

Microsoft Windows 2000 IAS RADIUS 서버에 대한 외부 인증을 사용하여 Cisco VPN 5000 Concentrator 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[Cisco VPN 5000 Concentrator 컨피그레이션](#)

[Microsoft Windows 2000 IAS RADIUS 서버 구성](#)

[결과 확인](#)

[VPN 클라이언트 구성](#)

[Concentrator 로그](#)

[문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 RADIUS를 사용하는 Microsoft Windows 2000 IAS(Internet Authentication Server)에 대한 외부 인증을 사용하여 Cisco VPN 5000 Concentrator를 구성하는 데 사용되는 절차에 대해 설명합니다.

참고: CHAP(Challenge Handshake Authentication Protocol)가 작동하지 않습니다. PAP>Password Authentication Protocol)만 사용합니다. 자세한 내용은 Cisco 버그 ID [CSCdt96941](#)([등록된](#) 고객만 해당)을 참조하십시오.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- Cisco VPN 5000 Concentrator Software 버전 6.0.16.0001

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 표기 규칙](#)을 참조하십시오.

Cisco VPN 5000 Concentrator 컨피그레이션

```
VPN5001_4B9CBA80

VPN5001_4B9CBA80> show config
Enter Password:

Edited Configuration not Present, using Running

[ General ]
EthernetAddress      = 00:02:4b:9c:ba:80
DeviceType           = VPN 5001 Concentrator
ConfiguredOn        = Timeserver not configured
ConfiguredFrom      = Command Line, from Console
EnablePassword      =
Password            =

[ IP Ethernet 0 ]
Mode                 = Routed
SubnetMask           = 255.255.255.0
IPAddress            = 172.18.124.223

[ IP Ethernet 1 ]
Mode                 = Off

[ IKE Policy ]
Protection           = MD5_DES_G1

[ VPN Group "rtp-group" ]
BindTo               = "ethernet0"
Transform            = esp(md5,des)
LocalIPNet           = 10.1.1.0/24
MaxConnections      = 10
IPNet                = 0.0.0.0/0

[ RADIUS ]
BindTo               = "ethernet0"
ChallengeType        = PAP
PAPAuthSecret        = "pappassword"
PrimAddress          = "172.18.124.108"
Secret               = "radiuspassword"
UseChap16            = Off
Authentication       = On

[ Logging ]
Level                = 7
Enabled              = On

Configuration size is 1065 out of 65500 bytes.
VPN5001_4B9CBA80#
```

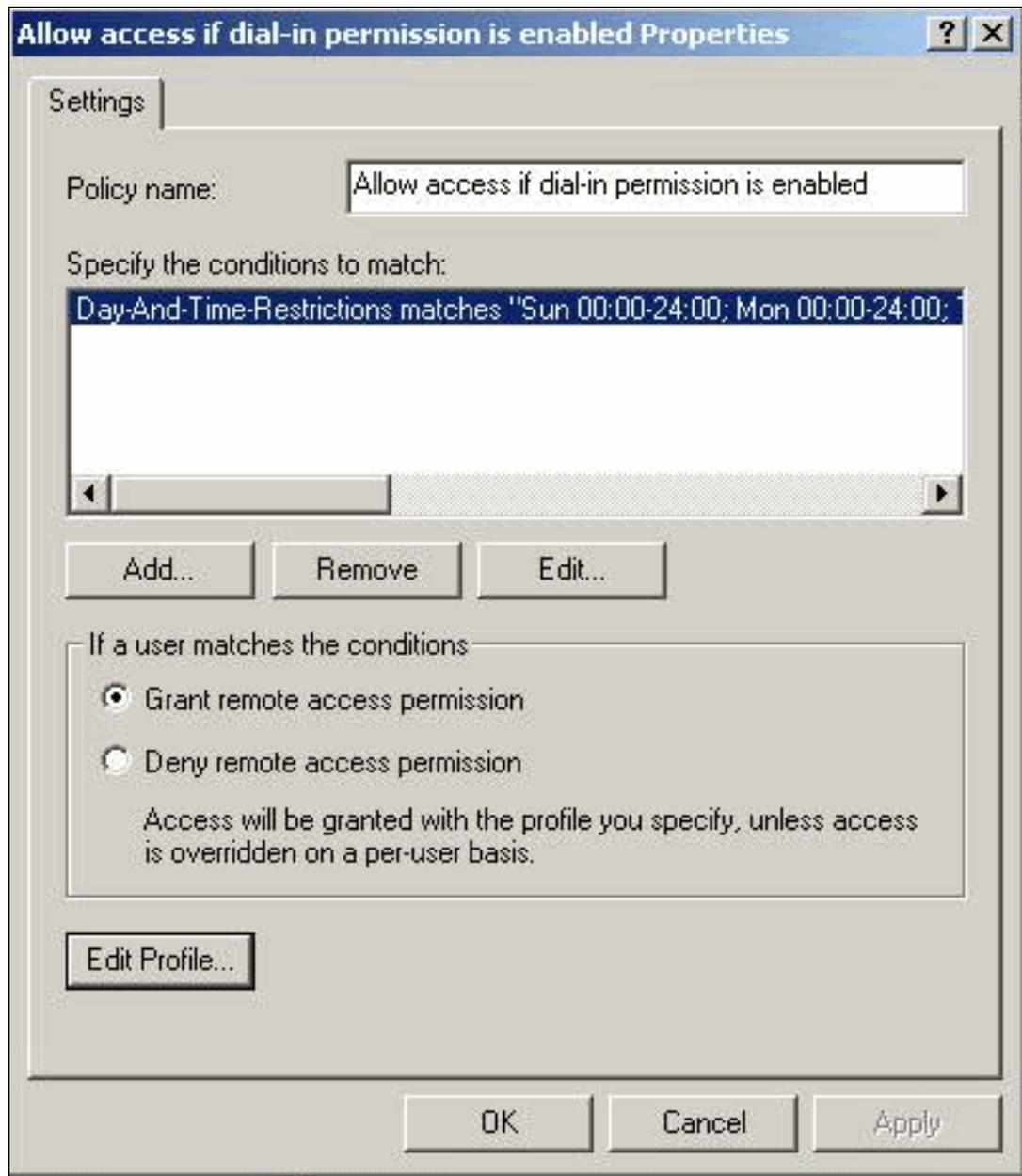
Microsoft Windows 2000 IAS RADIUS 서버 구성

이 단계는 간단한 Microsoft Windows 2000 IAS RADIUS 서버 구성을 안내합니다.

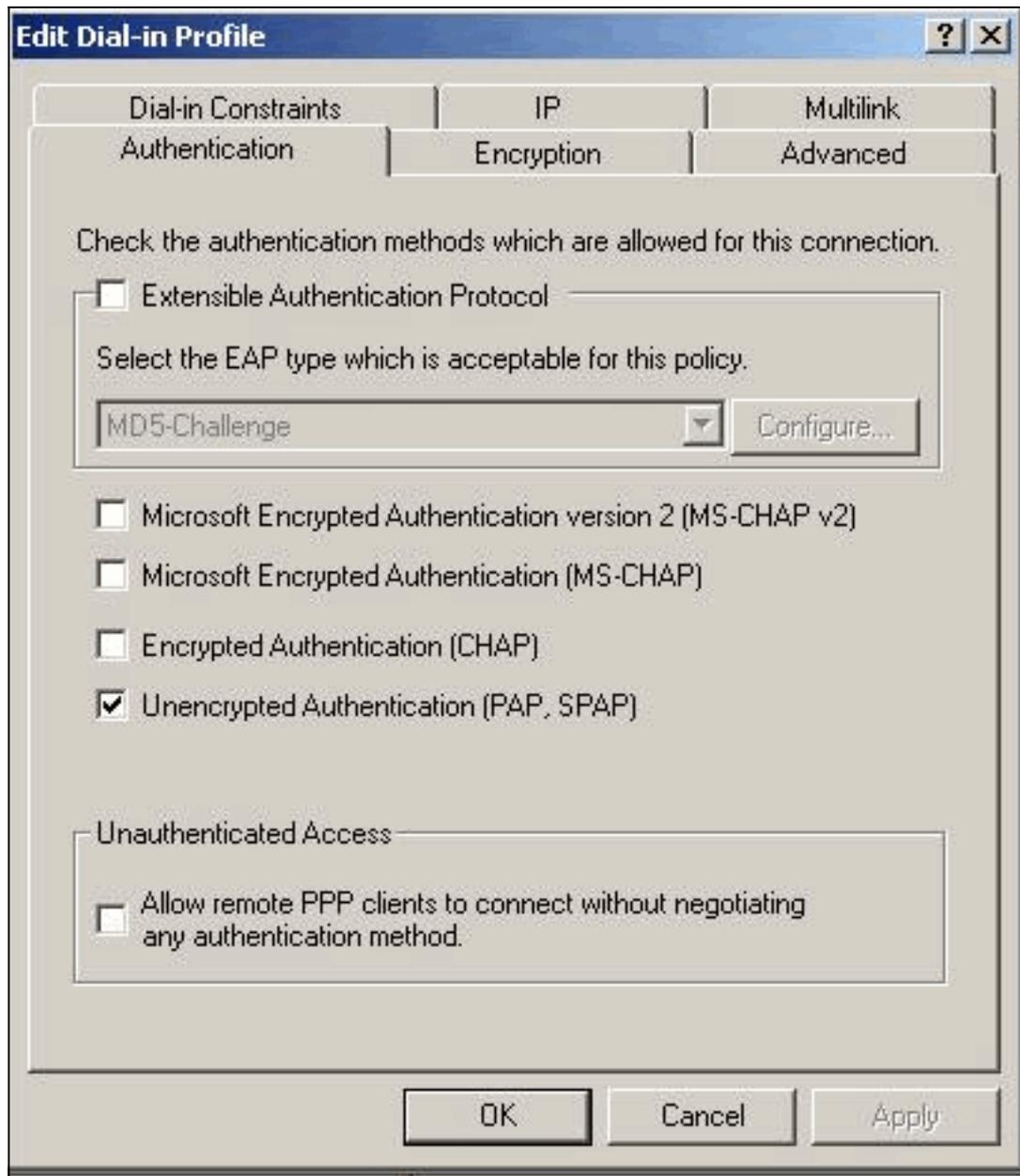
1. Microsoft Windows 2000 IAS 속성에서 **Clients**를 선택하고 새 클라이언트를 만듭니다.이 예에서는 VPN5000이라는 항목이 생성됩니다. Cisco VPN 5000 Concentrator의 IP 주소는 172.18.124.223입니다. Client-Vendor 드롭다운 상자에서 **Cisco**를 선택합니다. 공유 비밀은 [VPN Concentrator](#) 컨피그레이션의 [RADIUS] 섹션에 있는 암호입니다

The screenshot shows the 'VPN5000 Properties' dialog box. The 'Settings' tab is active. The 'Friendly name for client:' field contains 'VPN5000'. The 'Client address' section has 'Address (IP or DNS):' set to '172.18.124.223'. The 'Client-Vendor:' dropdown is set to 'Cisco'. The checkbox 'Client must always send the signature attribute in the request' is unchecked. The 'Shared secret:' and 'Confirm shared secret:' fields both contain 'xxxxxxx'. The 'OK', 'Cancel', and 'Apply' buttons are at the bottom.

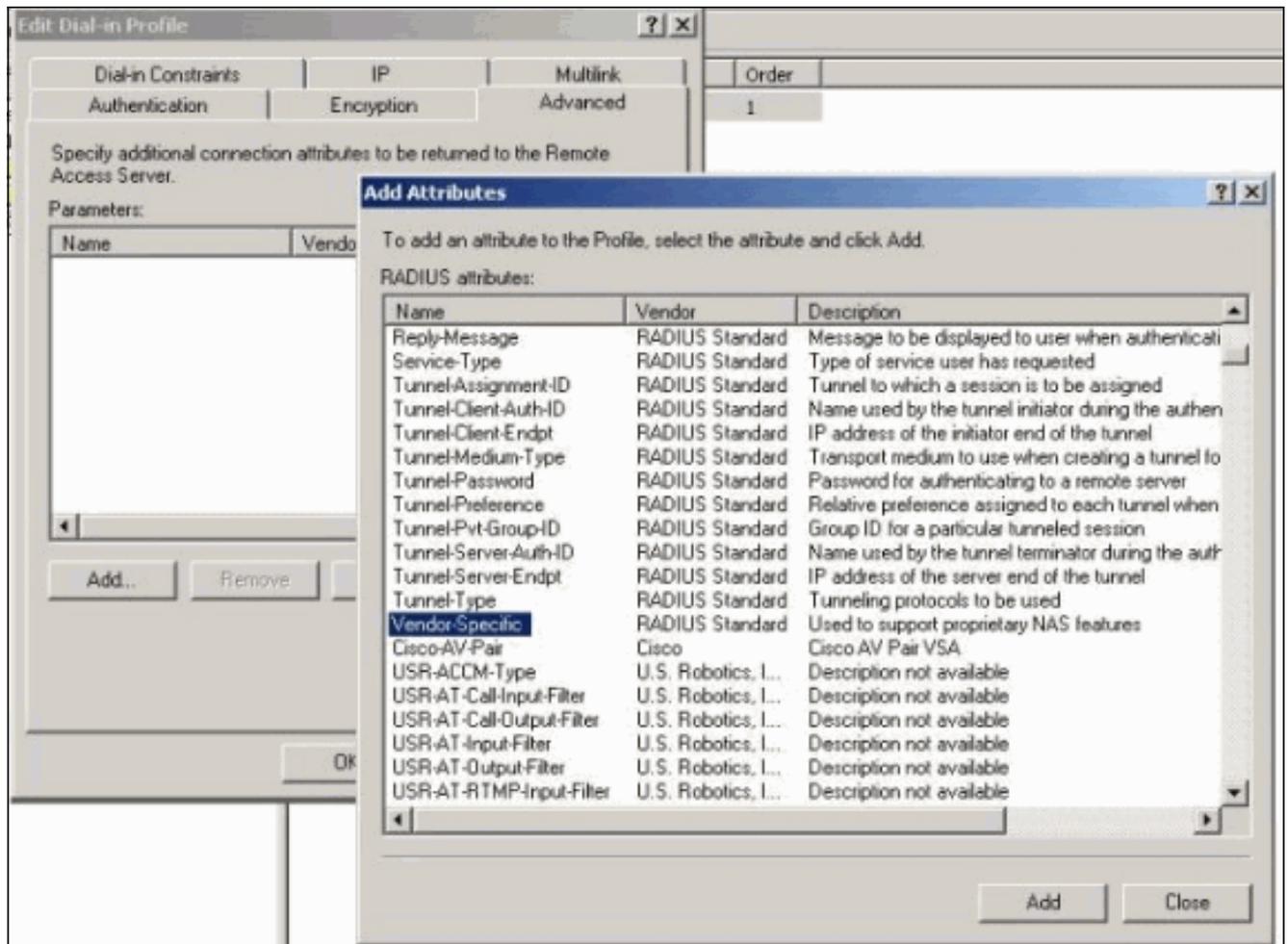
2. Remote Access Policy(원격 액세스 정책)의 속성 아래에서 "If a user matches the conditions(사용자가 조건과 일치할 경우)" 섹션 아래에서 **Grant remote access permission(원격 액세스 권한 부여)**을 선택한 다음 Edit Profile(프로필 수정)을 클릭합니다



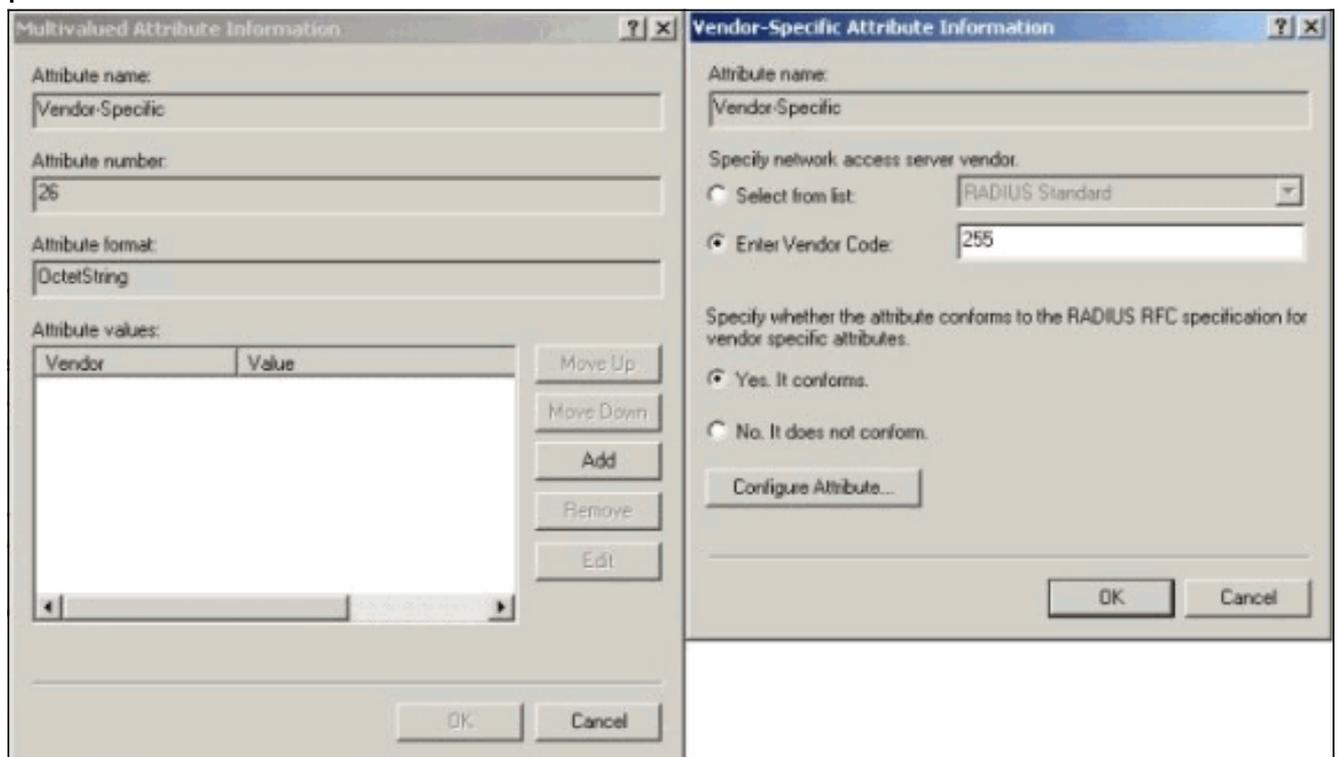
3. Authentication(인증) 탭을 클릭하고 Unencrypted Authentication(암호화되지 않은 인증)(PAP, SPAP)만 선택되었는지 확인합니다



4. Advanced(고급) 탭을 선택하고 Add(추가)를 클릭하고 Vendor-Specific(벤더별)을 선택합니다



5. 공급업체별 특성에 대한 다중값 속성 정보 대화 상자에서 **추가**를 클릭하여 판매업체별 특성 정보 대화 상자로 이동합니다. Enter **Vendor Code(공급업체 코드 입력)**를 선택하고 인접한 상자에 255를 입력합니다. 그런 다음 **예**를 선택합니다. 이를 준수하고 **특성 구성**을 클릭합니다



6. Configure VSA (RFC compliant)(VSA(RFC 호환) 구성) 대화 상자에서 Vendor-assigned attribute number에 4를 입력하고 Attribute 형식에 대한 String을 입력하고 Attribute 값에 대해 rtp-group(Cisco VPN 5000 Concentrator에 있는 VPN 그룹의 이름)을 입력합니다. 확인을 클

릭하고 5단계를 반복합니다



Configure VSA (RFC compliant)

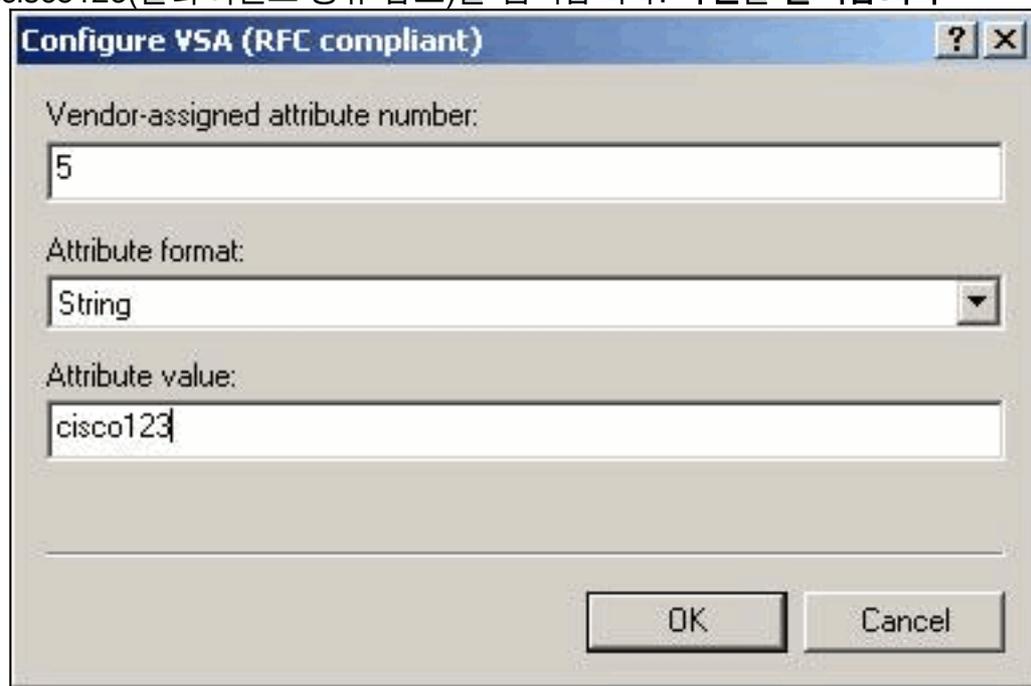
Vendor-assigned attribute number:
4

Attribute format:
String

Attribute value:
rtp-group

OK Cancel

7. Configure VSA (RFC compliant)(VSA(RFC 호환) 구성) 대화 상자에서 판매업체 지정 특성 번호에 4를 입력하고 Attribute(특성) 형식에 **String**(문자열)을 입력하고 Attribute 값에 대해 cisco123(클라이언트 공유 암호)을 입력합니다. **확인**을 클릭합니다



Configure VSA (RFC compliant)

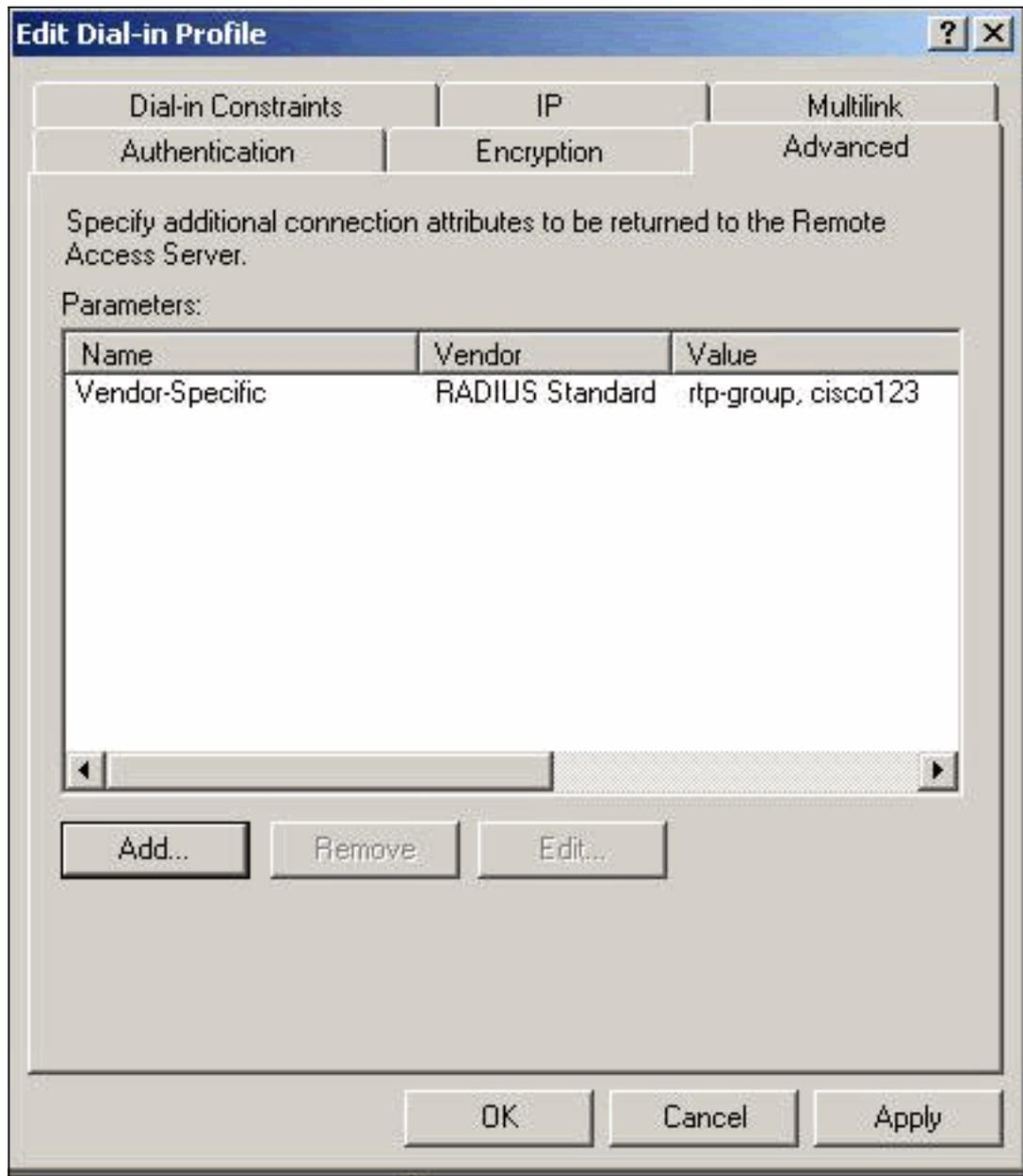
Vendor-assigned attribute number:
5

Attribute format:
String

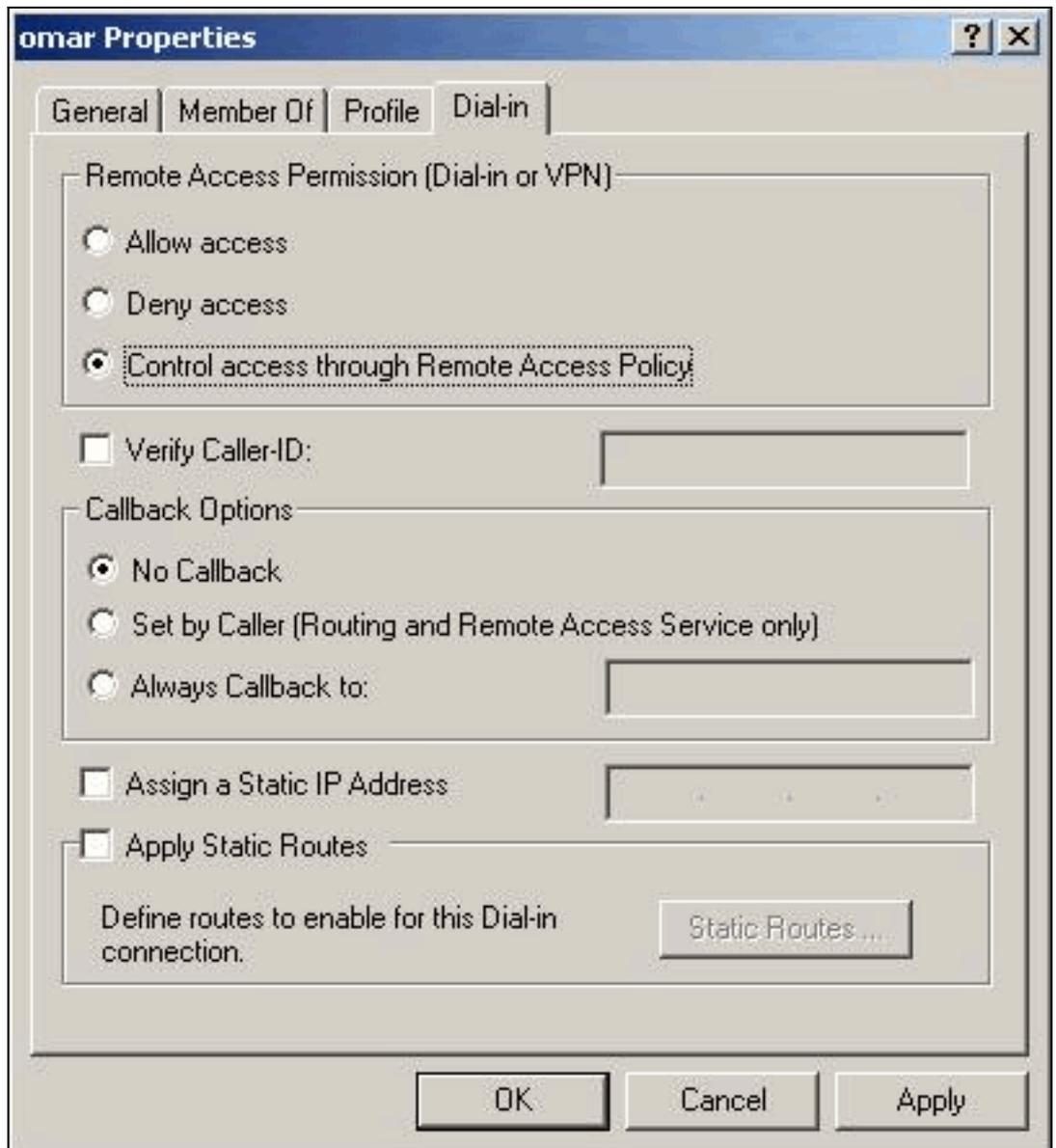
Attribute value:
cisco123

OK Cancel

8. Vendor-Specific 속성에는 두 개의 값(그룹 및 VPN 비밀번호)이 포함되어 있습니다



9. 사용자 속성에서 전화 접속 탭을 클릭하고 원격 액세스 정책을 통한 제어 액세스가 선택되었



는지 확인합니다.

결과 확인

이 섹션에서는 컨피그레이션이 제대로 작동하는지 확인하는 데 사용할 수 있는 정보를 제공합니다.

일부 **show** 명령은 [출력 인터프리터 툴](#) 에서 지원되는데(등록된 고객만), 이 툴을 사용하면 **show** 명령 출력의 분석 결과를 볼 수 있습니다.

- **show radius statistics** - RADIUS 섹션에서 식별된 VPN Concentrator와 기본 RADIUS 서버 간의 통신에 대한 패킷 통계를 표시합니다.
- **show radius config** - RADIUS 매개변수에 대한 현재 설정을 표시합니다.

show radius statistics 명령의 출력입니다.

```
VPN5001_4B9CBA80>show radius statistics
```

```
RADIUS Stats
```

Accounting	Primary	Secondary
Requests	0	na
Responses	0	na
Retransmissions	0	na

Bad Authenticators	0	na
Malformed Responses	0	na
Packets Dropped	0	na
Pending Requests	0	na
Timeouts	0	na
Unknown Types	0	na

Authentication	Primary	Secondary
Requests	3	na
Accepts	3	na
Rejects	0	na
Challenges	0	na
Retransmissions	0	na
Bad Authenticators	0	na
Malformed Responses	0	na
Packets Dropped	0	na
Pending Requests	0	na
Timeouts	0	na
Unknown Types	0	na

VPN5001_4B9CBA80>

show radius config 명령의 출력입니다.

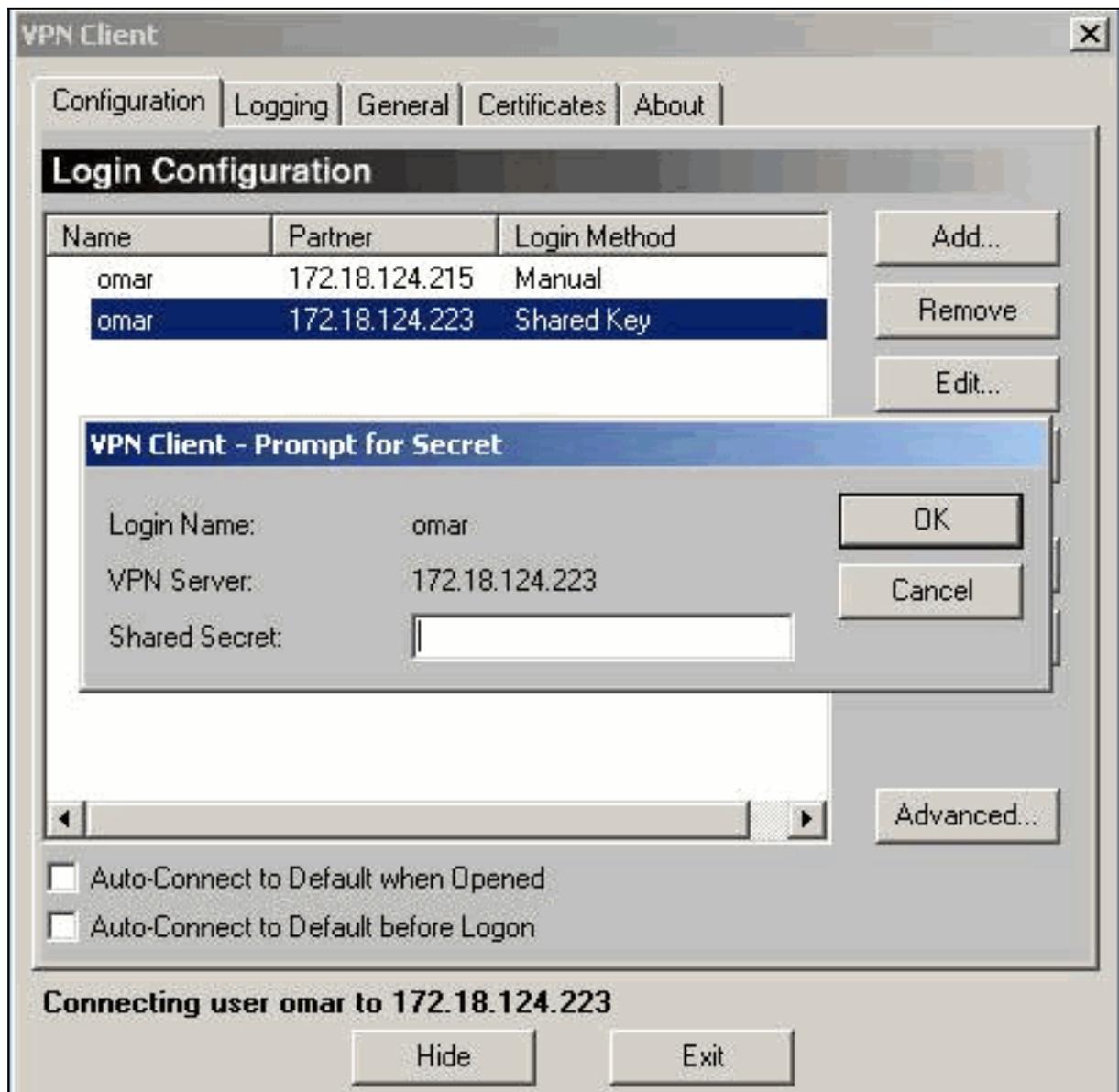
```
RADIUS      State    UDP  CHAP16
Authentication  On      1812 No
Accounting      Off     1813 n/a
Secret          'radiuspassword'
```

```
Server      IP address      Attempts  AcctSecret
Primary     172.18.124.108      5  n/a
Secondary   Off
```

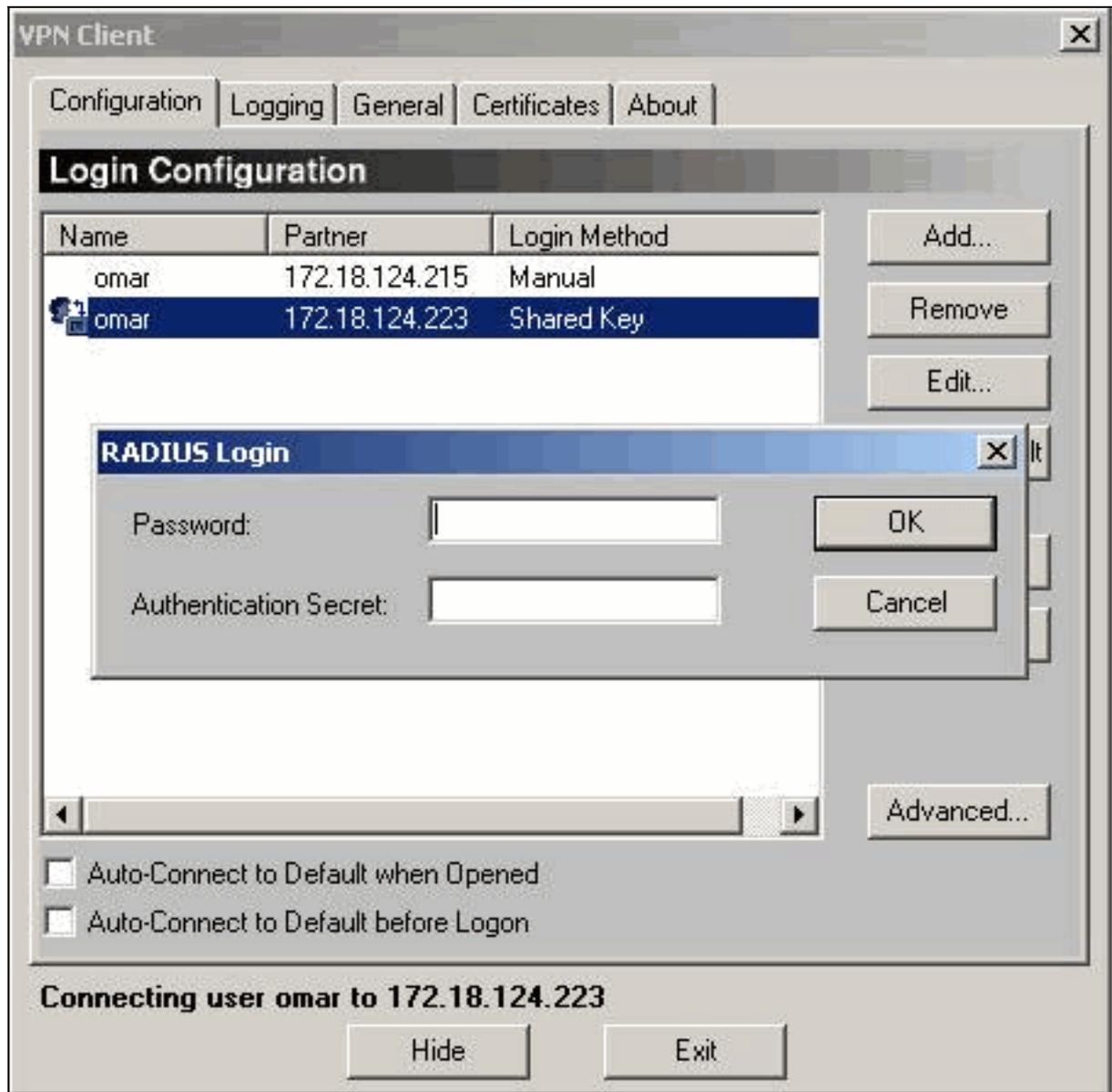
VPN 클라이언트 구성

이 절차에서는 VPN 클라이언트의 컨피그레이션을 안내합니다.

1. VPN Client 대화 상자에서 Configuration 탭을 선택합니다. 그런 다음 VPN Client-Prompt for Secret 대화 상자에서 VPN Server 아래에 공유 암호를 입력합니다. VPN Client 공유 비밀은 VPN Concentrator에서 특성 5의 VPN 비밀번호에 입력한 값입니다



- 공유 암호를 입력하면 암호 및 인증 암호를 입력하라는 메시지가 표시됩니다. 비밀번호는 해당 사용자의 RADIUS 비밀번호이며 인증 비밀은 [VPN Concentrator](#)의 [RADIUS] 섹션에 있는 PAP 인증 [비밀번호입니다](#)



[Concentrator 로그](#)

```

Notice 4080.11 seconds New IKE connection: [172.18.124.108]:1195:omar
Debug 4080.15 seconds Sending RADIUS PAP challenge to omar at 172.18.124.108
Debug 4087.52 seconds Received RADIUS PAP response from omar at 172.18.124.108, contacting
server
Notice 4088.8 seconds VPN 0:3 opened for omar from 172.18.124.108.
Debug 4088.8 seconds Client's local broadcast address = 172.18.124.255
Notice 4088.8 seconds User assigned IP address 10.1.1.1
Info 4094.49 seconds Command loop started from 10.1.1.1 on PTY2
  
```

[문제 해결](#)

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

[관련 정보](#)

- [Cisco VPN 5000 Series Concentrator 판매 중단 발표](#)
- [Cisco VPN 5000 Concentrator 지원 페이지](#)

- [Cisco VPN 5000 클라이언트 지원 페이지](#)
- [IPSec 지원 페이지](#)
- [Technical Support - Cisco Systems](#)