

Esempio di configurazione di VSA Cisco Airespace su Microsoft IAS Radius Server

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Premesse](#)

[Configurazione di IAS per VSA Airespace](#)

[Configurare il WLC come client AAA su IAS](#)

[Configurare i criteri di accesso remoto su IAS](#)

[Esempio di configurazione](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

[Introduzione](#)

In questo documento viene spiegato come configurare un server Microsoft Internet Authentication Service (IAS) per supportare gli attributi specifici del fornitore (VSA) di Cisco Airespace. Il codice del fornitore per i VSA Cisco Airespace è **14179**.

[Prerequisiti](#)

[Requisiti](#)

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Informazioni sulla configurazione di un server IAS
- Conoscenza della configurazione dei Lightweight Access Point (LAP) e dei Cisco Wireless LAN Controller (WLC)
- Conoscenza delle soluzioni Cisco Unified Wireless Security

[Componenti usati](#)

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Server Microsoft Windows 2000 con IAS
- Cisco 4400 WLC con software versione 4.0.206.0
- Cisco serie 1000 LAP
- scheda client wireless 802.11 a/b/g con firmware 2.5
- Aironet Desktop Utility (ADU) versione 2.5

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Nota: questo documento intende fornire al lettore un esempio della configurazione richiesta sul server IAS per supportare le VSA Cisco Airespace. La configurazione del server IAS descritta in questo documento è stata testata in laboratorio e funziona come previsto. In caso di problemi durante la configurazione del server IAS, contattare Microsoft per assistenza. Cisco TAC non supporta la configurazione del server Microsoft Windows.

In questo documento si presume che il WLC sia configurato per il funzionamento di base e che i LAP siano registrati sul WLC. Se si è un nuovo utente che cerca di configurare il WLC per il funzionamento di base con i LAP, fare riferimento alla [registrazione di un Lightweight AP \(LAP\) su un Wireless LAN Controller \(WLC\)](#).

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

Premesse

Nella maggior parte dei sistemi WLAN (Wireless LAN), ogni WLAN ha un criterio statico che si applica a tutti i client associati a un SSID (Service Set Identifier). Sebbene potente, questo metodo presenta delle limitazioni in quanto richiede ai client di associarsi a SSID diversi per ereditare criteri QoS e di sicurezza diversi.

Tuttavia, la soluzione Cisco Wireless LAN supporta le reti di identità, che consentono alla rete di annunciare un singolo SSID e a utenti specifici di ereditare diverse policy di sicurezza o QoS in base ai rispettivi profili utente. I criteri specifici che è possibile controllare utilizzando Identity Networking includono:

- **Quality of Service:** quando è presente in un'accettazione di accesso RADIUS, il valore del livello QoS sostituisce il valore QoS specificato nel profilo WLAN.
- **ACL:** quando l'attributo Access Control List (ACL) è presente in RADIUS Access Accept, il sistema applica l'ACL-Name alla stazione client dopo l'autenticazione. In questo modo si ignorano gli ACL assegnati all'interfaccia.
- **VLAN:** quando un nome di interfaccia VLAN o un tag VLAN è presente in un'accettazione di accesso RADIUS, il sistema posiziona il client su un'interfaccia specifica.
- **ID WLAN:** quando l'attributo WLAN-ID è presente nell'autorizzazione di accesso RADIUS, il sistema applica l'ID WLAN (SSID) alla stazione client dopo l'autenticazione. L'ID WLAN viene inviato dal WLC in tutte le istanze di autenticazione ad eccezione di IPsec. In caso di autenticazione Web, se il WLC riceve un attributo WLAN-ID nella risposta di autenticazione

dal server AAA e non corrisponde all'ID della WLAN, l'autenticazione viene rifiutata. Non è possibile utilizzare altri tipi di metodi di protezione.

- **Valore DSCP:** se presente in un'accettazione di accesso RADIUS, il valore DSCP sostituisce il valore DSCP specificato nel profilo WLAN.
- **802.1p-Tag:** quando è presente in un'accettazione di accesso RADIUS, il valore 802.1p sostituisce il valore predefinito specificato nel profilo WLAN.

Nota: la funzione VLAN supporta solo il filtro MAC, 802.1X e l'accesso protetto Wi-Fi (WPA). La funzionalità VLAN non supporta l'autenticazione Web o IPSec. Il database del filtro MAC locale del sistema operativo è stato esteso per includere il nome dell'interfaccia. In questo modo, i filtri MAC locali possono specificare l'interfaccia da assegnare al client. È possibile utilizzare anche un server RADIUS separato, ma il server RADIUS deve essere definito utilizzando i menu Security.

Per ulteriori informazioni sulle reti di identità, fare riferimento a [Configurazione di Identity Networking](#).

[Configurazione di IAS per VSA Airespace](#)

Per configurare gli IAS per le VSA Airespace, completare i seguenti passaggi:

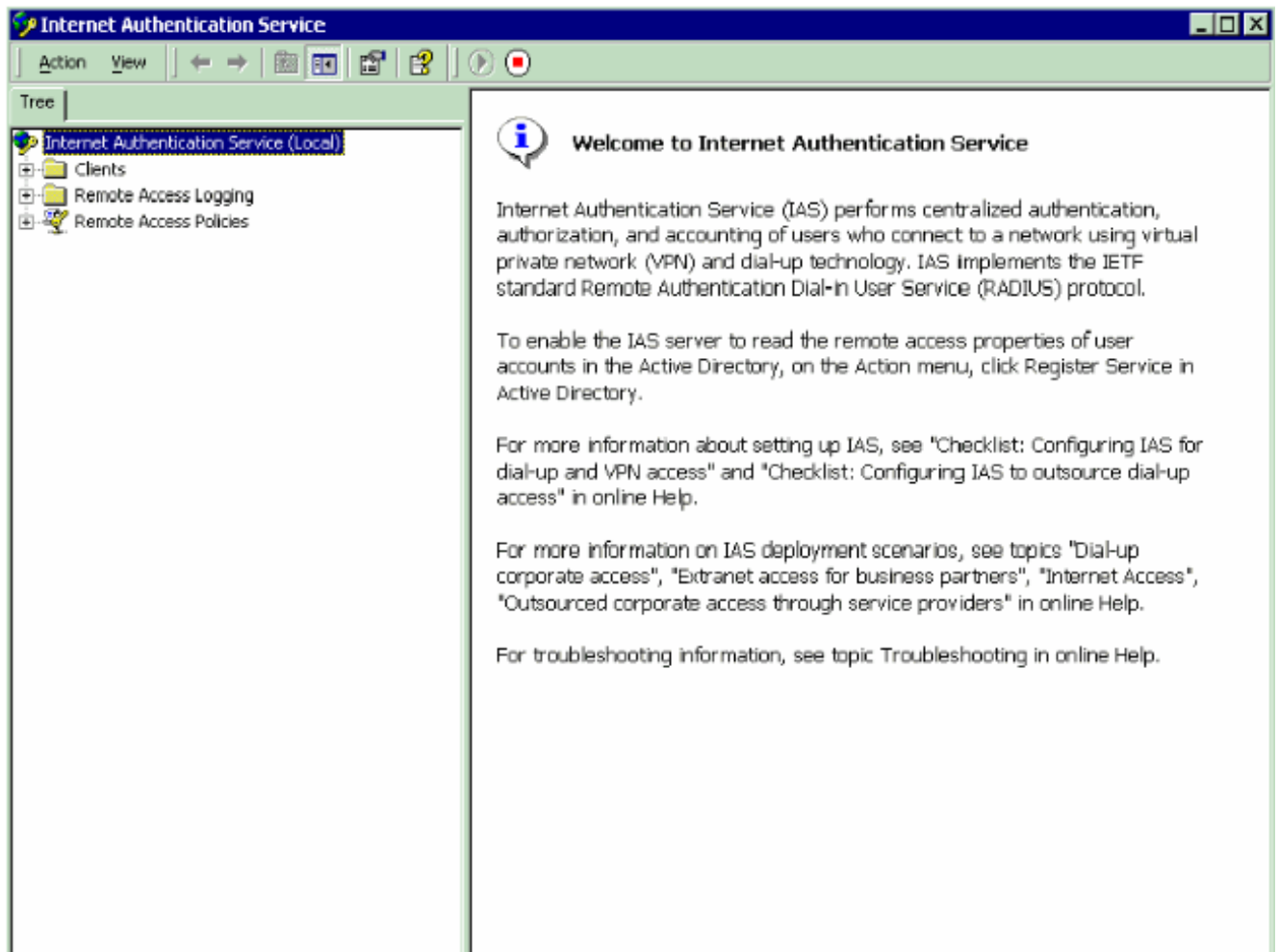
1. [Configurare il WLC come client AAA su IAS](#)
2. [Configurare i criteri di accesso remoto su IAS](#)

Nota: le VSA sono configurate in Criteri di accesso remoto.

[Configurare il WLC come client AAA su IAS](#)

Completare questa procedura per configurare il WLC come client AAA sullo switch IAS:

1. Per avviare IAS sul server Microsoft 2000, fare clic su **Programmi > Strumenti di amministrazione > Servizio di autenticazione Internet**.



2. Fare clic con il pulsante destro del mouse sulla cartella **Clients** e scegliere **New Client** per aggiungere un nuovo client RADIUS.
3. Nella finestra Add Client, immettere il nome del client e scegliere **RADIUS** come protocollo. Fare quindi clic su **Avanti**. Nell'esempio, il nome del client è *WLC-1*. **Nota:** per impostazione predefinita, il protocollo è impostato su 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. Nella finestra Aggiungi client RADIUS, immettere l'indirizzo IP del client, il fornitore del client e il **segreto condiviso**. Dopo aver immesso le informazioni sul client, fare clic su **Fine**. Nell'esempio viene mostrato un client denominato *WLC-1* con indirizzo IP *172.16.1.30*, il client-fornitore è impostato su *Cisco* e il segreto condiviso è *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]

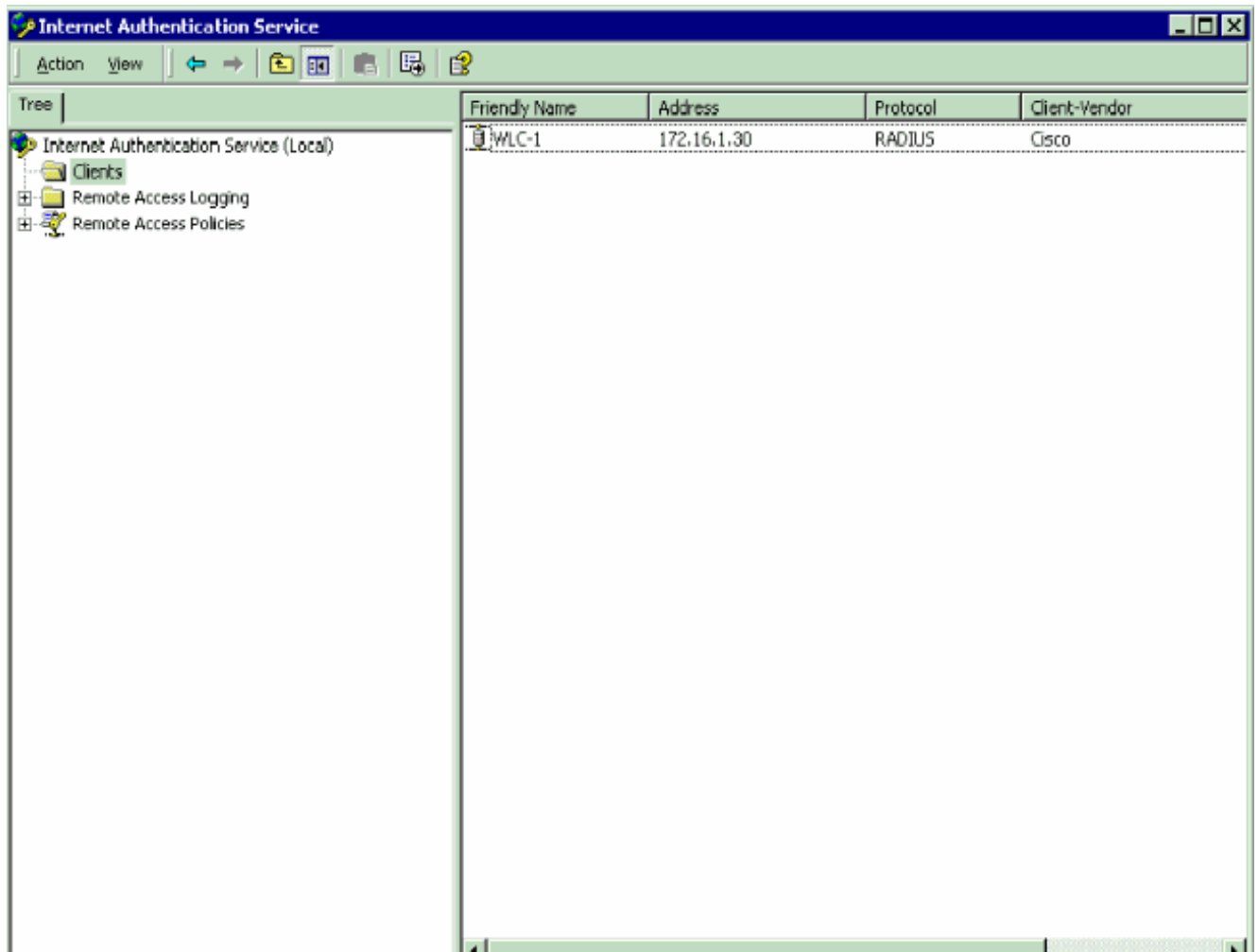
Client must always send the signature attribute in the request

Shared secret: [xxxxxxx]

Confirm shared secret: [xxxxxxx]

< Back Finish Cancel

Con queste informazioni, il WLC denominato WLC-1 viene aggiunto come client AAA del server IAS.

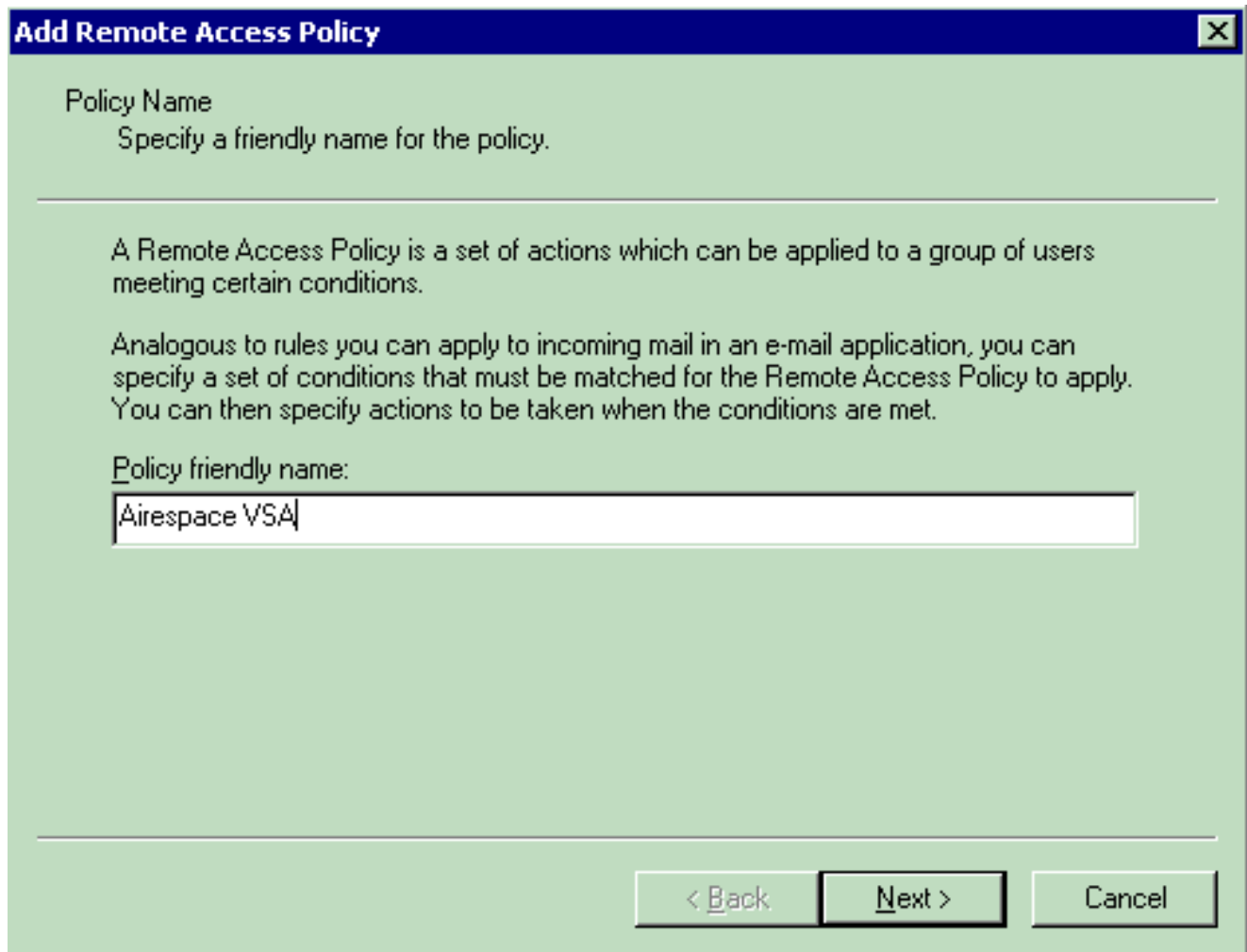


Il passaggio successivo consiste nella creazione di un criterio di accesso remoto e nella configurazione delle VSA.

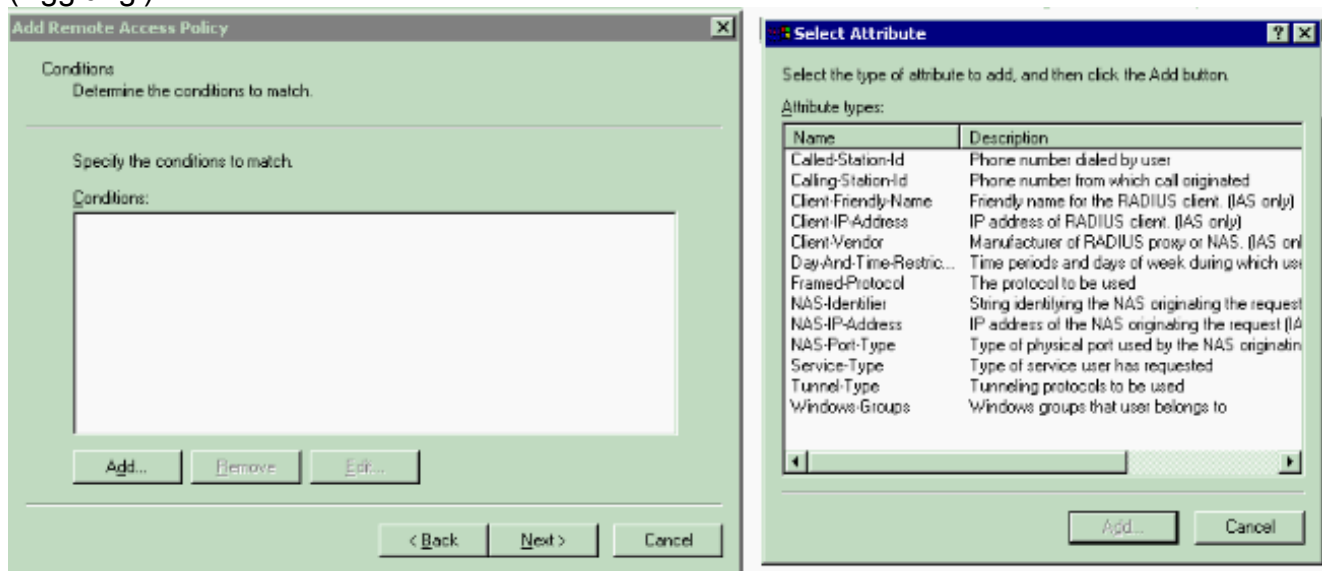
[Configurare i criteri di accesso remoto su IAS](#)

Completare questi passaggi per configurare un nuovo criterio di accesso remoto sullo IAS:

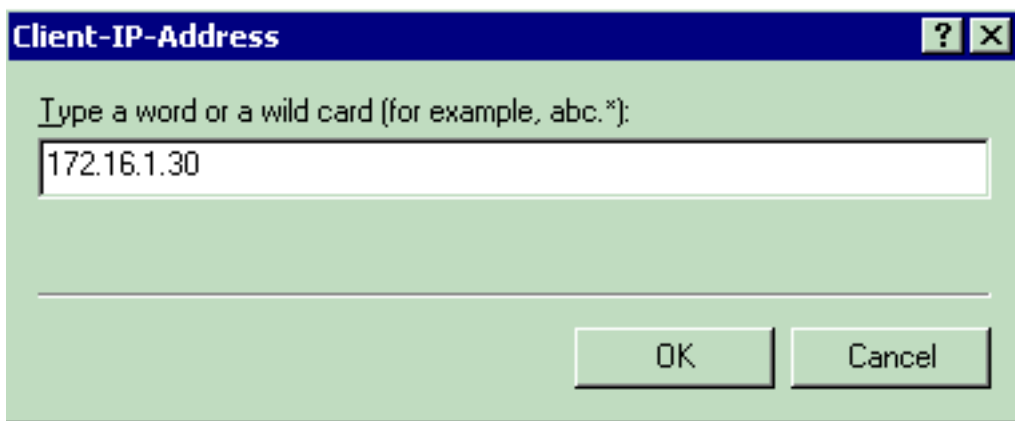
1. Fare clic con il pulsante destro del mouse su **Criteri di accesso remoto** e scegliere **Nuovo criterio di Accesso remoto MSs**. Viene visualizzata la finestra Nome criterio.
2. Immettere il nome del criterio e fare clic su **Avanti**.



3. Nella finestra successiva selezionare le condizioni a cui verranno applicati i criteri di accesso remoto. Per selezionare le condizioni, fare clic su **Add** (Aggiungi).



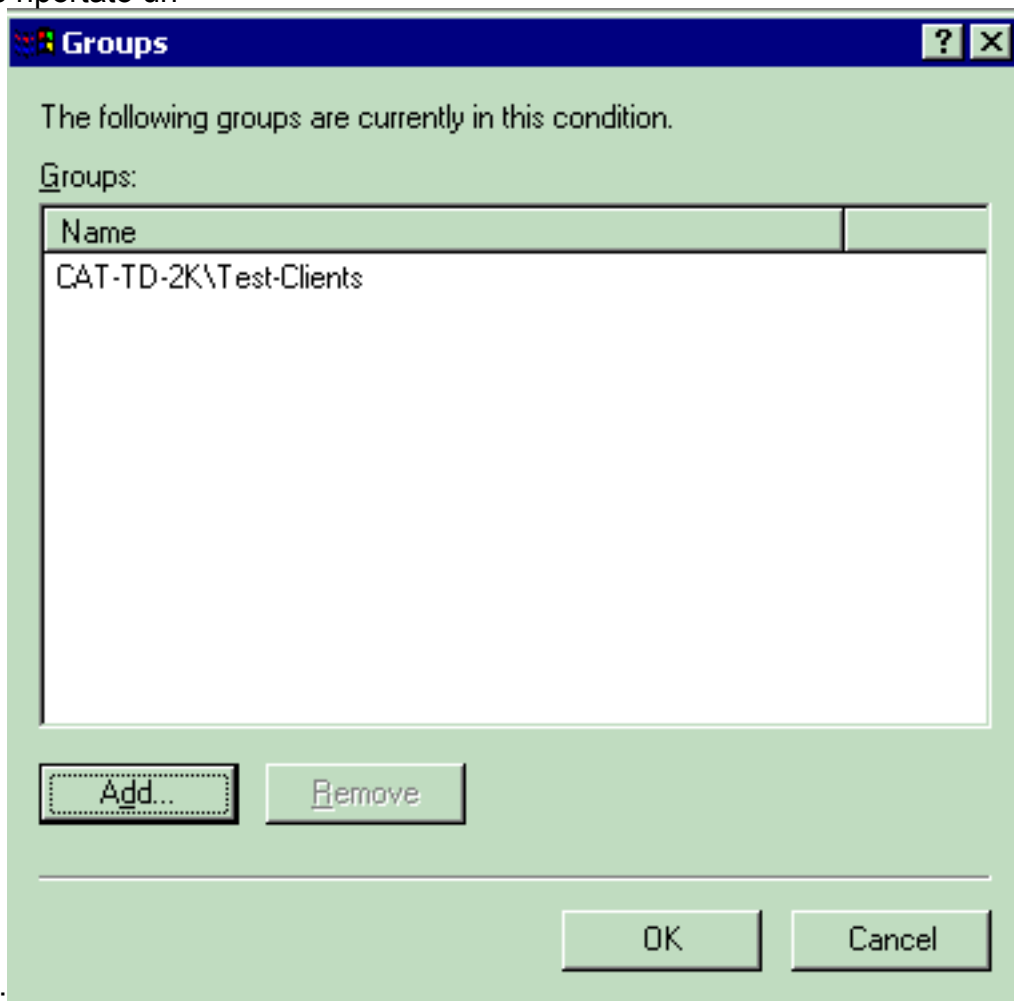
4. Dal menu Tipi di attributo, selezionare i seguenti attributi: **Client-IP-Address**: immettere l'indirizzo IP del client AAA. Nell'esempio, viene immesso l'indirizzo IP del WLC, in modo che il criterio venga applicato ai pacchetti provenienti dal



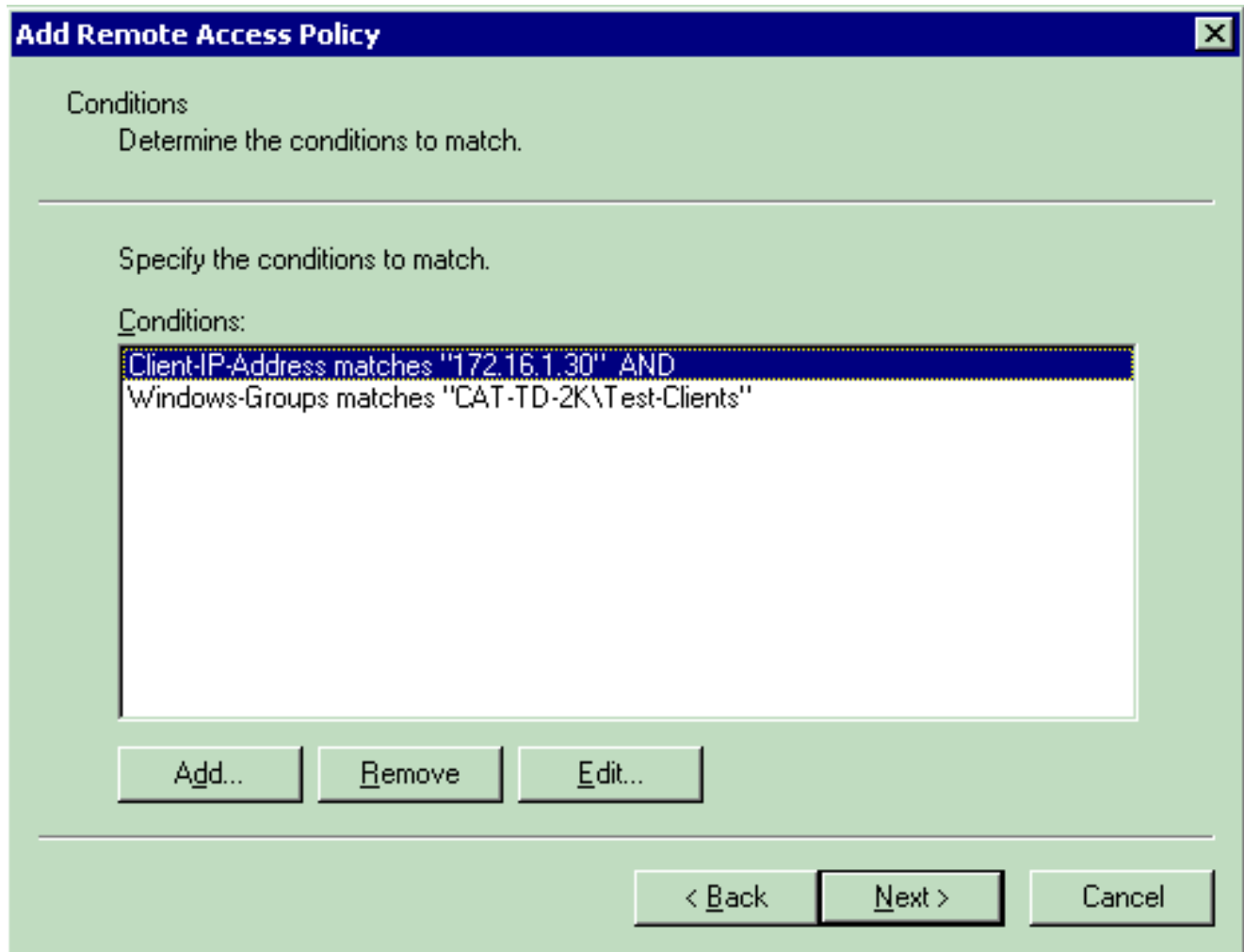
WLC.

Gruppi di

Windows: selezionare il gruppo di Windows (il gruppo di utenti) a cui applicare il criterio. Di seguito è riportato un

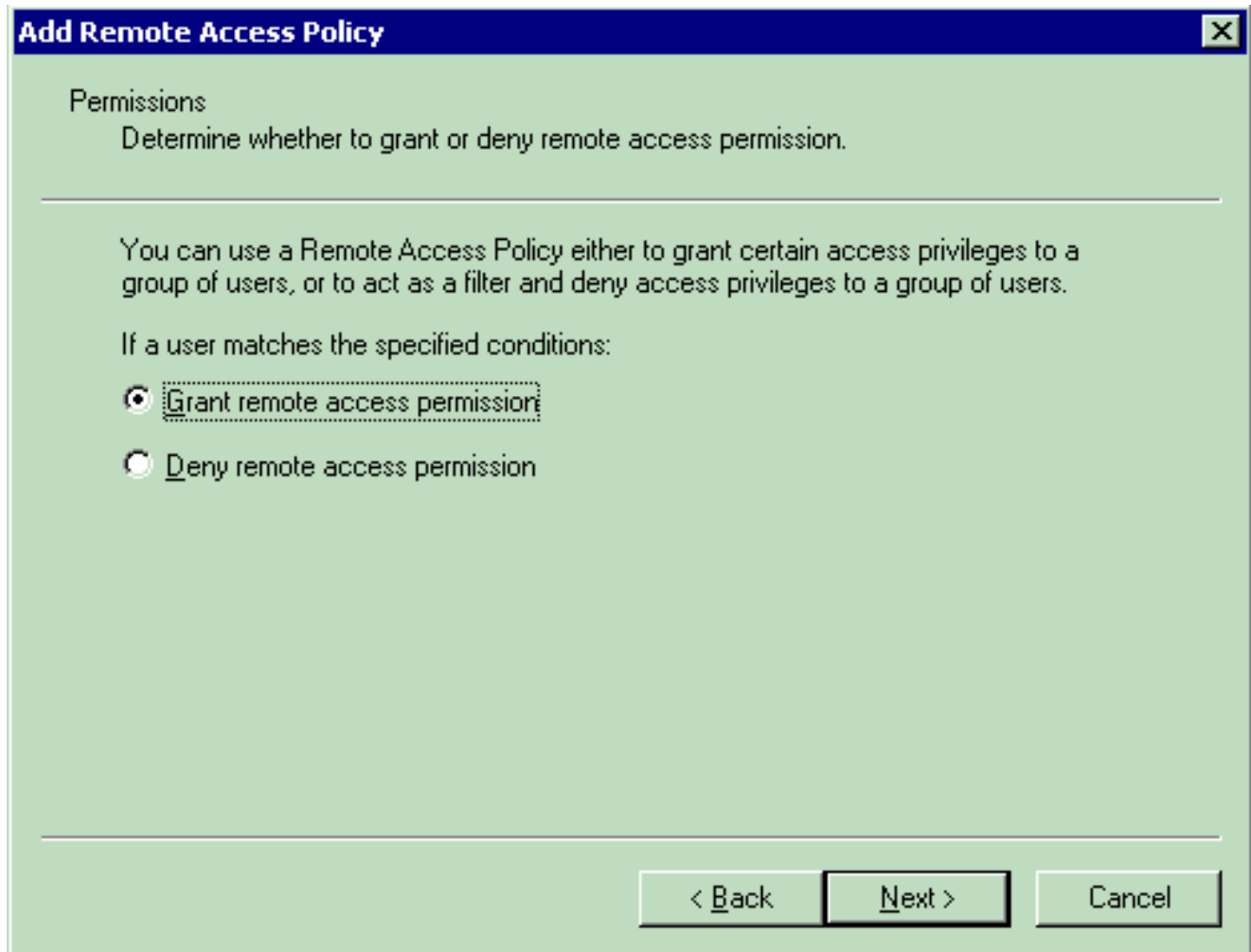


esempio:



In questo esempio vengono illustrate solo due condizioni. Se sono presenti altre condizioni, aggiungerle e fare clic su **Avanti**. Viene visualizzata la finestra Autorizzazioni.

5. Nella finestra Autorizzazioni scegliere **Concedi autorizzazione di accesso remoto**. Dopo aver scelto questa opzione, all'utente viene concesso l'accesso, purché soddisfi le condizioni specificate (dal passaggio 2).



6. Fare clic su **Next** (Avanti).

7. Il passaggio successivo consiste nell'impostare il profilo utente. Anche se è stato specificato che l'accesso agli utenti deve essere negato o concesso in base alle condizioni, il profilo può comunque essere utilizzato se le condizioni di questo criterio vengono ignorate per ogni utente.

Add Remote Access Policy



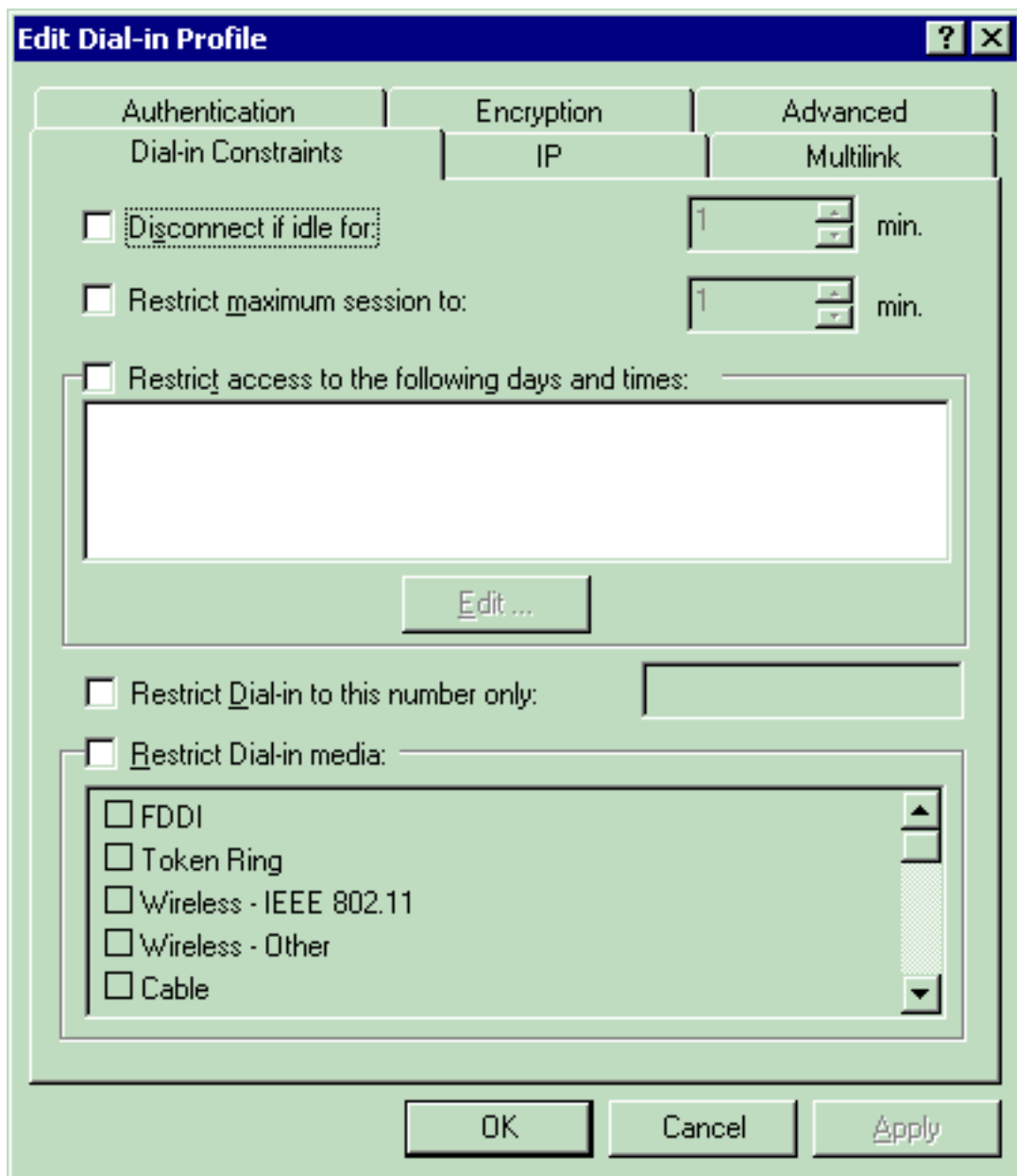
User Profile

Specify the user profile.

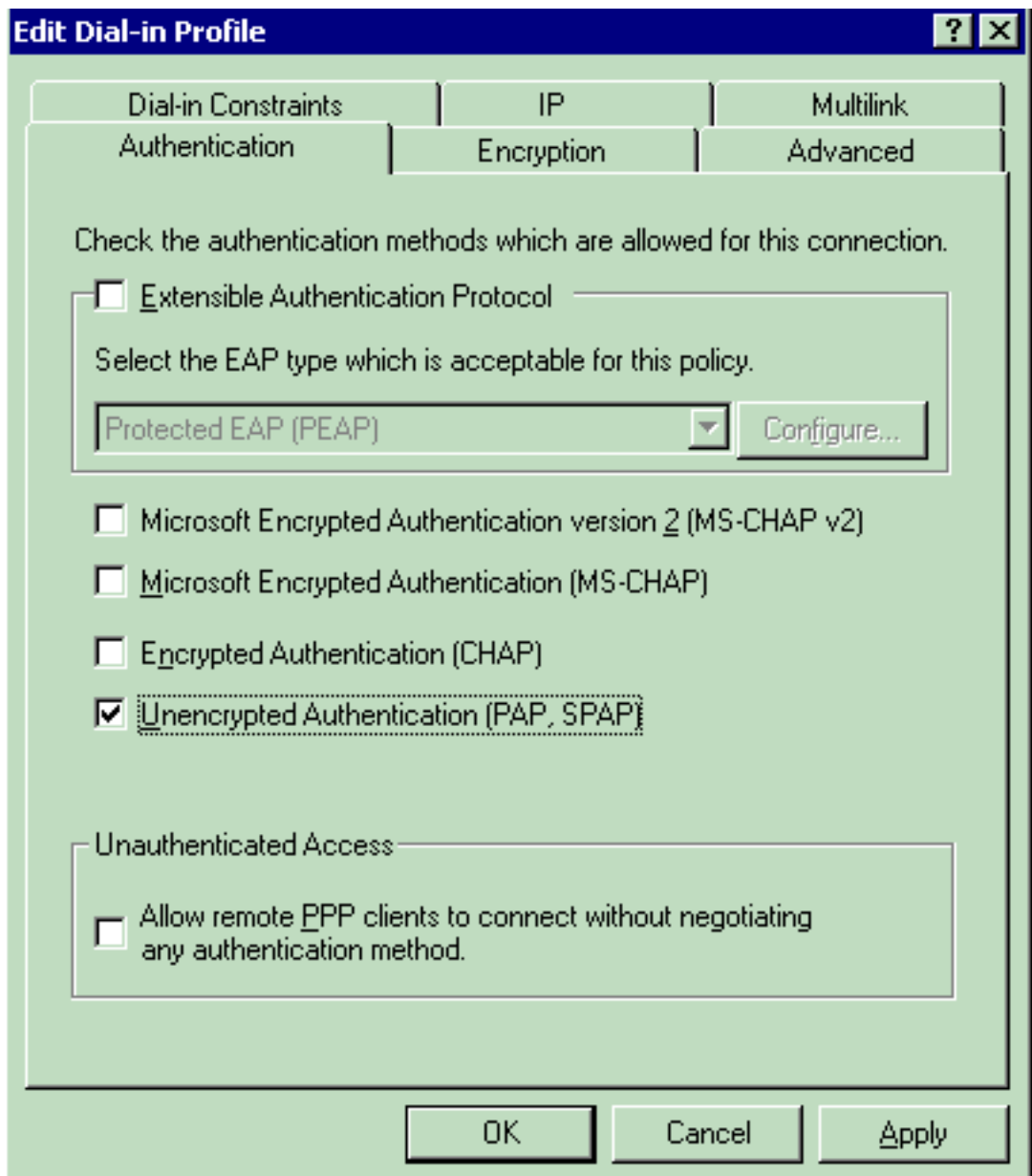
You can now specify the profile for users who matched the conditions you have specified.

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.

Per configurare il profilo utente, fare clic su **Modifica profilo** nella finestra Profilo utente. Viene visualizzata la finestra Modifica profilo chiamate in



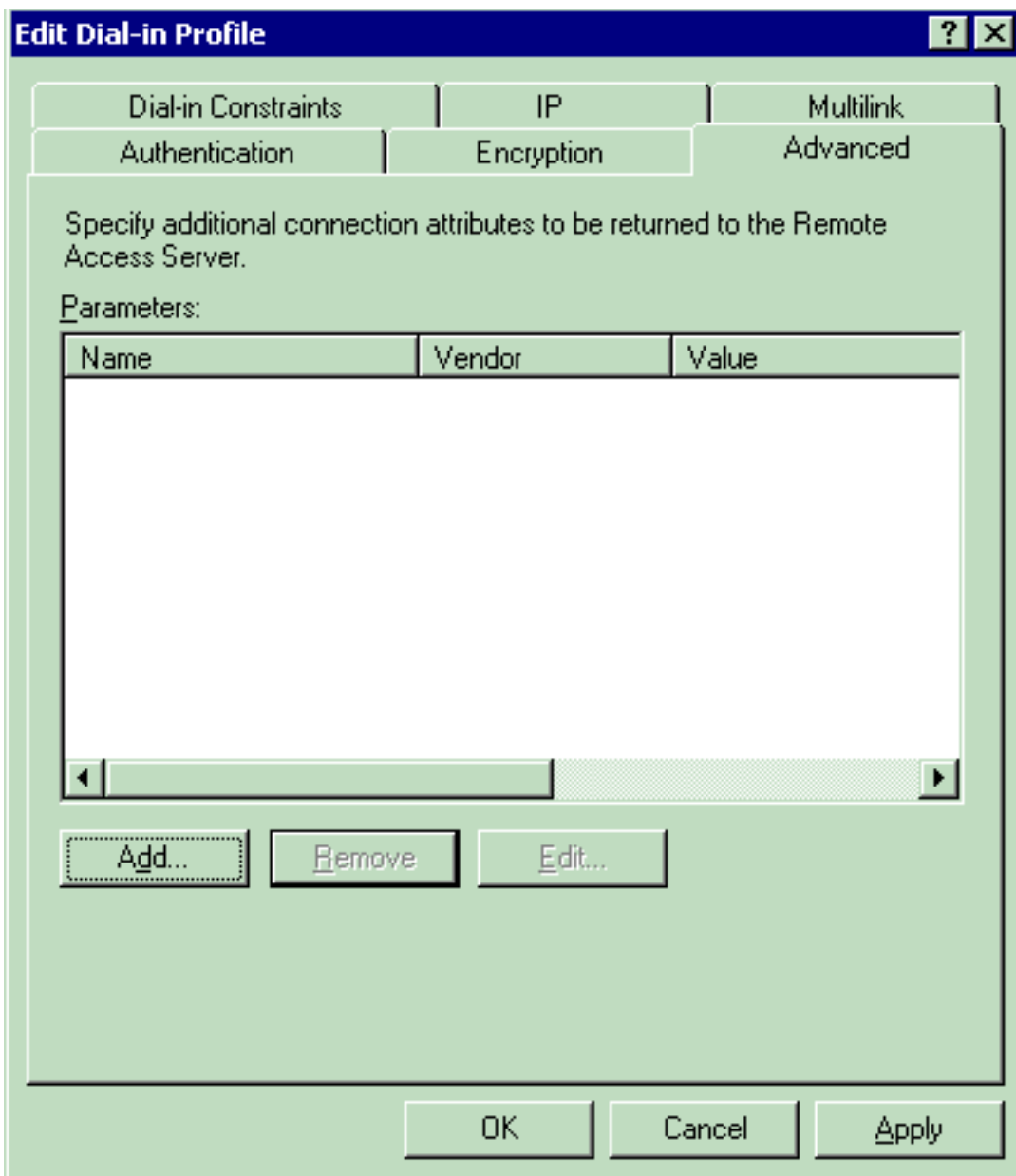
ingresso. Fare clic sulla scheda **Authentication** (Autenticazione), quindi selezionare il metodo di autenticazione utilizzato nella WLAN. In questo esempio viene utilizzata l'autenticazione non crittografata



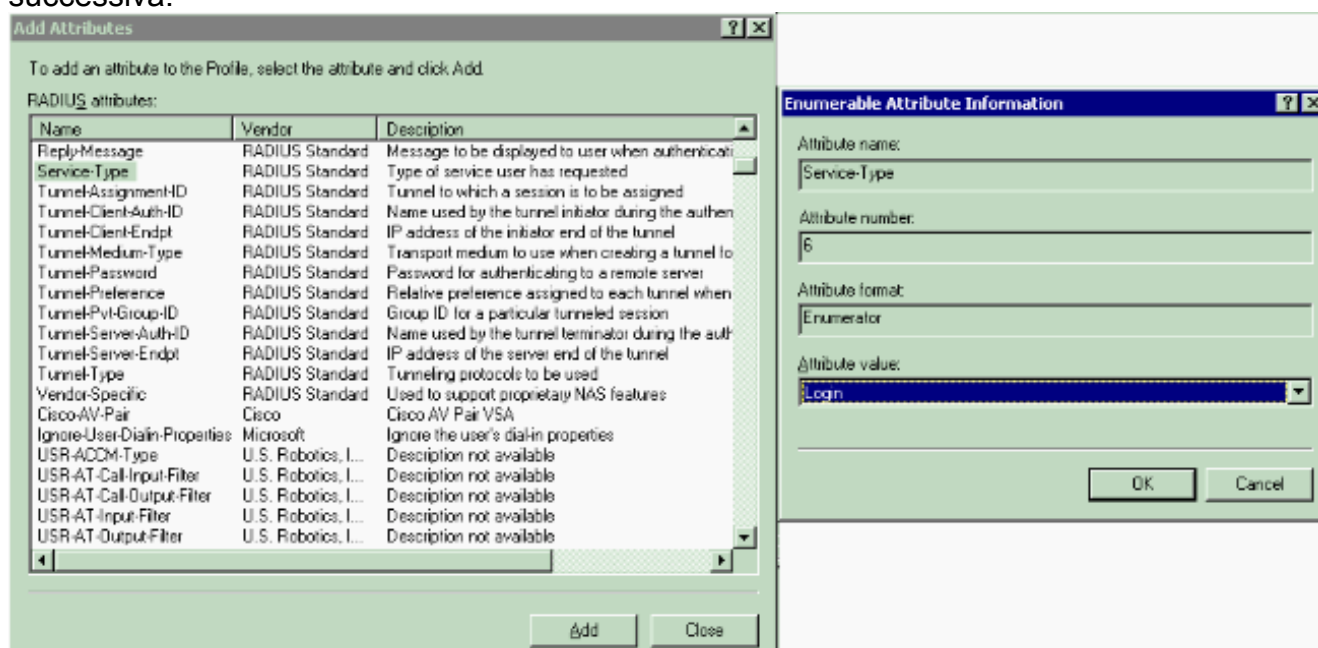
(PAP, SPAP).

e clic sulla scheda **Avanzate**. Rimuovete tutti i parametri di default e fate clic su **Aggiungi**

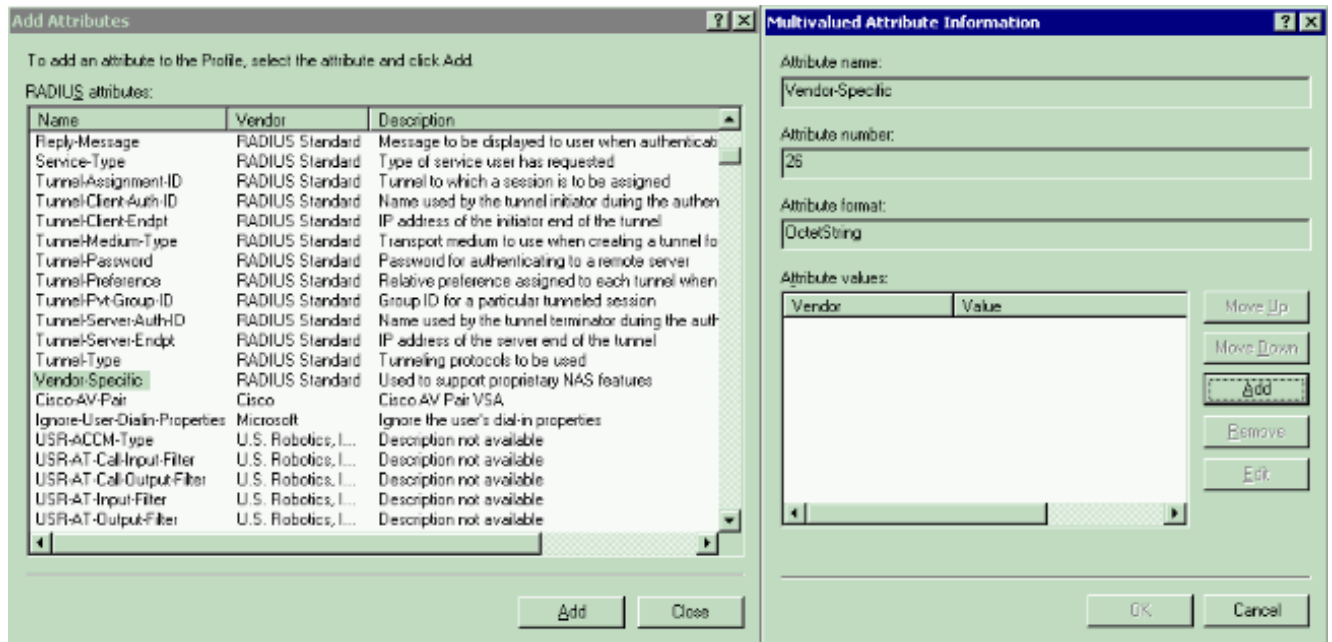
Far



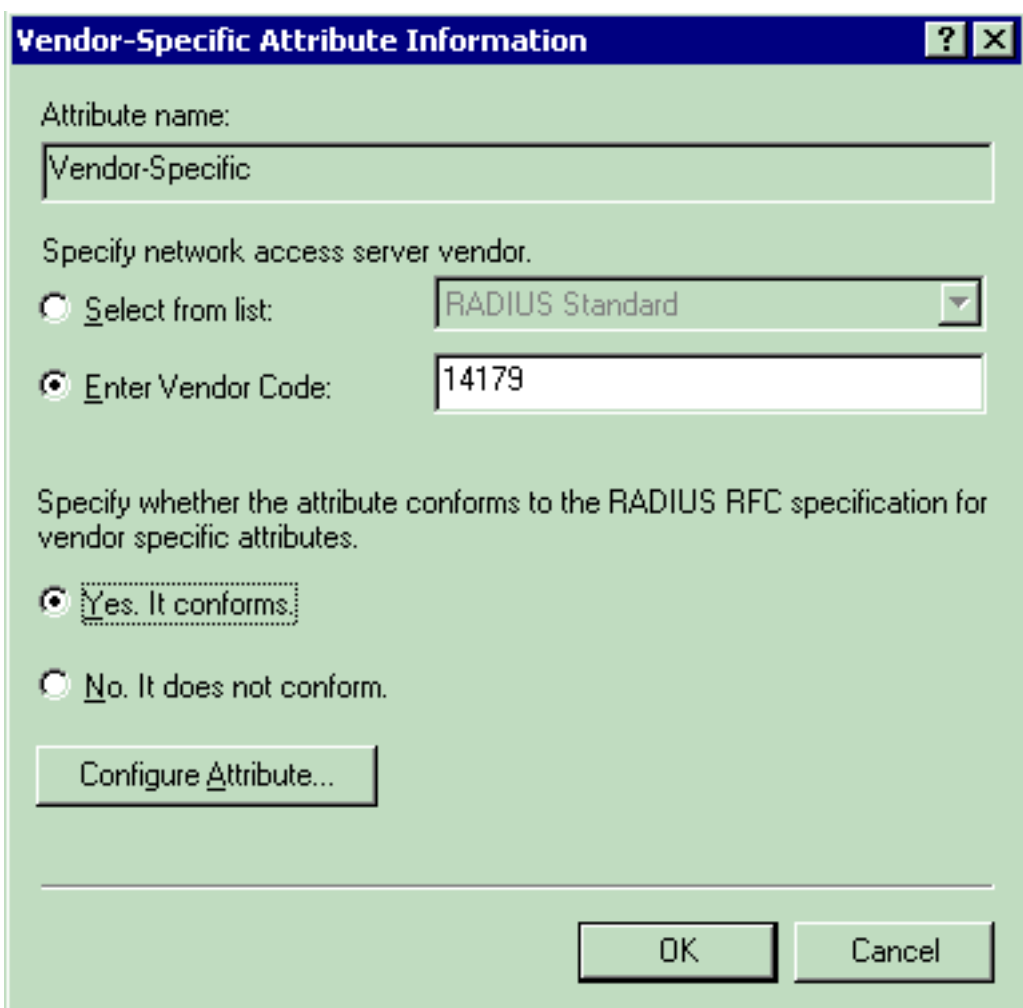
(Add). Dalla finestra **Aggiungi attributi**, selezionare **Service-Type**, quindi scegliere il valore **Login** dalla finestra successiva.



Quindi, selezionare l'attributo **specifico del fornitore** dall'elenco degli attributi RADIUS.

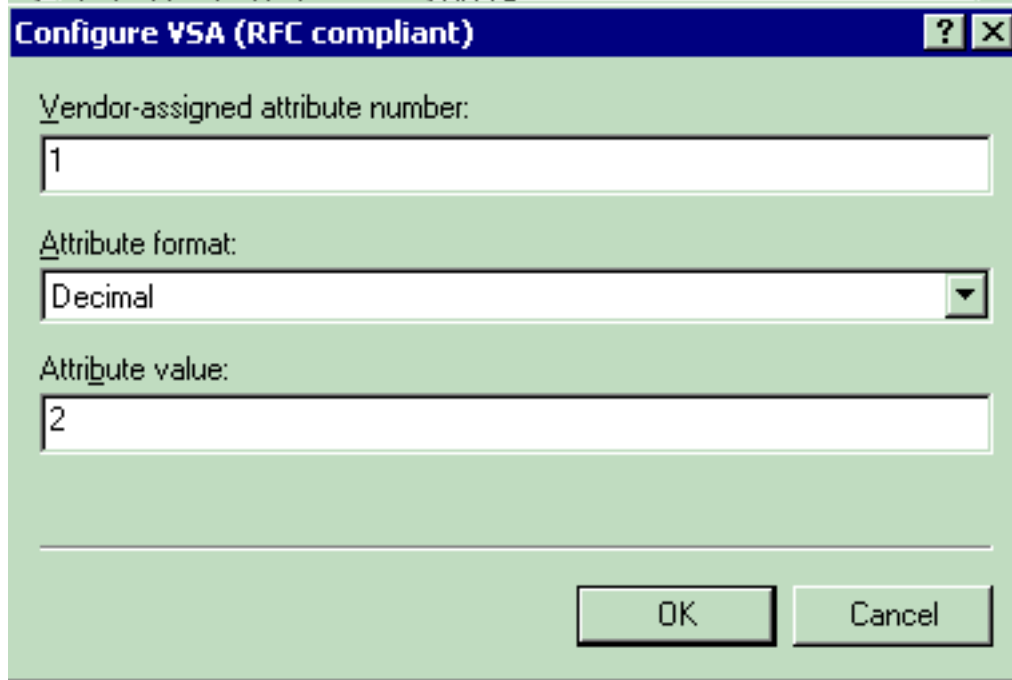


Per selezionare una nuova VSA, fare clic su **Add** (Aggiungi) nella finestra successiva. Viene visualizzata la finestra Informazioni attributi specifici del fornitore. In Specificare il fornitore del server di accesso alla rete, scegliere **Immettere il codice fornitore**. Immettere il codice del fornitore per le VSA Airespace. Il codice del fornitore per le VSA Cisco Airespace è **14179**. Poiché questo attributo è conforme alla specifica RFC RADIUS per le VSA, scegliere **Sì**. È



conforme.. Fare clic su **Configura attributo**. Nella finestra Configura VSA (RFC compliant), immettere il numero di

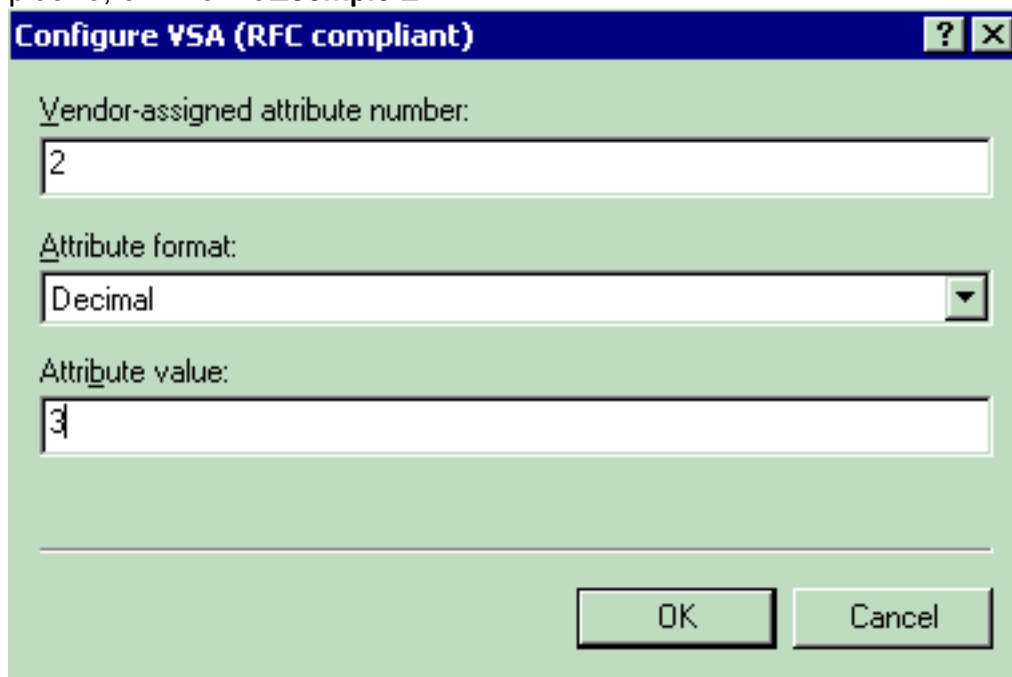
attributo assegnato dal fornitore, il formato dell'attributo e il valore dell'attributo, che dipendono dal VSA che si desidera utilizzare. Per impostare l'ID WLAN per singolo utente:
Nome attributo: Airespace-WLAN-Id
Numero attributo assegnato dal fornitore—1
Formato attributo: intero/decimale
Valore: WLAN-ID
Esempio 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" set to "Decimal", and "Attribute value" with the value "2". At the bottom, there are "OK" and "Cancel" buttons.

Per impostare il

profilo QoS per singolo utente:
Nome attributo: Airespace-QoS-Level
Numero attributo assegnato dal fornitore—2
Formato attributo: intero/decimale
Valore—0 - Argento; 1 - Oro; 2 - platino; 3 - Bronzo
Esempio 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" set to "Decimal", and "Attribute value" with the value "3". At the bottom, there are "OK" and "Cancel" buttons.

Per impostare il

valore DSCP per singolo utente:
Nome attributo: Airespace-DSCP
Numero attributo assegnato dal fornitore—3
Formato attributo: intero/decimale
Valore: valore DSCP
Esempio 3

Configure VSA (RFC compliant)

Vendor-assigned attribute number:

Attribute format:

Attribute value:

Per impostare il tag 802.1p per ogni utente:
Nome attributo: Airespace-802.1p-Tag
Numero attributo assegnato dal fornitore: 4
Formato attributo: intero/decimale
Valore—Tag 802.1p
Esempio 4

Configure VSA (RFC compliant)

Vendor-assigned attribute number:

Attribute format:

Attribute value:

Per impostare l'interfaccia (VLAN) per singolo utente:
Nome attributo: Airespace-Interface-Name
Numero attributo assegnato dal fornitore—5
Formato attributo: String
Value - Interface-Name
Esempio

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

Vendor-assigned attribute number:

Attribute format:

Attribute value:

[OK] [Cancel]

5 Per impostare l'ACL in base all'utente: Nome attributo: Airespace-ACL-Name Numero attributo assegnato dal fornitore—6 Formato attributo: String Value: ACL-Name Esempio 6

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

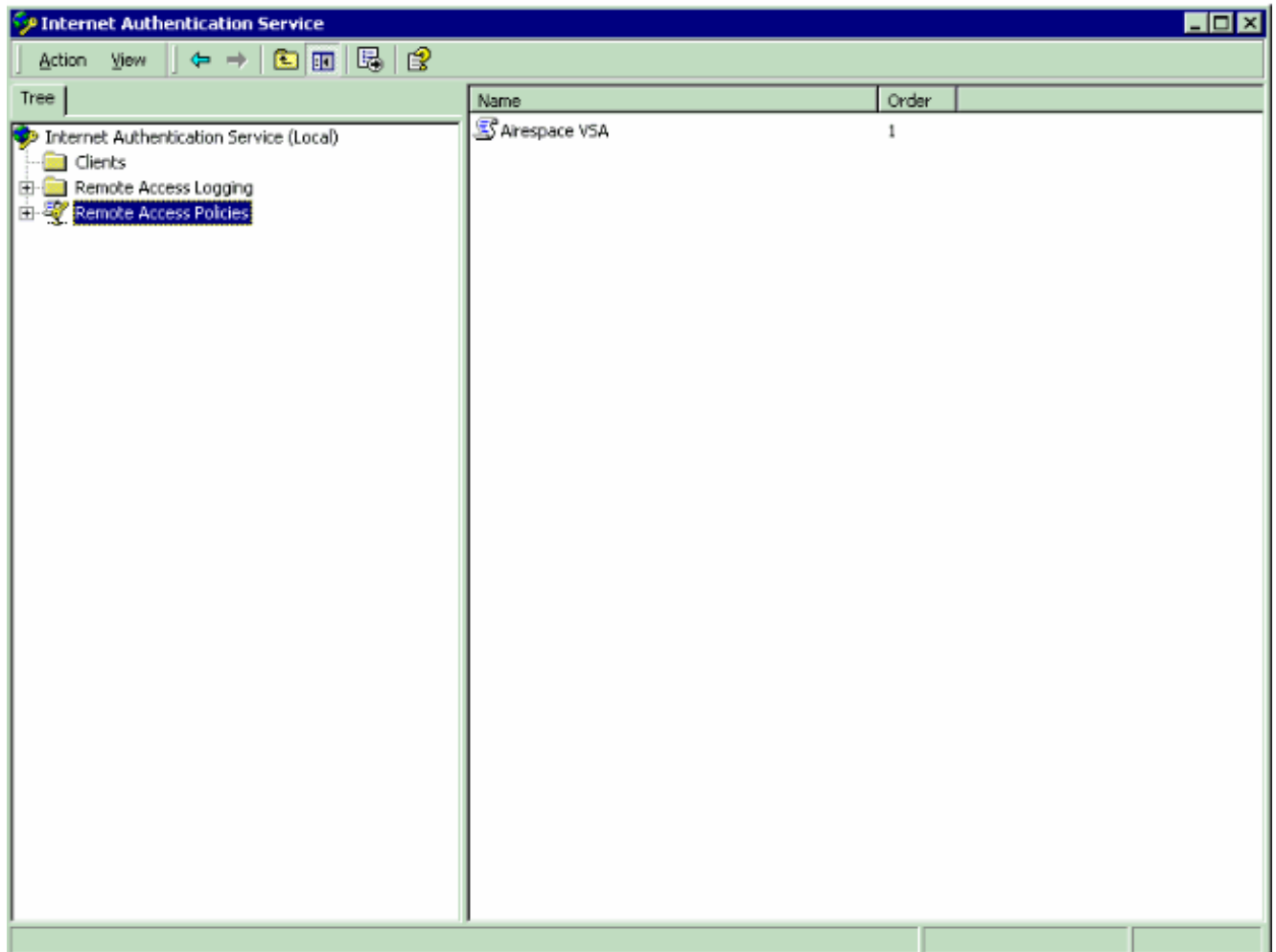
Vendor-assigned attribute number:

Attribute format:

Attribute value:

[OK] [Cancel]

8. Dopo aver configurato le VSA, fare clic su **OK** fino a visualizzare la finestra del profilo utente.
9. Quindi, fare clic su **Finish** (Fine) per completare la configurazione. È possibile visualizzare il nuovo criterio in Criteri di accesso remoto.



Esempio di configurazione

Nell'esempio, una WLAN è configurata per l'autenticazione Web. Gli utenti vengono autenticati dal server RADIUS IAS e il server RADIUS è configurato per allocare i criteri QoS per singolo utente.

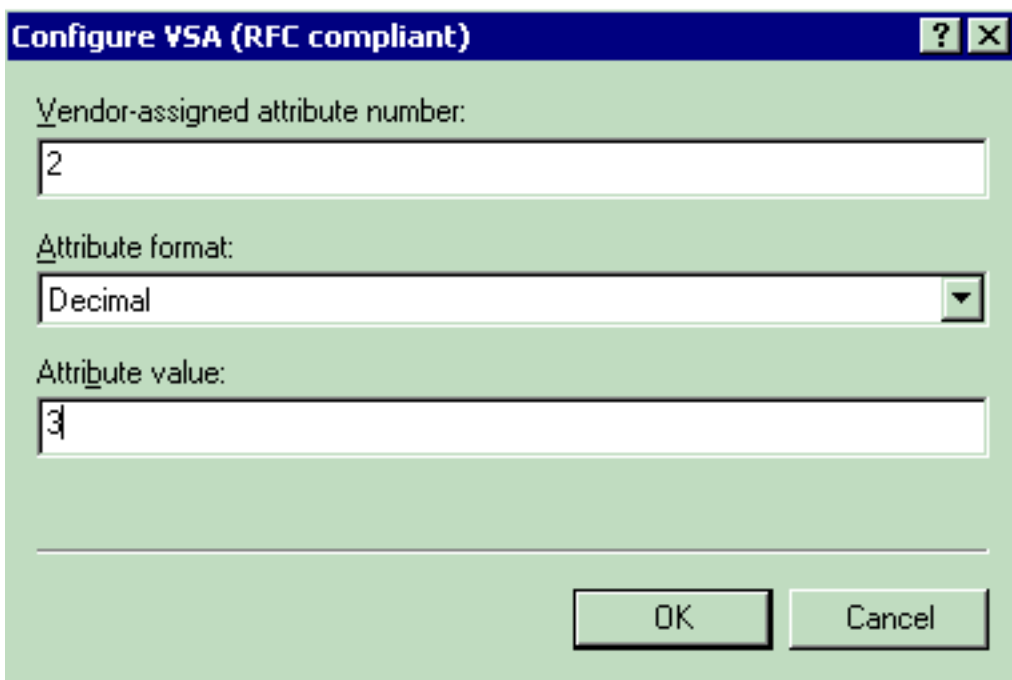
The screenshot displays the Cisco Systems WLAN configuration interface. The main content is divided into several sections:

- WLANs > Edit**: Shows WLAN ID 1 and WLAN SSID SSID-WLC2.
- General Policies**: Includes Radio Policy (All), Admin Status (Enabled), Session Timeout (secs) (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).
- Security Policies**: Shows Layer 2 Security (None) with MAC Filtering (Disabled), Layer 3 Security (None) with Web Policy (Enabled) and Authentication (Selected) options, and Preauthentication ACL (none).
- Radius Servers**: Shows Server 1 with Authentication Servers (IP:172.16.1.1, Port:1812) and Accounting Servers (none).

Red circles highlight the QoS setting, the AAA Override setting, and the Radius Servers configuration. A red box highlights the Layer 3 Security settings. Red text at the bottom 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'.

Come si può vedere da questa finestra, l'autenticazione Web è abilitata, il server di autenticazione è 172.16.1.1 e sulla WLAN è abilitata anche la sostituzione AAA. L'impostazione predefinita di QoS per questa WLAN è Silver.

Sul server RADIUS IAS, è configurato un criterio di accesso remoto che restituisce l'attributo QoS Bronze nella richiesta di accettazione RADIUS. A tale scopo, è necessario configurare la VSA specifica per l'attributo QoS.



Per informazioni dettagliate su come configurare un criterio di accesso remoto sul server IAS, vedere la sezione [Configurazione](#) del criterio di accesso remoto [sullo](#) IAS di questo documento.

Una volta configurati il server IAS, il WLC e il LAP per questa configurazione, i client wireless possono utilizzare l'autenticazione Web per connettersi.

[Verifica](#)

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Quando l'utente si connette alla WLAN con un ID utente e una password, il WLC passa le credenziali al server IAS RADIUS che autentica l'utente in base alle condizioni e al profilo utente configurati nei criteri di accesso remoto. Se l'autenticazione dell'utente ha esito positivo, il server RADIUS restituisce una richiesta di accettazione RADIUS contenente anche i valori di sostituzione AAA. In questo caso, viene restituito il criterio QoS dell'utente.

È possibile usare il comando **debug aaa all enable** per visualizzare la sequenza di eventi verificatisi durante l'autenticazione. Di seguito è riportato un esempio di output:

```
(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)
```

Come si può vedere dall'output, l'utente è autenticato. I valori di sostituzione AAA vengono quindi restituiti con il messaggio di accettazione RADIUS. In questo caso, all'utente viene data la politica QoS del Bronzo.

È possibile verificarlo anche sull'interfaccia utente del WLC. Di seguito è riportato un esempio:

The screenshot shows the Cisco WLC web interface. The main content area is titled 'Clients > Detail'. It is divided into 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

Nota: il profilo QoS predefinito per questo SSID è Silver. Tuttavia, poiché è stata selezionata la sostituzione AAA e l'utente è configurato con un profilo QoS Bronze sul server IAS, il profilo QoS predefinito viene sostituito.

Risoluzione dei problemi

Per risolvere i problemi di configurazione, è possibile usare il comando **debug aaa all enable** sul WLC. Nella sezione [Verifica](#) di questo documento viene mostrato un esempio dell'output di questo debug in una rete funzionante.

Nota: consultare le [informazioni importanti sui comandi di debug](#) prima di usare i comandi di debug.

Informazioni correlate

- [Guida alla configurazione di Cisco Wireless LAN Controller, versione 4.0](#)
- [Esempio di limitazione dell'accesso WLAN in base al SSID con WLC e Cisco Secure ACS](#)
- [Supporto dei prodotti wireless](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)