

Konfigurationsbeispiel für Cisco Airespace VSAs in Microsoft IAS Radius Server

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Hintergrundinformationen](#)

[Konfigurieren des IAS für Airespace VSAs](#)

[Konfigurieren des WLC als AAA-Client im IAS](#)

[Konfigurieren der Remote-Zugriffsrichtlinie auf dem IAS](#)

[Beispielkonfiguration](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird die Konfiguration eines Microsoft Internet Authentication Service (IAS)-Servers zur Unterstützung der VSAs (Vendor Specific Attributes) von Cisco beschrieben. Der Vendor-Code für Cisco Airespace VSAs lautet **14179**.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Kenntnisse der Konfiguration eines IAS-Servers
- Kenntnis der Konfiguration von Lightweight Access Points (LAPs) und Cisco Wireless LAN Controllern (WLCs)
- Kenntnisse der Cisco Unified Wireless Security-Lösungen

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Microsoft Windows 2000 Server mit IAS
- Cisco 4400 WLC mit Softwareversion 4.0.206.0
- LAPs der Cisco Serie 1000
- 802.11a/b/g Wireless Client-Adapter mit Firmware 2.5
- Aironet Desktop Utility (ADU) Version 2.5

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Hinweis: Dieses Dokument soll dem Leser ein Beispiel für die Konfiguration geben, die auf dem IAS-Server zur Unterstützung von Cisco Application VSAs erforderlich ist. Die in diesem Dokument vorgestellte IAS-Serverkonfiguration wurde im Labor getestet und funktioniert wie erwartet. Wenn Sie Probleme beim Konfigurieren des IAS-Servers haben, wenden Sie sich an Microsoft, um Hilfe zu erhalten. Das Cisco TAC unterstützt die Microsoft Windows-Serverkonfiguration nicht.

In diesem Dokument wird davon ausgegangen, dass der WLC für den Basisbetrieb konfiguriert ist und dass die LAPs beim WLC registriert sind. Wenn Sie ein neuer Benutzer sind und versuchen, den WLC für den Basisbetrieb mit LAPs einzurichten, lesen Sie die Informationen zur [LAP-Registrierung \(Lightweight AP\) an einen Wireless LAN Controller \(WLC\)](#).

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter [Cisco Technical Tips Conventions \(Technische Tipps von Cisco zu Konventionen\)](#).

Hintergrundinformationen

In den meisten WLAN-Systemen (WLAN) verfügt jedes WLAN über eine statische Richtlinie, die auf alle Clients angewendet wird, die einem Service Set Identifier (SSID) zugeordnet sind. Diese Methode ist zwar leistungsstark, bietet jedoch Einschränkungen, da Clients verschiedene SSIDs verknüpfen müssen, um unterschiedliche QoS- und Sicherheitsrichtlinien zu erben.

Die Cisco Wireless LAN-Lösung unterstützt jedoch Identitätsnetzwerke, die es dem Netzwerk ermöglichen, eine einzelne SSID und bestimmte Benutzer anzukündigen, um je nach ihren Benutzerprofilen unterschiedliche QoS- oder Sicherheitsrichtlinien zu erben. Die spezifischen Richtlinien, die Sie mithilfe von Identitätsnetzwerken steuern können, sind:

- **Quality of Service** - Wenn der QoS-Level-Wert in einem RADIUS Access Accept vorhanden ist, überschreibt er den im WLAN-Profil angegebenen QoS-Wert.
- **ACL** - Wenn das Attribut "Access Control List" (Zugriffssteuerungsliste) im RADIUS Access Accept (RADIUS-Zugriffsakzept) vorhanden ist, wendet das System den ACL-Namen nach der Authentifizierung auf die Client-Station an. Dadurch werden alle der Schnittstelle zugewiesenen ACLs außer Kraft gesetzt.
- **VLAN**: Wenn ein VLAN-Schnittstellename oder ein VLAN-Tag in einem RADIUS Access Accept vorhanden ist, platziert das System den Client auf einer bestimmten Schnittstelle.
- **WLAN-ID**: Wenn das WLAN-ID-Attribut im RADIUS Access Accept vorhanden ist, wendet das System die WLAN-ID (SSID) nach der Authentifizierung auf die Client-Station an. Die WLAN-

ID wird vom WLC in allen Authentifizierungsinstanzen außer IPSec gesendet. Wenn der WLC bei der Webauthentifizierung ein WLAN-ID-Attribut in der Authentifizierungsantwort des AAA-Servers erhält und es nicht mit der ID des WLAN übereinstimmt, wird die Authentifizierung abgelehnt. Andere Sicherheitsmethoden tun dies nicht.

- **DSCP Value (DSCP-Wert):** Wenn der Wert in einem RADIUS Access Accept vorhanden ist, überschreibt der DSCP-Wert den im WLAN-Profil angegebenen DSCP-Wert.
- **802.1p-Tag:** Wenn der 802.1p-Wert in einem RADIUS Access Accept vorhanden ist, wird er über den im WLAN-Profil angegebenen Standardwert gesetzt.

Hinweis: Die VLAN-Funktion unterstützt nur MAC-Filterung, 802.1X und Wi-Fi Protected Access (WPA). Die VLAN-Funktion unterstützt keine Webauthentifizierung oder IPSec. Die lokale MAC-Filter-Datenbank des Betriebssystems wurde um den Schnittstellennamen erweitert. Auf diese Weise können lokale MAC-Filter festlegen, welche Schnittstelle dem Client zugewiesen werden soll. Ein separater RADIUS-Server kann ebenfalls verwendet werden, der RADIUS-Server muss jedoch mithilfe der Sicherheitsmenüs definiert werden.

Weitere Informationen zu Identitätsnetzwerken finden Sie unter [Konfigurieren von Identitätsnetzwerken](#).

[Konfigurieren des IAS für Airespace VSAs](#)

Um den IAS für Airespace VSAs zu konfigurieren, müssen Sie die folgenden Schritte ausführen:

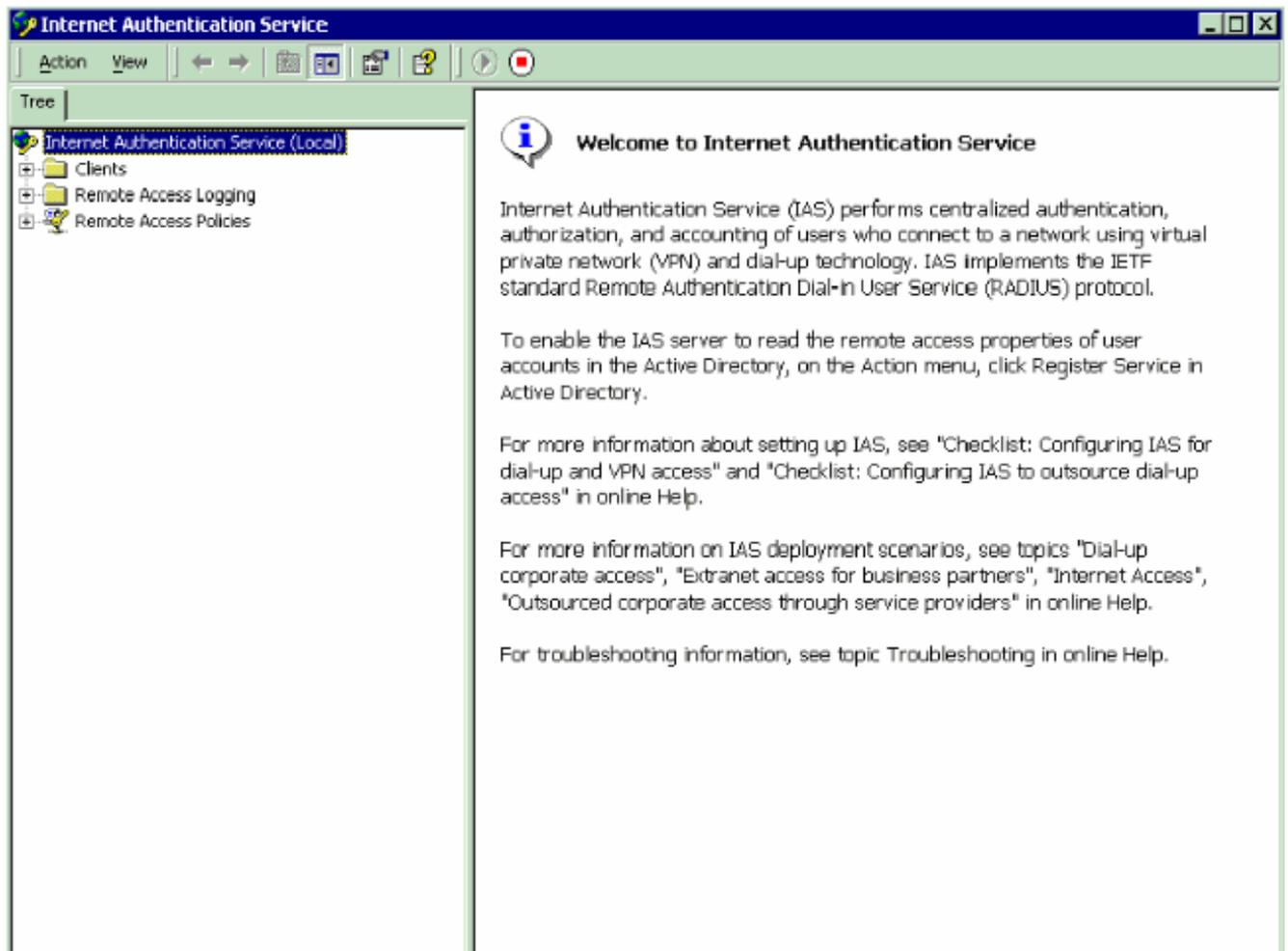
1. [Konfigurieren des WLC als AAA-Client im IAS](#)
2. [Konfigurieren der Remote-Zugriffsrichtlinie auf dem IAS](#)

Hinweis: Die VSAs werden unter "Remote Access Policy" (Remote-Zugriffsrichtlinie) konfiguriert.

[Konfigurieren des WLC als AAA-Client im IAS](#)

Gehen Sie wie folgt vor, um den WLC als AAA-Client im IAS zu konfigurieren:

1. Klicken Sie auf **Programme > Verwaltung > Internet Authentication Service**, um IAS auf dem Microsoft 2000-Server zu starten.



2. Klicken Sie mit der rechten Maustaste auf den Ordner **Clients**, und wählen Sie **Neuer Client** aus, um einen neuen RADIUS-Client hinzuzufügen.
3. Geben Sie im Fenster Add Client (Client hinzufügen) den Namen des Clients ein, und wählen Sie **RADIUS** als Protokoll aus. Klicken Sie anschließend auf **Weiter**. In diesem Beispiel lautet der Client-Name *WLC-1*. **Hinweis:** Standardmäßig ist das Protokoll auf RADIUS festgelegt.

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. Geben Sie im Fenster Add RADIUS Client (RADIUS-Client hinzufügen) die **Client-IP-Adresse**, die **Client-Vendor-Adresse** und den **geheimen Schlüssel ein**. Nachdem Sie die Client-Informationen eingegeben haben, klicken Sie auf **Fertig stellen**. Dieses Beispiel zeigt einen Client mit dem Namen *WLC-1* und der IP-Adresse *172.16.1.30*, der Client-Anbieter ist auf *Cisco* und der Shared geheime Client *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]

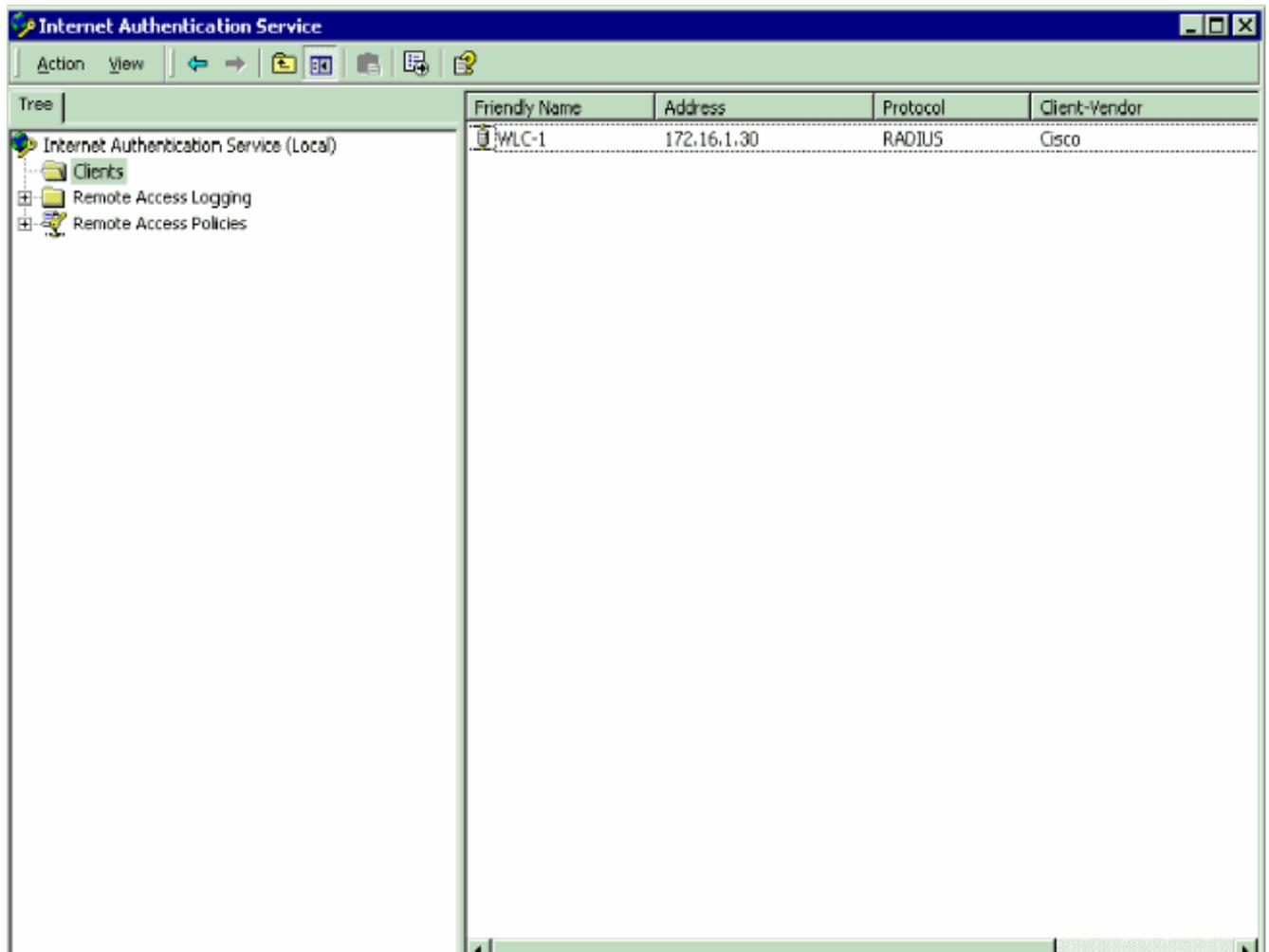
Client must always send the signature attribute in the request

Shared secret: [xxxxxxx]

Confirm shared secret: [xxxxxxx]

< Back Finish Cancel

Mit diesen Informationen wird der WLC mit dem Namen WLC-1 als AAA-Client des IAS-Servers hinzugefügt.

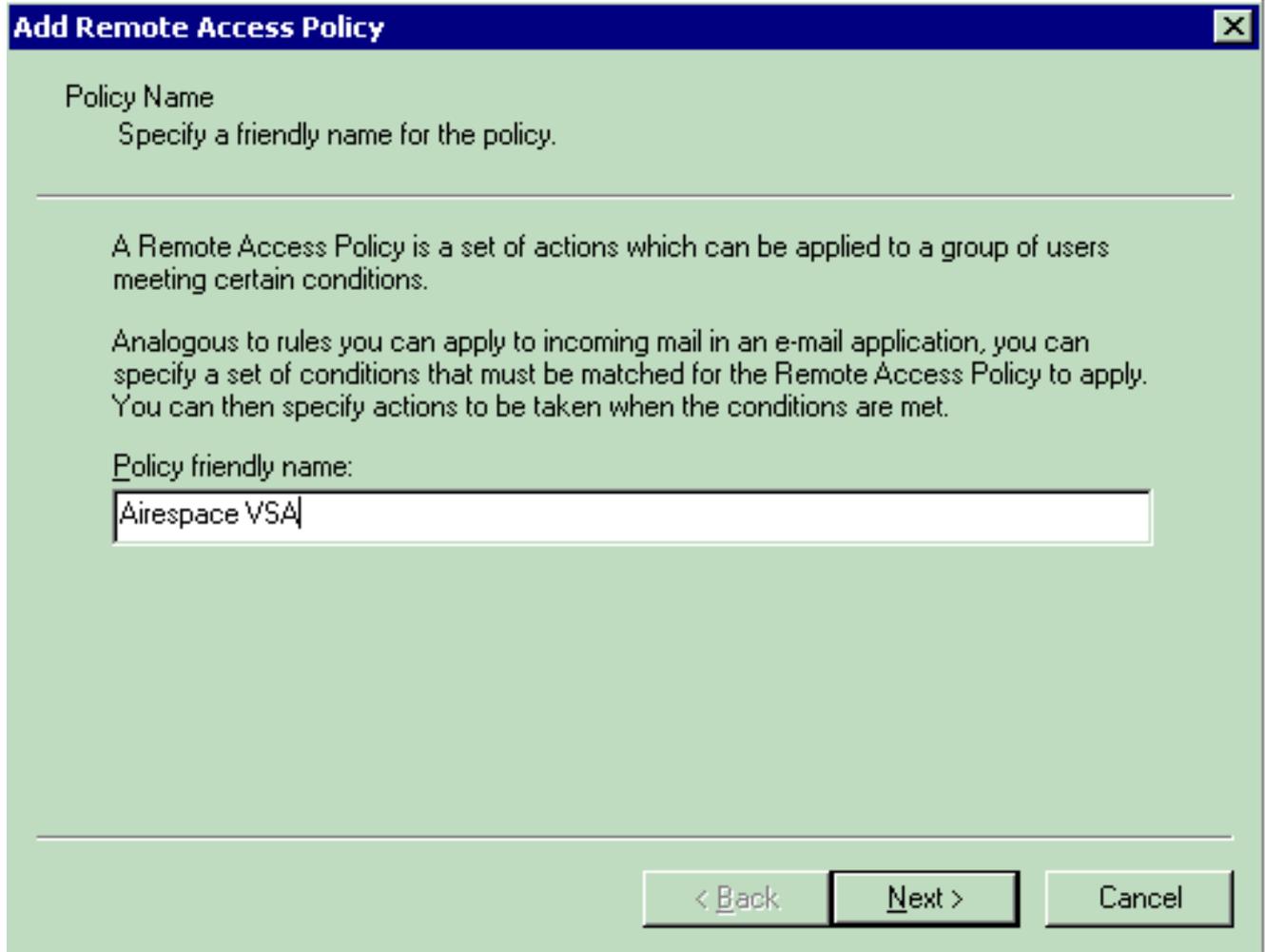


Im nächsten Schritt wird eine Remote-Zugriffsrichtlinie erstellt und die VSAs konfiguriert.

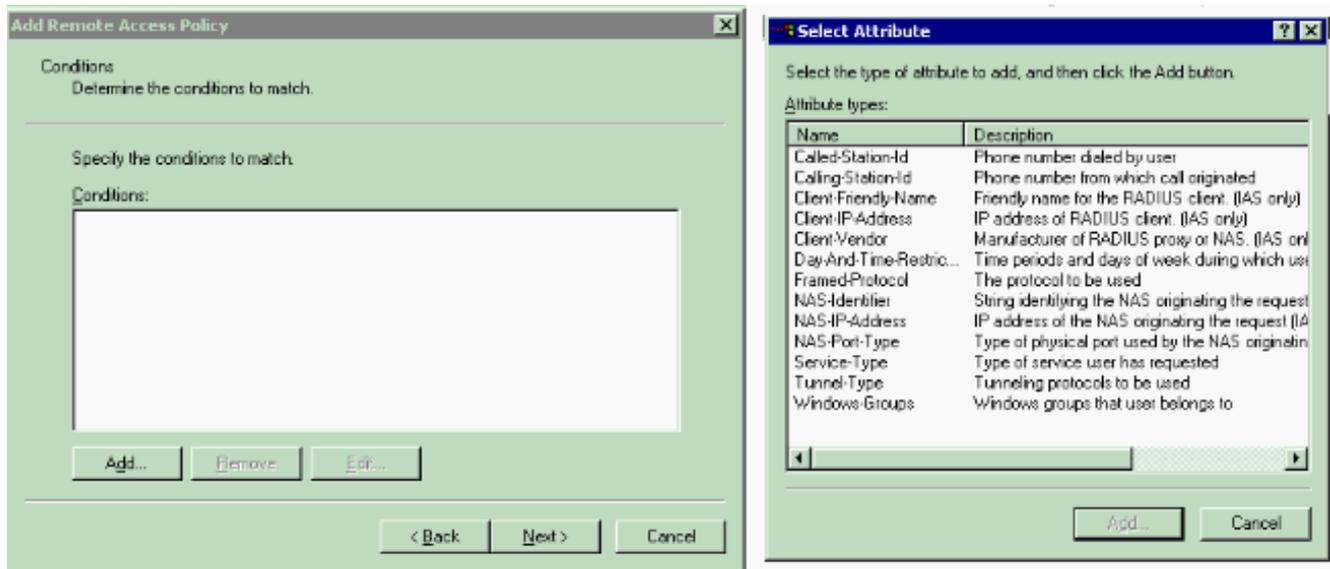
[Konfigurieren der Remote-Zugriffsrichtlinie auf dem IAS](#)

Gehen Sie wie folgt vor, um eine neue Remote Access Policy für den IAS zu konfigurieren:

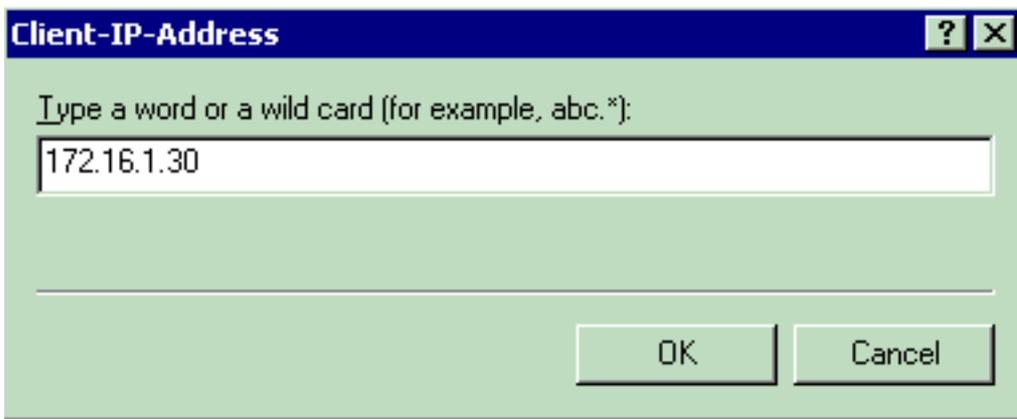
1. Klicken Sie mit der rechten Maustaste auf **Remote Access Policies (Remote-Zugriffsrichtlinien)**, und wählen Sie **New Remote AccessMS Policy (Neue Remote-Zugriffsrichtlinien)** aus. Das Fenster Policy Name (Richtliniename) wird angezeigt.
2. Geben Sie den Namen der Richtlinie ein, und klicken Sie auf **Weiter**.



3. Wählen Sie im nächsten Fenster die Bedingungen aus, für die die Remote-Zugriffsrichtlinie gilt. Klicken Sie auf **Hinzufügen**, um die Bedingungen auszuwählen.



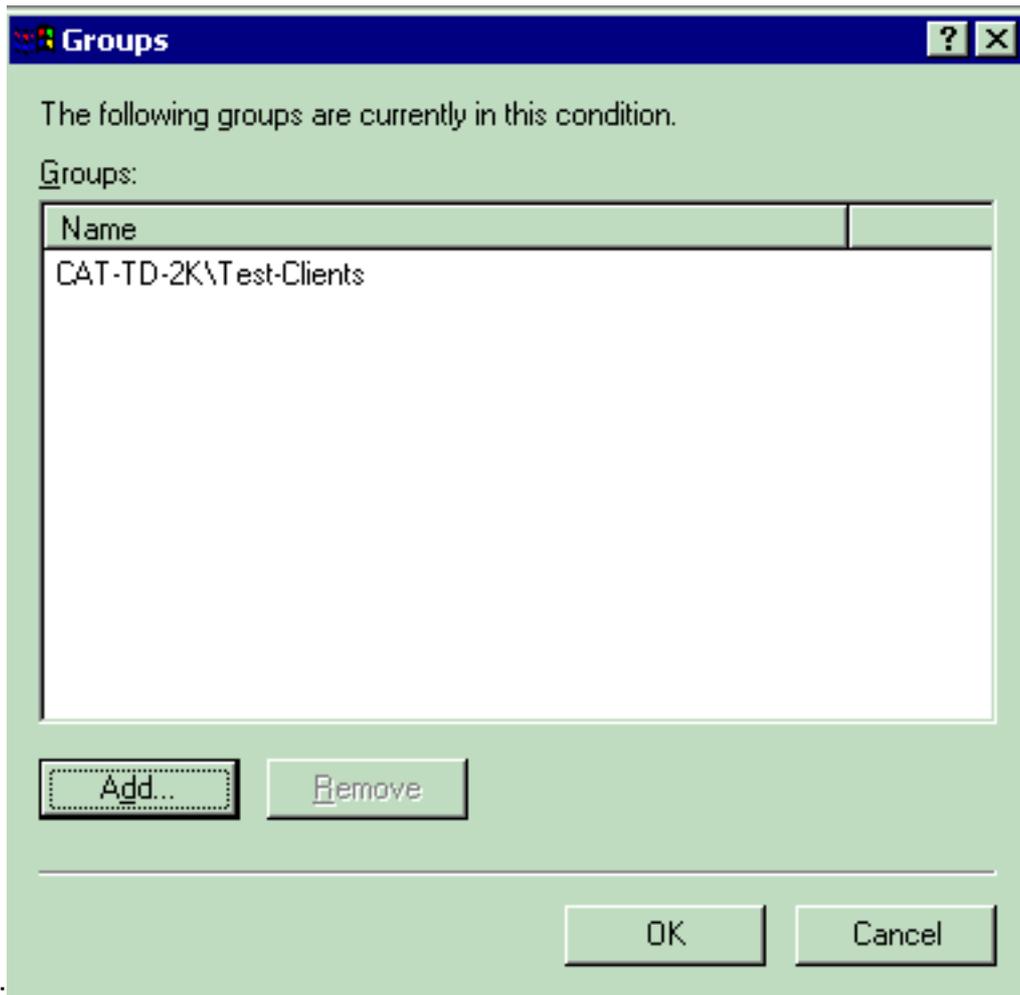
4. Wählen Sie im Menü Attributtypen die folgenden Attribute aus: **Client-IP-Adresse** - Geben Sie die IP-Adresse des AAA-Clients ein. In diesem Beispiel wird die IP-Adresse der WLCs eingegeben, sodass die Richtlinie für Pakete vom WLC



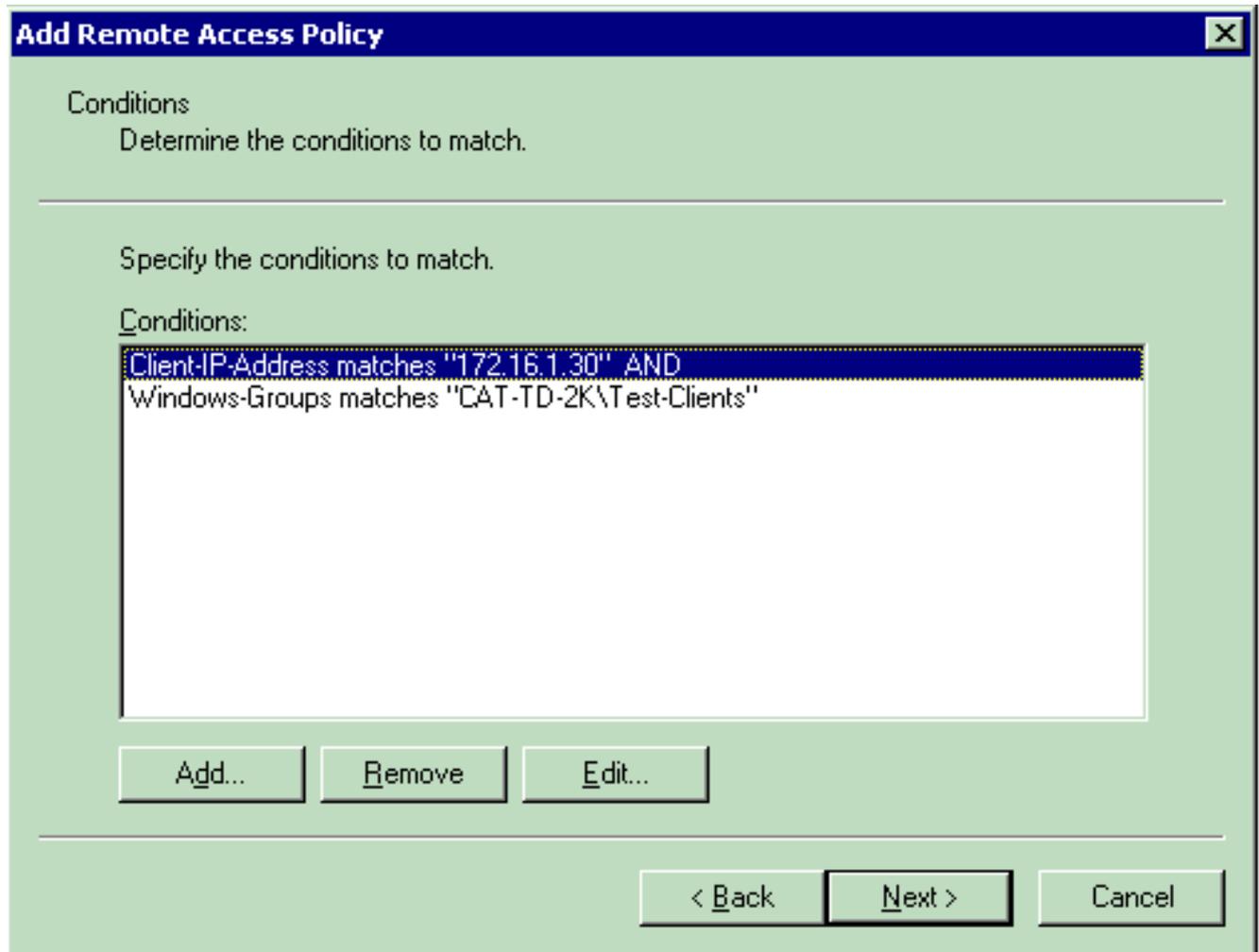
gilt.

Windows

Groups: Wählen Sie die Windows-Gruppe (die Benutzergruppe) aus, für die die Richtlinie gilt. Hier ein

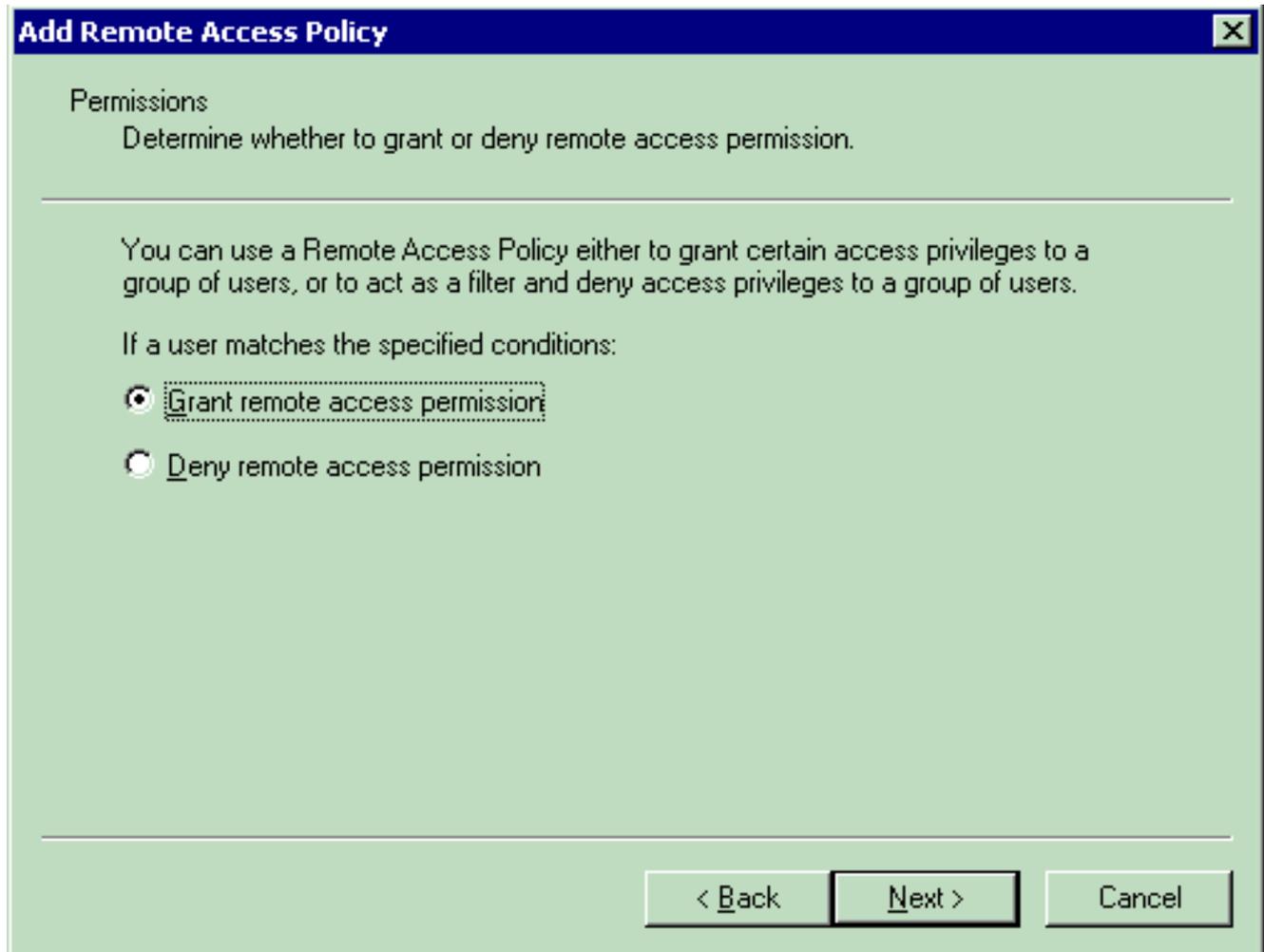


Beispiel:



Dieses Beispiel zeigt nur zwei Bedingungen. Wenn es weitere Bedingungen gibt, fügen Sie auch diese Bedingungen hinzu, und klicken Sie auf **Weiter**. Das Fenster Berechtigungen wird angezeigt.

5. Wählen Sie im Fenster "Berechtigungen" die Option **Remotezugriffsberechtigung erteilen aus**. Nachdem Sie diese Option ausgewählt haben, erhält der Benutzer Zugriff, sofern der Benutzer die angegebenen Bedingungen erfüllt (aus Schritt 2).



6. Klicken Sie auf **Weiter**.

7. Im nächsten Schritt wird das Benutzerprofil eingerichtet. Obwohl Sie angegeben haben, dass Benutzern aufgrund der Bedingungen der Zugriff verweigert oder gewährt werden soll, kann das Profil trotzdem verwendet werden, wenn die Bedingungen dieser Richtlinie pro Benutzer überschrieben werden.

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.

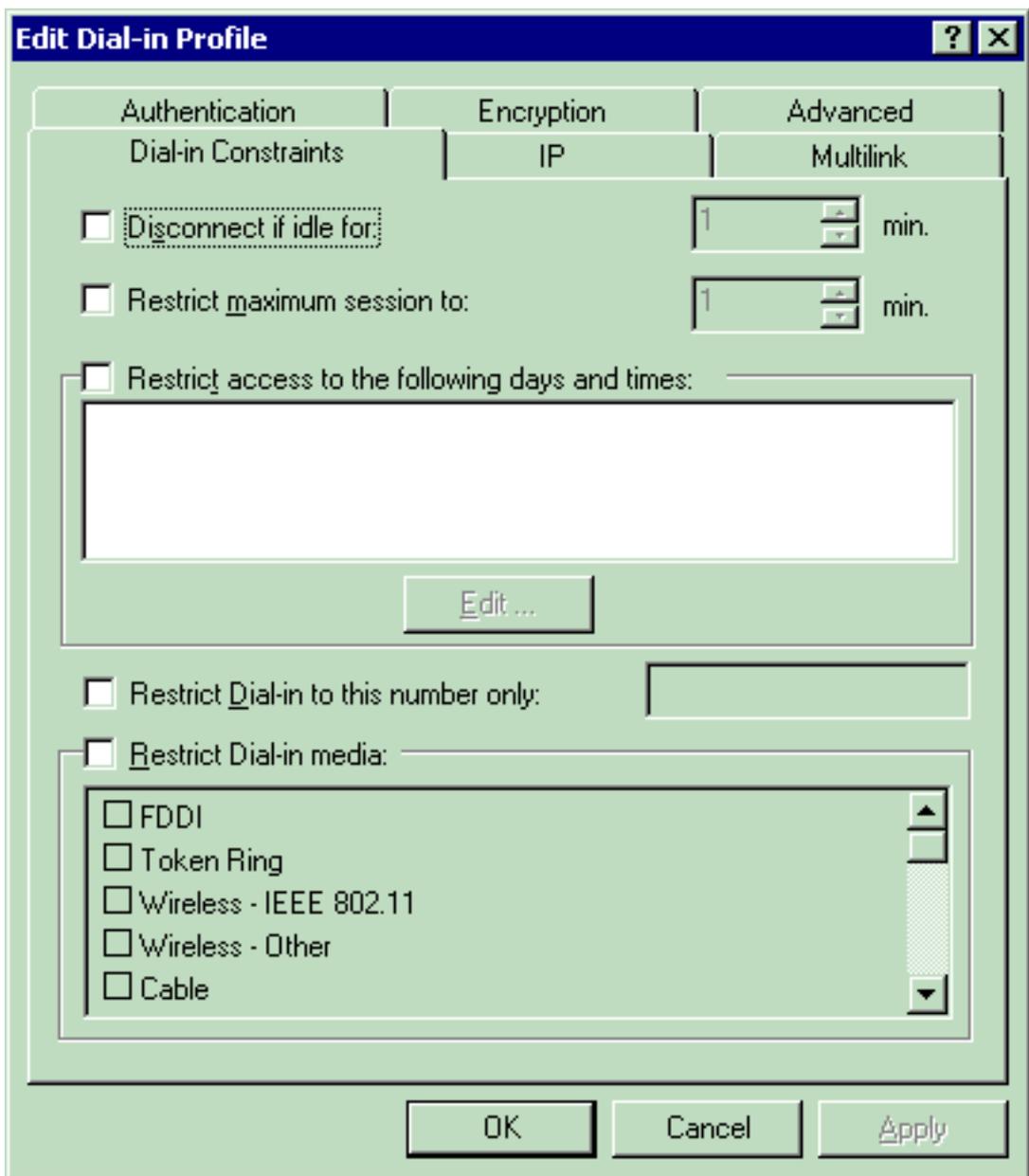
Edit Profile...

< Back

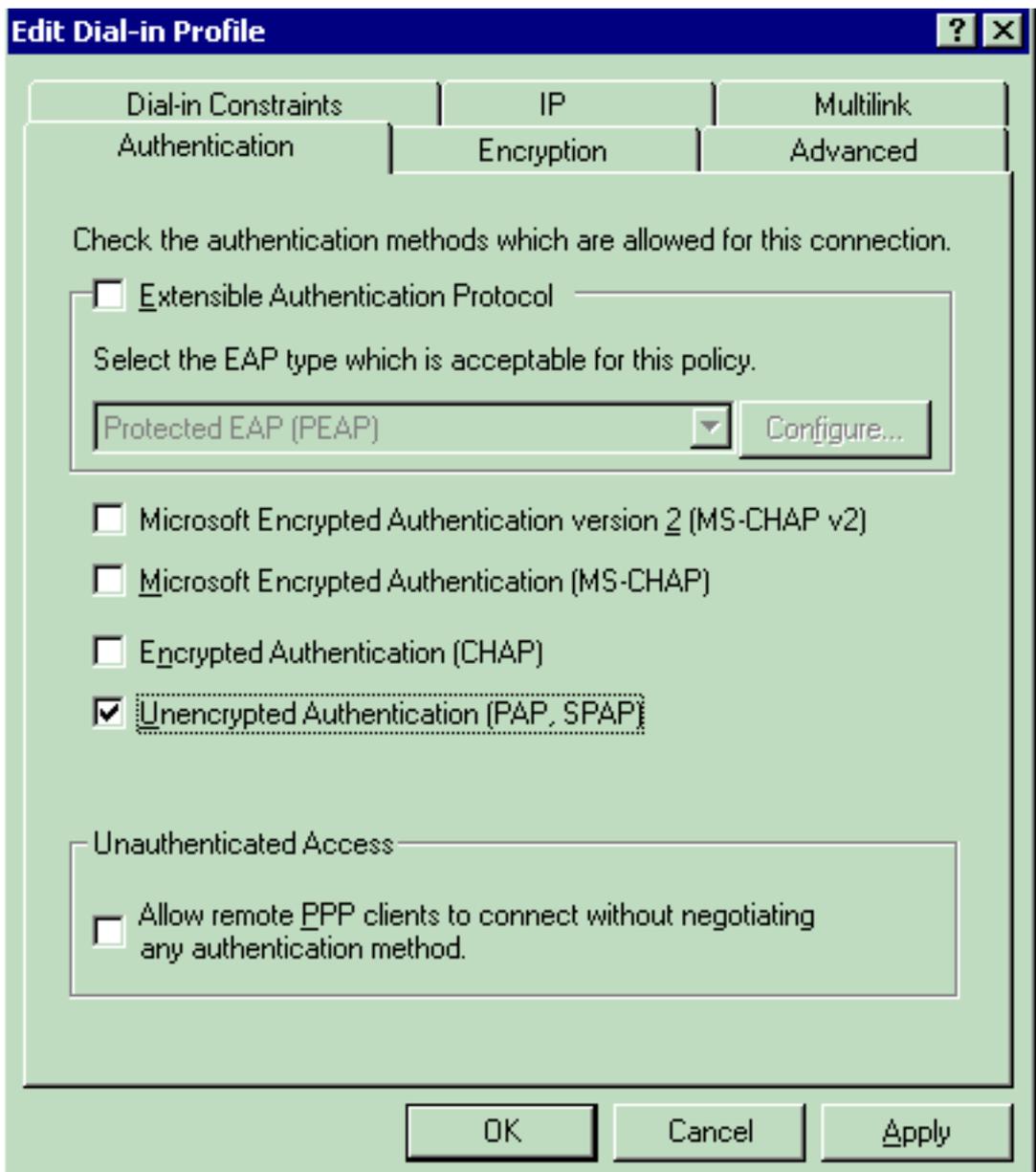
Finish

Cancel

Um das Benutzerprofil zu konfigurieren, klicken Sie im Fenster Benutzerprofil auf **Profil bearbeiten**. Das Fenster "Profil für die Einwahl bearbeiten" wird

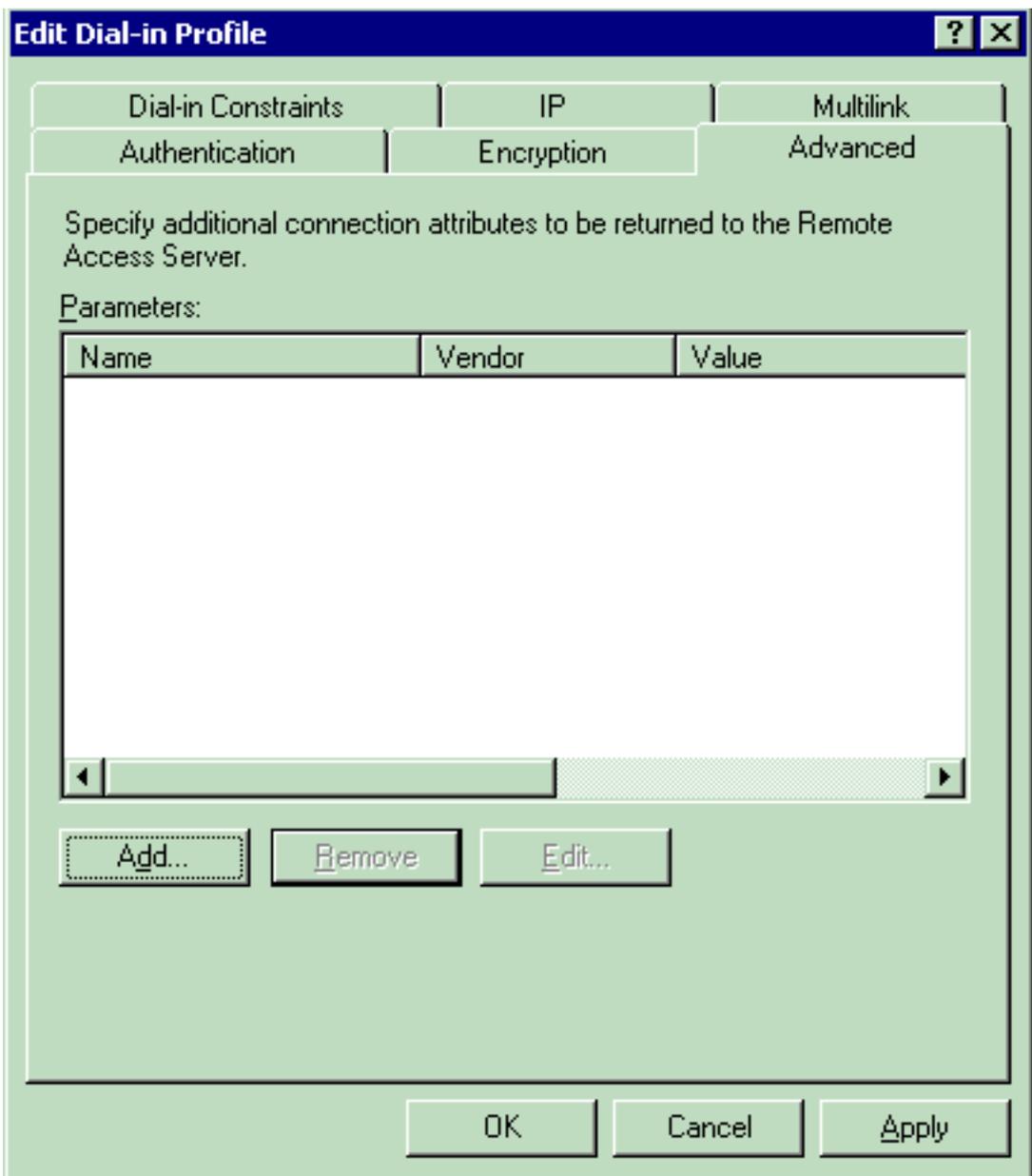


angezeigt. Klicken Sie auf die Registerkarte **Authentifizierung**, und wählen Sie die im WLAN verwendete Authentifizierungsmethode aus. In diesem Beispiel wird die unverschlüsselte Authentifizierung (PAP, SPAP) angezeigt. Klicken Sie auf die Registerkarte **Authentifizierung**, und wählen Sie die im WLAN verwendete Authentifizierungsmethode aus. In diesem Beispiel wird die unverschlüsselte Authentifizierung (PAP, SPAP) angezeigt.

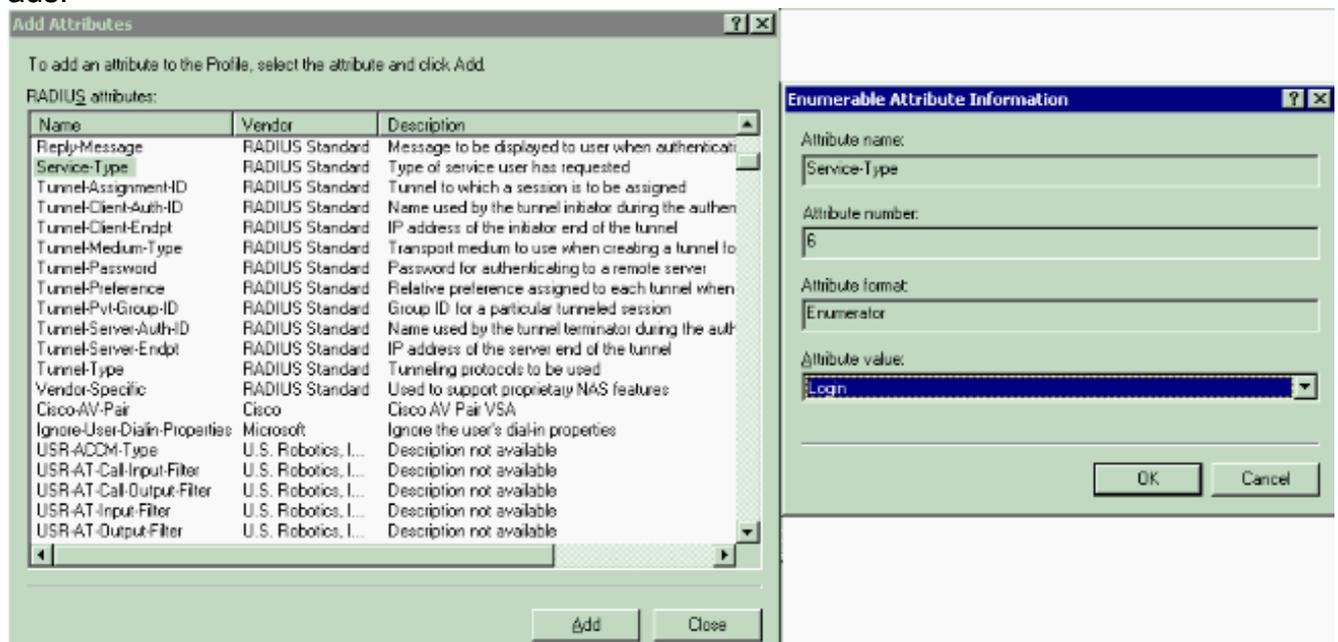


verwendet.

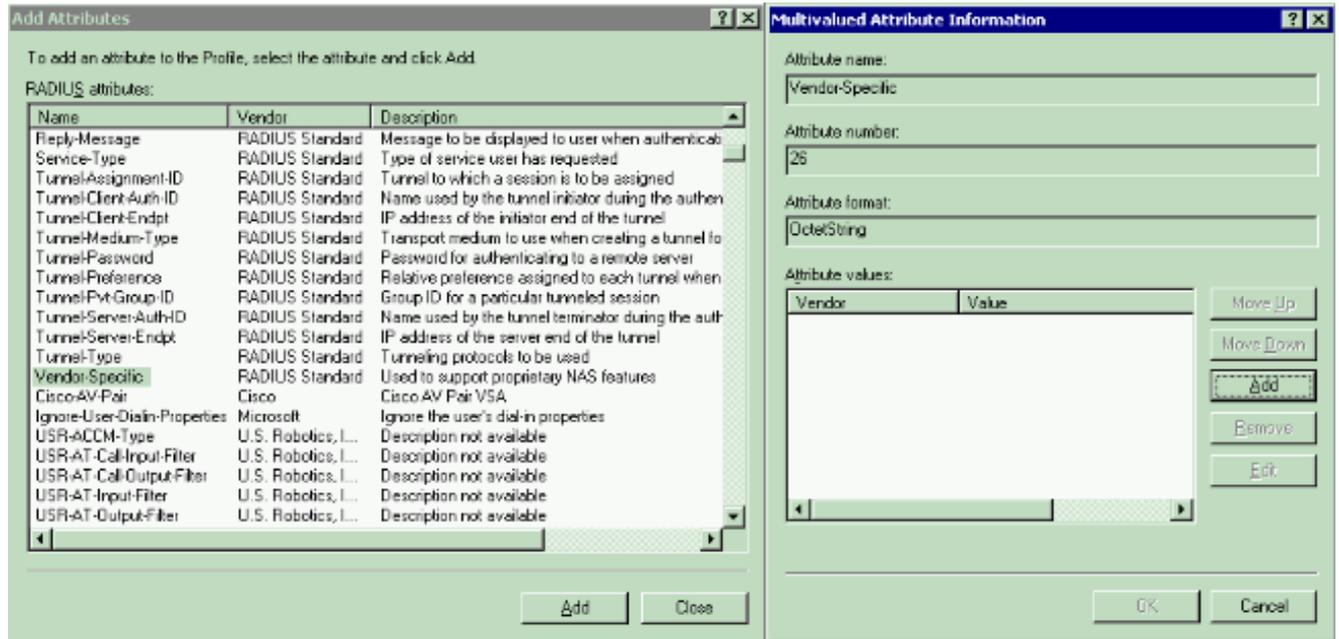
Klicken Sie auf die Registerkarte **Erweitert**. Entfernen Sie alle Standardparameter, und klicken Sie auf



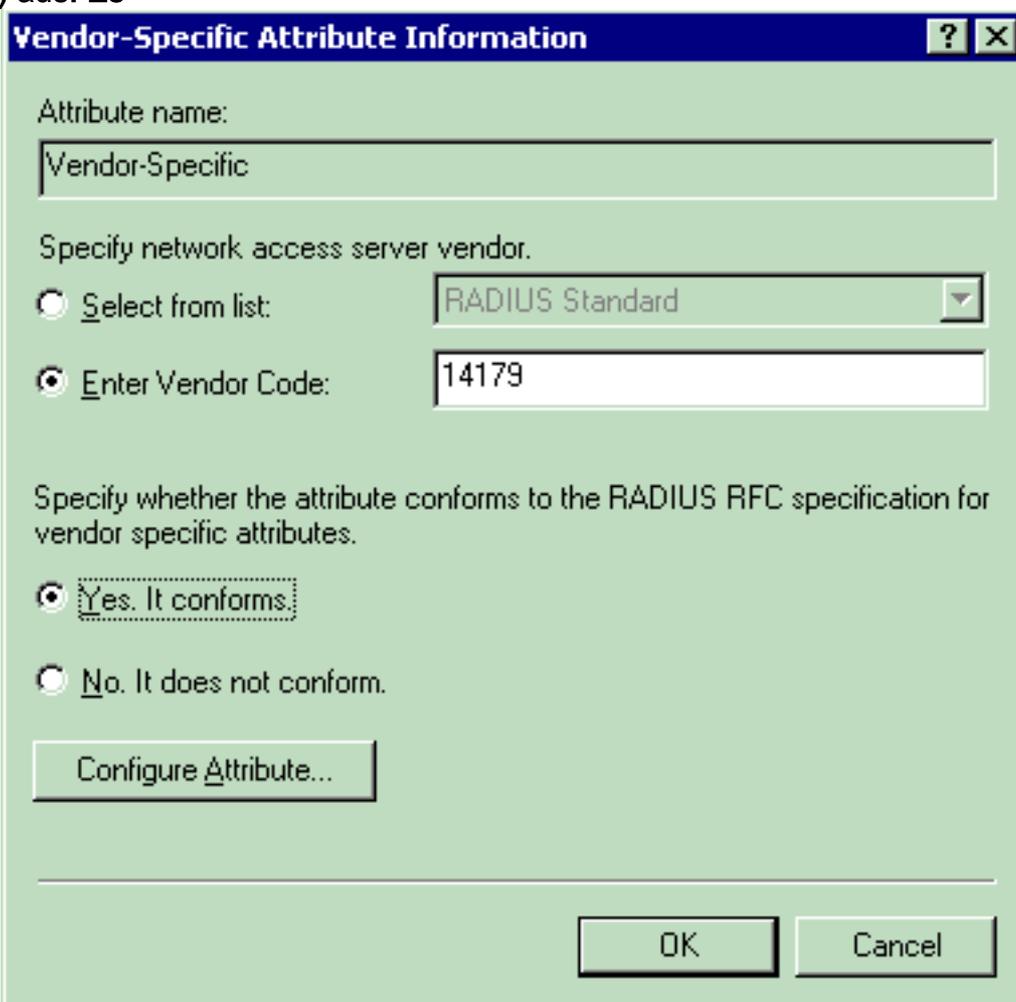
Hinzufügen. Wählen Sie im Fenster **Attribute hinzufügen** die Option **Service Typ** aus, und wählen Sie anschließend im nächsten Fenster den **Anmeldungswert** aus.



Als Nächstes müssen Sie das **anbieterspezifische** Attribut aus der RADIUS-Attributliste auswählen.

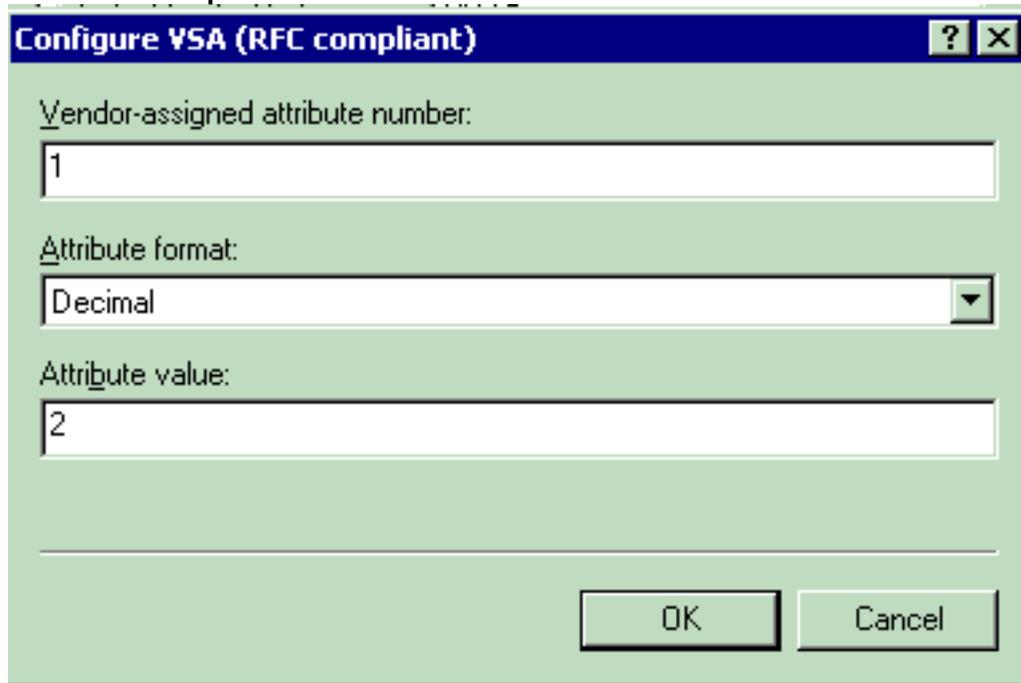


Klicken Sie im nächsten Fenster auf **Hinzufügen**, um ein neues VSA auszuwählen. Das Fenster Herstellerspezifische Attributinformationen wird angezeigt. Wählen Sie unter Anbieter für Netzwerkzugriffsserver angeben die Option **Anbietercode eingeben aus**. Geben Sie den Vendor Code für Airespace VSAs ein. Der Vendor-Code für Cisco Airespace VSAs lautet **14179**. Da dieses Attribut der RADIUS RFC-Spezifikation für VSAs entspricht, wählen Sie **Yes (Ja)** aus. Es



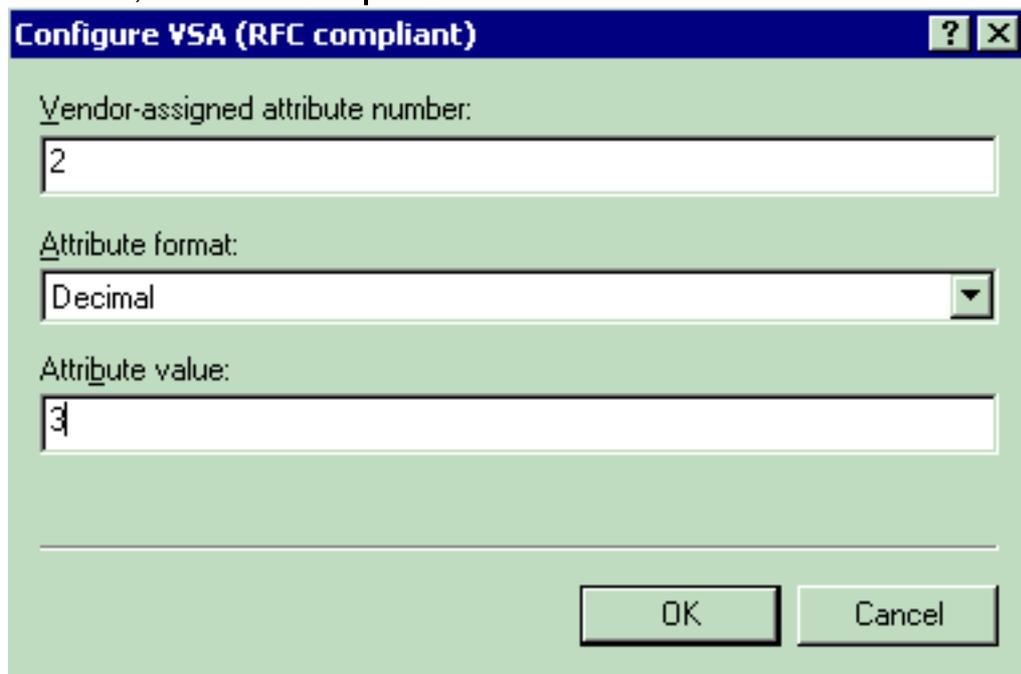
stimmt. Klicken Sie auf **Attribut konfigurieren**. Geben Sie im Fenster **Configure VSA (RFC-konform)** (VSA

konfigurieren) (RFC-konform) die vom Anbieter zugewiesene Attributnummer, das Attributformat und den Attributwert ein, die von dem VSA abhängen, das Sie verwenden möchten. So legen Sie die WLAN-ID auf Benutzerbasis fest: **Attributname** - AirRespace-WLAN-ID **Vom Anbieter zugewiesene Attributnummer: 1** **Attributformat** - Integer/Dezimal **Wert** - WLAN-ID **Beispiel 1**



So legen Sie das

QoS-Profil auf Benutzerbasis fest: **Attributname** - Airespace-QoS-Level **Vom Anbieter zugewiesene Attributnummer: 2** **Attributformat** - Integer/Dezimal **Wert: 0** - Silver; **1** - Gold; **2** - Platinum; **3** - Bronze **Beispiel 2**



So legen Sie den

DSCP-Wert auf Benutzerbasis fest: **Attributname** - Airespace-DSCP **Vom Anbieter zugewiesene Attributnummer** - **3** **Attributformat** - Integer/Dezimal **Wert** - DSCP-Wert **Beispiel 3**

Configure VSA (RFC compliant) ? X

Vendor-assigned attribute number:

Attribute format:

Attribute value:

OK Cancel

So legen Sie das 802.1p-Tag auf Benutzerbasis fest:**Attributname** - Airespace-802.1p-TagVom Anbieter zugewiesene Attributnummer - 4Attributformat - Integer/DezimalWert: 802.1p-TagBeispiel 4

Configure VSA (RFC compliant) ? X

Vendor-assigned attribute number:

Attribute format:

Attribute value:

OK Cancel

So legen Sie die Schnittstelle (VLAN) auf Benutzerbasis fest:**Attributname** - Airespace-Interface-NameVom Anbieter zugewiesene Attributnummer: 5Attributformat - ZeichenfolgeWert - SchnittstellennamenBeispiel 5

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

Vendor-assigned attribute number:

Attribute format:

Attribute value:

[OK] [Cancel]

So legen Sie die ACL auf Benutzerbasis fest:
Attributname - Airespace-ACL-Name
Vom Anbieter zugewiesene Attributnummer - 6
Attributformat - Zeichenfolge
Wert - ACL-Name
Beispiel 6

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

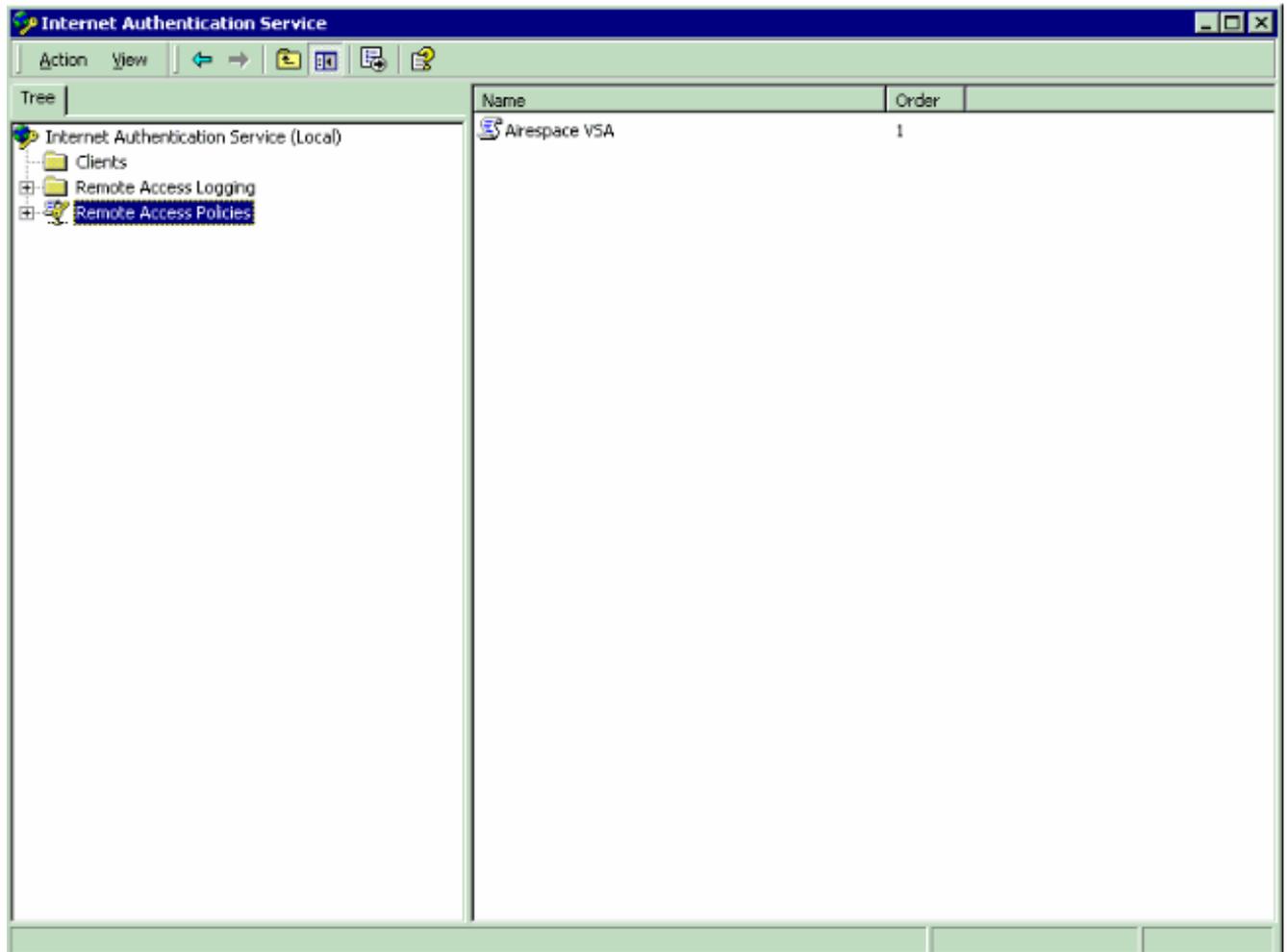
Vendor-assigned attribute number:

Attribute format:

Attribute value:

[OK] [Cancel]

8. Wenn Sie die VSAs konfiguriert haben, klicken Sie auf **OK**, bis das Fenster Benutzerprofil angezeigt wird.
9. Klicken Sie anschließend auf **Fertig stellen**, um die Konfiguration abzuschließen. Die neue Richtlinie wird unter "Remote Access Policies" (Remote-Zugriffsrichtlinien) angezeigt.



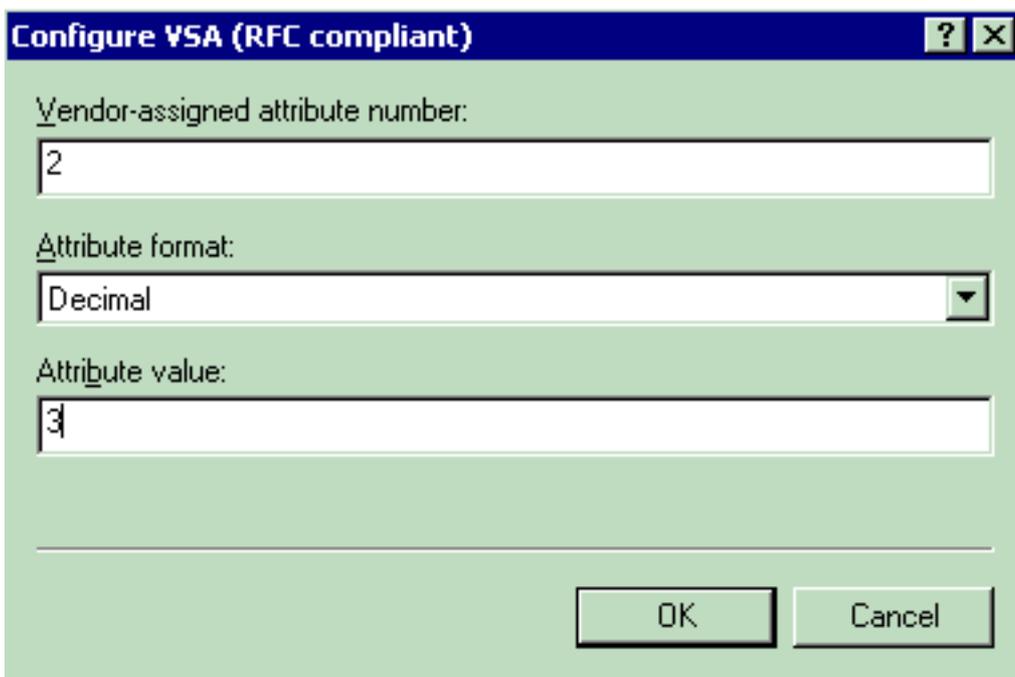
Beispielkonfiguration

In diesem Beispiel wird ein WLAN für die Webauthentifizierung konfiguriert. Die Benutzer werden vom IAS RADIUS-Server authentifiziert, und der RADIUS-Server ist so konfiguriert, dass QoS-Richtlinien auf Benutzerbasis zugewiesen werden.

The screenshot displays the Cisco Systems configuration page for a WLAN. The main configuration area is titled 'WLAN ID 1' and 'WLAN SSID 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 checked. 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 QoS, AAA Override, and Radius Server settings. A red box highlights the Layer 3 Security settings. Red text at the bottom provides warnings about Web Policy and CKIP support.

Wie Sie in diesem Fenster sehen, ist die Webauthentifizierung aktiviert, der Authentifizierungsserver ist 172.16.1.1, und AAA-override ist auch im WLAN aktiviert. Die QoS-StandardEinstellung für dieses WLAN ist auf Silver eingestellt.

Auf dem IAS RADIUS-Server wird eine Remote Access Policy konfiguriert, die das QoS-Attribut Bronze in der RADIUS Accept-Anforderung zurückgibt. Dies geschieht, wenn Sie das für das QoS-Attribut spezifische VSA konfigurieren.



Detaillierte Informationen zur Konfiguration einer [Remote-Zugriffsrichtlinie auf dem IAS](#)-Abschnitt dieses Dokuments finden Sie im Abschnitt Konfigurieren der Remote-Zugriffsrichtlinie.

Sobald der IAS-Server, der WLC und die LAP für diese Konfiguration konfiguriert sind, können die Wireless-Clients die Webauthentifizierung verwenden, um eine Verbindung herzustellen.

Überprüfung

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Wenn der Benutzer über eine Benutzer-ID und ein Kennwort eine Verbindung zum WLAN herstellt, übergibt der WLC die Anmeldeinformationen an den IAS RADIUS-Server, der den Benutzer anhand der Bedingungen und des Benutzerprofils authentifiziert, die in der Remote-Zugriffsrichtlinie konfiguriert wurden. Wenn die Benutzerauthentifizierung erfolgreich ist, gibt der RADIUS-Server eine RADIUS-Annahmeanforderung zurück, die auch die AAA-Überschreibungswerte enthält. In diesem Fall wird die QoS-Richtlinie des Benutzers zurückgegeben.

Sie können den Befehl **debug aaa all enable** ausführen, um die Ereignissequenz anzuzeigen, die während der Authentifizierung auftritt. Hier sehen Sie eine Beispielausgabe:

```
(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)

Wie Sie in der Ausgabe sehen können, wird der Benutzer authentifiziert. Anschließend werden AAA-Überschreibungswerte mit der Meldung RADIUS accept (RADIUS akzeptieren) zurückgegeben. In diesem Fall erhält der Benutzer die QoS-Richtlinie von Bronze.

Sie können dies auch auf der WLC-GUI überprüfen. Hier ein Beispiel:

The screenshot shows the Cisco WLC GUI with the following 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

Hinweis: Das Standard-QoS-Profil für diese SSID ist Silver. Da jedoch AAA-Überschreibungen ausgewählt und der Benutzer mit einem QoS-Profil von Bronze auf dem IAS-Server konfiguriert ist, wird das standardmäßige QoS-Profil überschrieben.

Fehlerbehebung

Sie können den Befehl **debug aa all enable** auf dem WLC verwenden, um die Konfiguration zu beheben. Ein Beispiel für die Ausgabe dieses Debuggens in einem funktionierenden Netzwerk finden Sie im Abschnitt [Überprüfen](#) dieses Dokuments.

Hinweis: Beachten Sie [vor der](#) Verwendung von **Debug**-Befehlen die [Informationen](#) zu [Debug-Befehlen](#).

Zugehörige Informationen

- [Konfigurationsleitfaden für Cisco Wireless LAN Controller, Version 4.0](#)
- [Einschränken des WLAN-Zugriffs auf der Basis der SSID mit WLC und Cisco Secure ACS - Konfigurationsbeispiel](#)
- [Wireless-Produktunterstützung](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)