

Microsoft IAS Radius サーバでの Cisco Airespace VSA の設定例

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[背景説明](#)

[Airespace VSA用のIASの設定](#)

[IASでAAAクライアントとしてWLCを設定する](#)

[IASでリモートアクセスポリシーを設定する](#)

[設定例](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

このドキュメントでは、Cisco Airespace Vendor Specific Attributes(VSA)をサポートするように Microsoft Internet Authentication Service(IAS)サーバを設定する方法について説明します。Cisco Airespace VSA のベンダー コードは 14179 です。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- IASサーバの設定方法に関する知識
- Lightweight Access Point (LAP; Lightweight アクセス ポイント) および Cisco Wireless LAN Controller (WLC; ワイヤレス LAN コントローラ)の設定についての知識
- Cisco Unified Wireless Security ソリューションについての知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- IAS がインストールされた Microsoft Windows 2000 サーバ

- ソフトウェア バージョン 4.0.206.0 が稼働している Cisco 4400 WLC
- Cisco 1000 シリーズ LAP
- ファームウェア 2.5 が稼働する 802.11 a/b/g ワイヤレス クライアント アダプタ
- Aironet Desktop Utility (ADU) バージョン 2.5

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

注 : このドキュメントは、Cisco Airespace VSAをサポートするためにIASサーバに必要な設定の例を読者に示すことを目的としています。このドキュメントで示されているIASサーバの設定は、ラボでテスト済みであり、期待どおりに動作します。IASサーバの設定に問題がある場合は、Microsoftに問い合わせてください。Cisco TAC では、Microsoft Windows サーバの設定に関するサポートは行っていません。

このドキュメントでは、基本動作に WLC が設定されており、WLC に LAP が登録されていることを前提としています。WLC で LAP との基本動作を初めて設定する場合は、『[ワイヤレス LAN コントローラ \(WLC \) への Lightweight AP \(LAP \) の登録](#)』を参照してください。

表記法

ドキュメント表記の詳細は、『[シスコテクニカルティップスの表記法](#)』を参照してください。

背景説明

一般的な WLAN システムでは、Service Set Identifier (SSID) に関連付けられたすべてのクライアントに適用されるスタティックなポリシーが各 WLAN に存在します。この方法は強力ですが、異なる QoS ポリシーやセキュリティ ポリシーを継承するために各クライアントを異なる SSID に関連付ける必要があるため、さまざまな制約があります。

ただし、Cisco Wireless LAN ソリューションでは、アイデンティティ ネットワーキングがサポートされています。この場合、ネットワーク上で 1 つの SSID のみをアドバタイズすることによって、特定のユーザがそれぞれのポリシーに基づいた異なる QoS ポリシーまたはセキュリティ ポリシーを継承できるようになります。特定のポリシーを制御するには、アイデンティティ ネットワーキングの次の機能を使用します。

- **Quality of Service :** RADIUS Access Accept に含まれている場合、その QoS レベルの値によって、WLAN プロファイルに設定された QoS 値が上書きされます。
- **ACL :** RADIUS Access Accept に、アクセスコントロール リスト (ACL) 属性が含まれている場合、システムによって、認証後にクライアント ステーションに ACL 名が適用されます。これは、インターフェイスに割り当てられた ACL を上書きします。
- **VLAN :** RADIUS Access Accept に VLAN Interface-Name または VLAN-Tag が含まれている場合、システムによって、クライアントが特定のインターフェイスに割り当てられます。
- **WLAN ID :** RADIUS Access Accept に WLAN ID が含まれている場合、システムによって、認証後にクライアント ステーションに WLAN ID (SSID) が適用されます。WLAN ID は、IPSec を除く、すべての認証のインスタンスの WLC によって送信されます。Web 認証では、WLC が AAA サーバからの認証応答で WLAN ID を受信したときに、WLAN の ID と一致しなかった場合には、認証は拒否されます。他のタイプのセキュリティ方式では、これは実行されません。

- **DSCP 値** : RADIUS Access Accept に含まれる場合、WLAN プロファイルに設定された DSCP 値が上書きされます。
- **802.1p タグ** : RADIUS Access Accept に含まれる場合、WLAN プロファイルに設定されたデフォルト値が上書きされます。

注 : VLAN機能は、MACフィルタリング、802.1X、およびWi-Fi Protected Access(WPA)のみをサポートします。Web 認証または IPSec はサポートされていません。インターフェイス名に対応するために、オペレーティングシステムのロカール MAC フィルタ データベースが拡張されています。その結果、ローカル MAC フィルタでは、クライアントに割り当てる必要があるインターフェイスを指定できるようになりました。別個の RADIUS サーバも使用できますが、Security メニューを使用して、その RADIUS サーバを定義する必要があります。

アイデンティティ ネットワーキングの詳細は、「[ID ネットワーキングの設定](#)」を参照してください。

[Airespace VSA用のIASの設定](#)

Airespace VSAのIASを設定するには、次の手順を実行する必要があります。

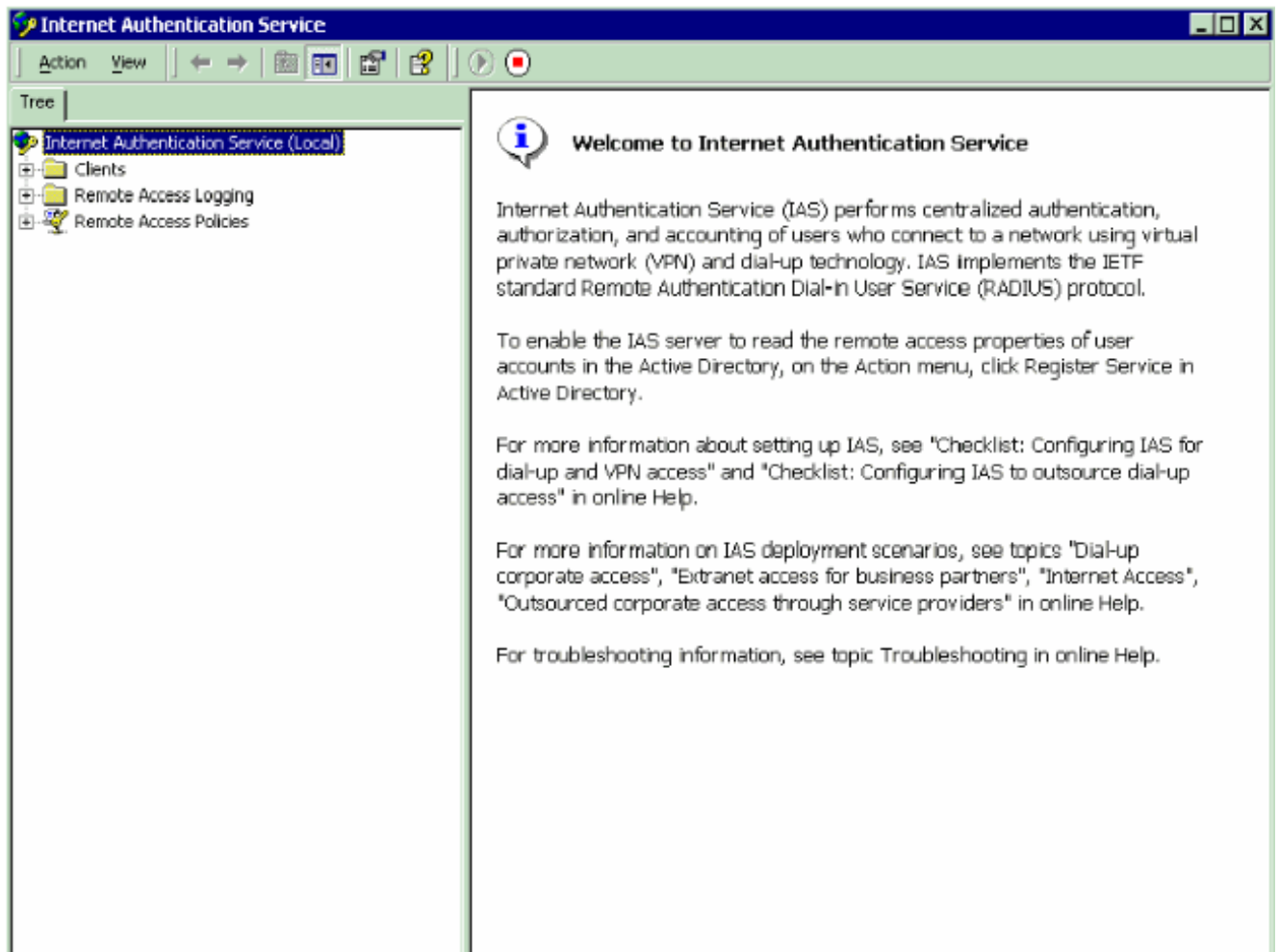
1. [IASでAAAクライアントとしてWLCを設定する](#)
2. [IASでリモートアクセスポリシーを設定する](#)

注 : VSAはリモートアクセスポリシーで設定されます。

[IASでAAAクライアントとしてWLCを設定する](#)

IASでAAAクライアントとしてWLCを設定するには、次の手順を実行します。

1. [Programs] > [Administrative Tools] > [Internet Authentication Service] の順に選択し、Microsoft 2000 サーバ上で IAS を起動します。



2. [Clients] フォルダを右クリックし、[New Client] を選択して、新しい RADIUS クライアントを追加します。
3. [Add Client] ウィンドウで、クライアントの名前を入力し、プロトコルとして [RADIUS] を選択します。次に、[Next] をクリックします。この例では、クライアントの名前は *WLC-1* です。注：デフォルトでは、プロトコルは RADIUS に設定されています。

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. [Add RADIUS Client] ウィンドウで、クライアント IP アドレス、クライアントのベンダー、および秘密共有鍵を入力します。クライアント情報を入力したら、[Finish] をクリックします。この例では、クライアントの名前は *WLC-1* であり、IP アドレスは *172.16.1.30*、クライアントのベンダーは *Cisco*、秘密共有鍵は *cisco123* と、それぞれ設定されています。

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]

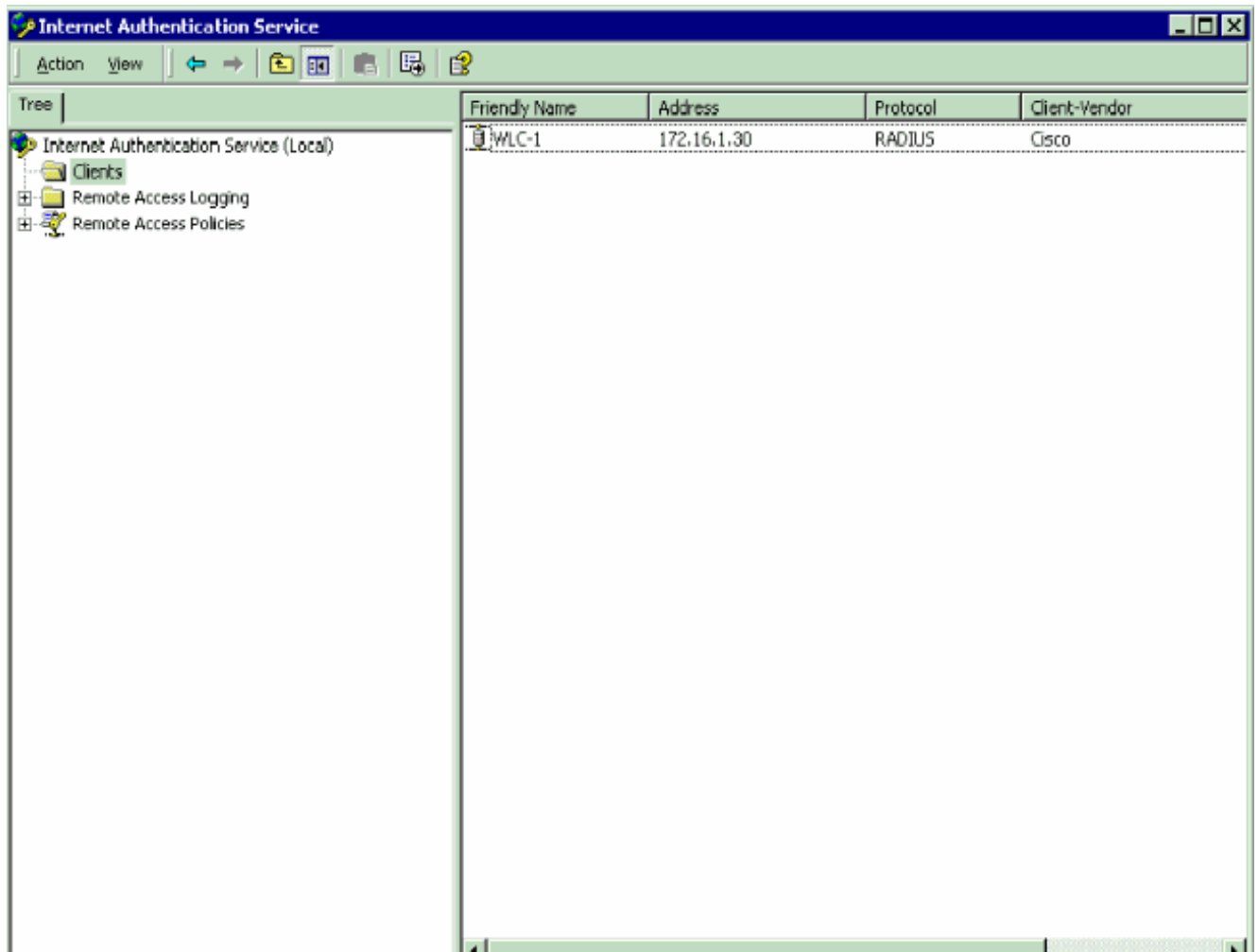
Client must always send the signature attribute in the request

Shared secret: [xxxxxxxx]

Confirm shared secret: [xxxxxxxx]

< Back Finish Cancel

この情報によって、IAS サーバの AAA クライアントとして、WLC-1 と名付けられた WLC が追加されます。

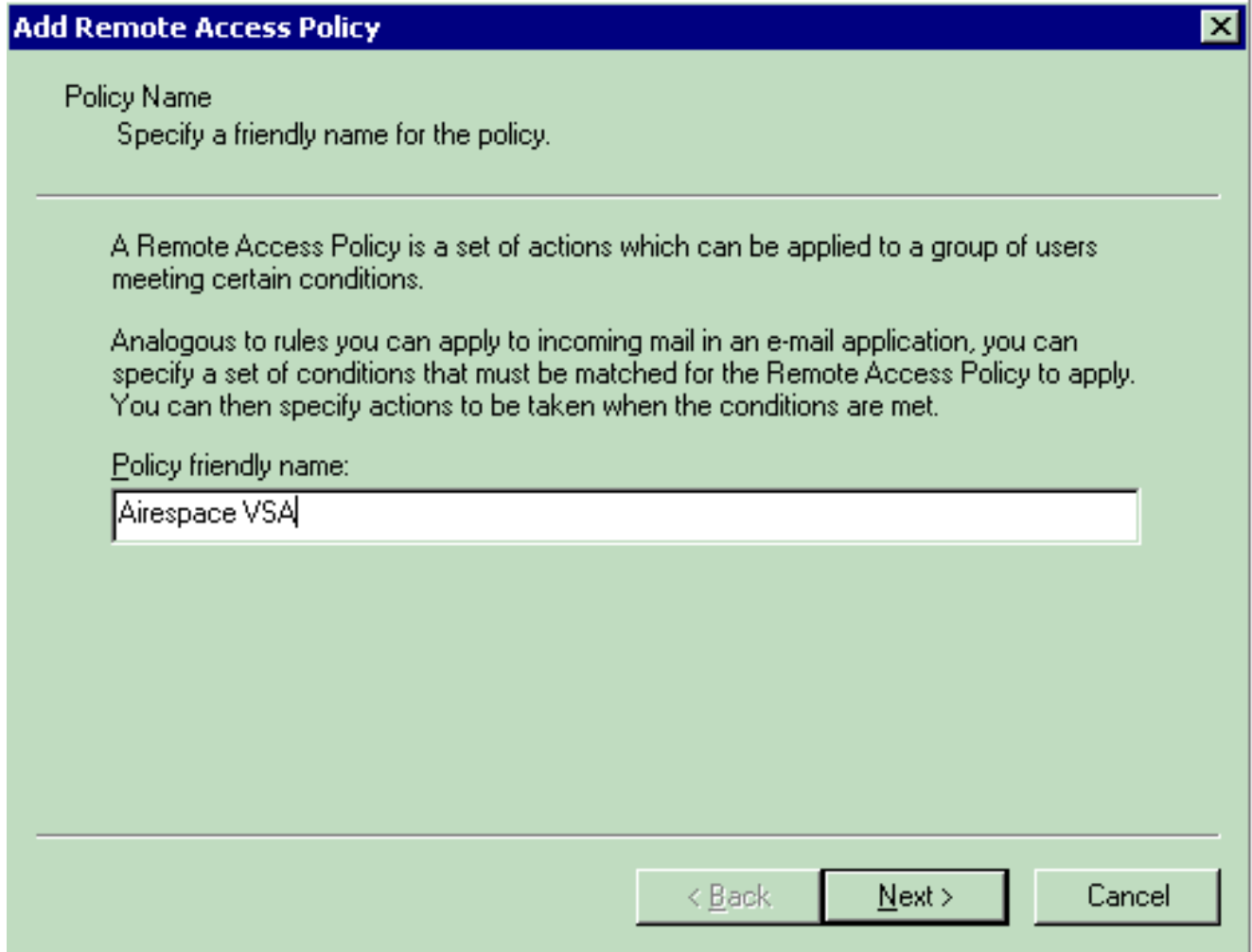


次の手順では、リモート アクセス ポリシーを作成し、VSA を設定します。

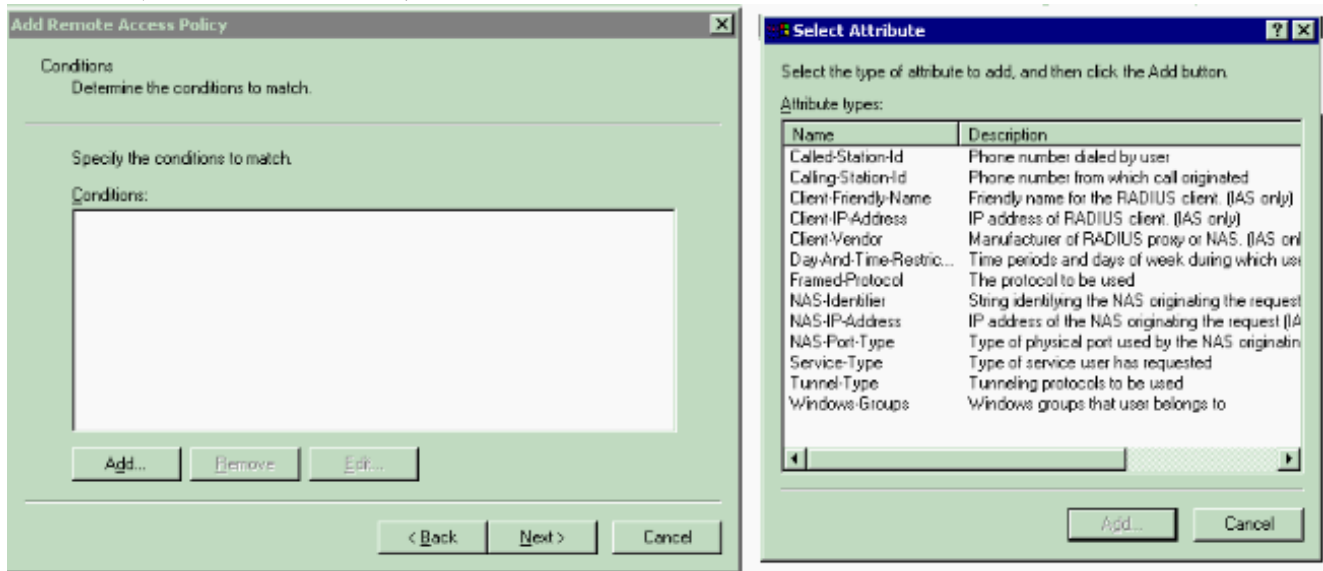
[IASでリモートアクセスポリシーを設定する](#)

IASで新しいリモートアクセスポリシーを設定するには、次の手順を実行します。

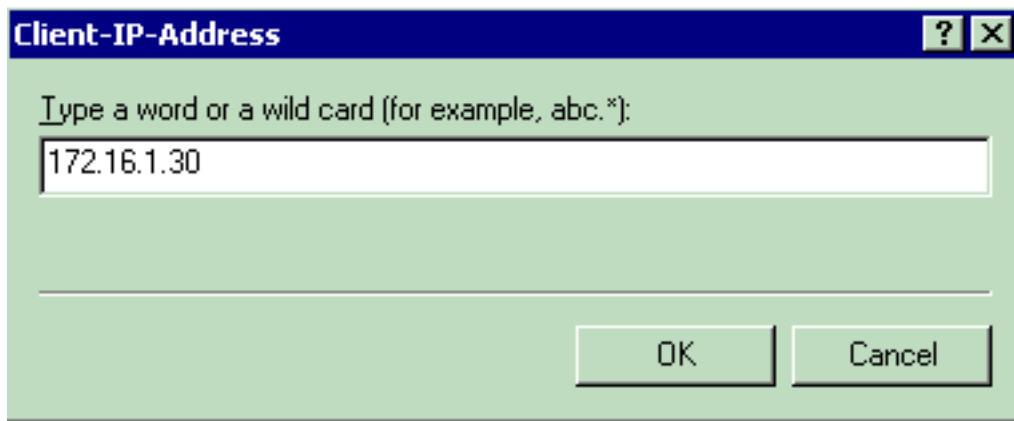
1. [リモートアクセスポリシー]を右クリックし、[新しいリモートアクセスポリシー]を選択します。[Policy Name] ウィンドウが表示されます。
2. ポリシーの名前を入力し、[Next] をクリックします。



3. 次のウィンドウで、リモート アクセス ポリシーが適用される条件を選択します。[Add] をクリックし、条件を選択します。

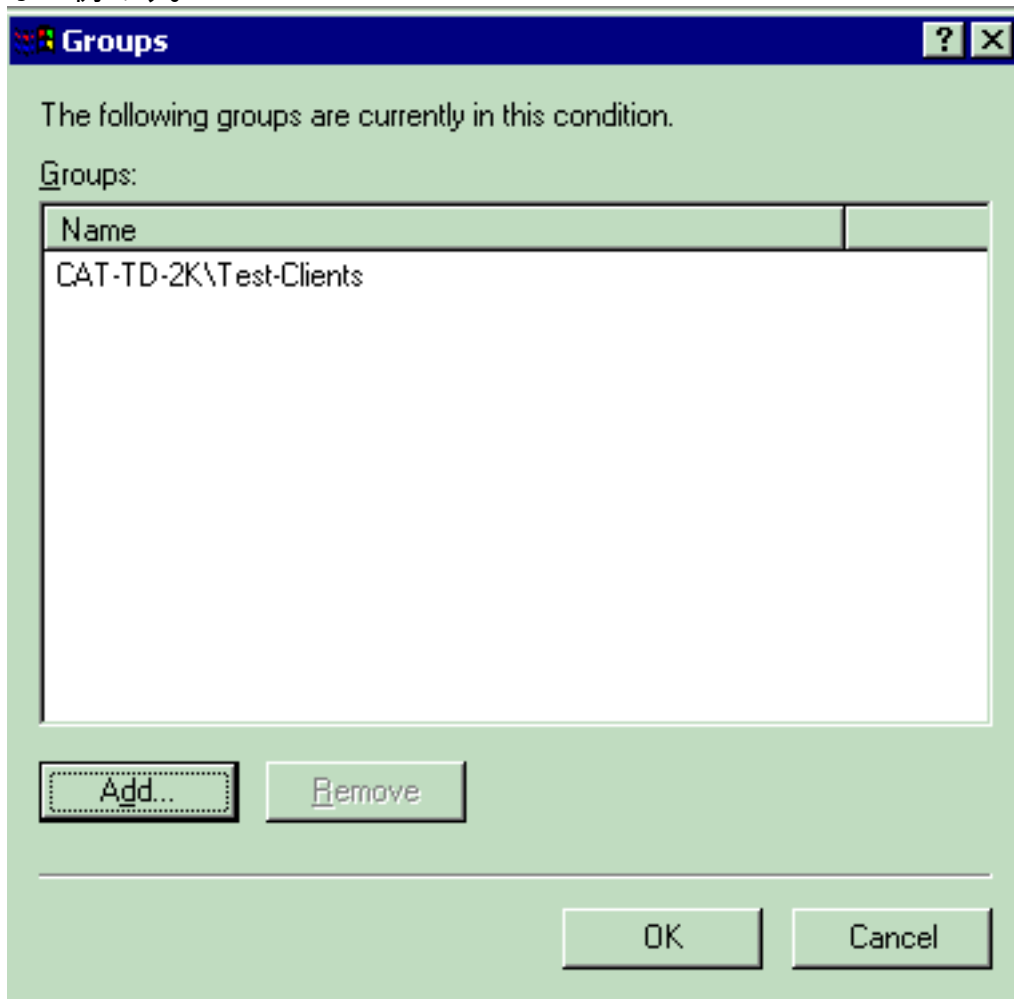


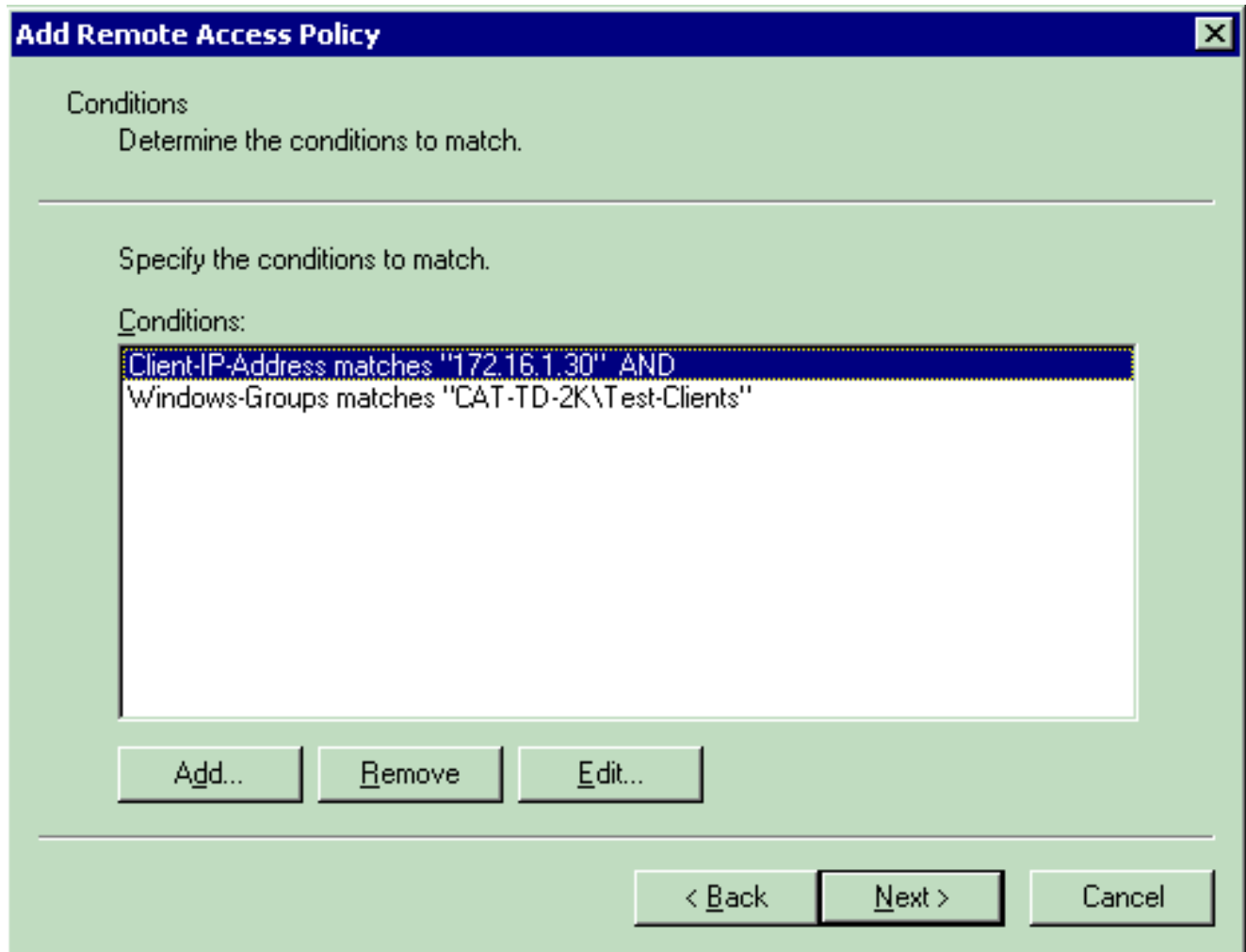
4. [Attribute types] メニューから、次の属性を選択します。[Client-IP-Address] : AAA クライアントの IP アドレスを入力します。この例では、WLC から送信されるパケットにポリシーが適用されるように、WLC の IP アドレスが入力されています。



[Windows

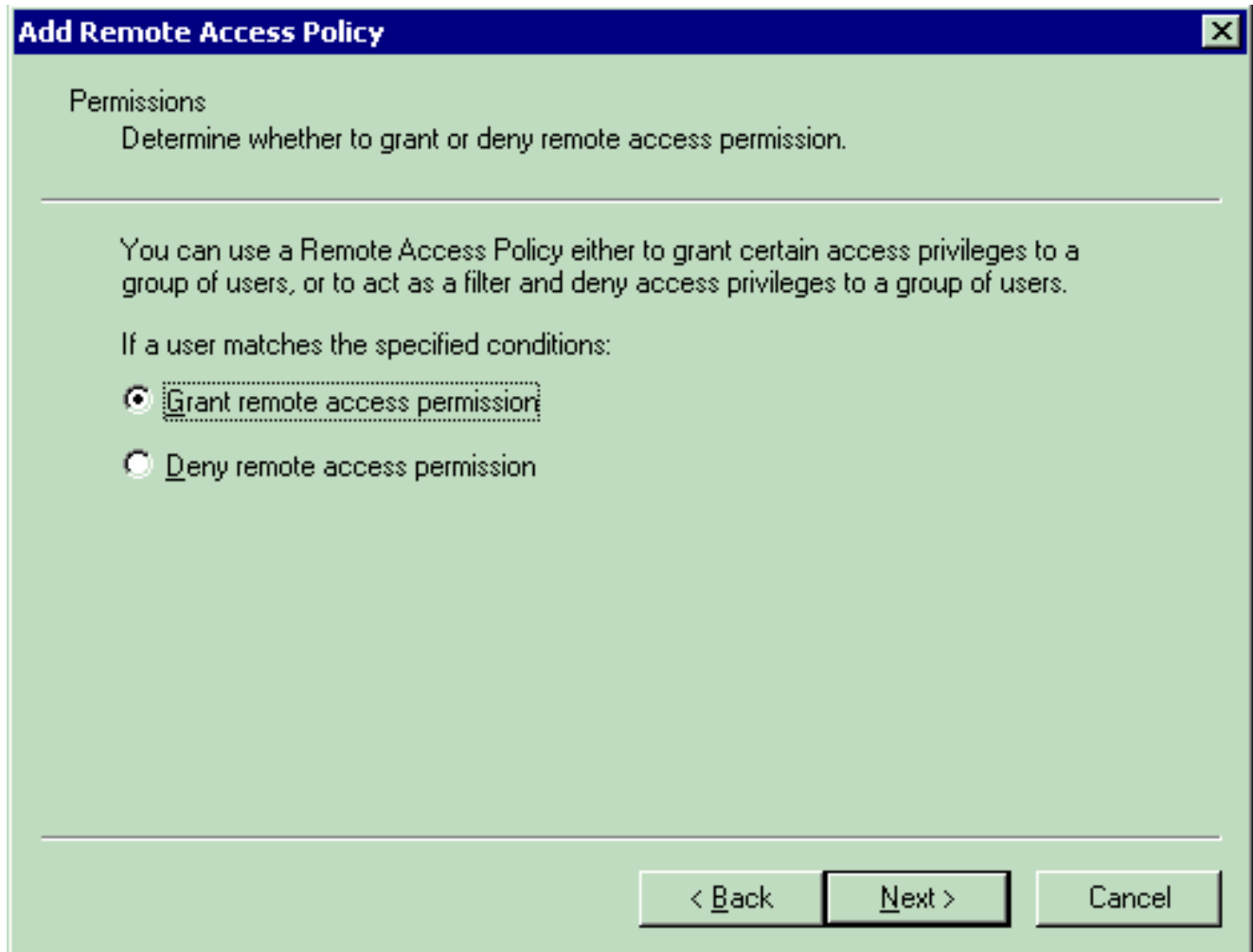
Groups] : ポリシーが適用される Windows グループ (ユーザグループ) を選択します。以下が一例です。



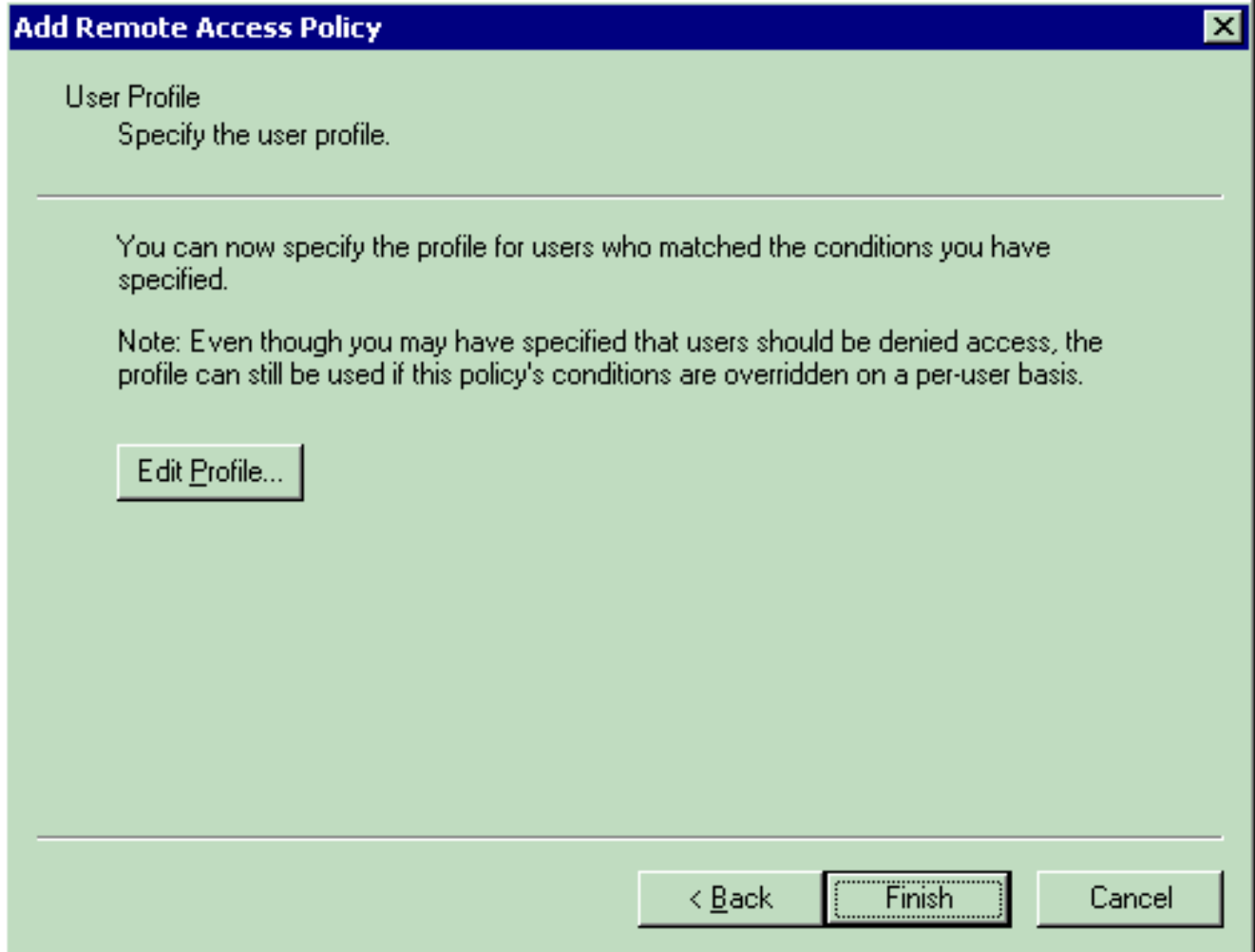


この例では、2つの条件が選択されています。さらに条件を増やすには、同じように条件を追加し、[Next] をクリックします。[Permissions] ウィンドウが表示されます。

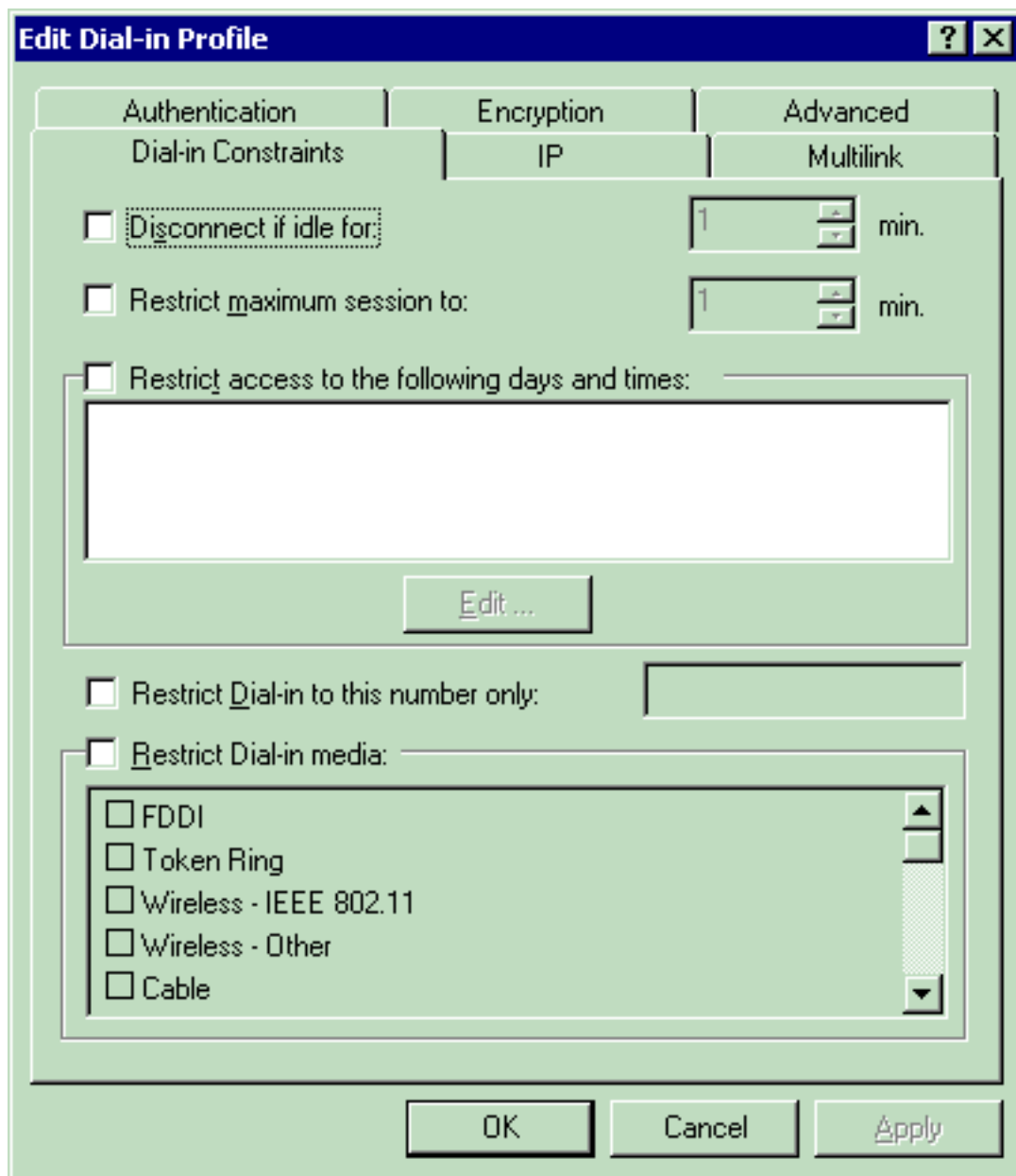
5. [Permissions] ウィンドウで、[Grant remote access permission] を選択します。このオプションを選択すると、(手順2で) 指定された条件に一致するユーザには、アクセスが提供されます。



6. [next] をクリックします。
7. 次の手順に従って、ユーザ プロファイルを設定します。条件に基づいて、アクセスを拒否または許可するユーザを指定した場合であっても、ユーザ単位でポリシーの条件が上書きされる場合には、従来どおりプロファイルを使用する必要があります。

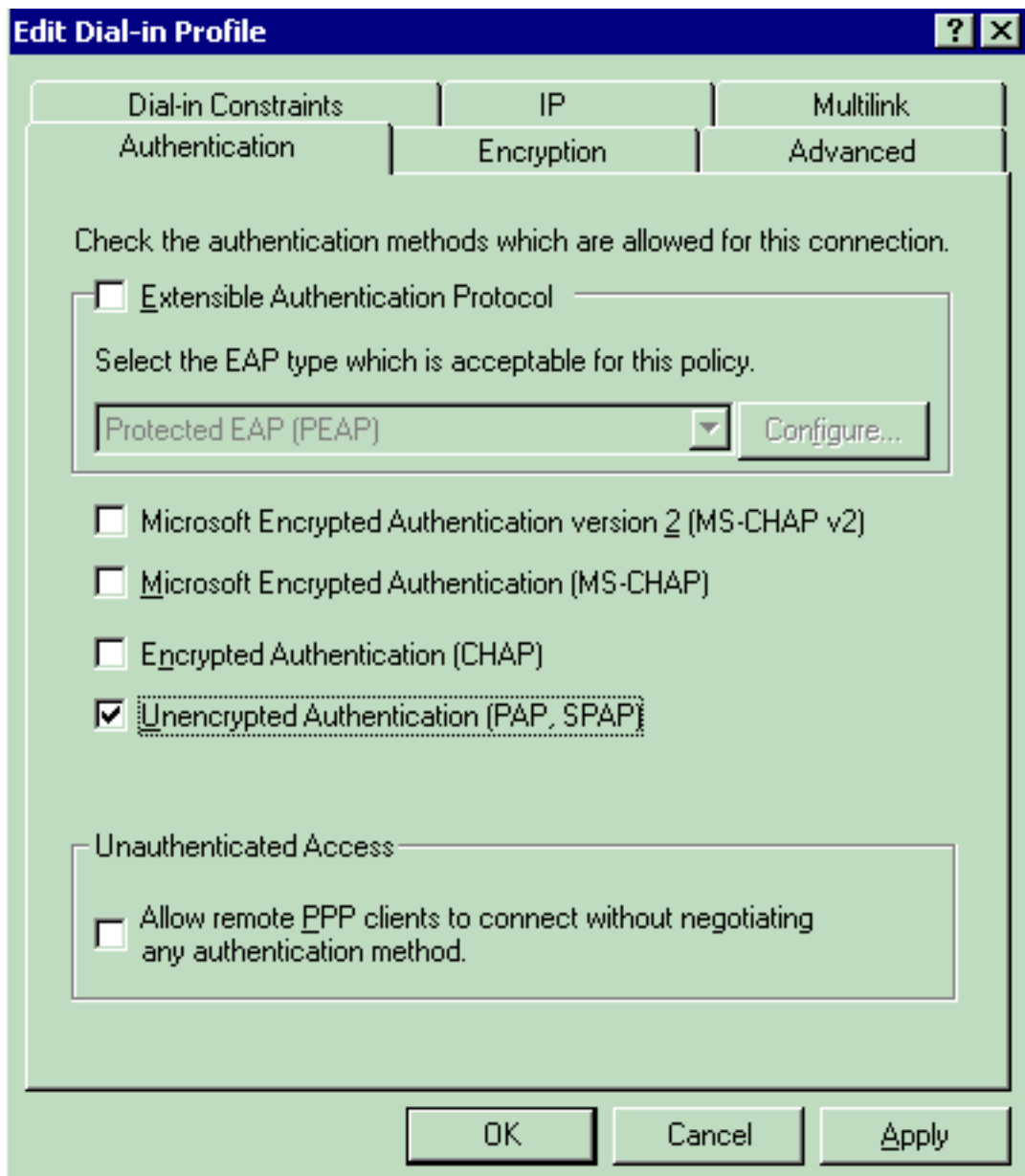


ユーザ プロファイルを設定するには、[User Profile] ウィンドウで、[Edit Profile] をクリックします。[Edit Dial-in Profile] ウィンドウが表示されます。



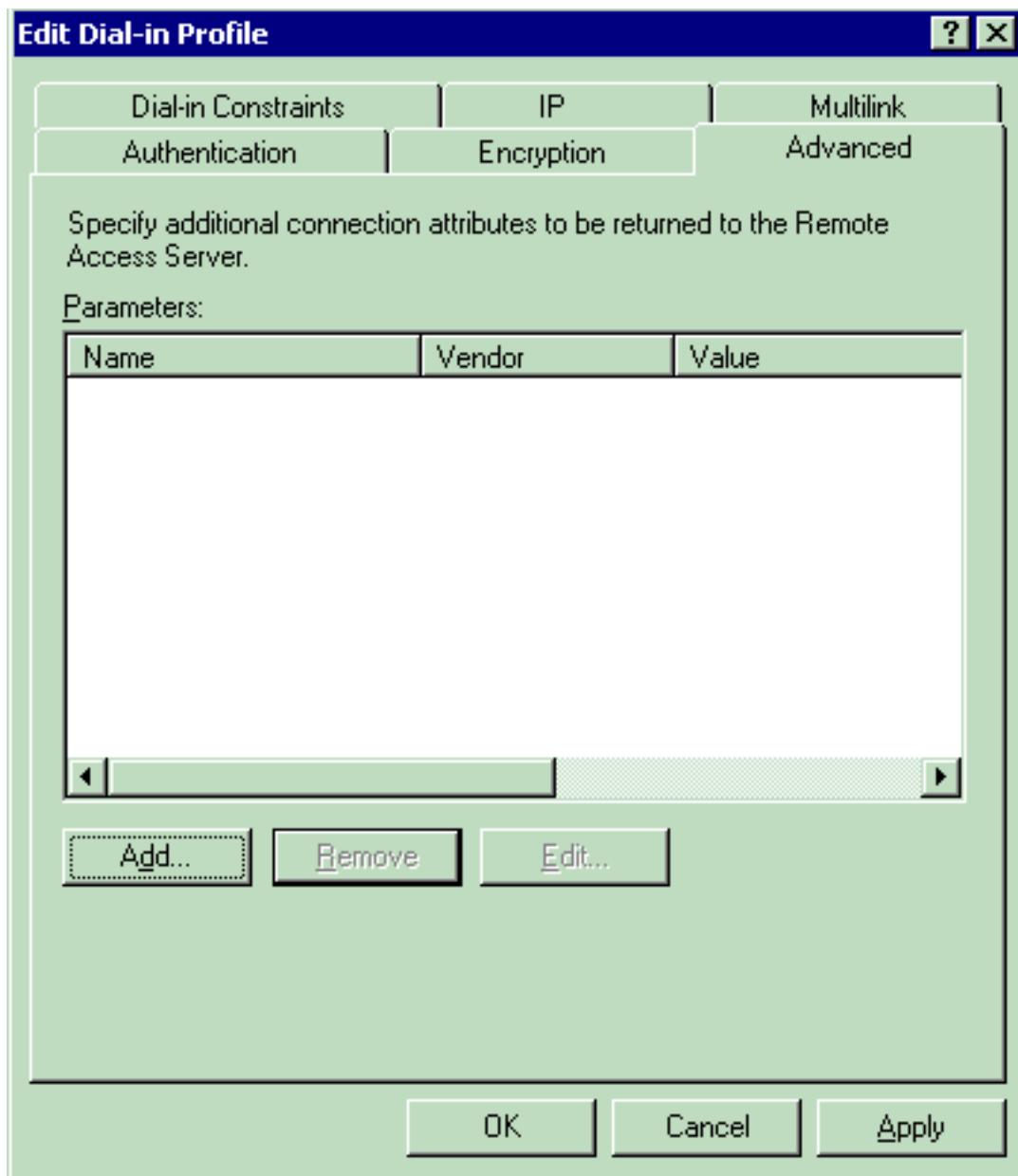
[Authentication]

タブをクリックし、WLAN に使用する認証方式を選択します。この例では、[Unencrypted Authentication (PAP,SPAP)] が選択されています。



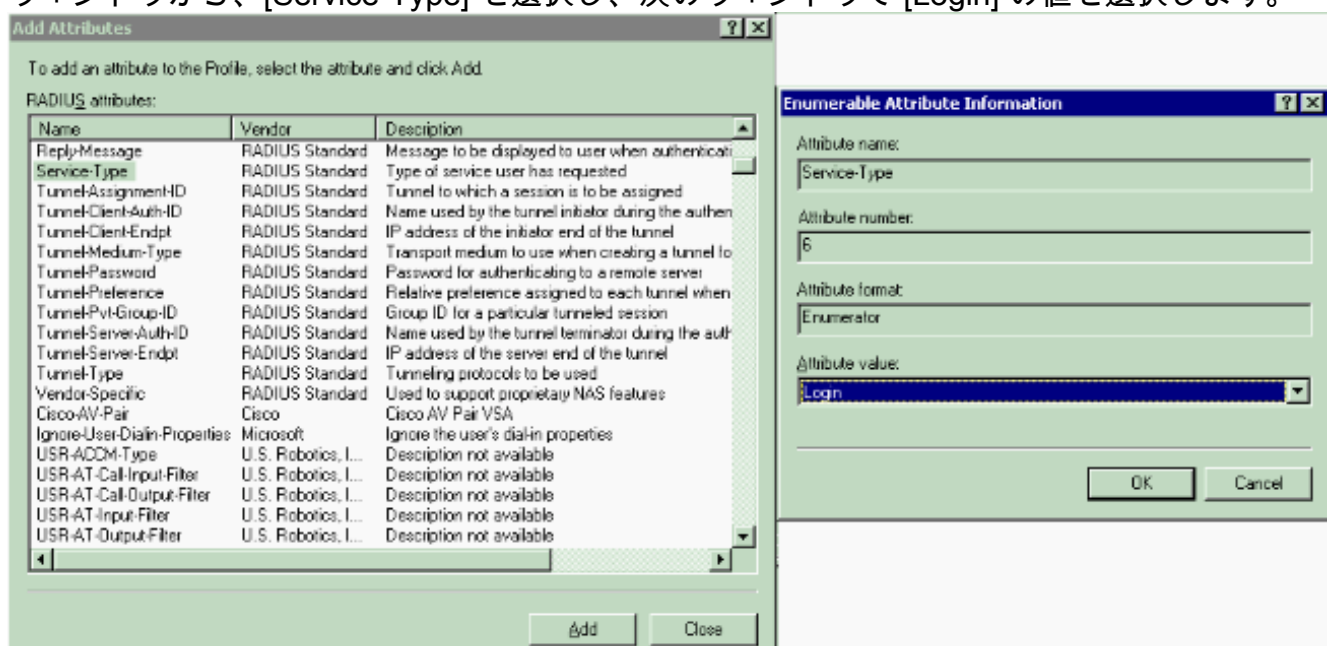
[Advanced] タブ

をクリックします。デフォルトのパラメータをすべて削除し、[Add] をクリックします。

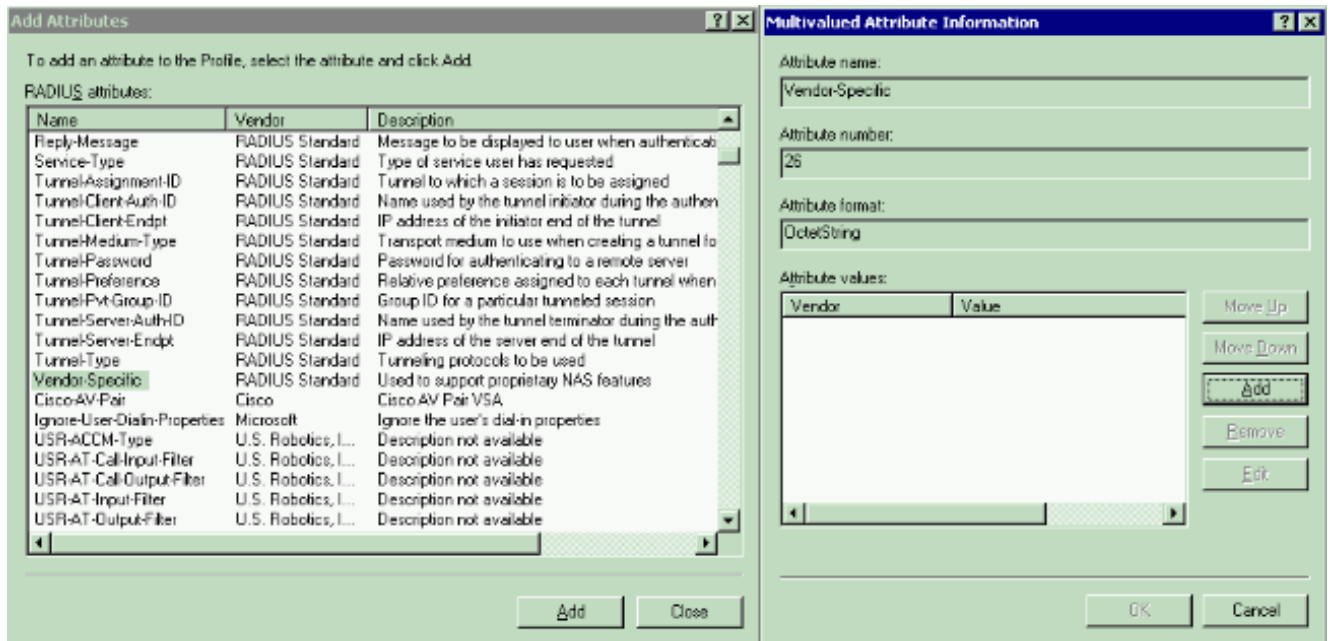


[Add Attributes]

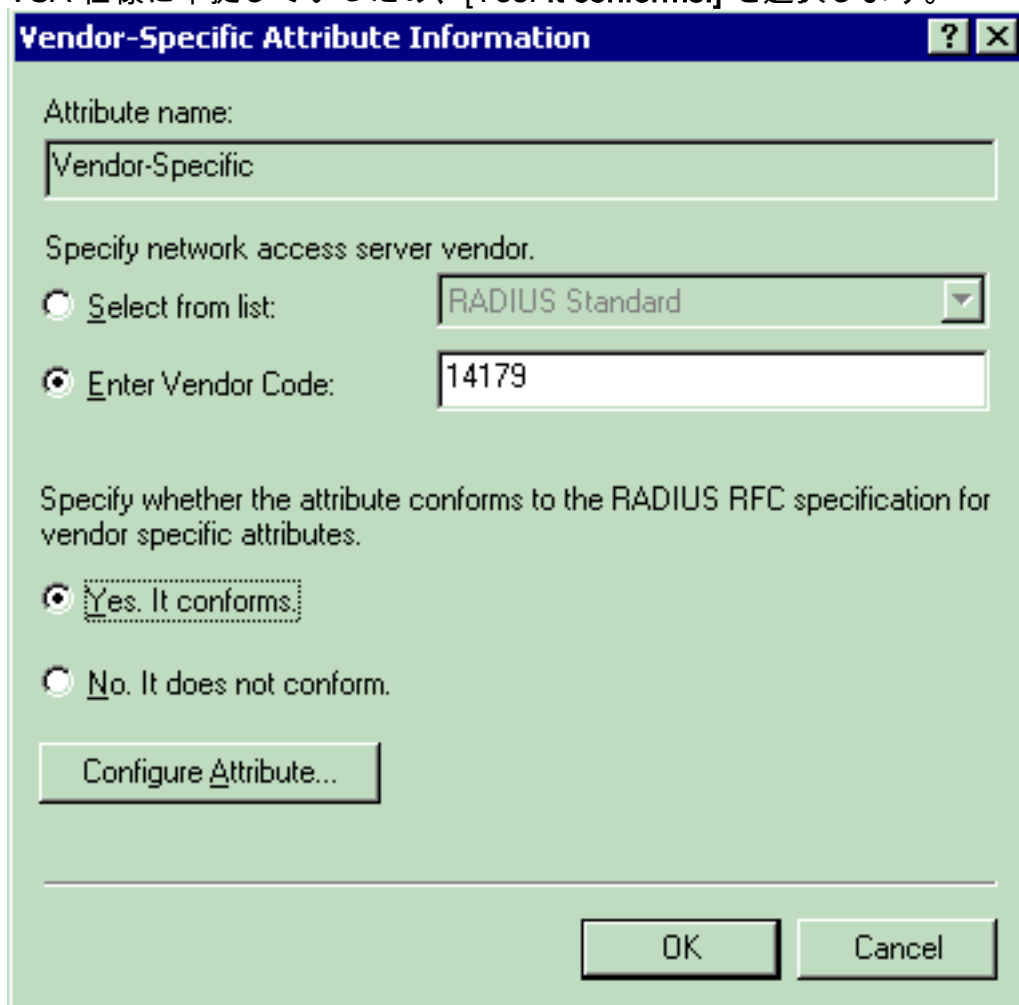
ウィンドウから、[Service-Type] を選択し、次のウィンドウで [Login] の値を選択します。



次に、RADIUS の属性リストから、[Vendor-Specific] を選択します。

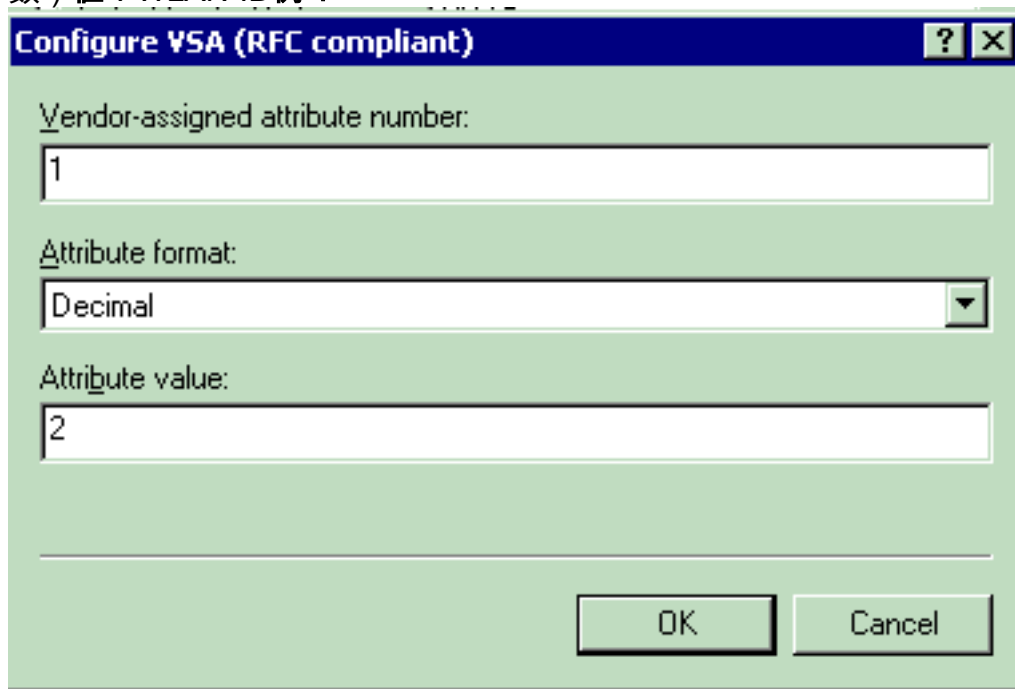


次のウィンドウで、[Add] をクリックして、新しい VSA を追加します。[Vendor-Specific Attribute Information] ウィンドウが表示されます。[Specify network access server vendor] の下で、[Enter Vendor Code] を選択します。Airespace VSA のベンダーコードを入力します。Cisco Airespace VSA のベンダーコードは 14179 です。この属性は、RADIUS RFC の VSA 仕様に準拠しているため、[Yes. It conforms.] を選択します。

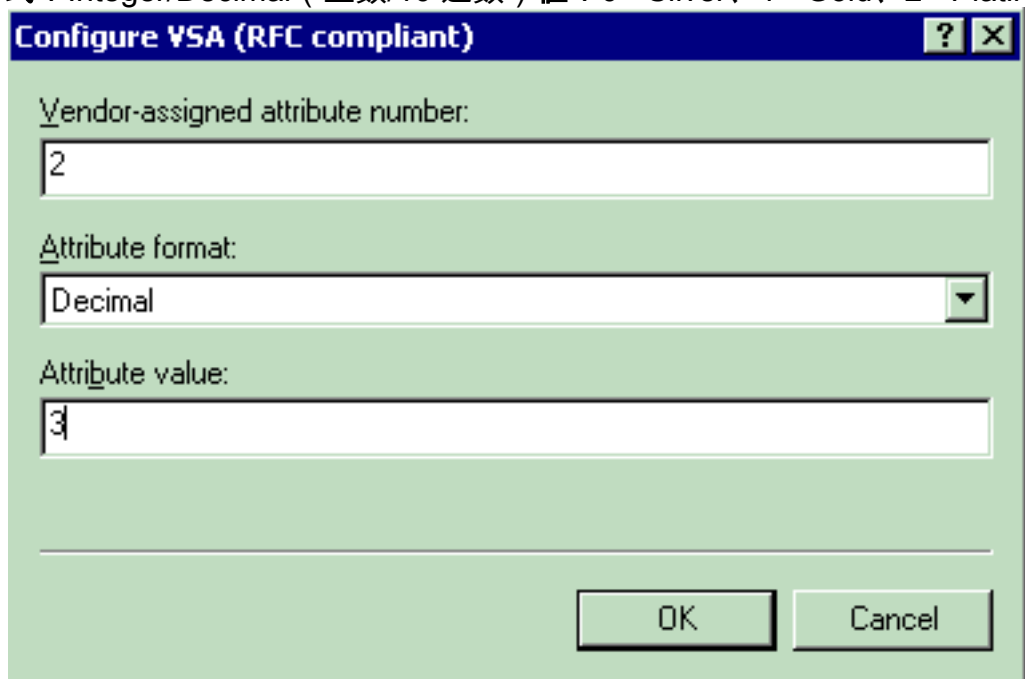


[Configure Attribute] をクリックします。[Configure VSA (RFC compliant)] ウィンドウで、ベンダーに割り当てられる属性番号、属性の形式、および属性値を入力します。実際の値は、使用する VSA によって異なります。ユーザごとに、次のように WLAN-ID を設定します。属性名：Airespace-WLAN-Idベンダーに割り当てられる属性番号：1属性の形式：Integer/Decimal (整数/10進

数) 値 : WLAN-ID例 1



ユーザーごとに、次のように QoS を設定します。属性名 : Airespace-QoS-Levelベンダーに割り当てられる属性番号 : 2属性の形式 : Integer/Decimal (整数/10 進数) 値 : 0 - Silver、1 - Gold、2 - Platinum、



3 - Bronze例 2

ユーザーごとに、次のように DSCP を設定します。属性名 : Airespace-DSCPベンダーに割り当てられる属性番号 : 3属性の形式 : Integer/Decimal (整数/10 進数) 値 : DSCP 値例 3

Configure VSA (RFC compliant)

Vendor-assigned attribute number:
3

Attribute format:
Decimal

Attribute value:
46

OK Cancel

ユーザごとに、次のように 802.1p タグを設定します。属性名：Airespace-802.1p-Tagベンダーに割り当てられる属性番号：4属性の形式：Integer/Decimal (整数/10 進数) 値：802.1p-Tag例 4

Configure VSA (RFC compliant)

Vendor-assigned attribute number:
4

Attribute format:
Decimal

Attribute value:
5

OK Cancel

ユーザごとに、次のように VLAN を設定します。属性名：Airespace-Interface-Nameベンダーに割り当てられる属性番号：5属性の形式：String (文字列) 値：インターフェイス名例 5

Configure VSA (RFC compliant)

Vendor-assigned attribute number:
5

Attribute format:
String

Attribute value:
vlan10

OK Cancel

ユーザごとに、次のように ACL を設定します。属性名 : Airespace-ACL-Nameベンダーに割り当てられる属性番号 : 6属性の形式 : String (文字列) 値 : ACL 名例 6

Configure VSA (RFC compliant)

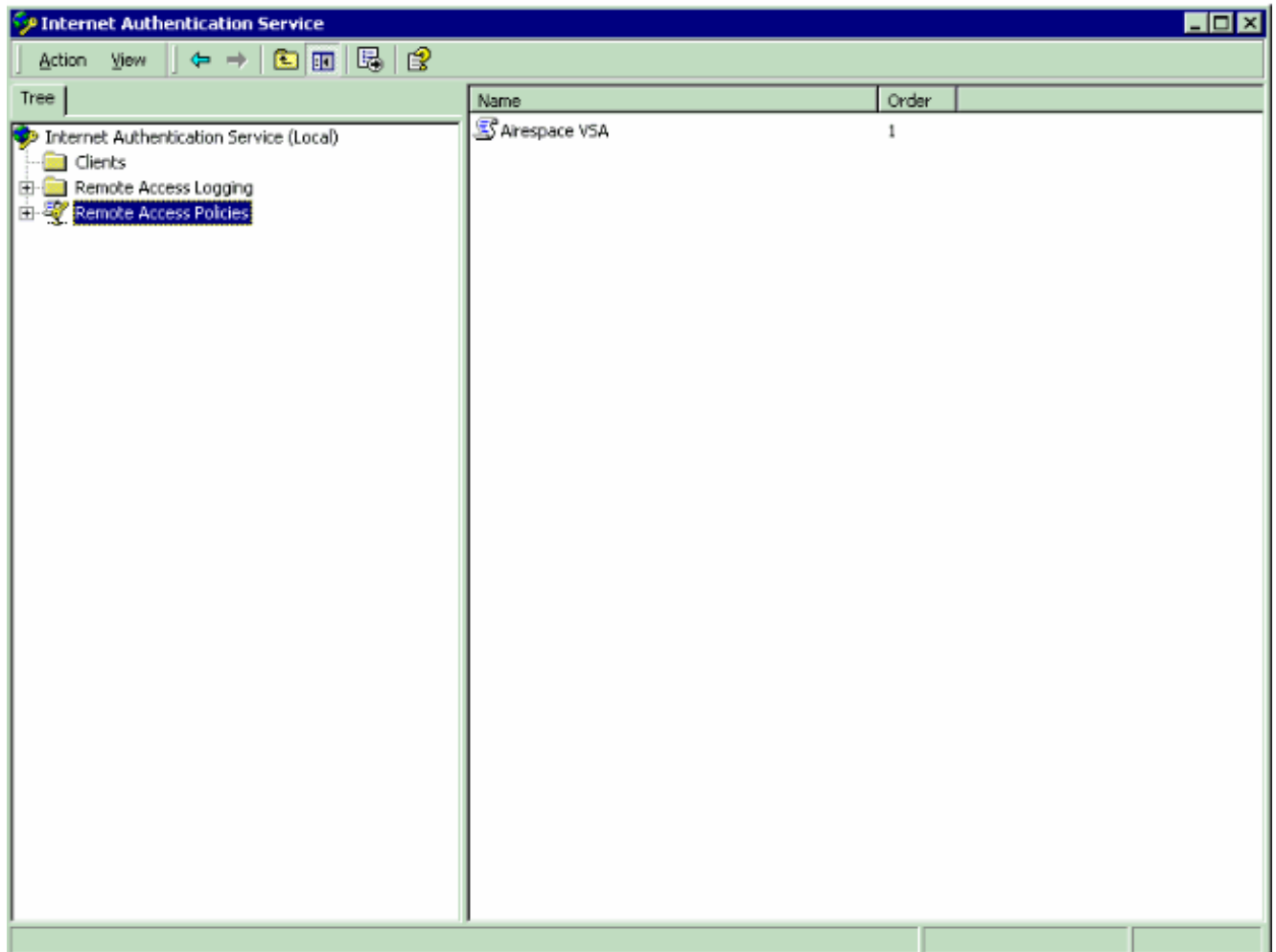
Vendor-assigned attribute number:
6

Attribute format:
String

Attribute value:
ACL1

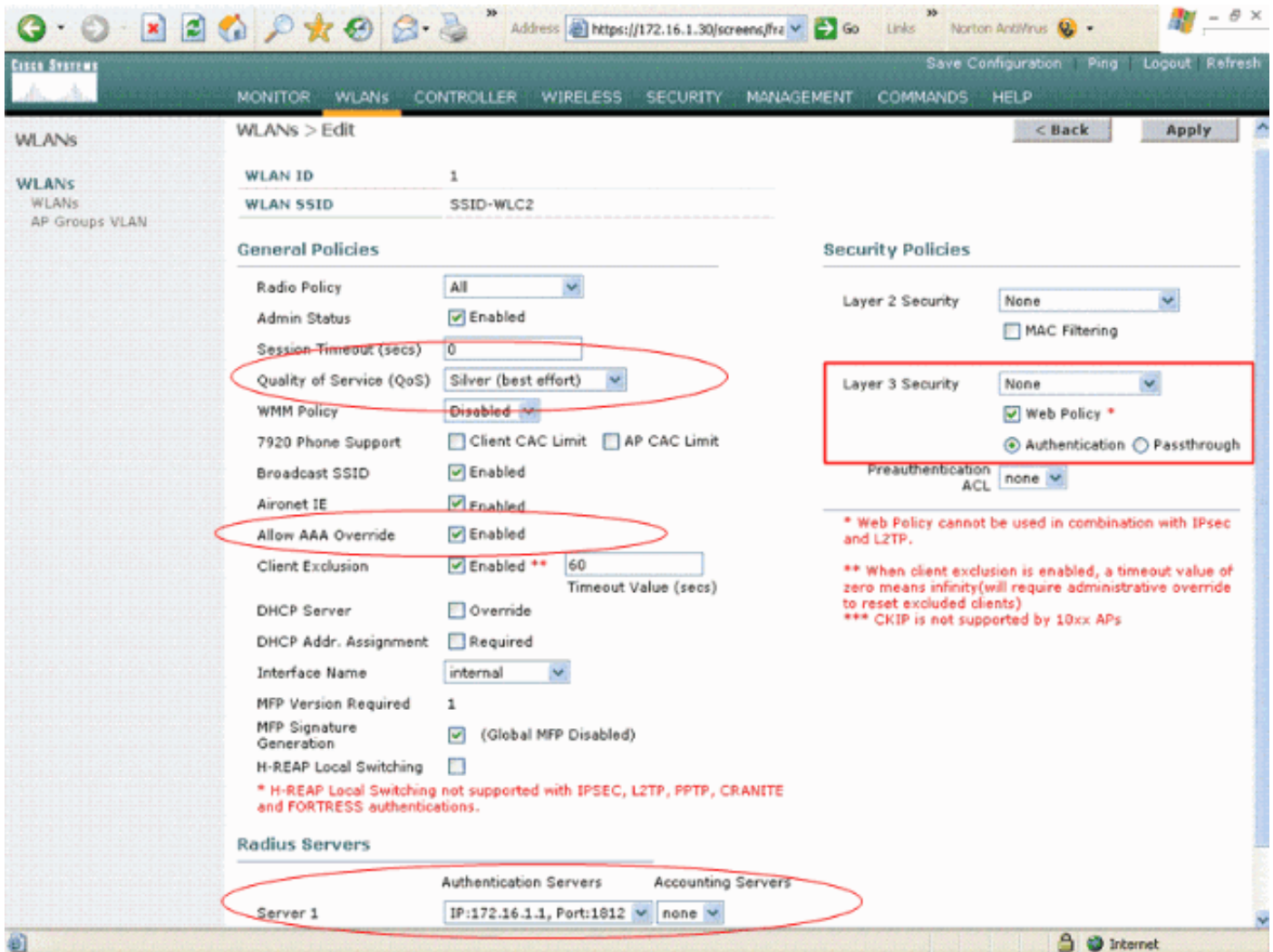
OK Cancel

- VSA の設定が完了したら、[OK] をクリックします。やがて、ユーザ プロファイル ウィンドウが表示されます。
- [Finish] をクリックして、設定を完了します。リモート アクセス ポリシーの下に新しいポリシーが表示されています。



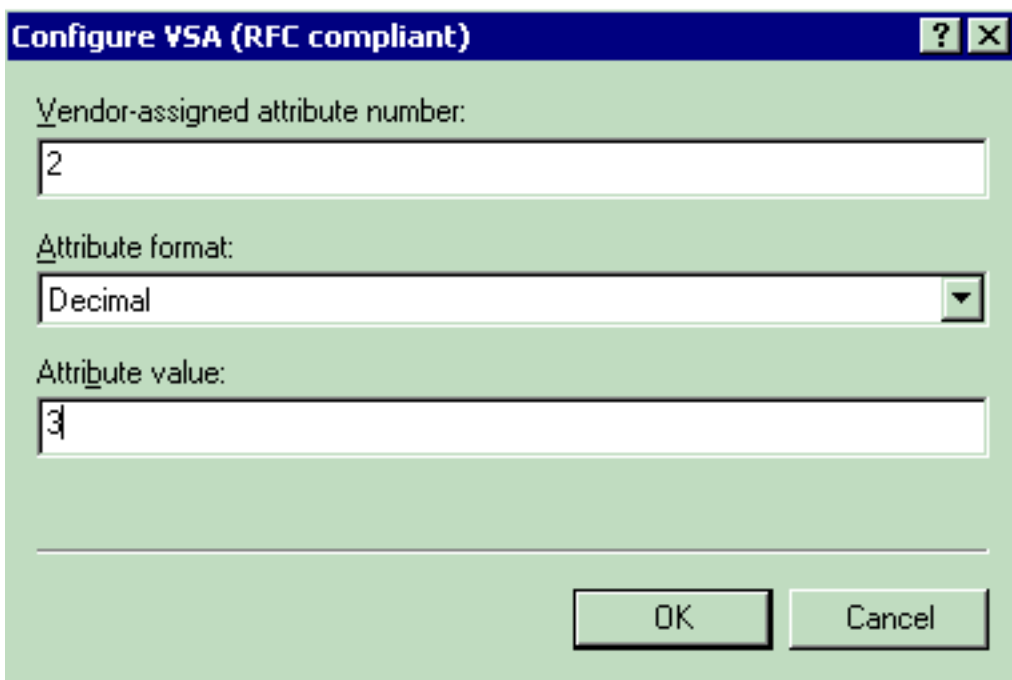
設定例

この例では、WLANはWeb認証用に設定されています。ユーザはIAS RADIUSサーバによって認証され、RADIUSサーバはユーザごとにQoSポリシーを割り当てるように設定されます。



ウィンドウに表示されているように、Web 認証がイネーブルにされています。認証サーバは 172.16.1.1 で、WLAN では、AAA Override もイネーブルにされています。この WLAN のデフォルトの QoS は、Silver に設定されています。

IAS RADIUS サーバでは、RADIUS Access Accept 要求に Bronze の QoS 属性を返すように、リモート アクセス ポリシーが設定されています。これは、QoS 属性専用 VSA を設定するときに実施されます。



IASサーバでリモートアクセスポリシーを設定する方法の詳細については、このドキュメントの「[IASのリモートアクセスポリシーの設定](#)」セクションを参照してください。

IASサーバ、WLC、およびLAPがこのセットアップ用に設定されると、ワイヤレスクライアントはWeb認証を使用して接続できます。

確認

ここでは、設定が正常に機能しているかどうかを確認します。

ユーザがユーザIDとパスワードを使用してWLANに接続すると、WLCはクレデンシャルをIAS RADIUSサーバに渡し、IAS RADIUSサーバはリモートアクセスポリシーで設定された条件とユーザプロファイルに対してユーザを認証します。ユーザ認証に成功した場合には、RADIUSサーバは、AAA Override 値も含む RADIUS Accept 要求を返します。この場合には、ユーザの QoS ポリシーが返されます。

認証中に発生するイベントのシーケンスを参照するために、**debug aaa all enable** コマンドを発行できます。次に出力例を示します。

```
(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)
```

出力結果から、ユーザが認証されていることが確認できます。また、RADIUS の Accept メッセージとともに、AAA Override 値が返されています。この例では、ユーザには Bronze の QoS ポリシーが与えられています。

これは、WLC GUI でも同じように確認できます。以下が一例です。

The screenshot shows the Cisco Systems WLC configuration page for a client. The page 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 (highlighted in red)
 - Diff Serv Code Point (DSCP): disabled
 - 802.1p Tag: disabled
 - Average Data Rate: disabled

注：このSSIDのデフォルトQoSプロファイルはSilverです。ただし、AAA Overrideが選択され、ユーザはIASサーバでBronzeのQoSプロファイルを使用して設定されているため、デフォルトのQoSプロファイルは上書きされます。

トラブルシューティング

WLCで `debug aaa all enable` コマンドを使用すると、設定のトラブルシューティングを行うことができます。稼働中のネットワークにおけるこのデバッグの出力例は、このドキュメントの「[確認](#)」セクションで参照できます。

注：[debug](#) コマンドを使用する前に、『[debug コマンドの重要な情報](#)』を参照してください。

関連情報

- [Cisco ワイヤレス LAN コントローラ コンフィギュレーション ガイド、リリース 4.0](#)
- [WLC と Cisco Secure ACS を使用した SSID に基づく WLAN アクセス制限の設定例](#)
- [ワイヤレス製品に関するサポート](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)