

Microsoft IAS RADIUS 서버의 Cisco Airespace VSA 구성 예

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[배경 정보](#)

[Airespace VSA에 대한 IAS 구성](#)

[IAS에서 WLC를 AAA 클라이언트로 구성](#)

[IAS에서 원격 액세스 정책 구성](#)

[컨피그레이션 예](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 Cisco VSA(Airespace Vendor Specific Attributes)를 지원하도록 Microsoft IAS(Internet Authentication Service) 서버를 구성하는 방법을 보여줍니다. Cisco Airespace VSA의 공급업체 코드는 14179입니다.

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- IAS 서버 구성 방법에 대한 지식
- LAP(Lightweight Access Point) 및 Cisco WLC(Wireless LAN Controller) 컨피그레이션에 대한 지식
- Cisco Unified Wireless Security 솔루션에 대한 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Microsoft Windows 2000 서버(IAS 포함)

- 소프트웨어 버전 4.0.206.0을 실행하는 Cisco 4400 WLC
- Cisco 1000 Series LAP
- 802.11 a/b/g 무선 클라이언트 어댑터(펌웨어 2.5 포함)
- Aironet Desktop Utility(ADU) 버전 2.5

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

참고: 이 문서는 Cisco Airespace VSA를 지원하기 위해 IAS 서버에 필요한 컨피그레이션의 예를 독자에게 제공하기 위한 것입니다. 이 문서에 제시된 IAS 서버 컨피그레이션은 Lab에서 테스트되었으며 예상대로 작동합니다. IAS 서버를 구성하는 데 문제가 있는 경우 Microsoft에 도움을 요청하십시오. Cisco TAC에서는 Microsoft Windows 서버 컨피그레이션을 지원하지 않습니다.

이 문서에서는 WLC가 기본 작동을 위해 구성되었으며 LAP가 WLC에 등록되었다고 가정합니다. LAP의 기본 작동을 위해 WLC를 설정하려는 새 사용자는 WLC([Wireless LAN Controller](#))에 대한 [LAP\(Lightweight AP\) 등록](#)을 참조하십시오.

표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 표기 규칙을 참고하십시오.](#)

배경 정보

대부분의 WLAN(무선 LAN) 시스템에서는 각 WLAN에 SSID(서비스 집합 식별자)와 연결된 모든 클라이언트에 적용되는 정적 정책이 있습니다. 강력하지만 이 방법은 여러 QoS 및 보안 정책을 상속하기 위해 클라이언트가 다른 SSID와 연결해야 하기 때문에 제한이 있습니다.

그러나 Cisco Wireless LAN Solution은 ID 네트워킹을 지원하므로, 네트워크에서 단일 SSID와 특정 사용자에게 사용자 프로필에 따라 다른 QoS 또는 보안 정책을 상속하도록 알릴 수 있습니다. ID 네트워킹을 사용하여 제어할 수 있는 특정 정책에는 다음이 포함됩니다.

- **QoS(서비스 품질)** - RADIUS Access Accept(RADIUS 액세스 수락)에 있는 경우 QoS 레벨 값이 WLAN 프로파일에 지정된 QoS 값을 재정의합니다.
- **ACL** - RADIUS Access Accept에 ACL(Access Control List) 특성이 있는 경우 시스템은 인증 후 클라이언트 스테이션에 ACL-Name을 적용합니다. 이는 인터페이스에 할당된 모든 ACL을 재정의합니다.
- **VLAN** - RADIUS Access Accept에 VLAN Interface-Name 또는 VLAN-Tag가 있으면 시스템은 클라이언트를 특정 인터페이스에 배치합니다.
- **WLAN ID** - RADIUS Access Accept(RADIUS 액세스 수락)에 WLAN-ID 특성이 있는 경우 시스템은 인증 후 WLAN-ID(SSID)를 클라이언트 스테이션에 적용합니다. WLAN ID는 IPsec을 제외한 모든 인증 인스턴스에서 WLC에 의해 전송됩니다. 웹 인증의 경우 WLC가 AAA 서버의 인증 응답에서 WLAN-ID 특성을 수신하고 WLAN의 ID와 일치하지 않으면 인증이 거부됩니다. 다른 유형의 보안 방법으로는 이러한 기능이 없습니다.
- **DSCP Value(DSCP 값)** - RADIUS Access Accept(RADIUS 액세스 수락)에 있는 경우 DSCP 값은 WLAN 프로파일에 지정된 DSCP 값을 재정의합니다.
- **802.1p-Tag** - RADIUS Access Accept에 있는 경우 802.1p 값이 WLAN 프로파일에 지정된 기본 값을 재정의합니다.

참고: VLAN 기능은 MAC 필터링, 802.1X 및 WPA(Wi-Fi Protected Access)만 지원합니다. VLAN 기능은 웹 인증 또는 IPsec을 지원하지 않습니다. 운영 체제의 로컬 MAC 필터 데이터베이스가 인터페이스

이름을 포함하도록 확장되었습니다.이렇게 하면 로컬 MAC 필터가 어떤 인터페이스를 클라이언트에 할당할지 지정할 수 있습니다.별도의 RADIUS 서버도 사용할 수 있지만 보안 메뉴를 사용하여 RADIUS 서버를 정의해야 합니다.

ID [네트워킹](#)에 대한 자세한 내용은 ID 네트워킹 구성을 참조하십시오.

[Airespace VSA에 대한 IAS 구성](#)

Airespace VSA에 대해 IAS를 구성하려면 다음 단계를 완료해야 합니다.

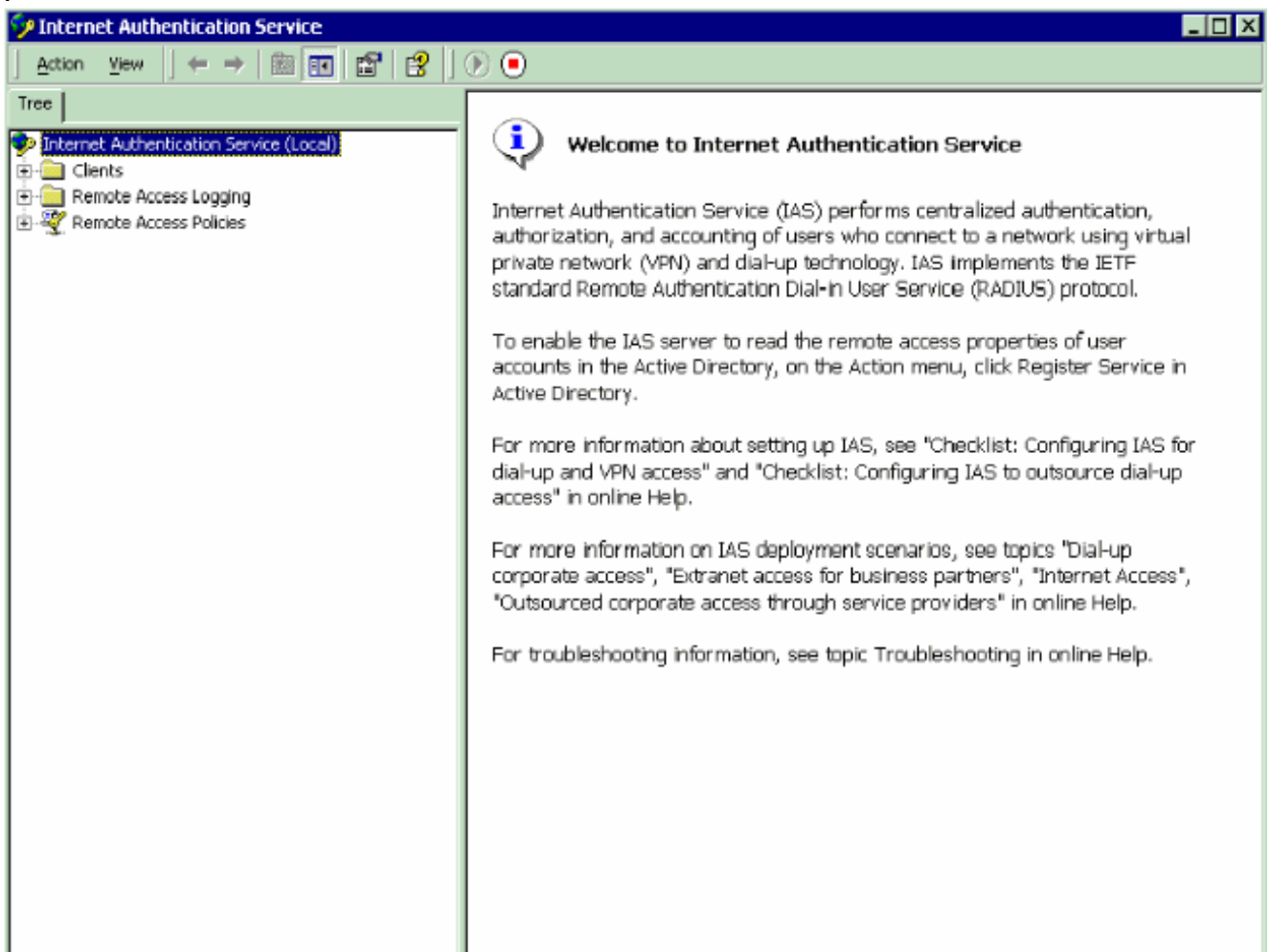
1. [IAS에서 WLC를 AAA 클라이언트로 구성](#)
2. [IAS에서 원격 액세스 정책 구성](#)

참고: VSA는 원격 액세스 정책 아래에 구성됩니다.

[IAS에서 WLC를 AAA 클라이언트로 구성](#)

IAS에서 WLC를 AAA 클라이언트로 구성하려면 다음 단계를 완료합니다.

1. Microsoft 2000 서버에서 IAS를 시작하려면 **프로그램 > 관리 도구 > 인터넷 인증 서비스**를 클릭합니다



2. 새 RADIUS 클라이언트를 추가하려면 **Clients** 폴더를 마우스 오른쪽 버튼으로 클릭하고 **New Client**를 선택합니다.
3. Add Client(클라이언트 추가) 창에서 클라이언트의 이름을 입력하고 **RADIUS**를 Protocol(프로

토콜)로 선택합니다.그런 다음 다음 다음을 클릭합니다.이 예에서 클라이언트 이름은 WLC-1입니다.
.참고: 기본적으로 프로토콜은 RADIUS로 설정됩니다

Add Client

Name and Protocol
Assign a name and protocol for the client.

Type a friendly name and protocol for the client.

Friendly name: WLC-1

Protocol: RADIUS

< Back Next > Cancel

4. Add RADIUS Client(RADIUS 클라이언트 추가) 창에서 **Client IP address(클라이언트 IP 주소)**, **Client-Vendor(클라이언트-벤더)** 및 **Shared secret(공유 암호)**를 입력합니다.클라이언트 정보를 입력한 후 Finish(마침)를 클릭합니다.이 예에서는 IP 주소가 172.16.1.30인 WLC-1이라는 클라이언트를 보여 주고, Client-Vendor는 Cisco로 설정되고 Shared 비밀은 cisco123입니다

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]

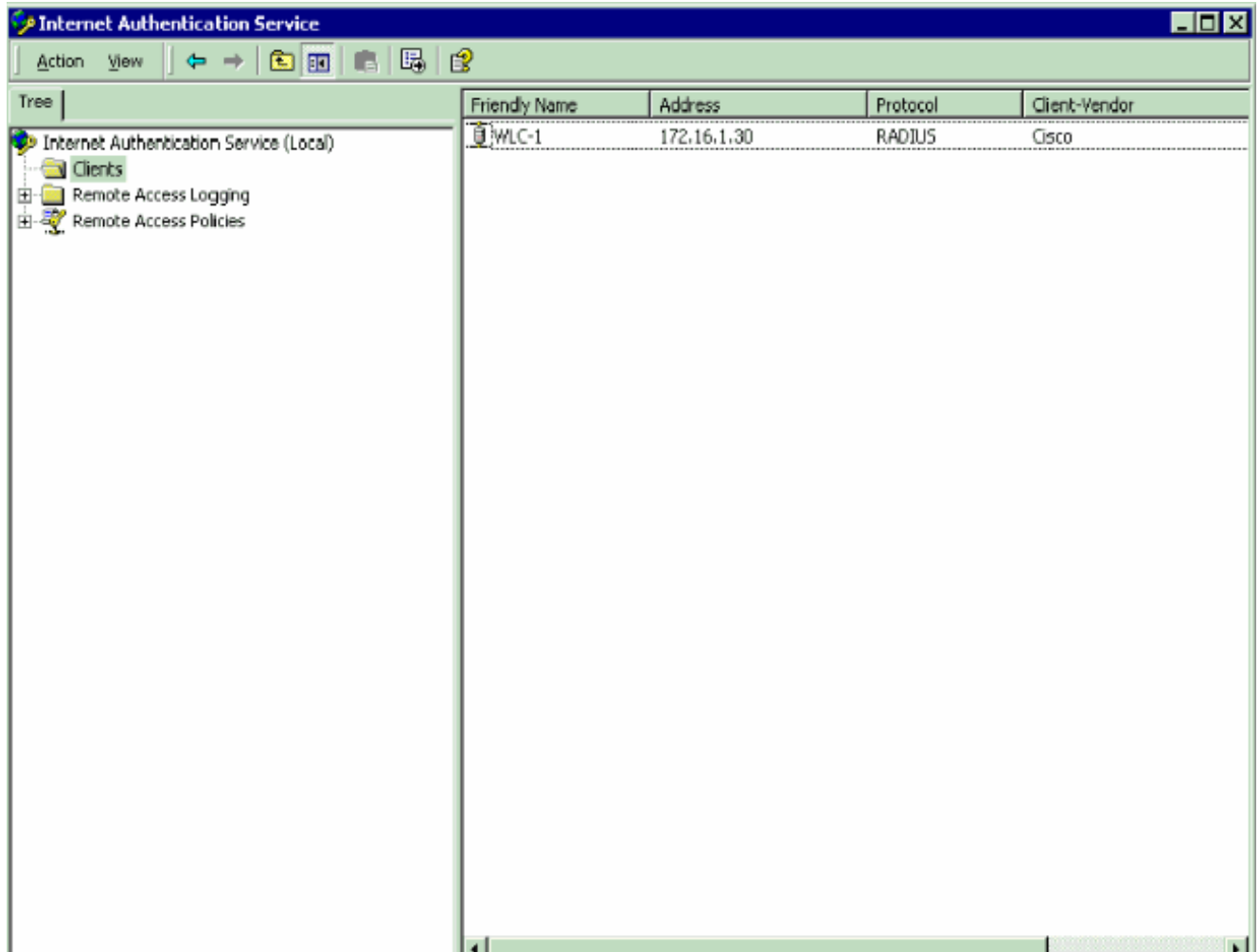
Client must always send the signature attribute in the request

Shared secret: [xxxxxxx]

Confirm shared secret: [xxxxxxx]

< Back Finish Cancel

이 정보를 사용하여 WLC-1이라는 WLC가 IAS 서버의 AAA 클라이언트로 추가됩니다

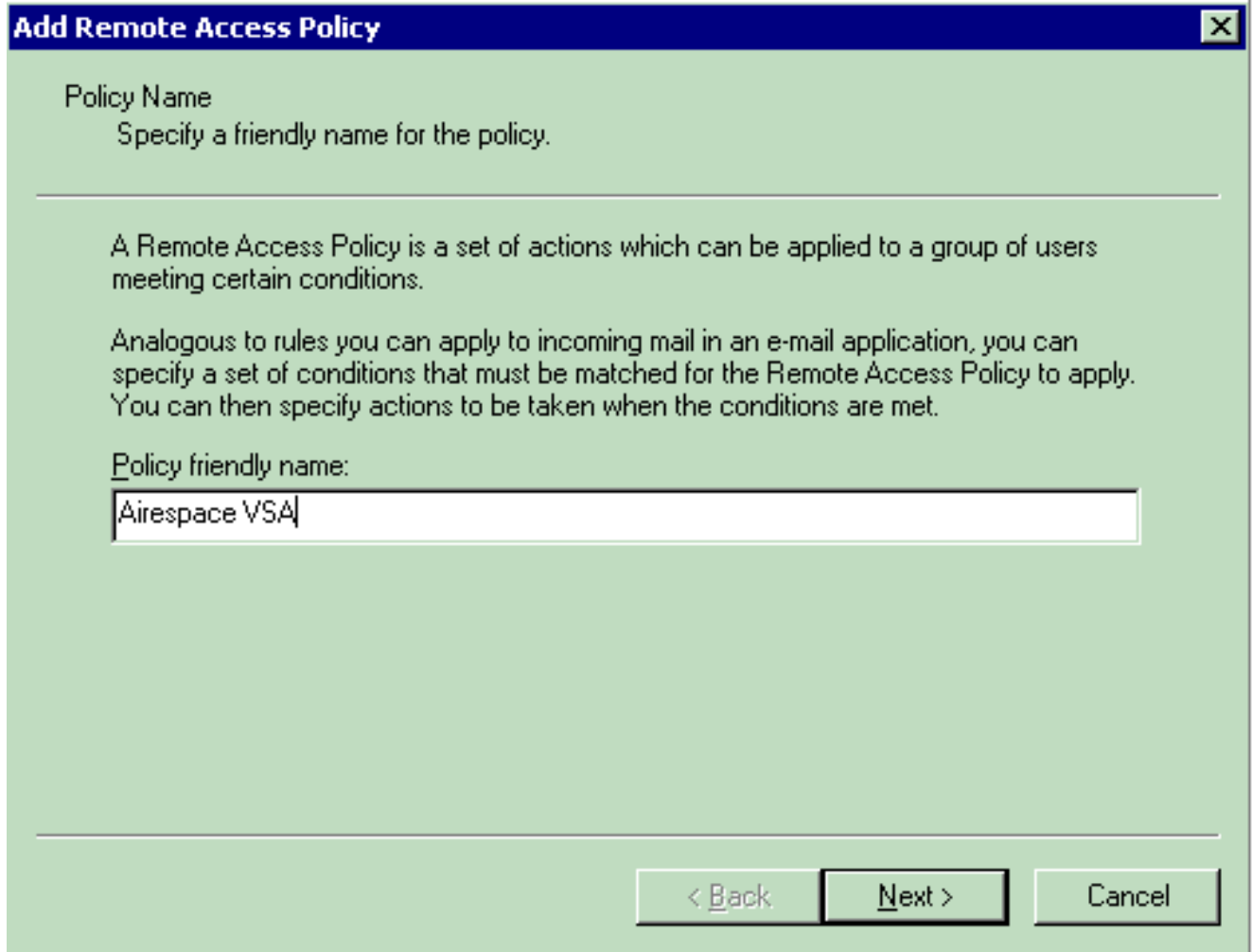


다음 단계는 원격 액세스 정책을 생성하고 VSA를 구성하는 것입니다.

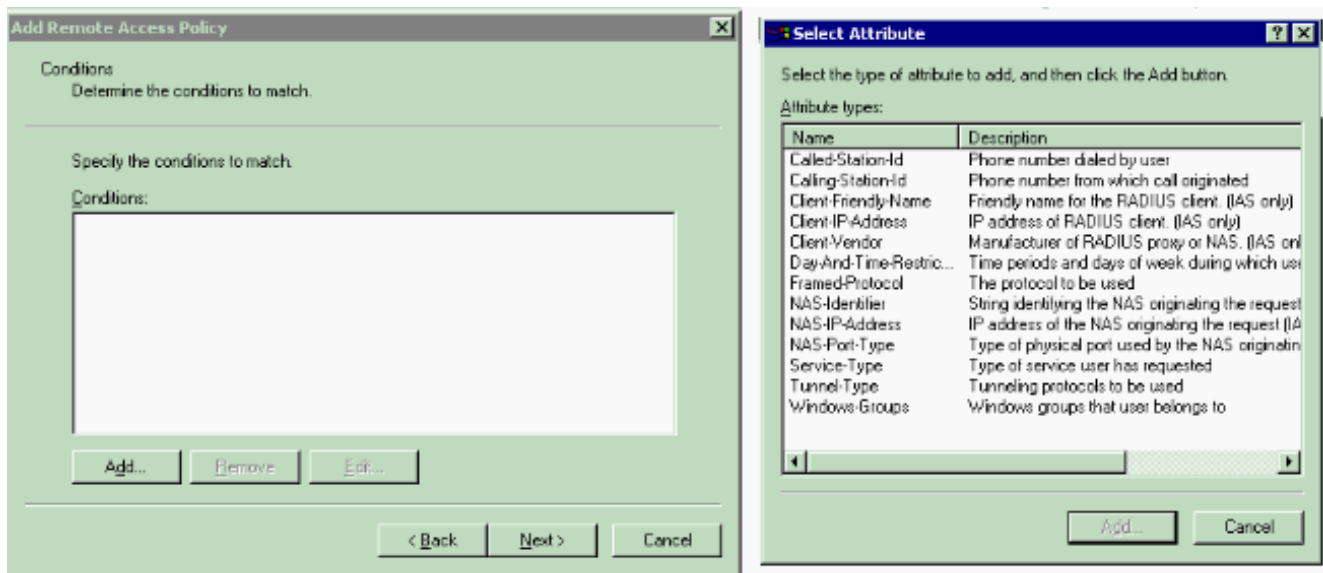
[IAS에서 원격 액세스 정책 구성](#)

IAS에서 새 원격 액세스 정책을 구성하려면 다음 단계를 완료합니다.

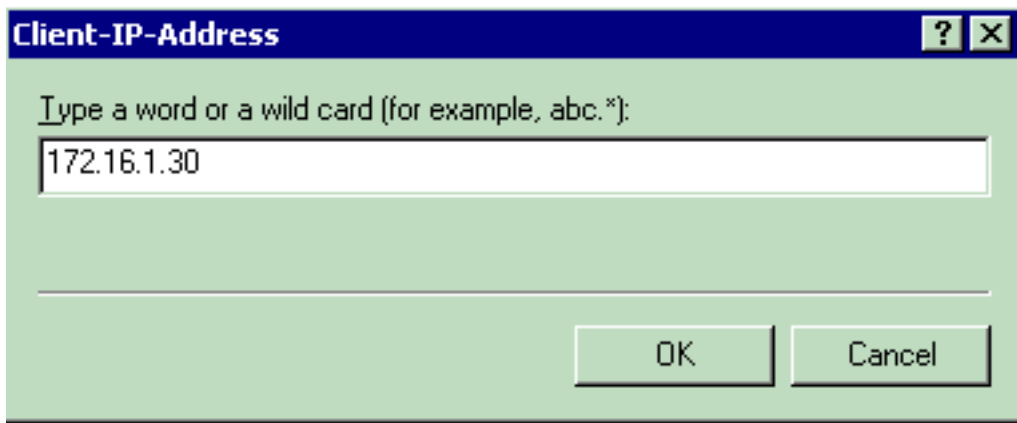
1. Remote Access Policies(원격 액세스 정책)를 마우스 오른쪽 버튼으로 클릭하고 **New Remote Access(새 원격 액세스)MSs Policy(MSs 정책)**를 선택합니다.Policy Name 창이 나타납니다.
2. 정책의 이름을 입력하고 Next(다음)를 클릭합니다



- 다음 창에서 원격 액세스 정책을 적용할 조건을 선택합니다. 조건을 선택하려면 **Add**를 클릭합니다

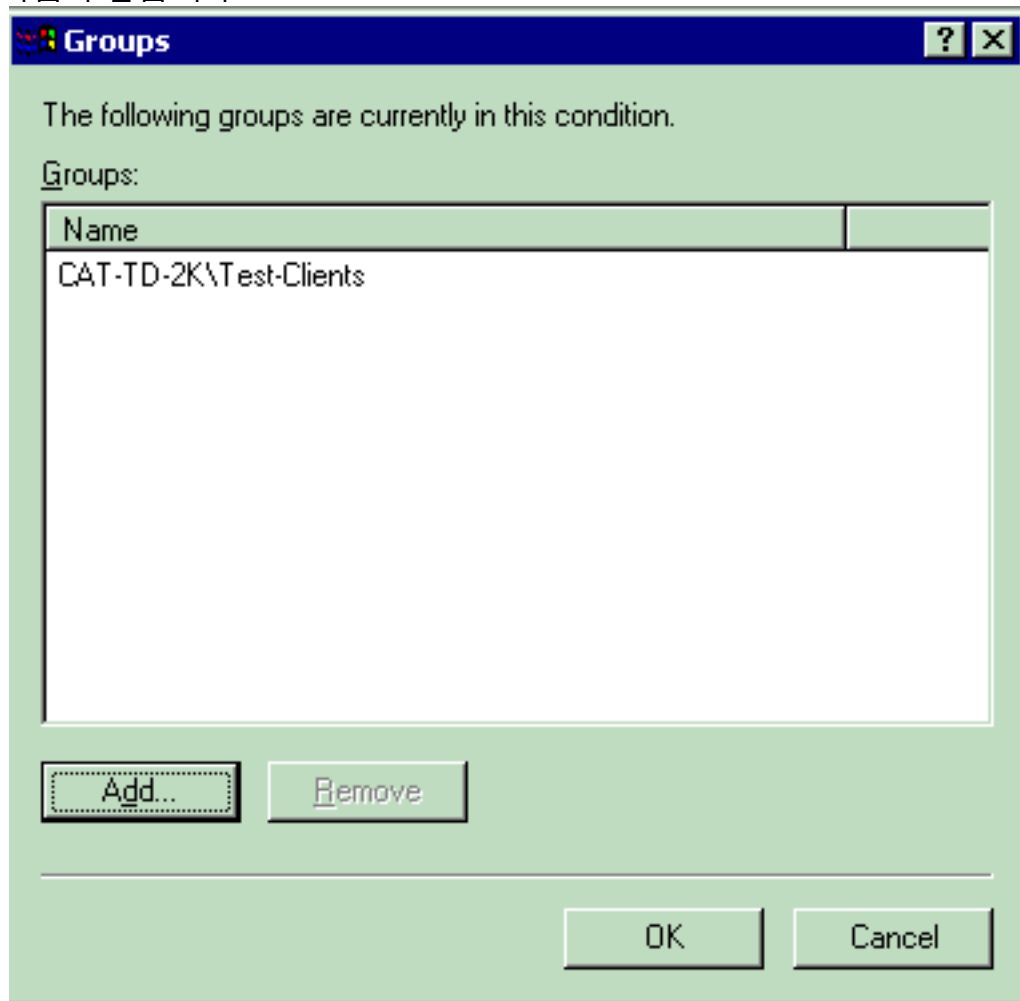


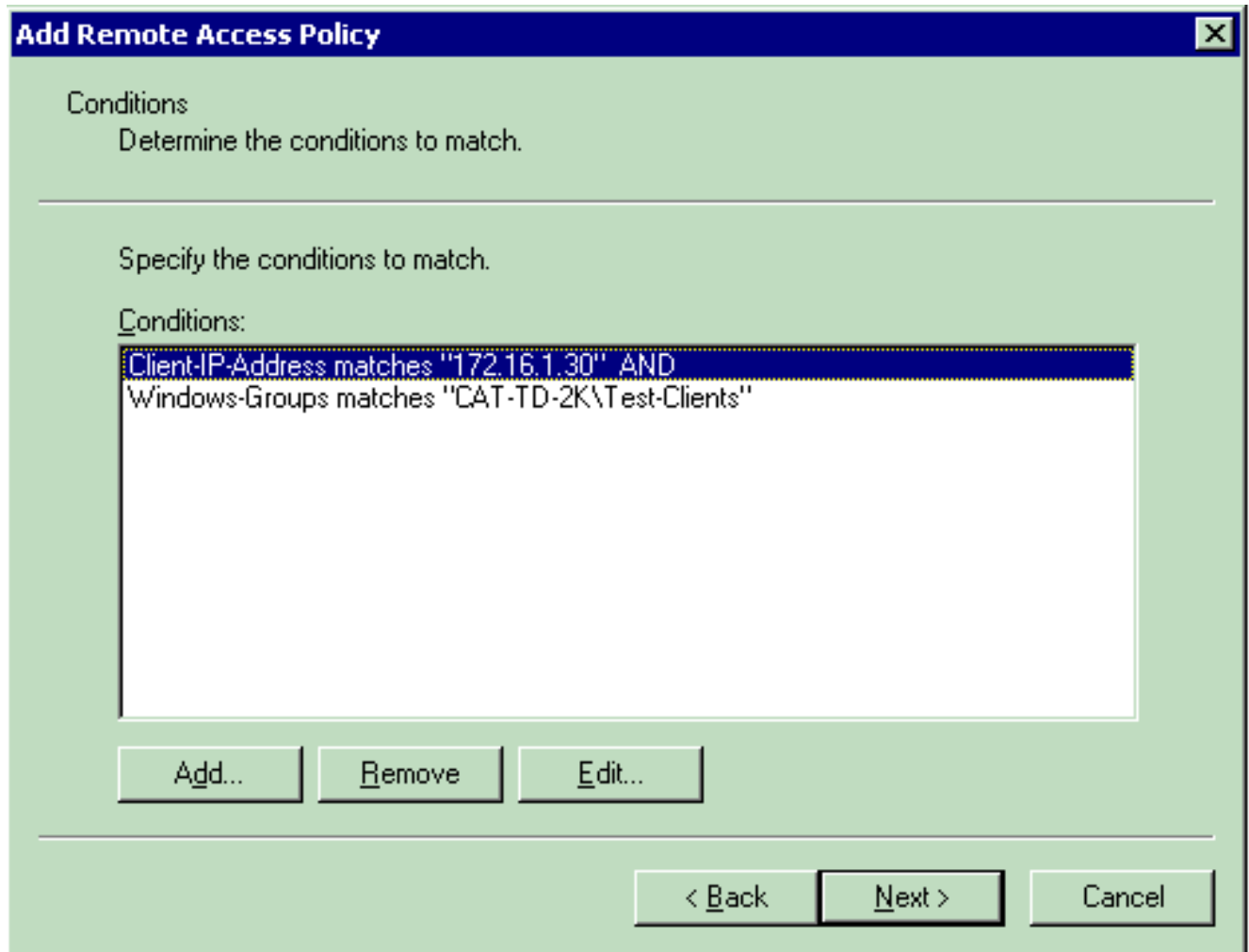
- 속성 유형 메뉴에서 다음 속성을 선택합니다. **Client-IP-Address(클라이언트-IP-주소)** - AAA 클라이언트의 IP 주소를 입력합니다. 이 예에서는 WLC의 패킷에 정책이 적용되도록 WLC IP 주소를 입력합니다



Windows

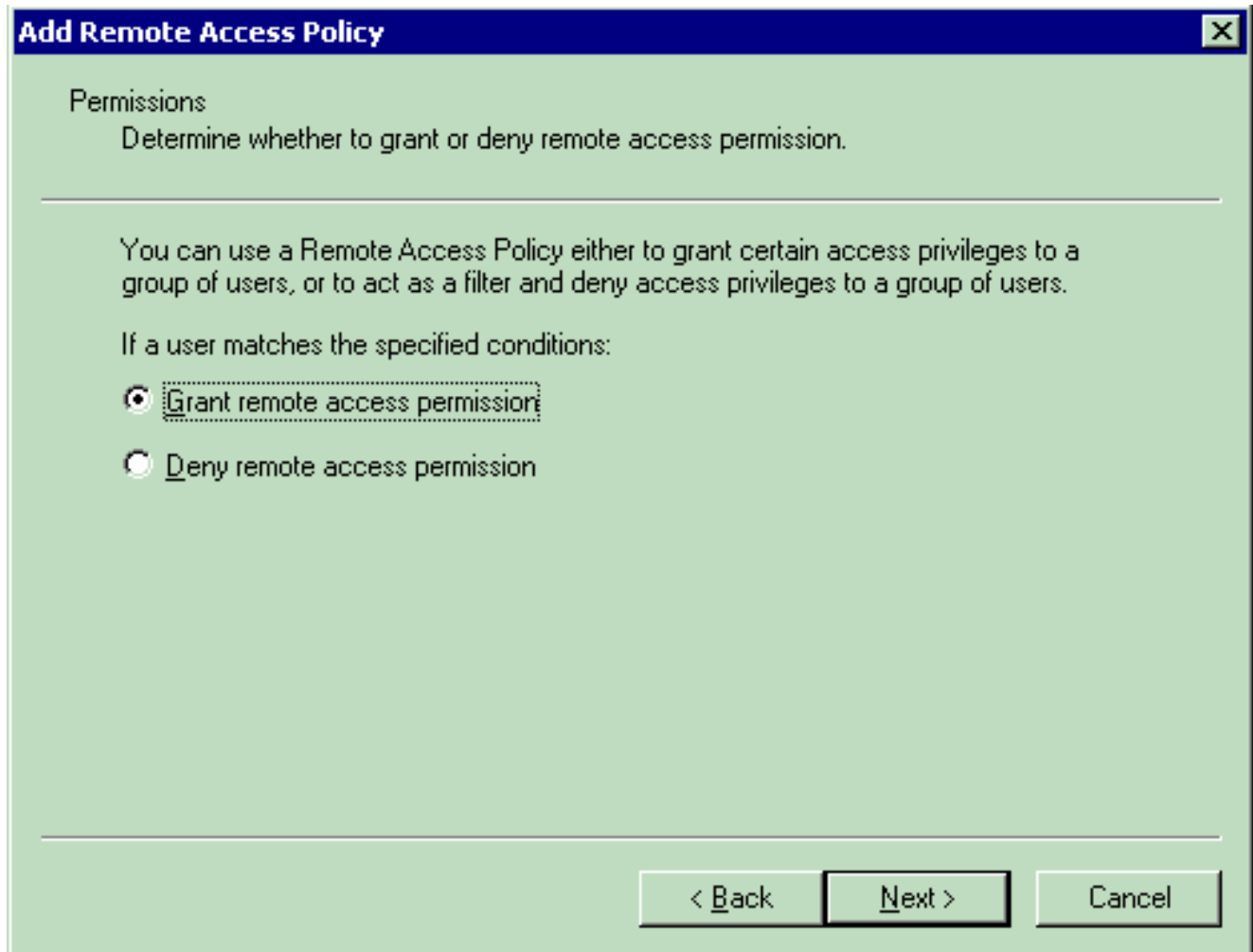
Groups(Windows 그룹) - 정책을 적용할 Windows 그룹(사용자 그룹)을 선택합니다.예를 들면 다음과 같습니다





이 예에서는 두 가지 조건만 표시합니다. 조건이 더 있는 경우 해당 조건도 추가하고 **Next(다음)**를 클릭합니다. 사용 권한 창이 나타납니다.

5. Permissions(권한) 창에서 **원격 액세스 권한 부여**를 선택합니다. 이 옵션을 선택하면 사용자가 지정된 조건(2단계)과 일치하면 사용자에게 액세스 권한이 부여됩니다.



6. Next(다음)를 클릭합니다.
7. 다음 단계는 사용자 프로필을 설정하는 것입니다.조건에 따라 사용자가 거부되거나 액세스 권한이 부여되도록 지정했을 수 있지만, 이 정책의 조건이 사용자 단위로 재정의된 경우에도 프로필을 사용할 수 있습니다

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.

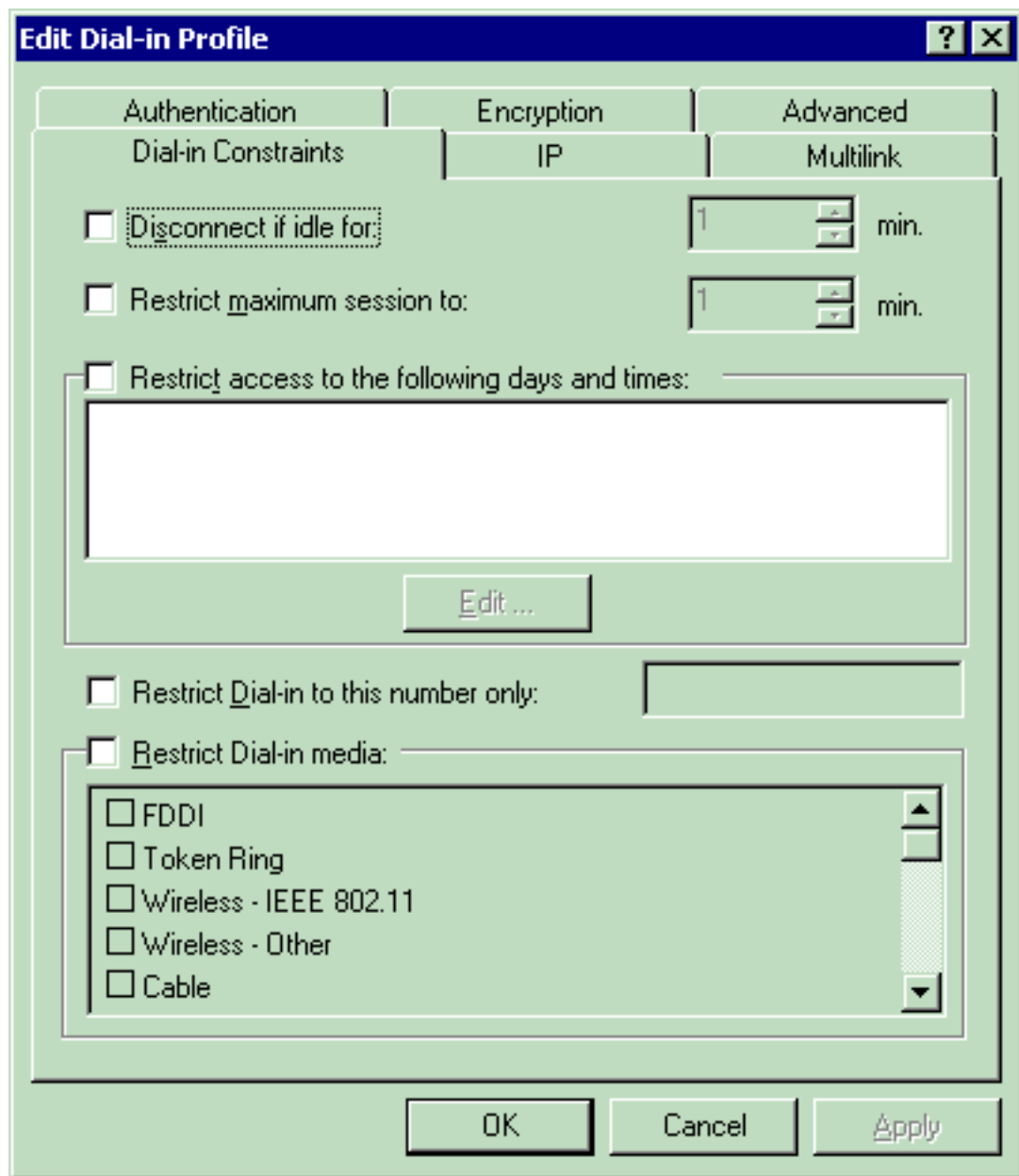
Edit Profile...

< Back

Finish

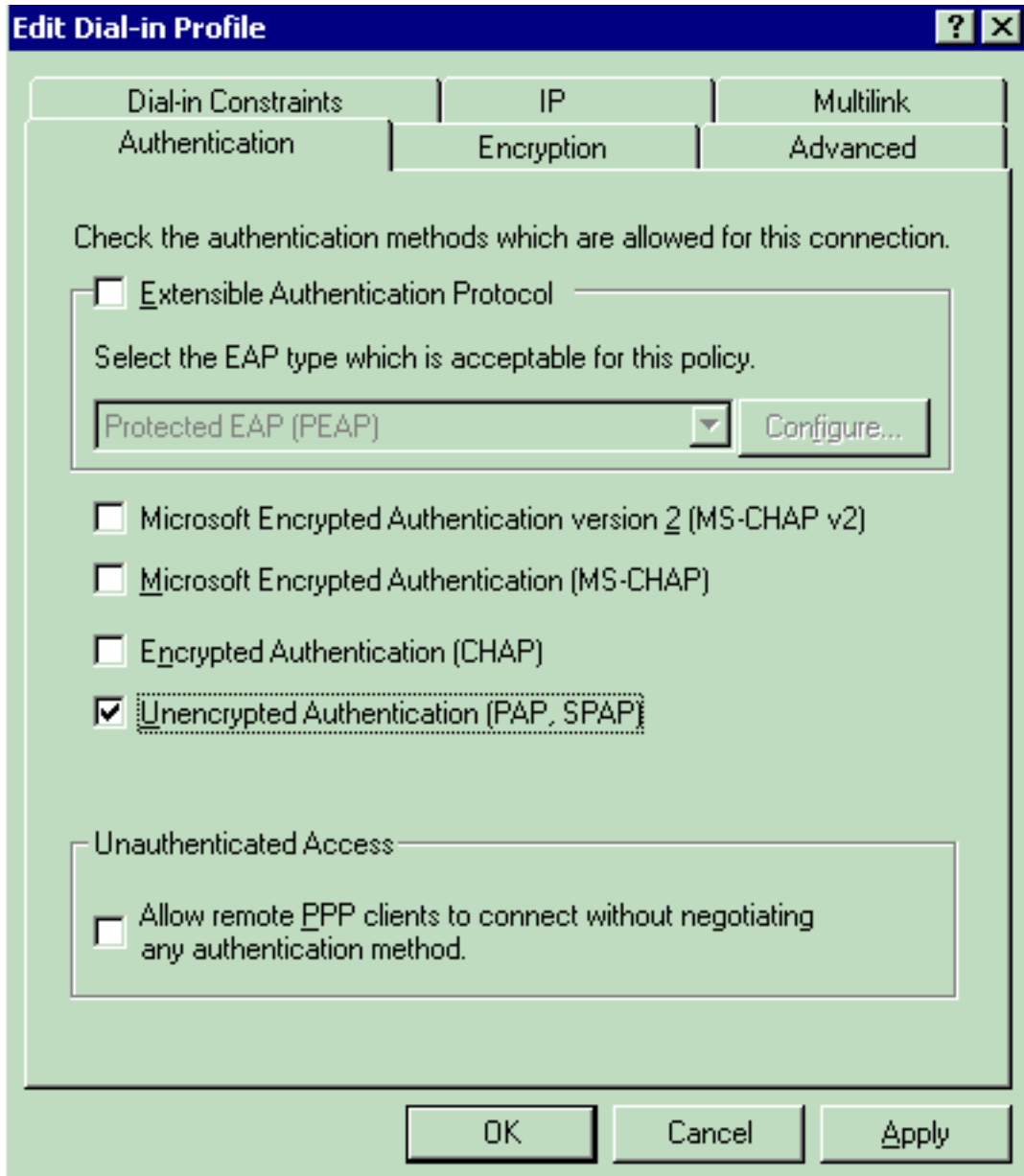
Cancel

사용자 프로필을 구성하려면 User Profile(사용자 프로필) 창에서 Edit Profile(프로필 수정)을 클릭합니다. 전화 접속 프로필 편집 창이 나타납니다



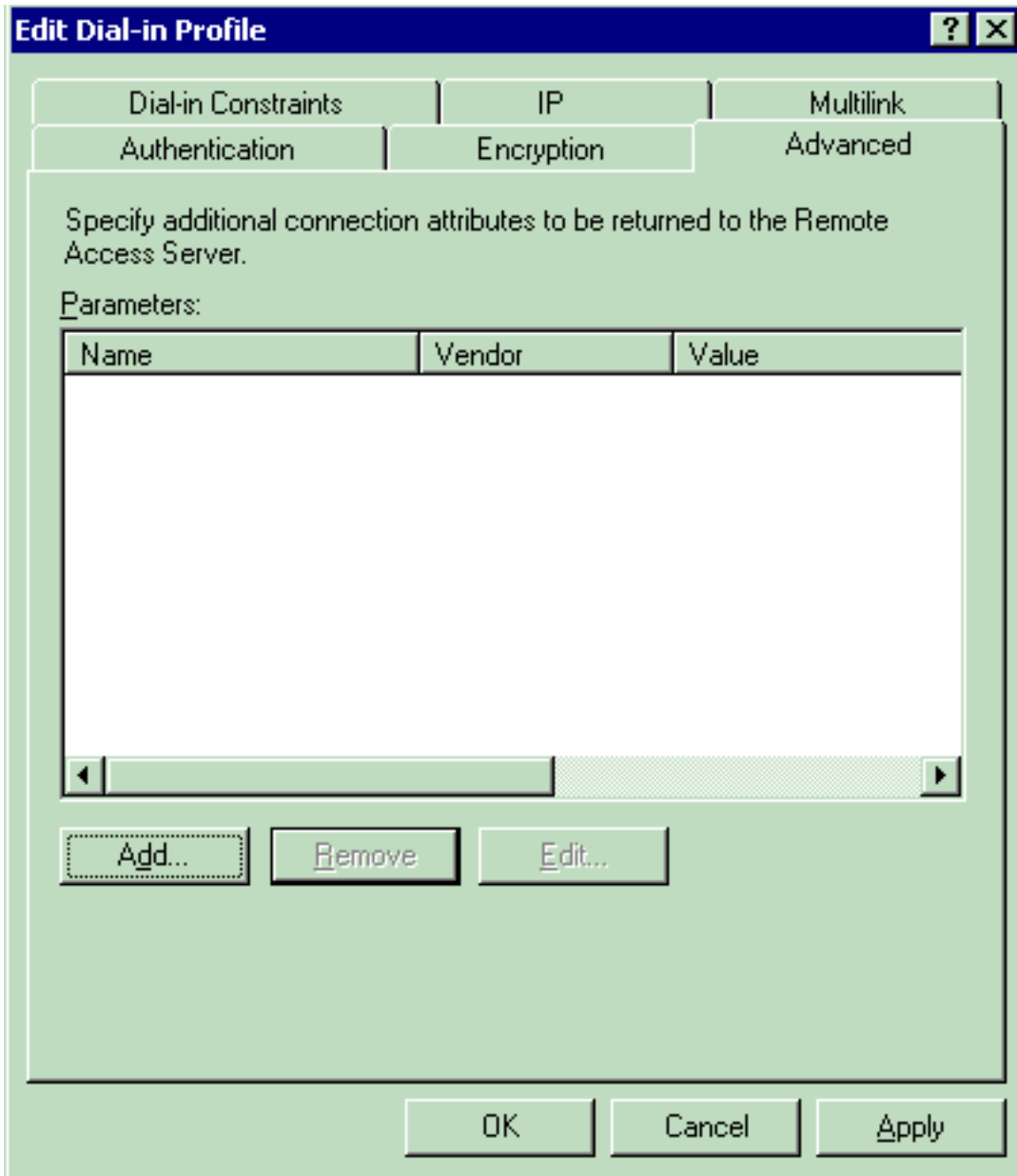
Authentication(

인증) 탭을 클릭한 다음 WLAN에서 사용되는 인증 방법을 선택합니다. 이 예에서는 암호화되지 않은 인증(PAP, SPAP)을 사용합니다



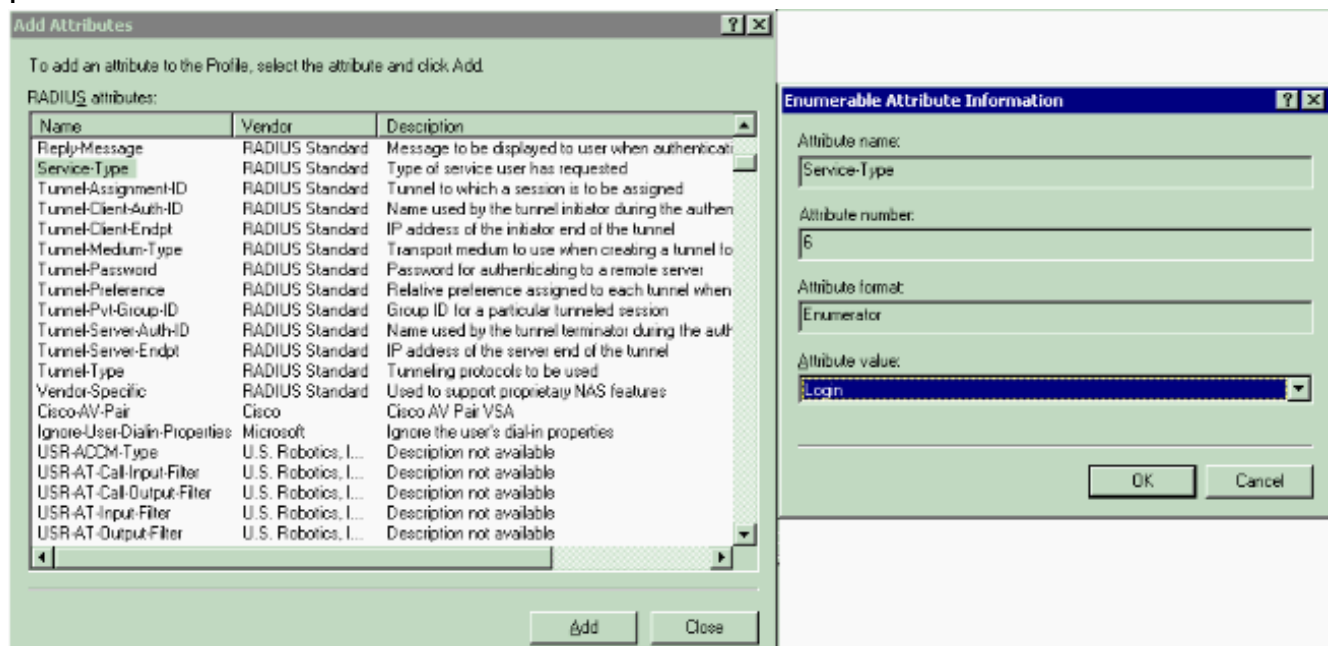
Advanced 탭을

클릭합니다. 모든 기본 매개변수를 제거하고 Add를 클릭합니다

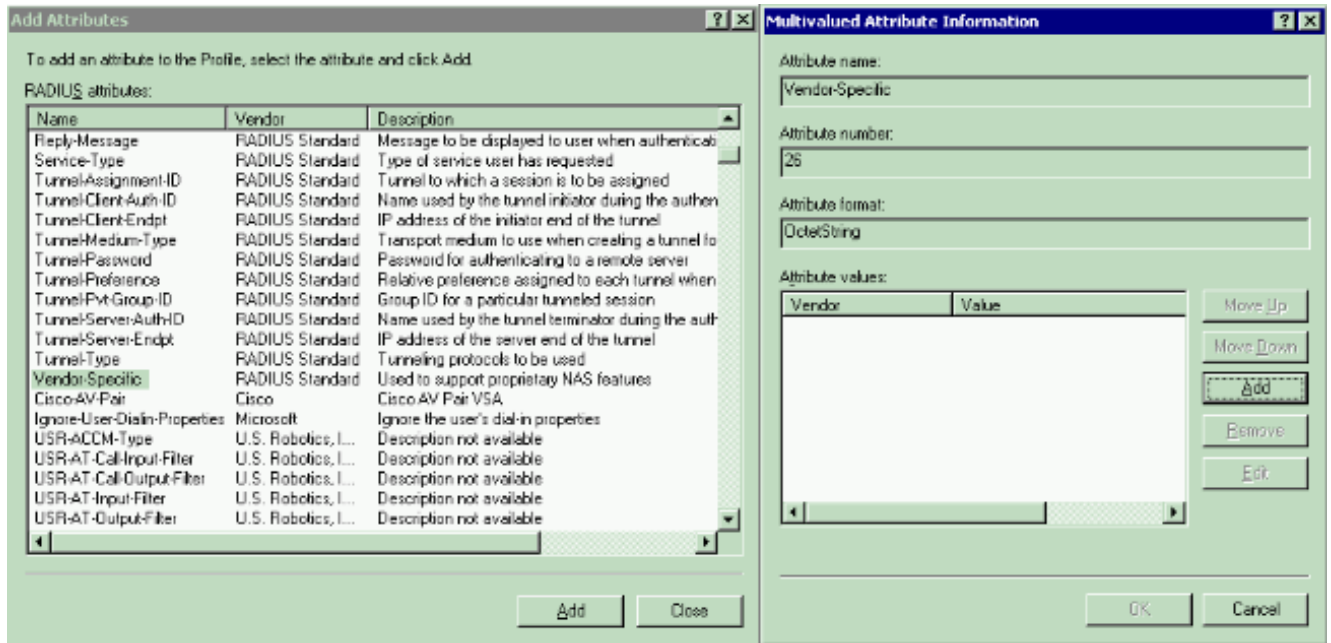


속성 추가 창에

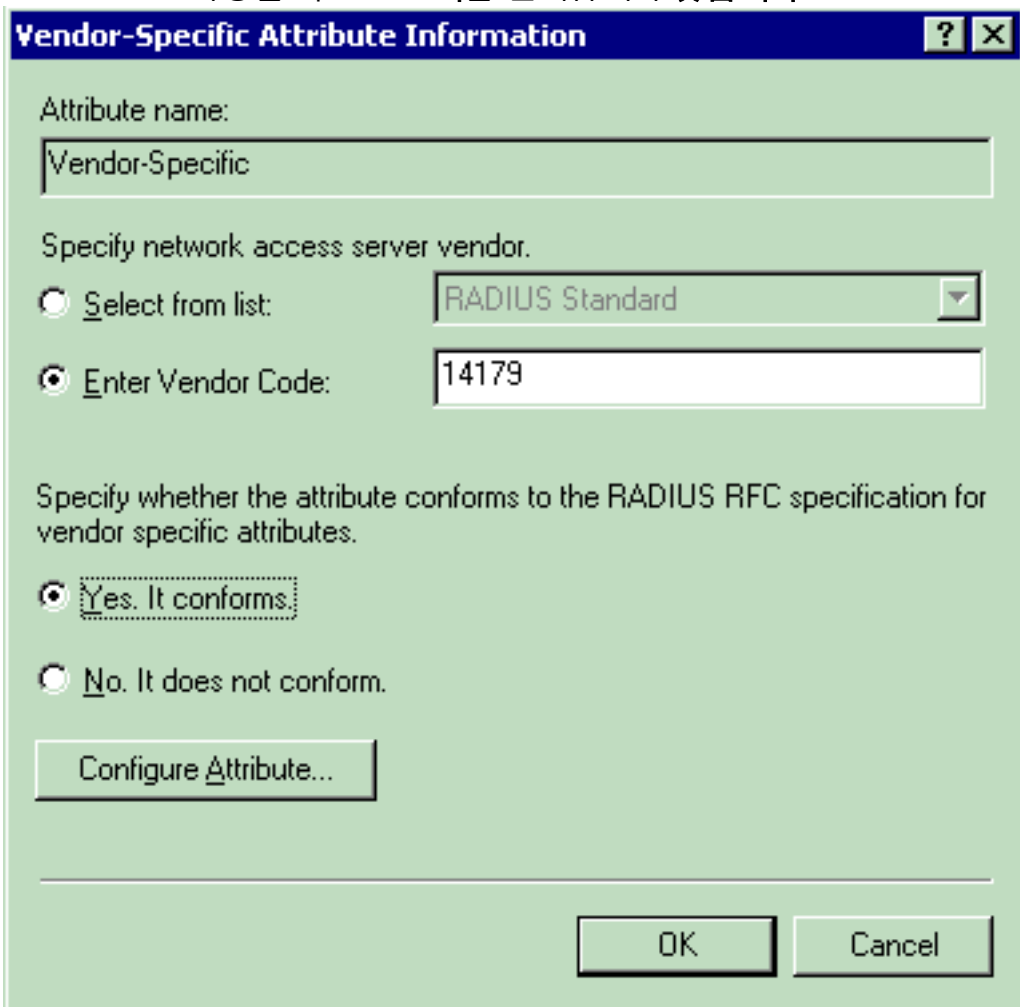
서 서비스 유형을 선택한 다음 다음 창에서 로그인 값을 선택합니다



그런 다음 RADIUS 특성 목록에서 Vendor-Specific 특성을 선택해야 합니다

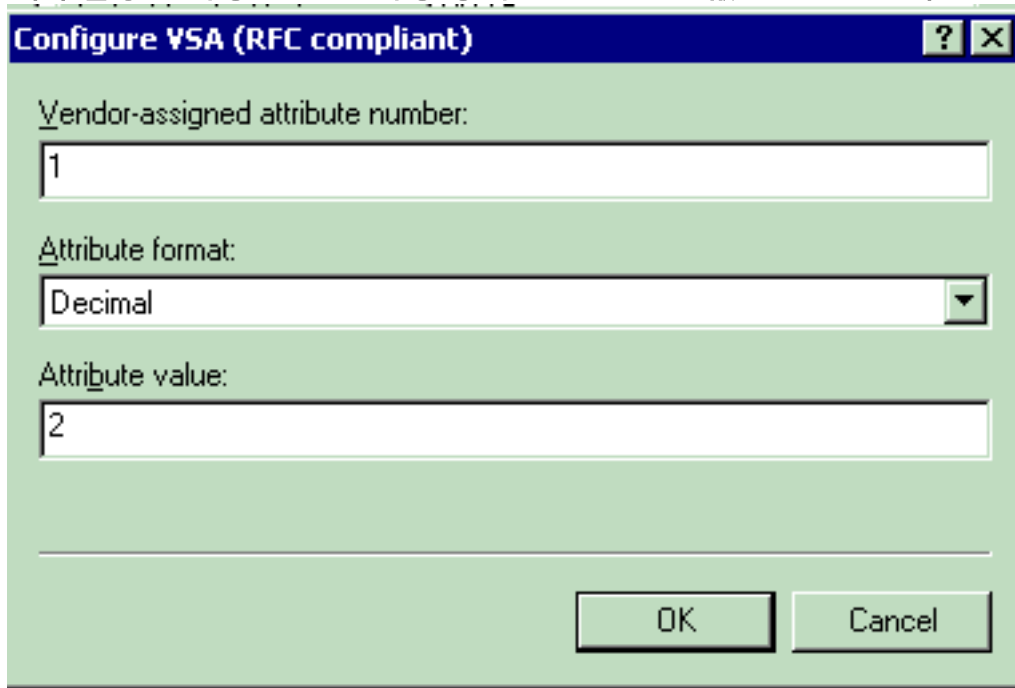


다음 창에서 Add(추가)를 클릭하여 새 VSA를 선택합니다. 판매업체 특정 속성 정보 창이 나타납니다. Specify network access server vendor(네트워크 액세스 서버 공급업체 지정)에서 Enter Vendor Code(벤더 코드 입력)를 선택합니다. Airespace VSA에 대한 공급업체 코드를 입력합니다. Cisco Airespace VSA의 공급업체 코드는 14179입니다. 이 특성은 VSA에 대한 RADIUS RFC 사양을 따르므로 예를 선택합니다. 맞습니다



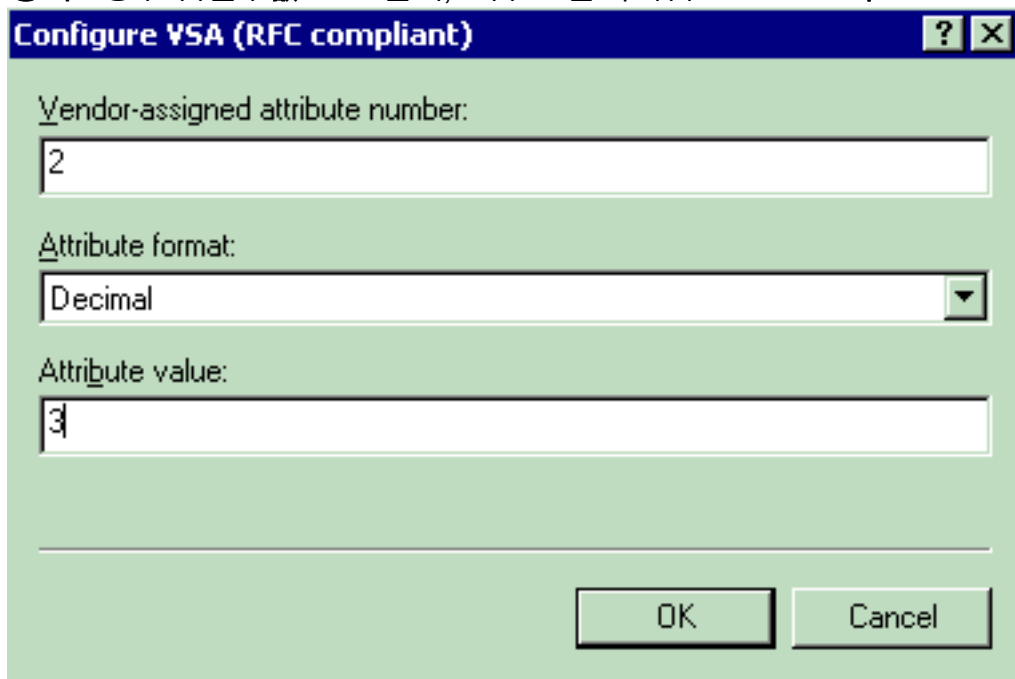
Configure Attribute를 클릭합니다. Configure VSA (RFC compliant)(VSA(VSA 호환) 구성) 창에서 사용할 VSA에 따라 달라지는 벤더 할당 특성 번호, Attribute 형식 및 Attribute(특성) 값을 입력합니다. 사용자별로 WLAN-ID를 설정하려면 Attribute Name(특성 이름) - Airespace-WLAN-Id 판매업

체가 할당한 특성 번호—1속성 형식 - 정수/십진수값 - WLAN-ID예 1



사용자별로 QoS 프

로파일을 설정하려면속성 이름—Airespace-QoS 레벨판매업체가 할당한 특성 번호—2속성 형식 - 정수/십진수값—0 - 실버;1. 금2 - 플래티넘3 - Bronze예 2



사용자별로 DSCP 값

을 설정하려면Attribute Name(특성 이름) - Airespace-DSCP판매업체가 할당한 특성 번호—3속성 형식 - 정수/십진수값 - DSCP 값예 3

Configure VSA (RFC compliant)

Vendor-assigned attribute number:
3

Attribute format:
Decimal

Attribute value:
46

OK Cancel

사용자별로 802.1p-Tag를 설정하는 경우 Attribute Name(특성 이름) - Airespace-802.1p-Tag 판매업체가 할당한 특성 번호—4속성 형식 - 정수/십진수값—802.1p-태그예 4

Configure VSA (RFC compliant)

Vendor-assigned attribute number:
4

Attribute format:
Decimal

Attribute value:
5

OK Cancel

사용자별로 인터페이스(VLAN)를 설정하는 경우 Attribute Name(특성 이름) - Airespace-Interface-Name 판매업체가 할당한 특성 번호—5속성 형식 - 문자열값 - 인터페이스 이름예 5

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

Vendor-assigned attribute number:

Attribute format:

Attribute value:

[OK] [Cancel]

사용자별로 ACL을 설정하는 경우 Attribute Name(특성 이름) - Airespace-ACL-Name 판매업체가 할당한 특성 번호—6 속성 형식 - 문자열값 - ACL-이름에 6

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

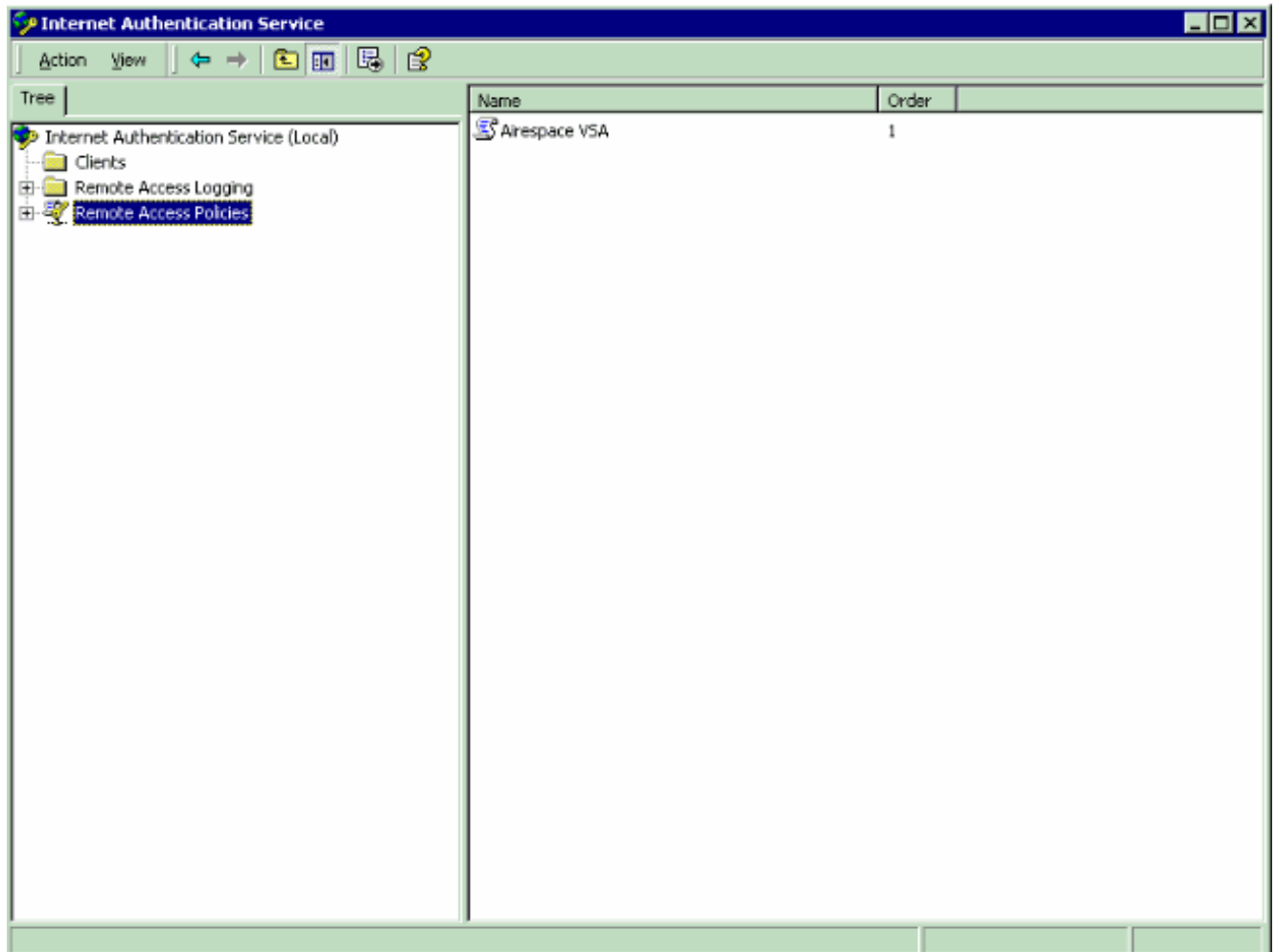
Vendor-assigned attribute number:

Attribute format:

Attribute value:

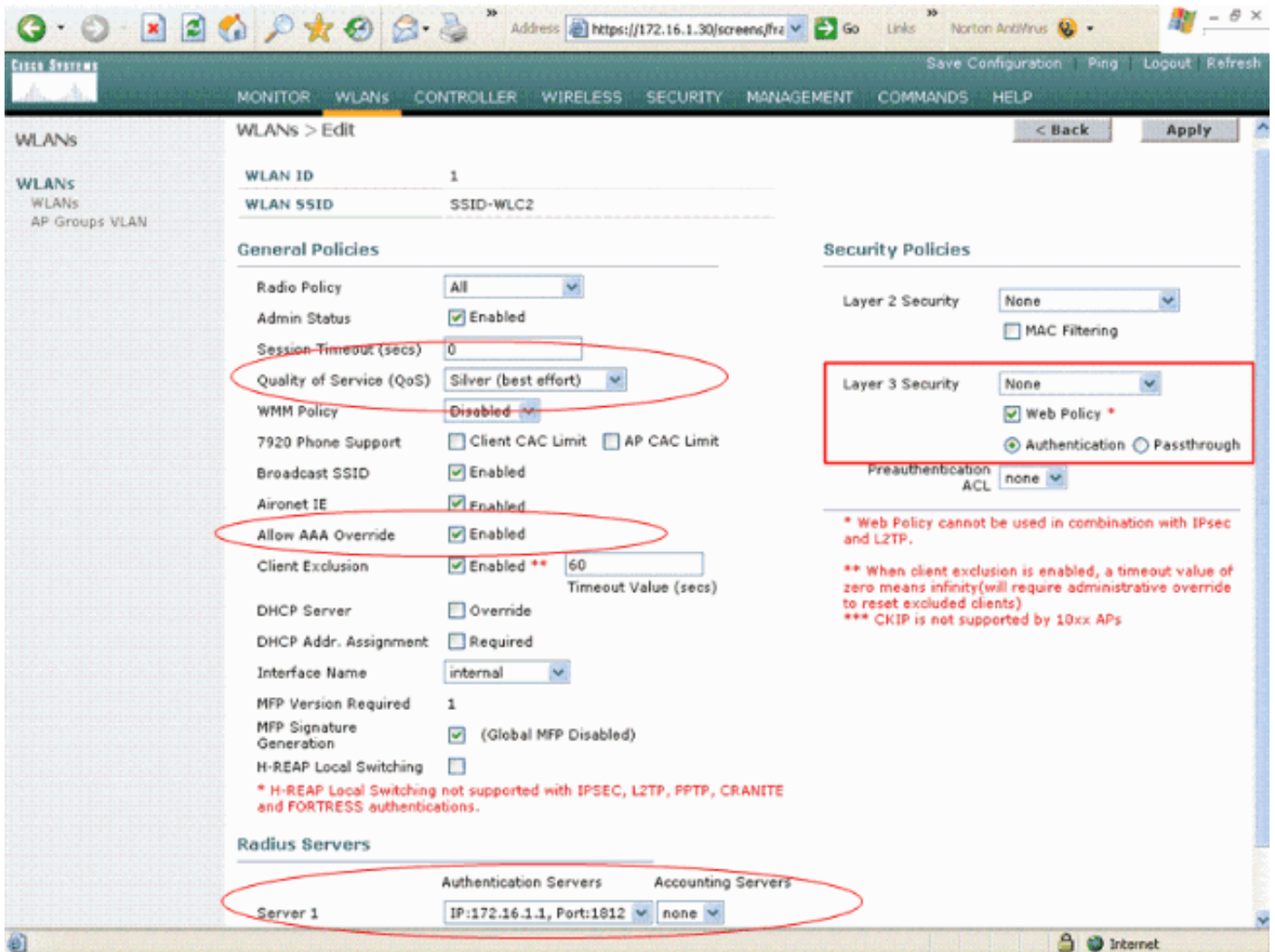
[OK] [Cancel]

8. VSA를 구성한 후 사용자 프로필 창이 표시될 때까지 OK를 클릭합니다.
9. 그런 다음 **Finish(마침)**를 클릭하여 컨피그레이션을 완료합니다. Remote Access Policies(원격 액세스 정책) 아래에서 새 정책을 볼 수 있습니다



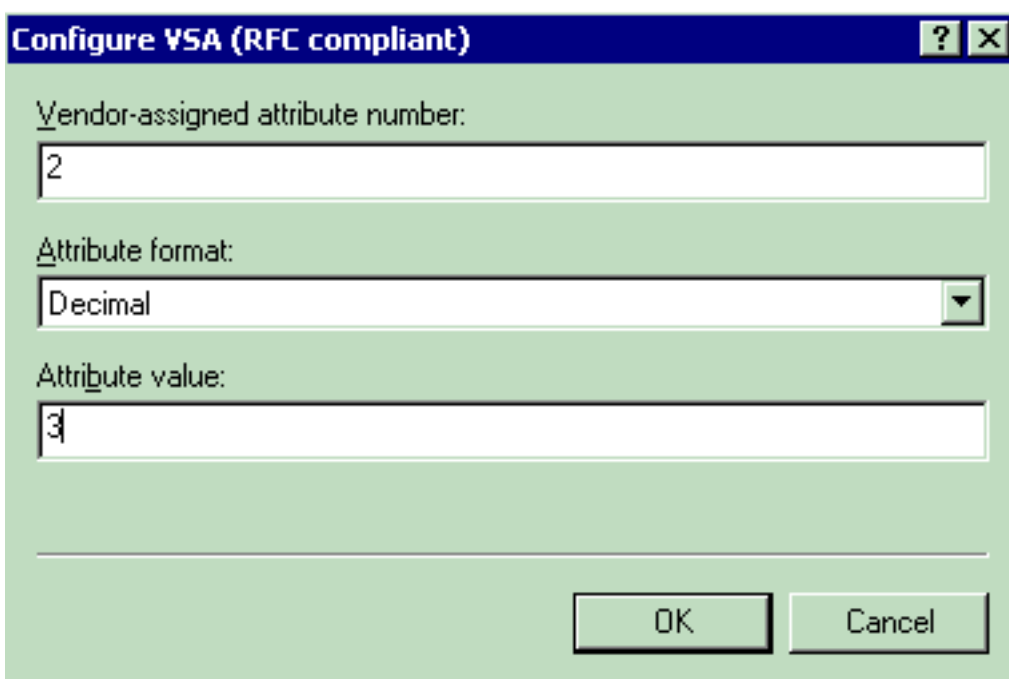
컨피그레이션 예

이 예에서는 웹 인증을 위해 WLAN이 구성됩니다.사용자는 IAS RADIUS 서버에서 인증되며 RADIUS 서버는 사용자별로 QoS 정책을 할당하도록 구성됩니다.



이 창에서 볼 수 있듯이 웹 인증이 활성화되고 인증 서버가 172.16.1.1이며 WLAN에서도 AAA 재정의가 활성화됩니다.이 WLAN에 대한 기본 QoS 설정은 Silver로 설정됩니다.

IAS RADIUS 서버에서 RADIUS 수락 요청의 QoS 특성 Bronze를 반환하는 원격 액세스 정책이 구성됩니다.이는 QoS 특성에 맞는 VSA를 구성할 때 수행됩니다.



IAS 서버에서 원격 액세스 정책을 구성하는 방법에 대한 자세한 내용은 이 문서의 [IAS](#) 섹션에서 원격 액세스 정책 구성 섹션을 참조하십시오.

IAS 서버, WLC 및 LAP가 이 설정에 대해 구성되면 무선 클라이언트는 웹 인증을 사용하여 연결할 수 있습니다.

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

사용자가 사용자 ID와 비밀번호를 사용하여 WLAN에 연결할 때 WLC는 IAS RADIUS 서버에 자격 증명을 전달하여 조건과 원격 액세스 정책에 구성된 사용자 프로필을 인증합니다. 사용자 인증에 성공하면 RADIUS 서버는 AAA 재정의 값도 포함하는 RADIUS 수락 요청을 반환합니다. 이 경우 사용자의 QoS 정책이 반환됩니다.

인증 중에 발생하는 이벤트 순서를 확인하기 위해 **debug aaa all enable** 명령을 실행할 수 있습니다. 다음은 샘플 출력입니다.

```
(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
...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)

```

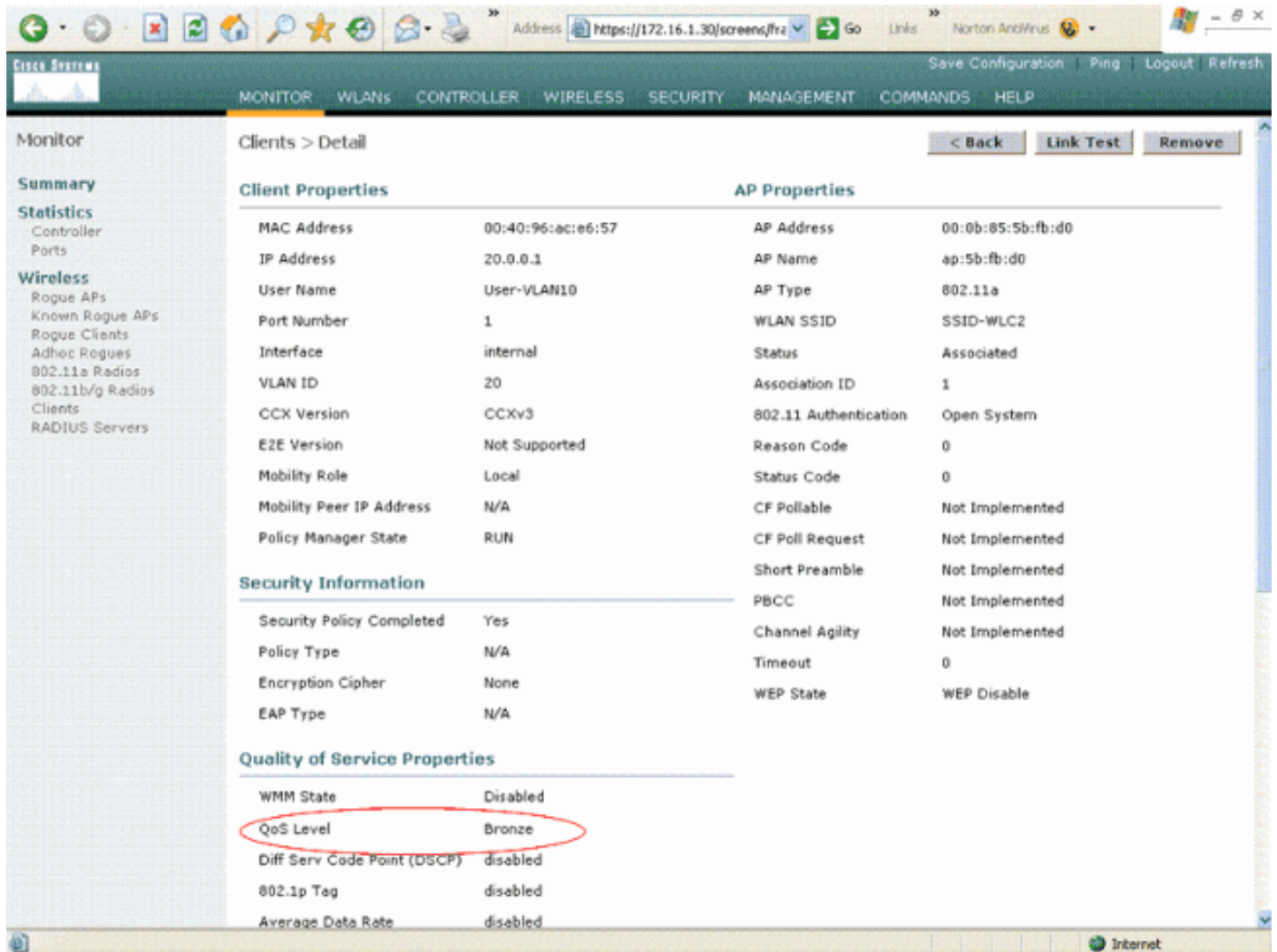
```

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)

```

출력에서 볼 수 있듯이 사용자는 인증됩니다.그런 다음 RADIUS 수락 메시지와 함께 AAA 재정의 값이 반환됩니다.이 경우 사용자에게 QoS 정책이 Bronze로 지정됩니다.

WLC GUI에서도 이를 확인할 수 있습니다.예를 들면 다음과 같습니다.



참고: 이 SSID의 기본 QoS 프로파일은 Silver입니다.그러나 AAA 재정의가 선택되고 사용자가 IAS 서버에서 QoS 프로파일인 Bronze로 구성되었으므로 기본 QoS 프로파일이 재정의됩니다.

문제 해결

WLC에서 `debug aaa all enable` 명령을 사용하여 컨피그레이션 문제를 해결할 수 있습니다.작업 네트워크에서 이 디버그 출력의 예는 이 문서의 [Verify](#) 섹션에 나와 있습니다.

참고: debug 명령을 사용하기 전에 디버그 [명령에 대한 중요 정보](#)를 참조하십시오.

관련 정보

- [Cisco Wireless LAN Controller 컨피그레이션 가이드, 릴리스 4.0](#)
- [WLC 및 Cisco Secure ACS 컨피그레이션을 통한 SSID를 기반으로 WLAN 액세스 제한 예](#)
- [무선 제품 지원](#)
- [기술 지원 및 문서 - Cisco Systems](#)