

Les VSAs de Cisco Airespace sur l'exemple de configuration du serveur RADIUS de Microsoft IAS

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Informations générales](#)

[Configurez IAS pour les VSAs d'Airespace](#)

[Configurez le WLC en tant que client d'AAA sur IAS](#)

[Configurez la stratégie d'accès à distance sur IAS](#)

[Exemple de configuration](#)

[Vérifiez](#)

[Dépannez](#)

[Informations connexes](#)

Introduction

Ce document t'affiche comment configurer un serveur de Service d'authentification Internet de Microsoft (IAS) pour prendre en charge les attributs spécifiques de constructeur de Cisco Airespace (les VSAs). Le code de constructeur pour les VSAs de Cisco Airespace est **14179**.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- La connaissance de la façon configurer un serveur d'IAS
- La connaissance de la configuration du Point d'accès léger (recouvrements) et des contrôleurs LAN Sans fil de Cisco (WLCs)
- La connaissance des solutions de sécurité de Cisco Unified Wireless

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Serveur de Microsoft Windows 2000 avec IAS
- Cisco 4400 WLC qui exécute la version de logiciel 4.0.206.0
- LAP de la gamme Cisco 1000
- adaptateur client sans fil du 802.11 a/b/g avec le micrologiciel 2.5
- Utilitaire de bureau Aironet (ADU) version 2.5

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Remarque: Ce document est destiné pour donner au lecteur un exemple sur la configuration exigée sur le serveur d'IAS pour prendre en charge les VSAs de Cisco Airespace. La configuration du serveur d'IAS présentée dans ce document a été testée dans le laboratoire et fonctionne comme prévue. Si vous avez le problème configurant le serveur d'IAS, contactez Microsoft pour l'aide. TAC de Cisco ne prend pas en charge la configuration du serveur de Microsoft Windows.

Ce document suppose que WLC est configuré pour les opérations de base et que les LAP sont enregistrés au WLC. Si vous êtes un nouvel utilisateur qui essaie d'installer le WLC pour l'opération de base avec les LAP, consultez l'[Enregistrement léger AP \(LAP\) sur un contrôleur LAN sans fil \(WLC\)](#).

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

Informations générales

Dans la plupart des systèmes Sans fil du RÉSEAU LOCAL (WLAN), chaque WLAN a une stratégie statique qui s'applique à tous les clients associés avec un Identifiant SSID (Service Set Identifier). Bien que puissante, cette méthode a des limitations parce qu'elle exige que les clients soient associés à des SSID différents afin d'hériter de QoS et de stratégies de sécurité différentes.

Cependant, la solution LAN Sans fil de Cisco prend en charge le réseau d'identité, qui permet au réseau pour annoncer un SSID simple et des utilisateurs spécifiques pour hériter de QoS différent ou de stratégies de sécurité basées sur leurs profils utilisateurs. Les stratégies spécifiques que vous pouvez contrôler utilisant le réseau d'identité incluent :

- **Qualité de service** — Si actuel dans un RAYON Access recevez, la valeur niveau QoS ignore la valeur de QoS spécifiée dans le profil WLAN.
- **ACL** — Quand l'attribut de liste de contrôle d'accès (ACL) est présent dans le RAYON Access recevez, le système s'applique l'Acl-nom à la station client après qu'elle authentifie. Ceci ignore n'importe quel ACLs qui sont assignés à l'interface.
- **VLAN** — Quand un Interface-nom ou la VLAN-balise VLAN est présente dans un RAYON Access recevez, le système place le client sur une interface spécifique.
- **ID de WLAN** — Quand l'attribut d'ID de WLAN est présent dans le RAYON Access recevez, le système s'applique l'ID de WLAN (SSID) à la station client après qu'elle authentifie. L'ID de WLAN est envoyé par le WLC dans tous les exemples de l'authentification excepté IPSec. En cas d'authentification Web, si le WLC reçoit un attribut d'ID de WLAN dans la réponse

d'authentification du serveur d'AAA, et de elle n'apparie pas l'ID du WLAN, authentification est rejeté. D'autres types de méthodes de Sécurité ne font pas ceci.

- **Valeur DSCP** — Si actuel dans un RAYON Access recevez, la valeur DSCP ignore la valeur DSCP spécifiée dans le profil WLAN.
- **802.1p-Tag** — Si actuel dans un RAYON Access recevez, la valeur 802.1p ignore le par défaut spécifié dans le profil WLAN.

Remarque: La caractéristique VLAN prend en charge seulement le filtrage MAC, le 802.1X, et le Protocole WPA (Wi-Fi Protected Access). La caractéristique VLAN ne prend en charge pas l'authentification Web ou l'IPSec. La base de données locale du filtre d'adresses MAC du système d'exploitation a été étendue pour inclure le nom d'interface. Ceci permet aux filtres d'adresses MAC locaux pour spécifier qui relie le client devraient être assignés. Un serveur distinct de RAYON peut également être utilisé, mais le serveur de RAYON doit être défini utilisant les menus Security.

Référez-vous à [configurer le réseau d'identité](#) pour plus d'informations sur le réseau d'identité.

[Configurez IAS pour les VSAs d'Airespace](#)

Afin de configurer IAS pour les VSAs d'Airespace, vous devez se terminer ces étapes :

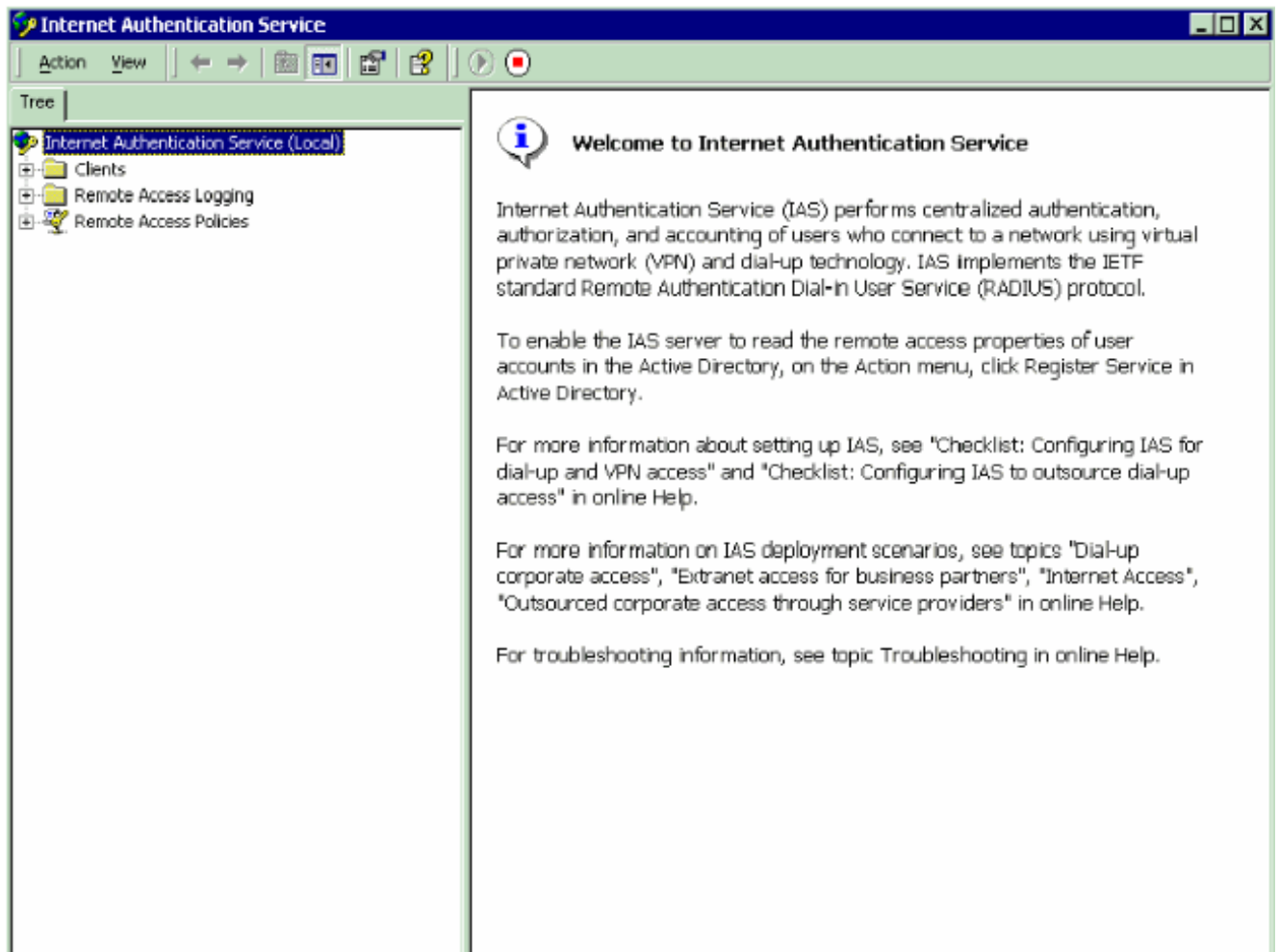
1. [Configurez le WLC en tant que client d'AAA sur IAS](#)
2. [Configurez la stratégie d'accès à distance sur IAS](#)

Remarque: Les VSAs sont configurés dans le cadre de la stratégie d'accès à distance.

[Configurez le WLC en tant que client d'AAA sur IAS](#)

Terminez-vous ces étapes afin de configurer le WLC en tant que client d'AAA sur IAS :

1. Cliquez sur les **programmes > les outils d'administration > le Service d'authentification Internet** afin de lancer IAS sur le serveur de Microsoft 2000.



2. Cliquez avec le bouton droit le répertoire de **clients** et choisissez le **nouveau client** afin d'ajouter un nouveau client RADIUS.
3. Dans la fenêtre de client d'ajouter, écrivez le nom du client et choisissez le **RAYON** comme Protocol. Cliquez ensuite sur **Next**. Dans cet exemple, le nom de client est *WLC-1*. **Remarque:** Par défaut, le protocole est placé au RAYON.

Add Client

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. Dans la fenêtre de client RADIUS d'ajouter, écrivez l'**adresse IP de client**, le **Client-constructeur**, et le **secret partagé**. Après que vous écriviez les informations de client, cliquez sur Finish. Cet exemple affiche un client nommé *WLC-1* avec une adresse IP de *172.16.1.30*, le Client-constructeur est placé à *Cisco*, et le secret partagé est *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]

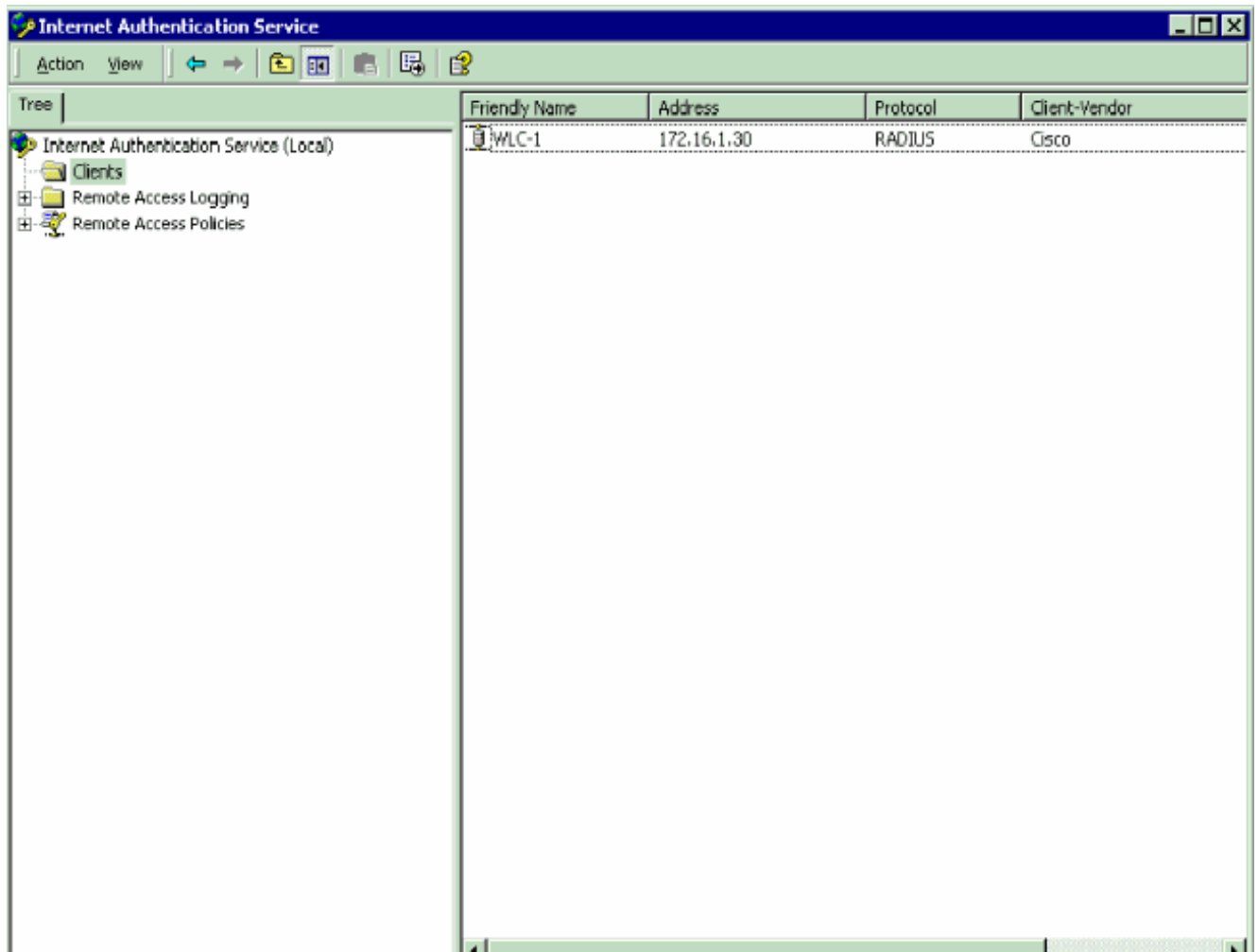
Client must always send the signature attribute in the request

Shared secret: [xxxxxxx]

Confirm shared secret: [xxxxxxx]

< Back Finish Cancel

Avec ces informations, le WLC WLC-1 nommé est ajouté comme client d'AAA du serveur d'IAS.

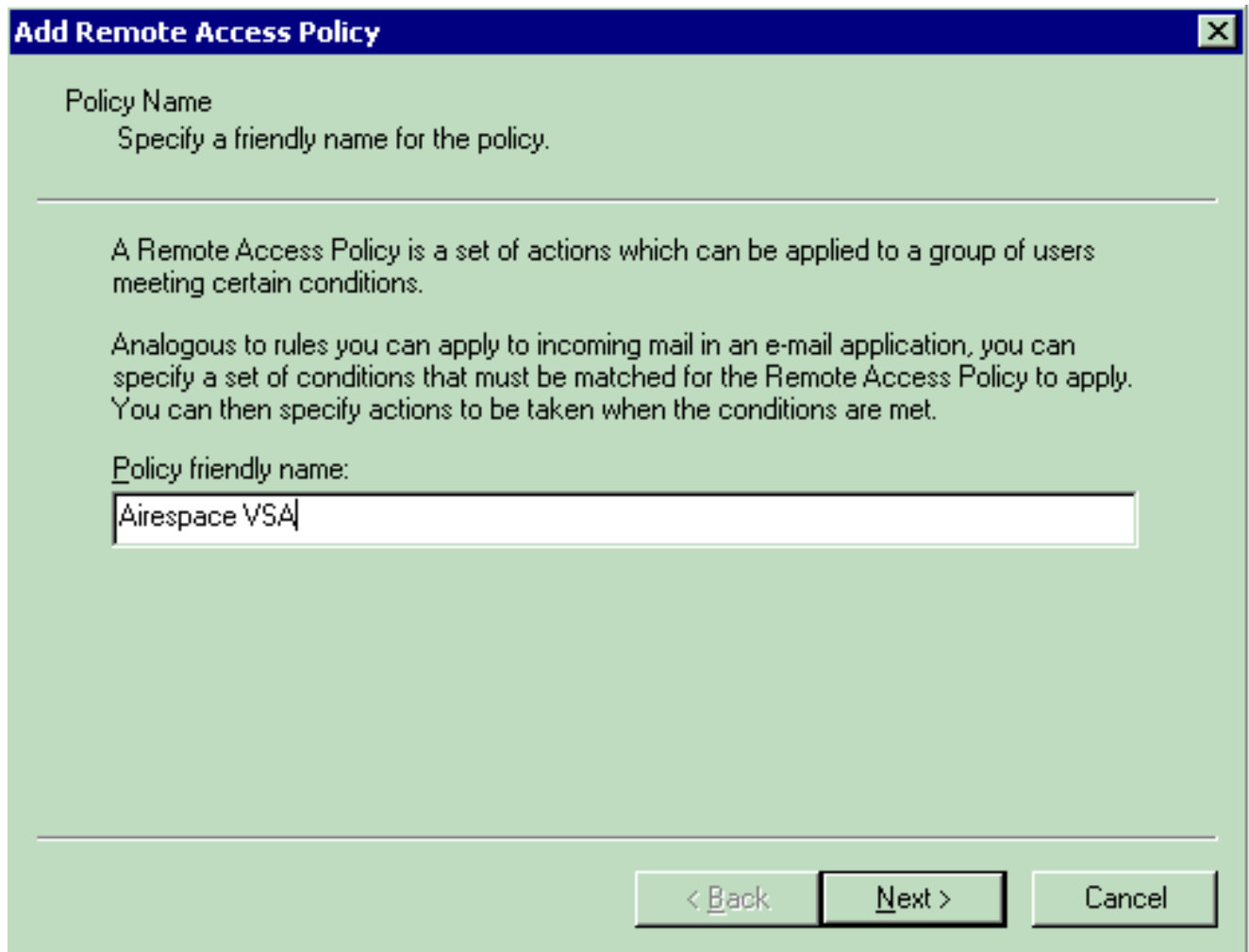


L'étape suivante est de créer une stratégie d'accès à distance et de configurer les VSAs.

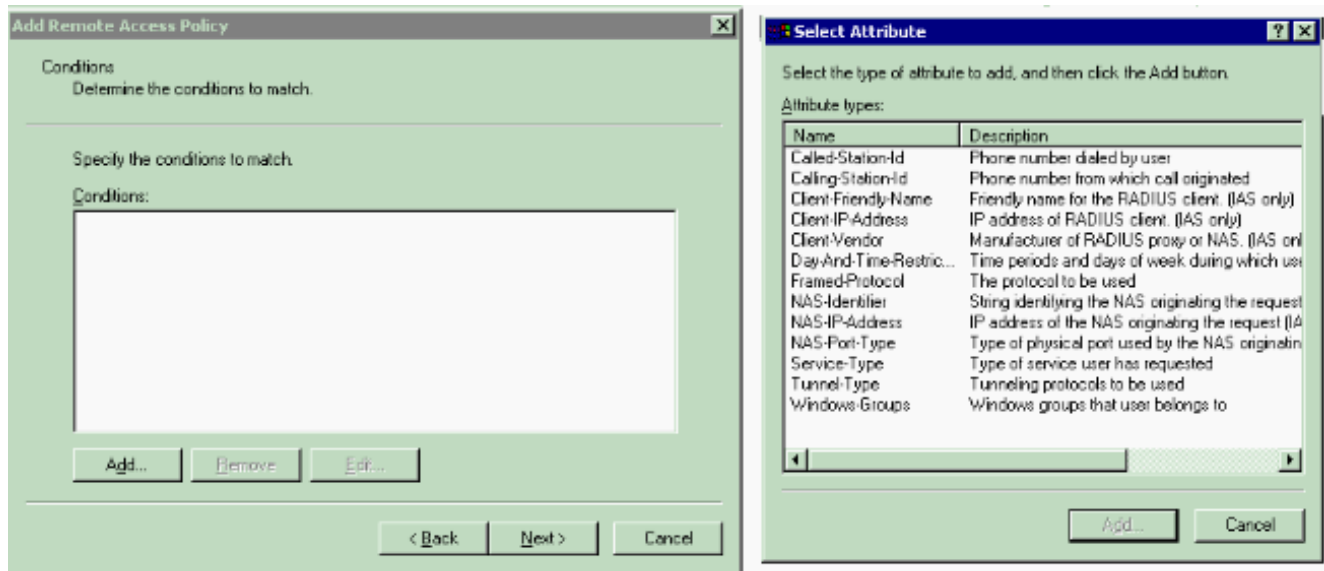
[Configurez la stratégie d'accès à distance sur IAS](#)

Terminez-vous ces étapes afin de configurer une nouvelle stratégie d'accès à distance sur IAS :

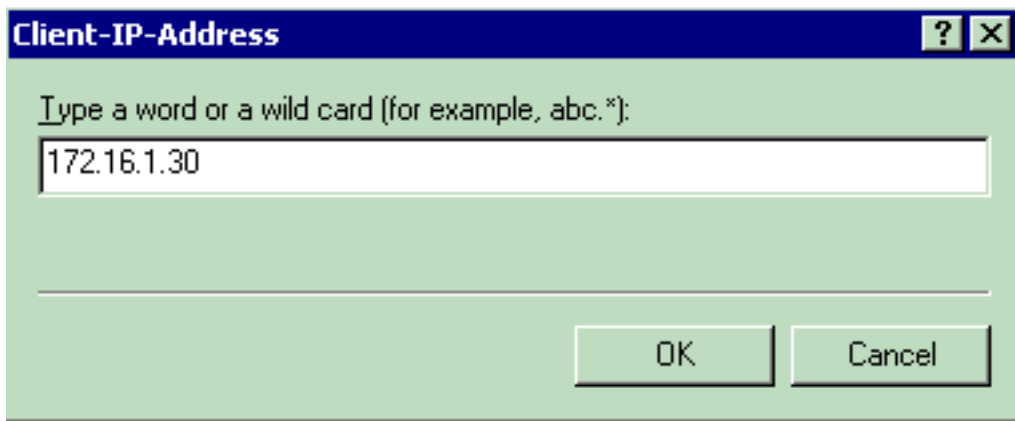
1. Cliquez avec le bouton droit les **stratégies d'accès à distance** et choisissez la **nouvelle stratégie distante d'AcceMSss**. La fenêtre de nom de stratégie apparaît.
2. Écrivez le nom de la stratégie et cliquez sur Next.



3. Dans la prochaine fenêtre, sélectionnez les conditions pour lesquelles la stratégie d'accès à distance s'appliquera. Cliquez sur Add afin de sélectionner les conditions.



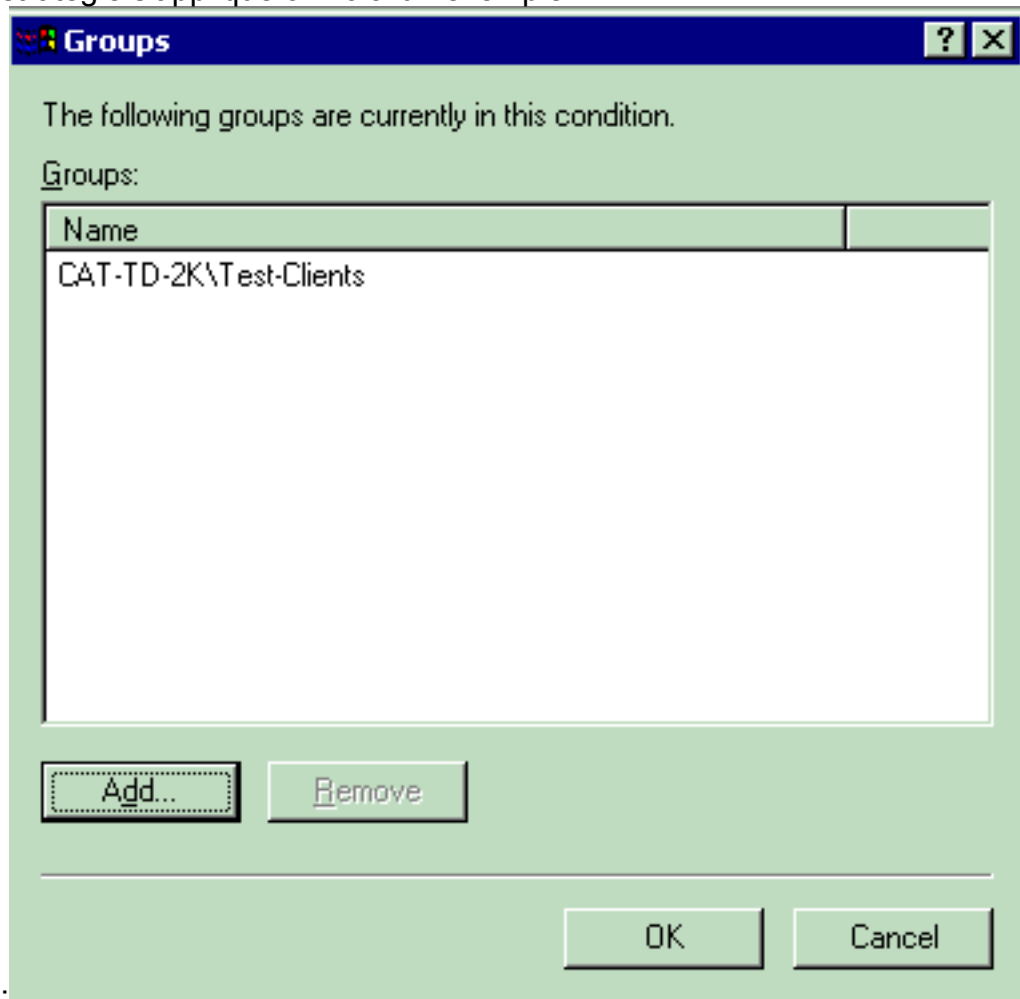
4. Du menu de types d'attribut, sélectionnez ces attributs : **Adresse IP du client** — Écrivez l'adresse IP du client d'AAA. Dans cet exemple, l'adresse IP de WLCs est écrite de sorte que la stratégie s'applique aux paquets à partir du

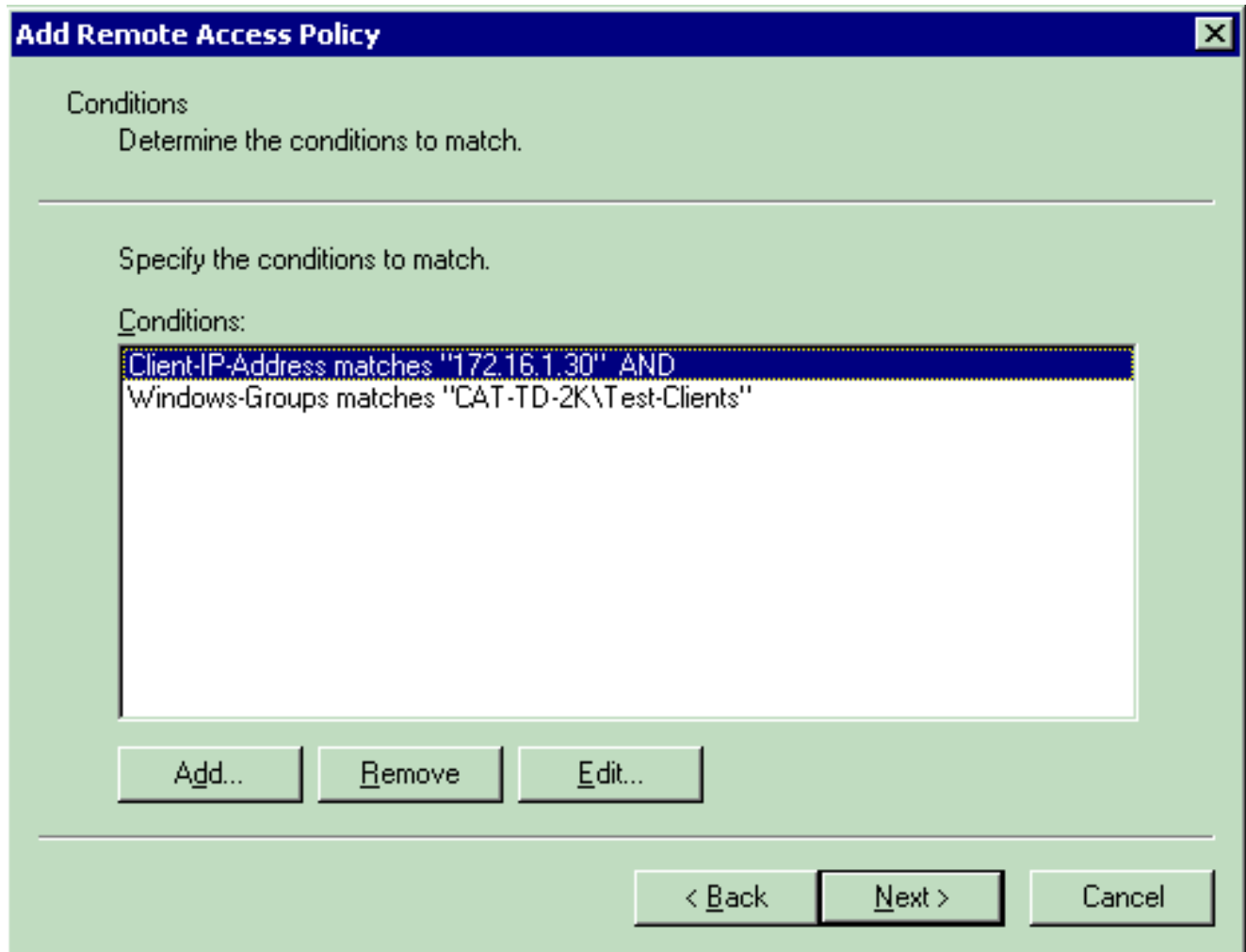


WLC.

Groupes de

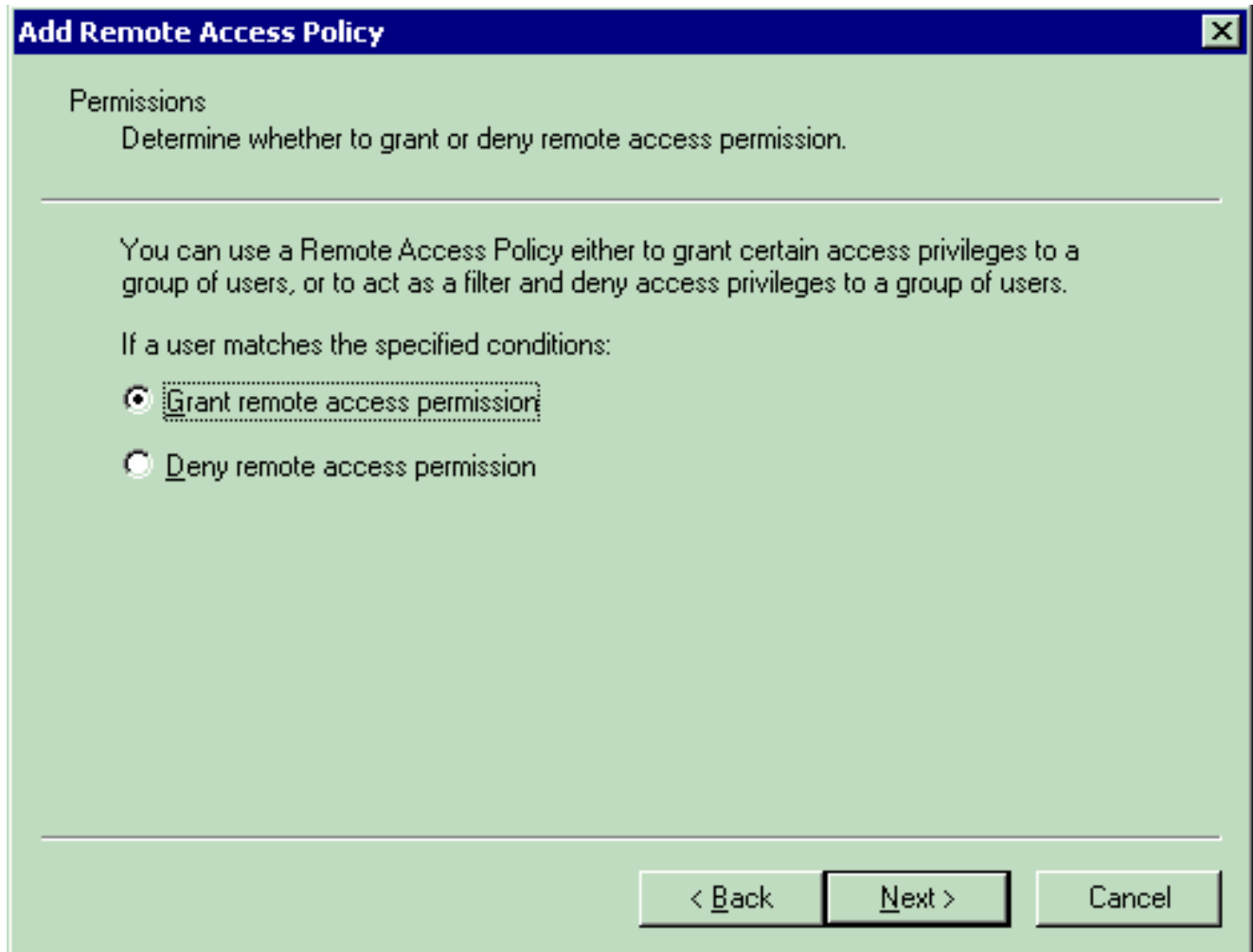
Windows — Sélectionnez le groupe de Windows (le groupe d'utilisateurs) pour lequel la stratégie s'appliquera. Voici un exemple





Cet exemple affiche seulement deux conditions. S'il y a plus de conditions, ajoutez ces conditions aussi bien et cliquez sur Next. La fenêtre d'autorisations apparaît.

5. Dans la fenêtre d'autorisations, choisissez l'**autorisation d'Accès à distance de Grant**. Après que vous choisissiez cette option, l'utilisateur est donné l'accès, si l'utilisateur apparie les conditions spécifiées (d'étape 2).



6. Cliquez sur **Next** (Suivant).
7. L'étape suivante est d'installer le profil utilisateur. Quoique vous pourriez avoir spécifié que des utilisateurs devraient être refusés ou accès basé sur accordé sur les conditions, le profil peut encore être utilisé si les états de cette stratégie sont ignorés sur une base par utilisateur.

Add Remote Access Policy



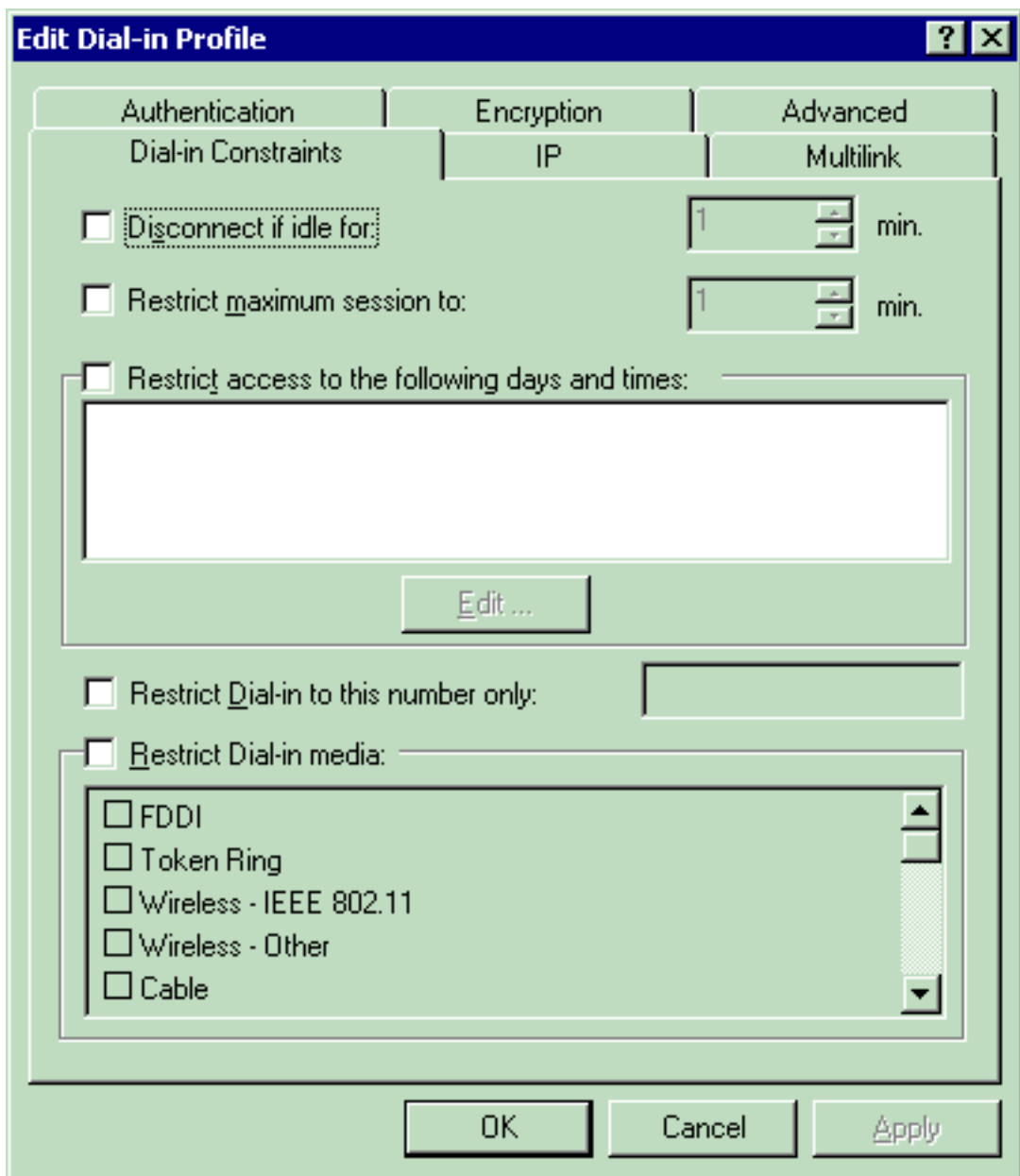
User Profile

Specify the user profile.

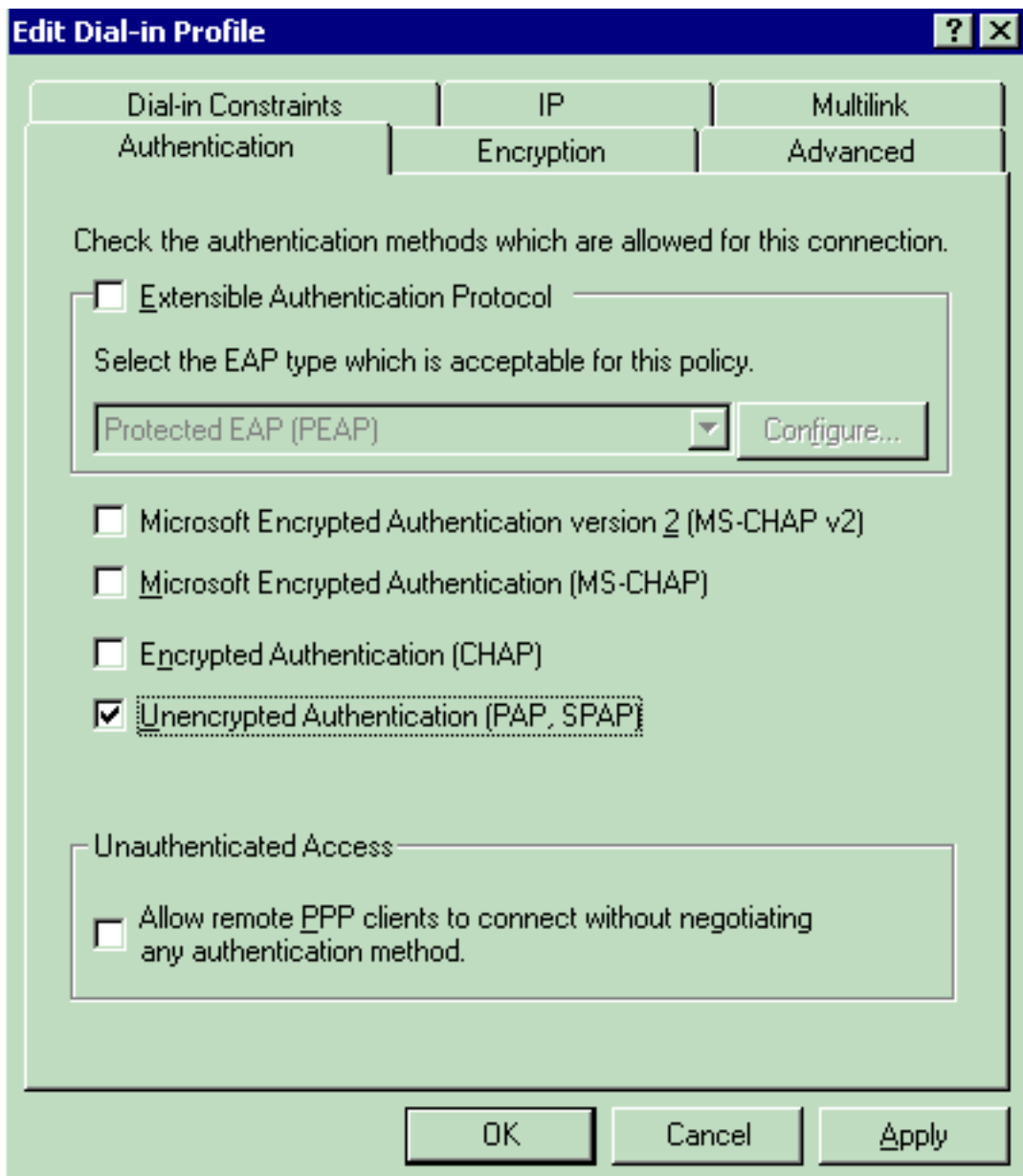
You can now specify the profile for users who matched the conditions you have specified.

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.

Afin de configurer le profil utilisateur, cliquez sur Edit le **profil** sur la fenêtre de profil utilisateur. La fenêtre de profil d'accès distant d'éditer



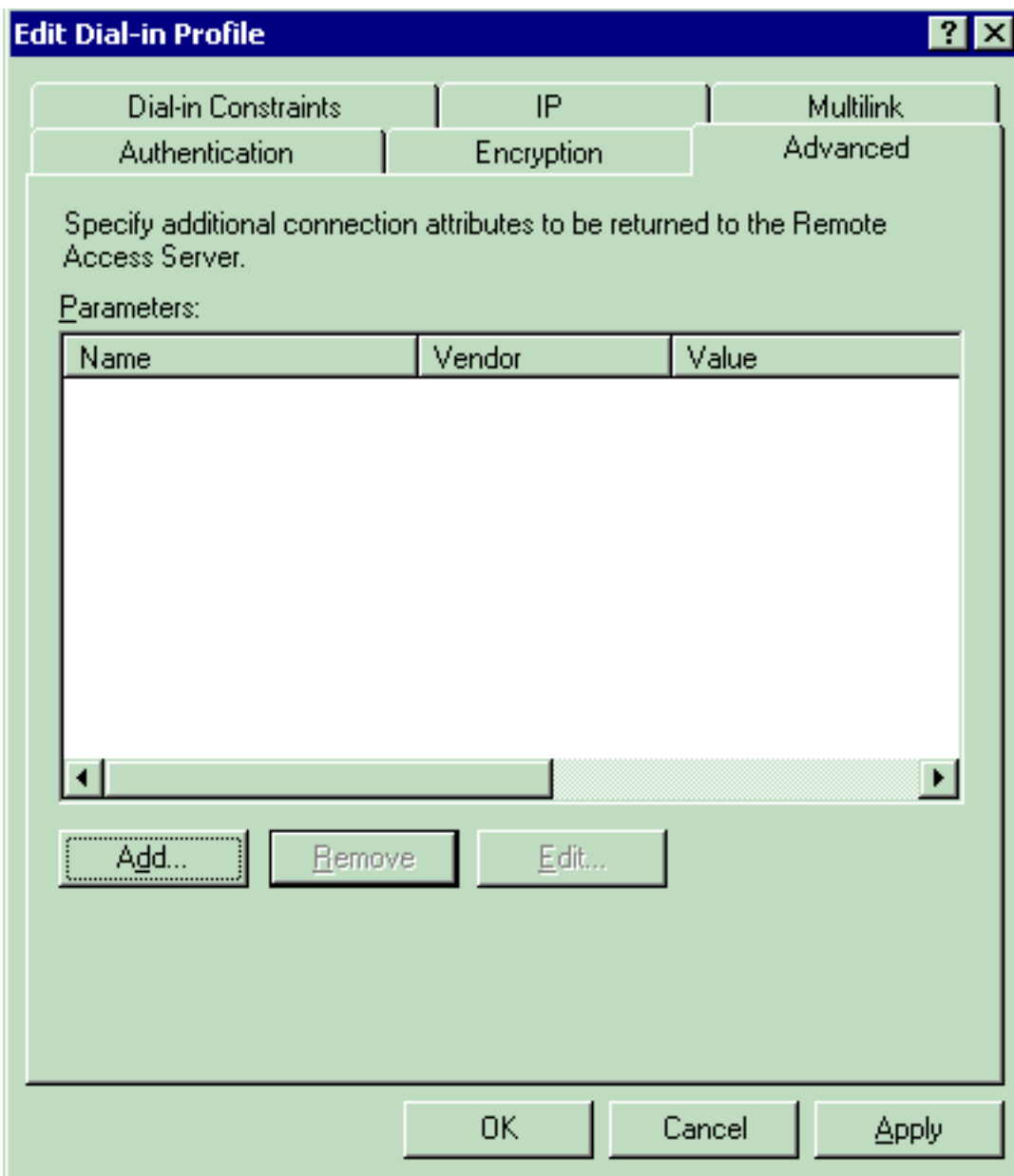
apparaît. Cliquez sur l'onglet d'**authentification**, puis choisissez la méthode d'authentification qui est utilisée dans le WLAN. Cet exemple utilise l'authentification décryptée (PAP,



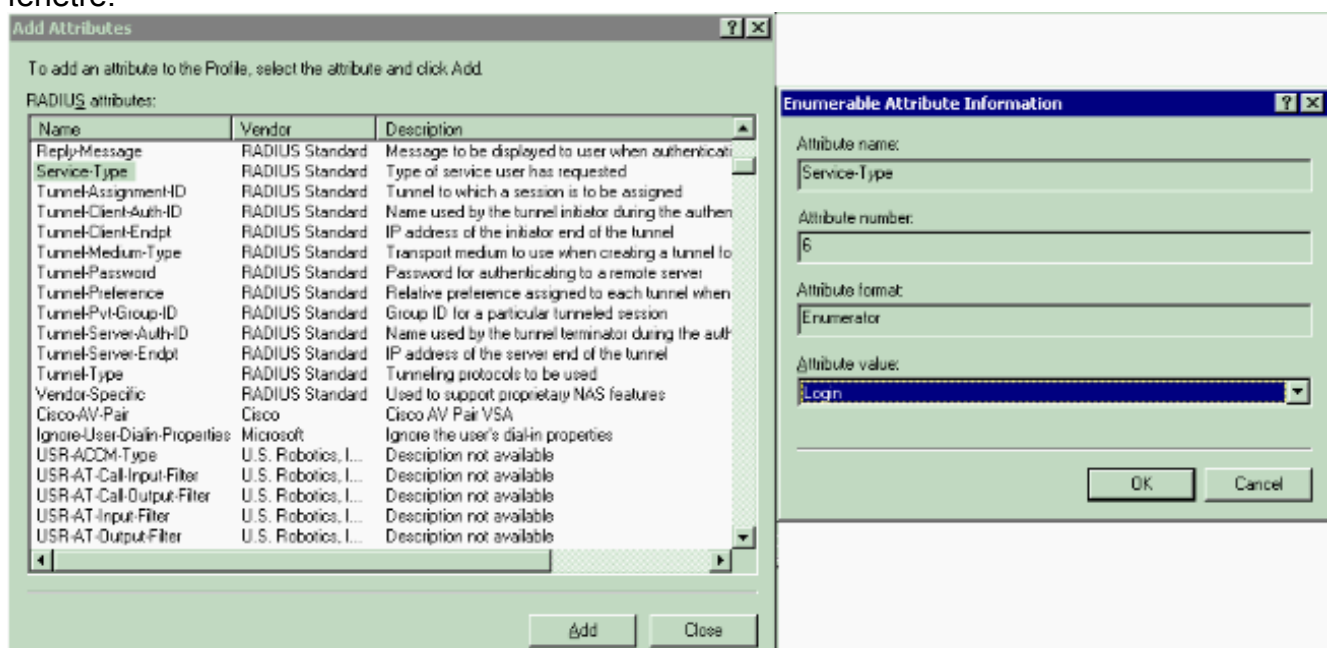
SPAP).

sur la tableau **avancée** retirent tous les paramètres par défaut et cliquent sur

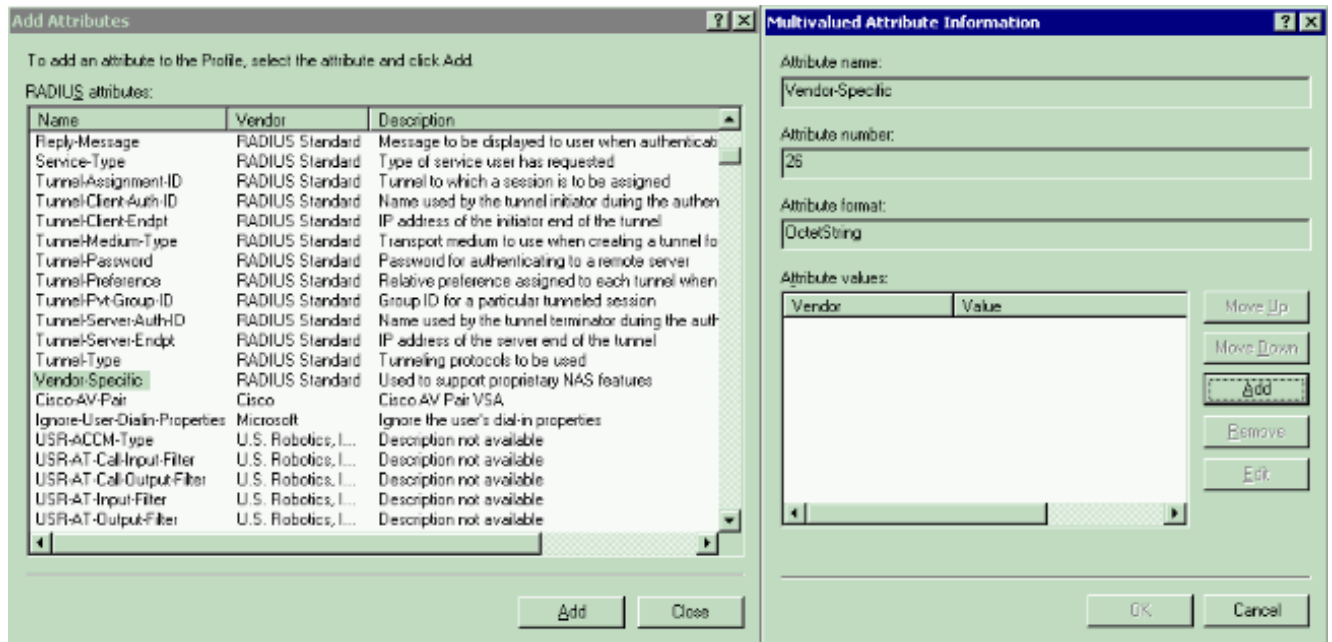
Cliquez



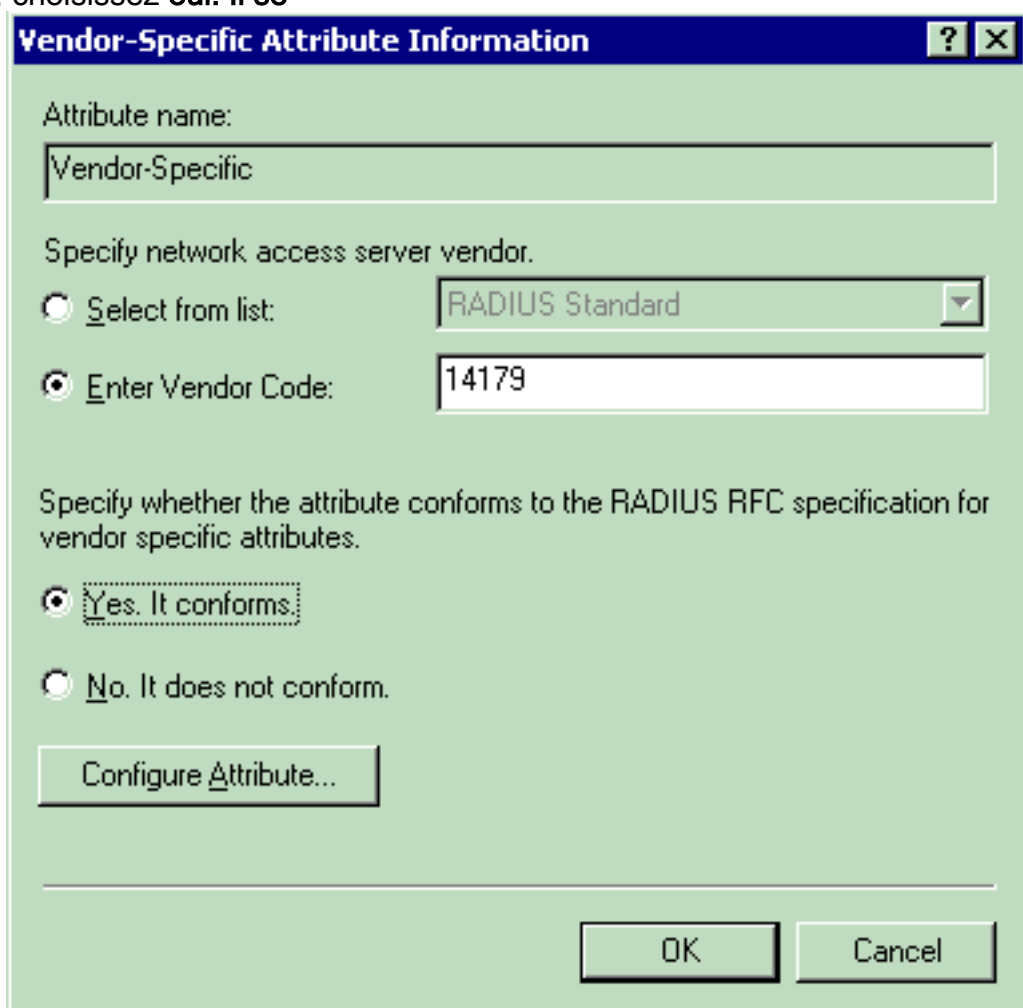
Add... De la fenêtre d'attributs d'ajouter, le type de service choisi, choisissent alors la valeur de procédure de connexion de la prochaine fenêtre.



Ensuite, vous devez sélectionner l'attribut de Constructeur-particularité de la liste d'attributs RADIUS.

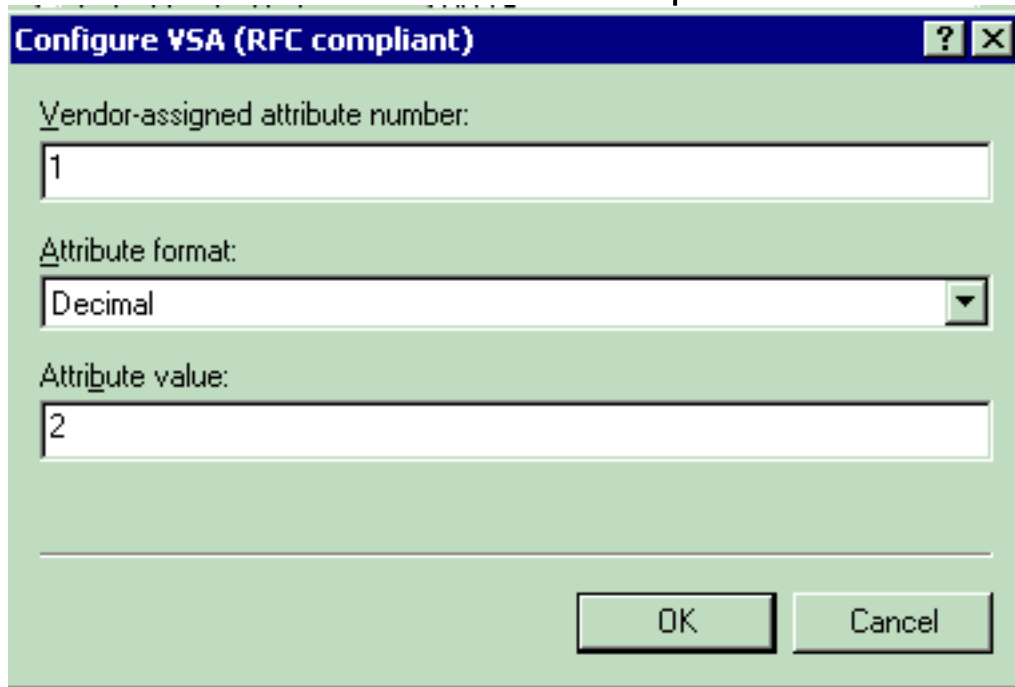


Dans la prochaine fenêtre, cliquez sur Add afin de sélectionner un nouveau VSA. La fenêtre de l'information d'attribut de Constructeur-particularité apparaît. Sous spécifiez le constructeur de serveur d'accès à distance, choisissez **écrivent le code de constructeur**. Écrivez le code de constructeur pour les VSAs d'Airespace. Le code de constructeur pour les VSAs de Cisco Airespace est **14179**. Puisque cet attribut se conforme à la spécification RFC de RAYON pour les VSAs, choisissez **oui**. Il se



conforme. Cliquez sur Configurer l'attribut. Dans la fenêtre VSA de configurer (RFC conforme), écrivez le nombre

Constructeur-assigné d'attribut, le format d'attribut et la valeur d'attribut, qui dépendent du VSA que vous voulez utiliser. Pour placer l'ID de WLAN sur une base par utilisateur :
Nom d'attribut — Airespace-WLAN-idnombre Constructeur-assigné d'attribut — 1
Format d'attribut — Entier/décimale
Valeur — ID de WLAN
Exemple 1



Configure VSA (RFC compliant)

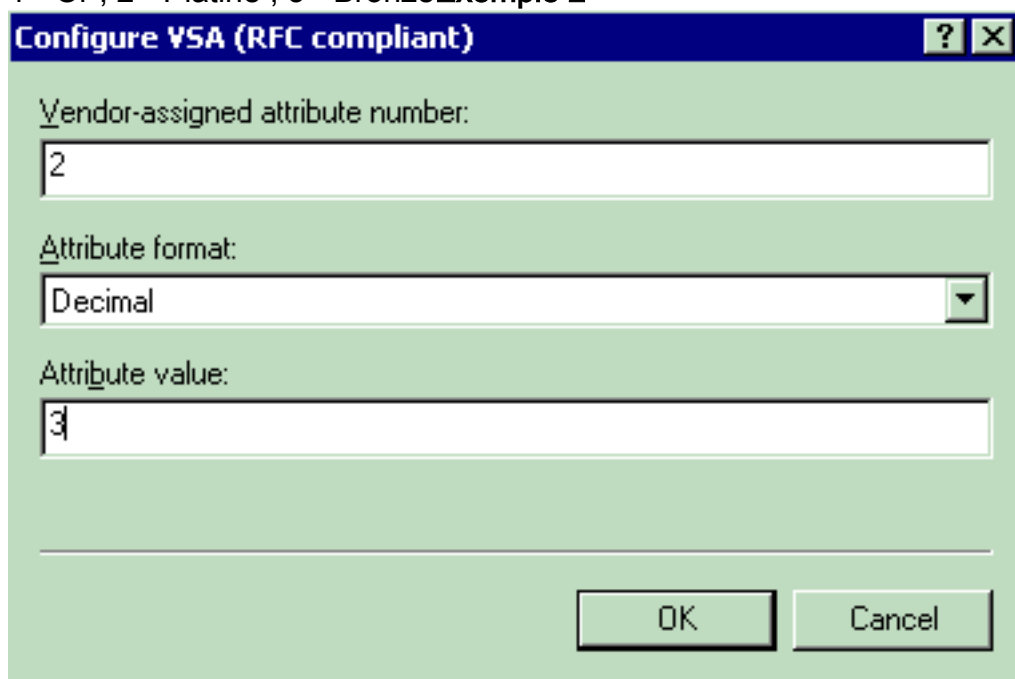
Vendor-assigned attribute number:
1

Attribute format:
Decimal

Attribute value:
2

OK Cancel

Pour placer le profil de QoS sur une base par utilisateur :
Nom d'attribut — Niveau Airespace QoS
Nombre Constructeur-assigné d'attribut — 2
Format d'attribut — Entier/décimale
Valeur — 0 - argent ; 1 - Or ; 2 - Platine ; 3 - Bronze
Exemple 2



Configure VSA (RFC compliant)

Vendor-assigned attribute number:
2

Attribute format:
Decimal

Attribute value:
3

OK Cancel

Pour placer la valeur DSCP sur une base par utilisateur :
Nom d'attribut — Airespace-DSCP
paumber Constructeur-assigné d'attribut — 3
Format d'attribut — Entier/décimale
Valeur — Valeur DSCP
[Exemple 3](#)

Configure VSA (RFC compliant)

Vendor-assigned attribute number:
3

Attribute format:
Decimal

Attribute value:
46

OK Cancel

Pour placer le 802.1p-Tag sur une base par utilisateur :
 Nom d'attribut — Airespace-802.1p-Tag
 nombre Constructeur-assigné d'attribut — 4
 Format d'attribut — Entier/décimale
 Valeur — 802.1p-

Configure VSA (RFC compliant)

Vendor-assigned attribute number:
4

Attribute format:
Decimal

Attribute value:
5

OK Cancel

Tag [Exemple 4](#) Pour placer l'interface (VLAN) sur une base par utilisateur :
 Nom d'attribut — Airespace-Interface-
 nom nombre Constructeur-assigné d'attribut — 5
 Format d'attribut — Chaîne
 Valeur — Interface-nom
 Exemple 5

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

Vendor-assigned attribute number:

Attribute format:

Attribute value:

[OK] [Cancel]

Pour placer l'ACL

sur une base par utilisateur : **Nom d'attribut** — Airespace-ACL-nomnombre Constructeur-assigné d'attribut — 6 **Format d'attribut** — Chaîne **Valeur** — Acl-nom **Exemple 6**

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

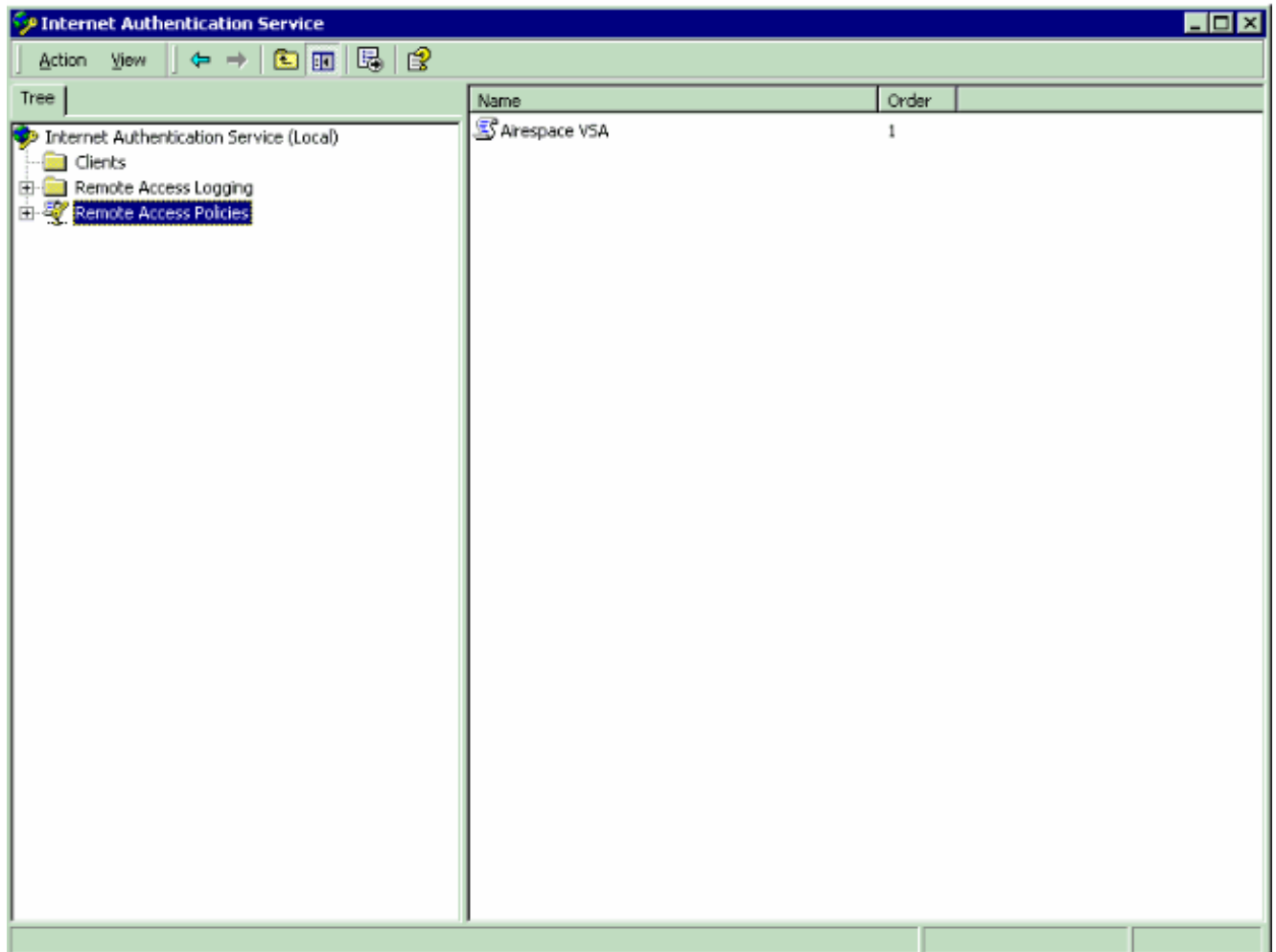
Vendor-assigned attribute number:

Attribute format:

Attribute value:

[OK] [Cancel]

8. Une fois que vous avez configuré les VSAs, cliquez sur OK jusqu'à ce que vous voyiez la fenêtre de profil utilisateur.
9. Puis, cliquez sur Finish afin de se terminer la configuration. Vous pouvez voir la nouvelle stratégie dans le cadre des stratégies d'accès à distance.



Exemple de configuration

Dans cet exemple, un WLAN est configuré pour l'authentification Web. Des utilisateurs sont authentifiés par le serveur de RAYON d'IAS, et le serveur de RAYON est configuré pour répartir des stratégies QoS sur une base par utilisateur.

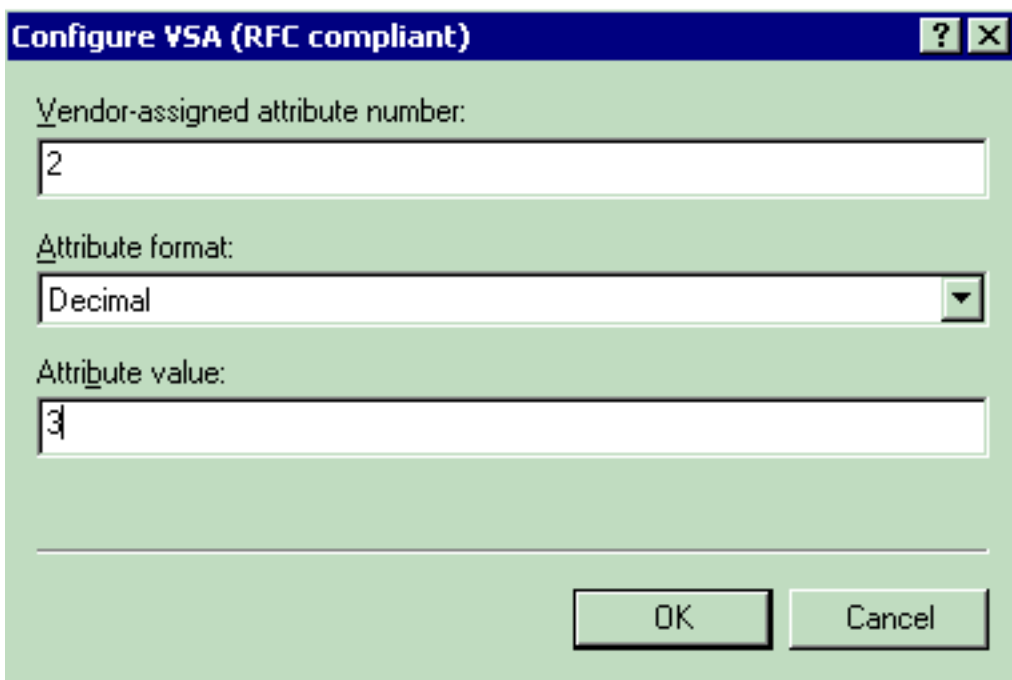
The screenshot displays the Cisco Systems WLAN configuration interface. The main content is divided into several sections:

- 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 ** 60), DHCP Server (Override), DHCP Addr. Assignment (Required), Interface Name (internal), MFP Version Required (1), MFP Signature Generation (Global MFP Disabled), and H-REAP Local Switching.
- Security Policies**: Includes Layer 2 Security (None), Layer 3 Security (None), Web Policy (checked), Authentication (checked), Passthrough (unchecked), 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, Allow AAA Override, and the Radius Servers section. 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".

Comme vous pouvez voir de cette fenêtre, l'authentification Web est activée, le serveur d'authentification est 172.16.1.1, et le dépassement d'AAA est également activé sur le WLAN. La configuration par défaut de QoS pour ce WLAN est placée pour argenter.

Sur le serveur de RAYON d'IAS, on configure une stratégie d'accès à distance qui retourne le QoS que bronze d'attribut dans le RAYON reçoit la demande. Ceci est fait quand vous configurez la particularité VSA à l'attribut de QoS.



Voyez le [configurer la stratégie d'accès à distance sur la](#) section d'[IAS de](#) ce document pour des informations détaillées sur la façon configurer une stratégie d'accès à distance sur le serveur d'IAS.

Une fois le serveur d'IAS, le WLC, et le RECOUVREMENT sont configurés pour cette installation, les clients sans fil peut employer l'authentification Web afin de se connecter.

Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Quand l'utilisateur se connecte au WLAN un user-id et mot de passe, le WLC passe les qualifications au serveur de RAYON d'IAS qui authentifie l'utilisateur contre aux conditions et au profil utilisateur configurés dans la stratégie d'accès à distance. Si l'authentification de l'utilisateur est réussie, le serveur de RAYON renvoie un RAYON reçoivent la demande qui contient également les valeurs de priorité d'AAA. Dans ce cas, la stratégie QoS de l'utilisateur est retournée.

Vous pouvez émettre le **debug aaa toute la commande d'enable** afin de voir la séquence d'opérations qui se produit pendant l'authentification. Voici un exemple de sortie :

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

```

Comme vous pouvez voir de la sortie, l'utilisateur est authentifié. Puis, des valeurs de priorité d'AAA sont retournées avec le RAYON reçoivent le message. Dans ce cas, l'utilisateur est donné la stratégie QoS du bronze.

Vous pouvez vérifier ceci sur le GUI WLC aussi bien. Voici un exemple :

The screenshot shows the Cisco Systems WLC configuration interface. 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 |

Remarque: Le profil par défaut de QoS pour ce SSID est argenté. Cependant, parce que le dépassement d'AAA est sélectionné et l'utilisateur est configuré avec un profil de QoS de bronze sur le serveur d'IAS, le profil de QoS de par défaut est ignoré.

Dépannez

Vous pouvez utiliser le **debug aaa toute la** commande d'**enable** sur le WLC de dépanner la configuration. Un exemple de la sortie de ceci mettent au point dans un réseau fonctionnant est affiché dans la section de [vérifier de](#) ce document.

Remarque: Référez-vous aux [informations importantes sur les commandes de débogage](#) avant d'utiliser les commandes de **débogage**.

Informations connexes

- [Guide de configuration du contrôleur LAN sans fil Cisco, version 4.0](#)
- [Exemple de configuration de restriction de l'accès au réseau local sans fil sur SSID avec WLC et Cisco Secure ACS](#)
- [Assistance produit sans fil](#)
- [Support et documentation techniques - Cisco Systems](#)