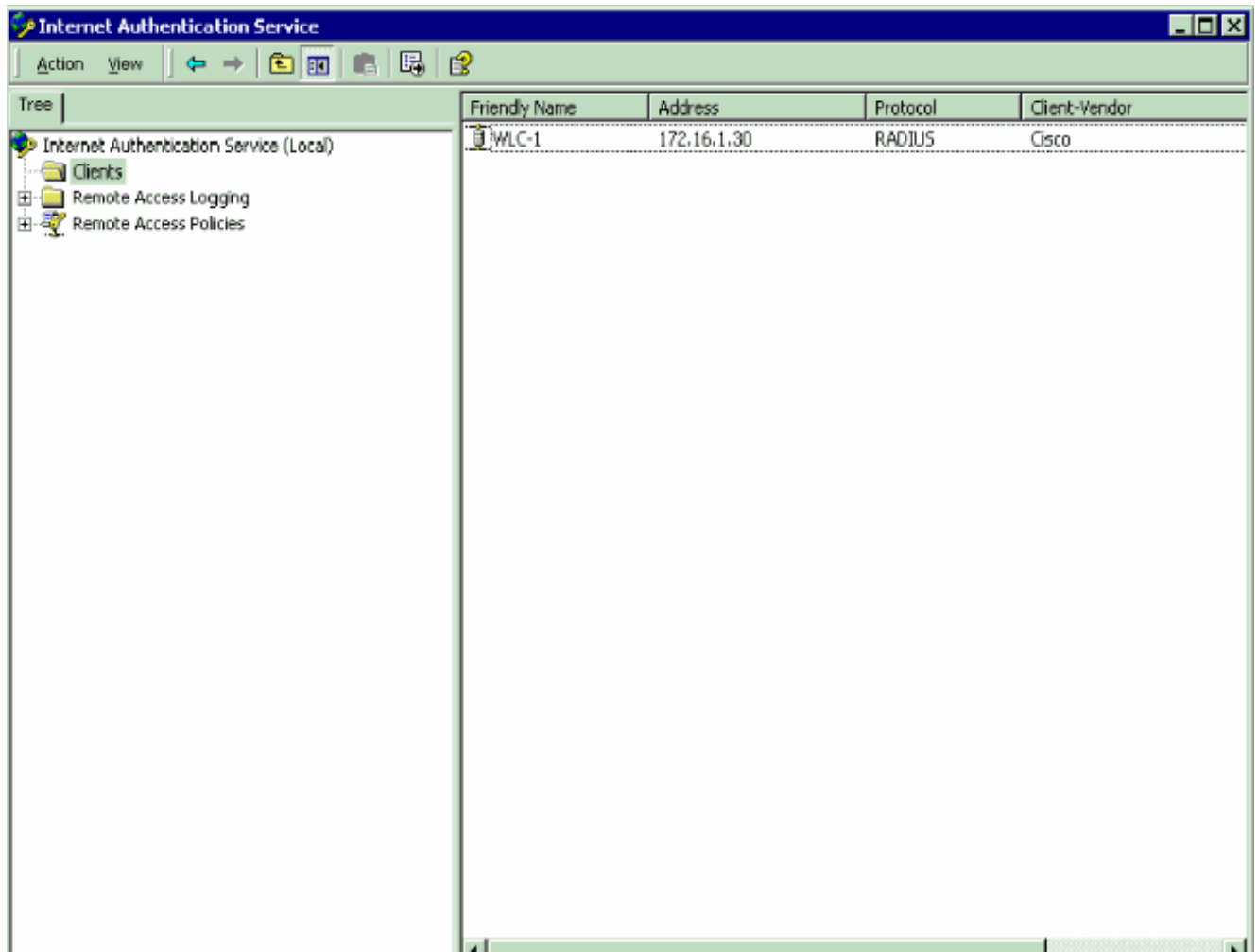
Client must always send the signature attribute in the request

Shared secret: [xxxxxxx]

Confirm shared secret: [xxxxxxx]

< Back Finish Cancel

Met deze informatie wordt de WLC genaamd WLC-1 toegevoegd als AAA-client van de IAS-server.

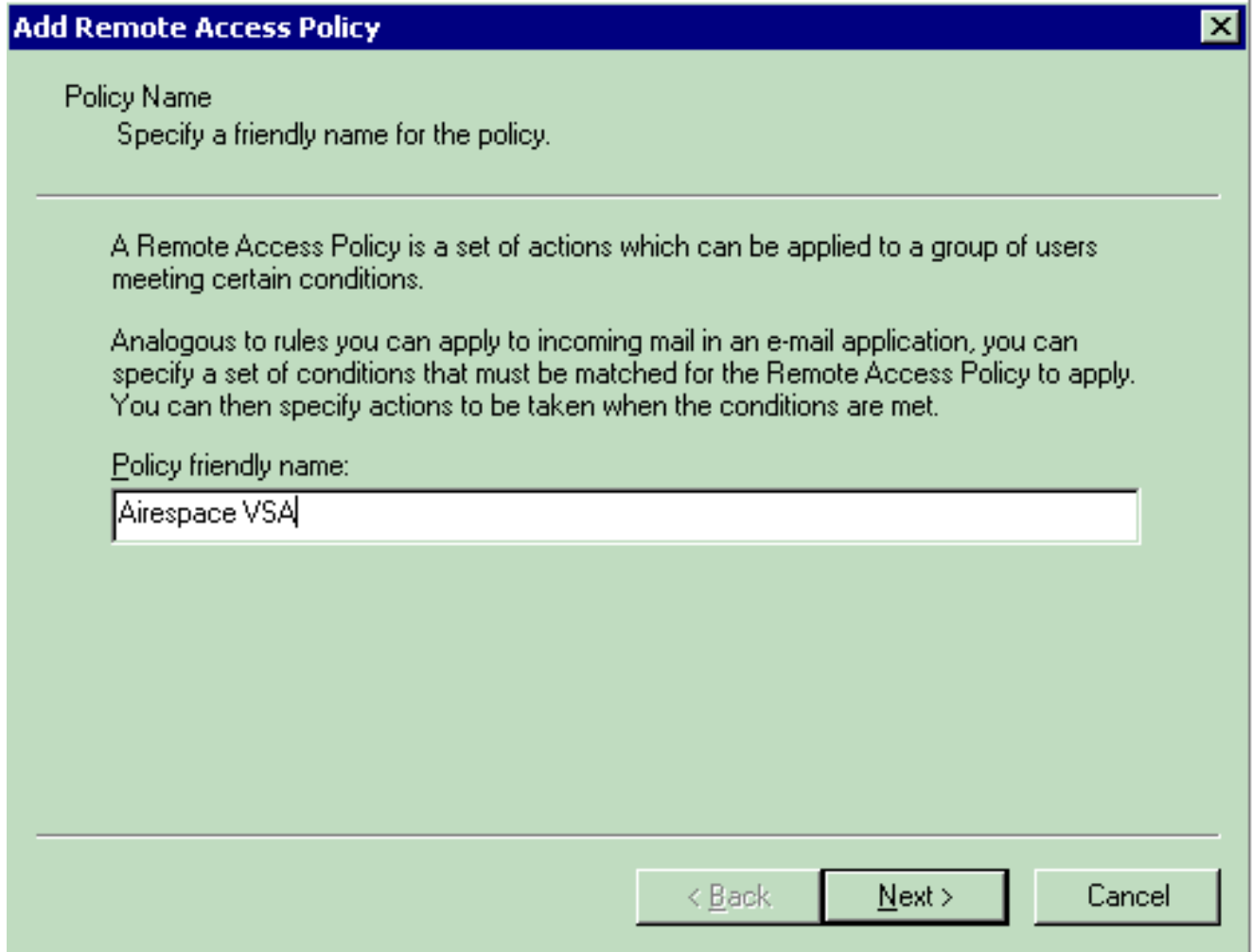


De volgende stap is een beleid voor toegang op afstand te maken en de VSA's te configureren.

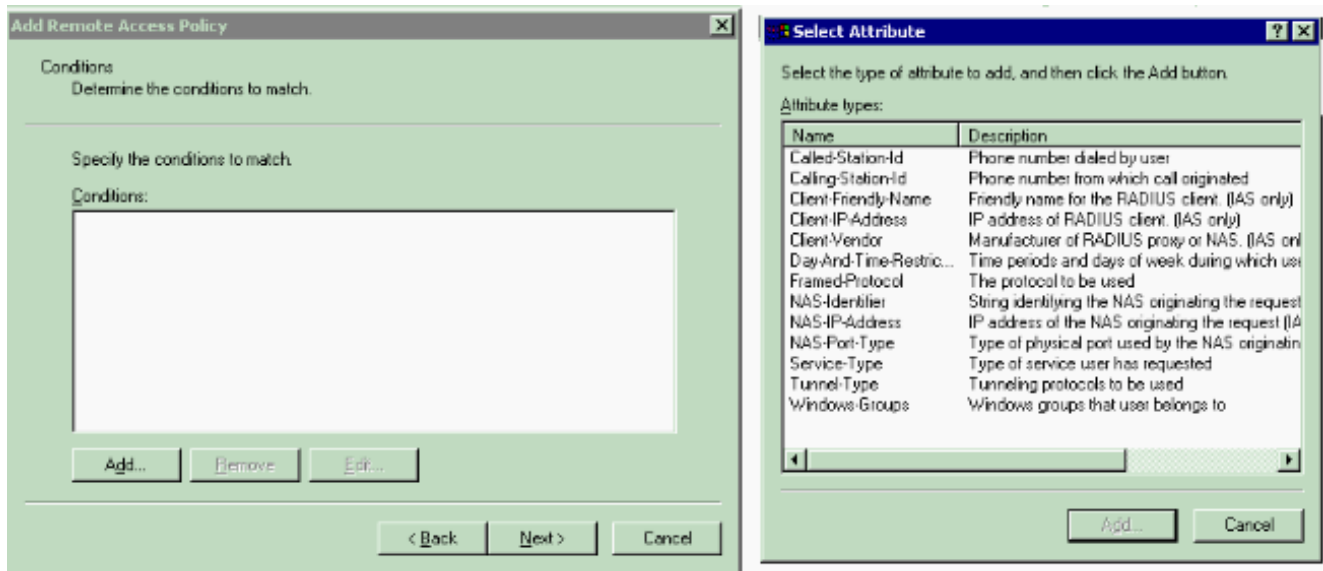
[Het externe toegangsbeleid op de IAS configureren](#)

Voltooi deze stappen om een nieuw beleid voor externe toegang op de IAS te vormen:

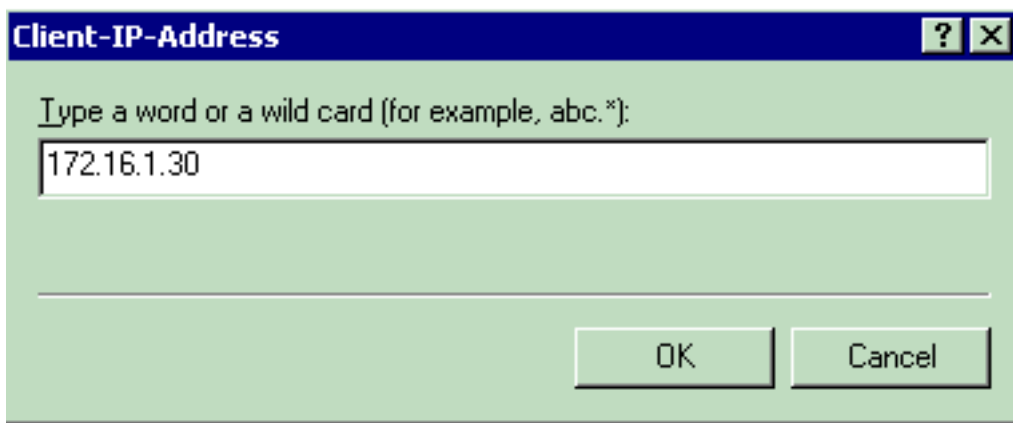
1. Klik met de rechtermuisknop op **beleid voor toegang op afstand** en kies **Nieuw Remote AccessMS-beleid**. Het venster Policy Name verschijnt.
2. Voer de naam van het beleid in en klik op **Volgende**.



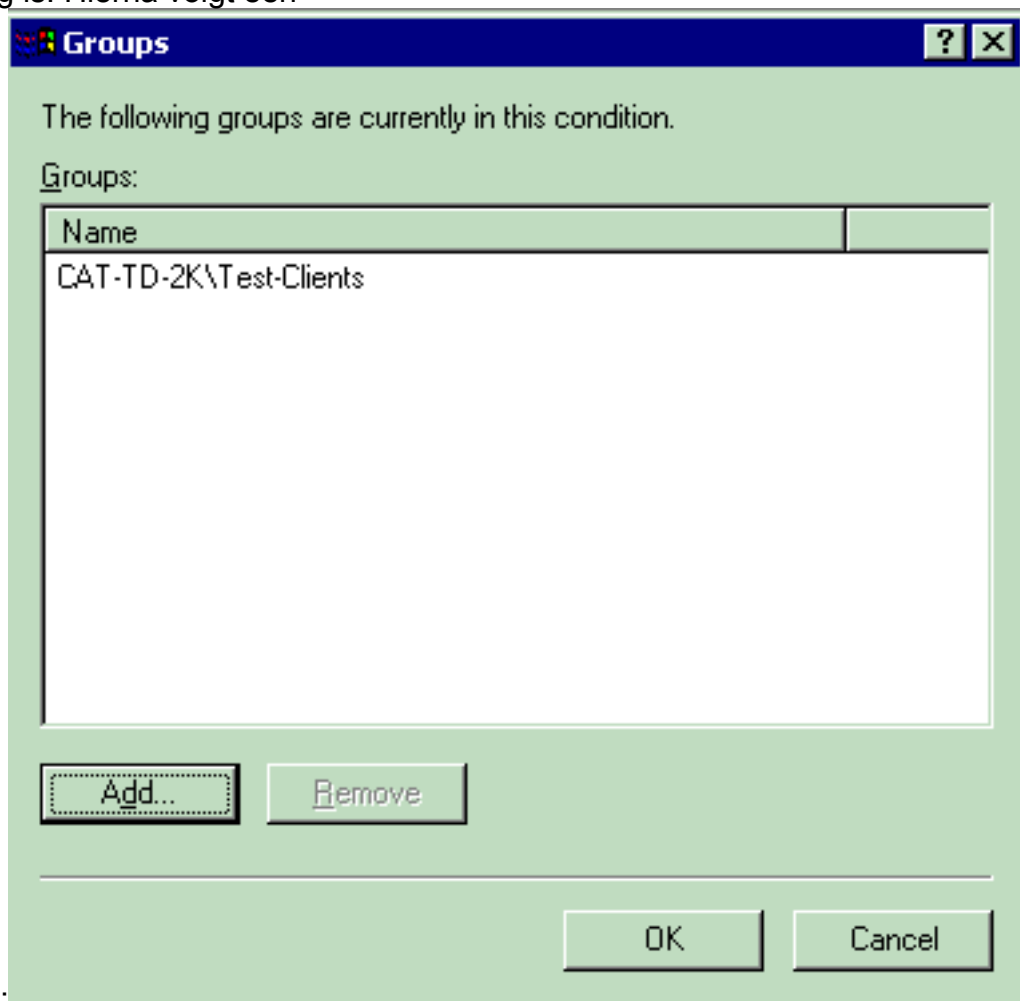
3. Selecteer in het volgende venster de voorwaarden waarvoor het beleid voor externe toegang van toepassing zal zijn. Klik op **Add** om de voorwaarden te selecteren.



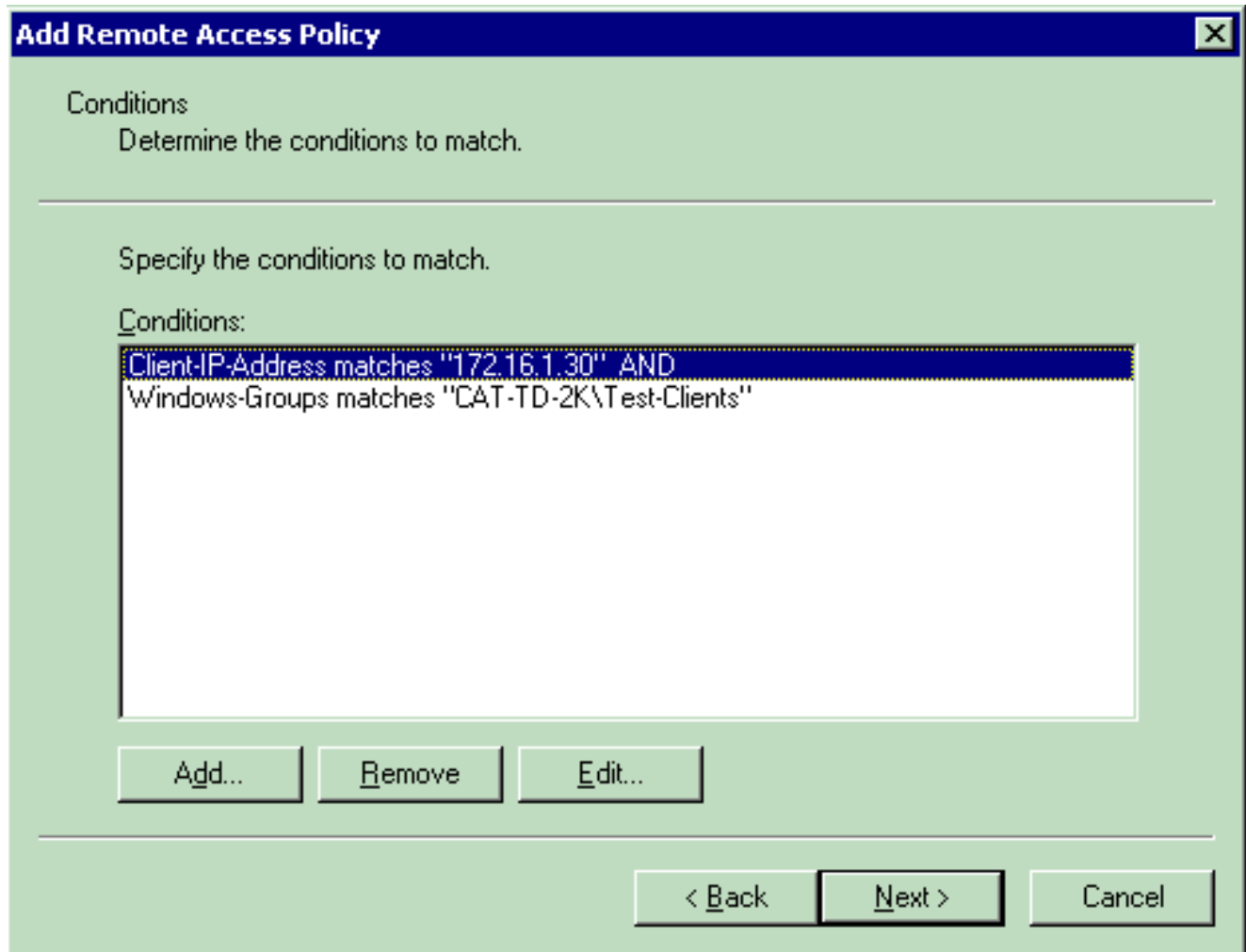
4. Selecteer in het menu Eigenschappen de volgende eigenschappen: **Client-IP-Adres**-Voer het IP-adres van de AAA-client in. In dit voorbeeld, wordt het IP van de WLCs adres ingevoerd zodat het beleid op pakketten van de WLC van toepassing



is. **Windows Groepen**-Selecteer de Windows-groep (de gebruikersgroep) waarvoor het beleid van toepassing is. Hierna volgt een

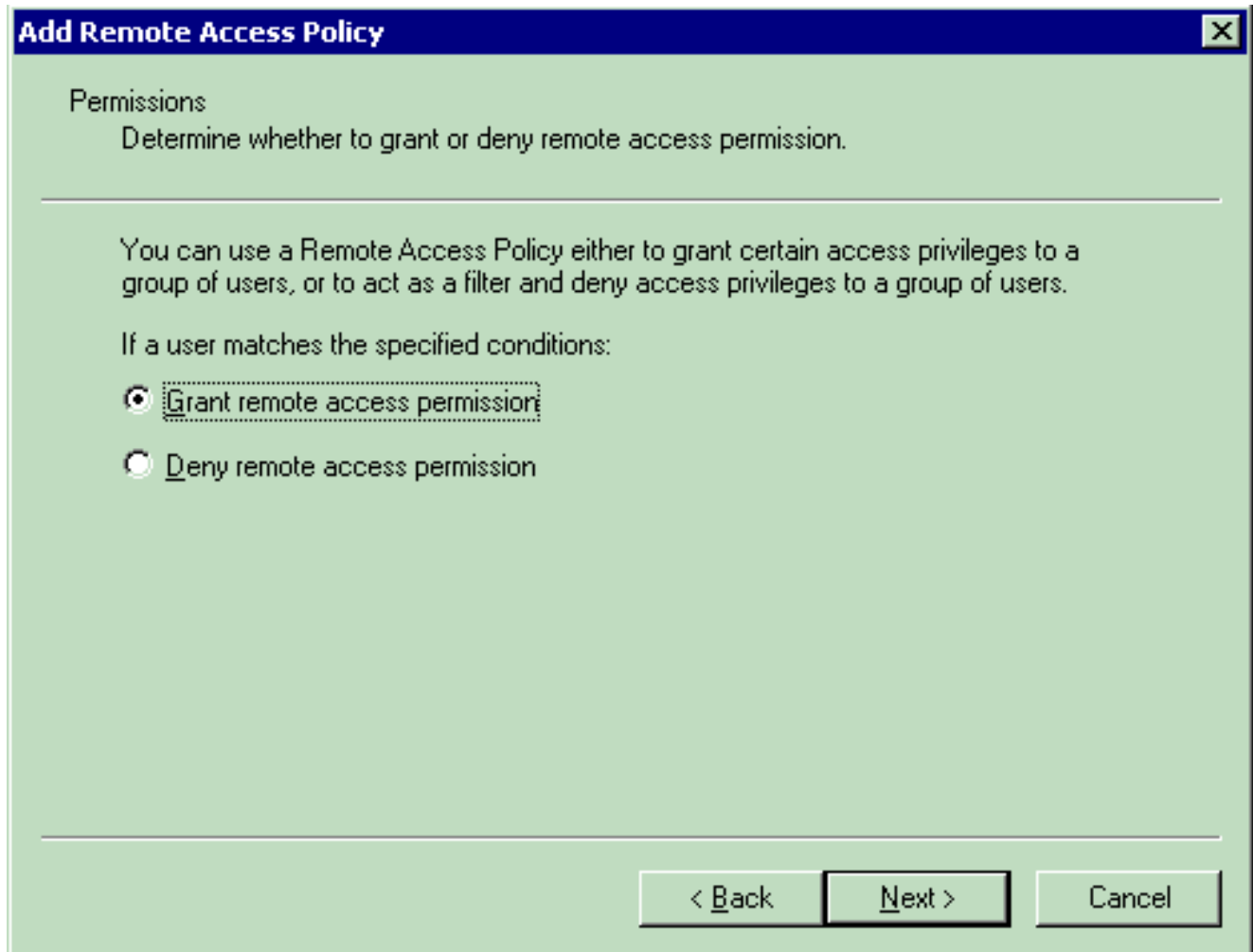


voorbeeld:



Dit voorbeeld laat slechts twee voorwaarden zien. Als er meer voorwaarden zijn, kunt u deze voorwaarden ook toevoegen en op **Volgende** klikken. Het venster Access verschijnt.

5. Kies in het venster **Toegang op afstand verlenen**. Nadat u deze optie hebt geselecteerd, krijgt de gebruiker toegang, mits de gebruiker de gespecificeerde voorwaarden aanpast (uit stap 2).



6. Klik op **Volgende**.

7. De volgende stap is het instellen van het gebruikersprofiel. Ook al zou u hebben opgegeven dat gebruikers op basis van de voorwaarden toegang geweigerd of verleend zouden moeten worden, het profiel kan nog steeds worden gebruikt als de voorwaarden van dit beleid op een per-gebruiker-basis worden overschreven.

Add Remote Access Policy



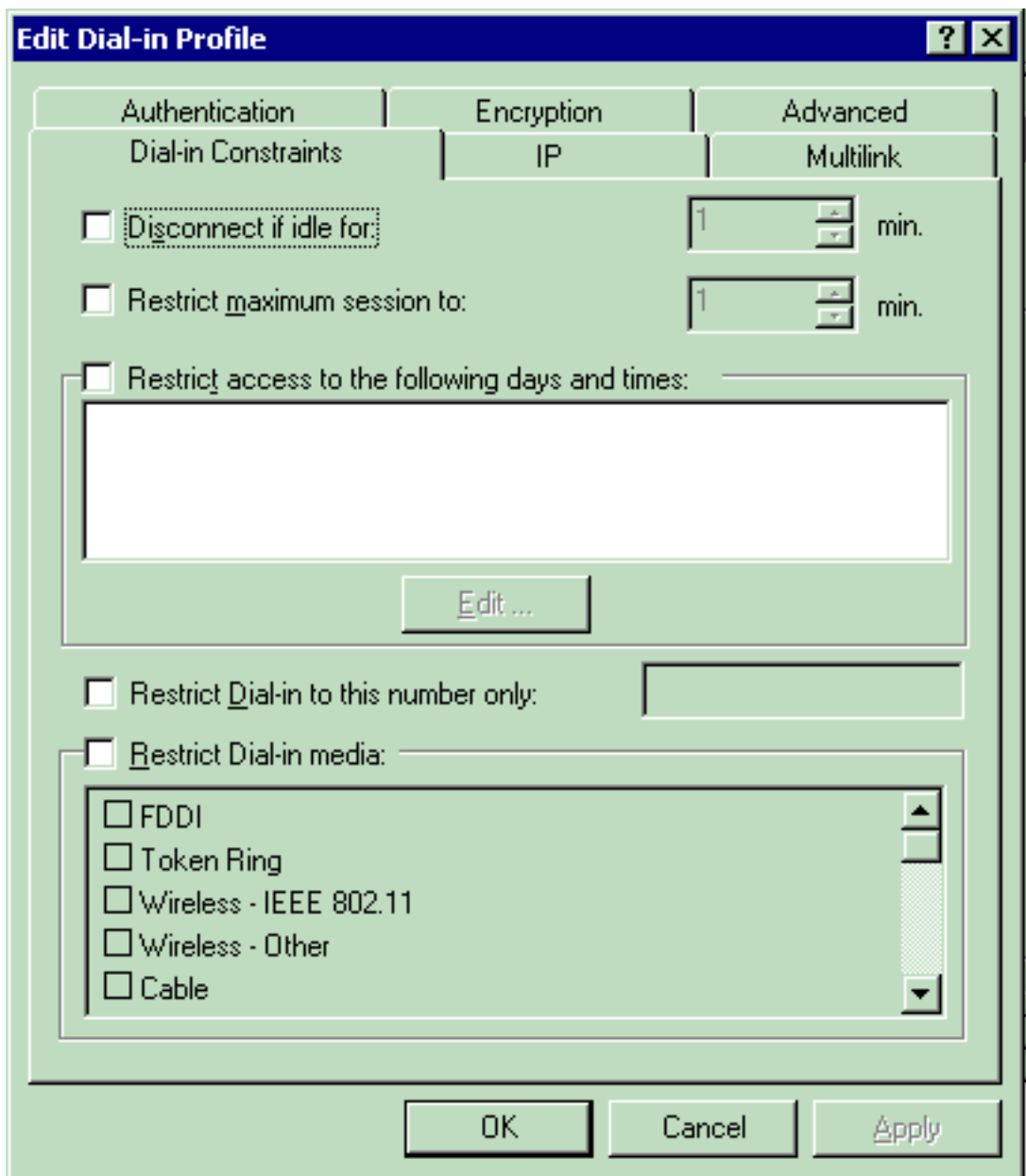
User Profile

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.

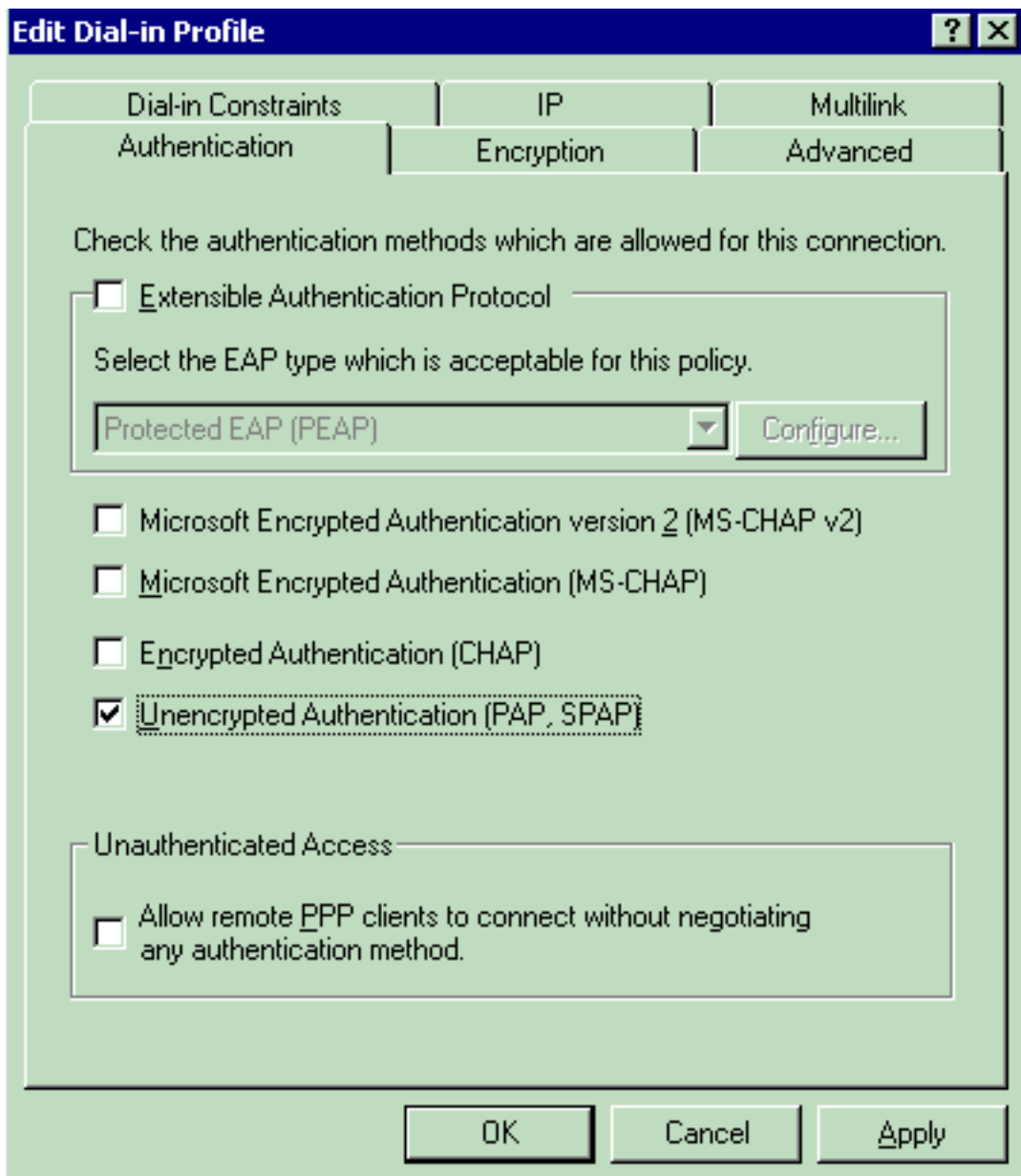
Klik om het gebruikersprofiel te configureren op **Profiel bewerken** in het venster Gebruikersprofiel. Het venster Profiel bewerken



verschijnt.

Klik

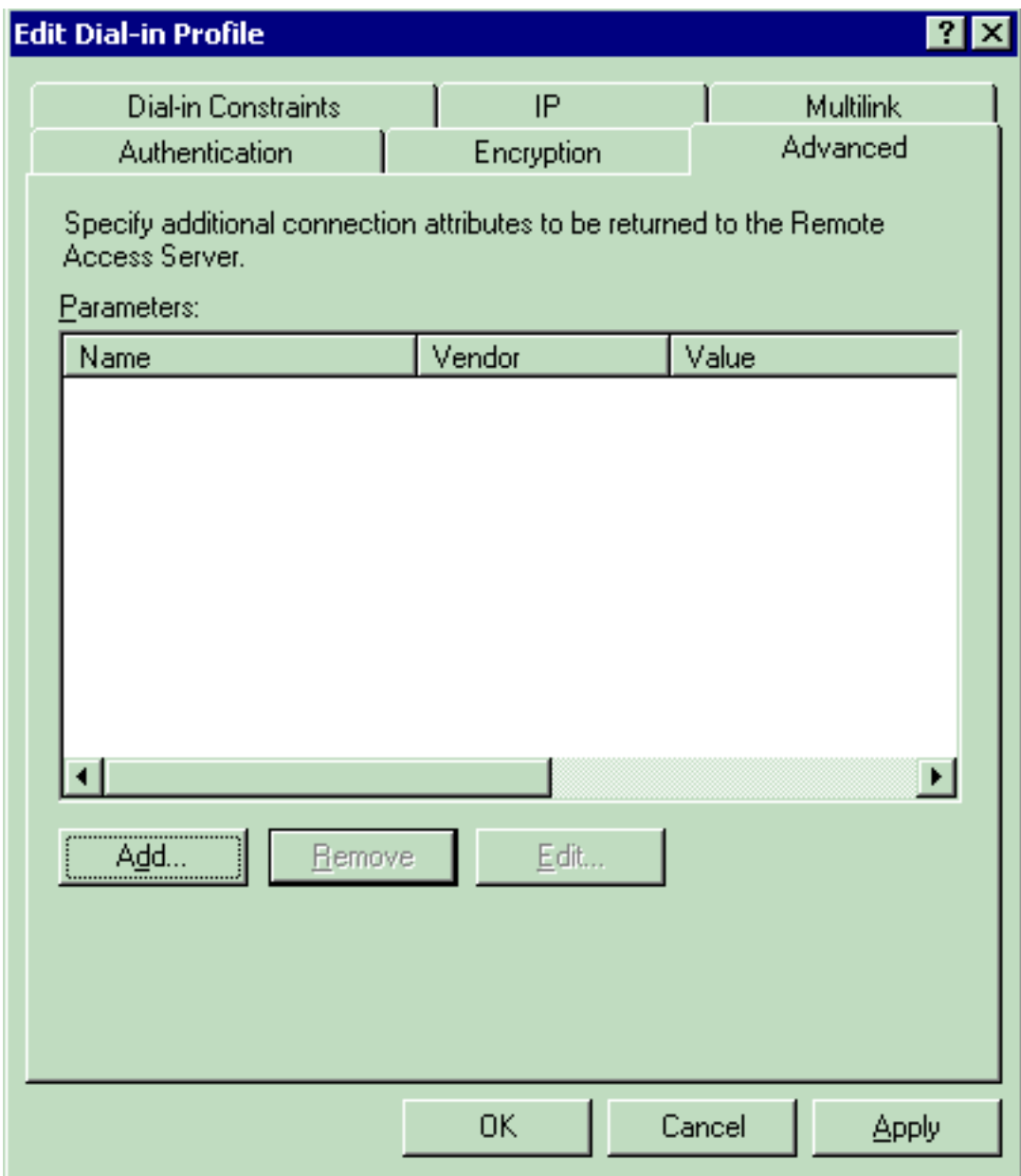
op het tabblad **Verificatie** en kies vervolgens de verificatiemethode die in WLAN wordt gebruikt. Dit voorbeeld gebruikt Unencryptie Verificatie (PAP,



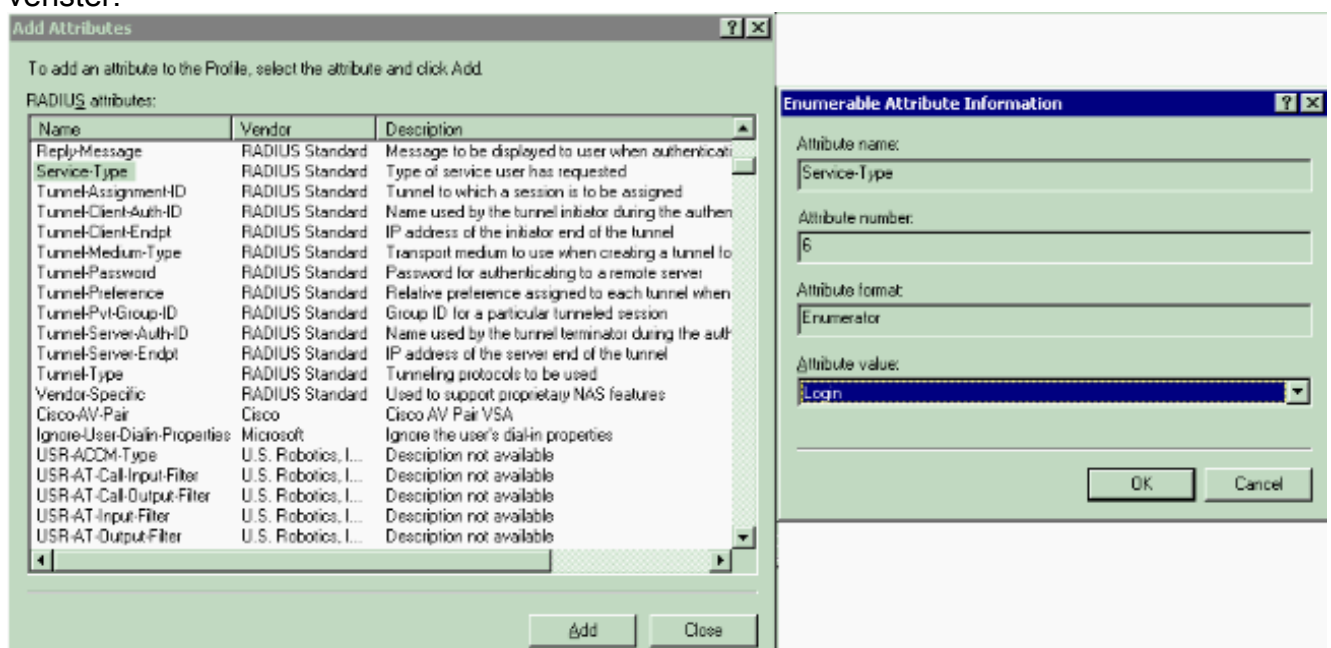
SPAP).

het tabblad **Geavanceerd**. Verwijder alle standaardparameters en klik op

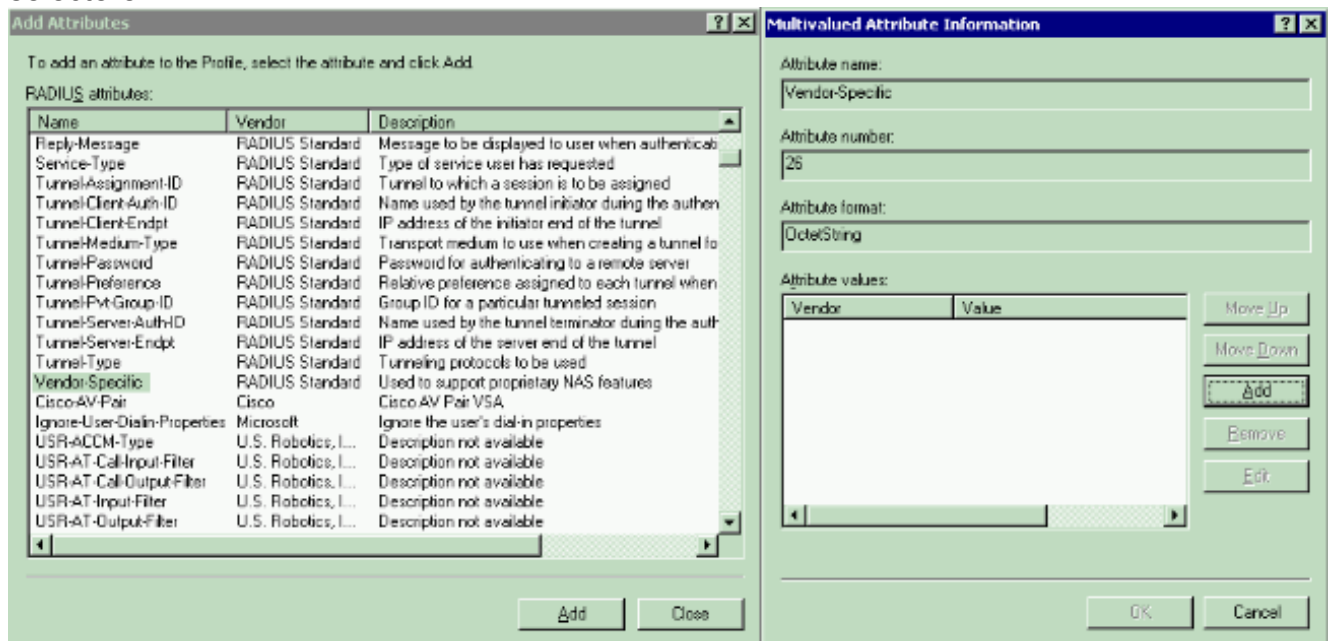
Klik op



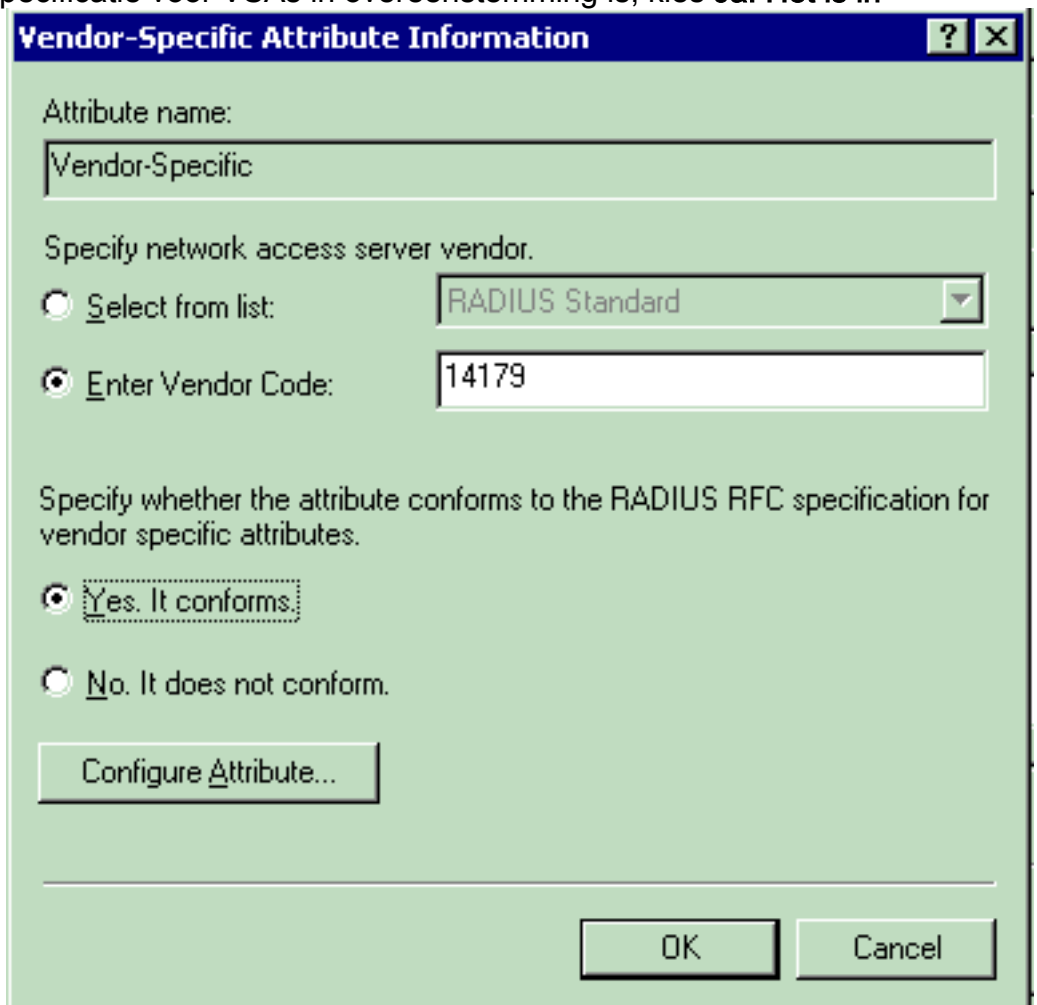
Toevoegen. Selecteer in het venster **Add Attributes** de optie **Service-Type** en kies vervolgens de Login-waarde uit het volgende venster.



Vervolgens moet u de **leverancierspecifieke** eigenschap van de RADIUS-lijst selecteren.



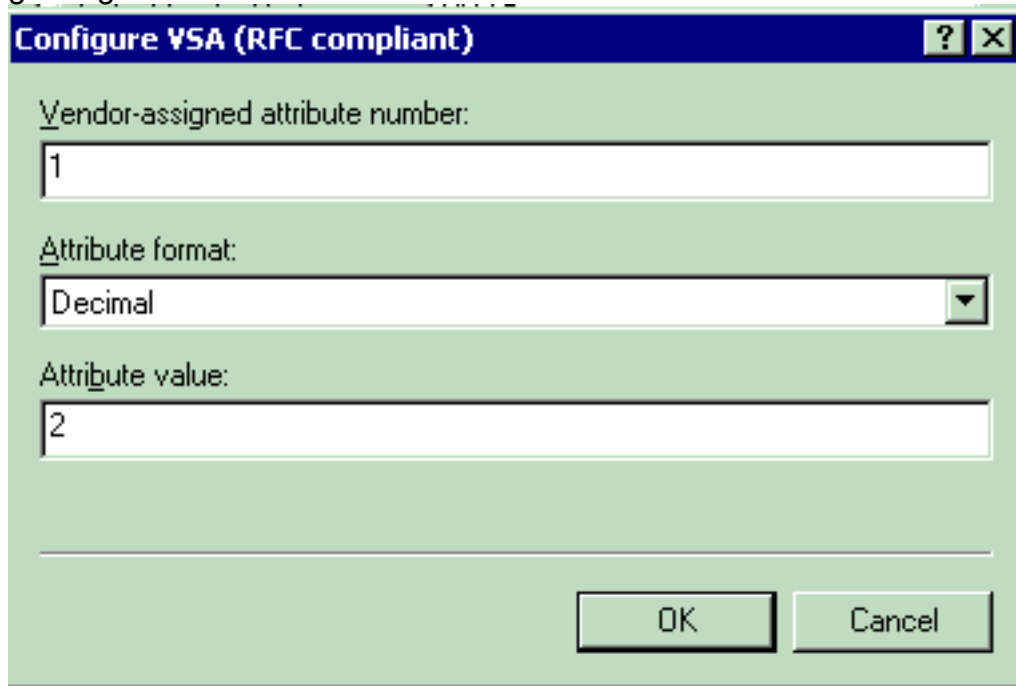
Klik in het volgende venster op **Add** om een nieuwe VSA te selecteren. Het venster Informatie over leverancierspecifieke kenmerken verschijnt. Selecteer onder Verkenner van netwerktoegangsserver de optie **Verkopers code invoeren**. Voer de leveranciercode in voor VSA's. De leveranciercode voor Cisco Airesponders is **14179**. Omdat deze eigenschap met de RADIUS RFC specificatie voor VSAs in overeenstemming is, kies **Ja**. Het is in



overeenstemming..

Klik op **Eigenschappen configureren**. Typ in het venster Configure VSA (RFC compatibel) het leveranciersnummer, de notatie en de waarde van Kenmerken, die afhankelijk zijn van de

VSA die u wilt gebruiken. Voor het instellen van de WLAN-ID op een gebruikersbasis: **Naam:** ABBYY-WLAN-id **Toewijzingsnummer van de verkoper - 1** **Opmaak van kenmerken:** geïntegreerd/decimaal **Waarde**—WLAN-id **Voorbeeld 1**



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

Vendor-assigned attribute number:
1

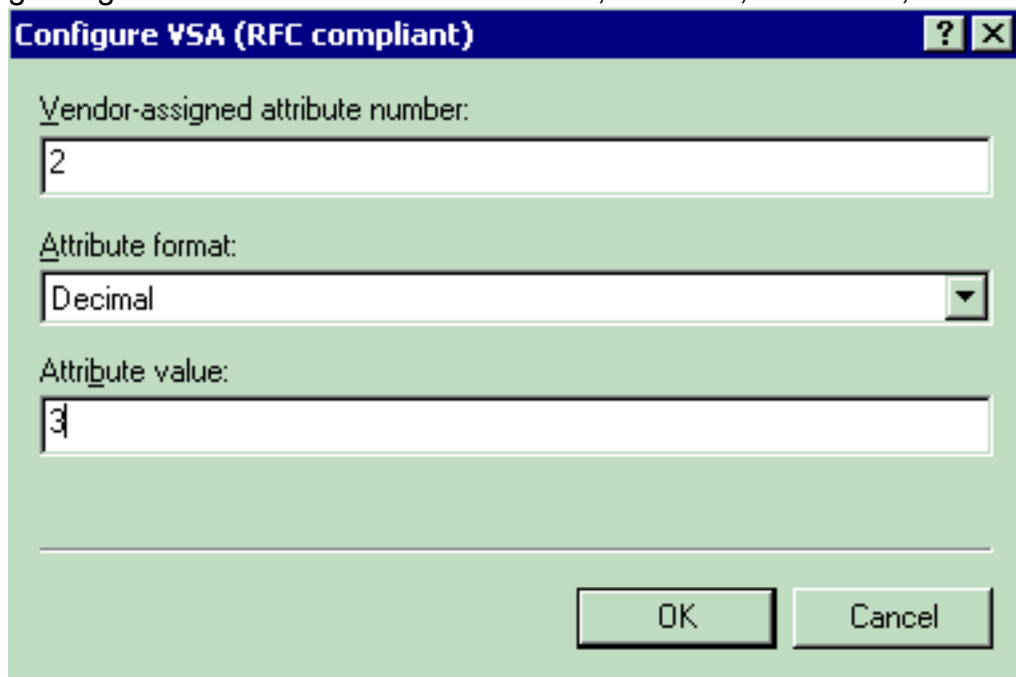
Attribute format:
Decimal

Attribute value:
2

OK Cancel

Voor het instellen

van het QoS-profiel per gebruiker: **Naam:** ABBYY-ABBYY QoS-niveau **Aan de verkoper toegewezen attributennummer** — 2 **Opmaak van kenmerken:** geïntegreerd/decimaal **Waarde**—0 - Silver; 1 - Goud; 2 - Platina; 3 - Bronze **Voorbeeld 2**



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

Vendor-assigned attribute number:
2

Attribute format:
Decimal

Attribute value:
3

OK Cancel

Voor het instellen

van de DSCP-waarde per gebruiker: **Naam van kenmerk**—Airespace-DSCP **Toewijzing van verkoper: 3** **Opmaak van kenmerken:** geïntegreerd/decimaal **Waarde**—DSCP-waarde **Voorbeeld 3**

Configure VSA (RFC compliant) ? X

Vendor-assigned attribute number:
3

Attribute format:
Decimal

Attribute value:
46

OK Cancel

Voor het instellen

van de 802.1p-tag per gebruiker:**Naam van kenmerk:** Airespace-802.1p-Tag
Toewijzingsnummer van de verkoper—4
Opmaak van kenmerken: geïntegreerd/decimaal
Waarde: 802.1p-label
Voorbeeld 4

Configure VSA (RFC compliant) ? X

Vendor-assigned attribute number:
4

Attribute format:
Decimal

Attribute value:
5

OK Cancel

Voor het instellen

van de interface (VLAN) per gebruiker:**Naam:**interface-interface-naam van
kenmerkEigendomsnummer van de verkoper—5
Opmaak-string van kenmerken
Waarde—interface-naam
Voorbeeld 5

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

Vendor-assigned attribute number:

Attribute format:

Attribute value:

[OK] [Cancel]

Om ACL op een per-gebruiker-basis in te stellen: **Naam van kenmerk**—Airespace-ACL-naam **Toewijzingsnummer van de verkoper**—6 **Opmaak-string van kenmerken** **Waarde**—ACL-naam **Voorbeeld 6**

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

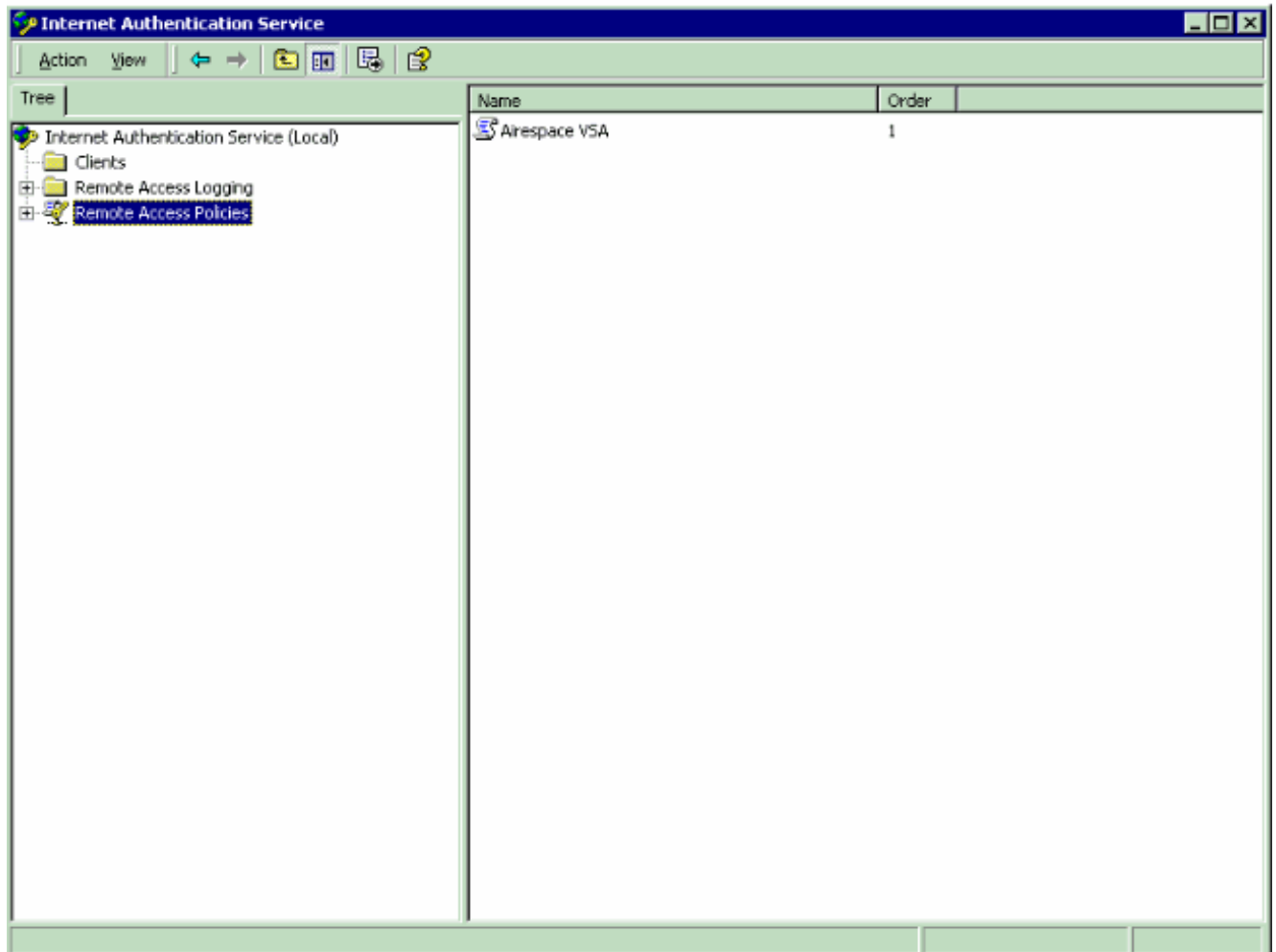
Vendor-assigned attribute number:

Attribute format:

Attribute value:

[OK] [Cancel]

8. Nadat u de VSA's hebt ingesteld, klikt u op **OK** totdat u het venster Gebruikersprofiel ziet.
9. Klik vervolgens op **Voltooien** om de configuratie te voltooien. U kunt het nieuwe beleid zien onder het beleid voor toegang op afstand.



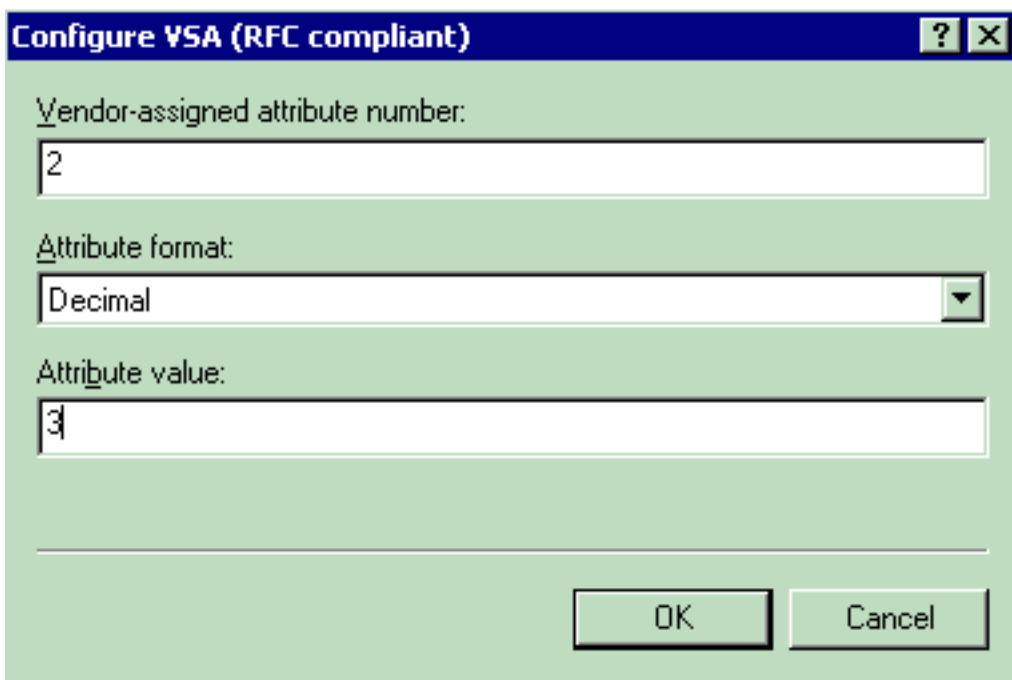
Configuratievoorbeeld

In dit voorbeeld wordt een WLAN geconfigureerd voor web-verificatie. Gebruikers worden geauthentiseerd door de IAS RADIUS-server en de RADIUS-server is ingesteld om het QoS-beleid per gebruiker toe te wijzen.

The screenshot displays the Cisco Systems configuration interface for a WLAN. The main configuration area is titled 'WLAN ID 1' and 'WLAN SSID SSID-WLC2'. Under 'General Policies', several settings are visible: 'Radio Policy' is set to 'All', 'Admin Status' is 'Enabled', 'Session Timeout (secs)' is '0', 'Quality of Service (QoS)' is 'Silver (best effort)', 'WMM Policy' is 'Disabled', '7920 Phone Support' includes 'Client CAC Limit' and 'AP CAC Limit', 'Broadcast SSID' is 'Enabled', 'Aironet IE' is 'Enabled', 'Allow AAA Override' is 'Enabled', 'Client Exclusion' is 'Enabled' with a '60' second timeout, 'DHCP Server' is 'Override', 'DHCP Addr. Assignment' is 'Required', 'Interface Name' is 'internal', 'MFP Version Required' is '1', 'MFP Signature Generation' is '(Global MFP Disabled)', and 'H-REAP Local Switching' is 'Disabled'. The 'Security Policies' section shows 'Layer 2 Security' as 'None', 'Layer 3 Security' as 'None', 'Web Policy' as 'Enabled', 'Authentication' as selected, 'Passthrough' as unselected, and 'Preauthentication ACL' as 'none'. The 'Radius Servers' section shows 'Server 1' with 'Authentication Servers' set to 'IP:172.16.1.1, Port:1812' and 'Accounting Servers' set to 'none'. Red circles highlight the 'Quality of Service (QoS)', 'Allow AAA Override', and 'Radius Servers' sections.

Zoals u vanuit dit venster kunt zien, is Web Authenticatie ingeschakeld, is de authenticatieserver 172.16.1.1 en AAA Override is ook ingeschakeld op het WLAN. De standaard QoS-instelling voor dit WLAN wordt ingesteld op Silver.

Op de IAS RADIUS-server is een beleid voor externe toegang ingesteld dat de QoS-eigenschap Bronze in de RADIUS-modus accepteert. Dit gebeurt wanneer u de VSA die specifiek is voor de QoS eigenschap configureren.



Zie het [Configureren van het beleid voor externe toegang in de IAS](#)-sectie van dit document voor gedetailleerde informatie over de manier waarop u een Afstandstoegangsbeleid op de IAS-server kunt configureren.

Zodra de IAS-server, de WLC en de LAP voor deze instelling zijn geconfigureerd, kunnen de draadloze klanten gebruik maken van web-authenticatie om verbinding te maken.

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Wanneer de gebruiker zich met een gebruikersid en een wachtwoord op WLAN aansluit, geeft de WLC de referenties door aan de IAS RADIUS-server die de gebruiker authenticceert aan de hand van de voorwaarden en het gebruikersprofiel die in het afstandstoegangsbeleid zijn ingesteld. Als de gebruikersverificatie succesvol is, retourneert de RADIUS-server een RADIUS accepteert een aanvraag die ook de AAA-omzeilingswaarden bevat. In dit geval wordt het QoS-beleid van de gebruiker geretourneerd.

U kunt **debug a** uitvoeren **allen toelaat** opdracht om de opeenvolging van gebeurtenissen te zien die tijdens authenticatie plaatsvindt. Hier wordt een voorbeelduitvoer weergegeven:

```
(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-Identifler.....
```

```

                                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
                                ...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)

Zoals u aan de uitvoer kunt zien, is de gebruiker echt gemaakt. Vervolgens worden AAA-overwinningswaarden teruggegeven met het RADIUS-bericht. In dit geval krijgt de gebruiker het QoS-beleid van Bronze.

U kunt dit ook controleren op de WLC GUI. Hierna volgt een voorbeeld:

The screenshot shows the Cisco Systems web interface for monitoring wireless clients. The main content area is titled 'Clients > Detail' and contains several sections:

- Client Properties:**

MAC Address	00:40:96:ac:e6:57
IP Address	20.0.0.1
User Name	User-VLAN10
Port Number	1
Interface	internal
VLAN ID	20
CCX Version	CCXv3
E2E Version	Not Supported
Mobility Role	Local
Mobility Peer IP Address	N/A
Policy Manager State	RUN
- AP Properties:**

AP Address	00:0b:85:5b:fb:d0
AP Name	ap:5b:fb:d0
AP Type	802.11a
WLAN SSID	SSID-WLC2
Status	Associated
Association ID	1
802.11 Authentication	Open System
Reason Code	0
Status Code	0
CF Pollable	Not Implemented
CF Poll Request	Not Implemented
Short Preamble	Not Implemented
PBCC	Not Implemented
Channel Agility	Not Implemented
Timeout	0
WEP State	WEP Disable
- Security Information:**

Security Policy Completed	Yes
Policy Type	N/A
Encryption Cipher	None
EAP Type	N/A
- Quality of Service Properties:**

WMM State	Disabled
QoS Level	Bronze
Diff Serv Code Point (DSCP)	disabled
802.1p Tag	disabled
Average Data Rate	disabled

Opmerking: het standaard QoS-profiel van deze SSID is Silver. Omdat AAA-Override echter is geselecteerd en de gebruiker is ingesteld met een QoS-profiel van Bronze op de IAS-server, wordt het standaard QoS-profiel overschreven.

Problemen oplossen

U kunt het **debug**-venster gebruiken en het **allen inschakelen** van de WLC om de configuratie problemen op te lossen. Een voorbeeld van de uitvoer van dit debug in een werknetswerk wordt weergegeven in het gedeelte [Verifiëren](#) van dit document.

Opmerking: Raadpleeg [Belangrijke informatie over debug Commands](#) voordat u **debug**-opdrachten gebruikt.

Gerelateerde informatie

- [Configuratie-gids voor Cisco draadloze LAN-controllers, release 4.0](#)
- [WLAN-toegang beperken op basis van SSID met WLC en Cisco Secure ACS-configuratievoorbeeld](#)
- [Ondersteuning voor wireless producten](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)