Microsoft IAS(Internet Authentication Service)를 사용하는 Unified Wireless Networks에서 PEAP

목차

소개

이 문서에서는 Microsoft IAS(Internet Authentication Service)를 RADIUS 서버로 사용하는 Cisco Unified Wireless 네트워크에서 Microsoft MS-CHAP(Challenge Handshake Authentication Protocol) 버전 2 인증을 사용하는 PEAP(Protected Extensible Authentication Protocol)를 설정하는 구성 예를 제공합니다.

사전 요구 사항

요구 사항

이 문서에서는 테스트를 쉽게 수행할 수 있도록 특정 컨피그레이션만 다루므로 독자가 기본 Windows 2003 설치 및 Cisco 컨트롤러 설치에 대해 알고 있다는 가정 하에 작성되었습니다.

참고: 이 문서는 PEAP - MS CHAP 인증을 위해 MS 서버에 필요한 컨피그레이션의 예를 독자에게 제공하기 위한 것입니다. 이 섹션에 제시된 Microsoft 서버 컨피그레이션은 Lab에서 테스트되었으며 예상대로 작동하는 것으로 확인되었습니다. Microsoft 서버를 구성하는 데 문제가 있으면 Microsoft에 도움을 요청하십시오. Cisco TAC에서는 Microsoft Windows 서버 컨피그레이션을 지원하지 않습니다.

Cisco 4400 Series Controller의 초기 설치 및 컨피그레이션 정보는 Quick Start Guide: Cisco 4400 Series Wireless LAN Controller를 참조하십시오.

Microsoft Windows 2003 설치 및 구성 가이드는 Windows Server 2003 R2 설치에서 찾을 수 있습니다.

시작하기 전에 테스트 랩의 각 서버에 Microsoft Windows Server 2003 SP1 운영 체제를 설치하고 모든 서비스 팩을 업데이트하십시오. 컨트롤러 및 LAP(Lightweight Access Point)를 설치하고 최신 소프트웨어 업데이트가 구성되었는지 확인합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 펌웨어 버전 4.0을 실행하는 Cisco 4400 Series 컨트롤러
- Cisco 1131 LWAPP(Lightweight Access Point Protocol) AP
- IAS(Internet Authentication Service), CA(Certificate Authority), DHCP 및 DNS(Domain Name System) 서비스가 설치된 Windows 2003 Enterprise Server(SP1)
- Windows XP Professional SP 2(및 업데이트된 서비스 팩) 및 Cisco Aironet 802.11a/b/g Wireless NIC(Network Interface Card)
- Aironet Desktop Utility 버전 4.0
- Cisco 3560 스위치

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.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

PEAP 개요

PEAP는 TLS(Transport Level Security)를 사용하여 무선 노트북 컴퓨터와 같은 인증 PEAP 클라이언트와 Microsoft IAS(Internet Authentication Service) 또는 RADIUS 서버와 같은 PEAP 인증자 간에 암호화된 채널을 생성합니다. PEAP는 인증 방법을 지정하지 않지만 PEAP에서 제공하는 TLS 암호화 채널을 통해 작동할 수 있는 EAP-MSCHAPv2와 같은 다른 EAP 인증 프로토콜에 대한 추가 보안을 제공합니다. PEAP 인증 프로세스는 두 가지 기본 단계로 구성됩니다.

PEAP 1단계: TLS 암호화 채널

무선 클라이언트는 AP와 연결됩니다. IEEE 802.11 기반 연결은 클라이언트와 LAP(Access Point)

간에 보안 연결이 생성되기 전에 개방형 시스템 또는 공유 키 인증을 제공합니다. 클라이언트와 액세스 포인트 간에 IEEE 802.11 기반 연결이 성공적으로 설정되면 TLS 세션이 AP와 협상됩니다. 무선 클라이언트와 IAS 서버 간에 인증이 성공적으로 완료되면 TLS 세션이 협상됩니다. 이 협상 내에서 파생된 키는 모든 후속 통신을 암호화하는 데 사용됩니다.

PEAP 2단계: EAP 인증 통신

EAP 협상을 포함하는 EAP 통신은 PEAP 인증 프로세스의 첫 번째 단계 내에서 PEAP에 의해 생성된 TLS 채널 내에서 발생합니다. IAS 서버는 EAP-MS-CHAP v2를 사용하여 무선 클라이언트를 인증합니다. LAP 및 컨트롤러는 무선 클라이언트와 RADIUS 서버 간의 메시지만 전달합니다. WLC와 LAP는 TLS 엔드포인트가 아니므로 이 메시지를 해독할 수 없습니다.

PEAP 단계 1이 발생하고 IAS 서버와 802.1X 무선 클라이언트 간에 TLS 채널이 생성된 후, 사용자가 PEAP-MS-CHAP v2와 함께 유효한 비밀번호 기반 자격 증명을 제공한 성공적인 인증 시도를 위해 RADIUS 메시지 시퀀스는 다음과 같습니다.

1. IAS 서버는 클라이언트에 ID 요청 메시지(EAP-Request/Identity)를 전송합니다.
2. 클라이언트는 ID 응답 메시지, 즉 EAP-Response/Identity로 응답합니다.
3. IAS 서버는 MS-CHAP v2 챌린지 메시지를 보냅니다. EAP-Request/EAP-Type=EAP MS-CHAP-V2(Challenge).
4. 클라이언트는 MS-CHAP v2 챌린지 및 응답으로 응답합니다. EAP-Response/EAP-Type=EAP-MS-CHAP-V2(응답).
5. 서버가 성공적으로 클라이언트를 인증한 경우 IAS 서버는 MS-CHAP v2 성공 패킷을 다시 보냅니다. EAP-Request/EAP-Type=EAP-MS-CHAP-V2(Success).
6. 클라이언트가 서버를 성공적으로 인증한 경우 클라이언트는 MS-CHAP v2 성공 패킷으로 응답합니다. EAP-Response/EAP-Type=EAP-MS-CHAP-V2(Success)
7. IAS 서버는 성공적인 인증을 나타내는 EAP-TLV를 전송합니다.
8. 클라이언트는 EAP-TLV 상태 성공 메시지로 응답합니다.
9. 서버에서 인증을 완료하고 일반 텍스트를 사용하여 EAP-Success 메시지를 보냅니다. 클라이언트 격리를 위해 VLAN이 구축된 경우 VLAN 특성이 이 메시지에 포함됩니다.

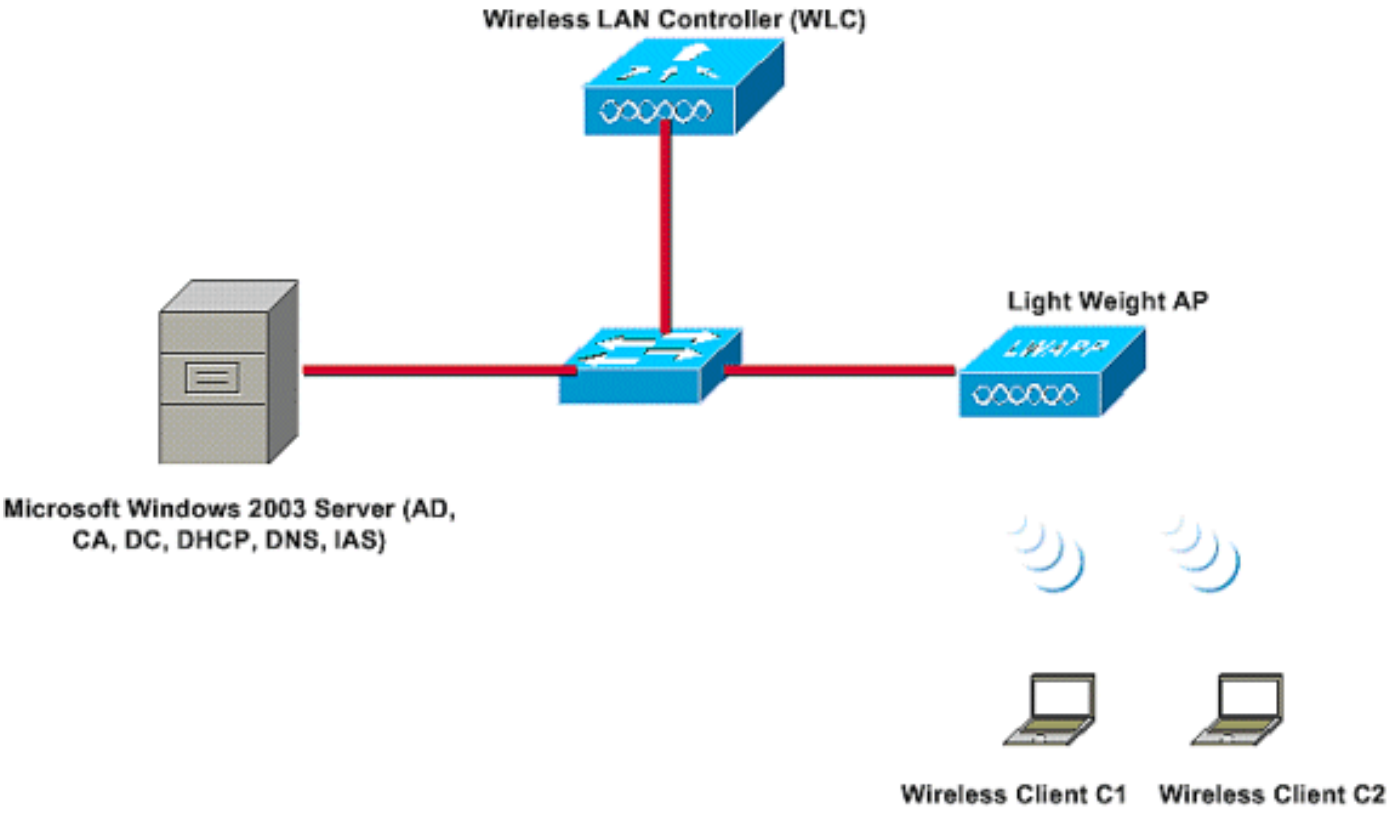
구성

이 문서에서는 PEAP MS-CHAP v2의 컨피그레이션에 대한 예를 제공합니다.

참고: 이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 명령 조회 도구(등록된 고객만 해당)를 사용하십시오.

네트워크 다이어그램

이 문서에서는 이 네트워크 설정을 사용합니다.



이 설치 프로그램에서 Microsoft Windows 2003 서버는 다음 역할을 수행합니다.

- Wireless.com 도메인의 도메인 **컨트롤러**
- DHCP/DNS 서버
- CA(Certificate Authority) 서버
- Active Directory - 사용자 데이터베이스를 유지 관리합니다.
- IAS(Internet Authentication Service) - 무선 사용자 인증

이 서버는 그림과 같이 레이어 2 스위치를 통해 유선 네트워크에 연결됩니다.

WLC(Wireless LAN Controller) 및 등록된 LAP도 레이어 2 스위치를 통해 네트워크에 연결됩니다.

무선 클라이언트 C1 및 C2는 WPA2(Wi-Fi Protected Access 2) - PEAP MSCHAP v2 인증을 사용하여 무선 네트워크에 연결합니다.

PEAP MSCHAP v2 인증을 사용하여 무선 클라이언트를 인증하도록 Microsoft 2003 서버, 무선 LAN 컨트롤러 및 경량 AP를 구성하는 것이 목적입니다.

다음 섹션에서는 이 설정을 위해 디바이스를 구성하는 방법에 대해 설명합니다.

설정

이 섹션에서는 이 WLAN에서 PEAP MS-CHAP v2 인증을 설정하는 데 필요한 컨피그레이션을 살펴봅니다.

- Microsoft Windows 2003 Server 구성
- WLC(Wireless LAN Controller) 및 경량 AP 구성
- 무선 클라이언트 구성

Microsoft Windows 2003 서버의 구성부터 시작합니다.

Microsoft Windows 2003 Server 구성

Microsoft Windows 2003 Server 구성

네트워크 설정 섹션에서 설명한 것처럼 네트워크에서 Microsoft Windows 2003 서버를 사용하여 이러한 기능을 수행합니다.

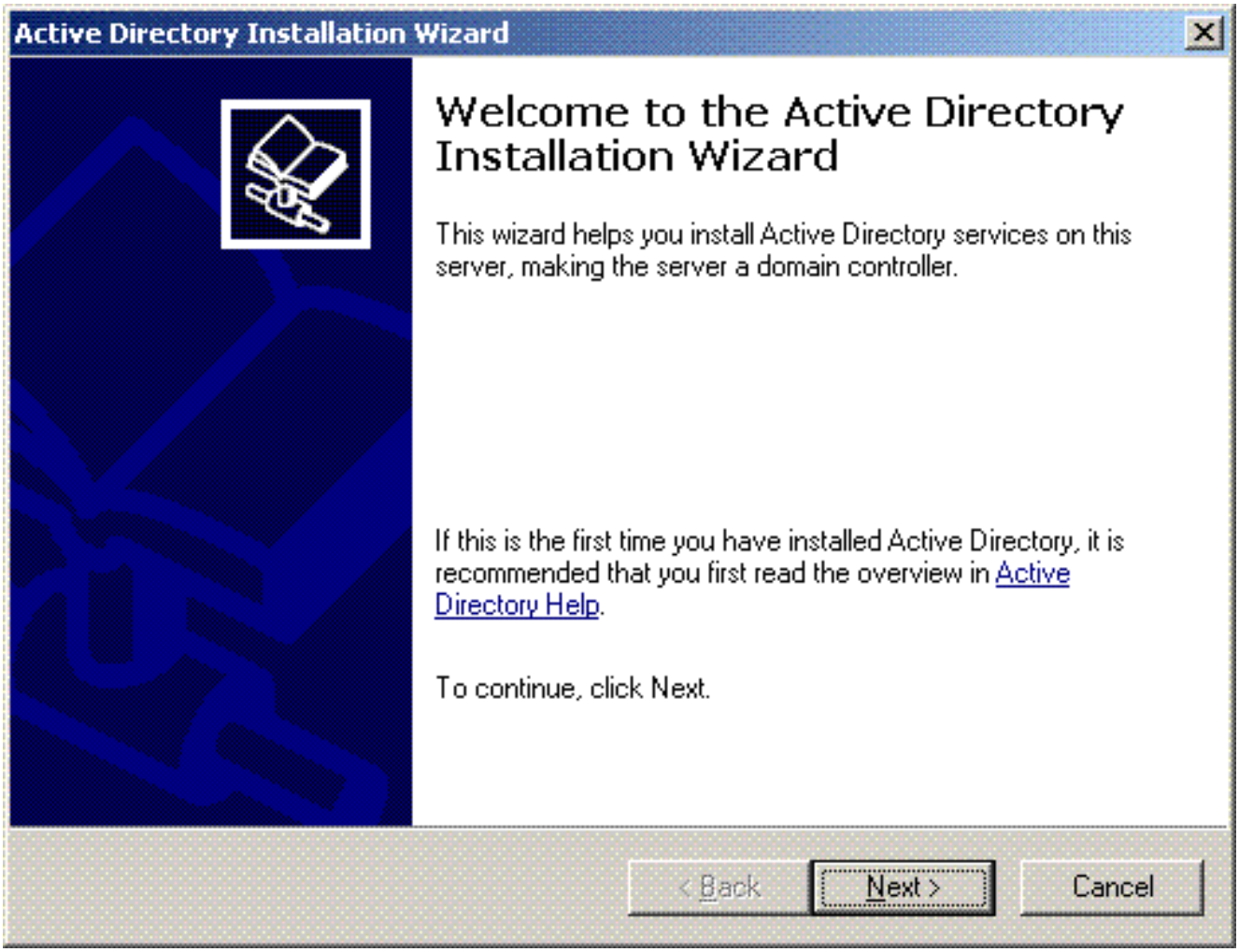
- **도메인 컨트롤러** - 도메인 무선용.
- **DHCP/DNS 서버**
- **CA(Certificate Authority) 서버**
- **IAS(Internet Authentication Service)** - 무선 사용자 인증
- **Active Directory** - 사용자 데이터베이스를 유지 관리합니다.

이러한 서비스에 대해 Microsoft Windows 2003 서버를 구성합니다. Microsoft Windows 2003 서버를 도메인 컨트롤러로 구성하는 것부터 시작합니다.

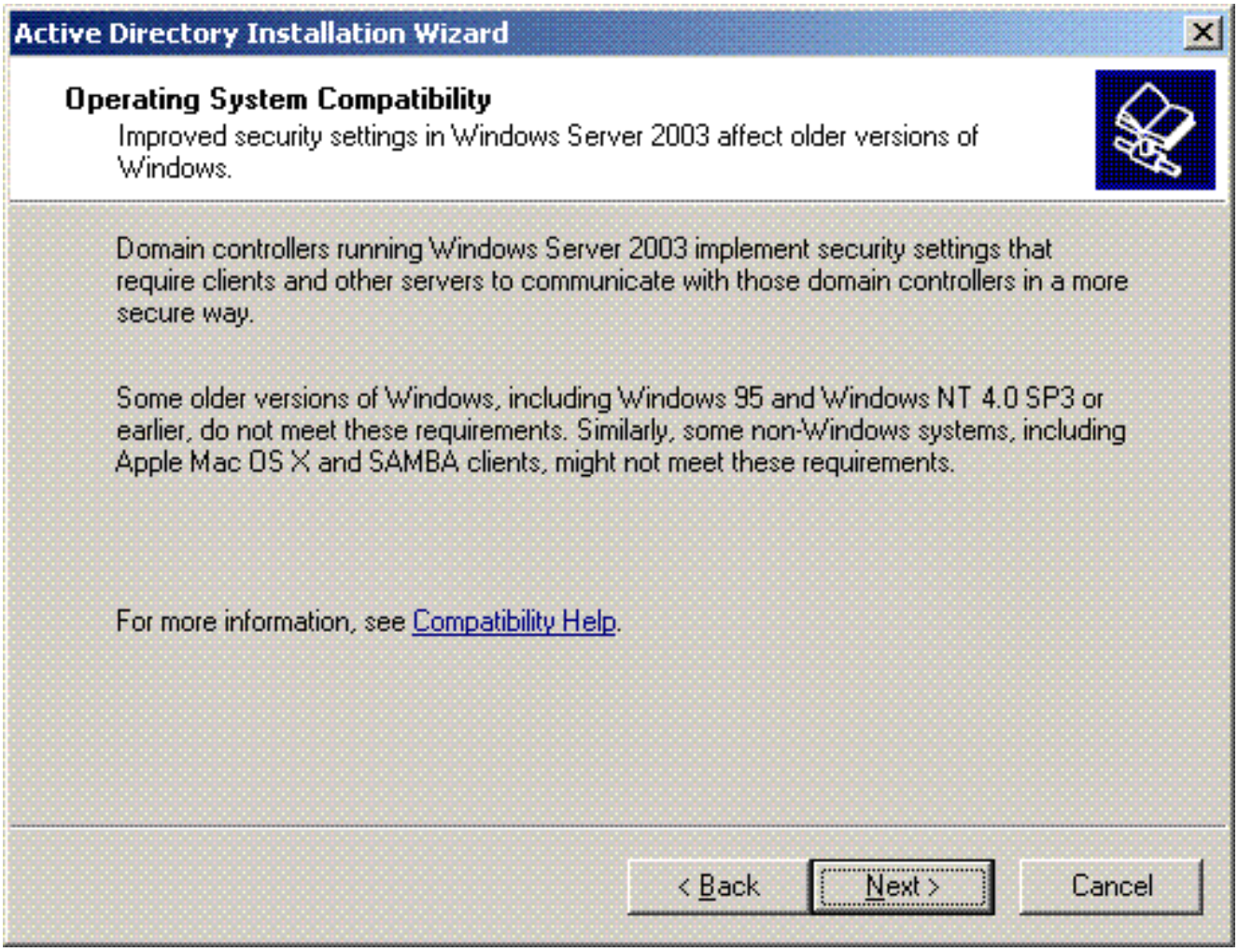
Microsoft Windows 2003 서버를 도메인 컨트롤러로 구성

Microsoft Windows 2003 서버를 도메인 컨트롤러로 구성하려면 다음 단계를 완료하십시오.

1. Start(**시작**)를 클릭하고 **Run(실행)**을 클릭한 **다음 dcpromo.exe**를 입력한 다음 **OK(확인)를** 클릭하여 Active Directory 설치 마법사를 시작합니다

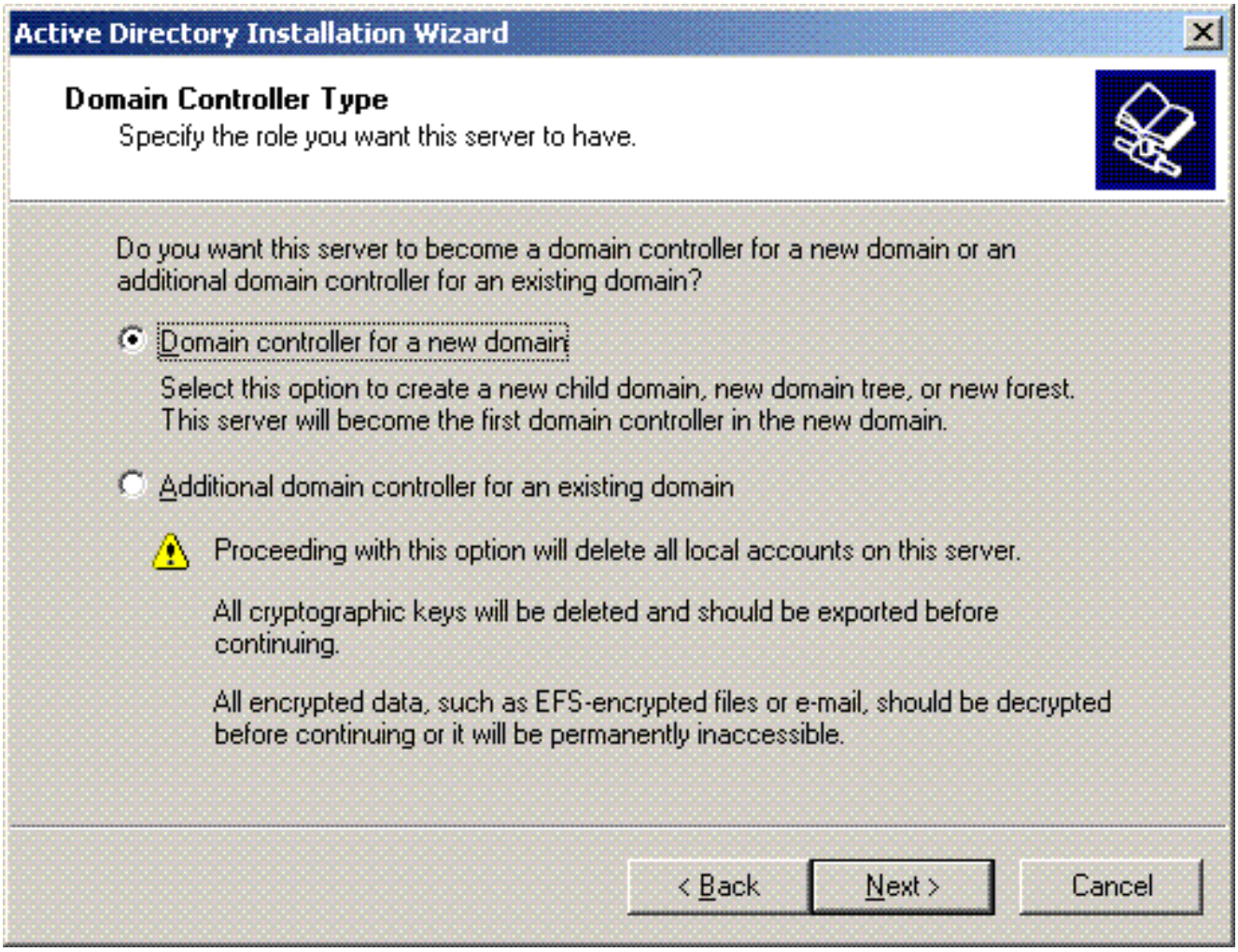


2. Next(**다음**)를 클릭하여 Active Directory 설치 마법사를 실행합니다



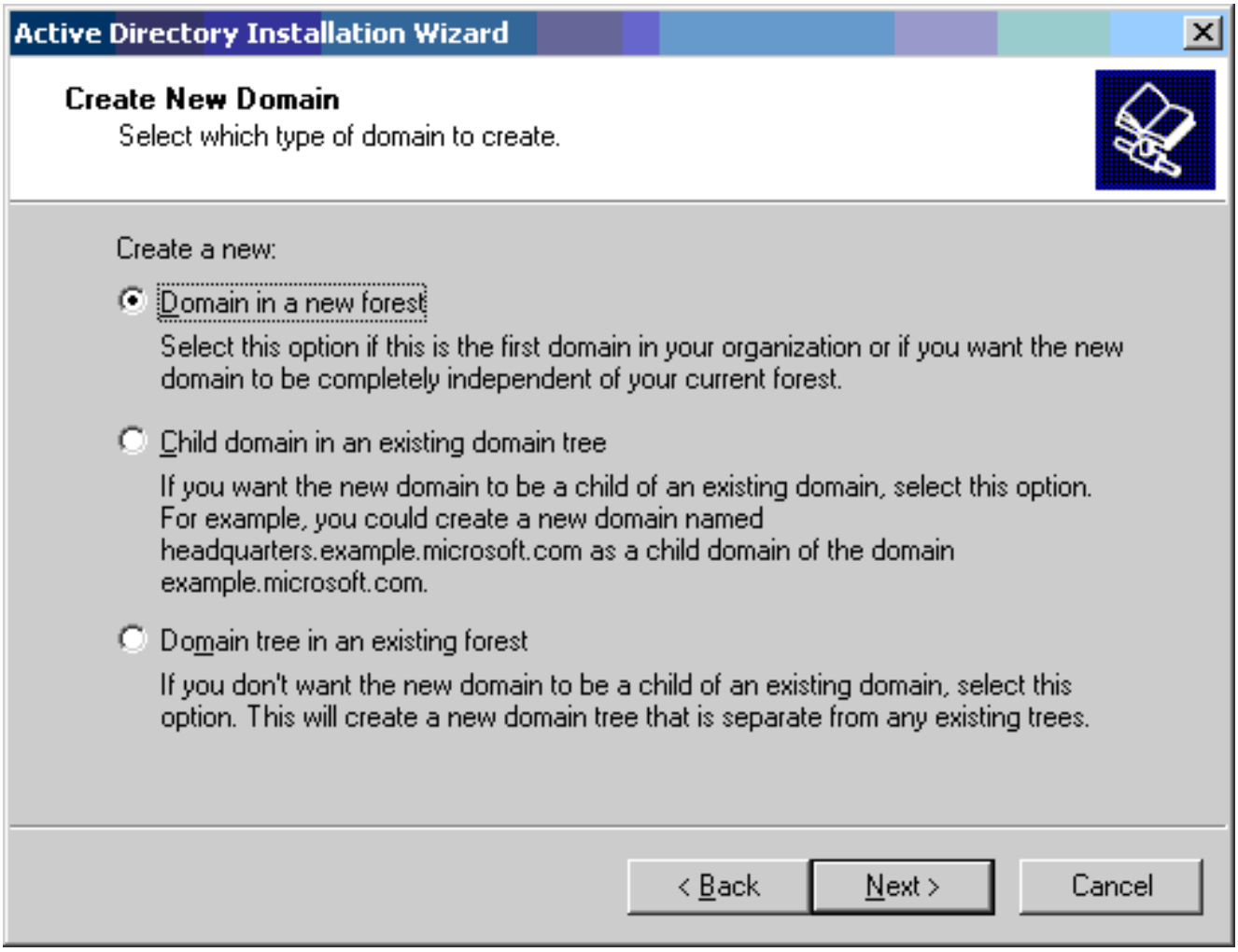
3. 새 도메인을 생성하려면 새 도메인에 대한 **Domain Controller(도메인 컨트롤러)** 옵션을 선택합니다

.



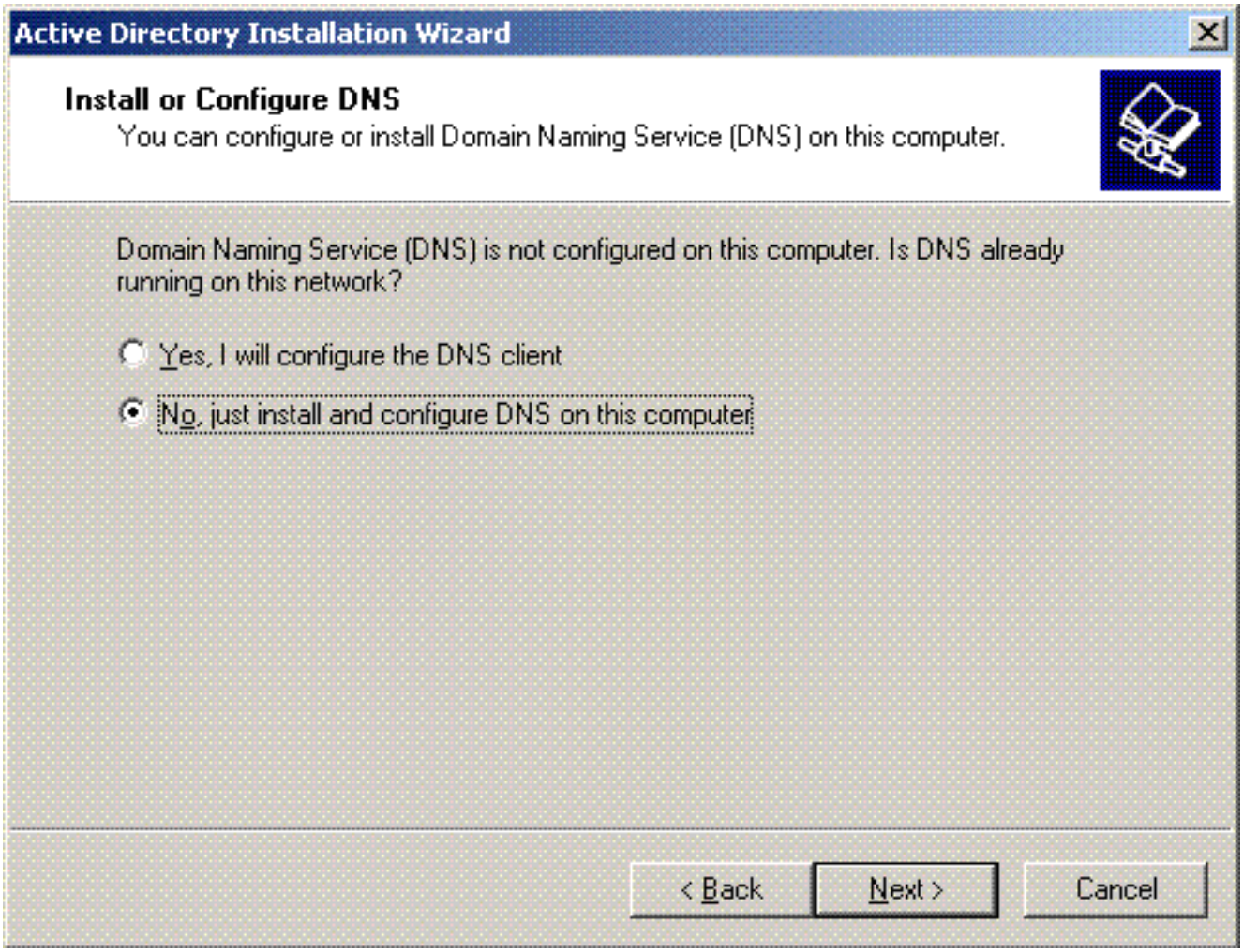
4. Next(**다음**)를 클릭하여 도메인 트리의 새 포리스트를 만듭니다

.



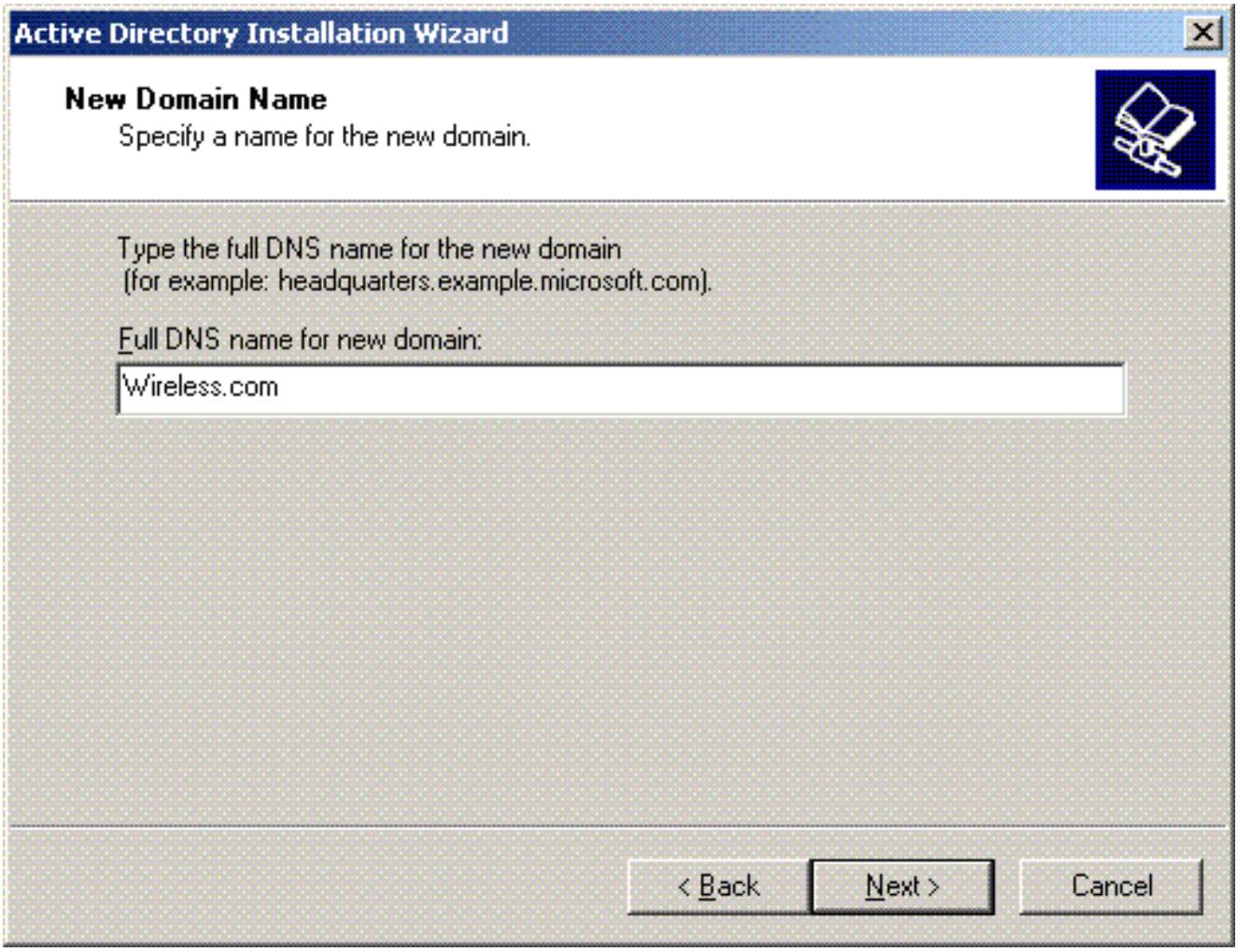
5. 시스템에 DNS가 설치되어 있지 않으면 마법사에서 DNS를 구성할 수 있는 옵션을 제공합니다. No(**아니요), Just Install and Configure DNS on this computer(이 컴퓨터**에 **DNS 설치 및** 구성만)를 선택합니다. **Next(다음)**를 클릭합니다

.



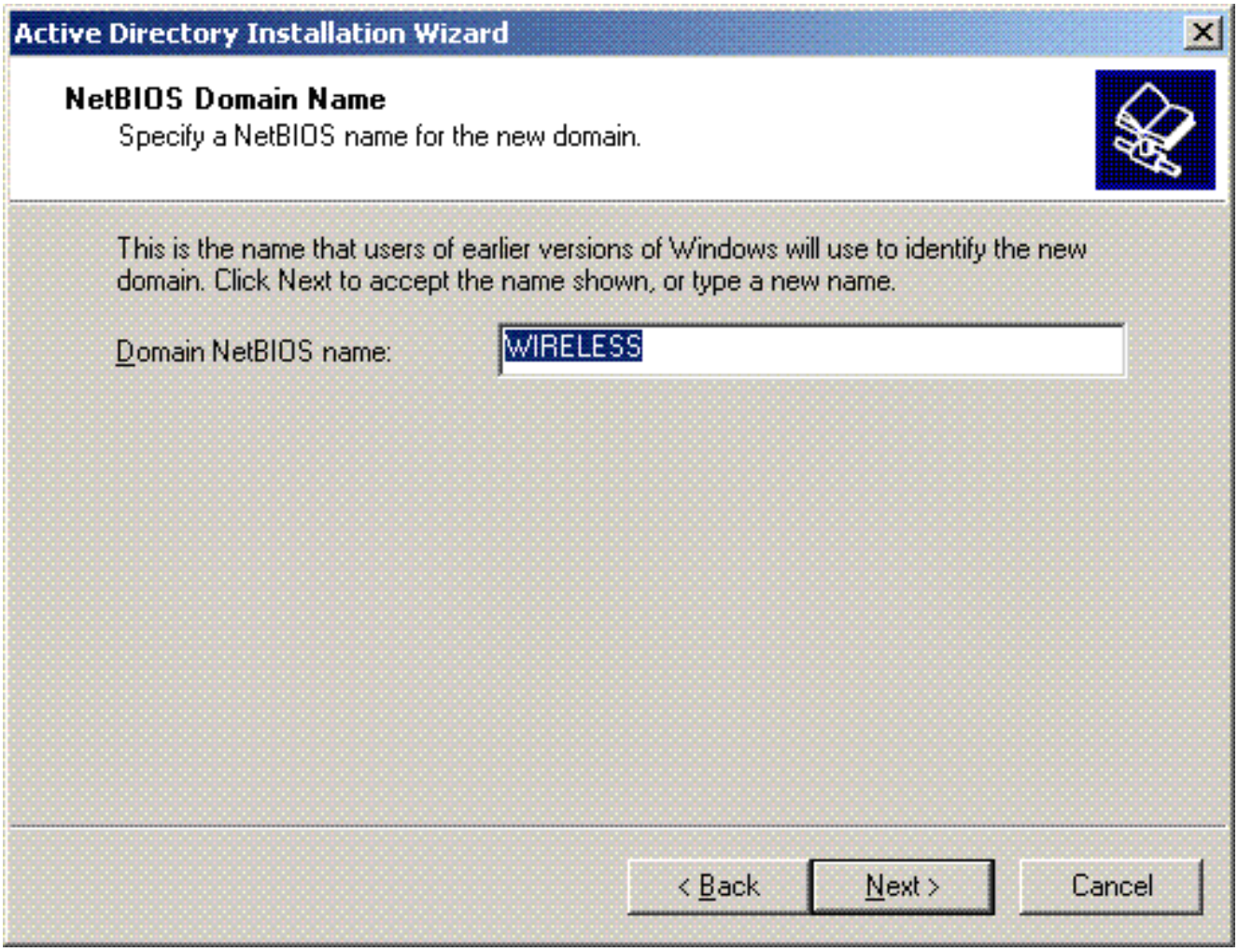
6. 새 도메인의 전체 DNS 이름을 입력합니다. 이 예에서는 **Wireless.com**이 사용되고 Next(**다음**)를 클릭합니다

.

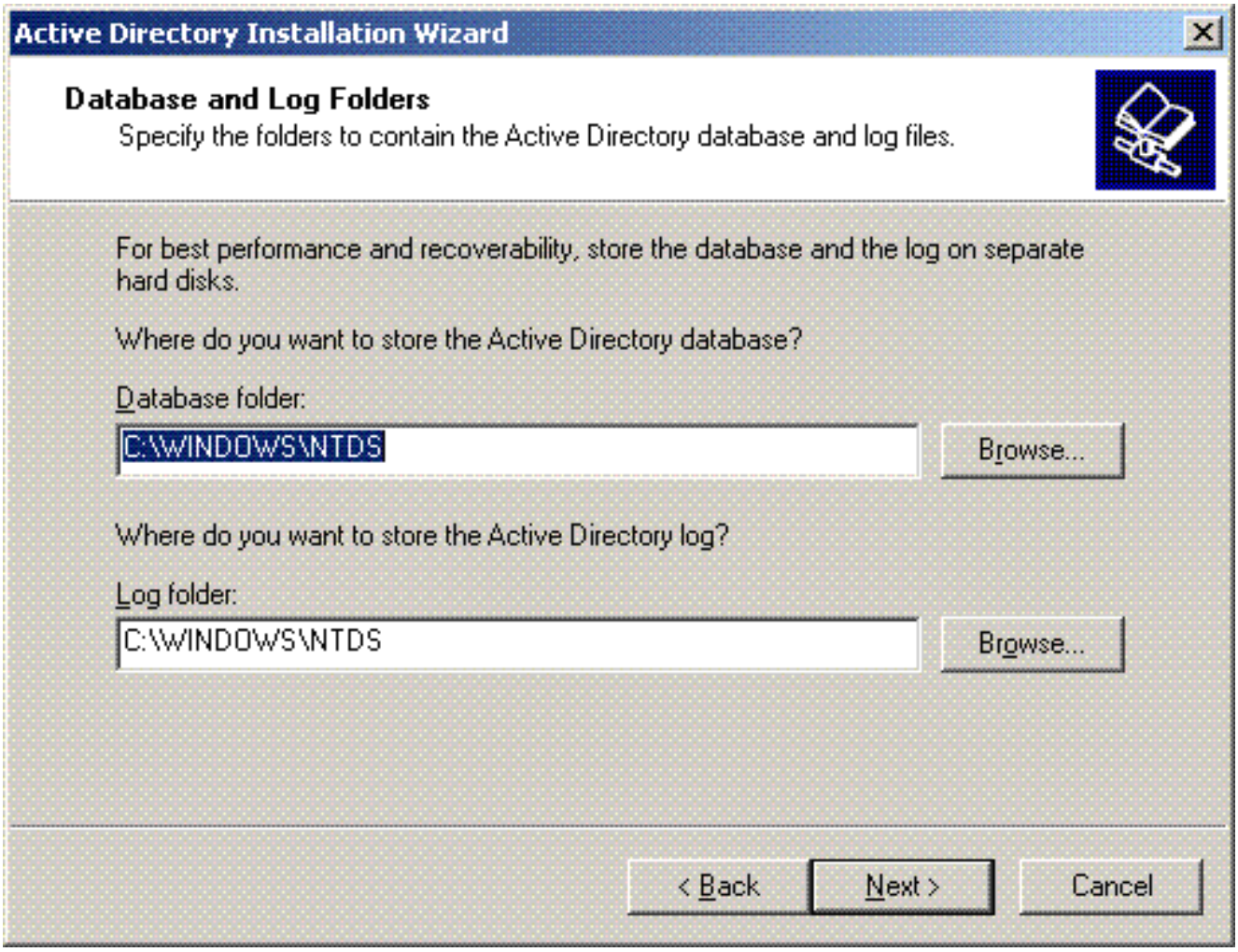


7. 도메인의 NETBIOS 이름을 입력하고 Next(**다음**)를 클릭합니다. 이 예에서는 WIRELESS를 **사용합니다**

.

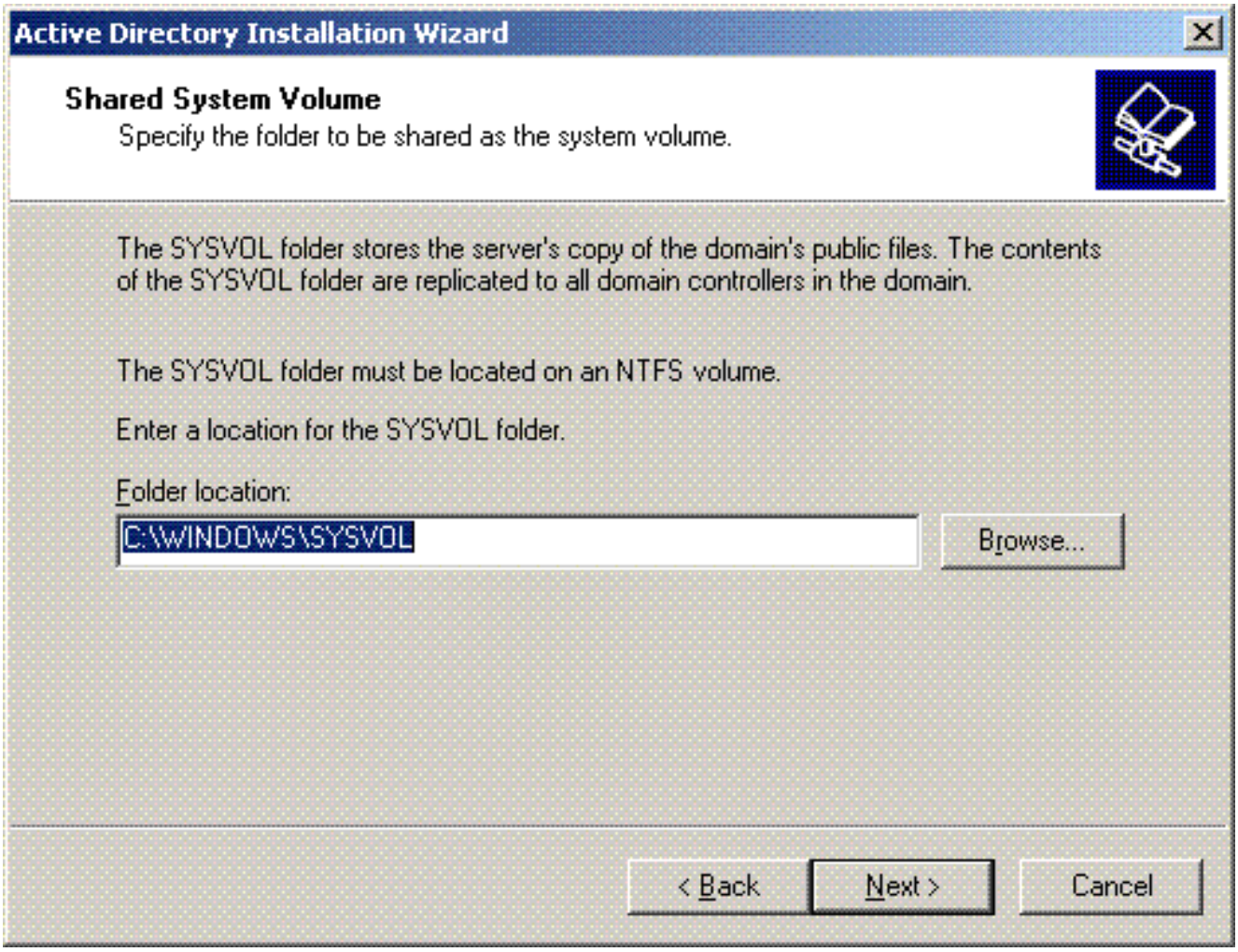


8. 도메인의 데이터베이스 및 로그 위치를 선택합니다. **Next(다음)**를 클릭합니다
.



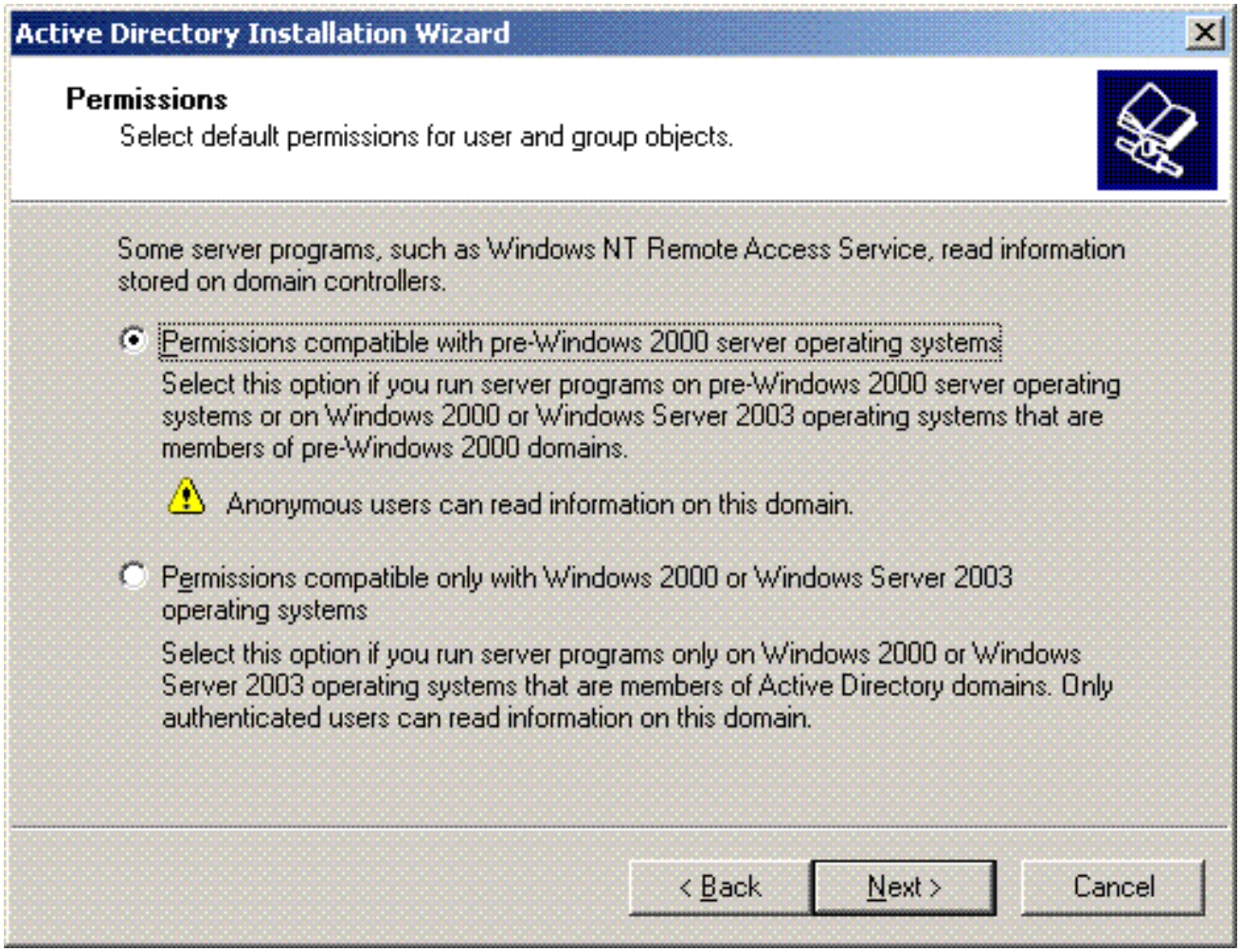
9. Sysvol 폴더의 위치를 선택합니다. **Next(다음)**를 클릭합니다

.



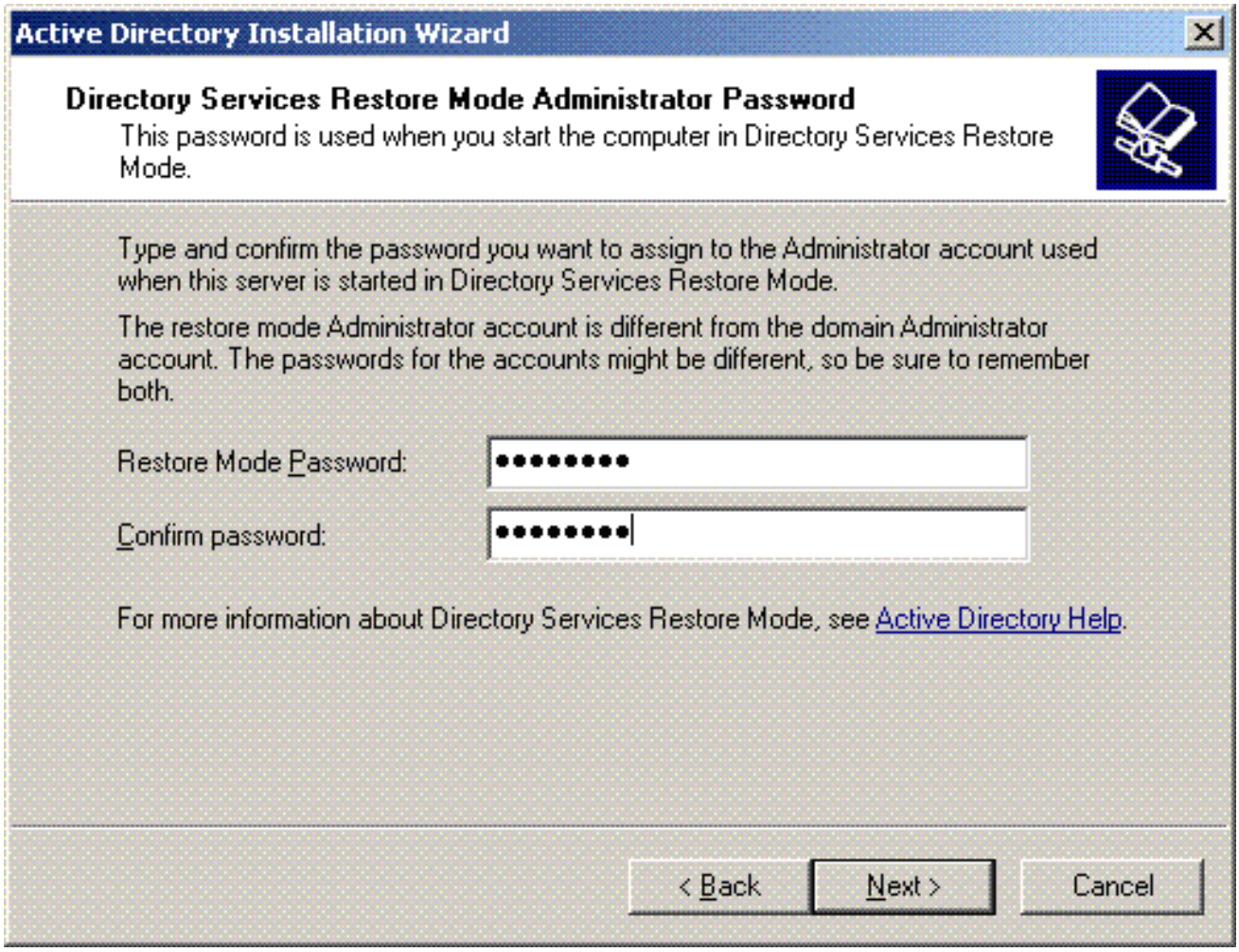
10. 사용자 및 그룹에 대한 기본 권한을 선택합니다. **Next(다음)**를 클릭합니다

.

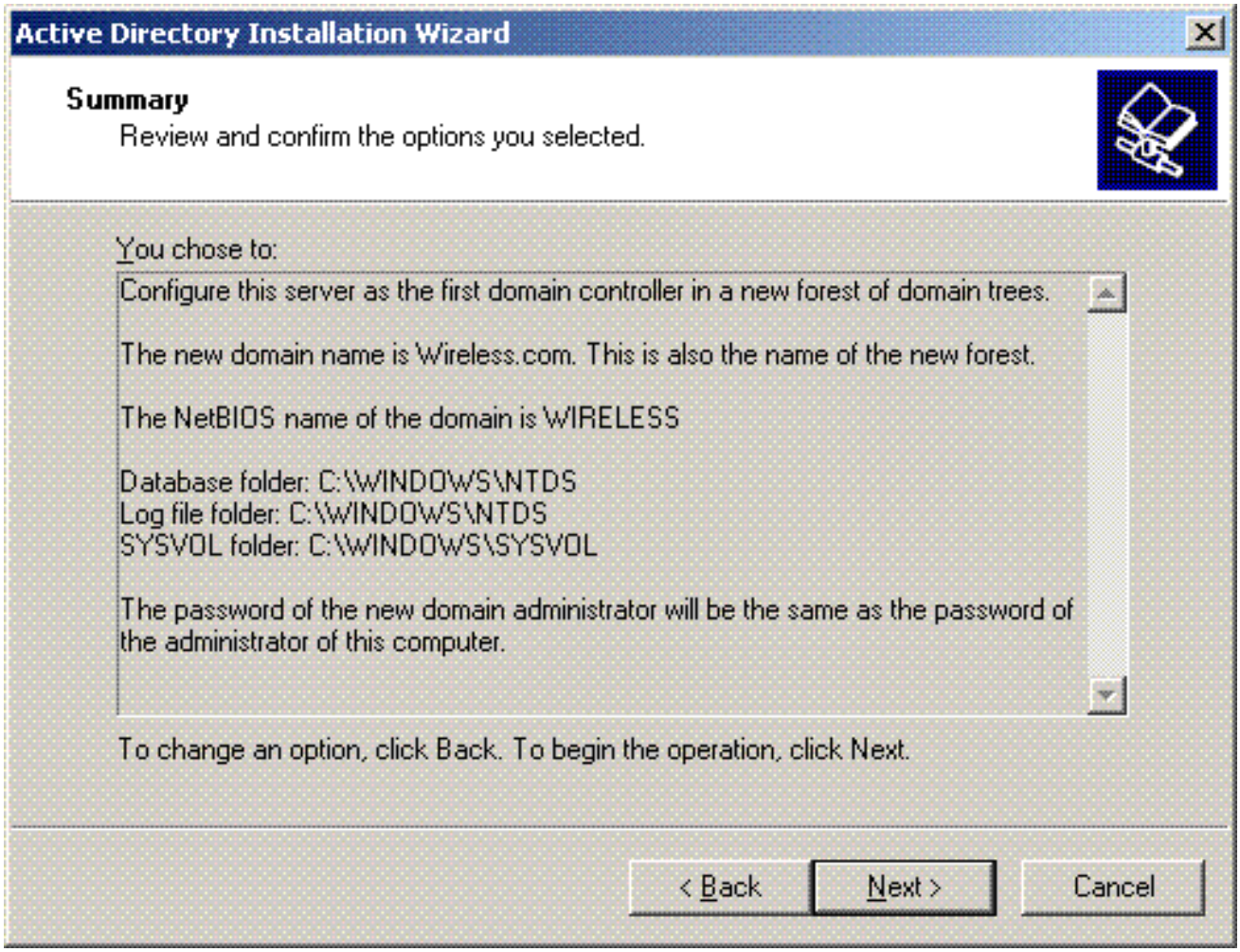


11. 관리자 암호를 설정하고 다음을 **클릭합니다**

.

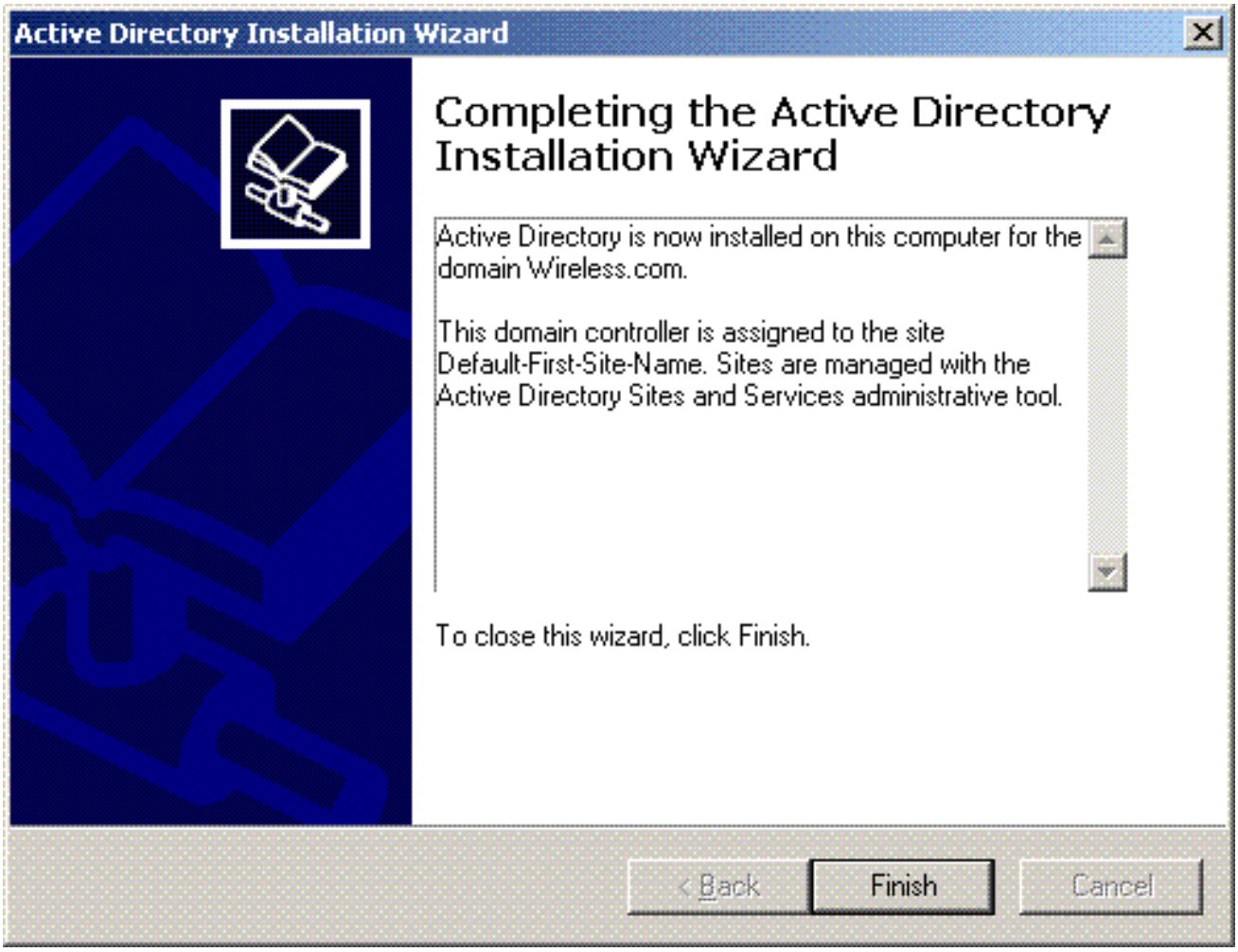


12. Next(**다음**)를 클릭하여 이전에 설정한 Domain Options(도메인 옵션)를 수락합니다
.

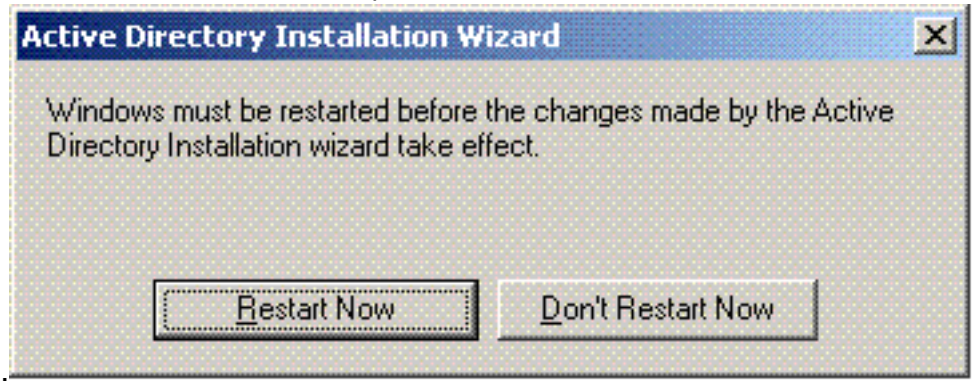


13. Finish(**마침**)를 클릭하여 Active Directory 설치 마법사를 닫습니다

.



14. 변경 사항을 적용하려면 서버를 다시 시작하십시오

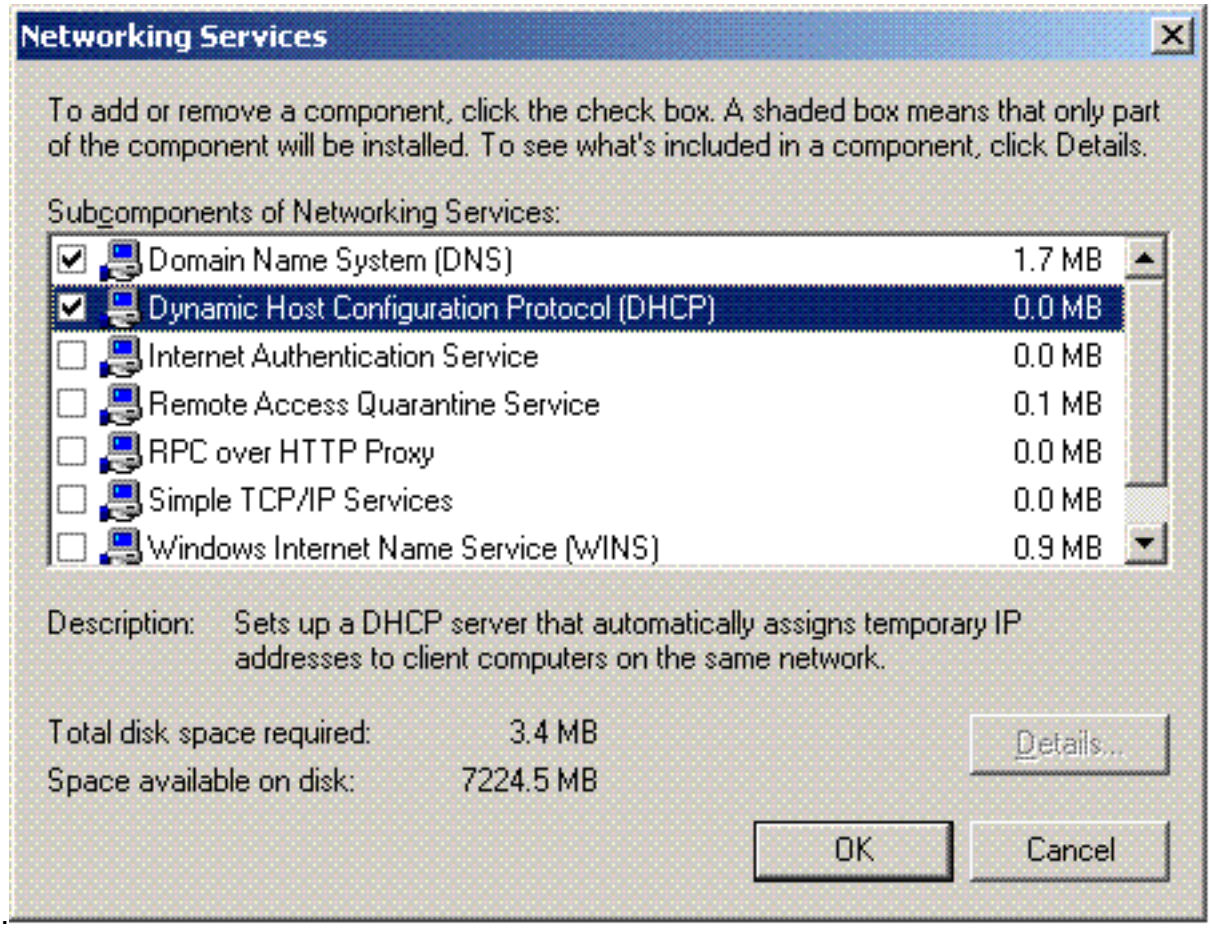


이 단계에서는 Microsoft Windows 2003 서버를 도메인 컨트롤러로 구성하고 새 도메인 **Wireless.com**을 만들었습니다. 그런 다음 서버에서 DHCP 서비스를 구성합니다.

Microsoft Windows 2003 Server에 DHCP 서비스 설치 및 구성

Microsoft 2003 서버의 DHCP 서비스는 무선 클라이언트에 IP 주소를 제공하는 데 사용됩니다. 이 서버에 DHCP 서비스를 설치하고 구성하려면 다음 단계를 완료하십시오.

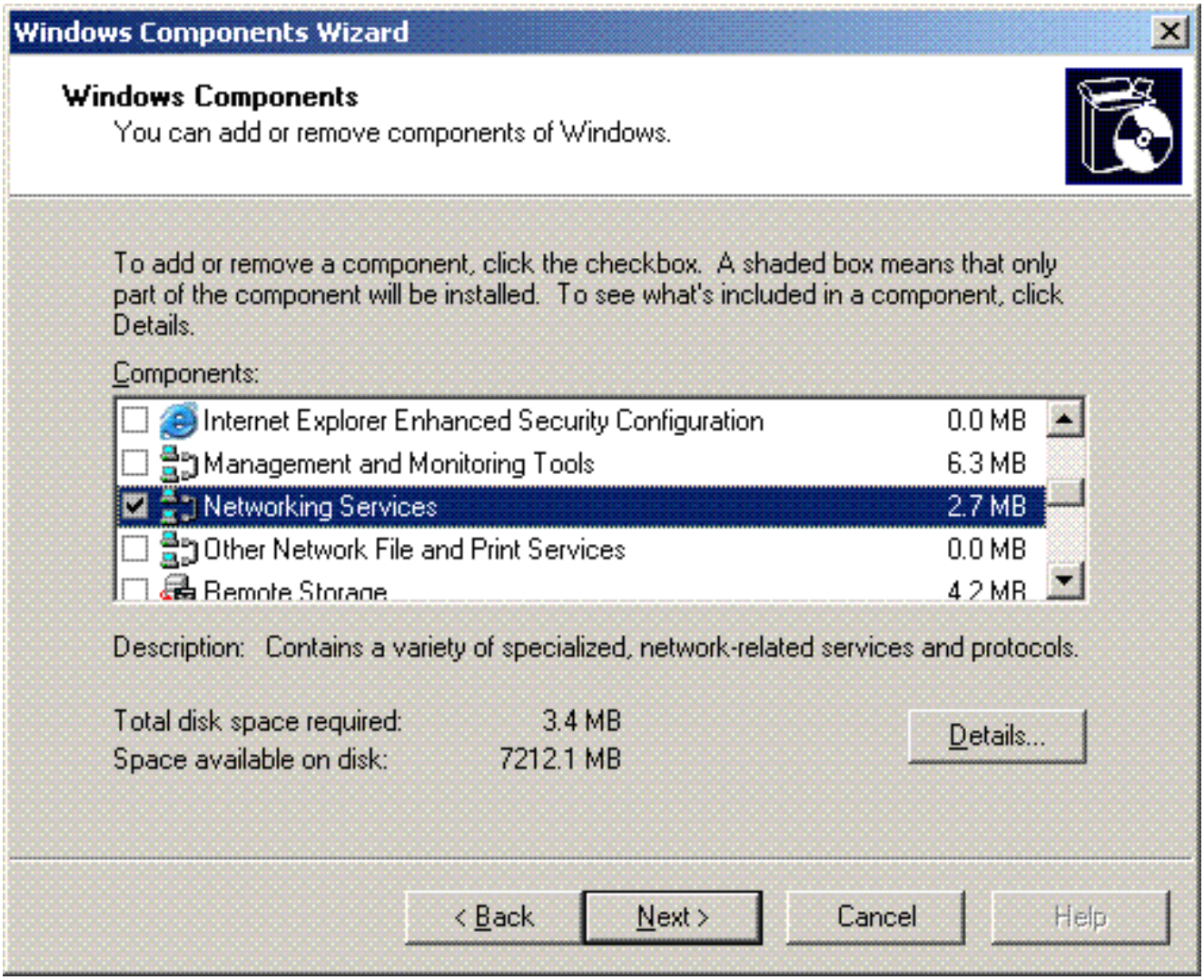
1. 제어판에서 **프로그램 추가/**제거를 클릭합니다.
2. **Windows 구성 요소 추가/제거를** 클릭합니다.
3. Networking **Services(네트워킹 서비스)**를 선택하고 Details(**세부사항)**를 클릭합니다.
4. DHCP**(Dynamic Host Configuration Protocol)를 선택하고 OK(확인)**를 클릭합니다



.

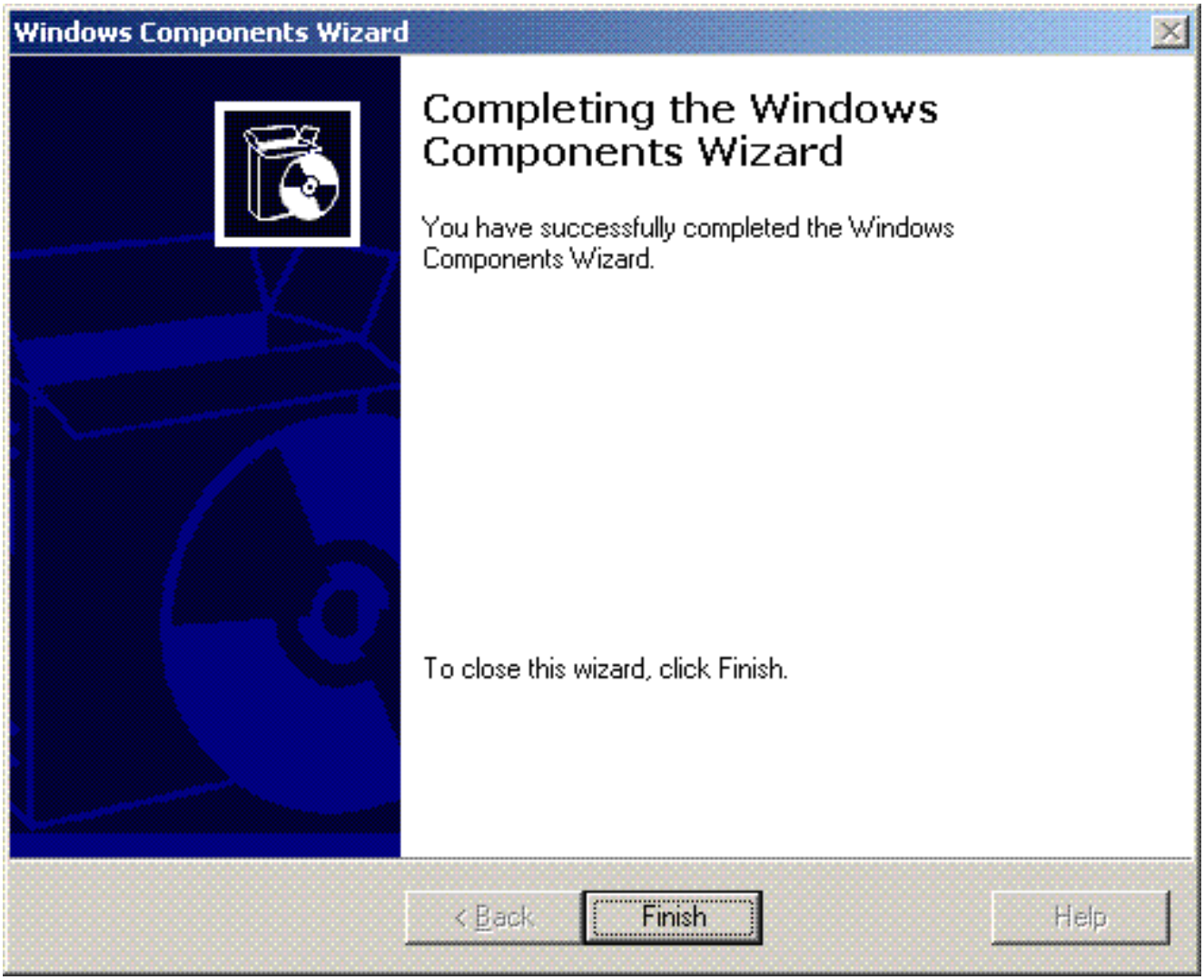
5. DHCP **서비스**를 설치하려면 다음을 클릭합니다

.

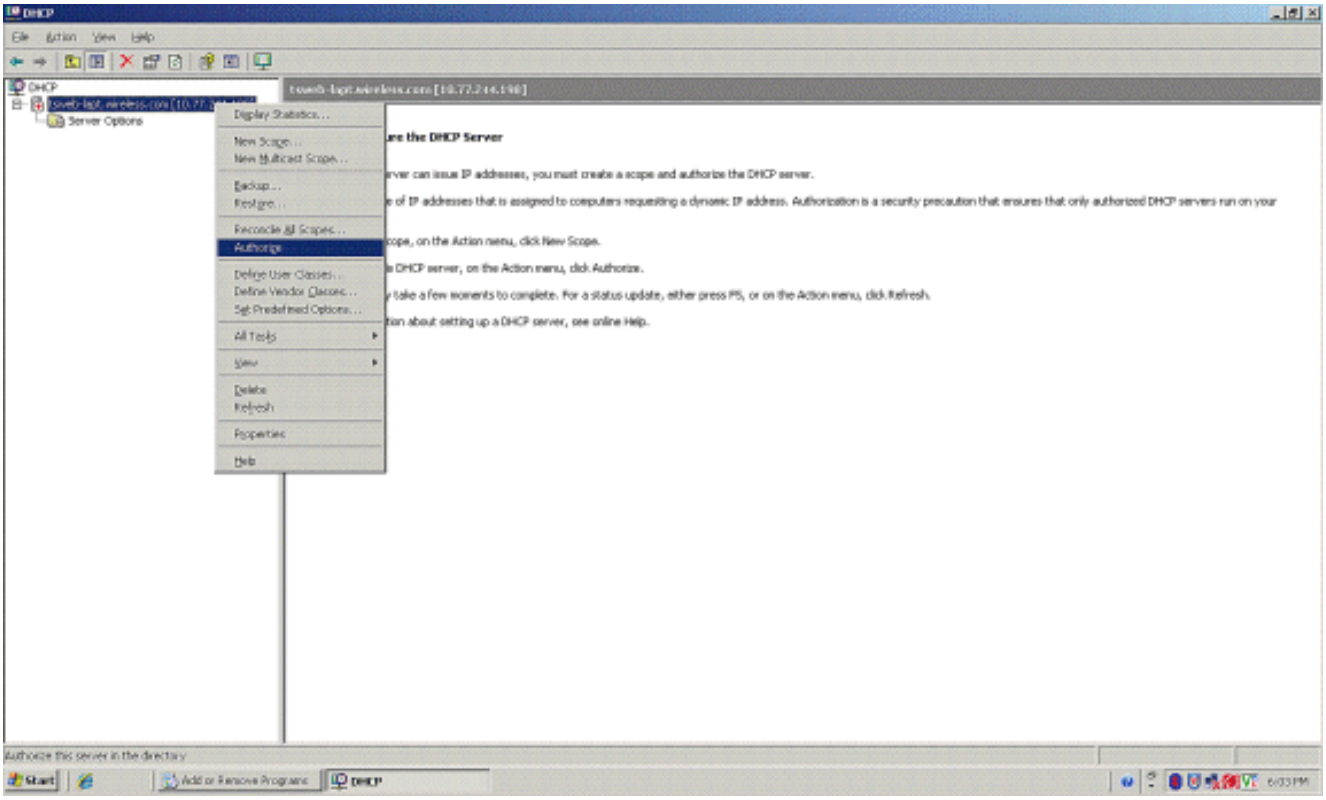


6. Finish(**마침**)를 클릭하여 설치를 완료합니다

.

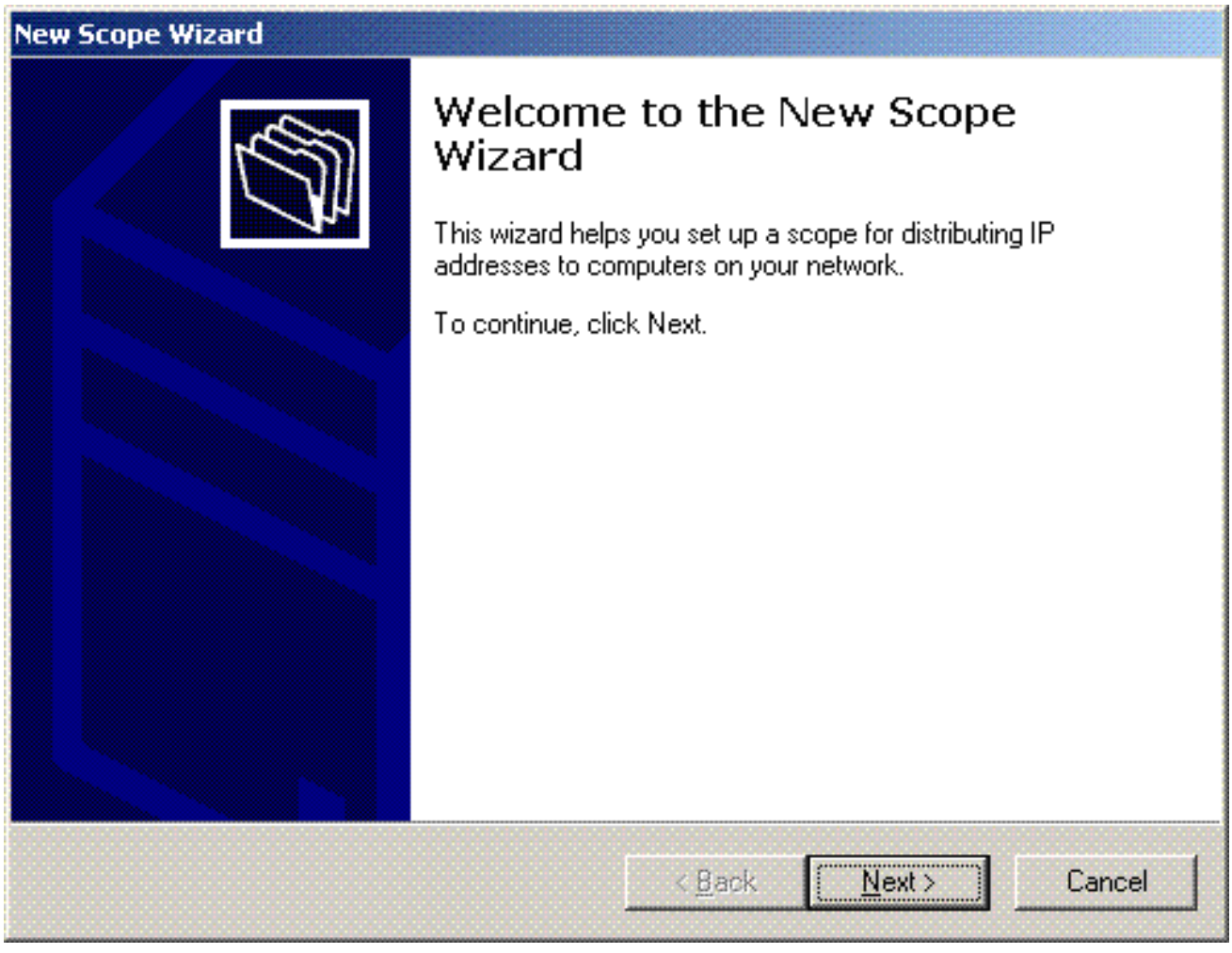


7. DHCP 서비스를 구성하려면 **Start(시작) > Programs(프로그램) > Administrative tools(관리 툴)**를 클릭하고 **DHCP** 스냅인을 클릭합니다.
8. DHCP 서버 - tsweb**-lapt.wireless.com**(이 예에서는)을 선택합니다.
9. Action(**작업)**을 클릭한 다음 Authorize(권한 **부여**)를 클릭하여 DHCP 서비스를 인증합니다
.



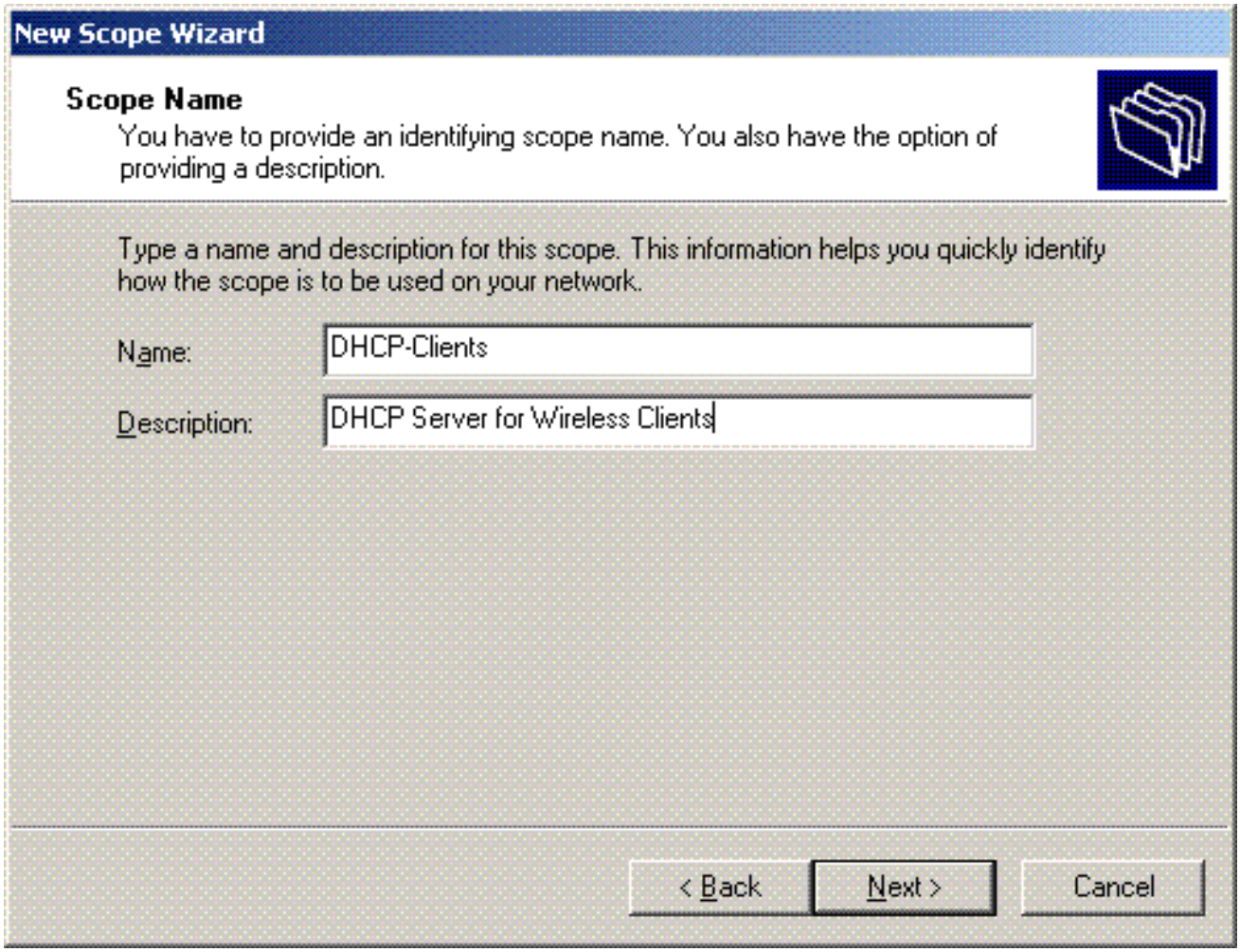
10. 콘솔 트리에서 tsweb-**lapt.wireless.com을 마우스** 오른쪽 단추로 클릭한 다음 **새 범위**를 클릭하여 무선 클라이언트의 IP 주소 범위를 정의합니다.
11. 새 범위 마법사의 새 범위 마법사 시작 페이지에서 다음을 **클릭합니다**

.



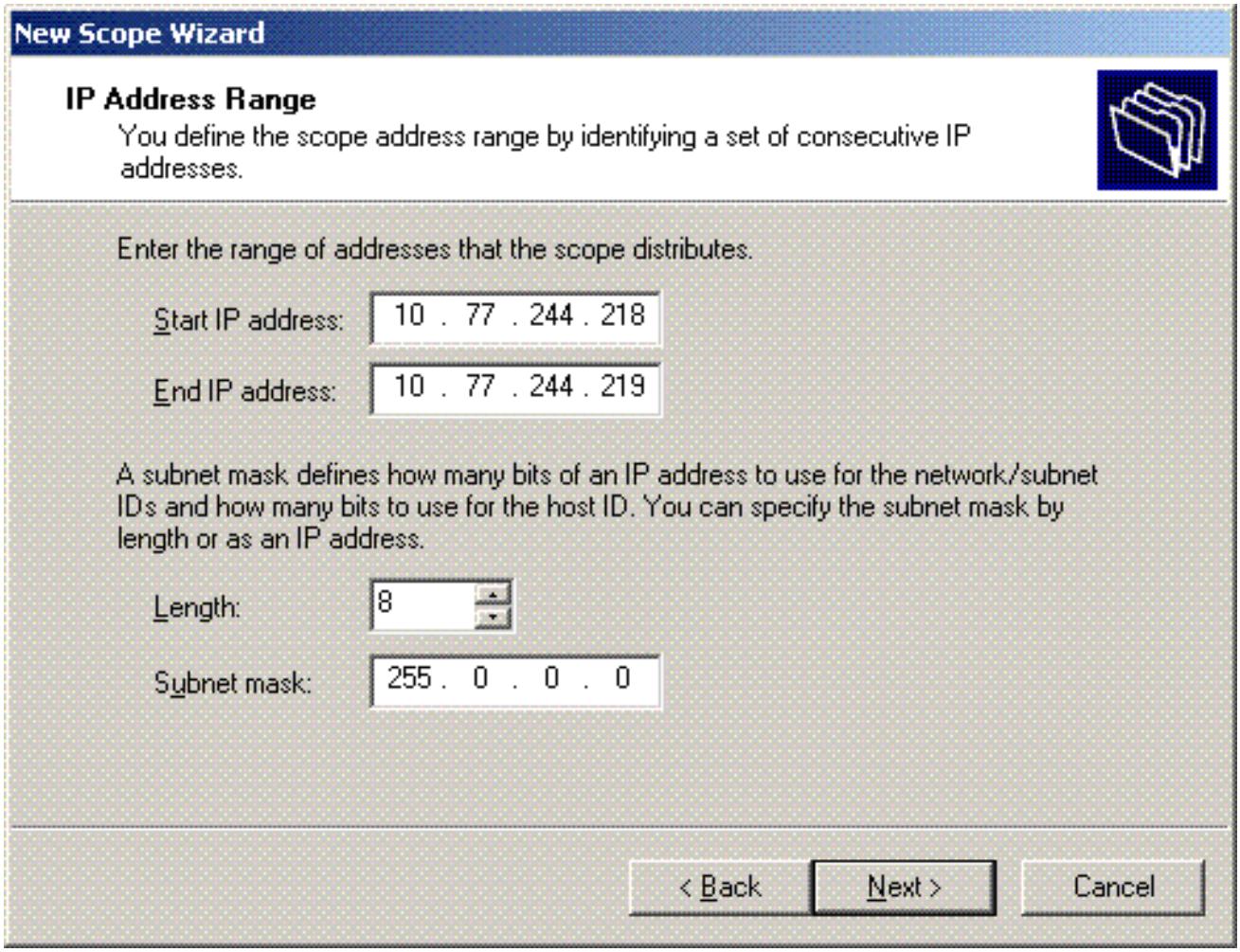
12. Scope Name 페이지에서 DHCP 범위의 이름을 입력합니다. 이 예에서는 DHCP-**Clients**를 범위 이름으로 사용합니다. **Next(다음)**를 클릭합니다

.



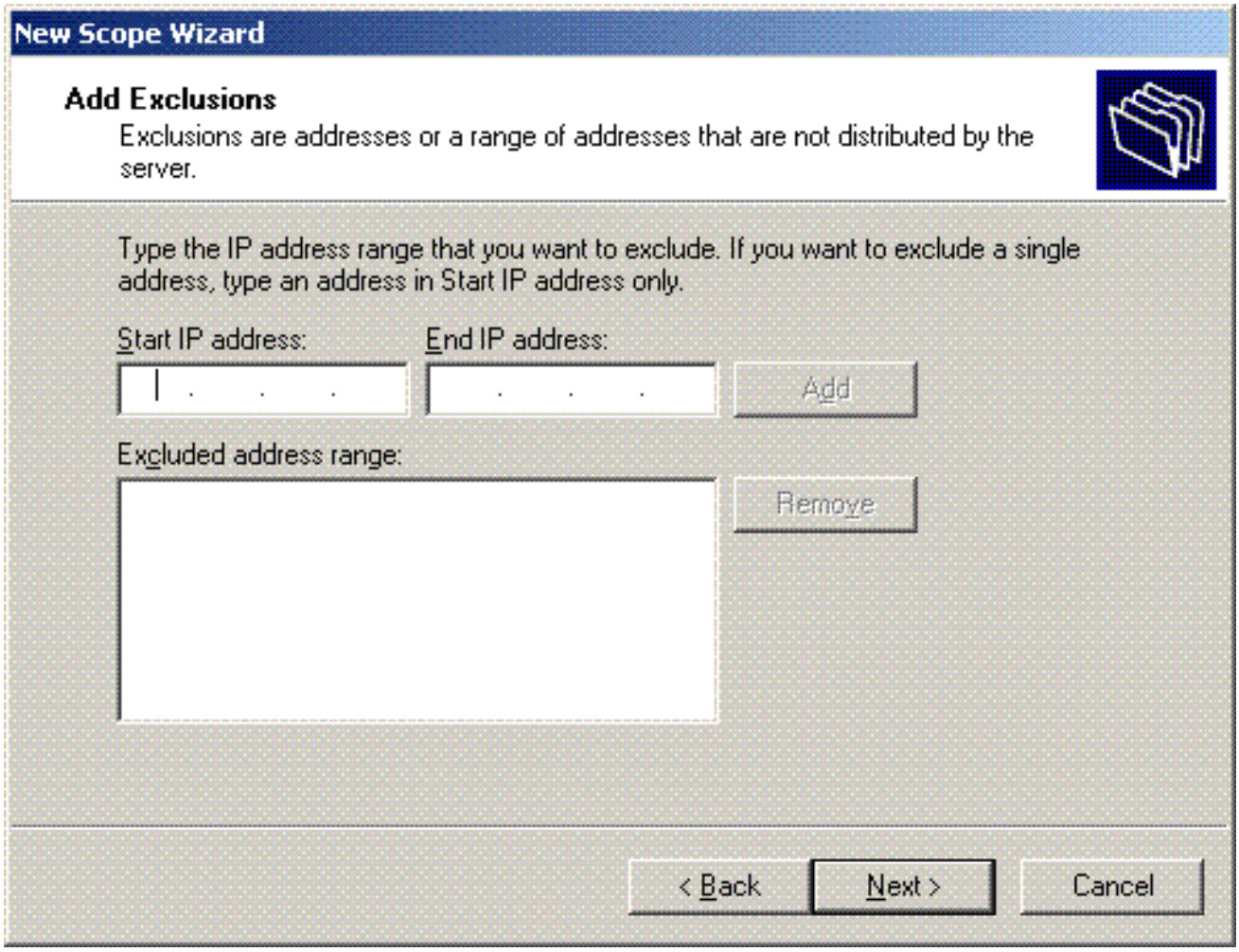
13. IP Address Range(IP 주소 범위) 페이지에서 범위의 시작 및 끝 IP 주소를 입력하고 Next(**다음**)를 클릭합니다

.

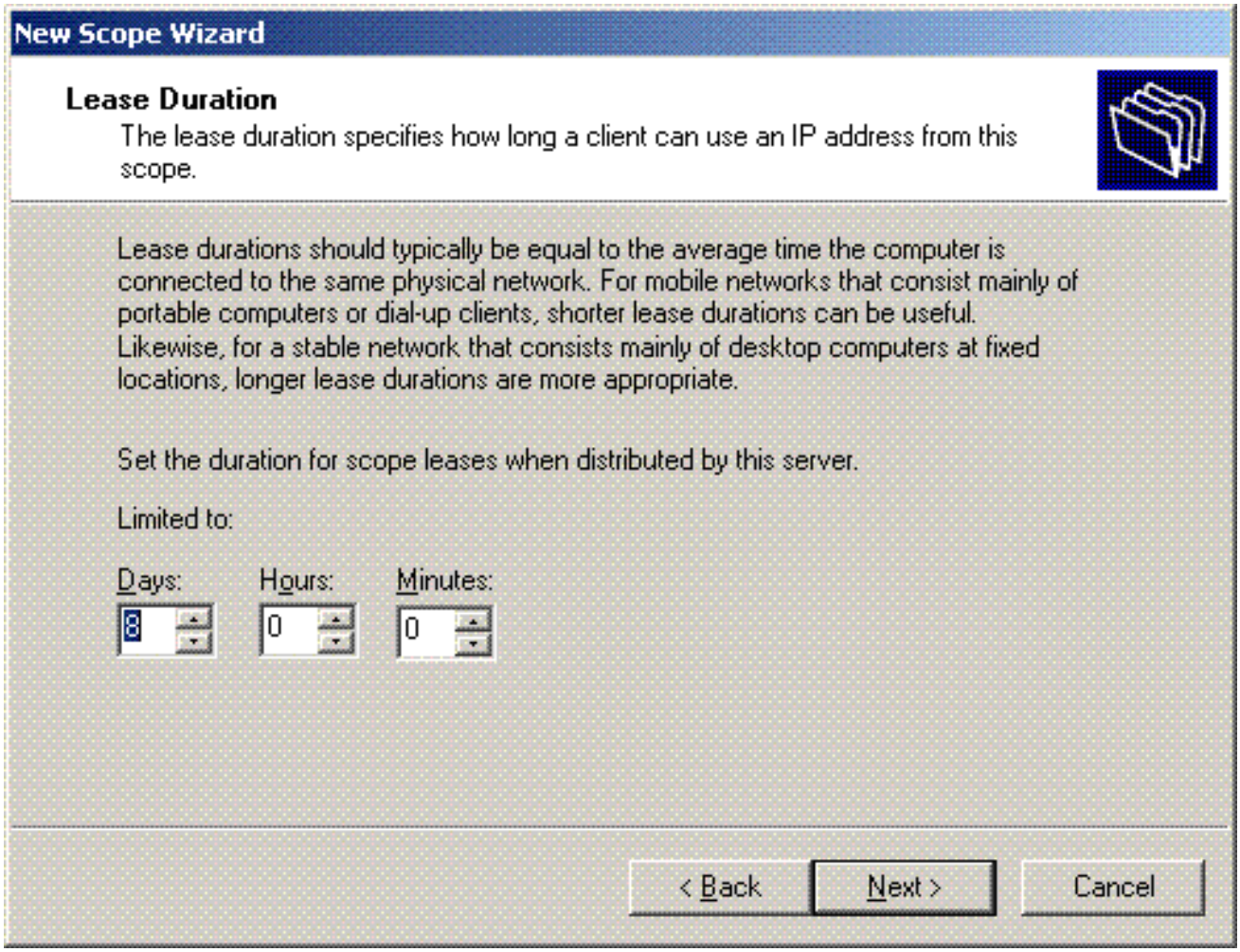


14. Add Exclusions(제외 추가) 페이지에서 DHCP 범위에서 예약/제외하려는 IP 주소를 언급합니다. **Next(다음)**를 클릭합니다

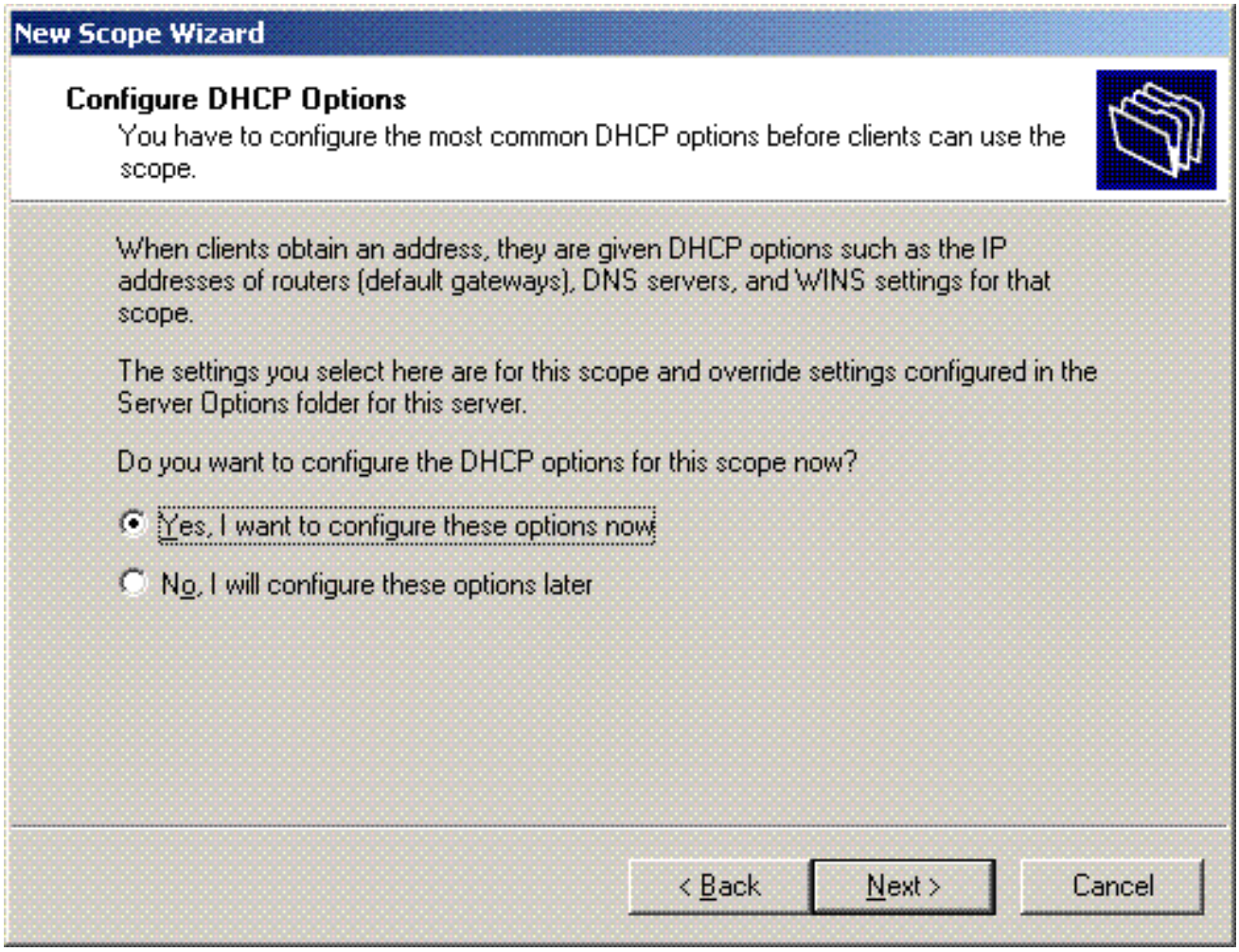
.



15. Lease Duration(리스 기간) 페이지에서 리스 기간을 언급하고 Next(**다음**)를 클릭합니다
.

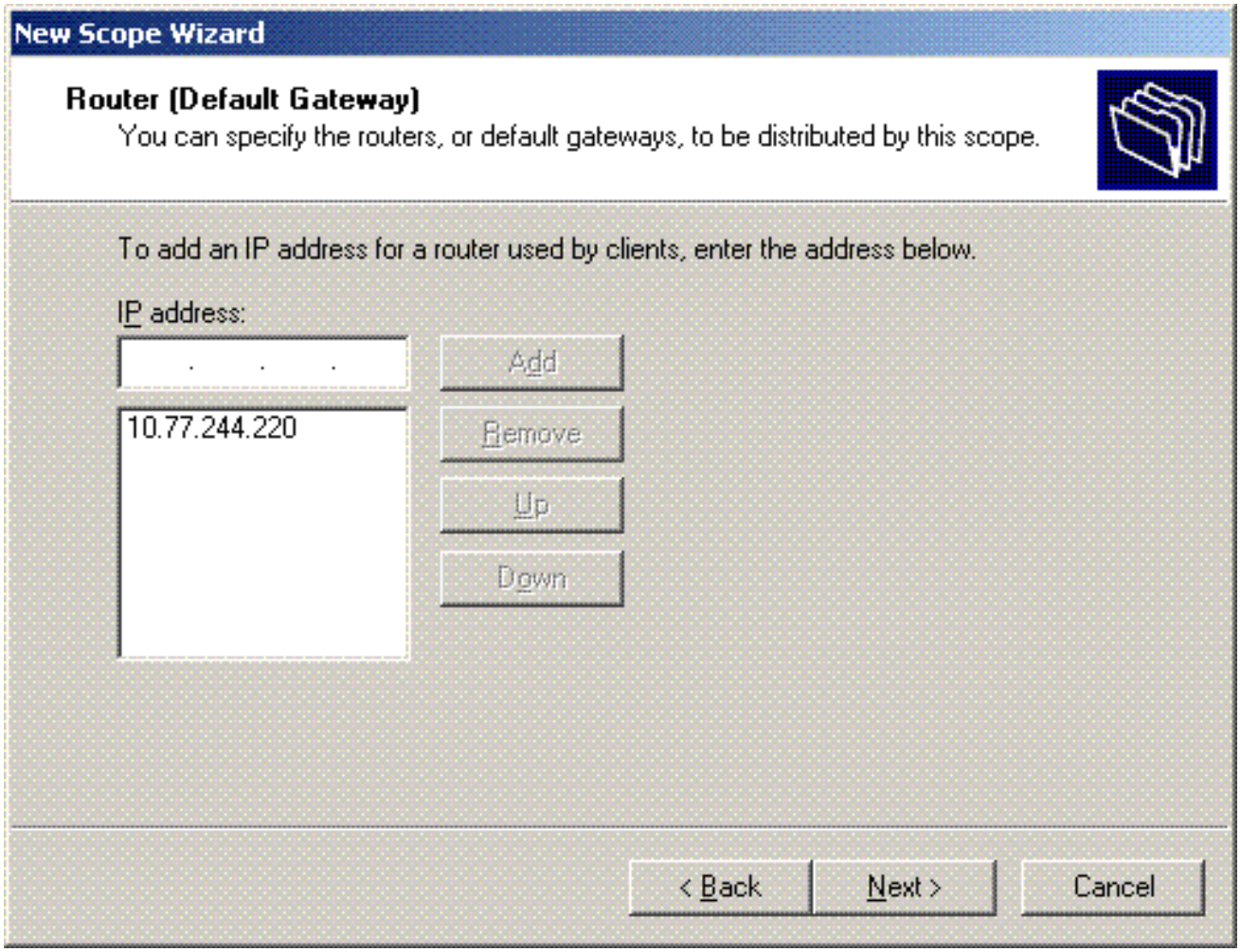


16. Configure DHCP options(DHCP 옵션 구성) 페이지에서 **Yes, I want to configure DHCP Option now(예, 지금 DHCP 옵션을 구성하겠습니다)**를 선택하고 **Next(다음)**를 클릭합니다 .



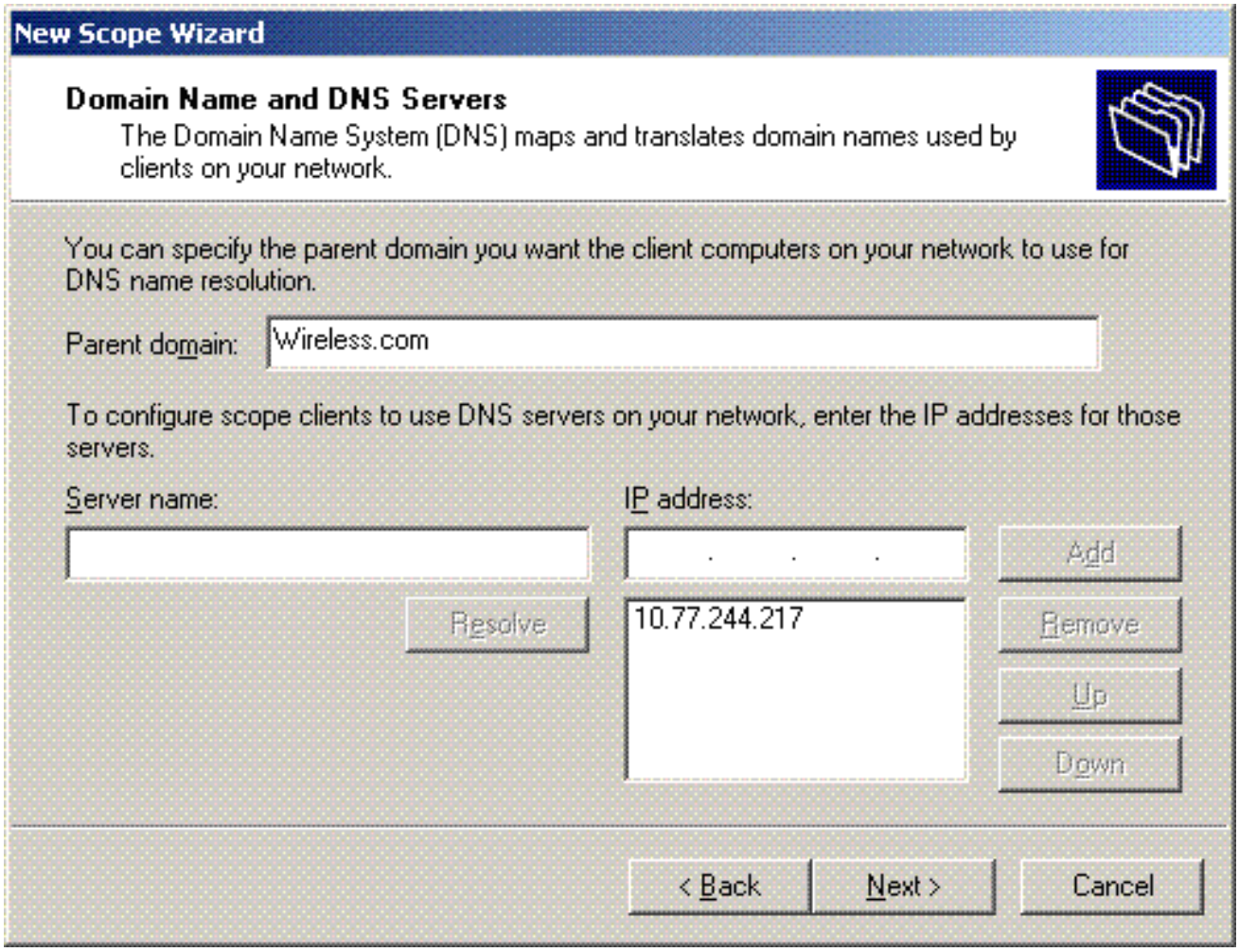
17. 기본 게이트웨이 라우터가 있는 경우 Router (Default Gateway)(라우터(기본 게이트웨이)) 페이지에서 게이트웨이 라우터의 IP 주소를 말하고 Next(**다음)**를 클릭합니다

.



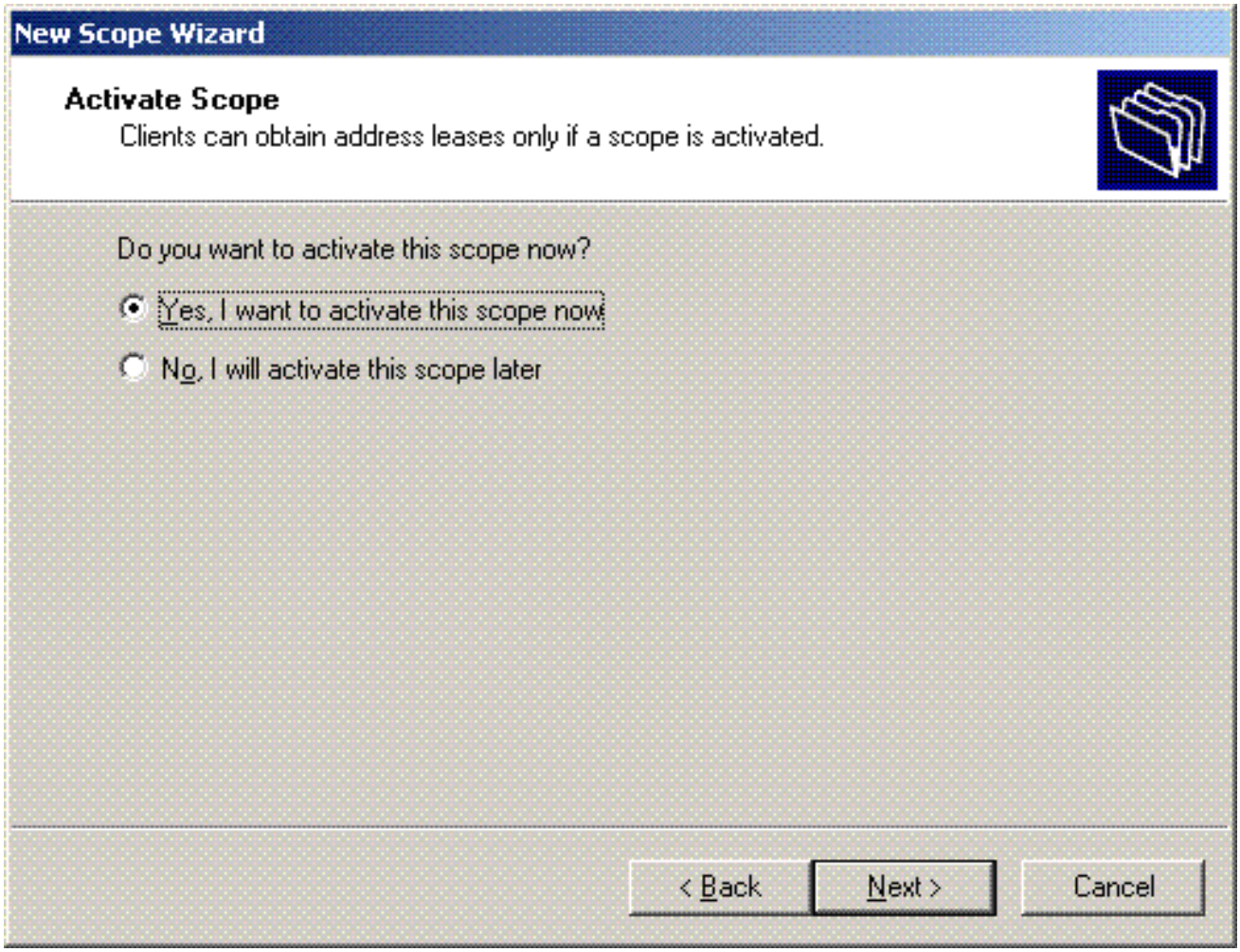
18. Domain Name and DNS servers(도메인 이름 및 DNS 서버) 페이지에서 이전에 구성한 도메인의 이름을 입력합니다. 이 예에서는 **Wireless.com을** 사용합니다. 서버의 IP 주소를 입력합니다. **Add(추가)**를 클릭합니다

.



19. **Next(다음)**를 클릭합니다.
20. WINS Server(WINS 서버) 페이지에서 Next(**다음**)를 클릭합니다.
21. Activate Scope(범위 활성화) 페이지에서 **Yes, I want to activate the scope now(예, 지금 범위를 활성화하겠습니다)**를 선택하고 **Next(다음)**를 클릭합니다

.

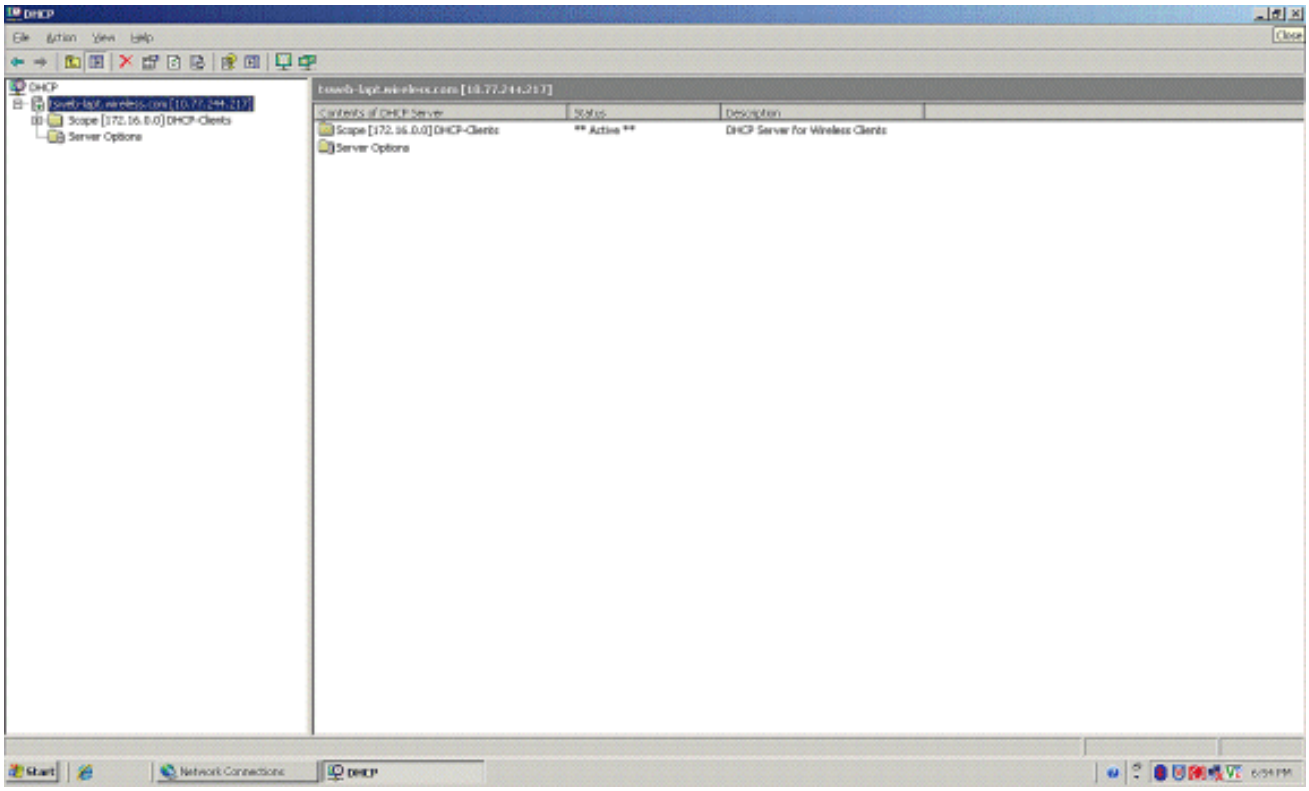


22. New Scope Wizard를 완료하면 Finish를 **클릭합니다**

.

23. DHCP Snapin 창에서 생성된 DHCP 범위가 활성 상태인지 확인합니다

.



이제 서버에서 DHCP/DNS가 활성화되었으므로 서버를 엔터프라이즈 CA(Certificate Authority) 서버로 구성합니다.

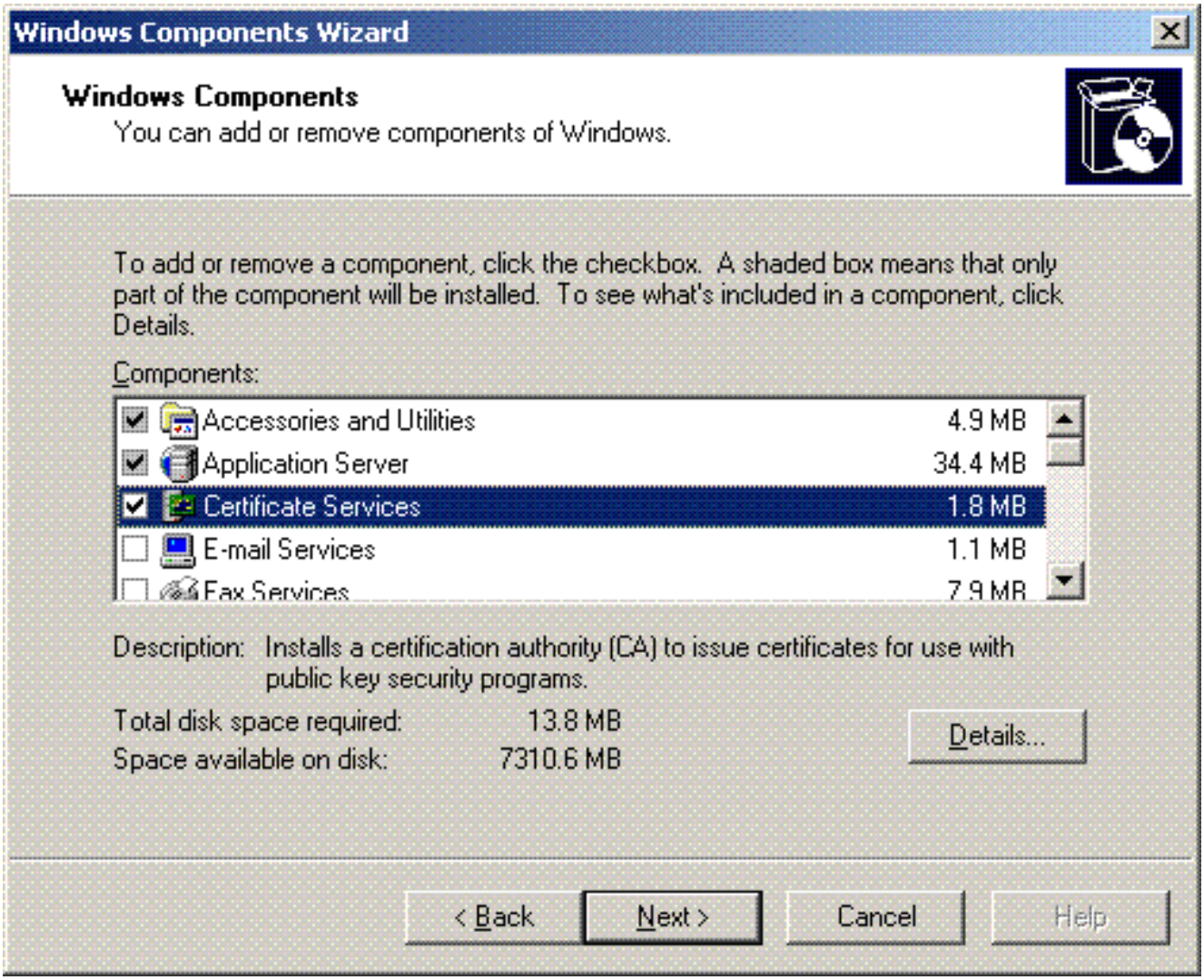
[Microsoft Windows 2003 Server를 CA(Certificate Authority) 서버로 설치 및 구성]

EAP-MS-CHAPv2를 사용하는 PEAP는 서버에 있는 인증서를 기반으로 RADIUS 서버를 검증합니다. 또한 서버 인증서는 클라이언트 컴퓨터에서 신뢰하는 공용 CA(인증 기관)에서 발급해야 합니다. 즉 공용 CA 인증서는 클라이언트 컴퓨터 인증서 저장소의 신뢰할 수 있는 루트 인증 기관 폴더에 이미 있습니다. 이 예에서는 Microsoft Windows 2003 서버를 IAS(Internet Authentication Service)에 인증서를 발급하는 CA(Certificate Authority)로 구성합니다.

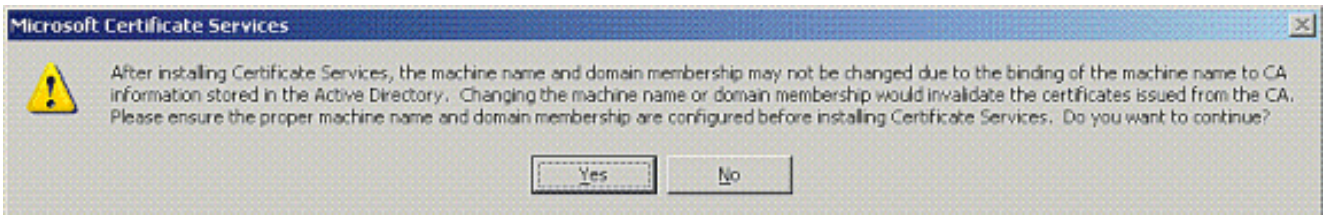
서버에 인증서 서비스를 설치하고 구성하려면 다음 단계를 완료하십시오.

1. 제어판에서 **프로그램 추가/제거를 클릭합니다**.
2. **Windows 구성 요소 추가/제거를** 클릭합니다.
3. Certificate **Services(인증서 서비스)를 클릭합니다**

.

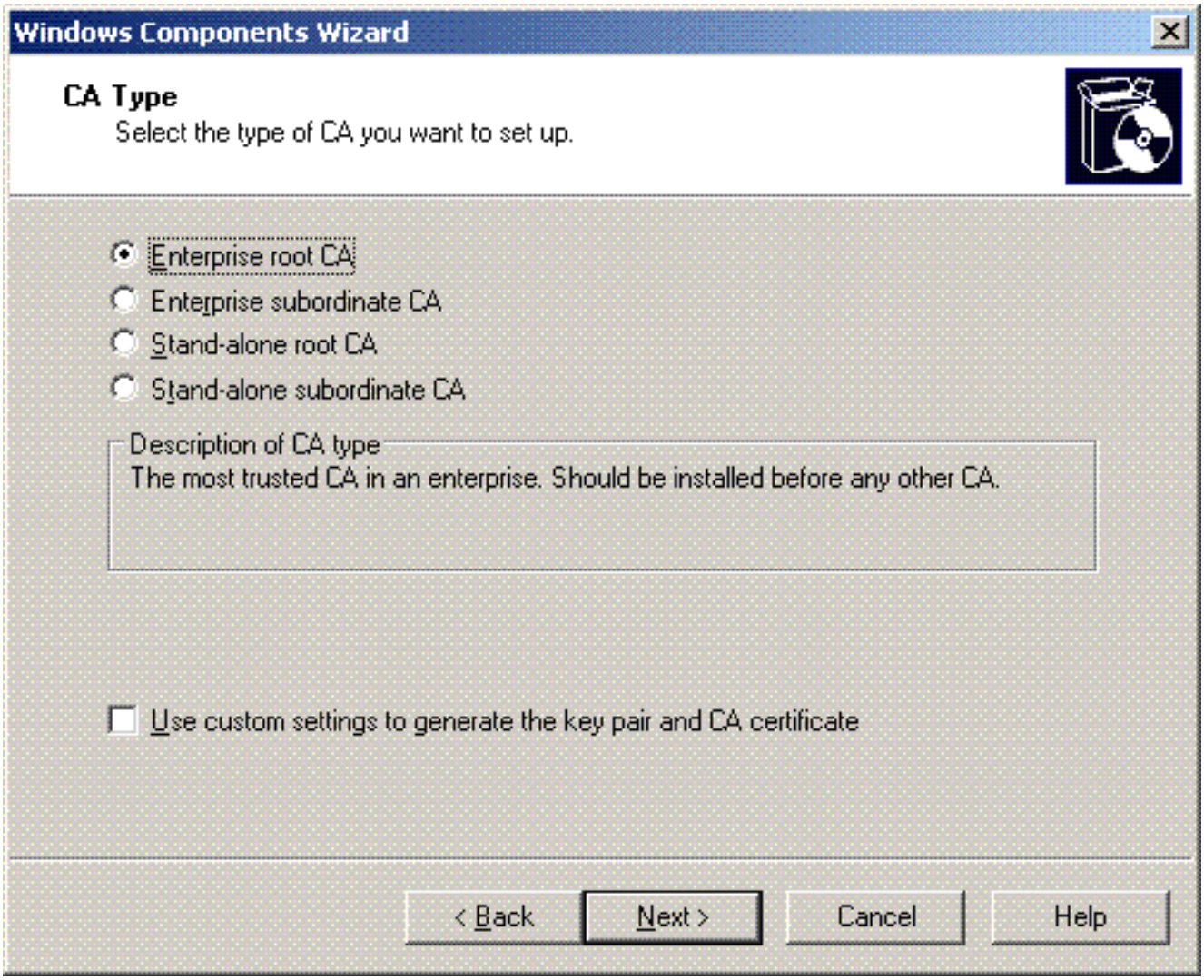


4. Certificate **Services를 설치한 후 컴퓨터의 이름을 바꿀 수 없으며 도메인에 가입하거나 도메인에서 제거할 수 없다는** 경고 메시지**가 나타나면 Yes(예)를 클릭합니다. 계속하시겠습니까?**



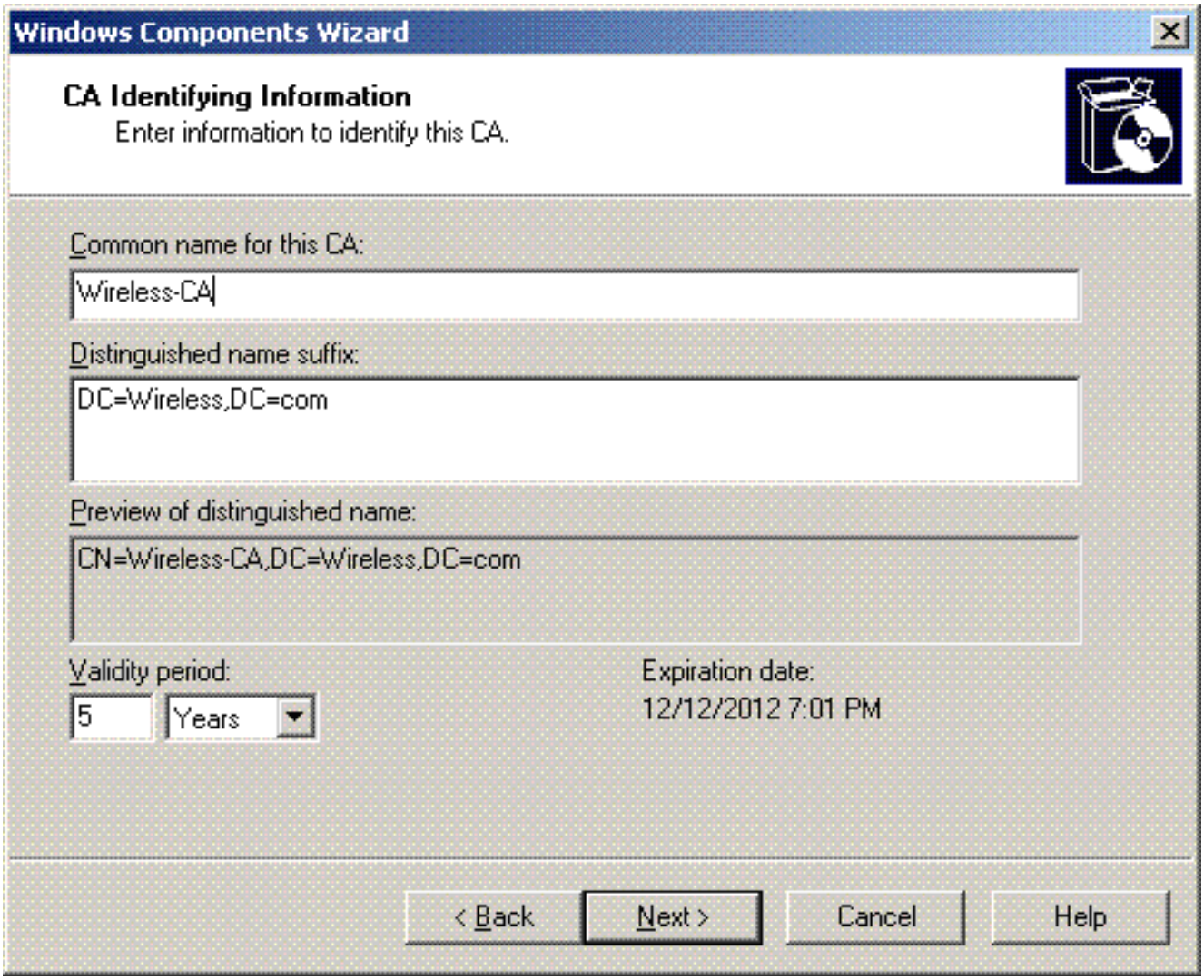
5. Certificate Authority Type(인증 기관 유형)에서 **Enterprise root CA(엔터프라이즈 루트 CA)**를 선택하고 **Next(다음)**를 클릭합니다

.



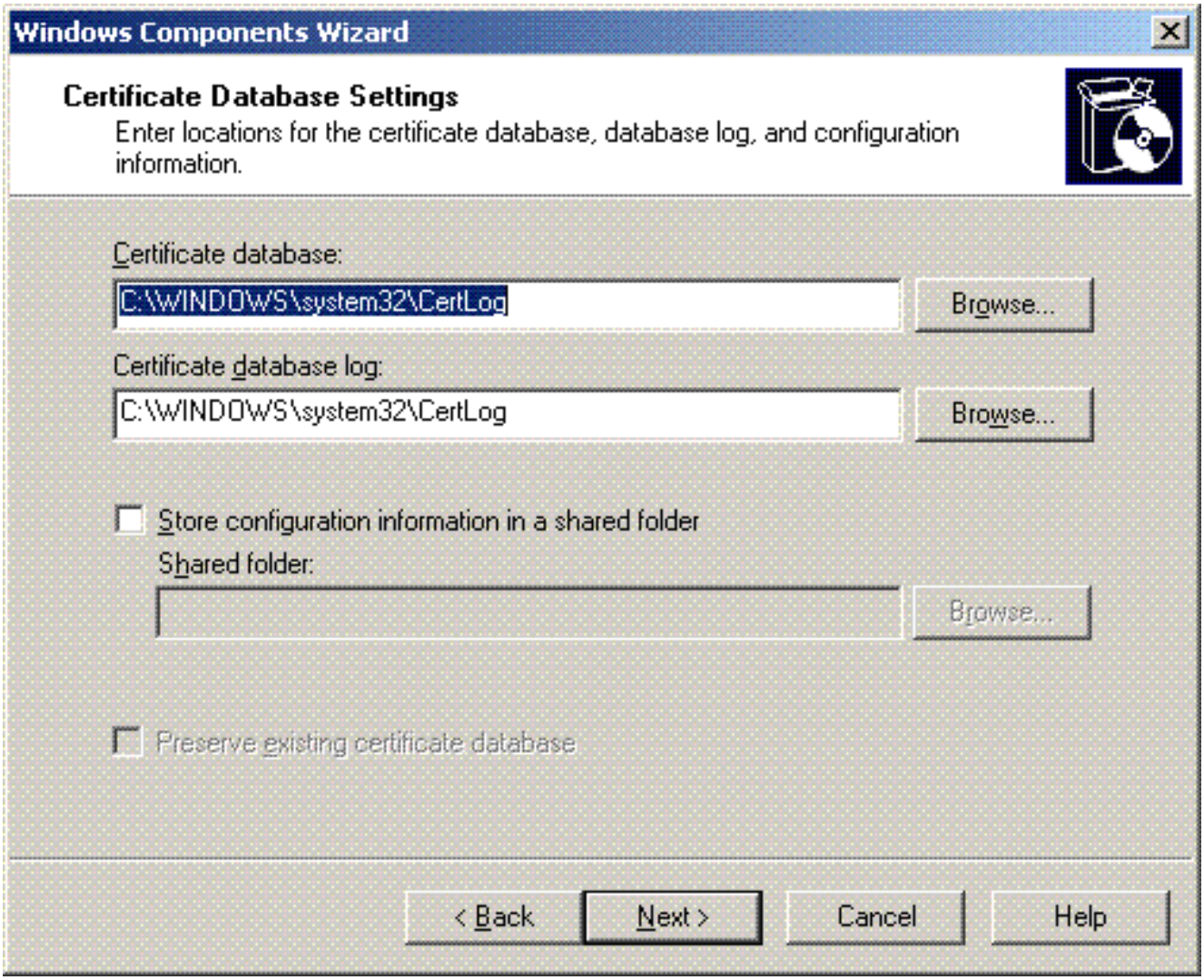
6. CA를 식별하는 이름을 입력합니다. 이 예에서는 **Wireless-CA를 사용합니다**. **Next(다음)**를 클릭합니다

.



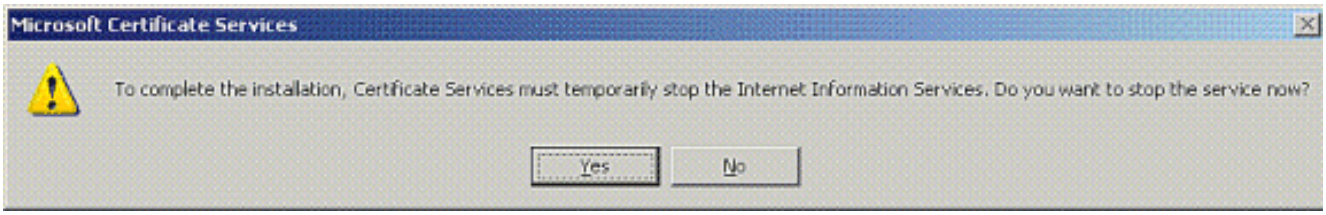
7. 인증서 데이터베이스 스토리지에 대해 "Cert Log" 디렉토리가 생성됩니다. **Next(다음)**를 클릭합니다

.



8. IIS가 활성화된 경우 계속하기 전에 중지해야 합니다. IIS를 **중지해야** 한다는 경고 메시지가 나타나면 OK(확인)를 클릭합니다. CA가 설치되면 자동으로 다시 시작됩니다

.



9. Finish(**마침**)를 클릭하여 CA(Certificate Authority) 서비스 설치를 완료합니다

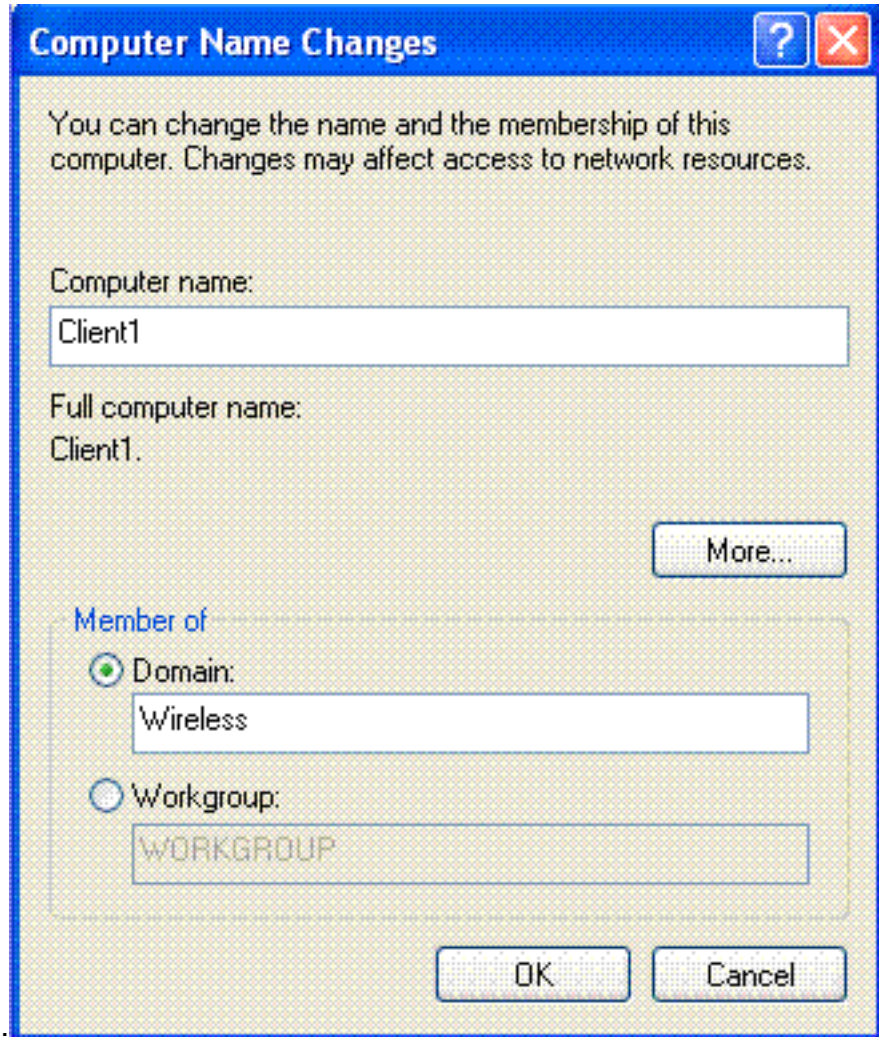
.

다음 단계는 Microsoft Windows 2003 서버에 인터넷 인증 서비스를 설치하고 구성하는 것입니다.

도메인에 클라이언트 연결

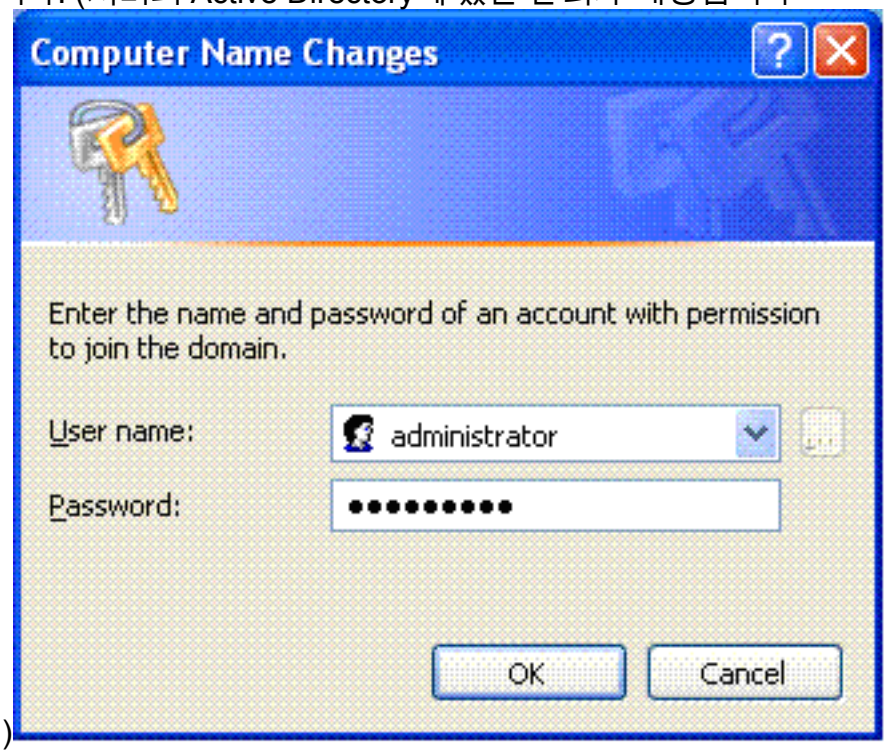
다음 단계는 클라이언트를 유선 네트워크에 연결하고 새 도메인에서 도메인별 정보를 다운로드하는 것입니다. 즉, 클라이언트를 도메인에 연결합니다. 이 작업을 수행하려면 다음 단계를 완료하십시오.

1. straight through 이더넷 케이블을 사용하여 클라이언트를 유선 네트워크에 연결합니다.
2. 클라이언트를 부팅하고 클라이언트의 사용자 이름/비밀번호로 로그인합니다.
3. 시작을 **클릭하고 실행**을 클릭한 다음 cmd를 **입력하고 확인** 을 클릭합니다.
4. 명령 프롬프트에서 ipconfig를 **입력하고 Enter**를 클릭하여 DHCP가 올바르게 작동하고 클라이언트가 DHCP 서버에서 IP 주소를 받았는지 확인합니다.
5. 클라이언트를 도메인에 가입시키려면 **내 컴퓨터**를 마우스 오른쪽 단추로 클릭하고 **속성**을 **선택합니다**.
6. **컴퓨터 이름** 탭을 클릭합니다.
7. 변경을 **클릭합니다**.
8. Domain(**도메인**)을 클릭하고 wireless.**com을** 입력한 다음 **OK(확인)를** 클릭합니다



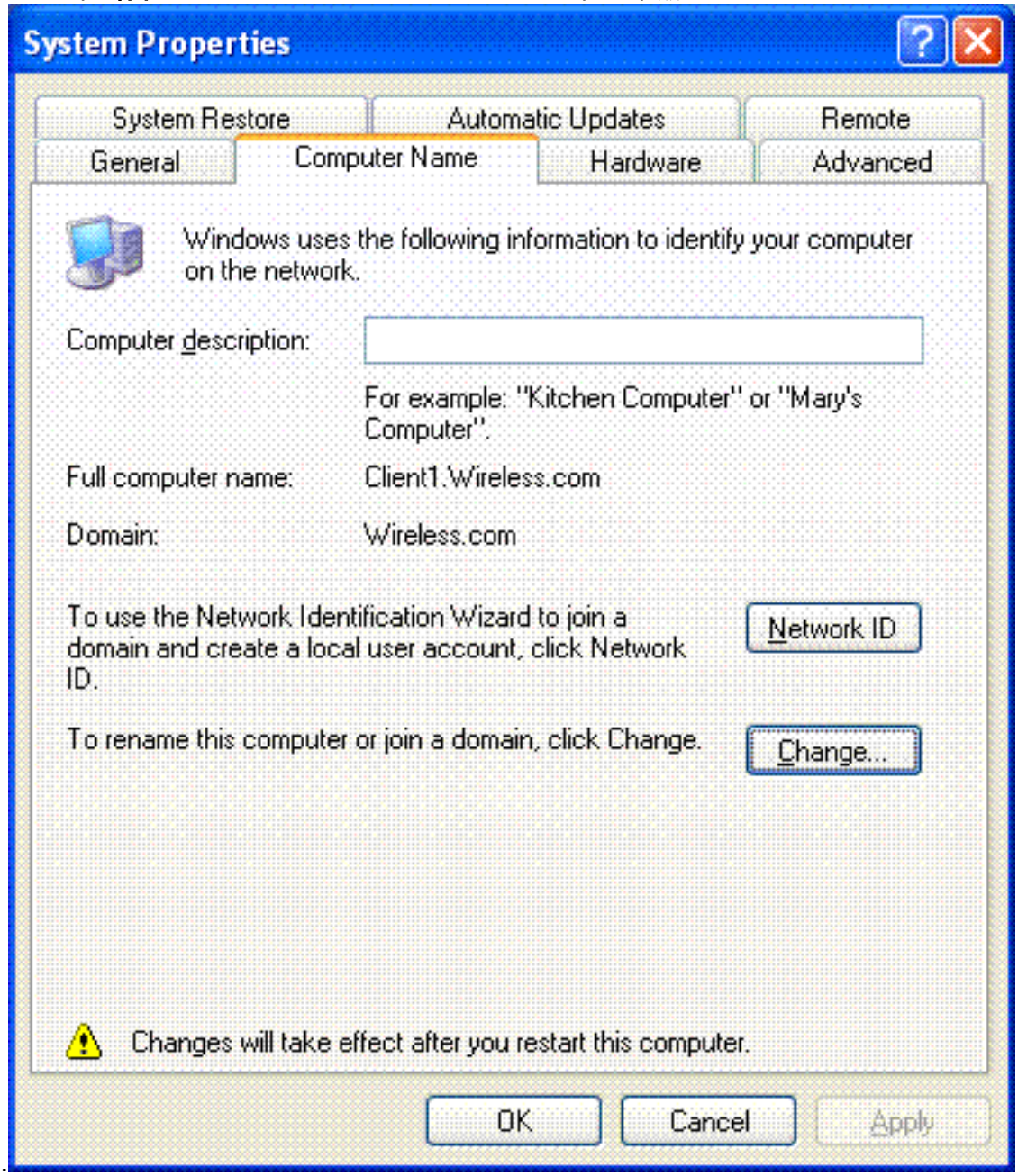
.

9. 클라이언트가 가입하는 도메인에 해당하는 사용자 이름 Administrator 및 비밀번호를 입력합니다. (서버의 Active Directory에 있는 관리자 계정입니다

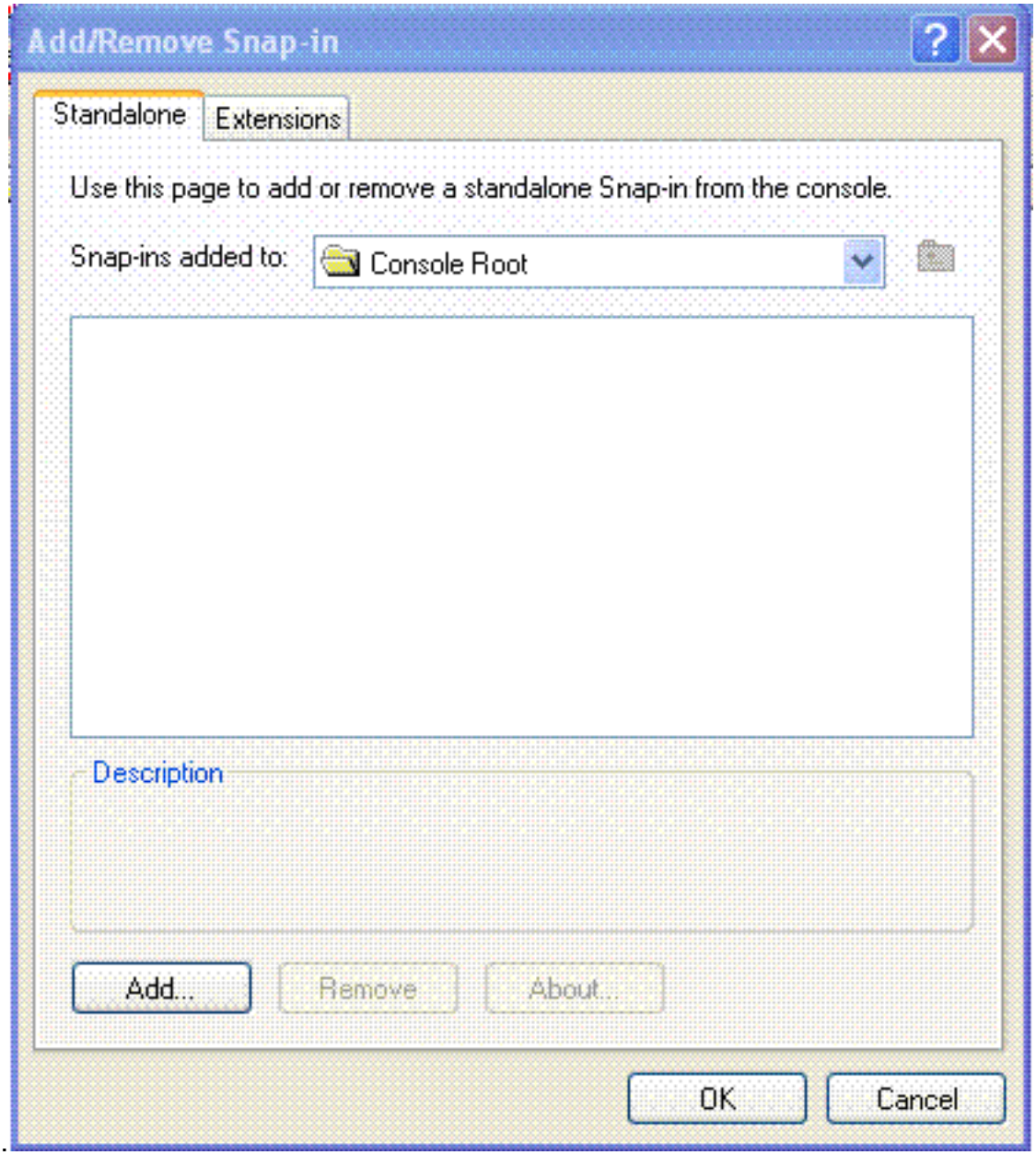


.)

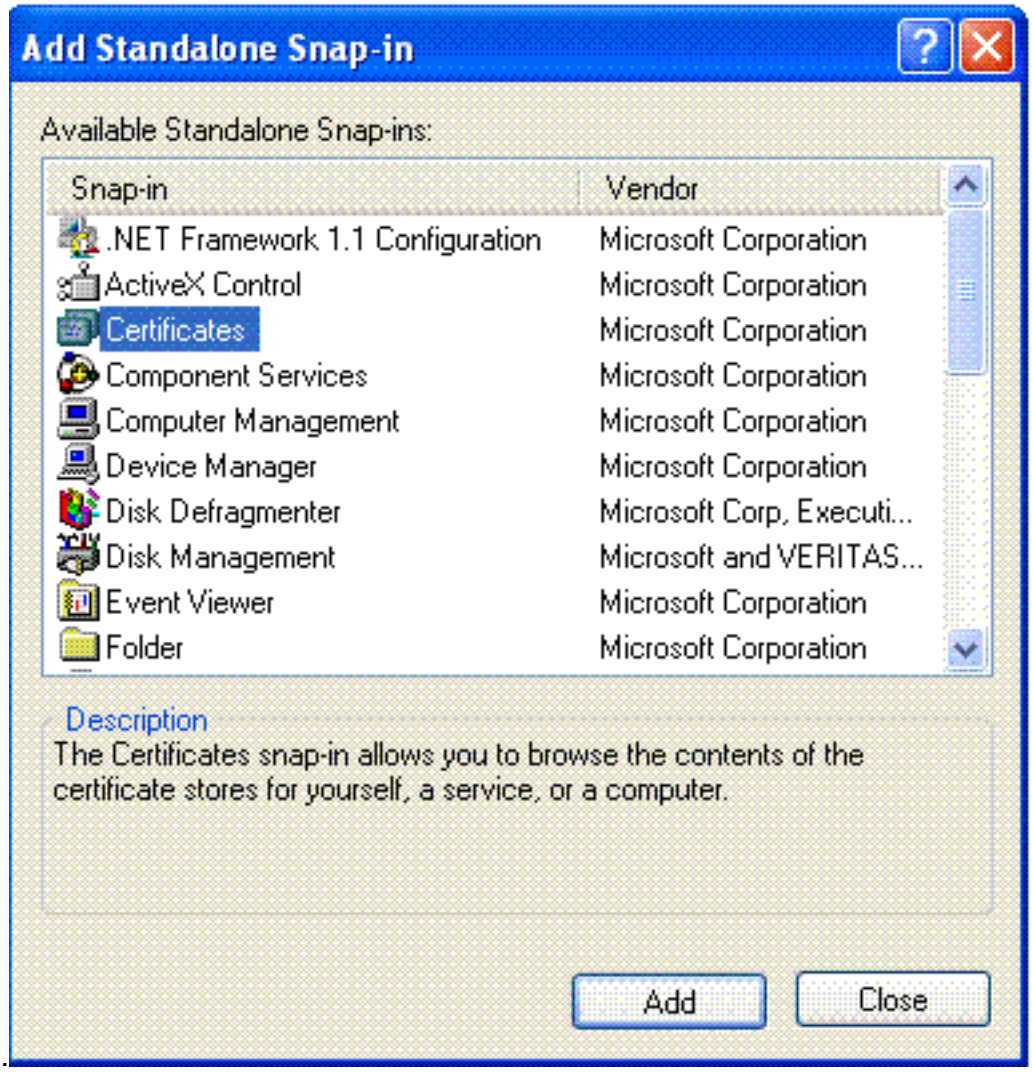
10. **OK(확인)**를 클릭합니다.
11. 컴퓨터를 다시 시작하려면 **Yes(예)**를 클릭합니다.
12. 컴퓨터가 다시 시작되면 사용자 이름 = **관리자**, 비밀번호 = **<도메인 비밀번호>**, 도메인 = **무선** 정보를 사용하여 **로그인합니다**.
13. **내** 컴퓨터**를 마우스 오른쪽 단추**로 클릭하고 속성**을 클릭합니다**.
14. 컴퓨터 **이름** 탭을 클릭하여 Wireless.com 도메인에 있는지 확인합니다



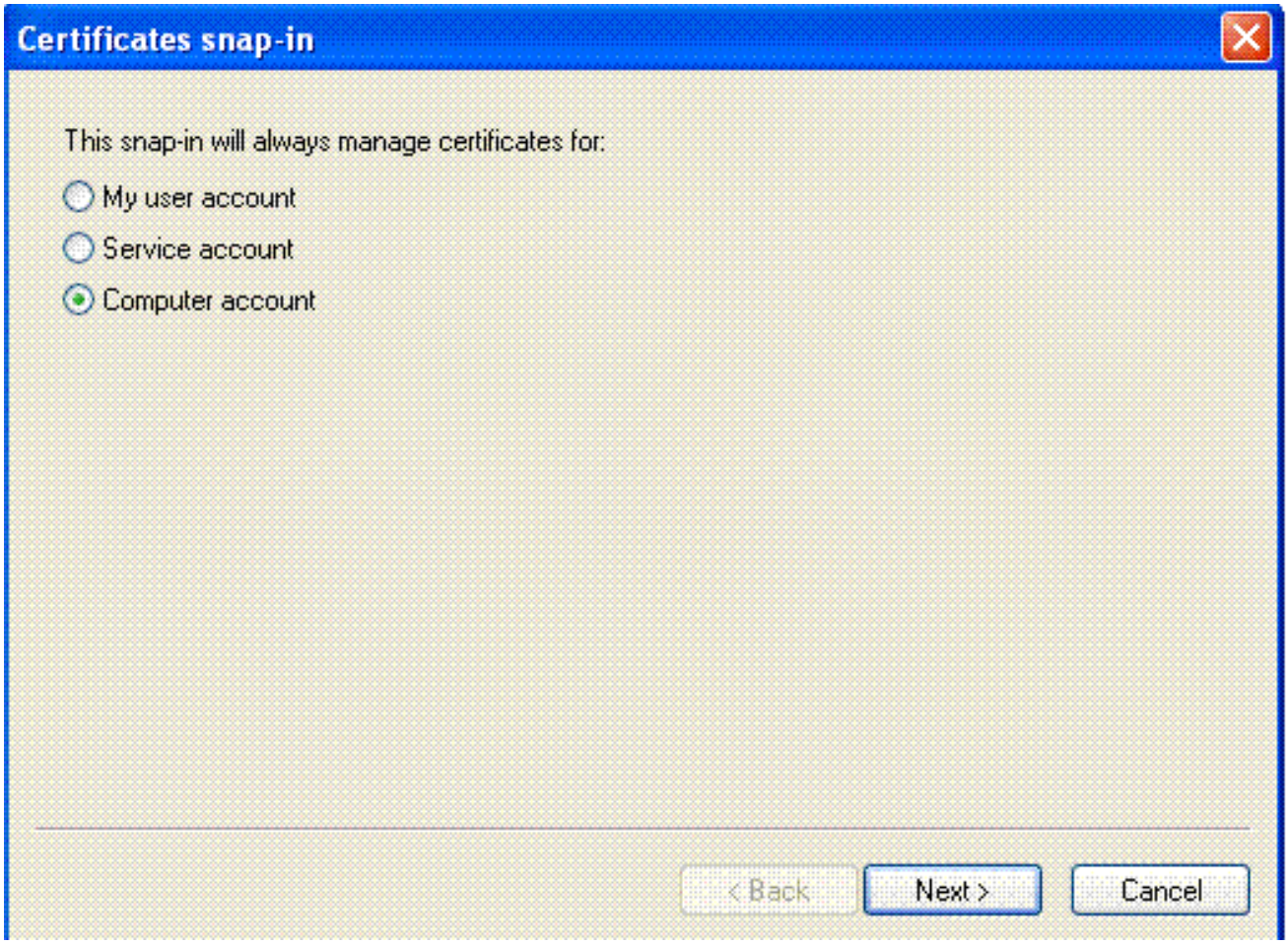
15. 다음 단계는 클라이언트가 서버에서 CA 인증서(trust)를 받았는지 확인하는 것입니다.
16. 시작을 **클릭하고 실행**을 클릭합니다. mmc를 **입력하고 확인** 을 클릭합니다.
17. 파일을 **클릭하고 스냅인 추가/**제거를 클릭합니다



18. **Add(추가)**를 클릭합니다.
19. Certificate(**인증서**)를 선택하고 Add(추가)**를 클릭합니다**

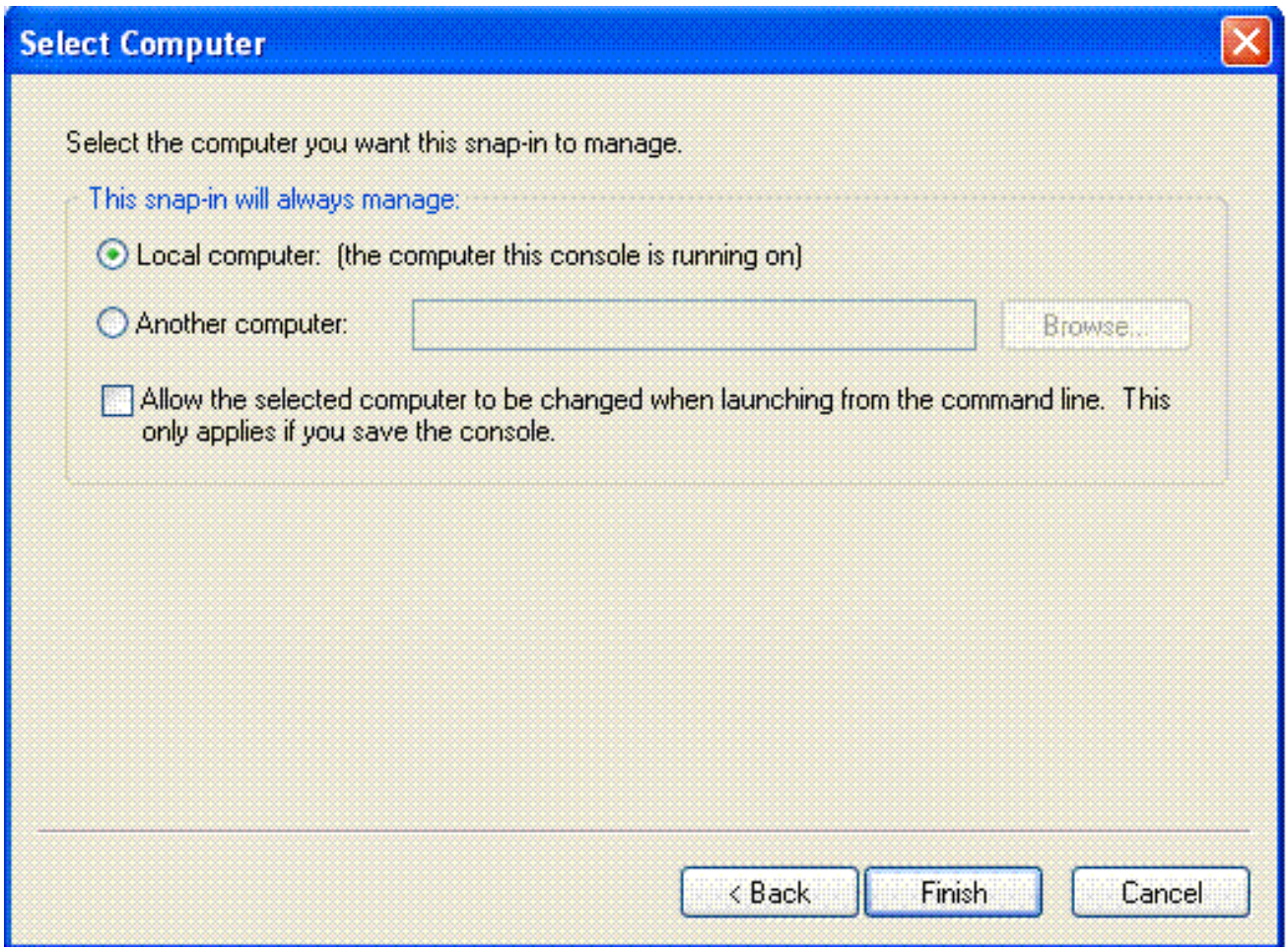


20. 컴퓨터 **계정**을 선택하고 **다음** 을 클릭합니다



21. Finish(**마침**)를 클릭하여 기본 로컬 컴퓨터를 적용합니다

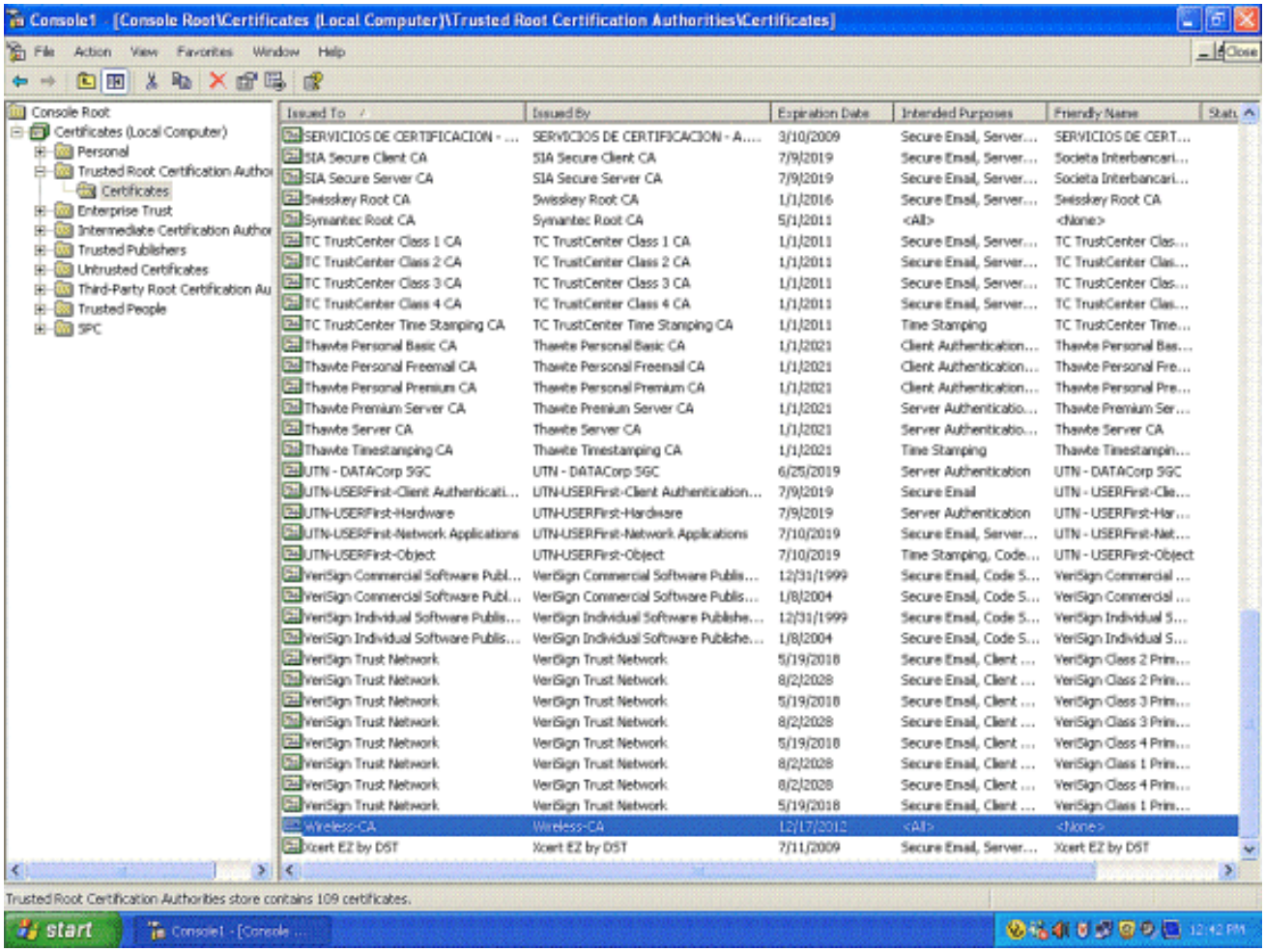
.



22. Close(**닫기**)를 클릭하고 **OK(확인)**를 클릭합니다.

23. Certificates(**인증서**)(**로컬 컴퓨터**)를 확장하고 Trusted **Root Certification Authorities**(**신뢰할 수 있는 루트 인증 기관**)를 확장하고 **Certificates**(**인증서**)를 클릭합니다. 목록에서 **무선**을 찾습니다

.



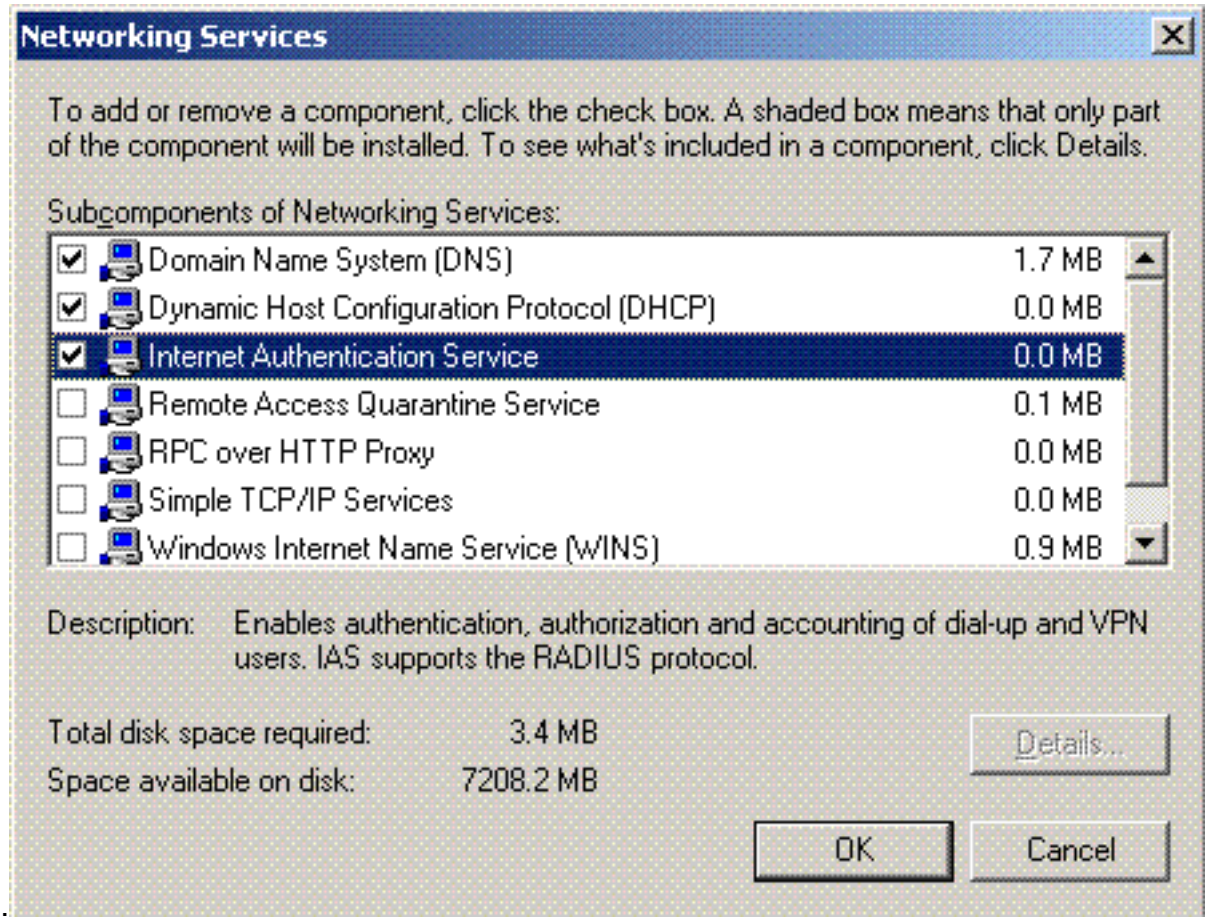
24. 도메인에 클라이언트를 더 추가하려면 이 절차를 반복합니다.

Microsoft Windows 2003 Server에 인터넷 인증 서비스 설치 및 인증서 요청

이 설정에서는 IAS(Internet Authentication Service)를 RADIUS 서버로 사용하여 PEAP 인증으로 무선 클라이언트를 인증합니다.

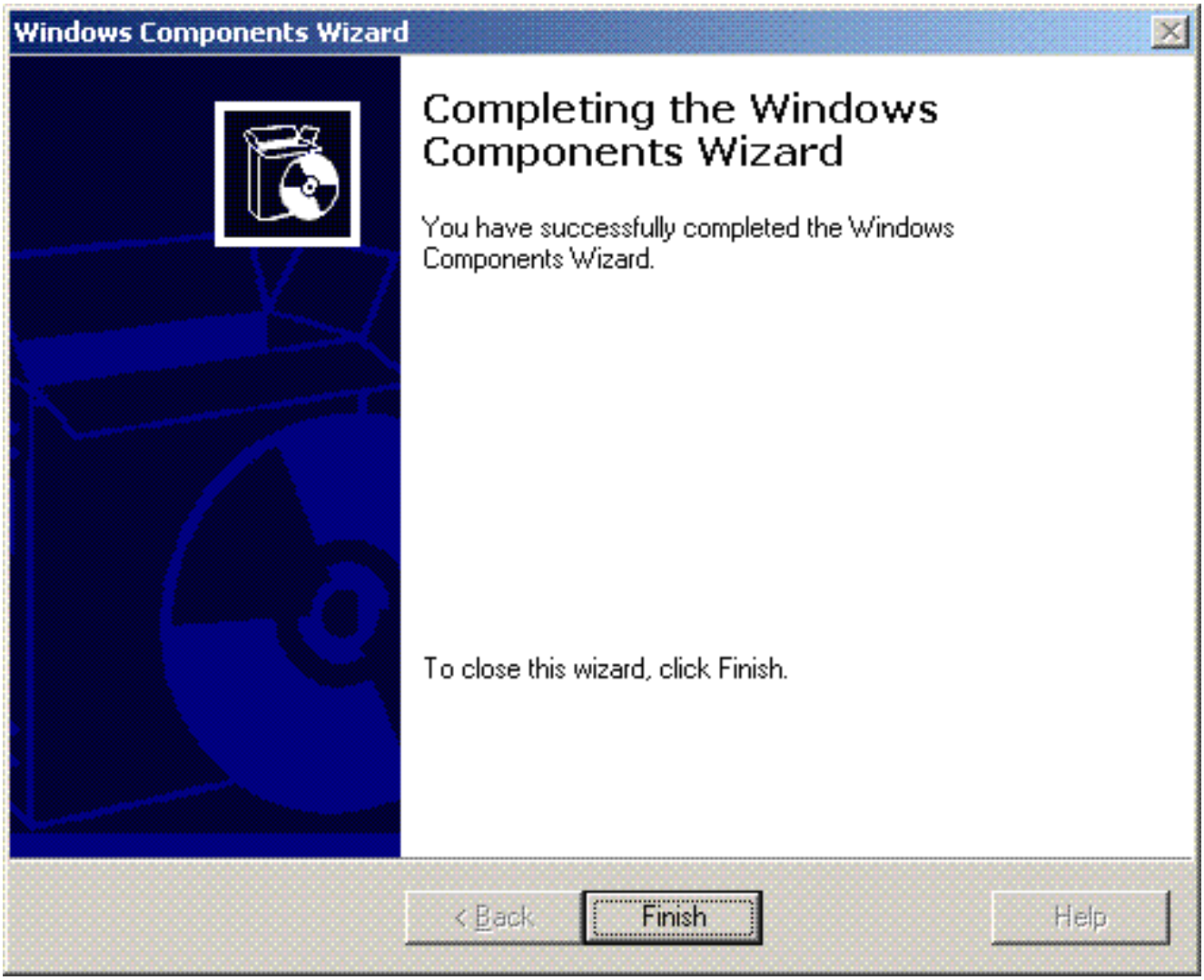
서버에 IAS를 설치하고 구성하려면 다음 단계를 완료하십시오.

1. 제어판에서 **프로그램 추가**/제거를 클릭합니다.
2. **Windows 구성 요소 추가/제거를** 클릭합니다.
3. Networking **Services**(**네트워킹 서비스**)를 선택하고 Details(**세부사항**)를 클릭합니다.
4. **Internet Authentication Service**(**인터넷 인증 서비스**)를 선택하고 **OK**(**확인**)를 클릭한 후 Next(**다음**)를 클릭합니다



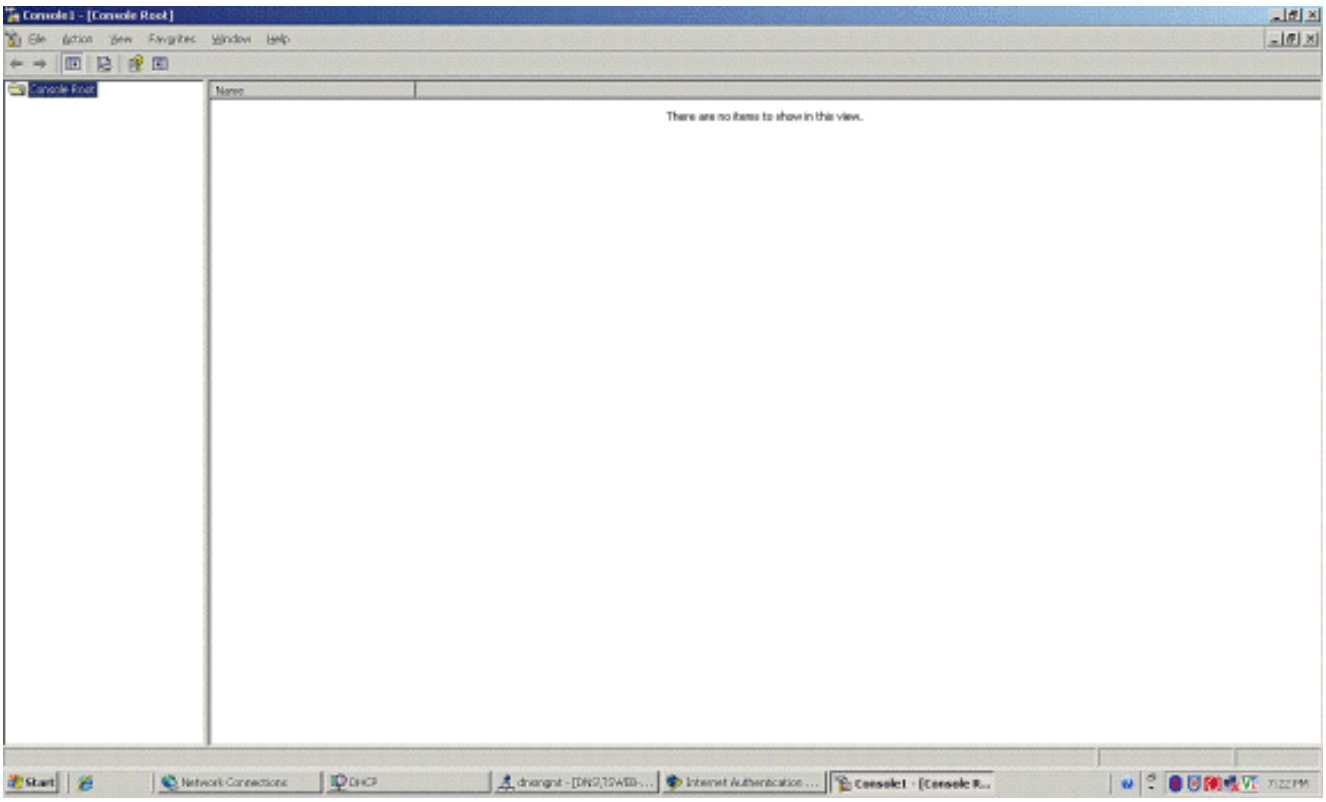
5. Finish(**마침**)를 클릭하여 IAS 설치를 완료합니다

.



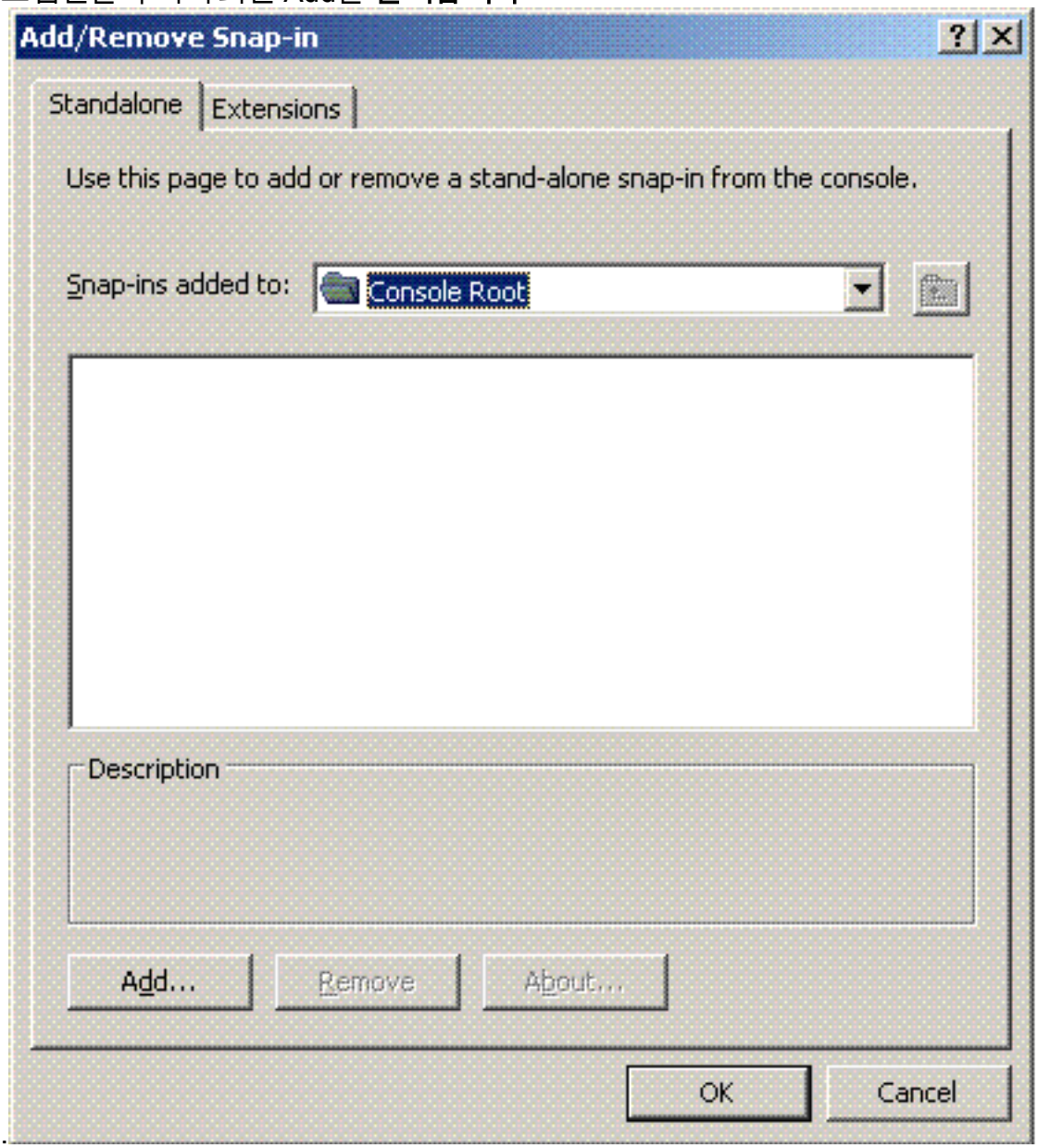
6. 다음 단계는 IAS(인터넷 인증 서비스)용 컴퓨터 인증서를 설치하는 것입니다.
7. 시작을 **클릭하고 실행**을 클릭합니다. mmc를 **입력하고 확인** 을 클릭합니다

.

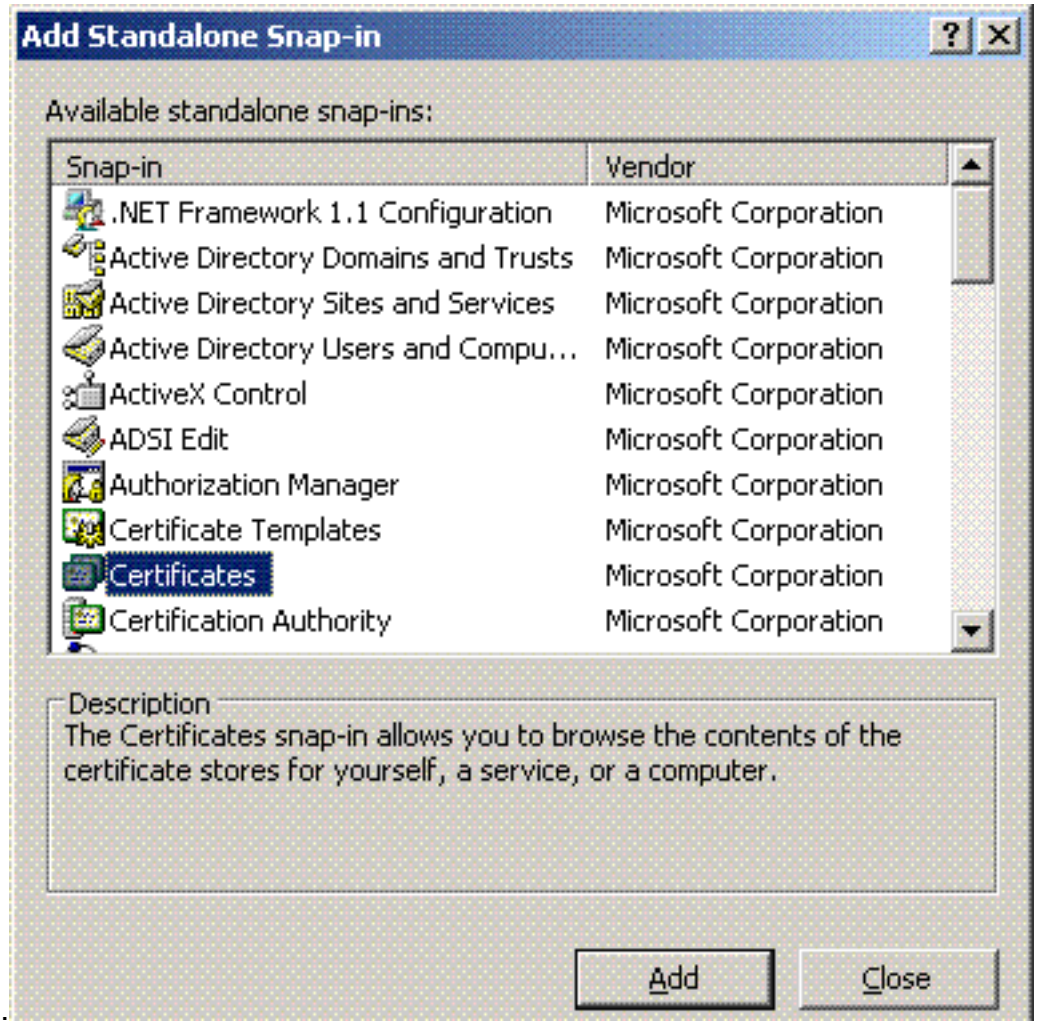


8. 파일 **메뉴**에서 콘솔을 클릭하고 **스냅인 추가/제거**를 선택합니다.

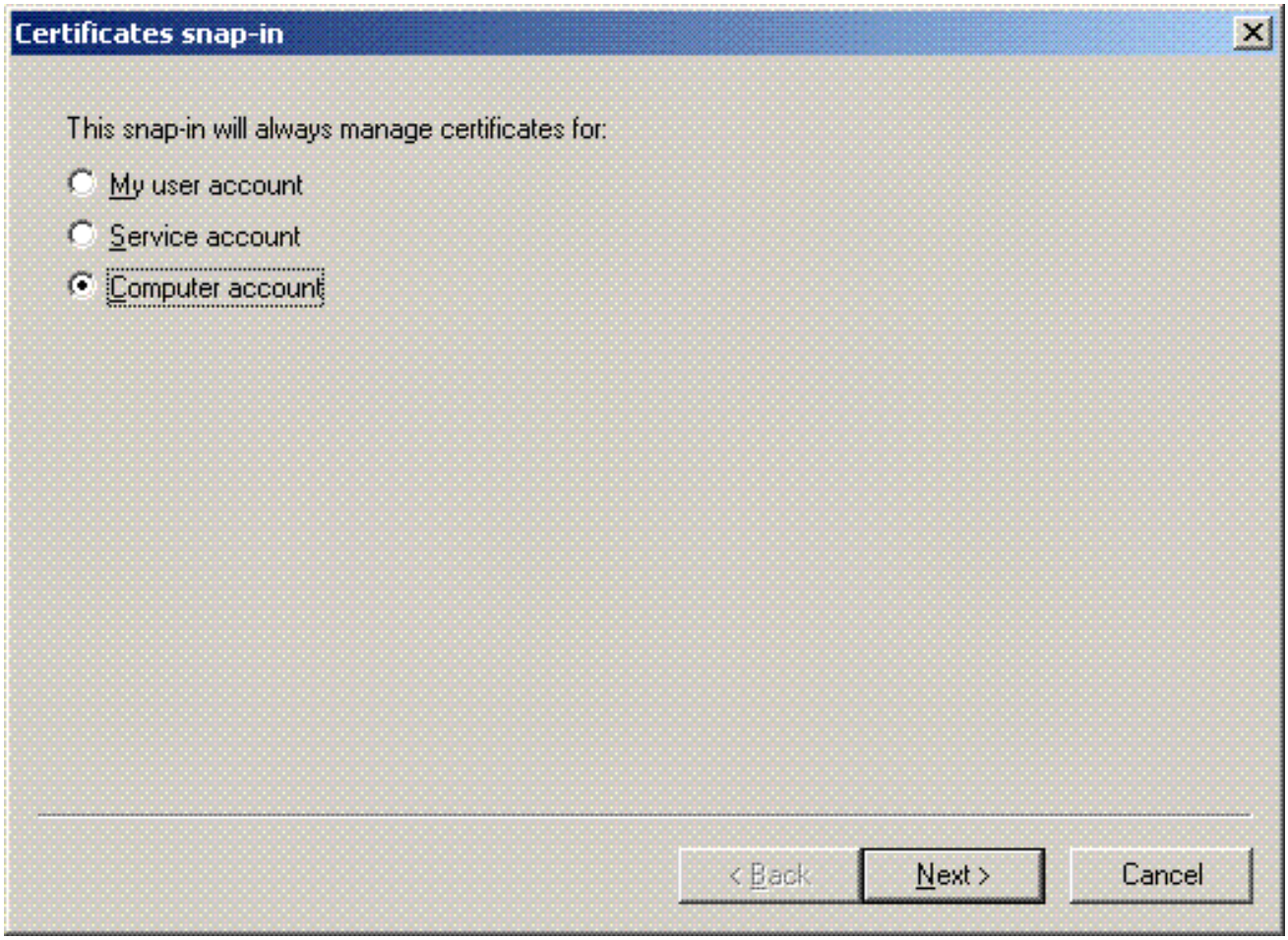
9. 스냅인을 추가하려면 Add를 **클릭합니다**



10. 스냅인 **목록**에서 Certificates(인증서)를 선택하고 Add(추가)**를 클릭합니다**

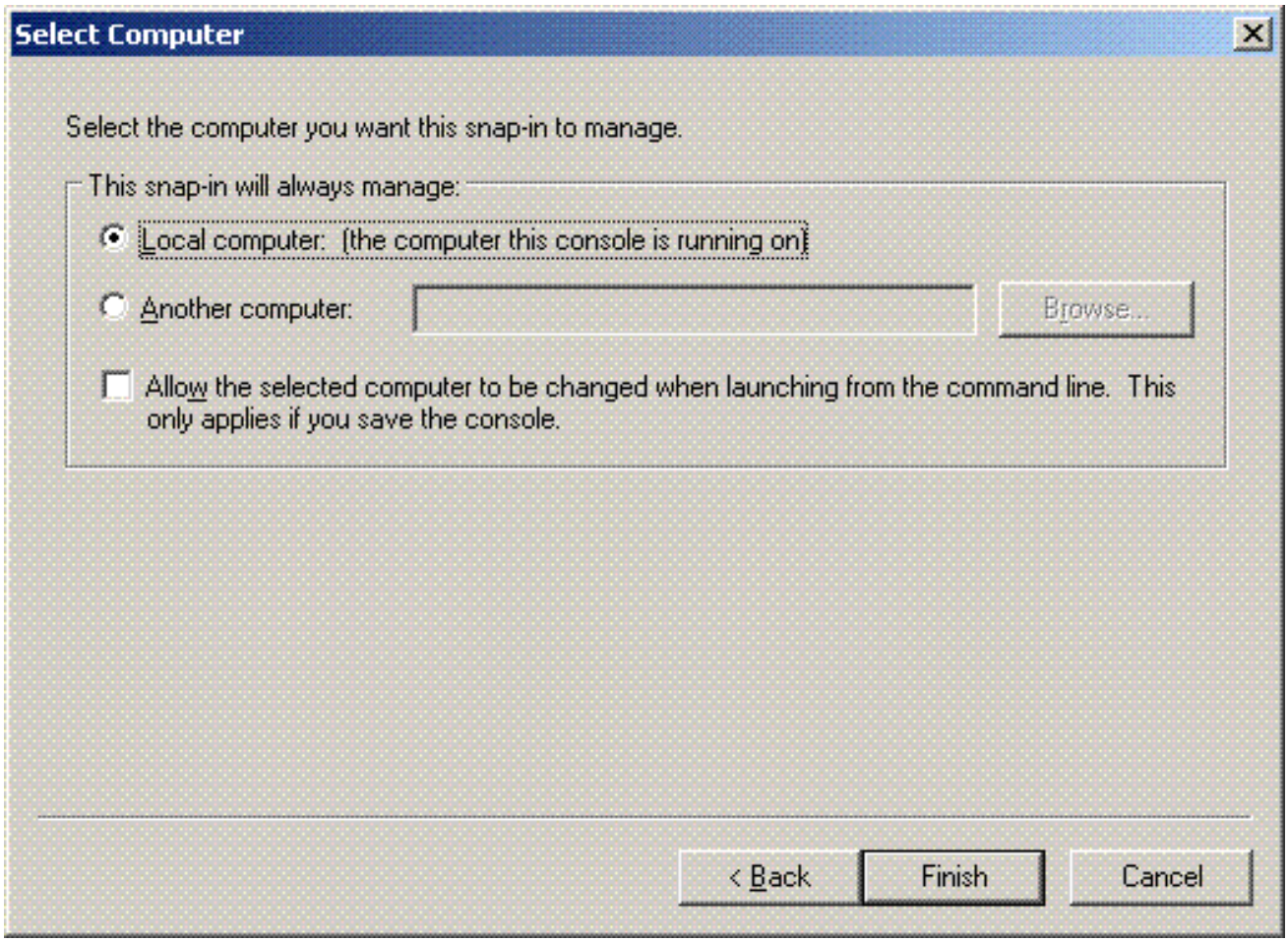


11. 컴퓨터 **계정**을 선택하고 **다음** 을 클릭합니다



12. Local **computer(로컬 컴퓨터)**를 선택하고 Finish(마침)**를 클릭합니다**

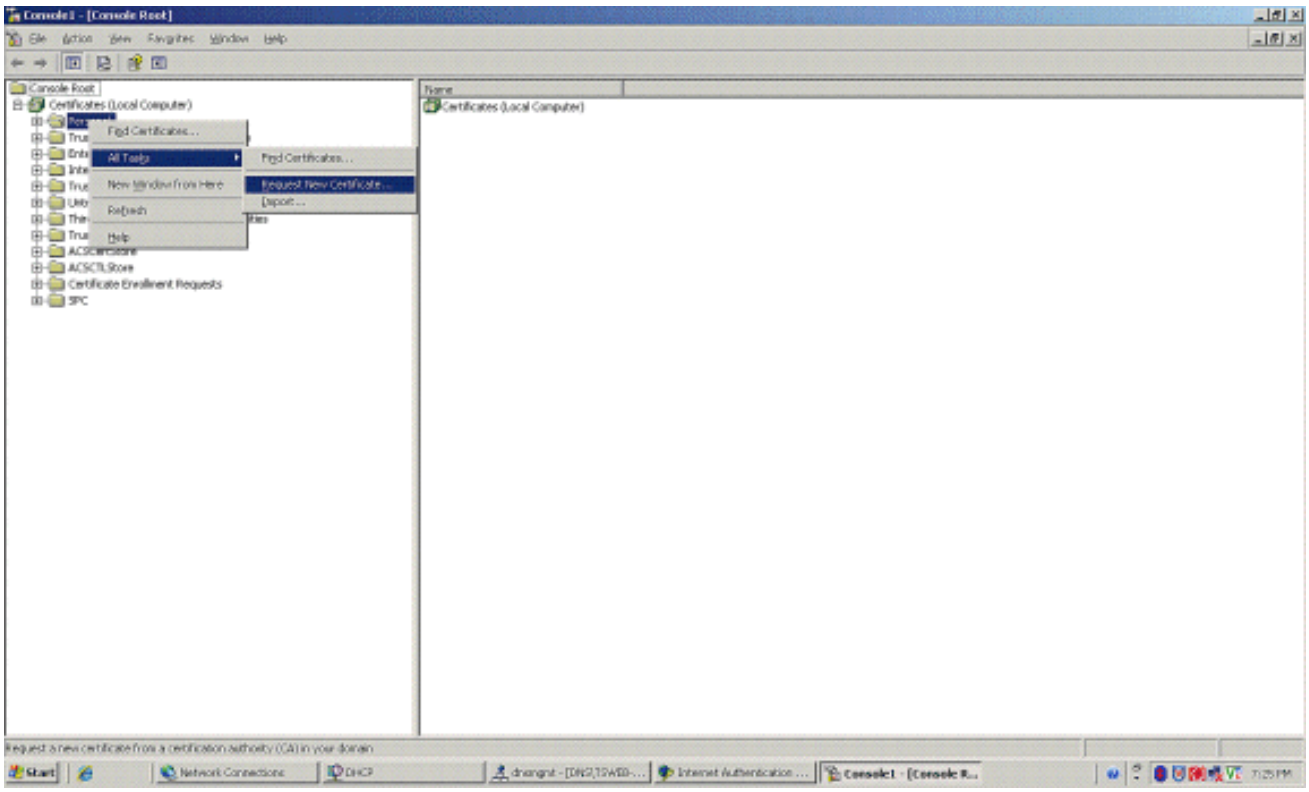
.



13. Close(**닫기**)를 클릭하고 **OK(확인)**를 클릭합니다.

14. Certificates(**인증서)(로컬 컴퓨터)**를 확장하고 **Personal** 폴더를 마우스 오른쪽 단추로 클릭한 다음 **All tasks(모든 작업)**를 선택한 다음 **Request New Certificate(새 인증서 요청)를 선택합니다**

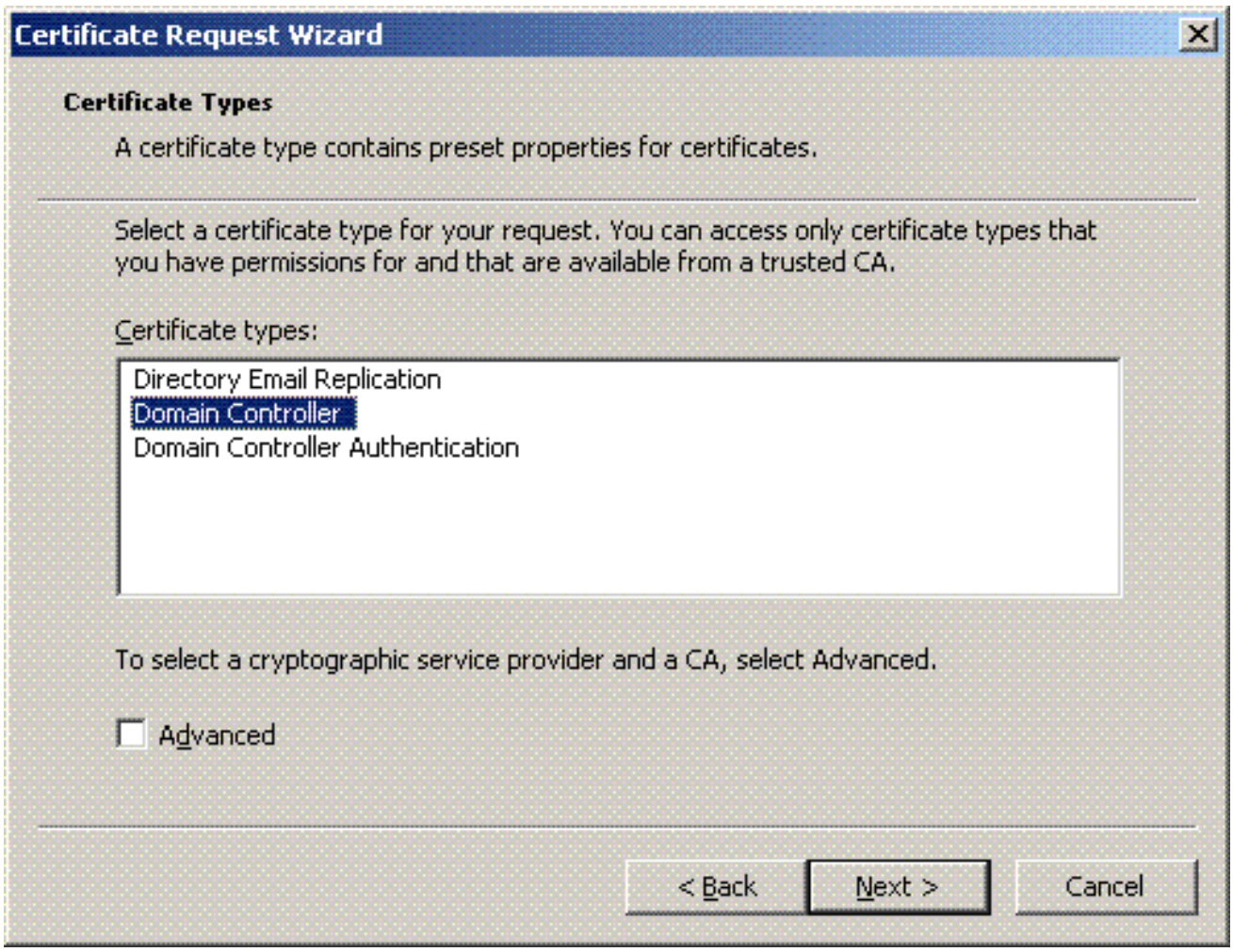
.



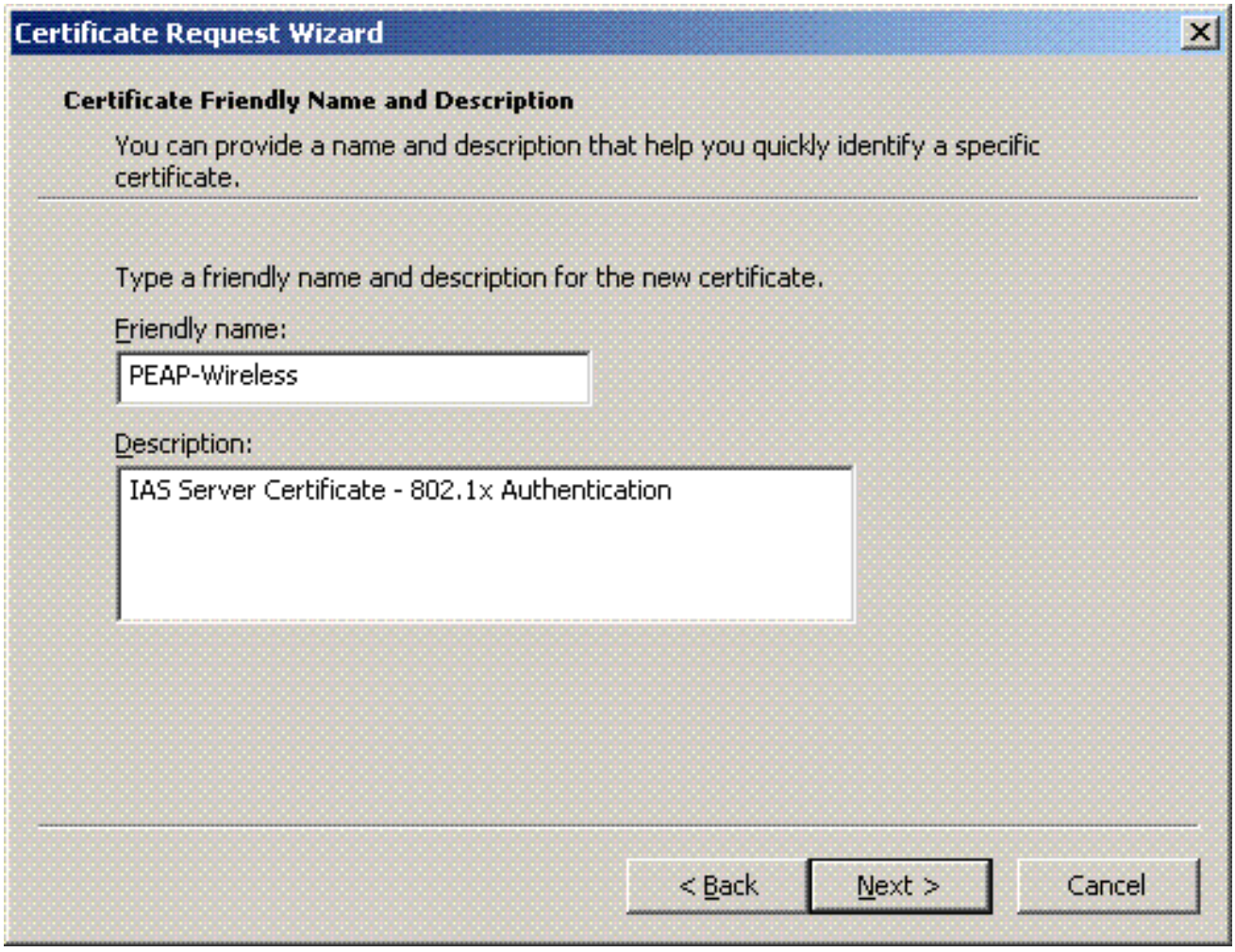
15. *인증서 요청 마법사 시작*에서 *다음을* 클릭합니다

.

16. **도메인 컨트롤러** 인증서 템플릿(DC 이외의 서버에서 컴퓨터 인증서를 요청하는 경우 **컴퓨터** 인증서 템플릿 선택)을 선택하고 **Next(다음)**를 클릭합니다

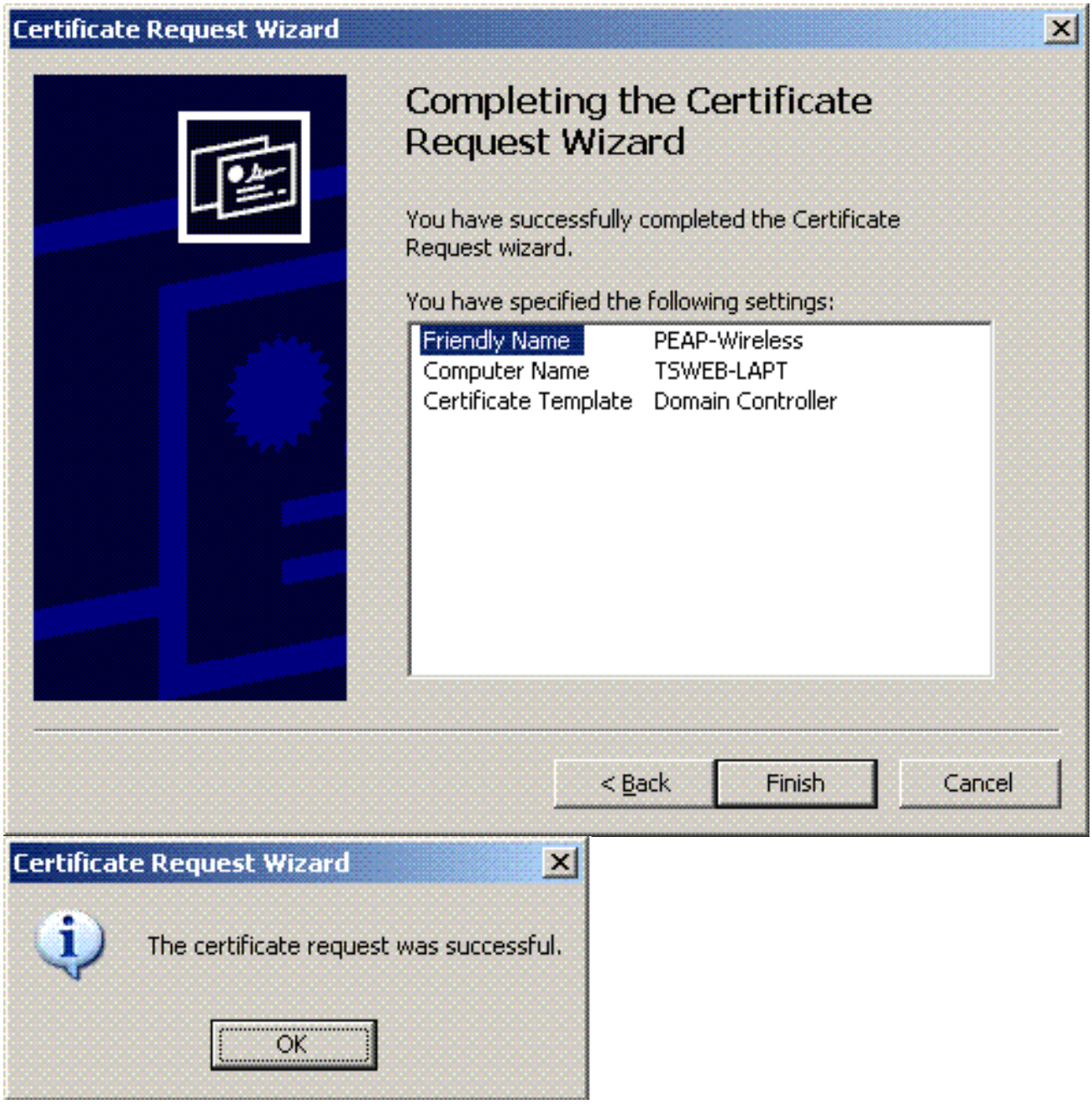


17. 인증서의 이름과 설명을 입력합니다



18. Finish(**마침**)를 클릭하여 인증 요청 마법사를 완료합니다

.

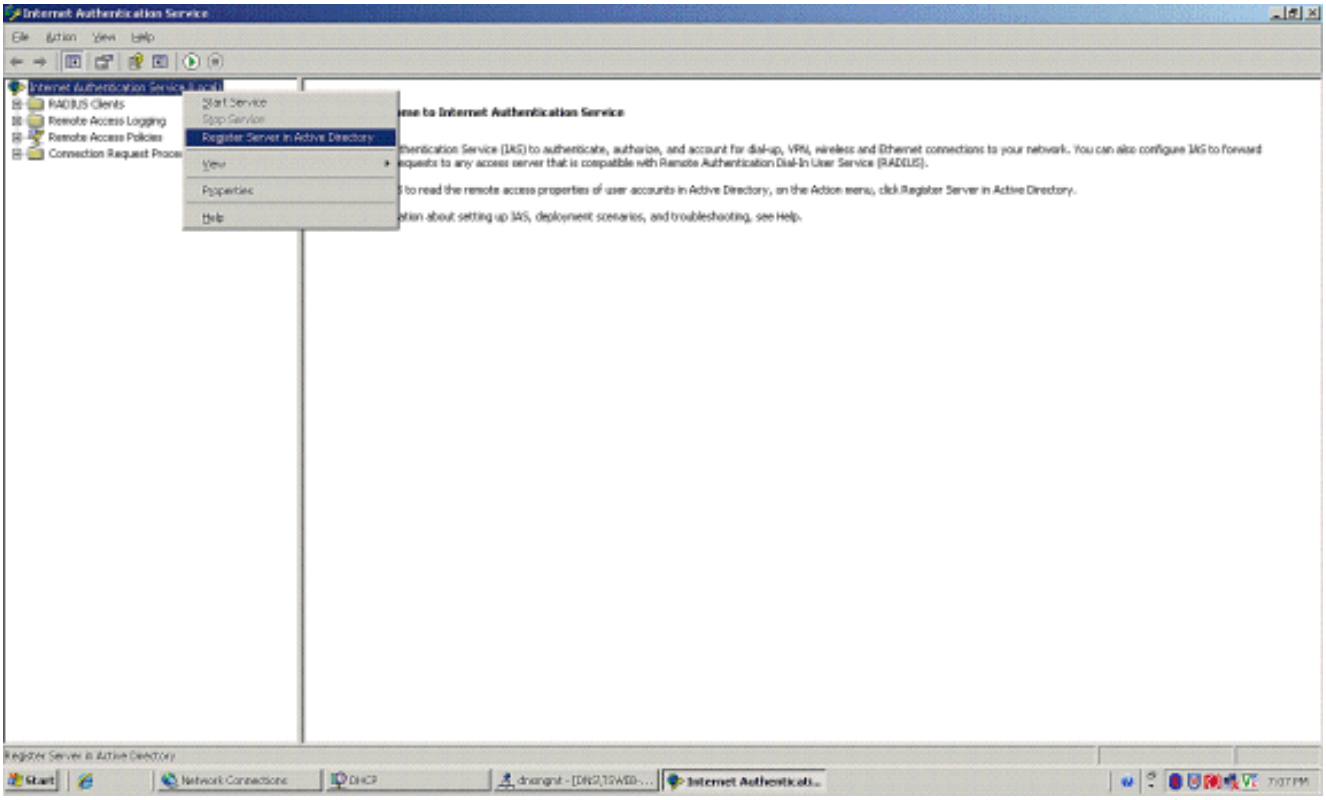


PEAP-MS-CHAP v2 인증을 위한 인터넷 인증 서비스 구성

IAS용 인증서를 설치하고 요청했으므로 인증을 위해 IAS를 구성합니다.

다음 단계를 완료하십시오.

1. **시작 > 프로그램 > 관리 도구**를 클릭하고 **인터넷 인증 서비스** 스냅인을 클릭합니다.
2. IAS(**Internet Authentication Service)를 마우스 오른쪽 단추**로 클릭한 다음 **Active Directory에서 서비스 등록을 클릭합니다**
.

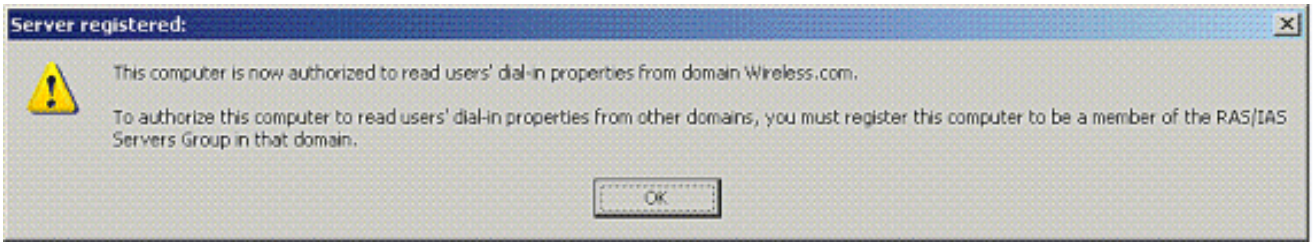


3. Register **Internet Authentication Service in Active Directory(Active Directory에 인터넷 인증 서비스 등록)** 대화 상자가 나타나고 **OK(확인)**를 클릭합니다. 이를 통해 IAS는 Active Directory에서 사용자를 인증할 수 있습니다

.

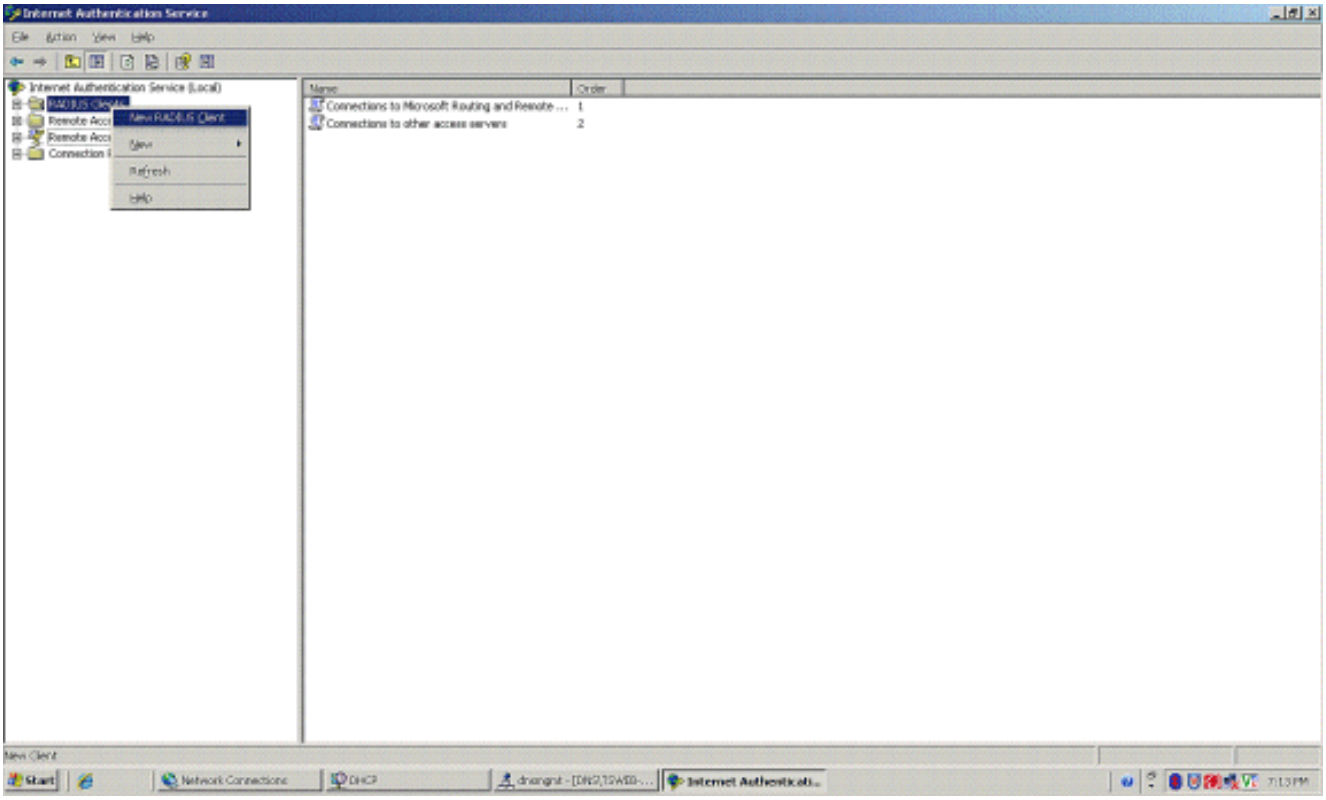
4. 다음 대화 상자에서 **OK**(확인)를 클릭합니다

.



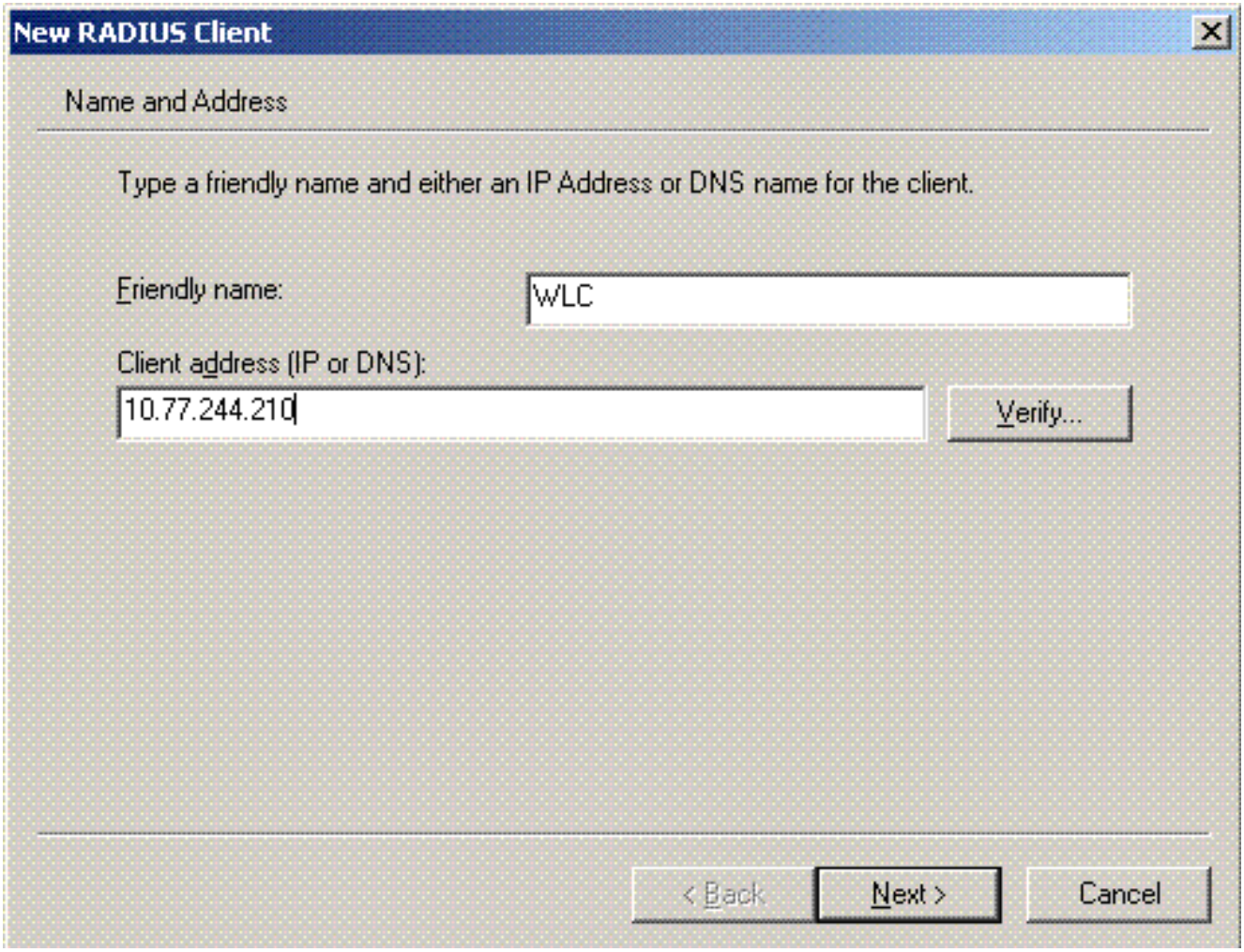
5. MS IAS 서버에서 Wireless LAN Controller를 AAA 클라이언트로 추가합니다.
6. RADIUS Clients(RADIUS 클라이언트)를 마우스 **오른쪽 버튼**으로 클릭하고 **New RADIUS Client(새 RADIUS 클라이언트)를** 선택합니다

.



7. 클라이언트의 이름(이 경우 WLC)을 입력하고 WLC의 IP 주소를 입력합니다. **Next(다음)**를 클릭합니다

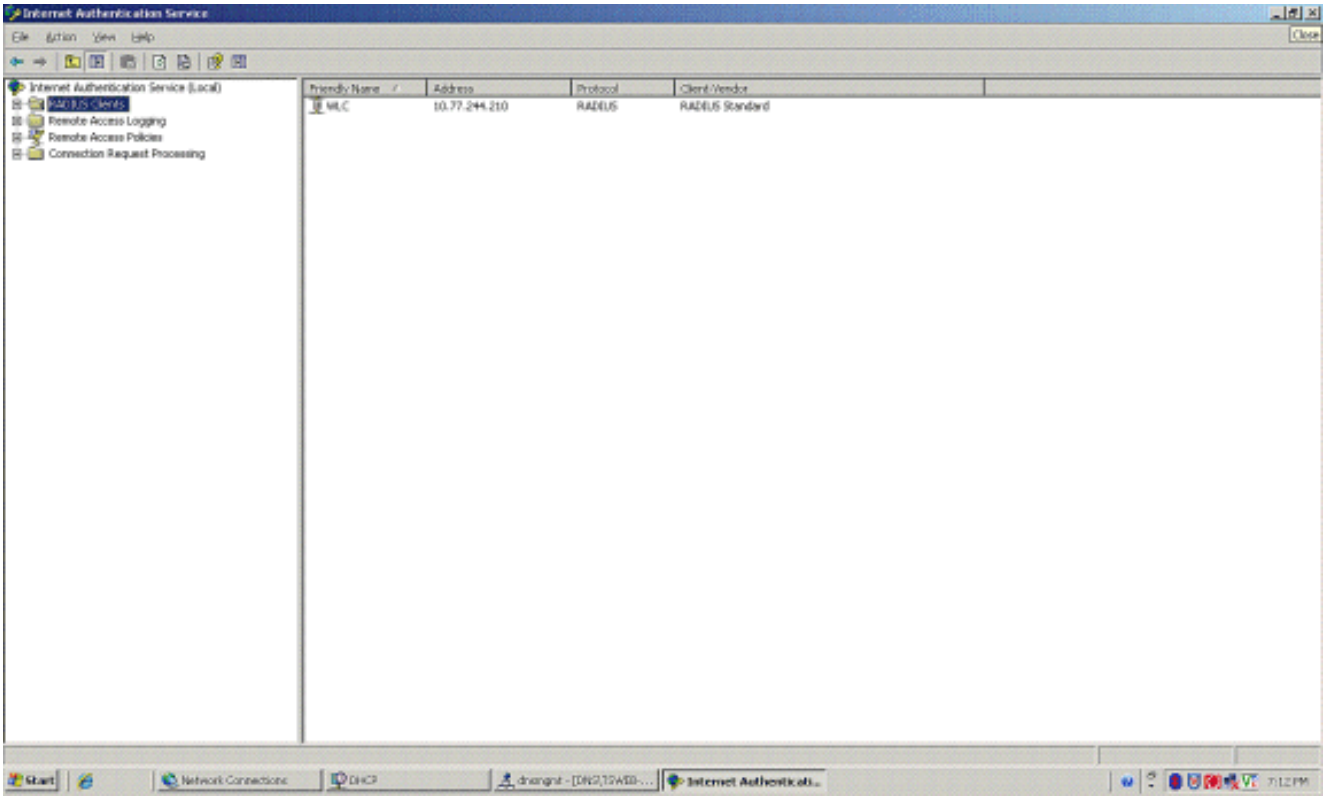
.



8. 다음 페이지의 Client-Vendor(클라이언트 벤더)에서 RADIUS Standard(**RADIUS 표준)**를 선택하고 공유 암호를 입력한 다음 Finish(마침)를 **클릭합니다**.

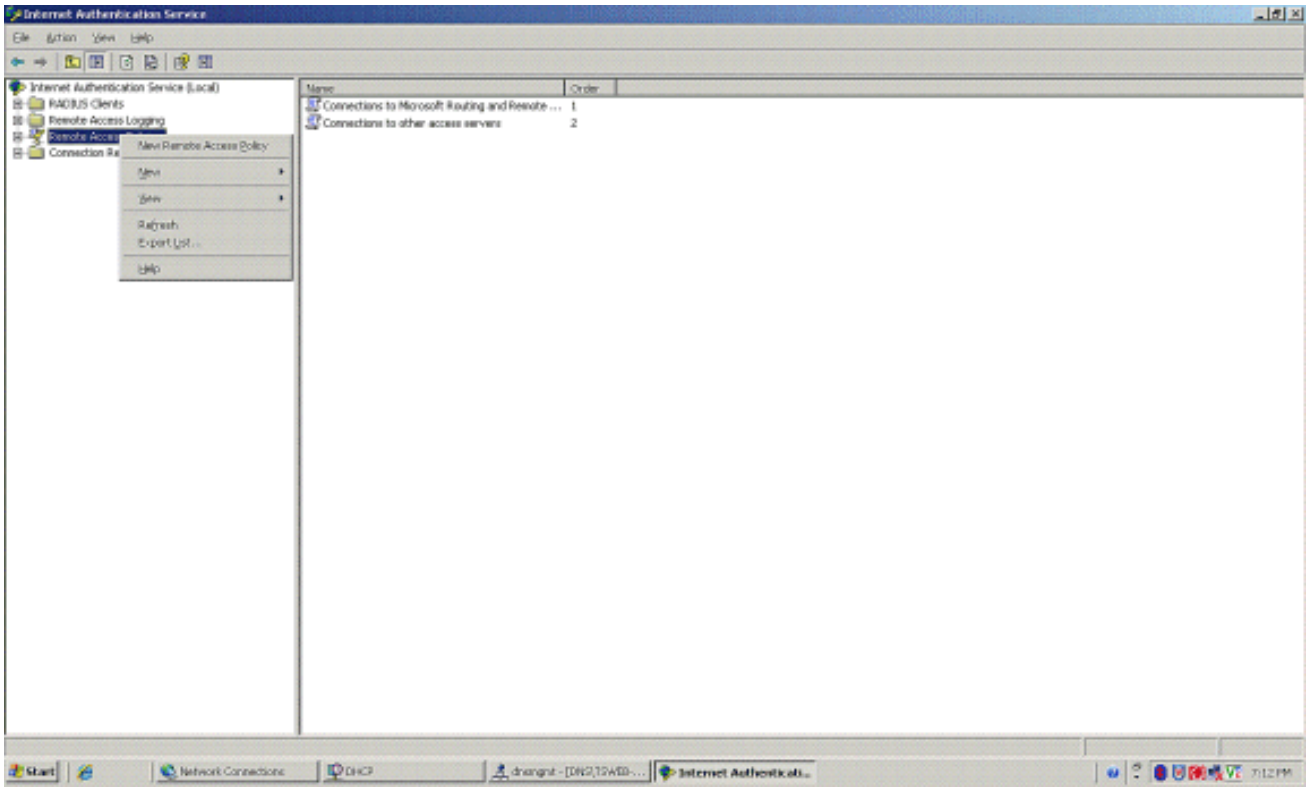
9. WLC가 IAS에서 AAA 클라이언트로 추가되었는지 확인합니다

.



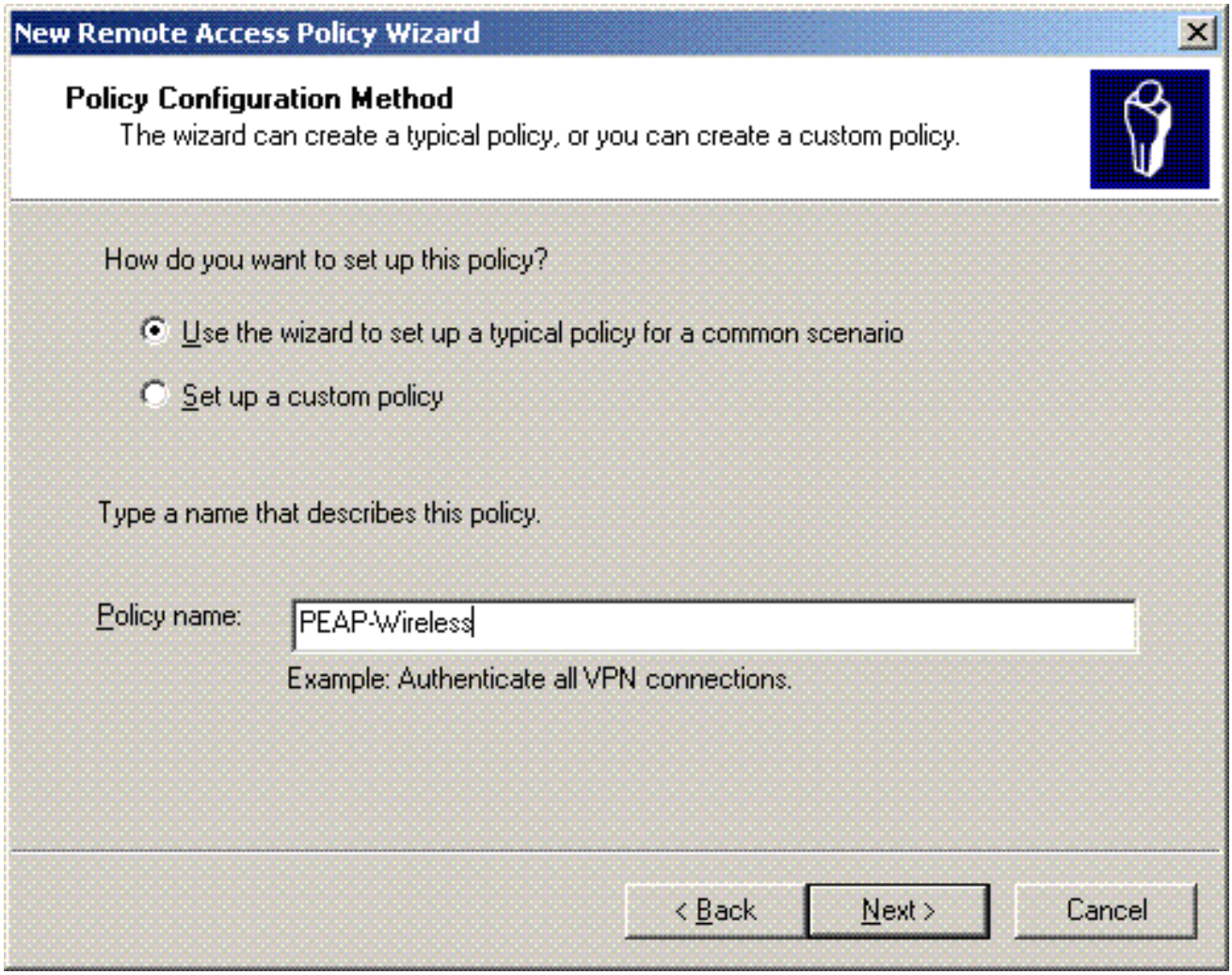
10. 클라이언트에 대한 원격 액세스 정책을 생성합니다.
11. 이렇게 하려면 Remote Access Policies(원격 액세스 정책)를 마우스 오른쪽 **버튼으로** 클릭하고 **New Remote Access Policy(새 원격 액세스 정책)**를 선택합니다

.

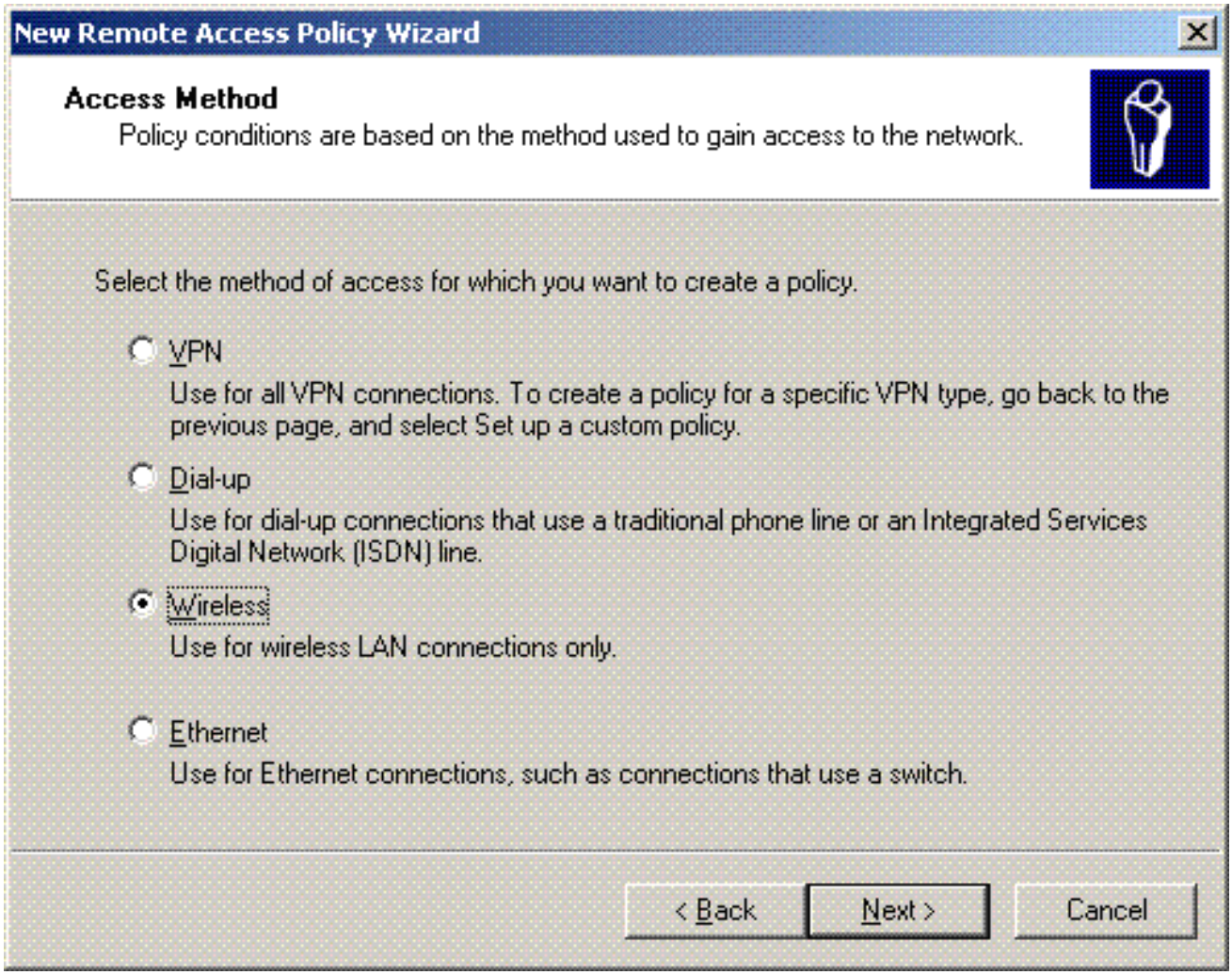


12. 원격 액세스 정책의 이름을 입력합니다. 이 예에서는 PEAP라는 이름을 **사용합니다**. 그런 다음 **Next(다음)**를 클릭합니다

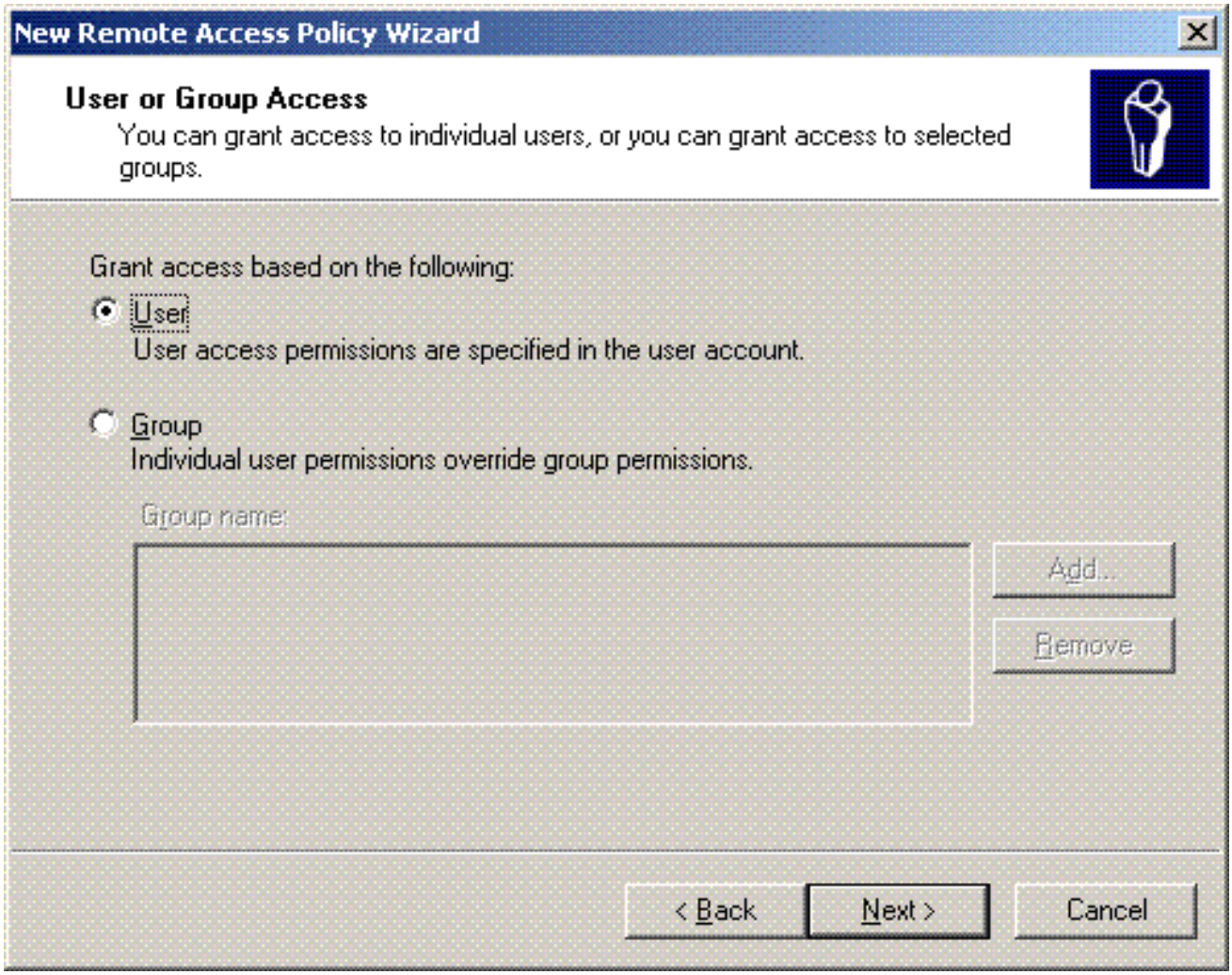
.



13. 요구 사항에 따라 정책 특성을 선택합니다. 이 예에서는 Wireless를 **선택합니다**
.

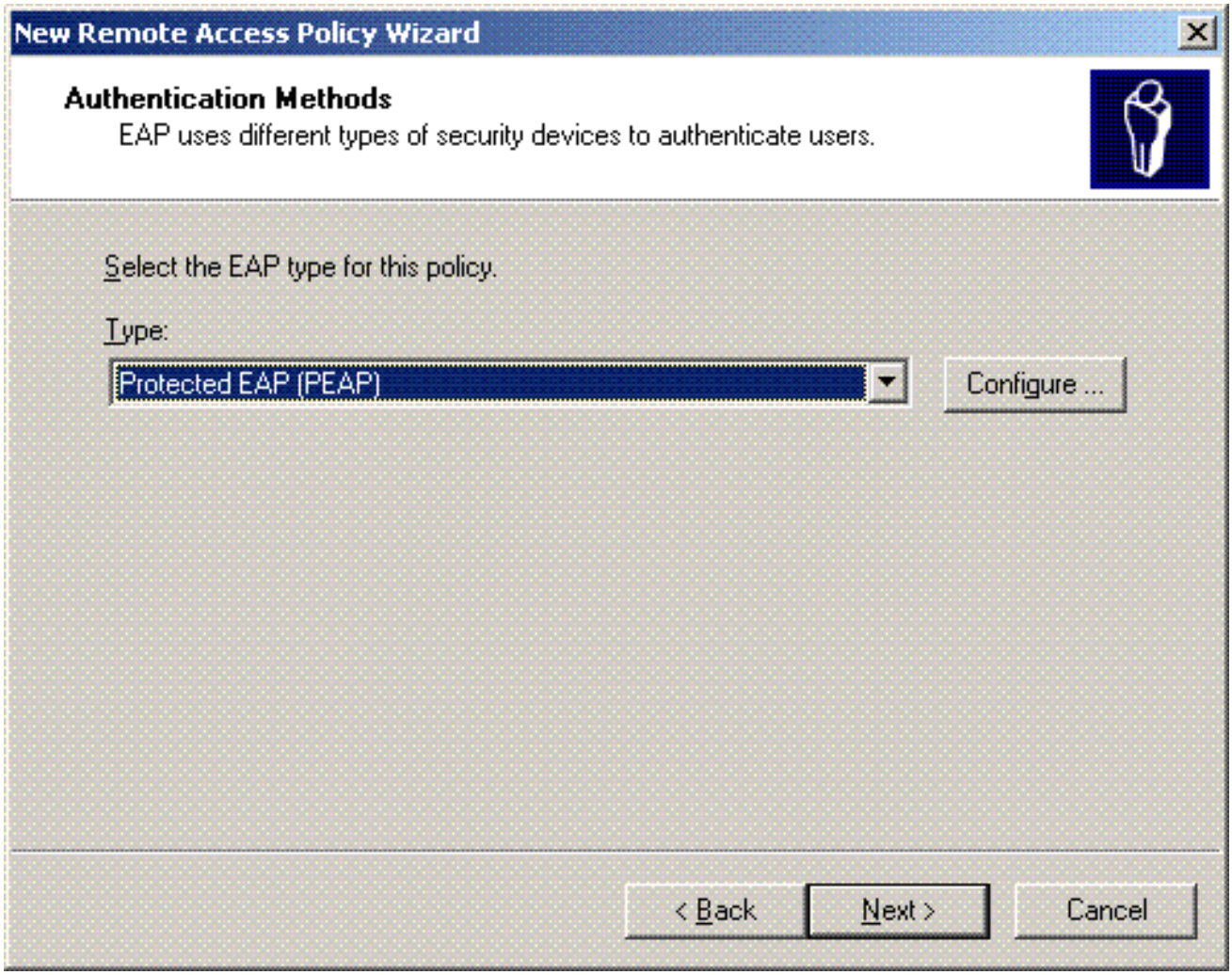


14. 다음 페이지에서 사용자를 선택하여 이 원격 액세스 정책을 사용자 목록에 적용합니다
.

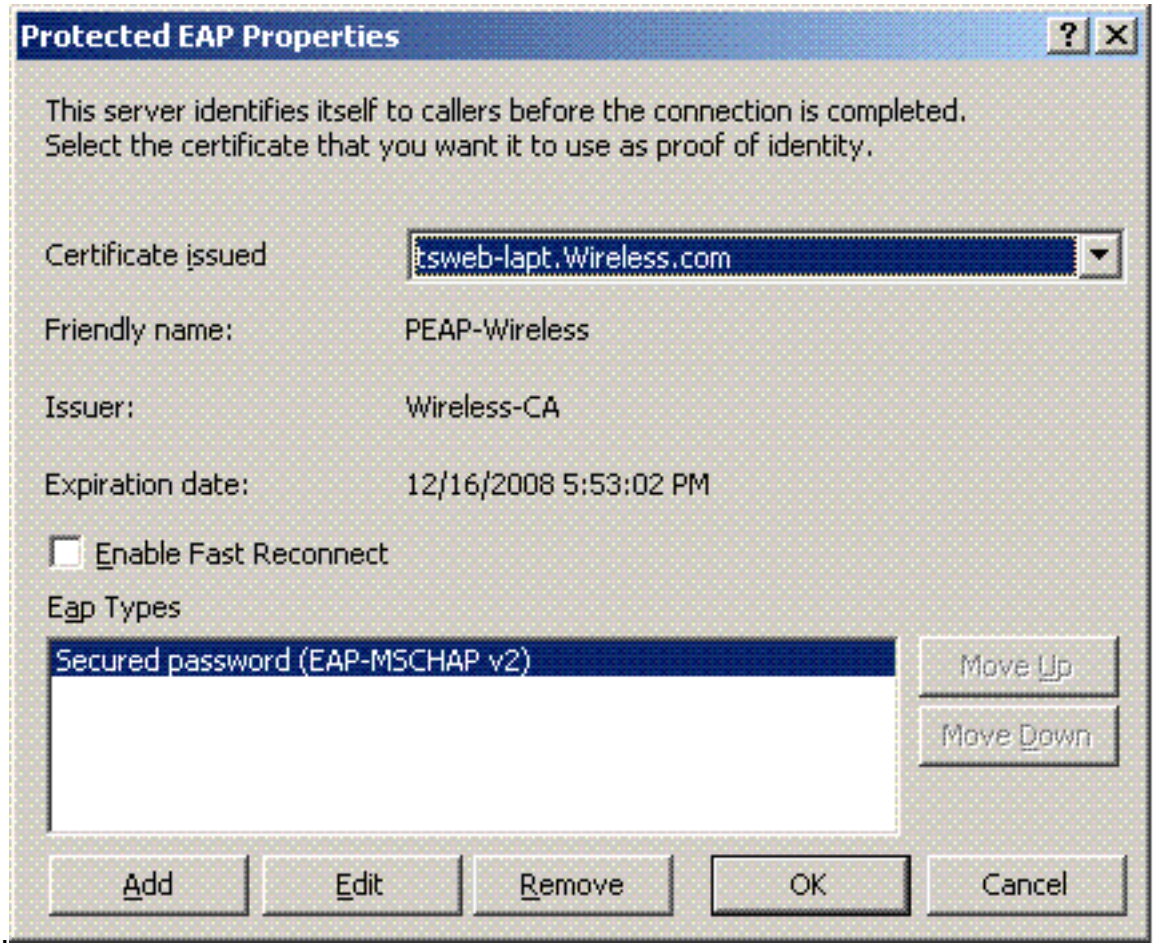


15. Authentication Methods(인증 방법)에서 PEAP**(Protected EAP)**를 선택하고 Configure(**구성**)를 클릭합니다

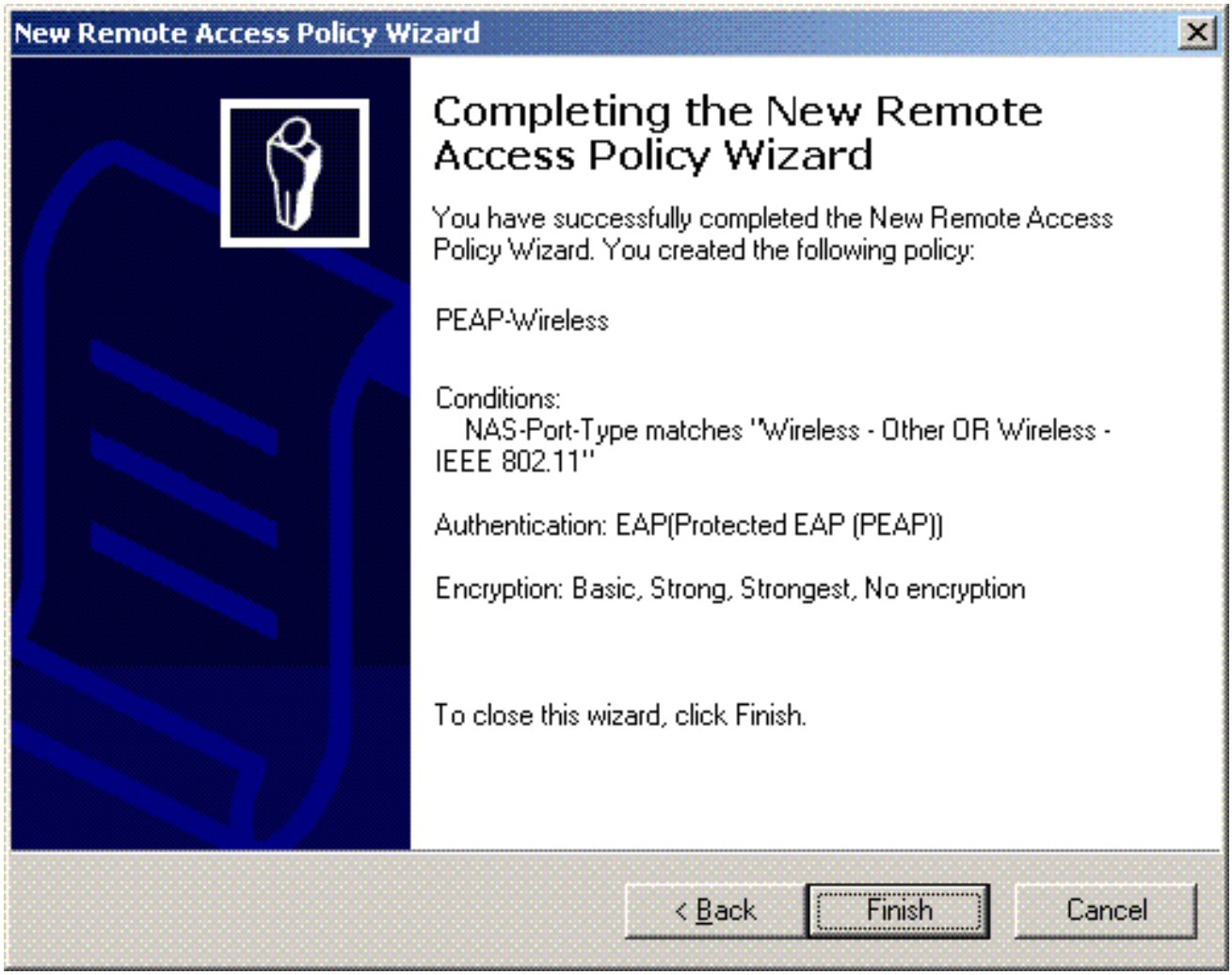
.



16. **Protected EAP Properties(보호된 EAP 속성)** 페이지의 Certificate Issued(인증서 발급됨) 드롭다운 메뉴에서 적절한 인증서를 선택하고 **OK(확인)**를 클릭합니다

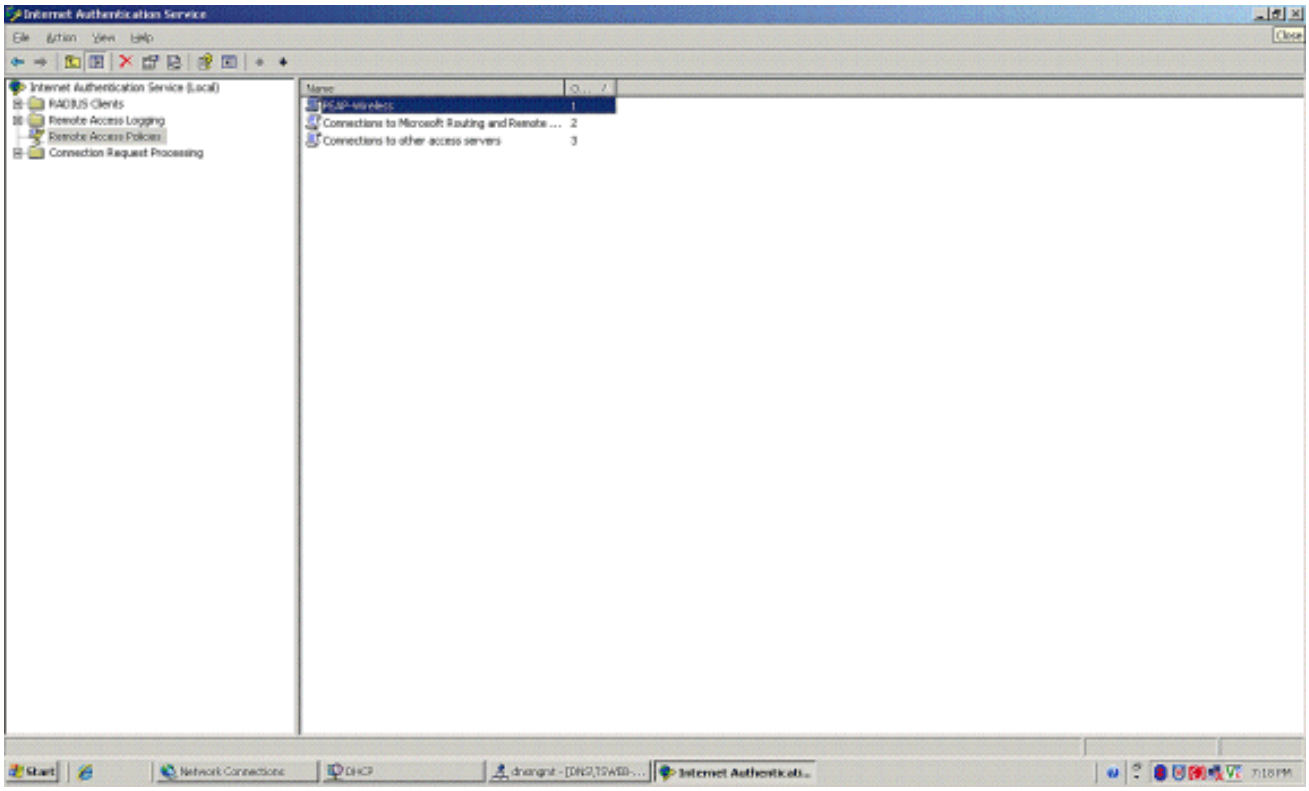


17. 원격 액세스 정책의 세부 정보를 확인하고 Finish(마침)를 **클릭합니다**

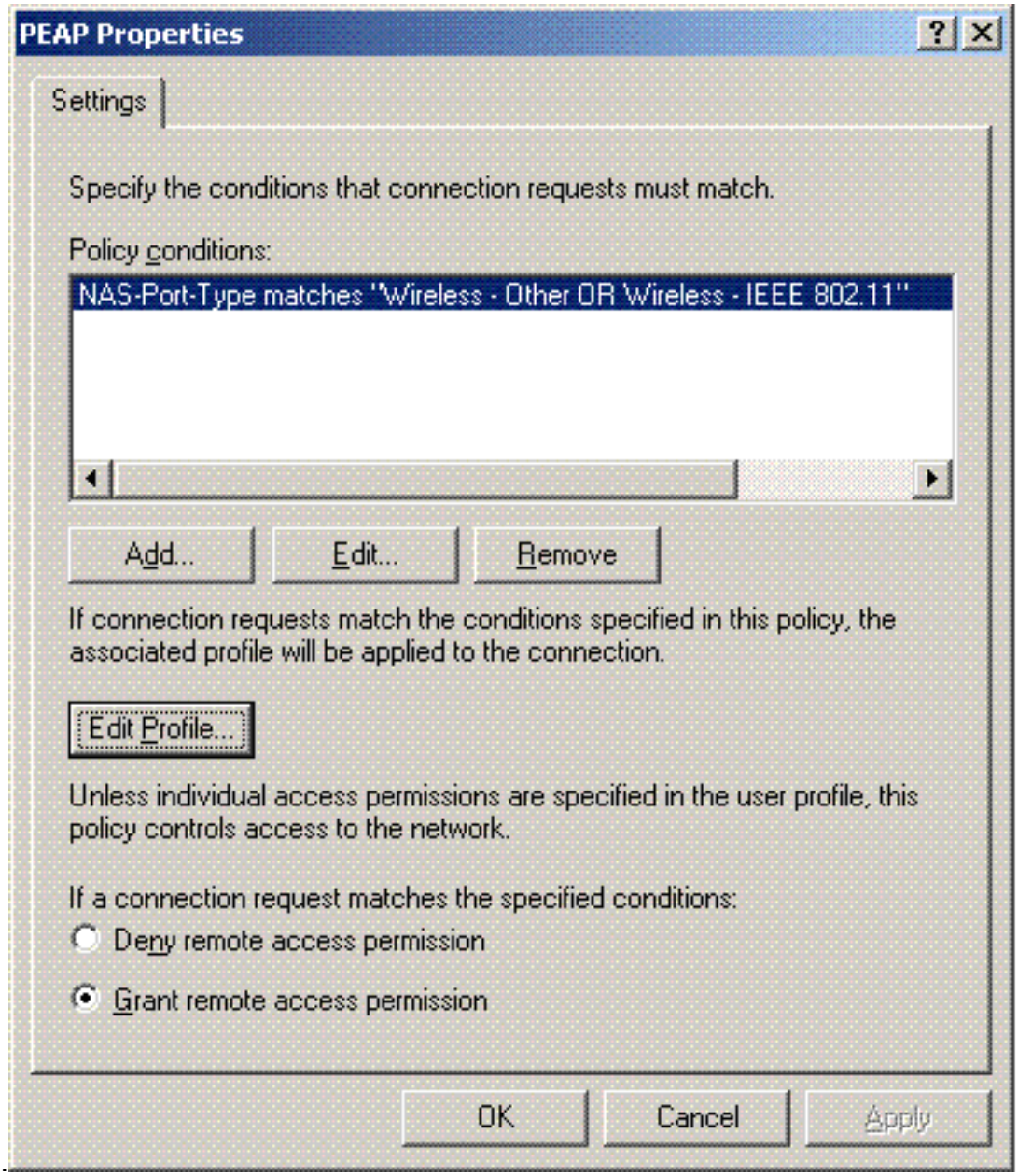


18. 원격 액세스 정책이 목록에 추가되었습니다

.



19. 정책을 마우스 오른쪽 단추로 클릭하고 속성을 **클릭합니다**. **"연결 요청이 지정된 조건**과 일치하는 **경우"에서 "원격 액세스 권한 부여"를** 선택합니다

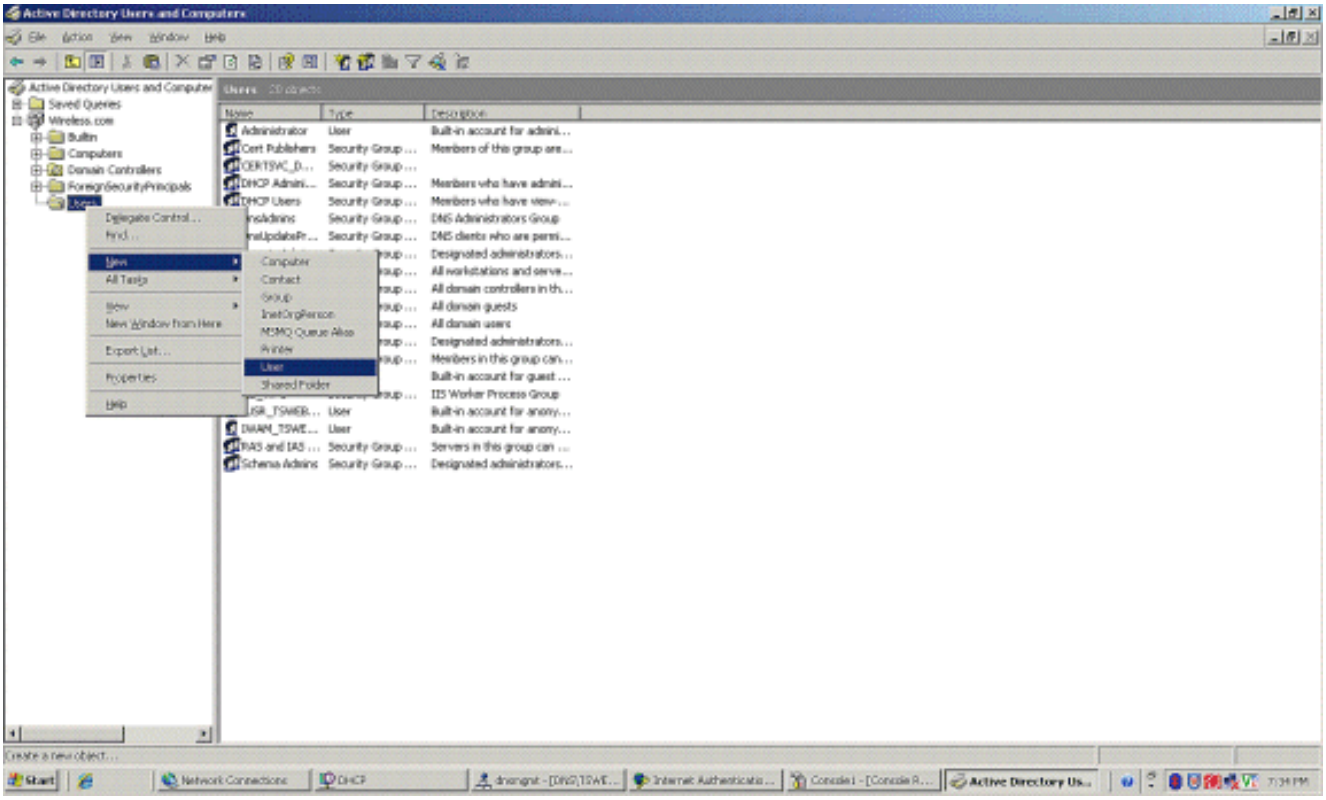


Active Directory에 사용자 추가

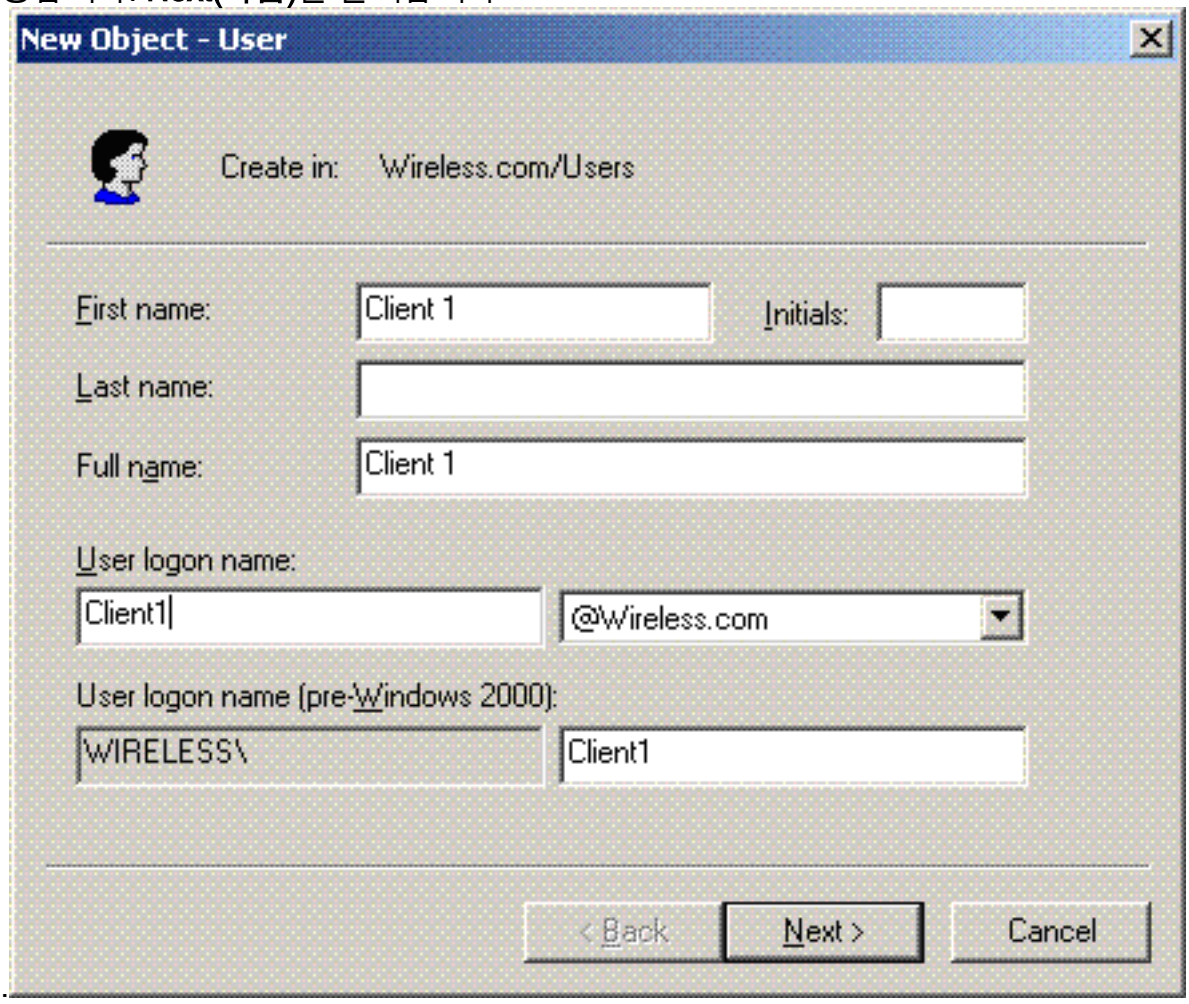
이 설정에서는 사용자 데이터베이스가 Active Directory에서 유지 관리됩니다.

Active Directory 데이터베이스에 사용자를 추가하려면 다음 단계를 완료하십시오.

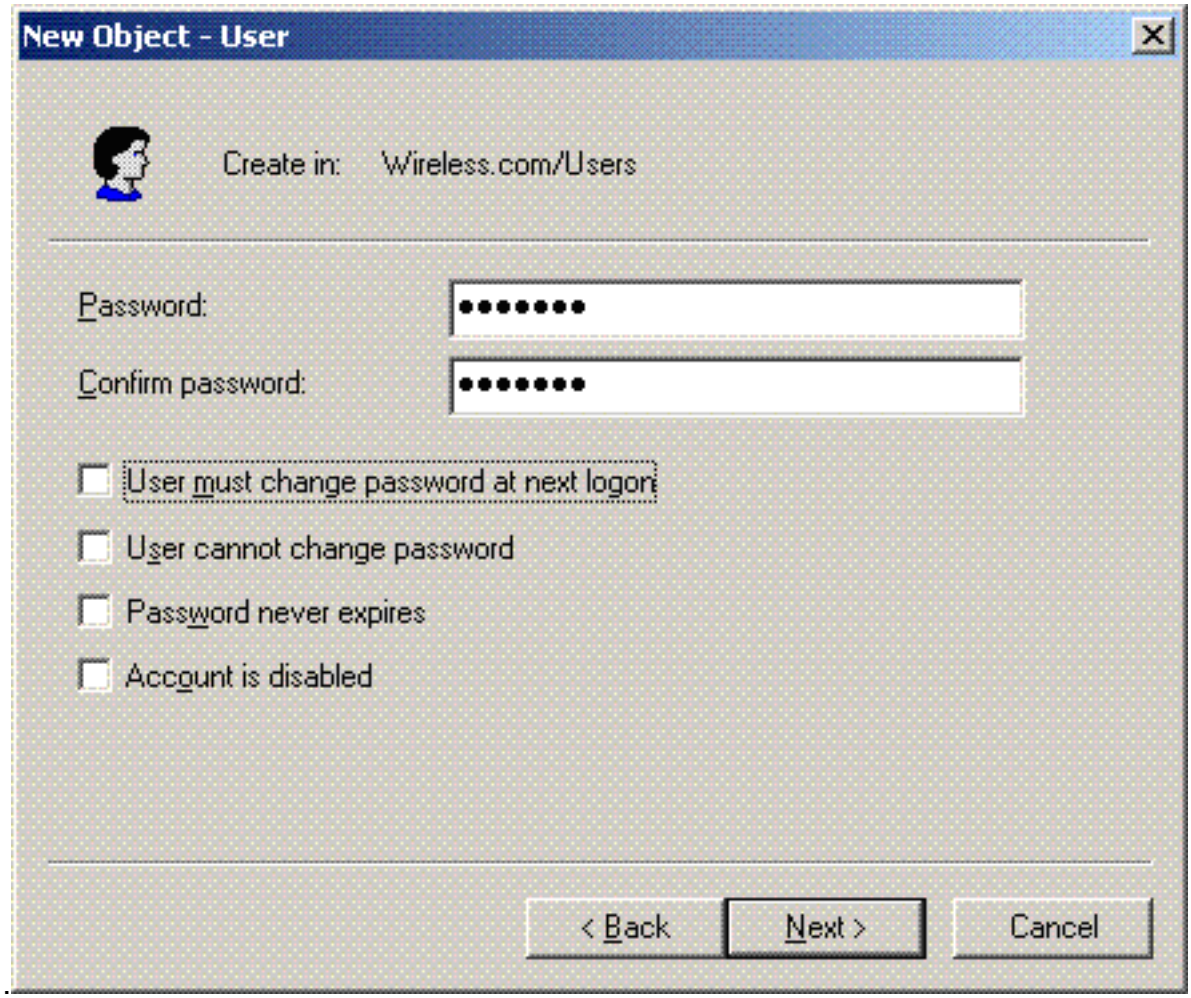
1. Active Directory 사용자 및 컴퓨터 콘솔 트리에서 사용자를 마우스 오른쪽 단추로 클릭하고 **새로 만들기**를 클릭한 다음 **사용자**를 **클릭합니다**
.



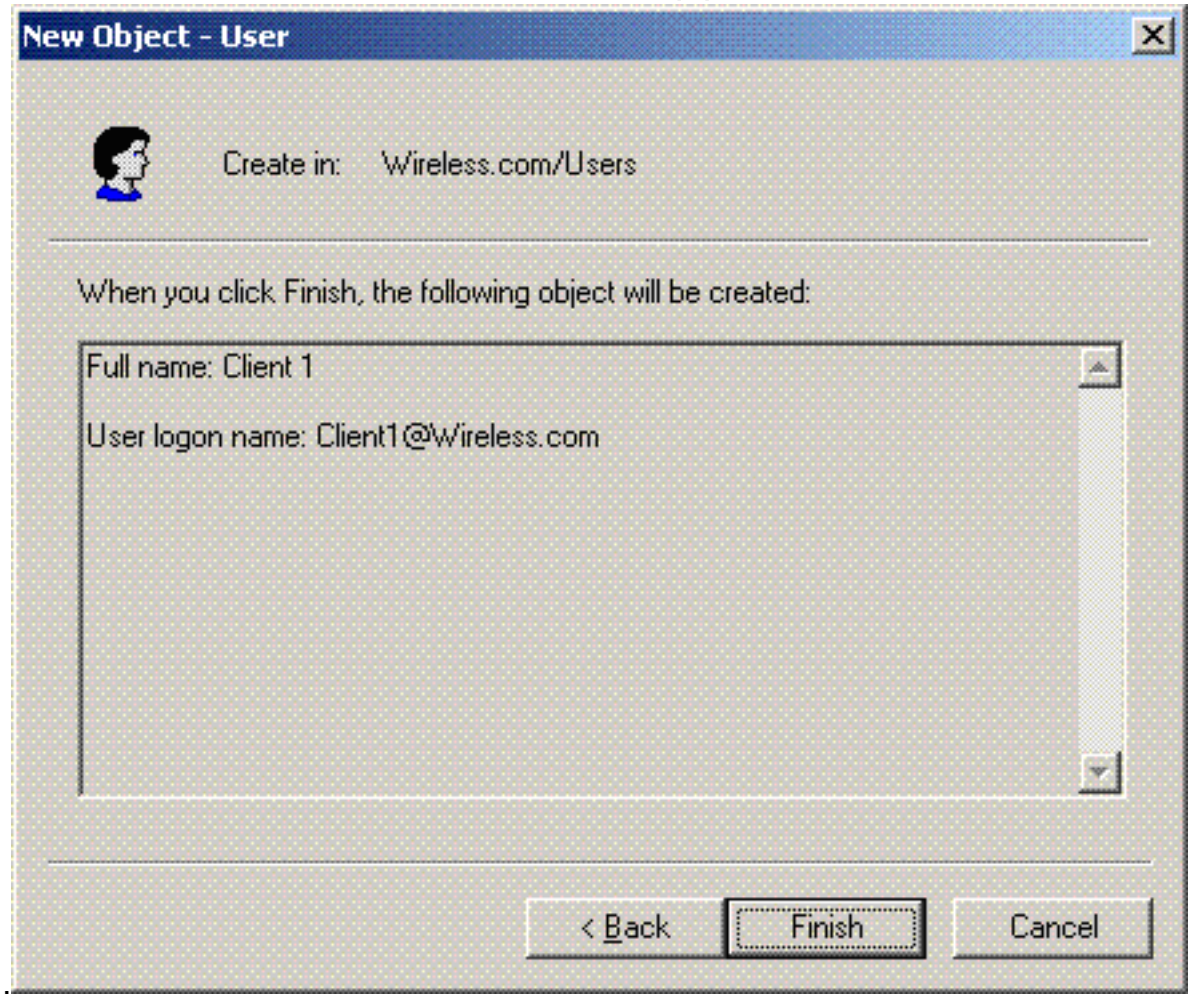
2. 새 개체 - 사용자 대화 상자에서 무선 사용자의 이름을 입력합니다. 이 예에서는 이름 필드에 **WirelessUser**라는 이름을 사용하고 사용자 로그온 이름 **필드**에 WirelessUser라는 이름을 사용합니다. **Next(다음)**를 클릭합니다



3. New Object - User(새 개체 - 사용자) 대화 상자의 Password(비밀번호) 및 Confirm password(비밀번호 확인) 필드에 원하는 비밀번호를 입력합니다. 사용자가 **다음 로그온 시 암호를 변경해야 함 확인란**의 선택을 취소하고 **다음** 을 클릭합니다



4. 새 개체 - 사용자 대화 상자에서 마침을 **클릭합니다**

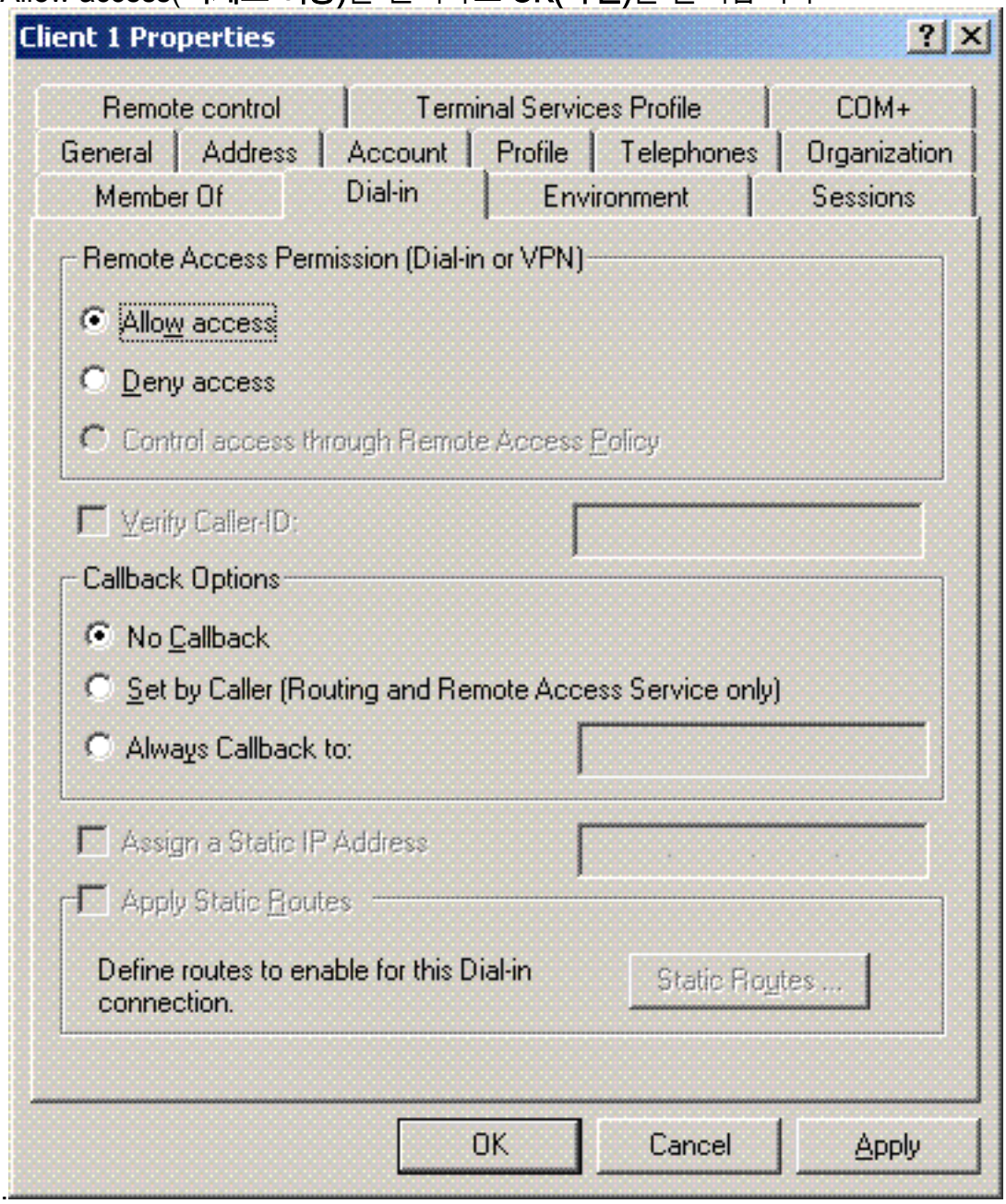


5. 추가 사용자 계정을 생성하려면 2~4단계를 반복합니다.

사용자에 대한 무선 액세스 허용

다음 단계를 완료하십시오.

1. Active Directory 사용자 및 컴퓨터 콘솔 트리에서 **Users(사용자) 폴더**를 클릭하고 **WirelessUser**를 마우스 오른쪽 단추로 클릭한 다음 **Properties(속성)를** 클릭하고 Dial-in(전화 걸기) 탭**으로 이동합니다.**
2. Allow access(**액세스 허용)**를 선택하고 **OK(확인)**를 클릭합니다



무선 LAN 컨트롤러 및 경량 AP 구성

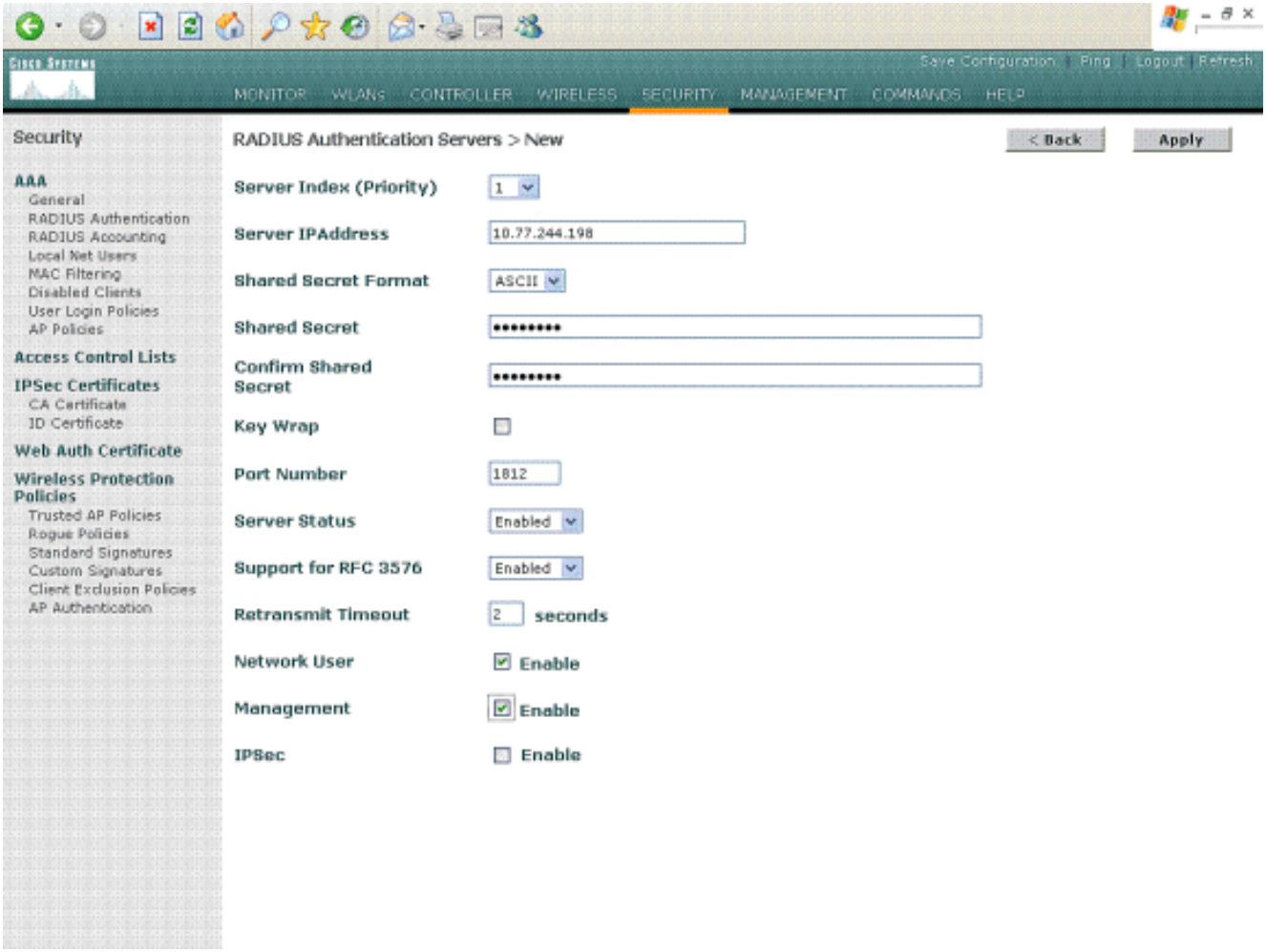
이제 이 설정에 대한 무선 장치를 구성합니다. 여기에는 무선 LAN 컨트롤러, 경량 AP 및 무선 클라이언트의 컨피그레이션이 포함됩니다.

MS IAS RADIUS 서버를 통한 RADIUS 인증을 위한 WLC 구성

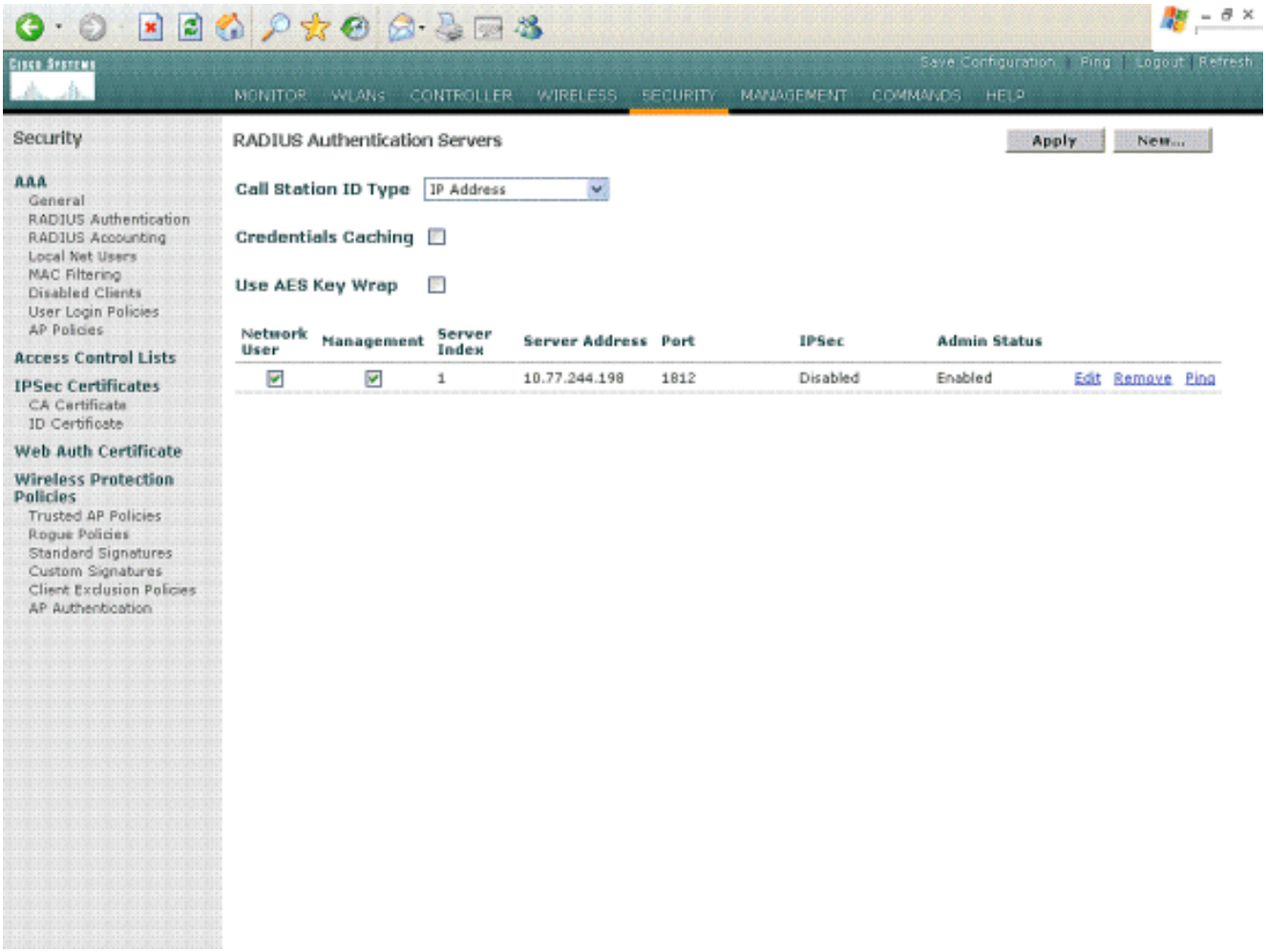
먼저 MS IAS를 인증 서버로 사용하도록 WLC를 구성합니다. 외부 RADIUS 서버에 사용자 자격 증명을 전달하려면 WLC를 구성해야 합니다. 그런 다음 외부 RADIUS 서버는 사용자 자격 증명을 확인하고 무선 클라이언트에 대한 액세스를 제공합니다. 이를 위해 **Security(보안) > RADIUS Authentication(**RADIUS 인증) 페이지에서 MS IAS **서버를 RADIUS 서버로** 추가합니다.

다음 단계를 완료하십시오.

1. 컨트롤러 GUI에서 **Security** and **RADIUS Authentication(보안** 및 RADIUS 인증)을 선택하여 RADIUS Authentication Servers(RADIUS 인증 서버) 페이지를 표시합니다. 그런 다음 **New(새로** 만들기)를 클릭하여 RADIUS 서버를 정의합니다



2. RADIUS Authentication Servers(RADIUS 인증 서버) **> New(새) 페이지에서 RADIUS 서버 매개변수를** 정의합니다. 이러한 매개변수에는 RADIUS 서버 IP 주소, 공유 암호, 포트 번호 및 서버 상태가 포함됩니다. Network User and Management(네트워크 사용자 및 관리) 확인란은 관리 및 네트워크 사용자에 대해 RADIUS 기반 인증을 적용할지 여부를 결정합니다. 이 예에서는 MS IAS를 IP 주소가 10.77.244.198인 RADIUS 서버로 사용합니다
.



3. Apply를 **클릭합니다**.
4. MS IAS 서버가 WLC에 Radius 서버로 추가되었으며 무선 클라이언트를 인증하는 데 사용할 수 있습니다.

클라이언트에 대한 WLAN 구성

무선 클라이언트가 연결되는 SSID(WLAN)를 구성합니다. 이 예에서는 SSID를 생성하고 이름을 PEAP**로 지정합니다**.

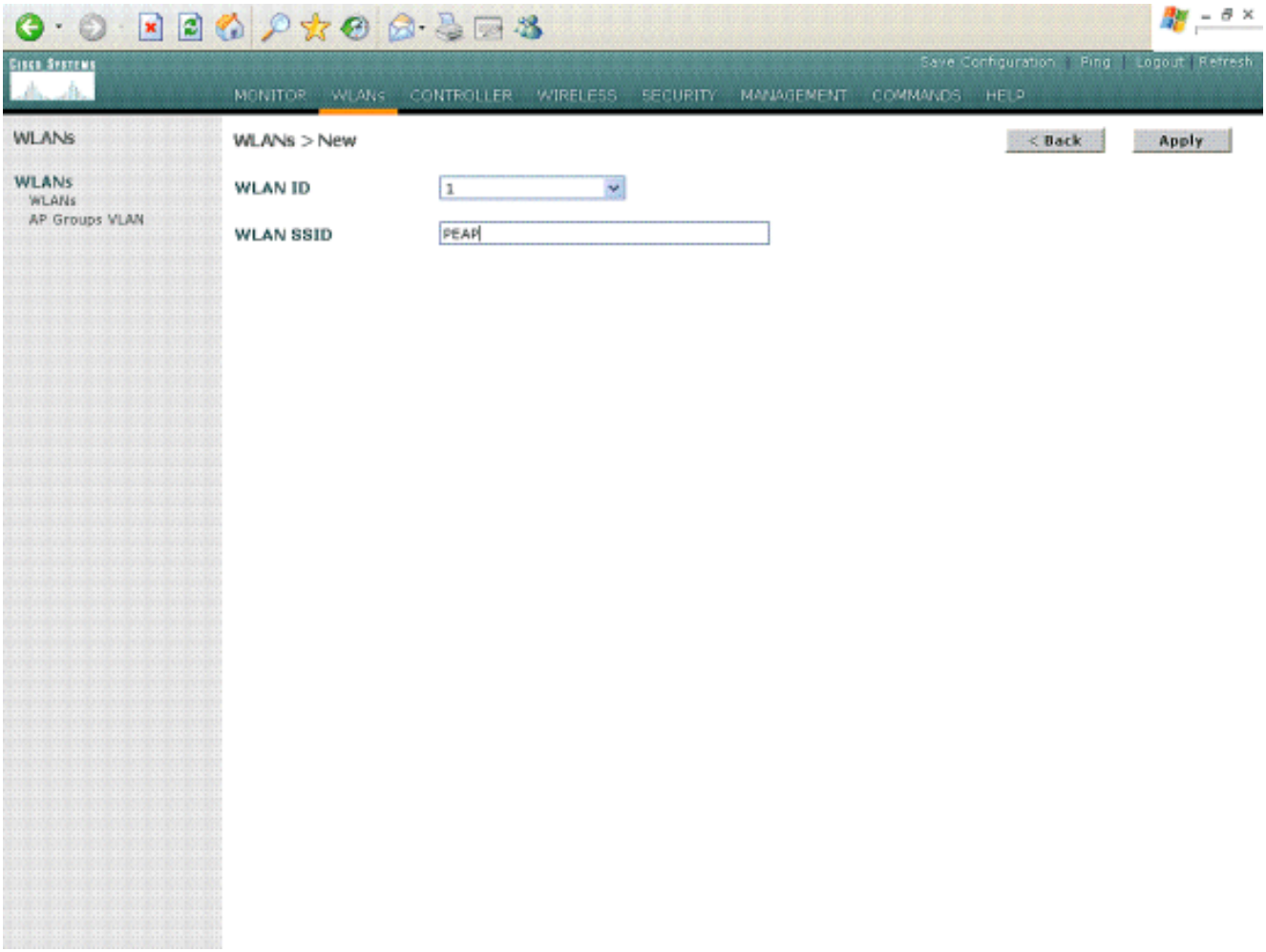
클라이언트가 EAP 기반 인증(이 경우 PEAP-MSCHAPv2)을 수행하고 암호화 메커니즘으로 AES를 사용하도록 계층 2 인증을 WPA2로 정의합니다. 다른 모든 값은 기본값으로 둡니다.

참고: 이 문서에서는 WLAN을 관리 인터페이스와 바인딩합니다. 네트워크에 여러 VLAN이 있는 경우 별도의 VLAN을 생성하여 SSID에 바인딩할 수 있습니다. WLC에 VLAN을 구성하는 방법에 대한 자세한 내용은 무선 LAN 컨트롤러 컨피그레이션 예의 VLAN을 참조하십시오.

WLC에서 WLAN을 구성하려면 다음 단계를 완료하십시오.

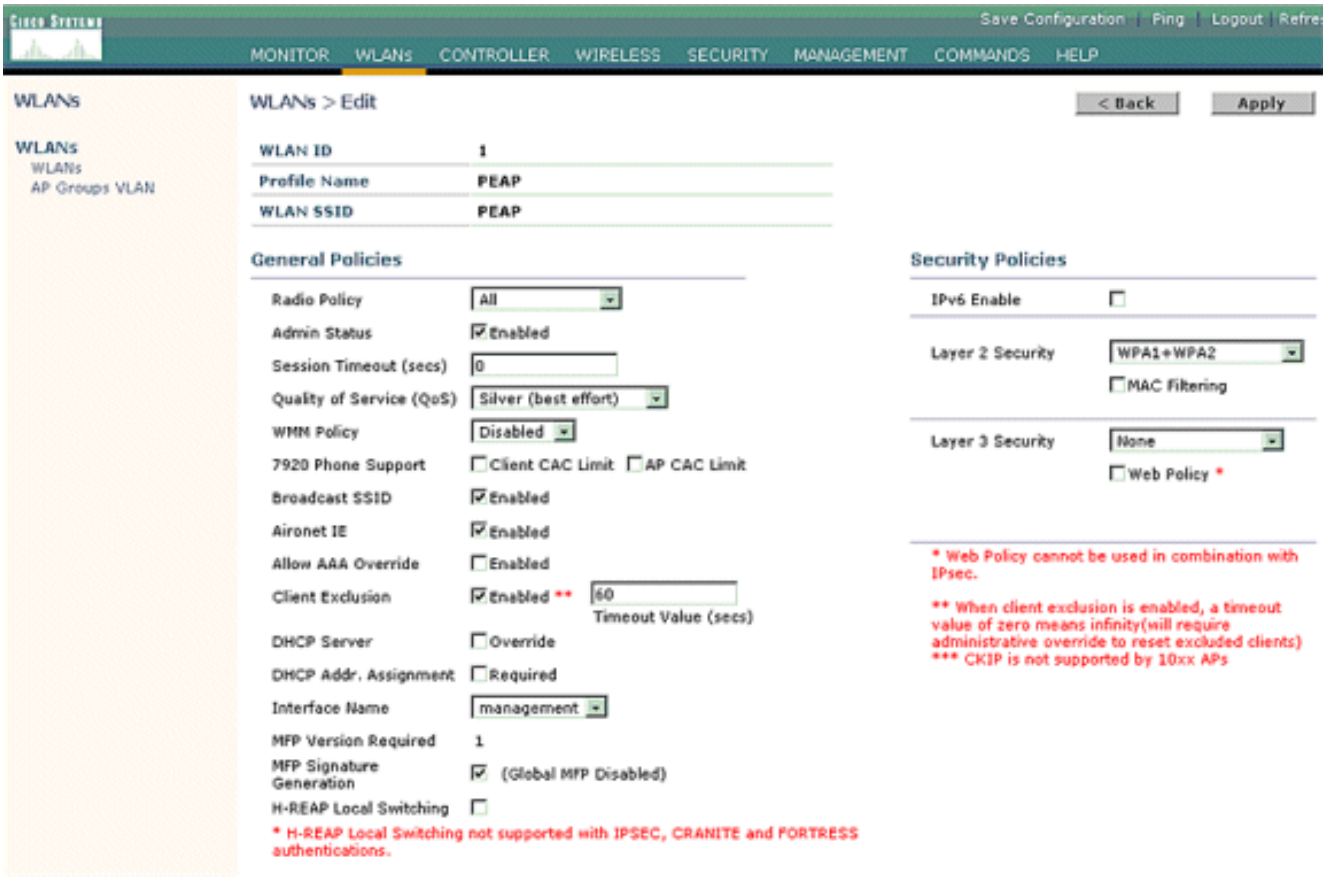
1. WLANs **페이지**를 표시하려면 컨트롤러의 GUI에서 WLANs를 클릭합니다. 이 페이지에는 컨트롤러에 있는 WLAN이 나열됩니다.
2. 새 **WLAN**을 생성하려면 New(새로 만들기)를 선택합니다. WLAN에 대한 WLAN ID 및 WLAN SSID를 입력하고 Apply를 **클릭합니다**

.



3. 새 WLAN을 생성하면 새 WLAN에 대한 **WLAN > Edit** 페이지가 나타납니다. 이 페이지에서는 일반 정책, RADIUS 서버, 보안 정책 및 802.1x 매개변수를 비롯하여 이 WLAN에 특정한 다양한 매개변수를 정의할 수 있습니다

.

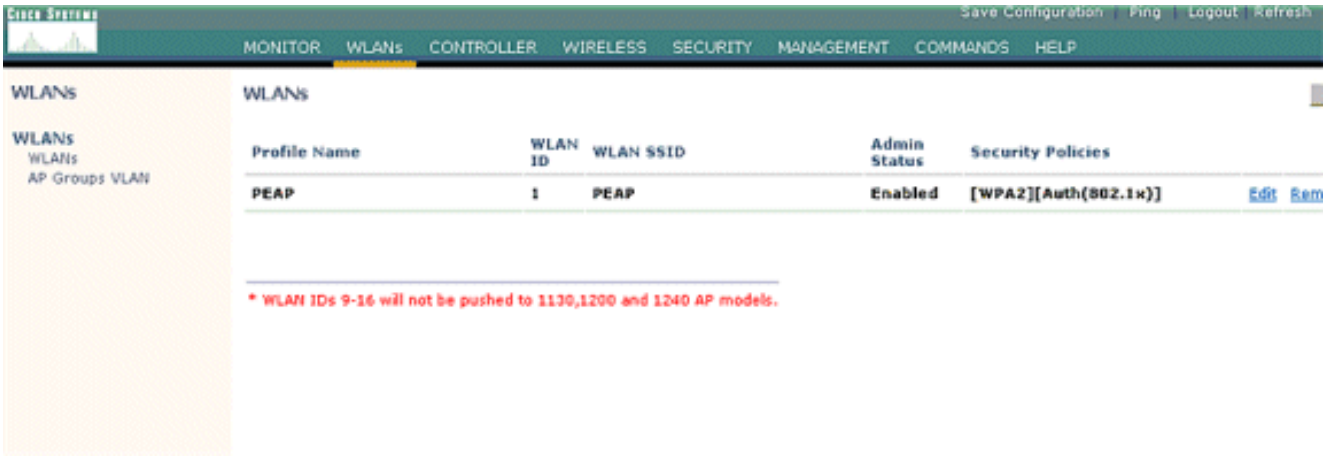


4. WLAN**을 활성화하려면** General Policies(일반 정책)에서 Admin Status(관리 상태)를 선택합니다. AP가 해당 비콘 프레임에서 SSID를 브로드캐스트하도록 하려면 Broadcast SSID**를 선택합니다**.
5. Layer 2 Security(레이어 2 보안) 아래에서 **WPA1+WPA2를** 선택합니다. 이렇게 하면 WLAN에서 WPA가 활성화됩니다. 페이지를 아래로 스크롤하여 WPA 정책을 선택합니다. 이 예에서는 WPA2 및 AES 암호화를 사용합니다. RADIUS Servers(RADIUS 서버) 아래의 풀다운 메뉴에서 적절한 RADIUS 서버를 선택합니다. 이 예에서는 **10.77.244.198**(MS IAS 서버의 IP 주소)을 사용합니다. 다른 매개변수는 WLAN 네트워크의 요구 사항에 따라 수정할 수 있습니다

.

6. Apply**를 클릭합니다**

.



무선 클라이언트 구성

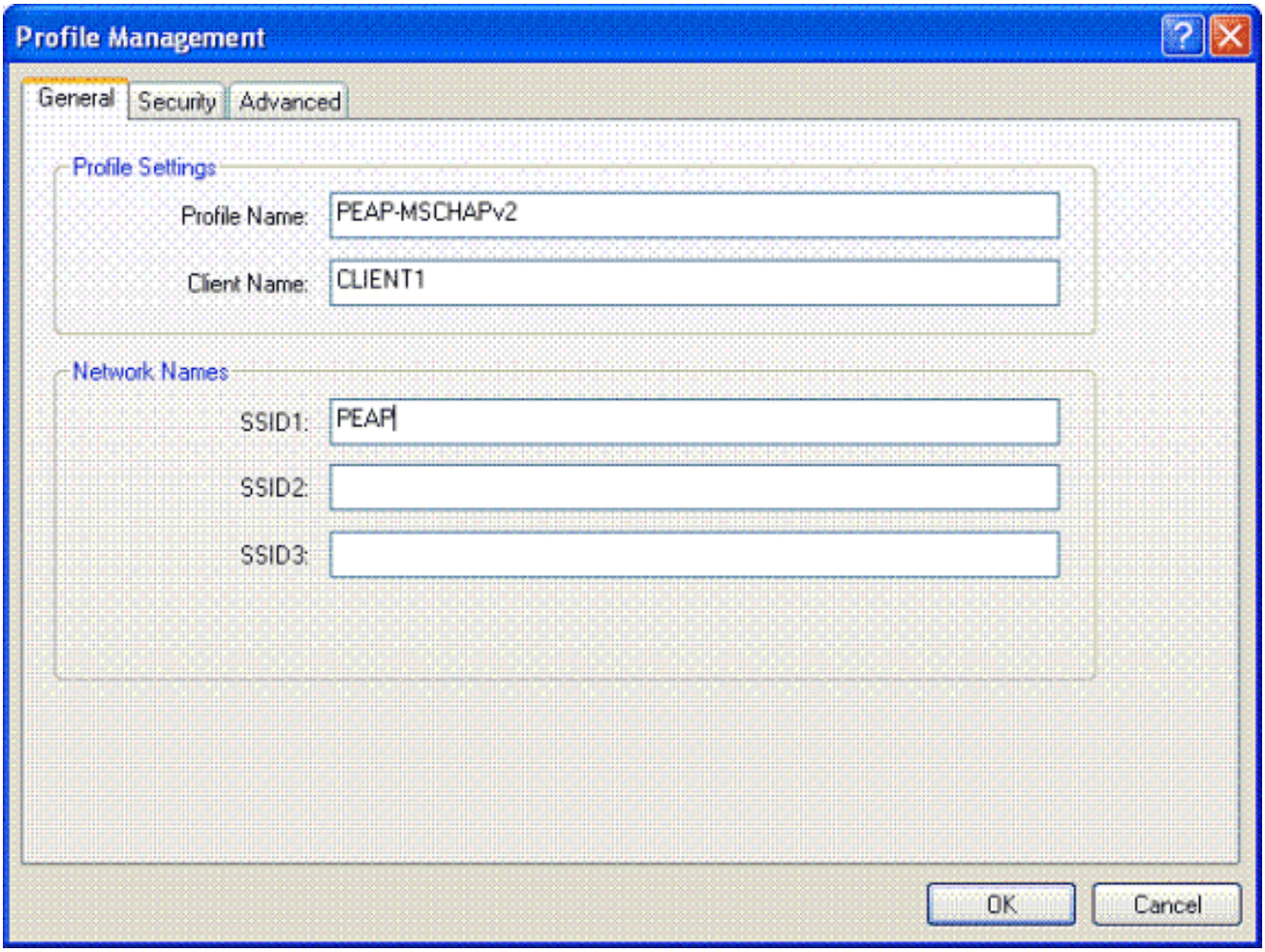
PEAP-MS CHAPv2 인증을 위한 무선 클라이언트 구성

이 예에서는 Cisco Aironet Desktop Utility를 사용하여 무선 클라이언트를 구성하는 방법에 대한 정보를 제공합니다. 클라이언트 어댑터를 구성하기 전에 최신 버전의 펌웨어 및 유틸리티가 사용되는지 확인하십시오. Cisco.com의 Wireless downloads(무선 다운로드) 페이지에서 최신 버전의 펌웨어 및 유틸리티를 찾습니다.

ADU를 사용하여 Cisco Aironet 802.11 a/b/g Wireless 클라이언트 어댑터를 구성하려면 다음 단계를 완료하십시오.

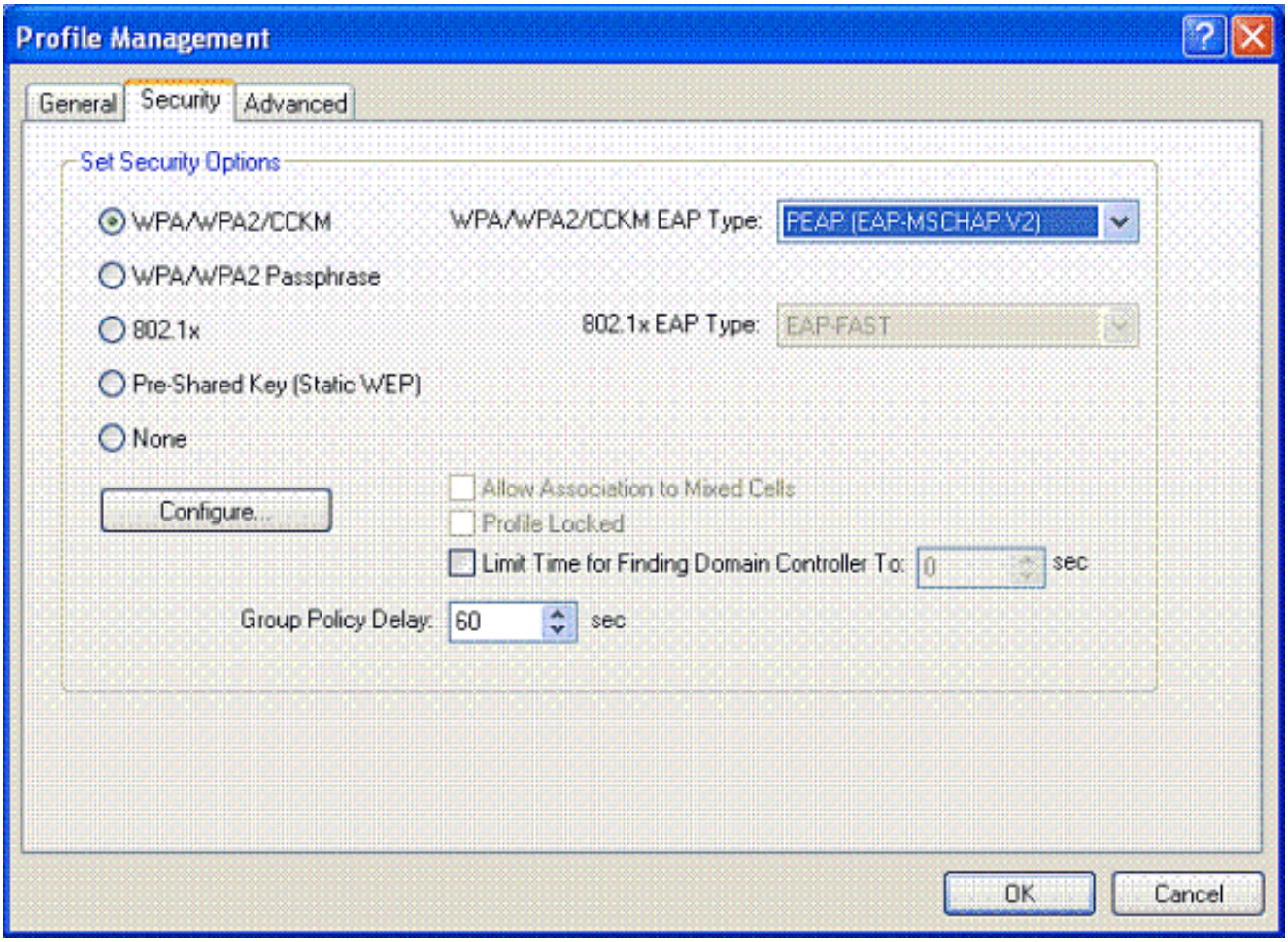
1. Aironet Desktop Utility를 엽니다.
2. 프로필 **관리를** 클릭하고 새로 만들기**를** 클릭하여 프로필을 정의합니다.
3. General(일반) 탭에서 프로파일 이름과 SSID를 입력합니다. 이 예에서는 WLC(PEAP)에서 구성한 SSID를 사용합니다

.

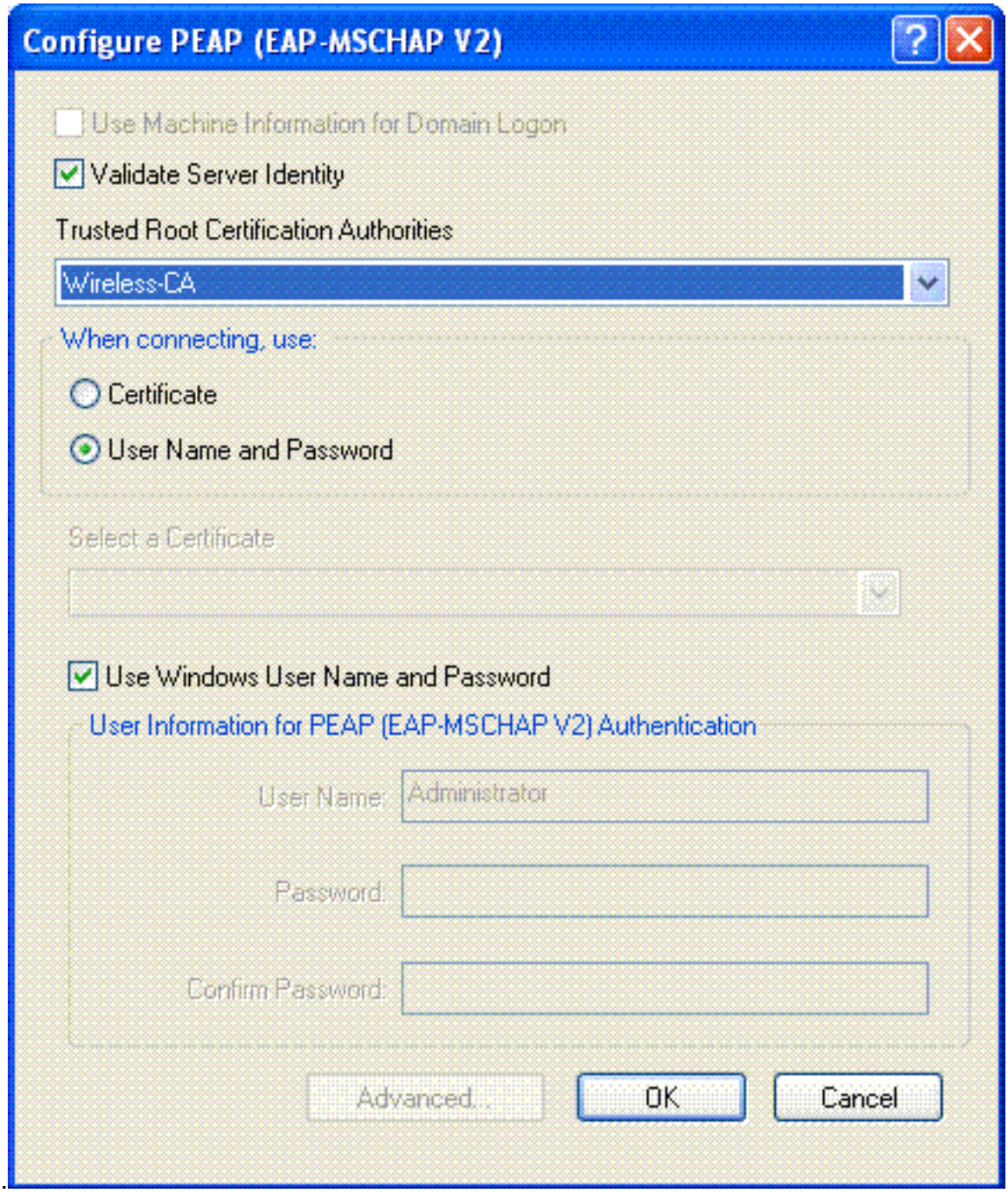


4. Security(보안) 탭을 선택하고 **WPA/WPA2/CCKM을 선택합니다.** WPA/WPA2/CCKM EAP 아래에서 PEAP **[EAP-MSCHAPv2]를** 선택하고 Configure(**구성)**를 클릭합니다

.



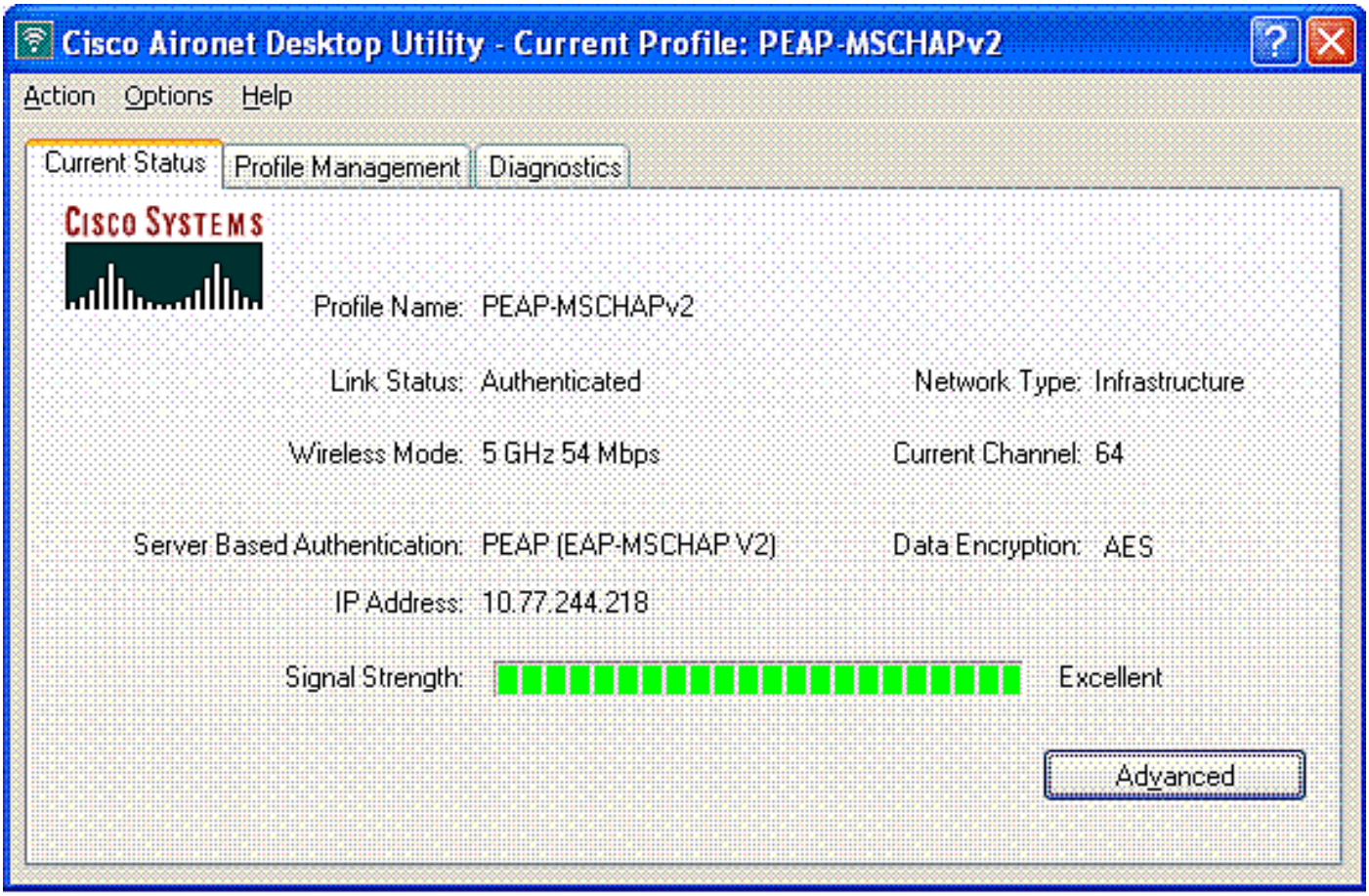
5. Validate **Server Certificate(서버 인증서 검증)**를 선택하고 Trusted Root Certificate Authorities(신뢰할 수 있는 루트 인증 기관) 드롭다운 메뉴에서 **Wireless-CA**를 선택합니다



6. **OK(확인)**를 클릭하고 프로파일을 활성화합니다.**참고:** Microsoft XP SP2에서 Protected EAP-Microsoft Challenge Handshake Authentication Protocol Version 2(PEAP-MSCHAPv2)를 사용하고 무선 카드가 Microsoft WZC(Wireless Zero Configuration)에서 관리되는 경우 Microsoft 핫픽스 KB885453을 적용해야 합니다. 이렇게 하면 PEAP 빠른 재시작과 관련된 인증에서 여러 가지 문제가 발생하지 않습니다.

확인 및 문제 해결

컨피그레이션이 정상적으로 작동하는지 확인하려면 무선 클라이언트 Client1에서 프로파일 PEAP-MSCHAPv2를 활성화합니다.



ADU에서 프로파일 PEAP-MSCHAPv2가 활성화되면 클라이언트는 802.11 개방 인증을 수행한 다음 PEAP-MSCHAPv2 인증을 수행합니다. 다음은 성공적인 PEAP-MSCHAPv2 인증의 예입니다.

debug 명령을 사용하여 발생하는 이벤트의 순서를 이해할 수 있습니다.

OIT(Output Interpreter Tool)(등록된 고객만 해당)는 특정 **show** 명령을 지원합니다. OIT를 사용하여 **show** 명령 출력 분석을 볼 수 있습니다.

Wireless LAN Controller의 이러한 디버그 명령은 유용합니다.

- **debug dot1x events enable** - 802.1x 이벤트의 디버깅을 구성하려면
- **debug aaa events enable** - AAA 이벤트의 디버깅을 구성하기 위해 사용합니다.
- **debug mac addr <mac address>** - MAC 디버깅을 구성하려면 debug mac 명령을 사용합니다
- **debug dhcp message enable** - DHCP 오류 메시지의 디버그를 구성하려면

다음은 debug dot1x events enable 명령 및 **debug client <mac address> 명령의** 출력입니다.

debug dot1x events enable:

```
Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Received EAPOL START from
   mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Sending EAP-Request/Identity to
   mobile 00:40:96:ac:e6:57 (EAP Id 2)
Tue Dec 18 06:58:45 2007: 00:40:96:ac:e6:57 Received Identity Response (count=2) from
   mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for
   mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to
   mobile 00:40:96:ac:e6:57 (EAP Id 3)
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from
```

mobile 00:40:96:ac:e6:57 (EAP Id 3, EAP Type 25)
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 4)
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 4, EAP Type 25)
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 5)
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 5, EAP Type 25)
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 6)
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 6, EAP Type 25)
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 7)
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 7, EAP Type 25)
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 8)
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 8, EAP Type 25)
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 9)
Tue Dec 18 06:58:51 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 9, EAP Type 25)
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 10)
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 10, EAP Type 25)
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 11)
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 11, EAP Type 25)
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 12)
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 12, EAP Type 25)
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Processing Access-Accept for mobile 00:40:96:ac:e6:57**
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Creating a new PMK Cache Entry for station 00:40:96:ac:e6:57 (RSN 0)**
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Sending EAP-Success to mobile 00:40:96:ac:e6:57 (EAP Id 13)**
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Sending default RC4 key to mobile 00:40:96:ac:e6:57**
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Sending Key-Mapping RC4 key to**

mobile 00:40:96:ac:e6:57
Tue Dec 18 06:58:52 2007: 00:40:96:ac:e6:57 **Received Auth Success while in Authenticating state for mobile 00:40:96:ac:e6:57**

디버그 mac 주소 <MAC 주소>:

Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Association received from mobile 00:40:96:ac:e6:57 on AP 00:0b:85:51:5a:e0**
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 STA: 00:40:96:ac:e6:57 - rates (8): 12 18 24 36 48 72 96 108 0 0 0 0 0 0 0 0
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 RUN (20) Change state to START (0)**
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 START (0) Initializing policy**
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 START (0) Change state to AUTHCHECK (2)**
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 AUTHCHECK (2) Change state to 8021X_REQD (3)**
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 10.77.244.218 8021X_REQD (3)** Plumbed mobile LWAPP rule on AP 00:0b:85:51:5a:e0
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Changing state for mobile 00:40:96:ac:e6:57 on AP 00:0b:85:51:5a:e0 from Associated to Associated**
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Stopping deletion of Mobile Station: 00:40:96:ac:e6:57 (callerId: 48)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Sending Assoc Response to station 00:40:96:ac:e6:57 on BSSID 00:0b:85:51:5a:e0 (status 0)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Changing state for mobile 00:40:96:ac:e6:57 on AP 00:0b:85:51:5a:e0 from Associated to Associated
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 10.77.244.218 Removed NPU entry.
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 dot1x - moving mobile 00:40:96:ac:e6:57 into Connecting state
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Sending EAP-Request/Identity to mobile 00:40:96:ac:e6:57 (EAP Id 1)**
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Received EAPOL START from mobile 00:40:96:ac:e6:57**
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **EAP State update from Connecting to Authenticating for mobile 00:40:96:ac:e6:57**
Wed Dec 19 02:31:49 2007: **00:40:96:ac:e6:57 dot1x - moving mobile 00:40:96:ac:e6:57 into Authenticating state**
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Entering Backend Auth Req state (id=3) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 3)**
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 **Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 3, EAP Type 25)**
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Entering Backend Auth Req state (id=4) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 4)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 4, EAP Type 25)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57 Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57

```
   Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Entering Backend Auth Req state (id=5) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 5)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 5, EAP Type 25)
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Entering Backend Auth Req state (id=6) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:49 2007: 00:40:96:ac:e6:57
   Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 6)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 9, EAP Type 25)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Entering Backend Auth Req state (id=10) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 10)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 10, EAP Type 25)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Processing Access-Challenge for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Entering Backend Auth Req state (id=11) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Sending EAP Request from AAA to mobile 00:40:96:ac:e6:57 (EAP Id 11)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Received EAP Response from mobile 00:40:96:ac:e6:57 (EAP Id 11, EAP Type 25)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Entering Backend Auth Response state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Processing Access-Accept for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Creating a new PMK Cache Entry for station 00:40:96:ac:e6:57 (RSN 0)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Sending EAP-Success to mobile 00:40:96:ac:e6:57 (EAP Id 12)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Sending default RC4 key to mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57
   Sending Key-Mapping RC4 key to mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218
   8021X_REQD (3) Change state to L2AUTHCOMPLETE (4)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218
   L2AUTHCOMPLETE (4) Plumbed mobile LWAPP rule on AP 00:0b:85:51:5a:e0
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218
   L2AUTHCOMPLETE (4) Change state to RUN (20)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
   (20) Reached PLUMBFASTPATH: from line 4041
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
   (20) Replacing Fast Path rule
  type = Airespace AP Client
  on AP 00:0b:85:51:5a:e0, slot 0, interface = 2
  ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 5006
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN (20)
  Card = 0 (slot 0), InHandle = 0x00000000,
```

```
   OutHandle = 0x00000000, npuCryptoFlag = 0x0000
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
   (20) Successfully plumbed mobile rule (ACL ID 255)
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 10.77.244.218 RUN
   (20) Reached RETURN: from line 4041
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Entering Backend
   Auth Success state (id=12) for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 Received Auth Success
   while in Authenticating state for mobile 00:40:96:ac:e6:57
Wed Dec 19 02:31:56 2007: 00:40:96:ac:e6:57 dot1x -
   moving mobile 00:40:96:ac:e6:57 into Authenticated state
```

참고: Microsoft 서플리컨트를 사용하여 PEAP 인증을 위한 Cisco Secure ACS로 인증할 경우, 클라이언트는 성공적으로 인증되지 않을 수 있습니다. 초기 연결은 성공적으로 인증될 수 있지만 이후의 빠른 연결 인증 시도는 성공적으로 연결되지 않는 경우가 있습니다. 이는 알려진 문제입니다. 이 문제에 대한 자세한 내용과 동일한 문제를 해결할 수 있는 방법은 여기에서 확인할 수 있습니다.

관련 정보

- ACS 4.0 및 Windows 2003을 사용하는 Unified Wireless Networks에서 PEAP
- WLAN 컨트롤러(WLC)를 사용한 EAP 인증 컨피그레이션 예
- 버전 3.2, 4.0, 4.1로 WLC(Wireless LAN Controller) 소프트웨어 업그레이드
- Cisco 4400 Series Wireless LAN Controller 컨피그레이션 가이드
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.