EAP-FAST 및 LDAP 서버 컨피그레이션을 사용하는 무선 LAN 컨트롤러의 로컬 EAP 인증 예

목차

소개

이 문서에서는 WLC(Wireless LAN Controller)에서 EAP(Extensible Authentication Protocol) - FAST(Flexible Authentication via Secure Tunneling) 로컬 EAP 인증을 구성하는 방법에 대해 설명합니다. 또한 이 문서에서는 로컬 EAP에서 사용자 자격 증명을 검색하고 사용자를 인증하기 위해 LDAP(Lightweight Directory Access Protocol) 서버를 백엔드 데이터베이스로 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 펌웨어 4.2를 실행하는 Cisco 4400 Series WLC
- Cisco Aironet 1232AG Series LAP(Lightweight Access Point)
- 도메인 컨트롤러, LDAP 서버 및 Certificate Authority 서버로 구성된 Microsoft Windows 2003 서버.
- 펌웨어 릴리스 4.2를 실행하는 Cisco Aironet 802.11 a/b/g Client Adapter
- 펌웨어 버전 4.2를 실행하는 Cisco Aironet Desktop Utility(ADU)

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.

배경 정보

무선 LAN 컨트롤러에 대한 로컬 EAP 인증은 무선 LAN 컨트롤러 버전 4.1.171.0에 도입되었습니다.

로컬 EAP는 사용자 및 무선 클라이언트가 컨트롤러에서 로컬로 인증될 수 있는 인증 방법입니다. 백엔드 시스템이 중단되거나 외부 인증 서버가 다운될 때 무선 클라이언트에 대한 연결을 유지하려는 원격 사무실에서 사용하도록 설계되었습니다. 로컬 EAP를 활성화하면 컨트롤러는 인증 서버 및 로컬 사용자 데이터베이스 역할을 하므로 외부 인증 서버에 대한 의존성을 제거합니다. 로컬 EAP는 사용자를 인증하기 위해 로컬 사용자 데이터베이스 또는 LDAP 백엔드 데이터베이스에서 사용자 자격 증명을 검색합니다. 로컬 EAP는 컨트롤러와 무선 클라이언트 간에 LEAP, EAP-FAST, EAP-TLS, P EAPv0/MSCHAPv2 및 PEAPv1/GTC 인증을 지원합니다.

로컬 EAP는 LDAP 서버를 백엔드 데이터베이스로 사용하여 사용자 자격 증명을 검색할 수 있습니다.

LDAP 백엔드 데이터베이스를 사용하면 컨트롤러가 특정 사용자의 자격 증명(사용자 이름 및 비밀번호)에 대해 LDAP 서버에 쿼리할 수 있습니다. 이러한 자격 증명은 사용자를 인증하는 데 사용됩니다.

LDAP 백엔드 데이터베이스는 다음과 같은 로컬 EAP 방법을 지원합니다.

- EAP-FAST/GTC
- EAP-TLS
- PEAPv1/GTC

LEAP, EAP-FAST/MSCHAPv2 및 PEAPv0/MSCHAPv2도 지원되지만 LDAP 서버**가 일반 텍스트 비밀번호를 반환하도록 설정된 경우에만 지원됩니다**. 예를 들어 Microsoft Active Directory는 일반 텍스트 비밀번호를 반환하지 않으므로 지원되지 않습니다. 일반 텍스트 비밀번호를 반환하도록 LDAP 서버를 구성할 수 없는 경우 LEAP, EAP-FAST/MSCHAPv2 및 PEAPv0/MSCHAPv2는 지원되지 않습니다.

참고: 컨트롤러에 RADIUS 서버가 구성되어 있으면 컨트롤러는 먼저 RADIUS 서버를 사용하여 무선 클라이언트를 인증하려고 시도합니다. RADIUS 서버가 시간 초과되었거나 RADIUS 서버가 구성되지 않았기 때문에 RADIUS 서버를 찾을 수 없는 경우에만 로컬 EAP가 시도됩니다. 4개의 RADIUS 서버가 구성된 경우 컨트롤러는 첫 번째 RADIUS 서버, 두 번째 RADIUS 서버, 로컬 EAP로 클라이언트를 인증하려고 시도합니다. 클라이언트가 수동으로 재인증을 시도할 경우 컨트롤러는 세 번째 RADIUS 서버, 네 번째 RADIUS 서버, 로컬 EAP를 차례로 시도합니다.

이 예에서는 WLC의 로컬 EAP 방법으로 EAP-FAST를 사용합니다. 이 방법은 LDAP 백엔드 데이터베이스에 무선 클라이언트의 사용자 자격 증명을 쿼리하도록 구성됩니다.

구성

이 문서에서는 클라이언트 및 서버 측의 인증서와 함께 EAP-FAST를 사용합니다. 이를 위해 **Microsoft CA(Certificate Authority) 서버**를 사용하여 클라이언트 및 서버 인증서를 생성합니다.

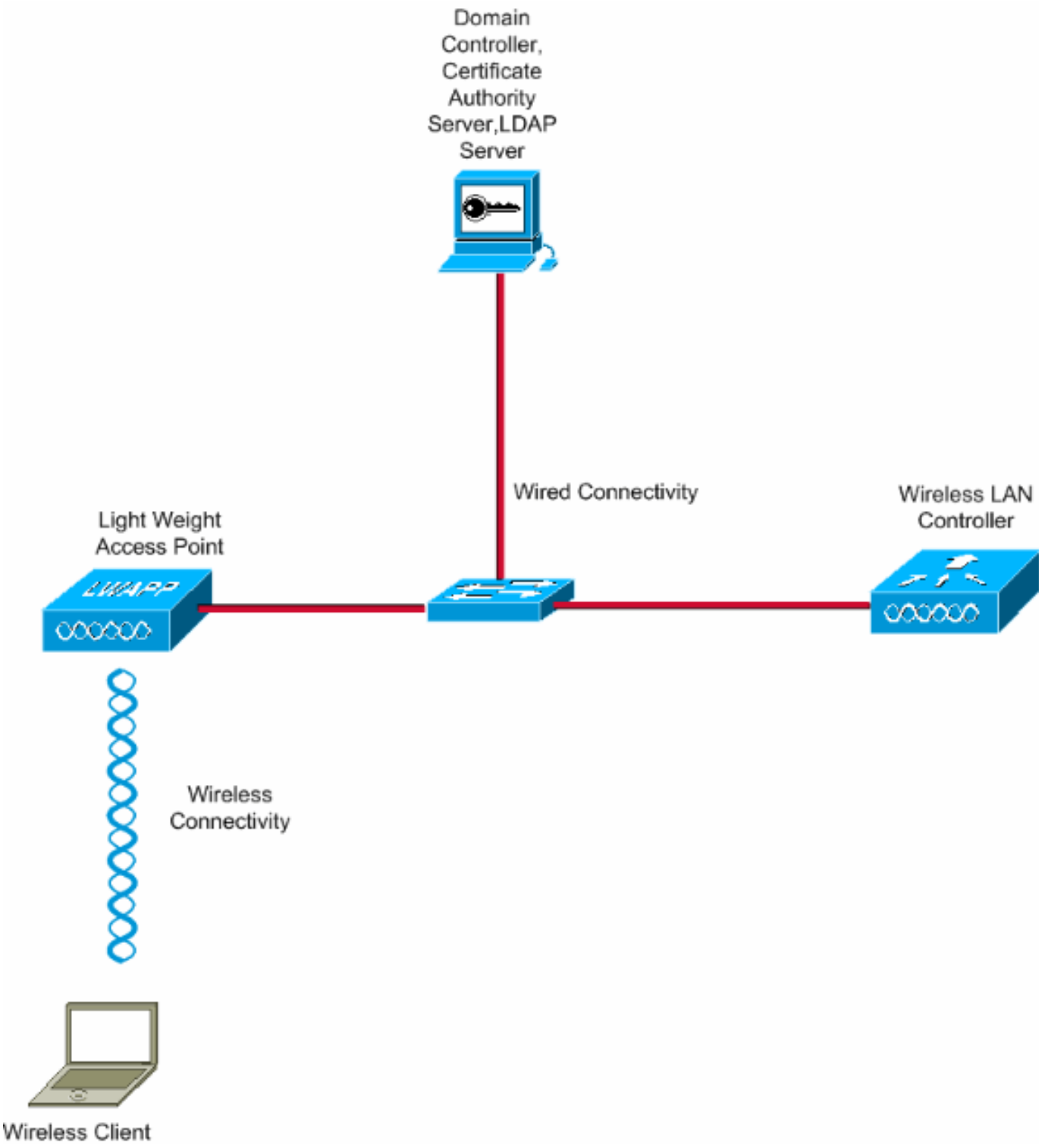
사용자 자격 증명은 LDAP 서버에 저장되므로, 인증서 검증에 성공하면 컨트롤러가 LDAP 서버를 쿼리하여 사용자 자격 증명을 검색하고 무선 클라이언트를 인증합니다.

이 문서에서는 다음 컨피그레이션이 이미 있는 것으로 가정합니다.

- LAP가 WLC에 등록됩니다. 등록 프로세스에 대한 자세한 내용은 WLC(Wireless LAN Controller)에 LAP(Lightweight AP) 등록을 참조하십시오.
- DHCP 서버는 무선 클라이언트에 IP 주소를 할당하도록 구성됩니다.
- Microsoft Windows 2003 Server는 도메인 컨트롤러와 CA 서버로 구성됩니다. 이 예에서는 **wireless.com**을 도메인으로 사용합니다.Windows 2003 서버를 도메인 컨트롤러로 구성하는 방법에 대한 자세한 내용은 Windows 2003을 도메인 컨트롤러로 구성을 참조하십시오.Windows 2003 서버를 Enterprise CA 서버로 구성하려면 Microsoft Windows 2003 Server를 CA(Certificate Authority) 서버로 설치 및 구성을 참조하십시오.

네트워크 다이어그램

이 문서에서는 이 네트워크 설정을 사용합니다.



설정

이 구성을 구현하려면 다음 단계를 완료하십시오.

- WLC에서 로컬 EAP 인증 방법으로 EAP-FAST 구성
- LDAP 서버 구성
- 무선 클라이언트 구성

WLC에서 로컬 EAP 인증 방법으로 EAP-FAST 구성

앞에서 언급한 것처럼 이 문서에서는 클라이언트 및 서버 측의 인증서가 포함된 EAP-FAST를 로컬 EAP 인증 방법으로 사용합니다. 첫 번째 단계는 다음 인증서를 다운로드하여 서버(이 경우 WLC) 및 클라이언트에 설치하는 것입니다.

WLC와 클라이언트는 각각 CA 서버에서 이러한 인증서를 다운로드해야 합니다.

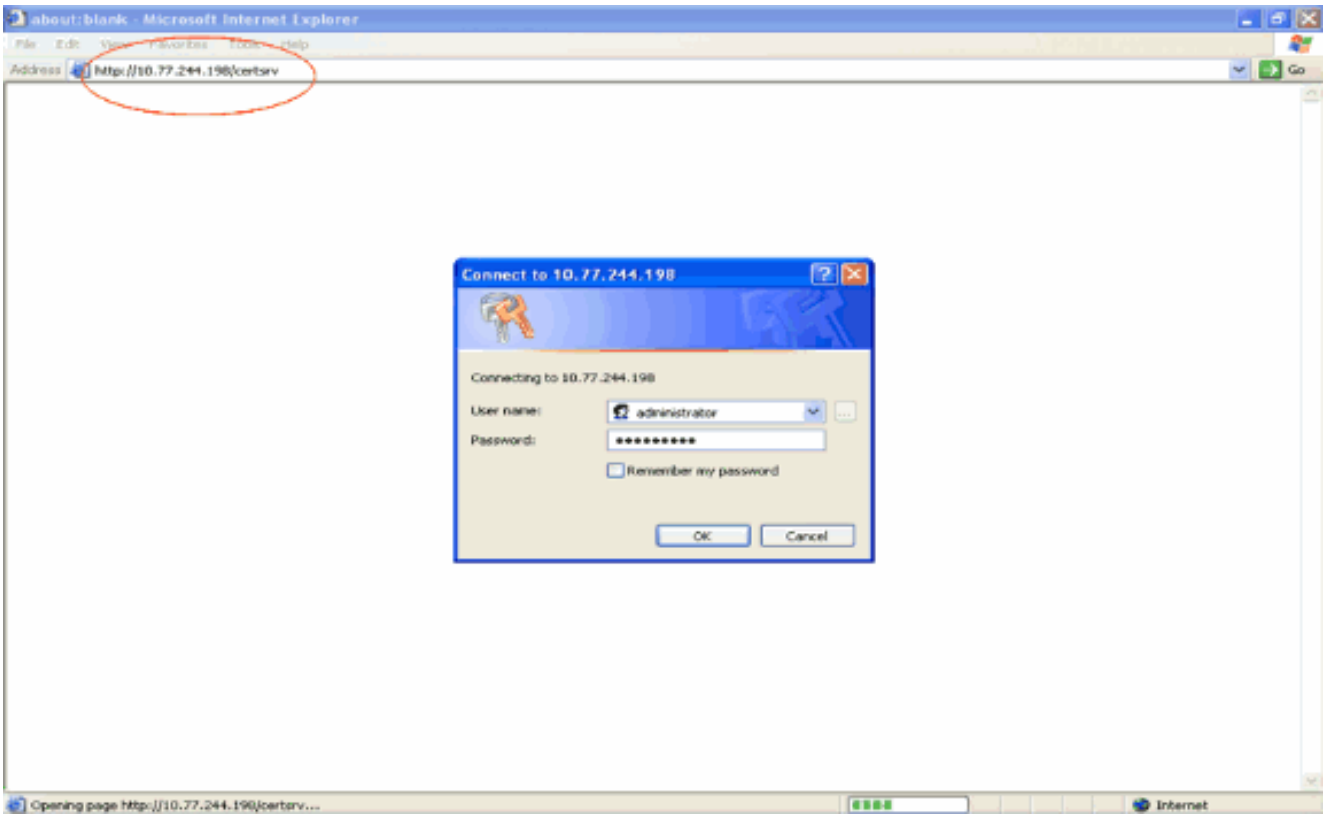
- 디바이스 인증서(WLC용 1개 및 클라이언트용 1개)
- WLC에 대한 PKI(Public Key Infrastructure)의 루트 인증서 및 클라이언트에 대한 CA 인증서

WLC에 대한 디바이스 인증서 생성

CA 서버에서 WLC에 대한 디바이스 인증서를 생성하려면 다음 단계를 수행합니다. 이 디바이스 인증서는 WLC에서 클라이언트에 인증하는 데 사용됩니다.

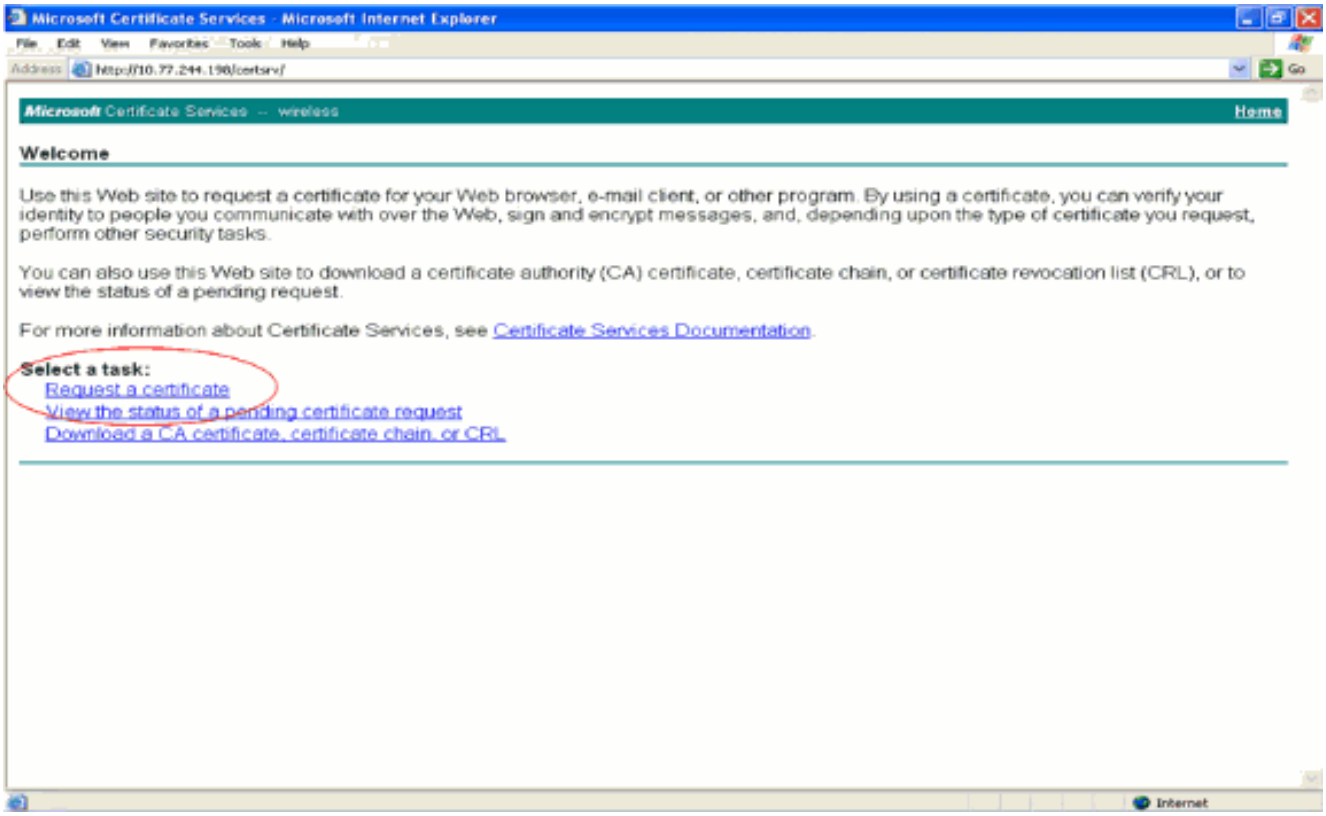
1. CA 서버**에** 대한 네트워크 **연결이 있는** PC에서 http://**<CA** 서버의 **IP 주소>/certsrv**로 이동합니다. CA 서버의 관리자로 로그인합니다

.



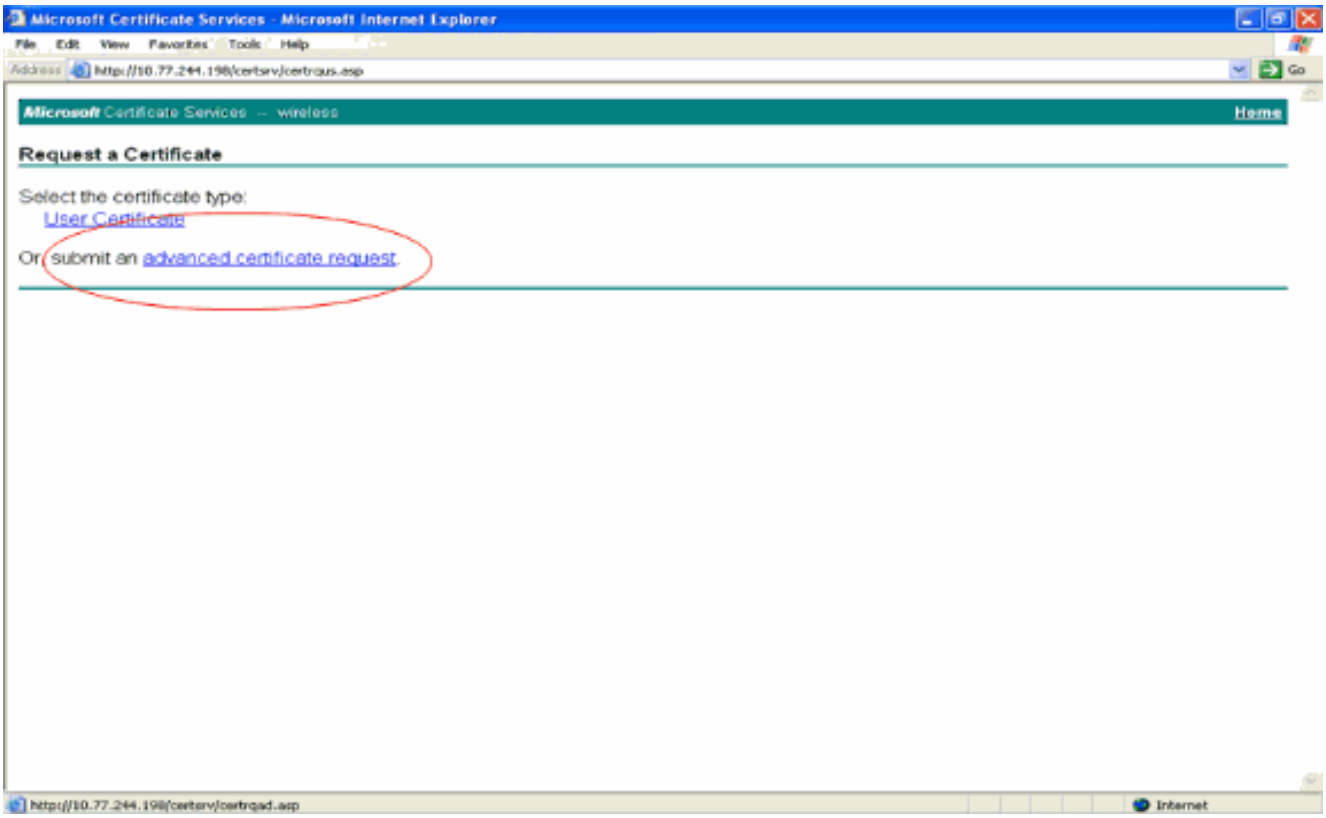
2. Request **a certificate(인증서 요청)를 선택합니다**

.



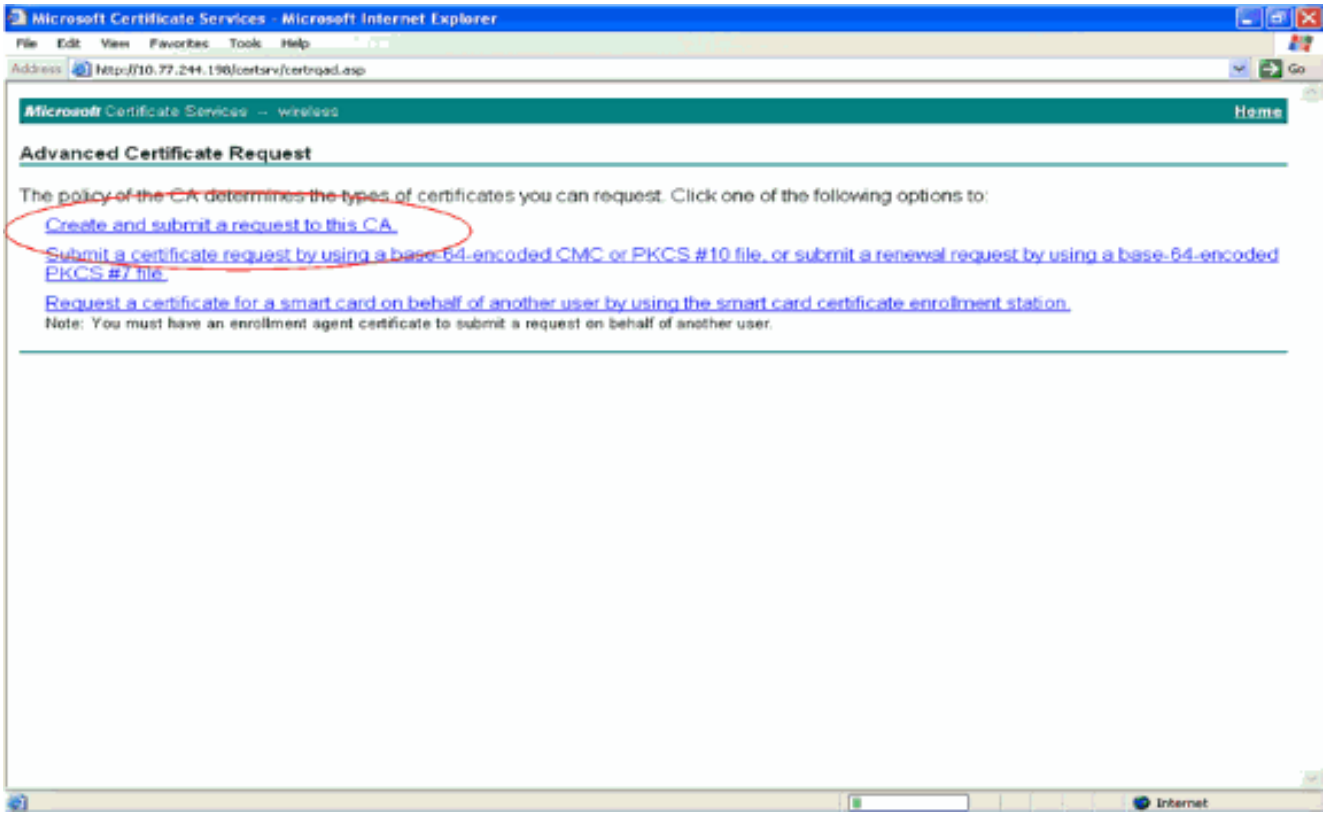
3. Request a Certificate(인증서 요청) 페이지에서 **advanced certificate request(고급 인증서 요청)**를 클릭합니다

.



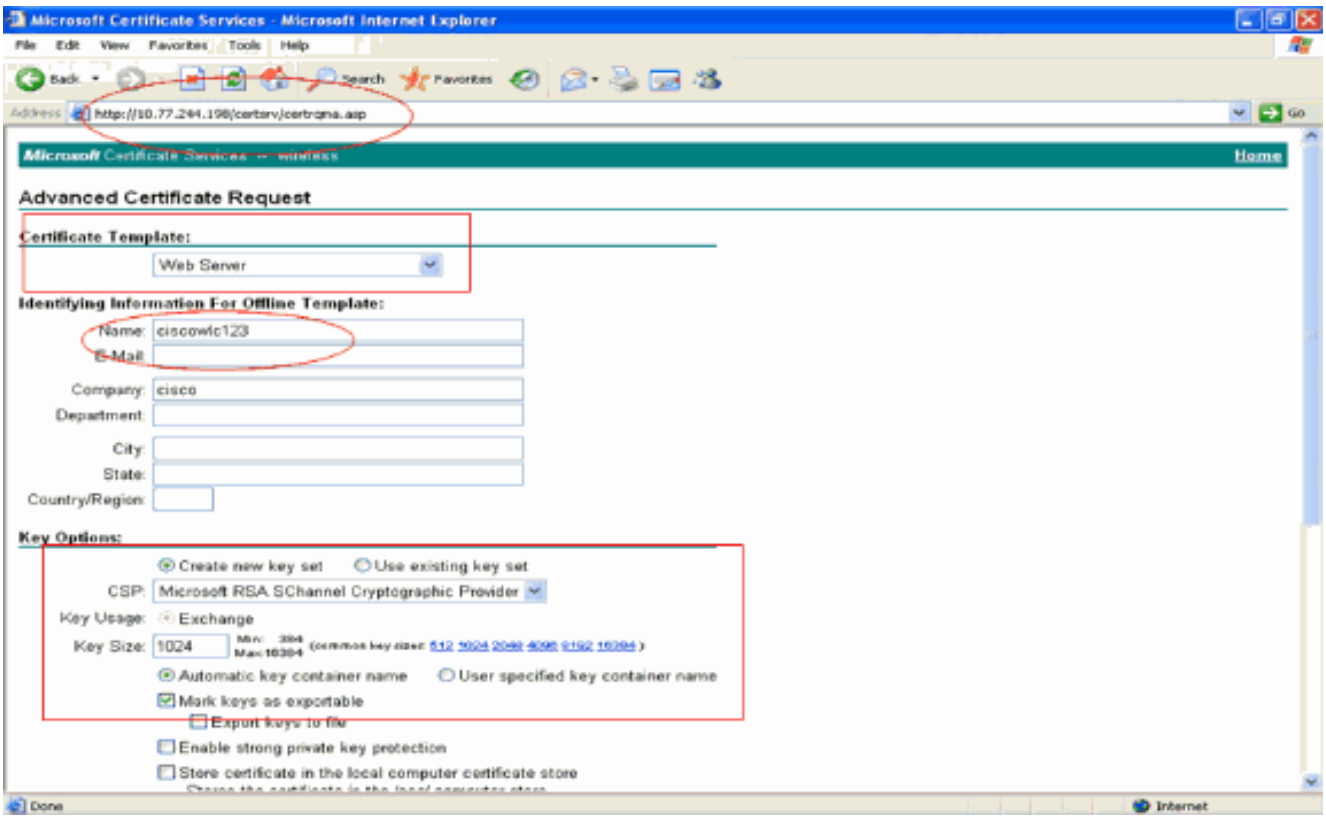
4. Advanced Certificate Request(고급 인증서 요청) 페이지에서 Create(생성)를 클릭하고 **이 CA에 요청을 제출합니다**. 그러면 Advanced certificate request(고급 인증서 요청) 양식으로 이동합니다

.



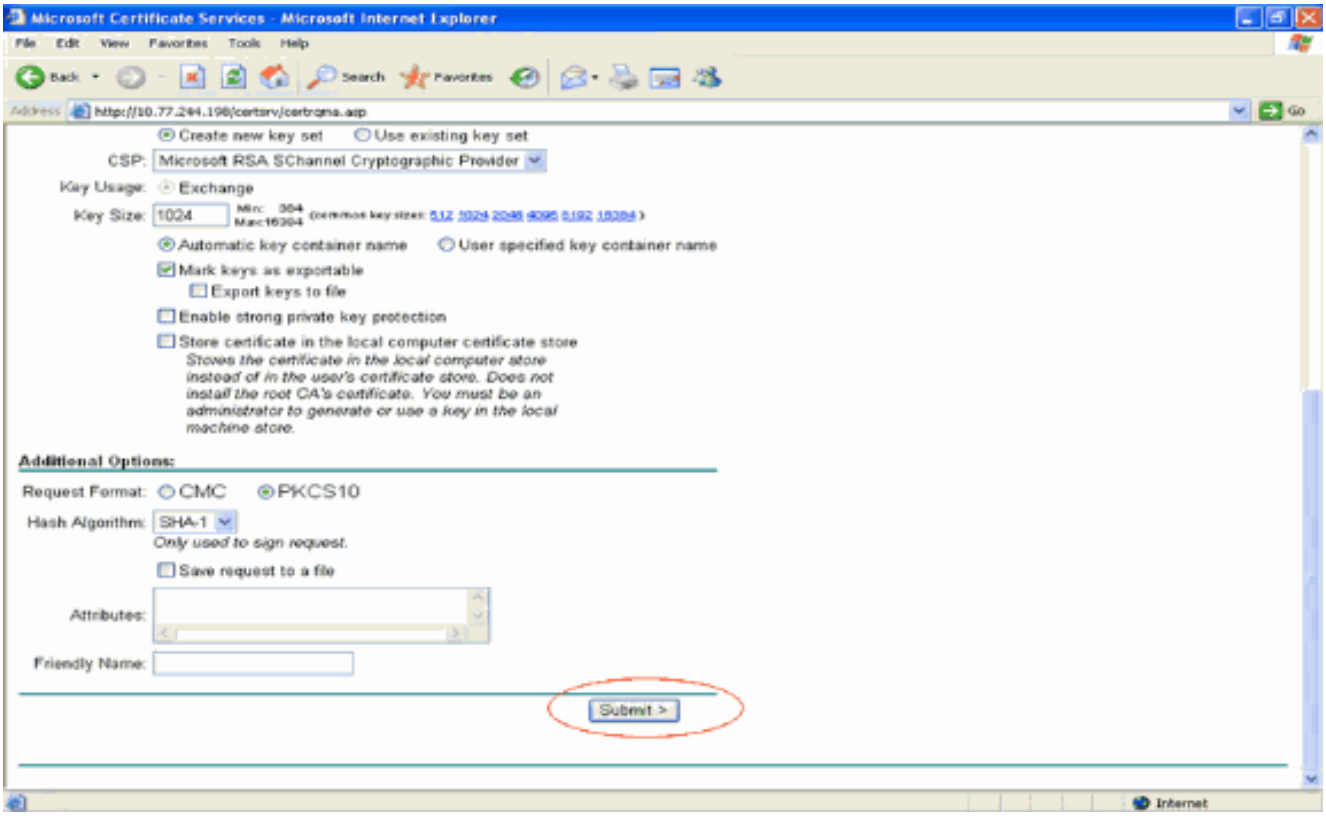
5. Advanced Certificate(고급 인증서) 요청 양식에서 **Web Server(웹 서버)**를 Certificate Template(인증서 템플릿)으로 선택합니다. 그런 다음 이 디바이스 인증서에 이름을 지정합니다.이 예에서는 인증서 이름을 ciscowlc123으로 사용합니다. 요구 사항에 따라 다른 식별 정보를 입력합니다.
6. Key Options(**키 옵션**) 섹션에서 Mark Keys as Exportable(키를 내보낼 수 **있는 것으로 표시) 옵션을** 선택합니다. 웹 서버 템플릿을 선택하는 경우 이 특정 옵션이 회색으로 비활성화되어 활성화 또는 비활성화될 수 없는 경우가 있습니다. 이러한 경우 브라우저 **메뉴**에서 Back(뒤로)을 클릭하여 한 페이지로 돌아가고 다시 이 페이지로 돌아갑니다. 이번에는 Mark Keys as Exportable(키를 내보낼 수 있는 것으로 표시) 옵션을 사용할 수 있습니다

.



7. 기타 필요한 필드를 모두 구성하고 Submit(제출)을 **클릭합니다**

.

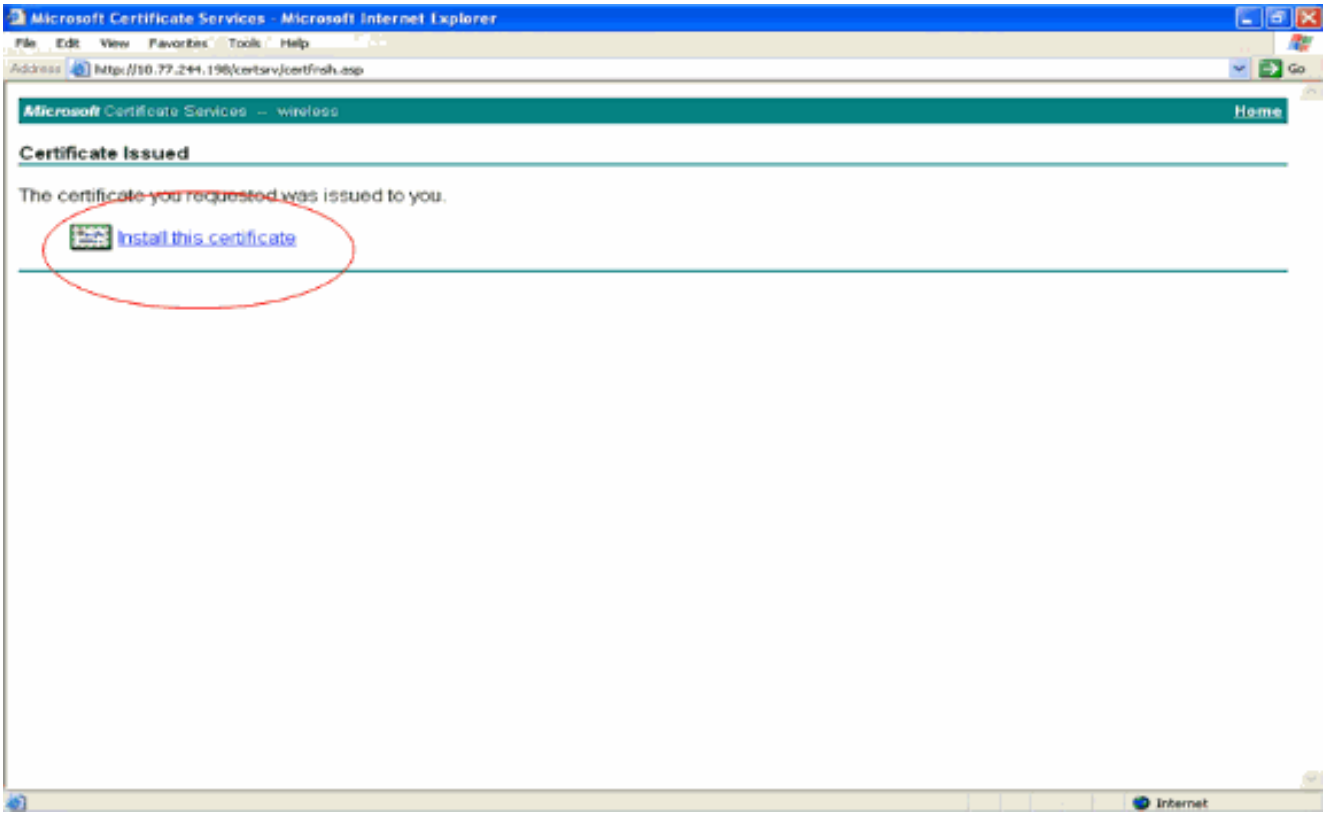


8. 인증서 요청 **프로세스**를 허용하려면 다음 창에서 Yes(**예**)를 클릭합니다

.

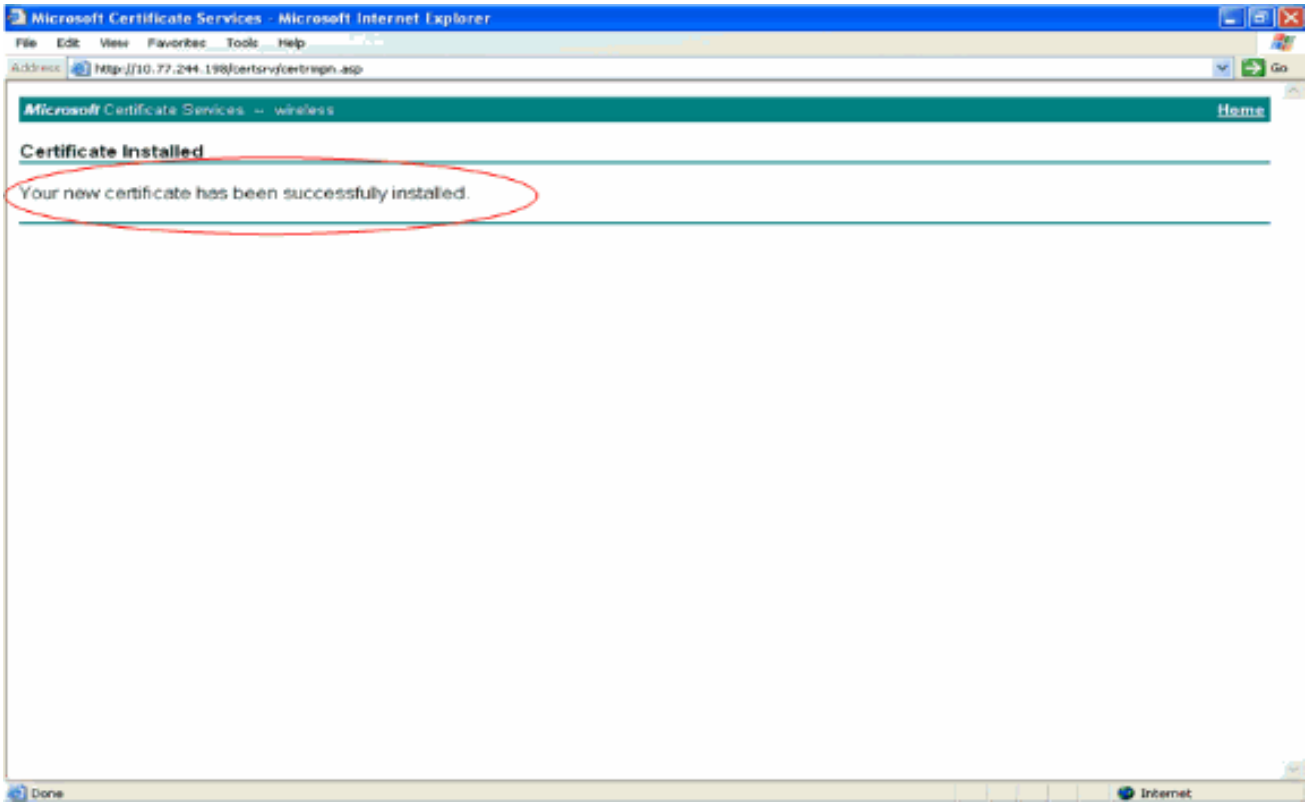
9. Certificate Issued(발급된 인증서) 창이 나타나며, 이는 인증서 요청 프로세스가 성공했음을 나타냅니다. 다음 단계는 이 PC의 인증서 저장소에 발급된 인증서를 설치하는 것입니다. Install **this certificate(이 인증서 설치)를 클릭합니다**

.



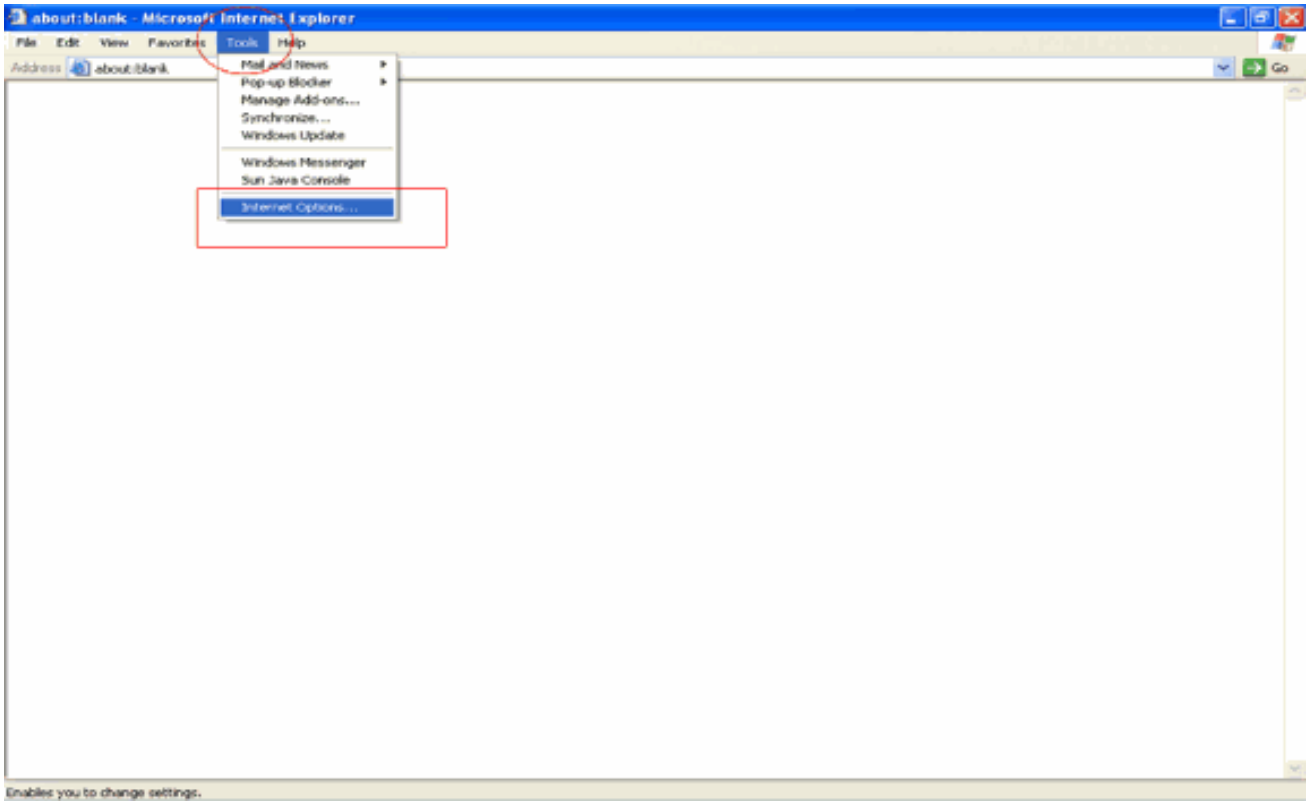
10. CA 서버에 요청이 생성되는 PC에 새 인증서가 성공적으로 설치됩니다

.



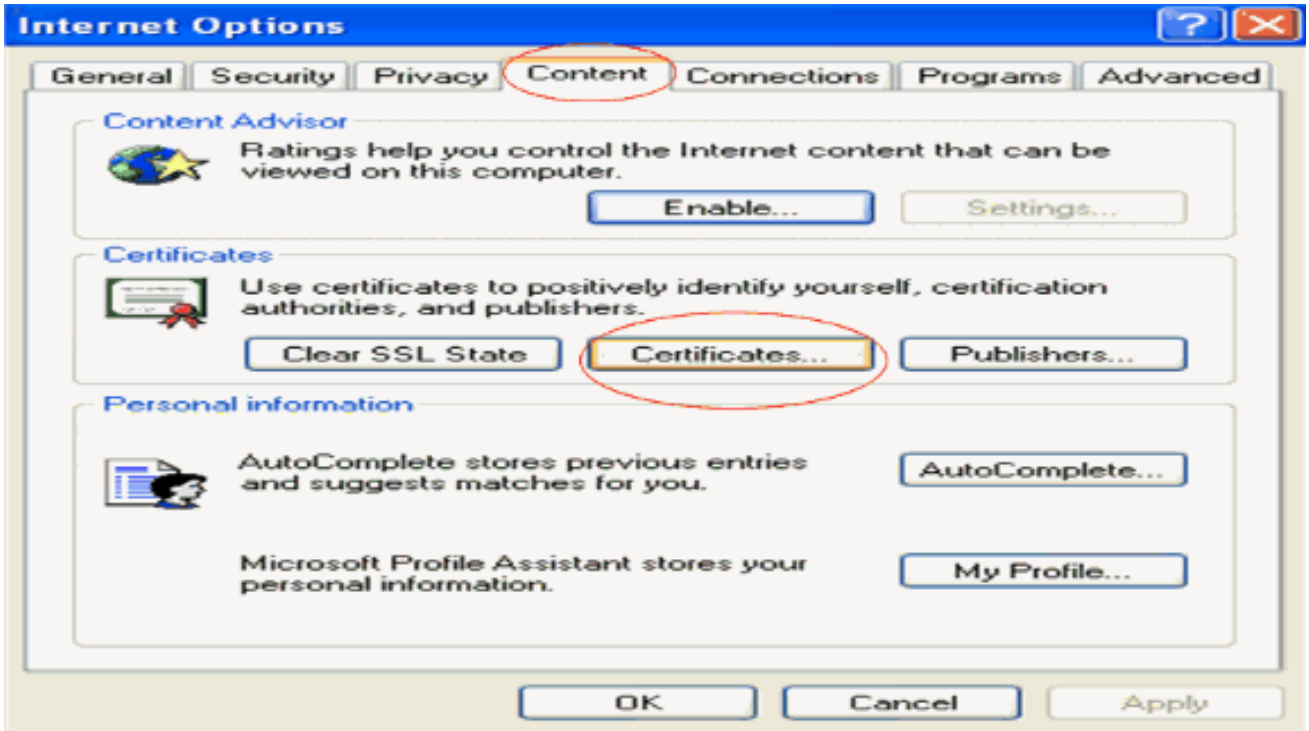
11. 다음 단계는 이 인증서를 인증서 저장소에서 하드 디스크로 파일로 내보내는 것입니다. 이 인증서 파일은 나중에 WLC에 인증서를 다운로드하는 데 사용됩니다.인증서 저장소에서 인증서를 내보내려면 Internet Explorer 브라우저를 열고 **도구 > 인터넷 옵션**을 클릭합니다

.



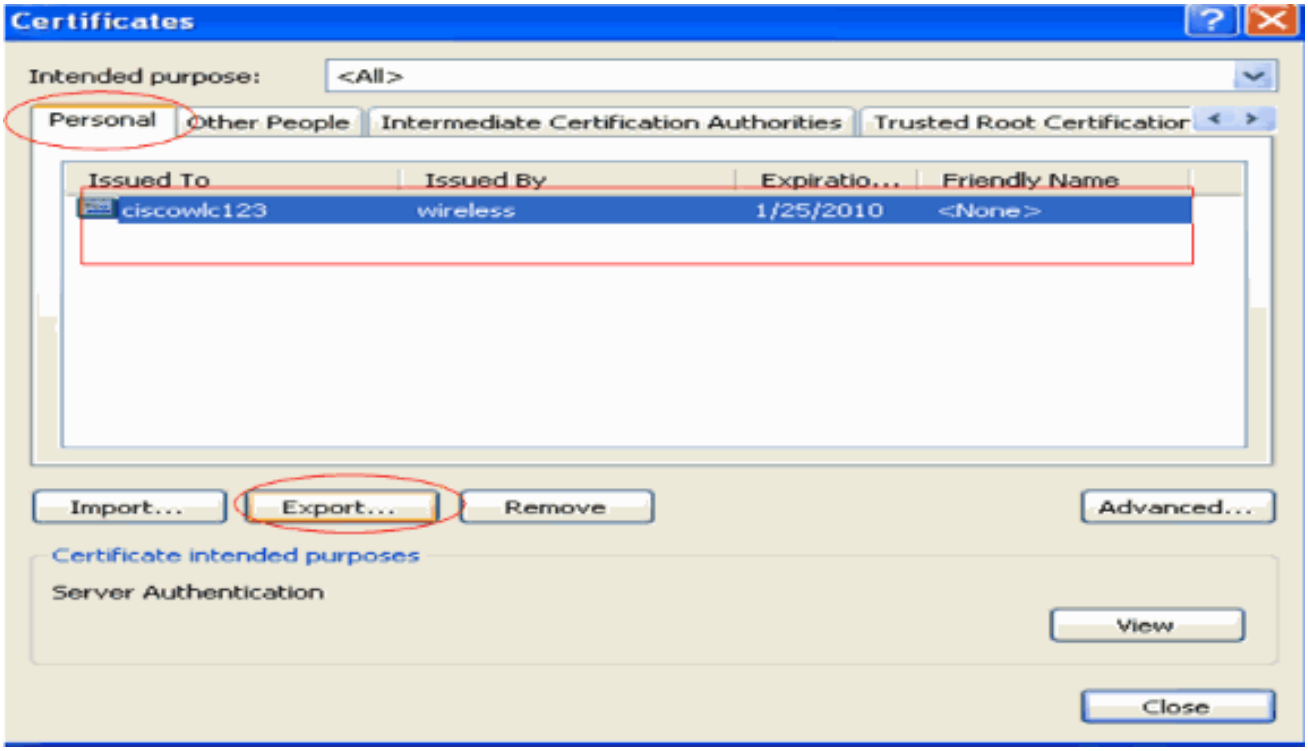
12. 인증서**가 기본적**으로 설치된 인증서 저장소로 이동하려면 Content(콘텐츠) > Certificates(인증서)를 클릭합니다

.



13. 디바이스 인증서는 일반적으로 **개인** 인증서 목록 아래에 설치됩니다. 여기에 새로 설치된 인증서가 표시됩니다. 인증서를 선택하고 Export(내보내기)**를 클릭합니다**

.

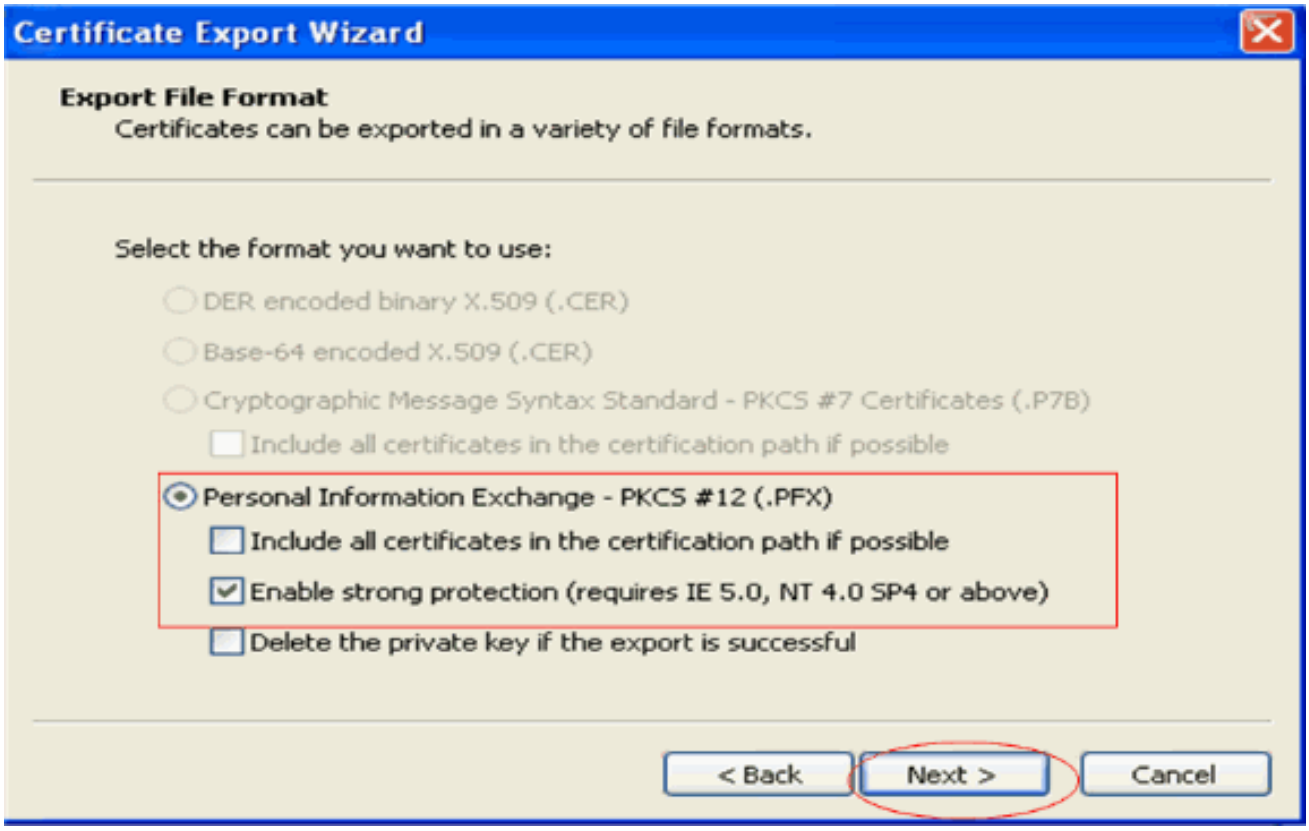


14. 다음 **창**에서 다음을 클릭합니다. **Certificate** Export **Wizard(인증서 내보내기 마법사) 창**에서 **Yes(예), export the private key(개인 키 내보내기) 옵션을** 선택합니다. **Next(다음)**를 클릭합니다

.

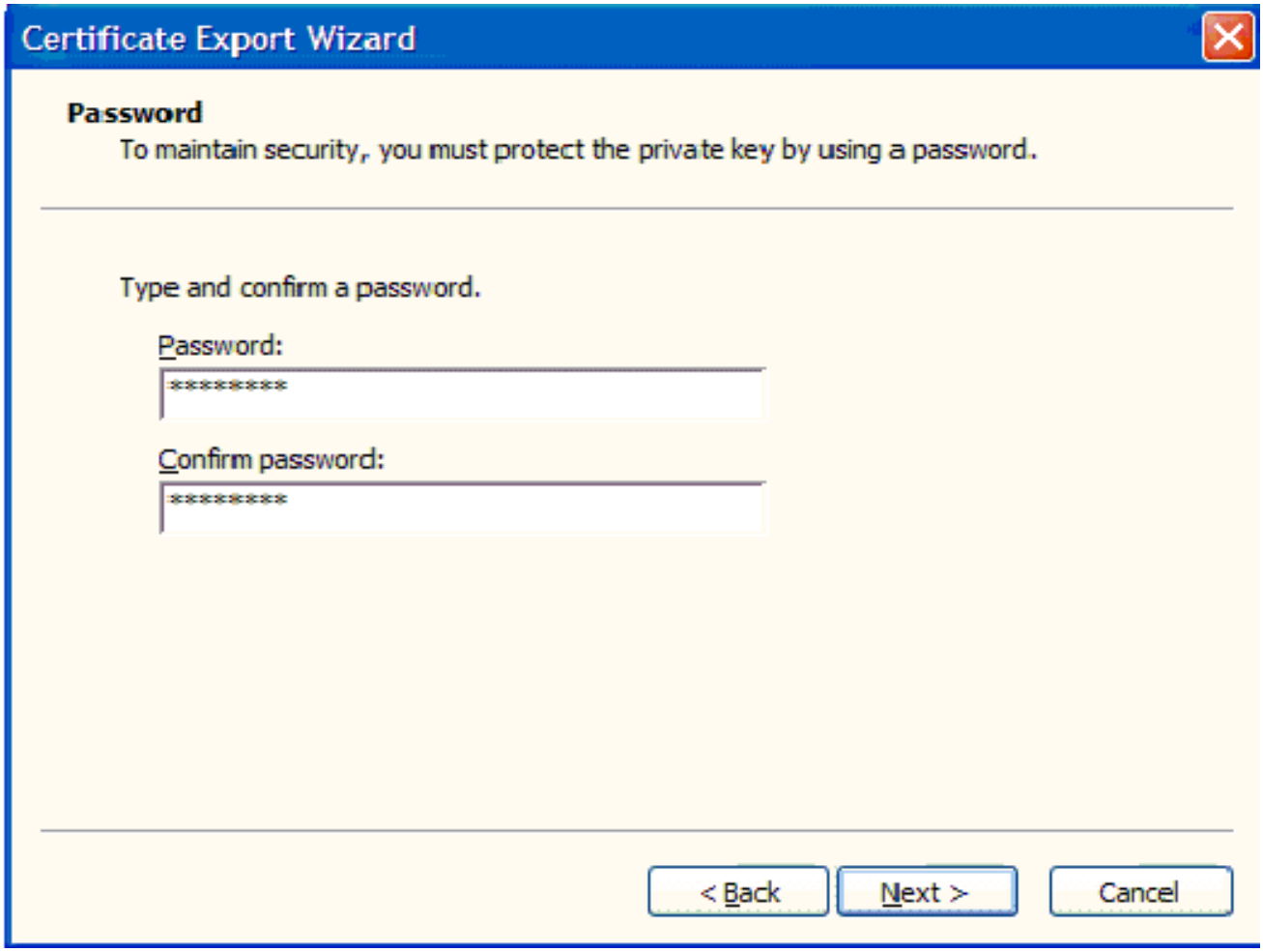
15. 내보내기 파일 형식을 .PFX로 **선택하고 강력한 보호** 사용 **옵션을** 선택합니다. **Next(다음)**를 클릭합니다

.



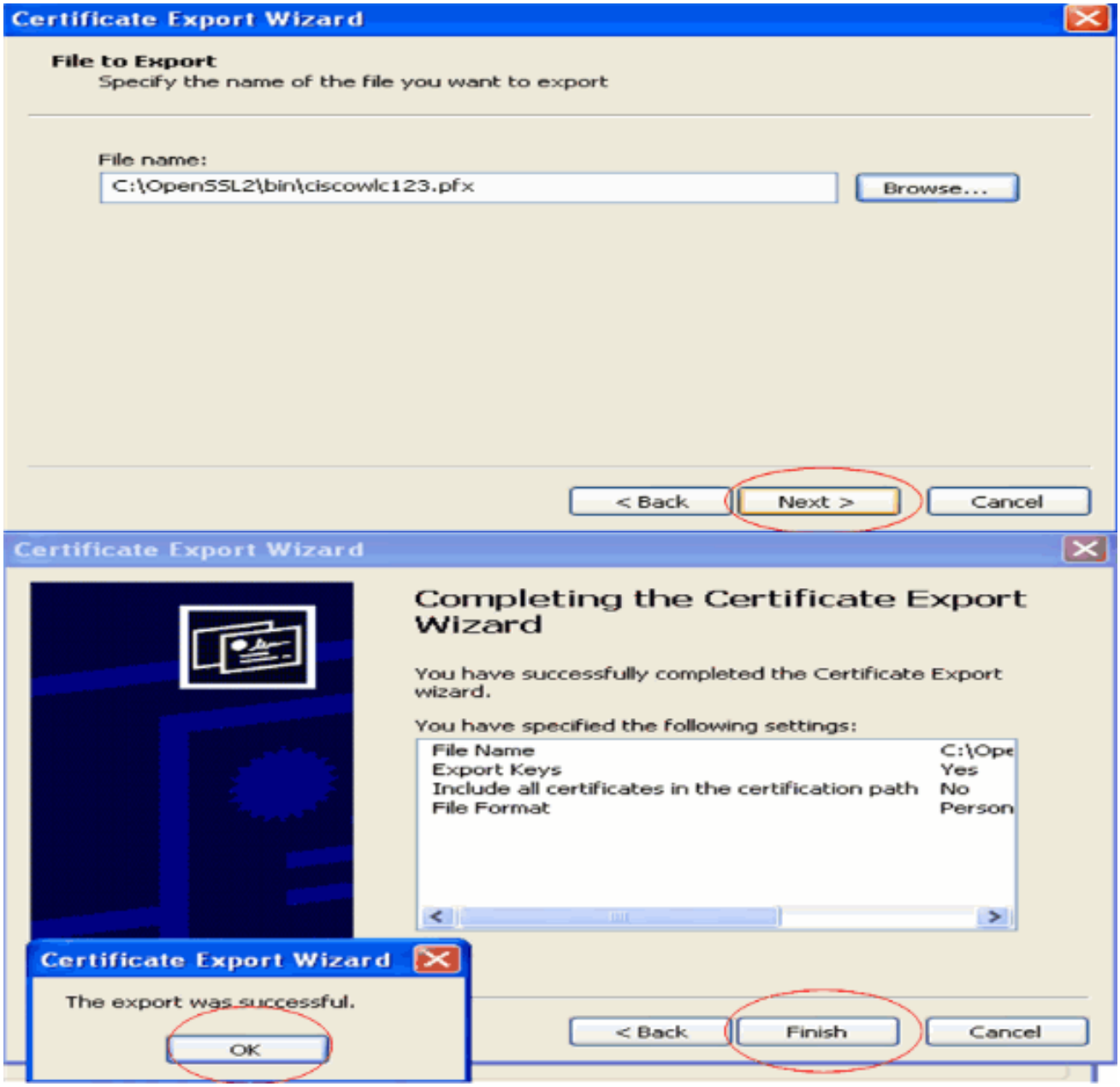
16. Password(비밀번호) 창에 비밀번호를 입력합니다. 이 예에서는 **cisco**를 비밀번호로 사용합니다

.



17. 인증서 파일(.PFX 파일)을 하드 디스크에 저장합니다. Next(**다음**)를 클릭하여 내보내기 프로세스를 성공적으로 완료합니다

.



WLC에 디바이스 인증서 다운로드

이제 WLC 장치 인증서를 .PFX 파일로 사용할 수 있으므로 다음 단계는 컨트롤러에 파일을 다운로드하는 것입니다. Cisco WLC는 .PEM 형식의 인증서만 수락합니다. 따라서 먼저 openSSL 프로그램을 사용하여 .PFX 또는 PKCS12 형식 파일을 PEM 파일로 변환해야 합니다.

OpenSSL 프로그램을 사용하여 PFX의 인증서를 PEM 형식으로 변환

PEM 형식으로 변환하기 위해 openSSL이 설치된 모든 PC에 인증서를 복사할 수 있습니다. openSSL 프로그램의 bin 폴더에 있는 Openssl.exe 파일에 다음 명령을 입력합니다.

참고: OpenSSL 웹 사이트에서 openSSL을 다운로드할 수 있습니다.

```
openssl>pkcs12 -in ciscowlc123.pfx -out ciscowlc123.pem
!--- ciscowlc123 is the name used in this example for the exported file. !--- You can specify
any name to your certificate file. Enter Import Password : cisco
!--- This is the same password that is mentioned in step 16 of the previous section. MAC
```

```
verified Ok Enter PEM Pass phrase : cisco
!--- Specify any passphrase here. This example uses the PEM passphrase as cisco. Verifying - PEM
pass phrase : cisco
```

인증서 파일이 PEM 형식으로 변환됩니다. 다음 단계는 PEM 형식 디바이스 인증서를 WLC에 다운로드하는 것입니다.

참고: 그 전에 PEM 파일을 다운로드할 PC에 TFTP 서버 소프트웨어가 있어야 합니다. 이 PC는 WLC에 연결되어 있어야 합니다. TFTP 서버에는 PEM 파일이 저장된 위치에 지정된 현재 및 기본 디렉토리가 있어야 합니다.

변환된 PEM 형식 디바이스 인증서를 WLC에 다운로드

이 예에서는 WLC의 CLI를 통한 다운로드 프로세스에 대해 설명합니다.

1. 컨트롤러 CLI에 로그인합니다.
2. transfer download datatype eapdevcert **명령을** 입력합니다.
3. **transfer download serverip *10.77.244.196 명령을*** 입력합니다.10.77.244.196은 TFTP 서버의 IP 주소입니다.
4. transfer download **filename ciscowlc*.pem 명령을*** 입력합니다.이 예에서 사용되는 파일 이름은 ciscowlc123.pem입니다.
5. transfer **download certpassword** 명령을 입력하여 인증서의 비밀번호를 설정합니다.
6. 업데이트된 설정을 보려면 **transfer download start** 명령을 입력합니다.그런 다음 현재 **설정**을 확인하고 다운로드 프로세스를 시작하라는 프롬프트가 표시되면 y를 응답합니다.다음 예에서는 download 명령 출력을 보여 줍니다.

```
(Cisco Controller) >transfer download start

Mode............................................ TFTP
Data Type....................................... Vendor Dev Cert
TFTP Server IP.................................. 10.77.244.196
TFTP Packet Timeout............................. 6
TFTP Max Retries................................ 10
TFTP Path.......................................
TFTP Filename................................... ciscowlc.pem

This may take some time.
Are you sure you want to start? (y/N) y
TFTP EAP CA cert transfer starting.
Certificate installed.
Reboot the switch to use the new certificate.
Enter the reset system command to reboot the controller.
     The controller is now loaded with the device certificate.
```

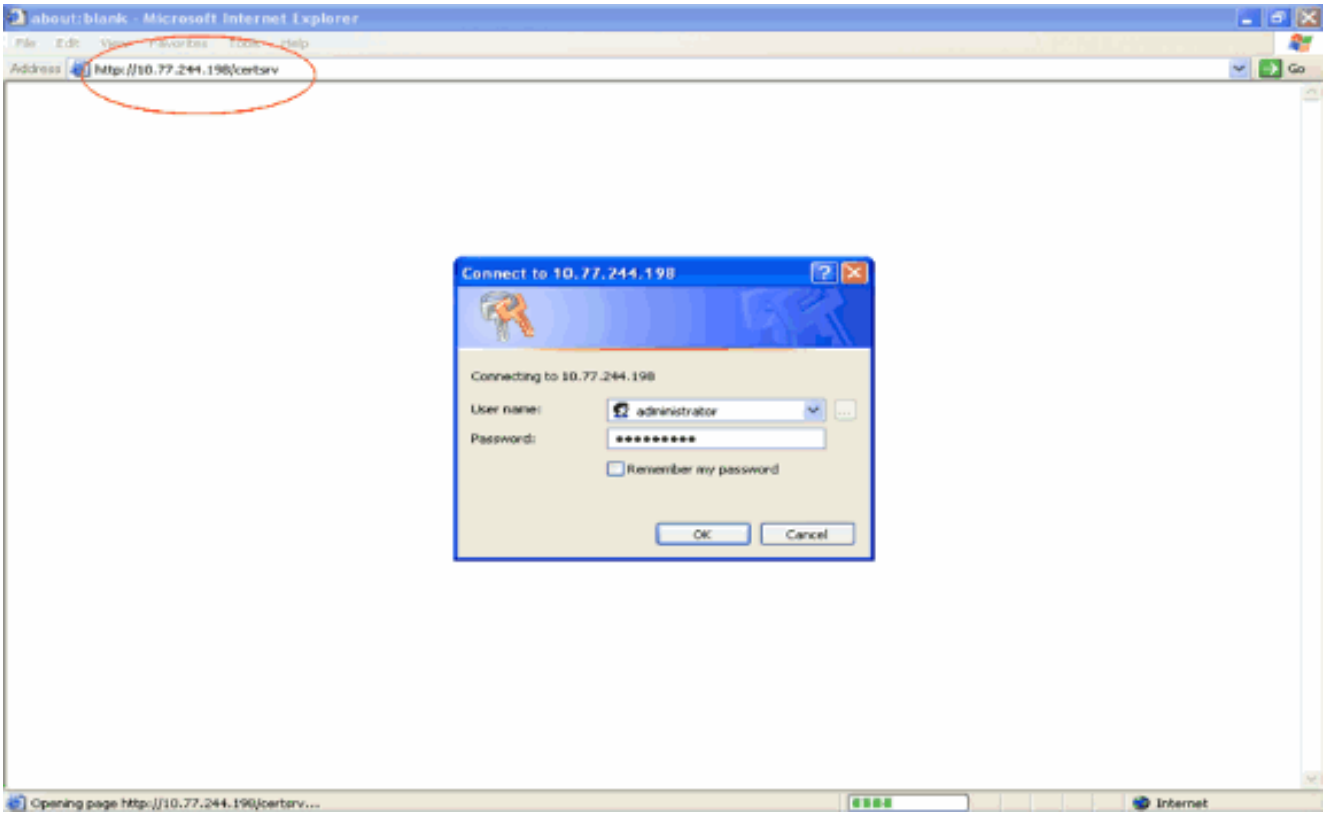
7. 컨트롤러를 **재부팅하려면 reset system** 명령을 입력합니다. 이제 컨트롤러가 디바이스 인증서와 함께 로드됩니다.

PKI의 루트 인증서를 WLC에 설치합니다

이제 디바이스 인증서가 WLC에 설치되었으므로 다음 단계는 CA 서버에서 WLC에 PKI의 루트 인증서를 설치하는 것입니다. 다음 단계를 수행합니다.

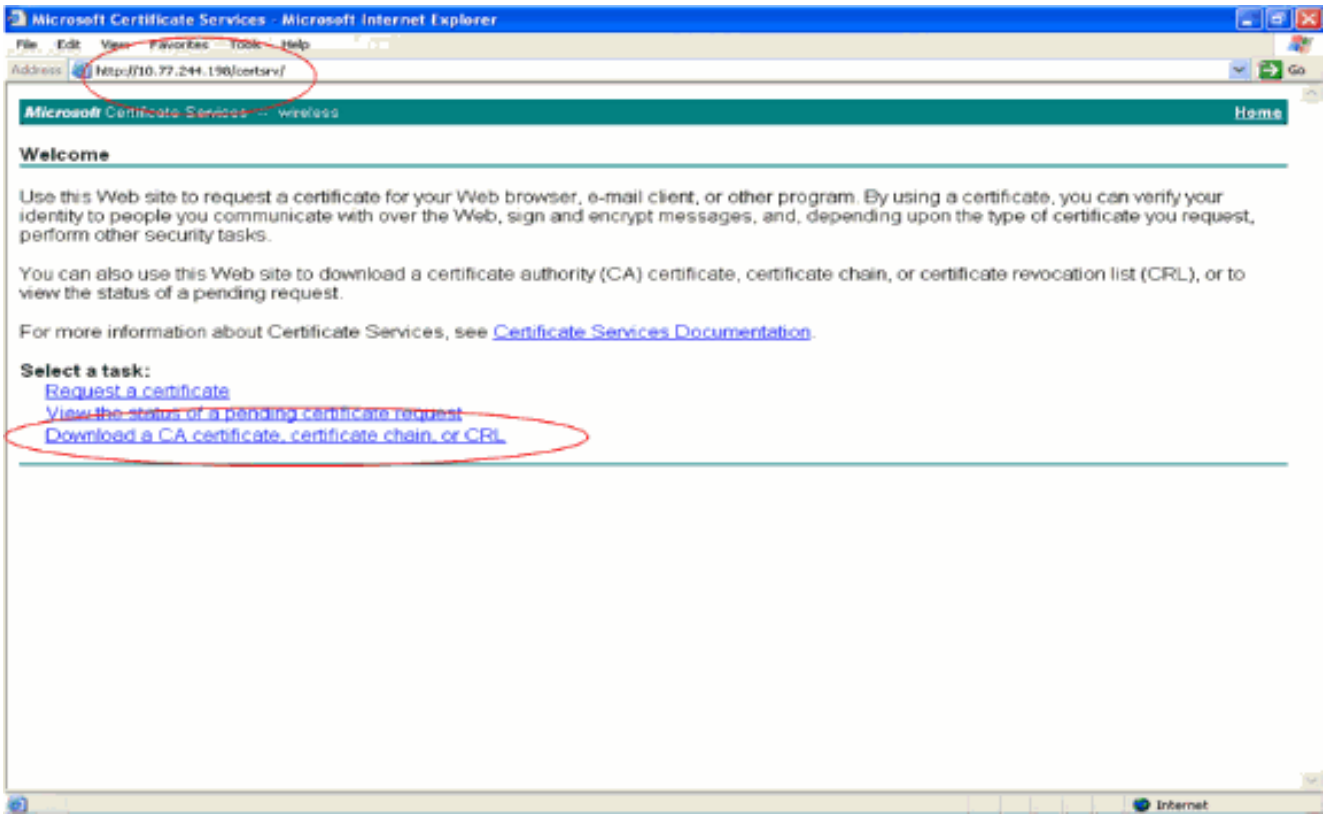
1. CA 서버**에** 대한 네트워크 **연결이 있는** PC에서 http://**<CA** 서버의 **IP 주소>/certsrv**로 이동합니다. CA 서버의 관리자로 로그인합니다

   .



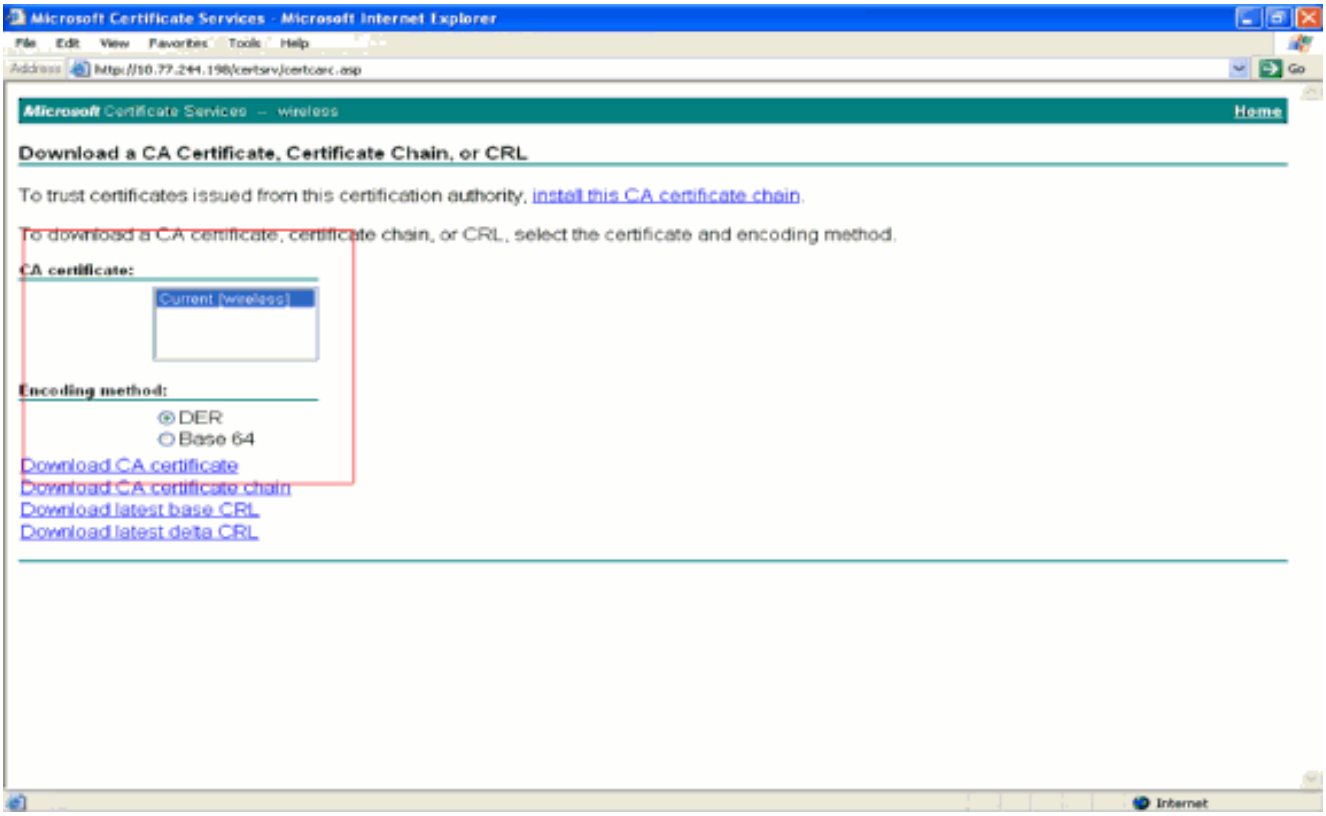
2. Download **a CA certificate, certificate chain, or CRL(CA 인증서, 인증서 체인 또는 CRL 다운로드)을 클릭합니다**

.



3. 결과 페이지에서 CA 서버에서 사용 가능한 현재 CA 인증서를 CA **인증서** 상자 아래에 볼 수 있습니다. 인코딩 **방법**으로 DER를 선택하고 Download **CA certificate(CA 인증서 다운로드)**를 클릭합니다

.

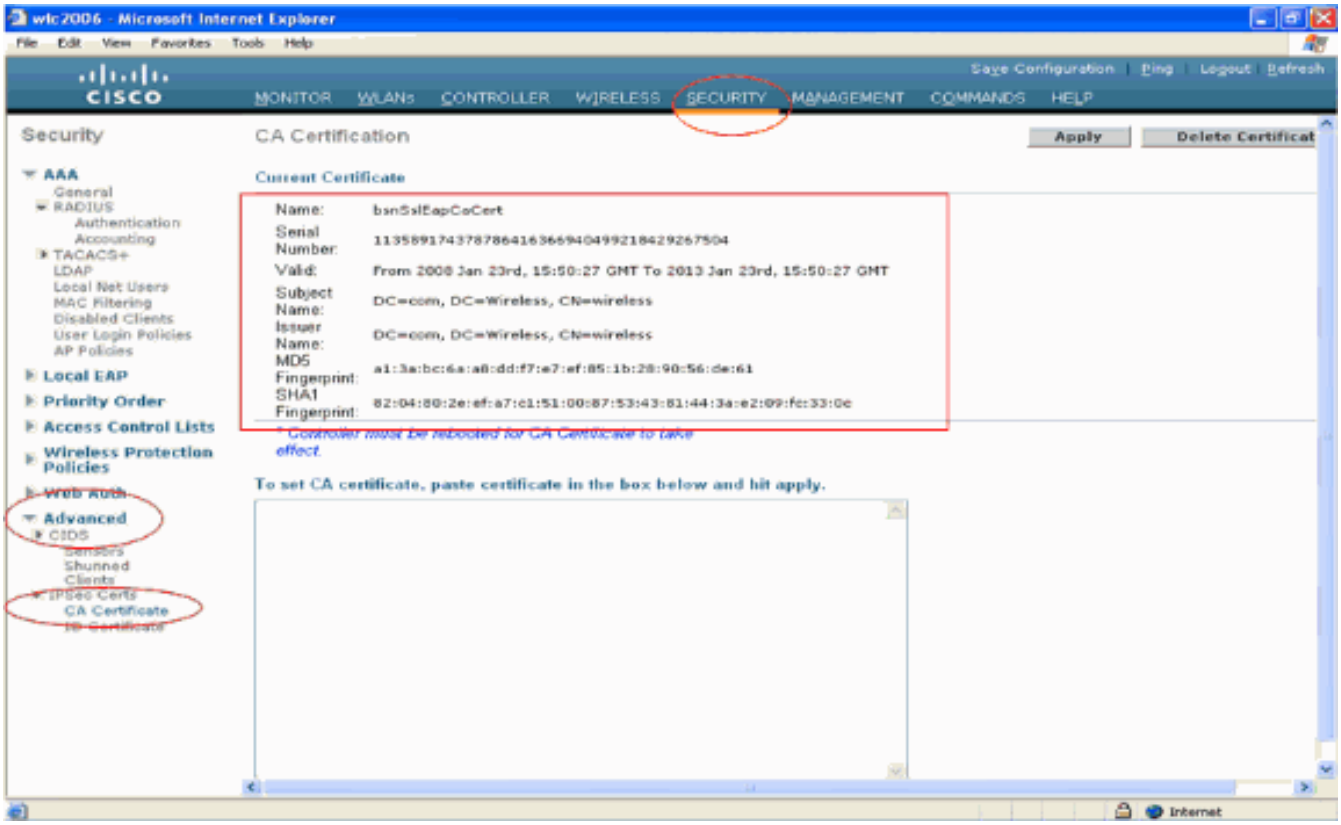


4. 인증서를 **.cer 파일로** 저장합니다. 이 예에서는 certnew.**cer**을 파일 이름으로 사용합니다.
5. 다음 단계는 .cer 파일을 PEM 형식으로 변환하여 컨트롤러에 다운로드하는 것입니다. 이 단계를 수행하려면 다음 변경 사항과 함께 Downloading the Device Certificate to the WLC(디바이스 인증서를 WLC에 다운로드) 섹션에서 설명한 절차를 반복합니다.openSSL "-in" 및 "-out" 파일은 **certnew.cer** 및 **certnew.pem입니다**.또한 이 프로세스에서는 PEM 암호나 가져오기 비밀번호가 필요하지 않습니다.또한 **.cer** 파일을 **.pem** 파일로 변환하는 **openSSL** 명령은 **다음**과 같습니다.**x509 -in *certnew.cer* -inform DER -out *certnew.pem* -outform PEM**Download the Converted PEM Format Device Certificate to the WLC(변환된 PEM 형식 디바이스 인증서를 WLC에 다운로드) 섹션의 2단계에서 WLC에 인증서를 다운로드하는 명령은 다음과 같습니다 .(Cisco Controller)>**다운로드 데이터 유형 eapcacert 전송**WLC에 다운로드할 파일은 certnew.**pem입니다**.

다음과 같이 컨트롤러 GUI에서 WLC에 인증서가 설치되어 있는지 확인할 수 있습니다.

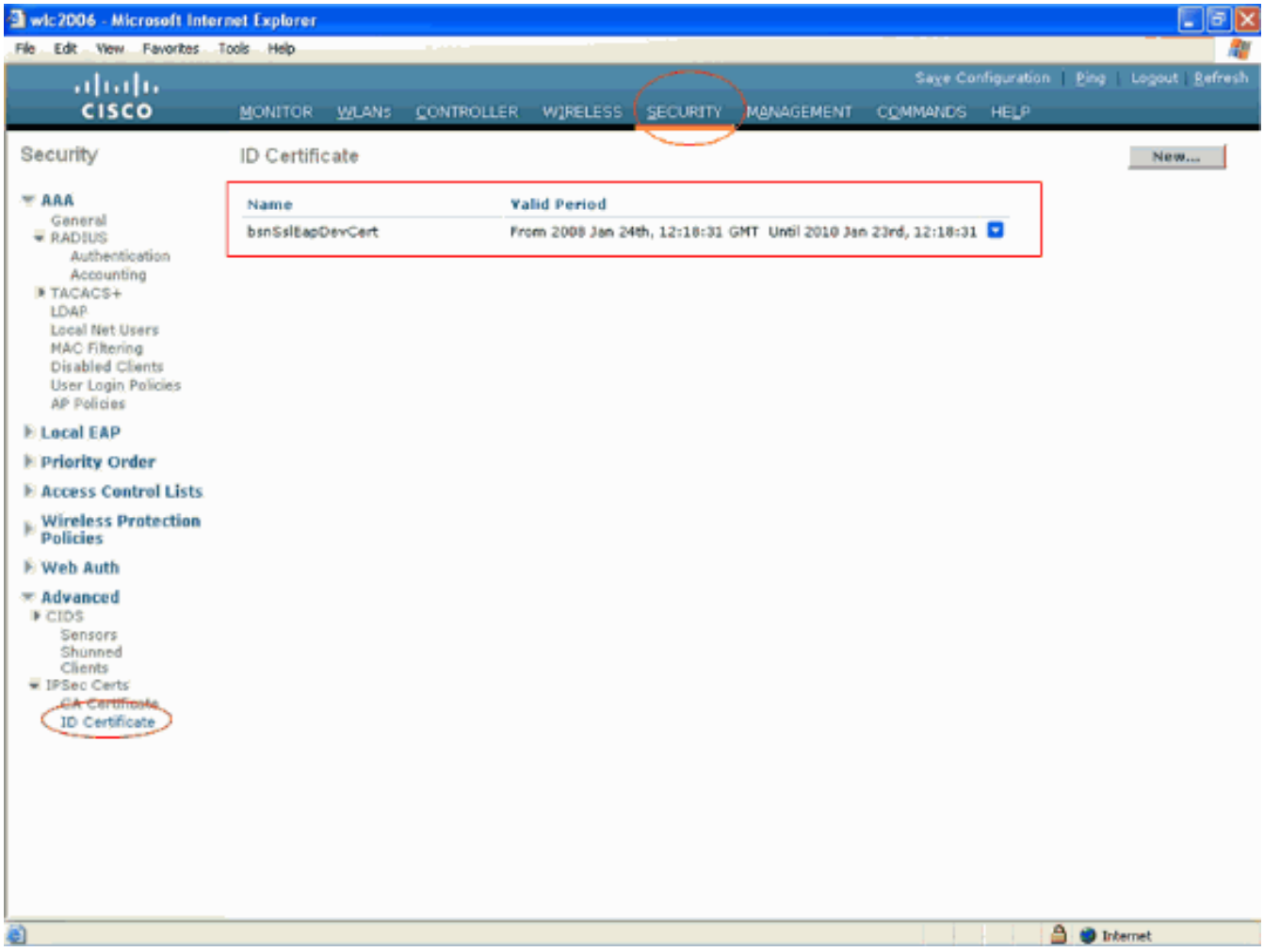
- WLC GUI에서 Security(**보안**)를 **클릭합니다**. Security(보안) 페이지의 왼쪽에 **나타나는 작업**에서 **Advanced(고급) > IPSec** Certs(IPSec 인증서)를 클릭합니다. 설치된 **CA 인증서**를 보려면 CA Certificate(CA 인증서)를 클릭합니다. 예를 들면 다음과 같습니다

.



- 디바이스 인증서가 WLC에 설치되어 있는지 확인하려면 WLC GUI에서 Security(**보안**)를 클릭합니다. Security(보안) 페이지의 왼쪽에 **나타나는 작업**에서 **Advanced(고급) > IPSec** Certs(IPSec 인증서)를 클릭합니다. 설치된 디바이스 **인증서**를 보려면 **ID** Certificate(**ID 인증서**)**를** 클릭합니다. 예를 들면 다음과 같습니다

.



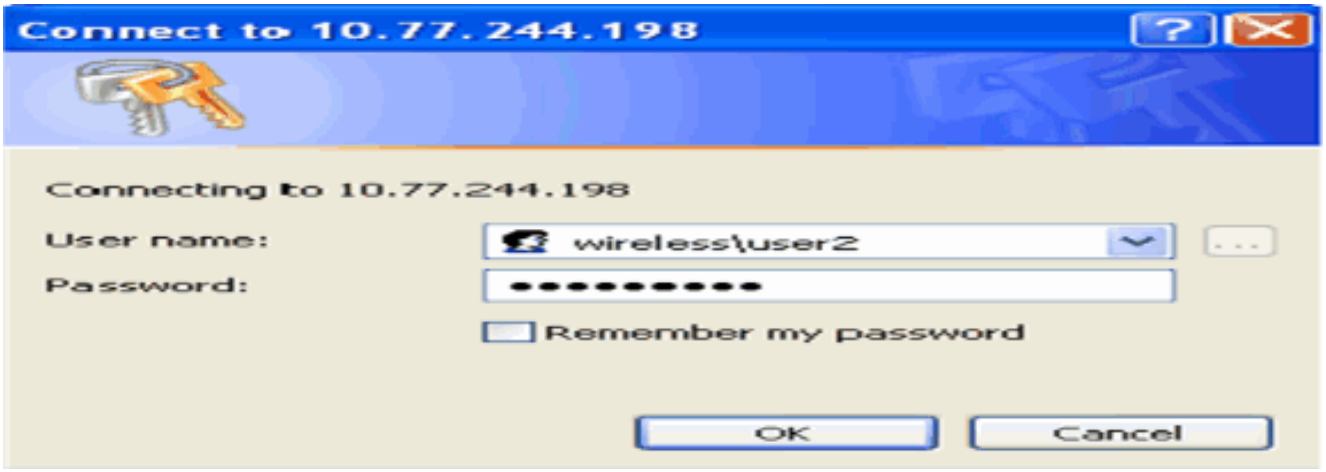
클라이언트에 대한 디바이스 인증서 생성

이제 디바이스 인증서 및 CA 인증서가 WLC에 설치되었으므로 다음 단계는 클라이언트에 대해 이러한 인증서를 생성하는 것입니다.

클라이언트에 대한 디바이스 인증서를 생성하려면 다음 단계를 수행합니다. 이 인증서는 클라이언트에서 WLC에 인증하는 데 사용됩니다. 이 문서에서는 Windows XP Professional 클라이언트에 대한 인증서를 생성하는 단계에 대해 설명합니다.

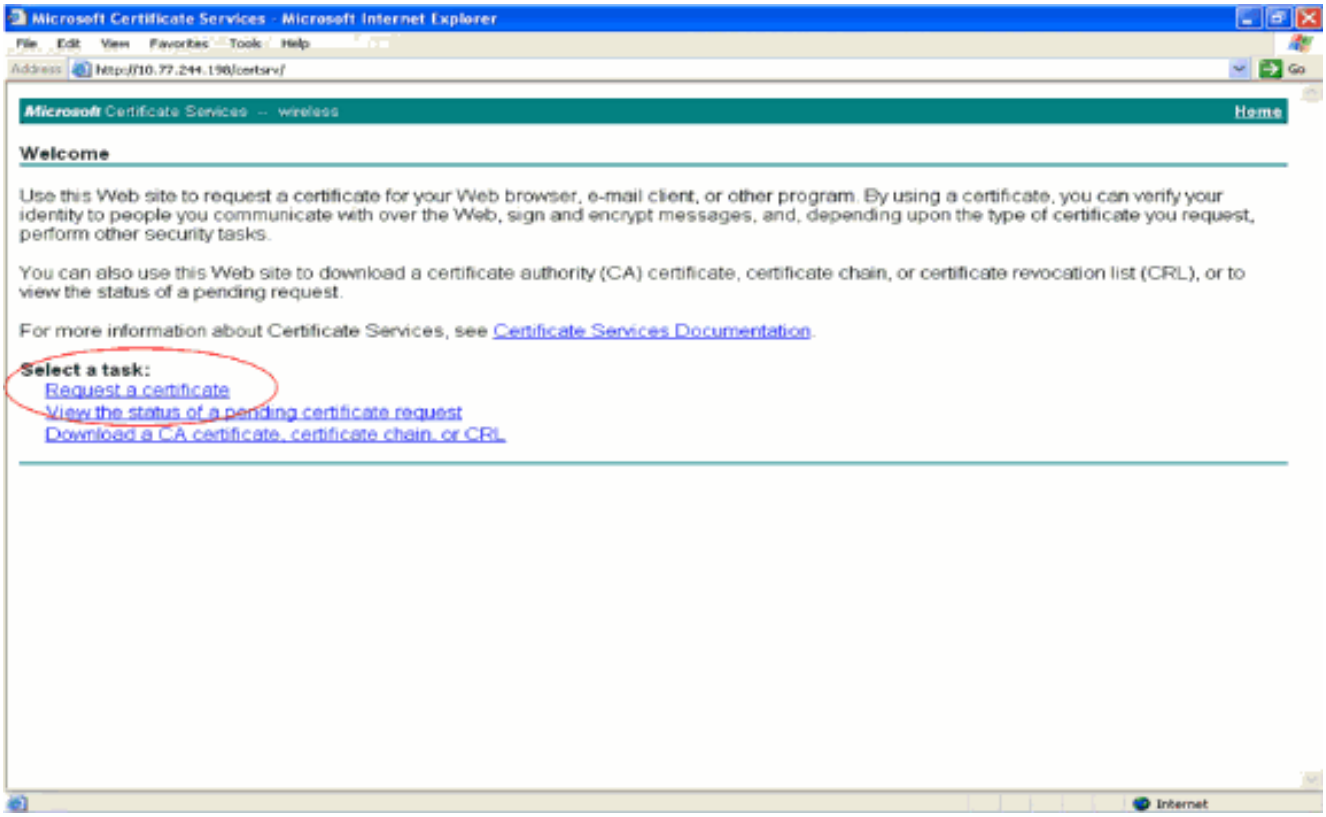
1. 인증서를 설치해야 **하는 클라이언트**에서 http://**<CA 서버**의 **IP 주소>/**certsrv로 이동합니다. CA 서버에 domain name\username으로 로그인합니다. 사용자 이름은 이 XP 시스템을 사용하는 사용자의 이름이어야 하며, 사용자는 CA 서버와 동일한 도메인의 일부로 이미 구성되어 있어야 합니다

.



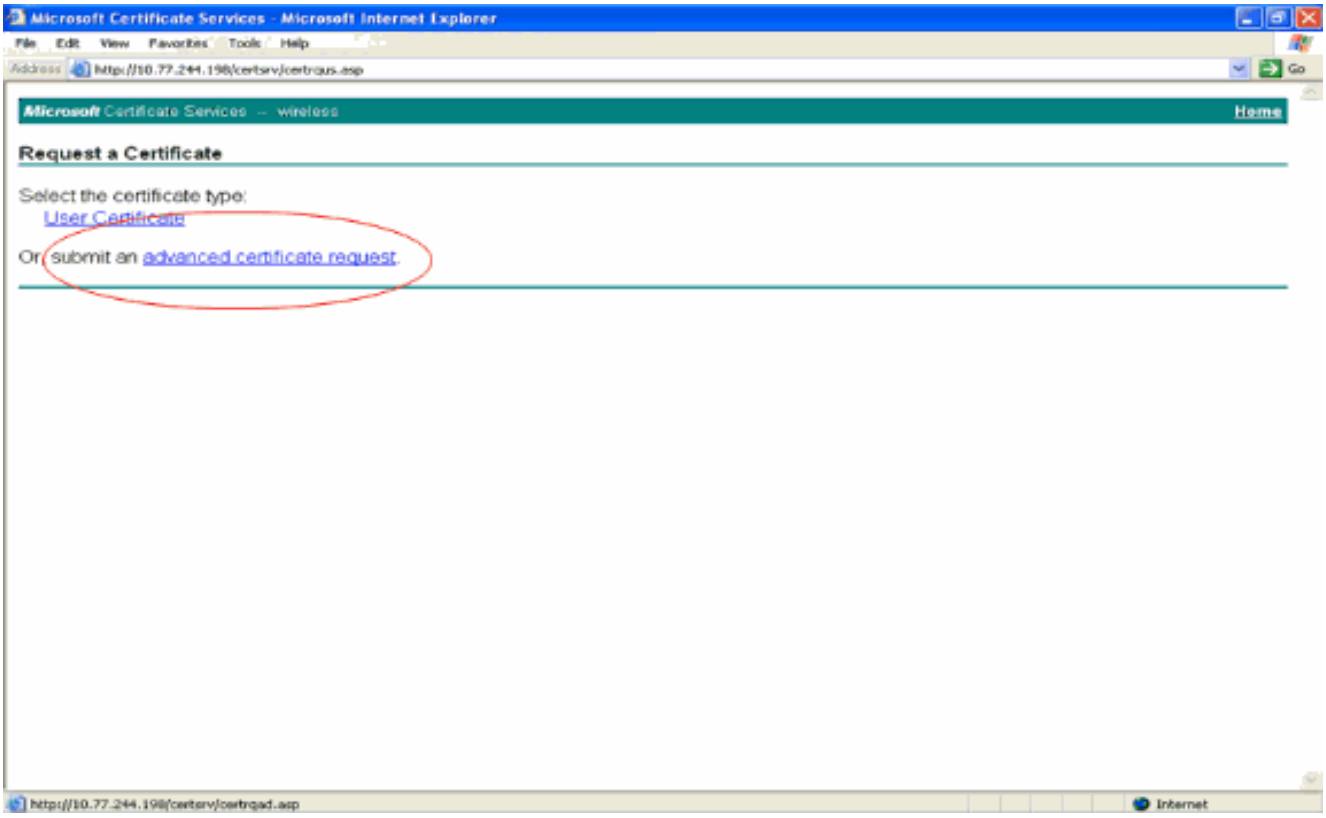
2. Request **a certificate(인증서 요청)를 선택합니다**

.



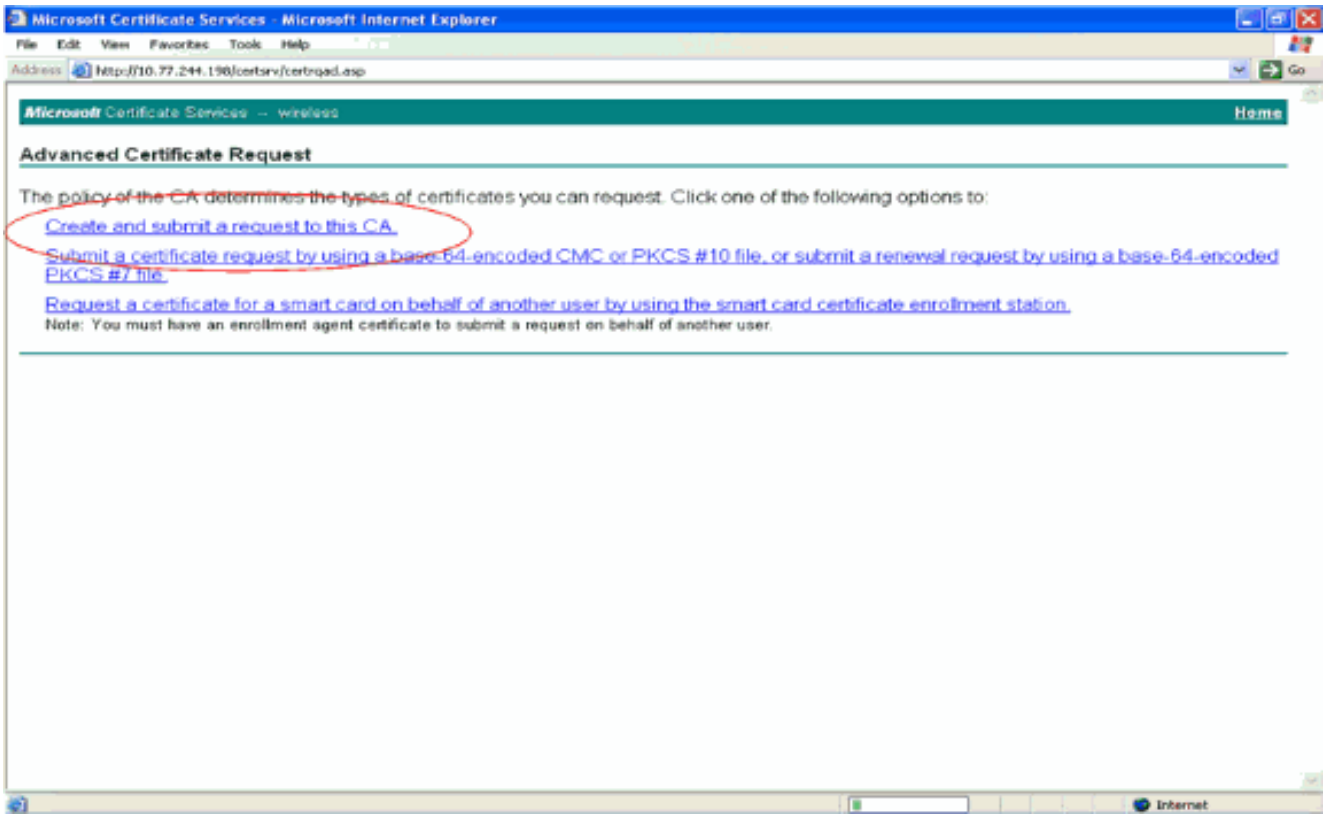
3. Request a Certificate(인증서 요청) 페이지에서 **advanced certificate request(고급 인증서 요청)**를 클릭합니다

.



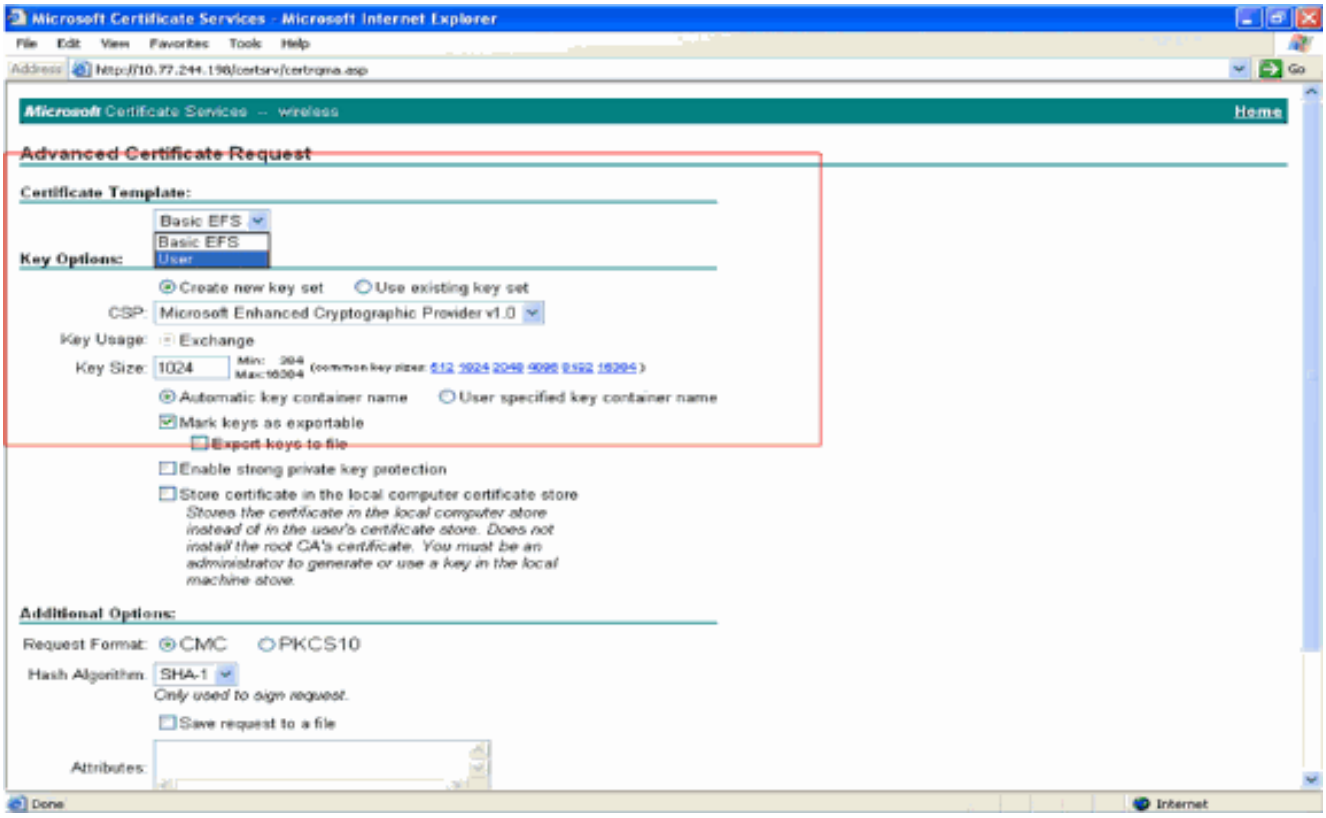
4. Advanced Certificate Request(고급 인증서 요청) 페이지에서 Create(생성)를 클릭하고 **이 CA에 요청을 제출합니다**. 그러면 Advanced Certificate(고급 인증서) 요청 양식으로 이동합니다

.



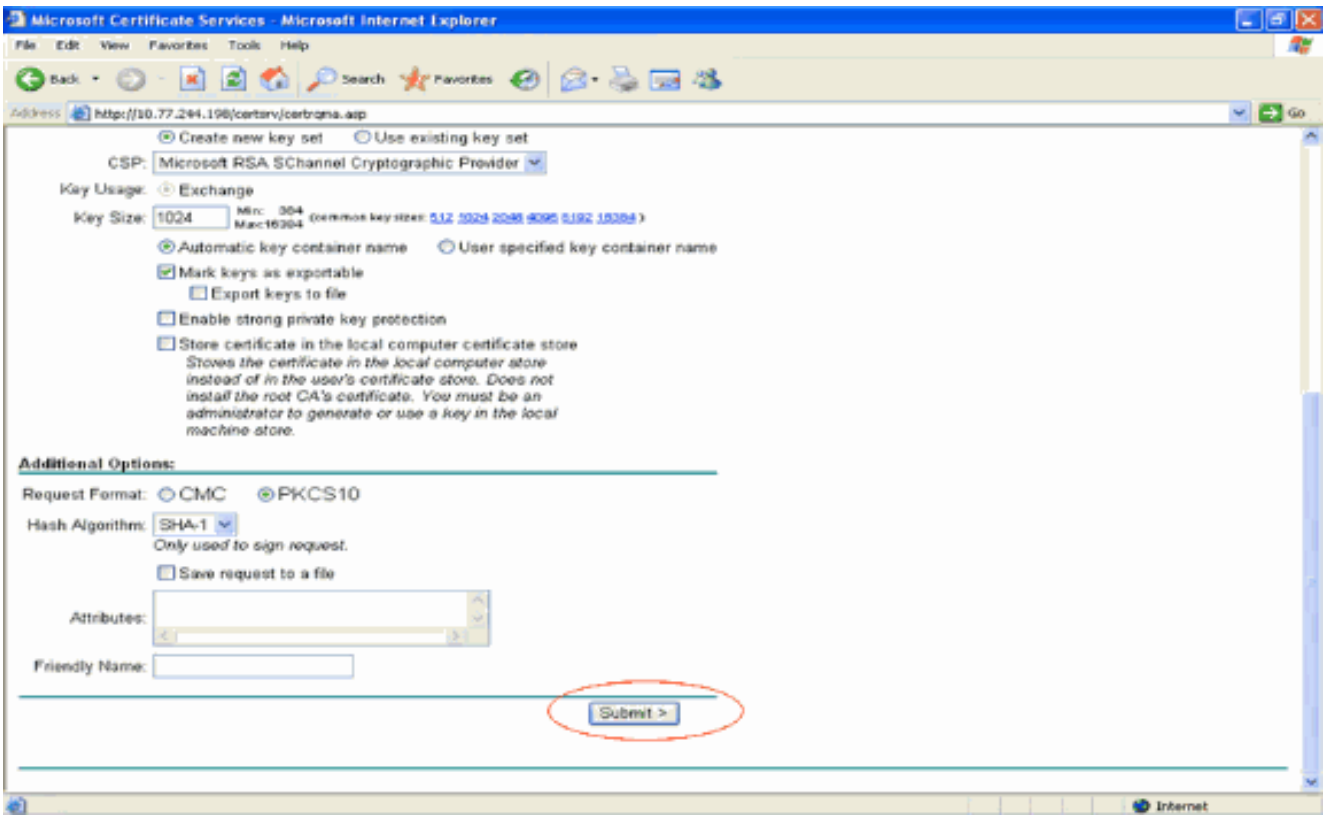
5. Advanced Certificate(고급 인증서) 요청 양식의 Certificate Template(인증서 템플릿) 드롭다운 메뉴에서 User(**사용자)**를 선택합니다.Key options(키 옵션) 섹션에서 다음 매개변수를 선택합니다.Key Size(키 크기) 필드에 키 크기를 입력합니다. 이 예에서는 **1024**를 **사용합니다**.내보낼 수 있는 **키로 표시 옵션을** 선택합니다

.



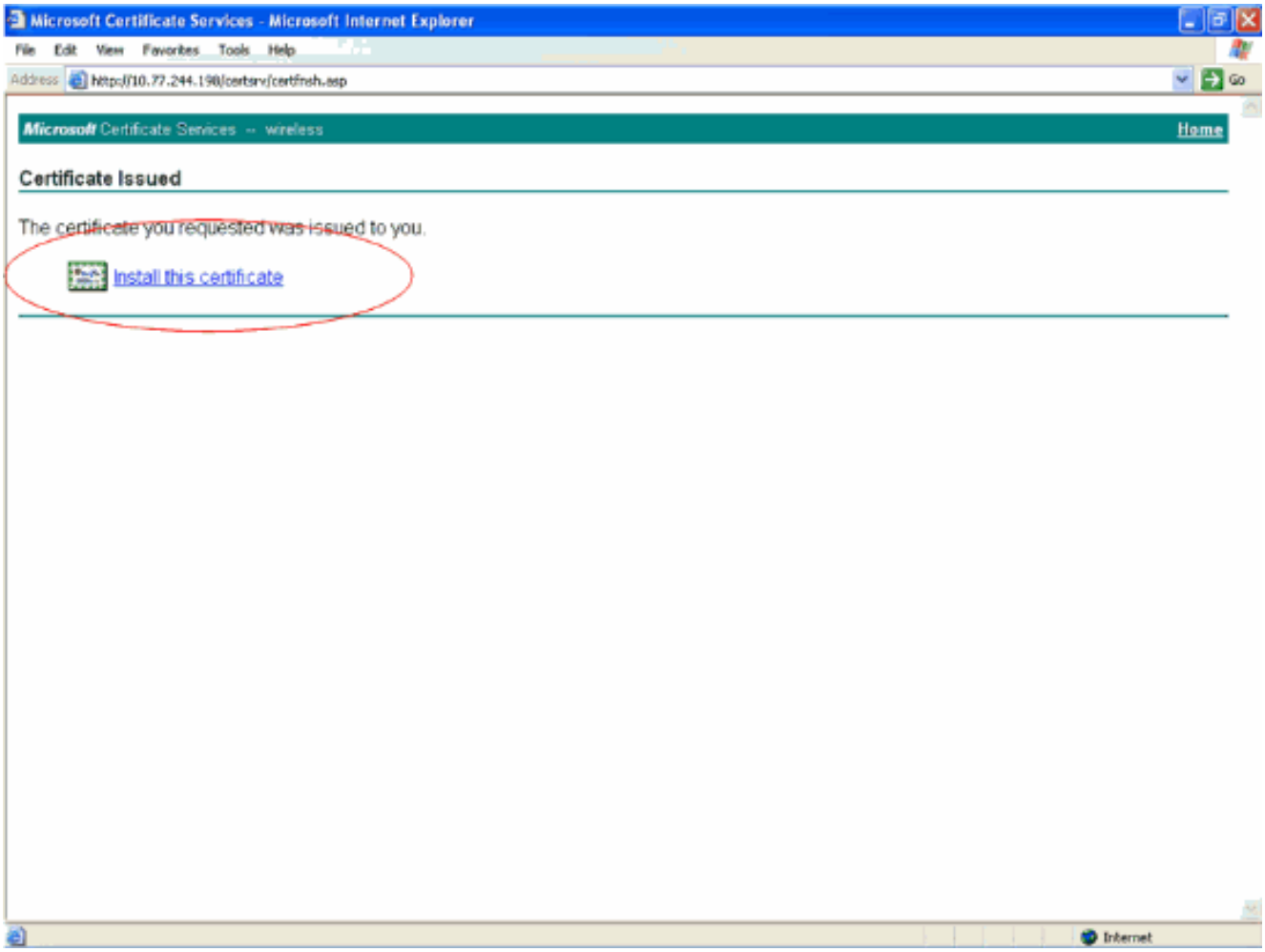
6. 기타 필요한 필드를 모두 구성하고 Submit(제출)을 **클릭합니다**

.



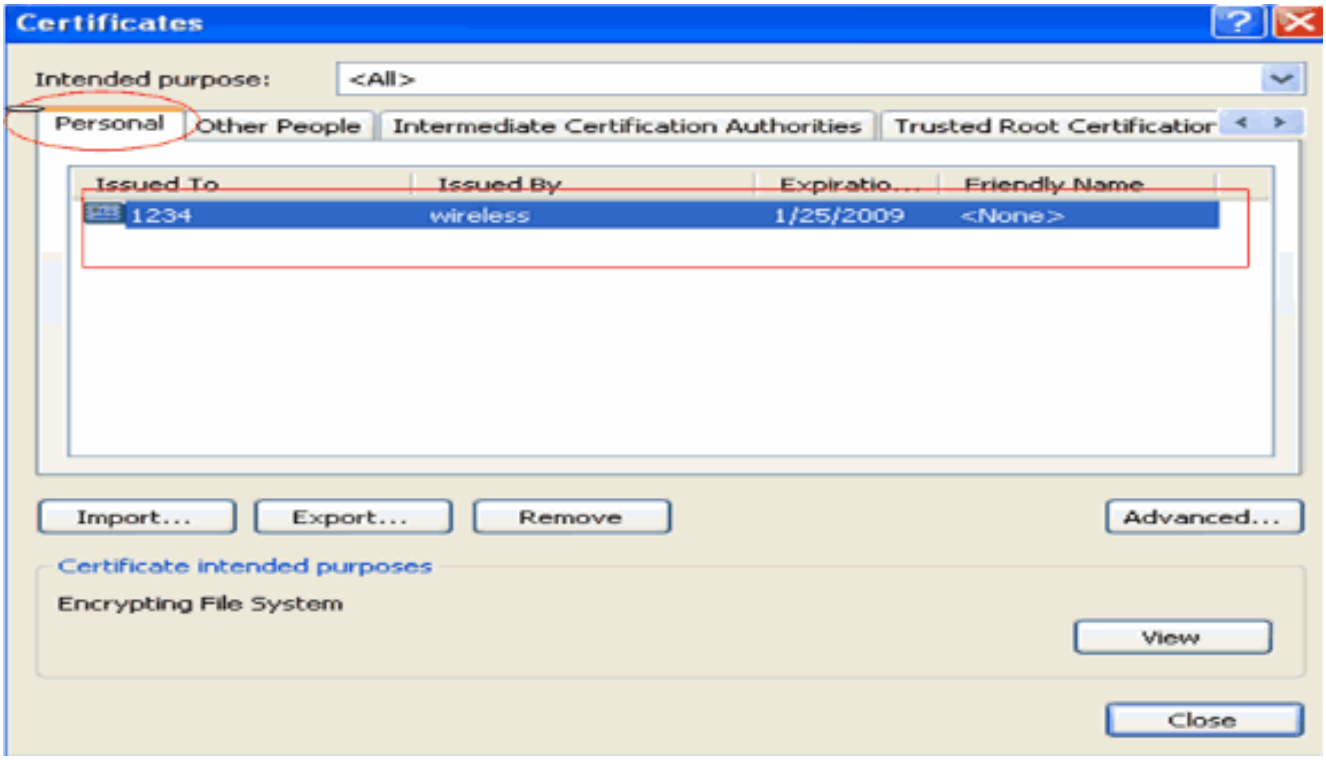
7. 이제 요청에 따라 클라이언트의 디바이스 인증서가 생성됩니다. 인증서 **저장소에 인증서**를 설치하려면 Install the certificate를 클릭합니다

.



8. 클라이언트의 IE 브라우저에서 **Tools > Internet Options > Content > Certificates**의 Personal certificate 목록 아래에 설치된 클라이언트의 디바이스 인증서를 찾을 수 있습니다

.



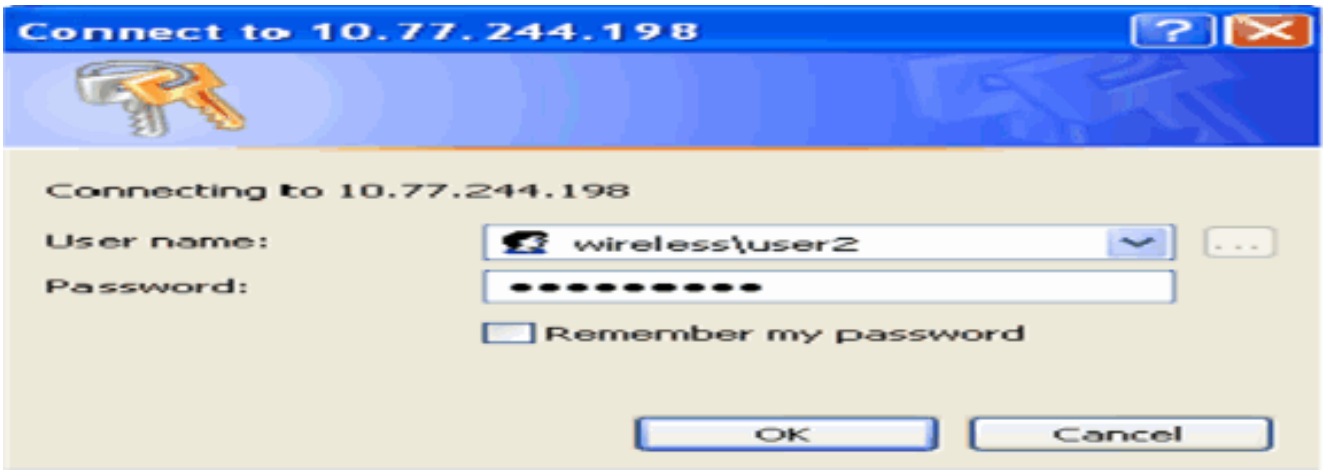
클라이언트에 대한 디바이스 인증서가 클라이언트에 설치됩니다.

클라이언트에 대한 루트 CA 인증서 생성

다음 단계는 클라이언트에 대한 CA 인증서를 생성하는 것입니다. 클라이언트 PC에서 다음 단계를 완료합니다.

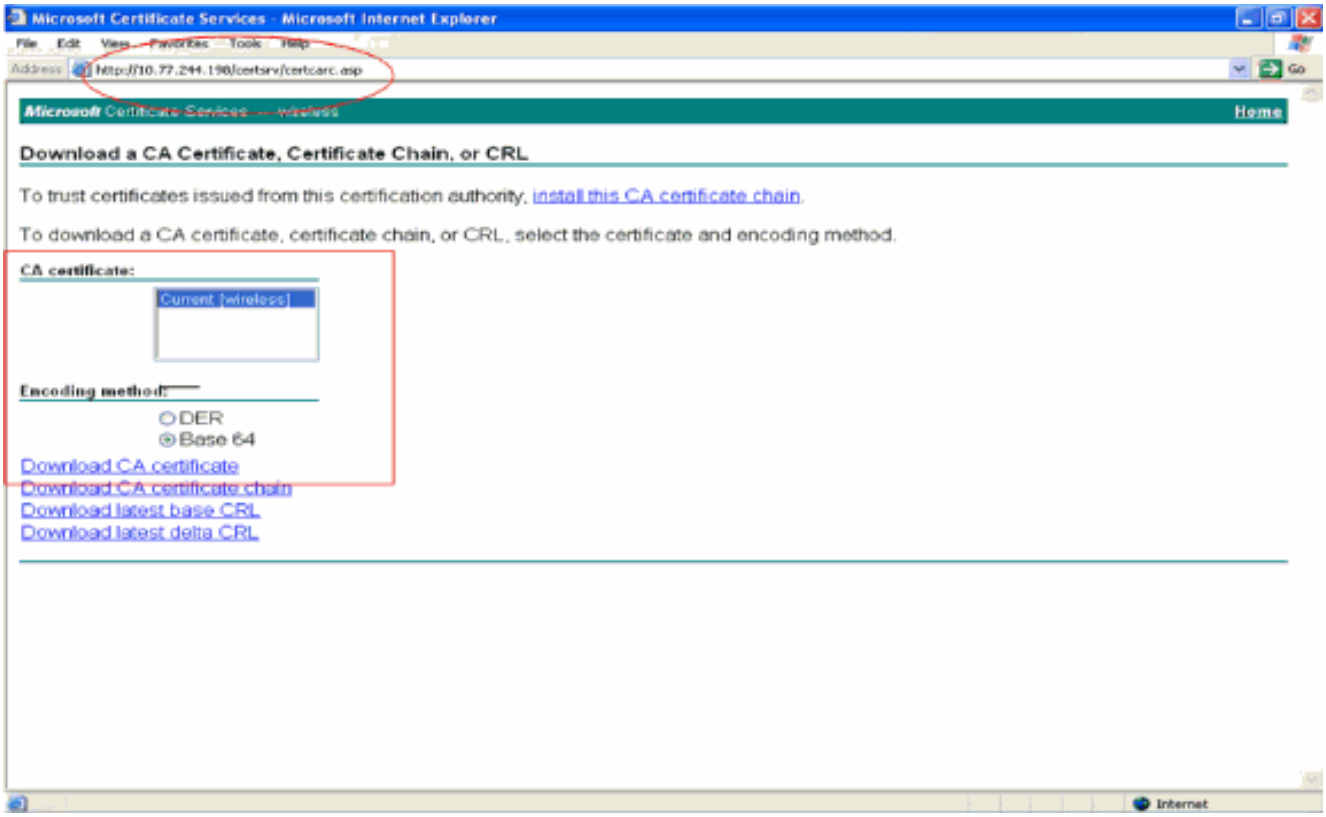
1. 인증서를 설치해야 **하는 클라이언트**에서 http://**<CA 서버**의 **IP 주소>/**certsrv로 이동합니다. CA 서버에 domain name\username으로 로그인합니다. 사용자 이름은 이 XP 시스템을 사용하는 사용자의 이름이어야 하며, 사용자는 CA 서버와 동일한 도메인의 일부로 이미 구성되어 있어야 합니다

   .



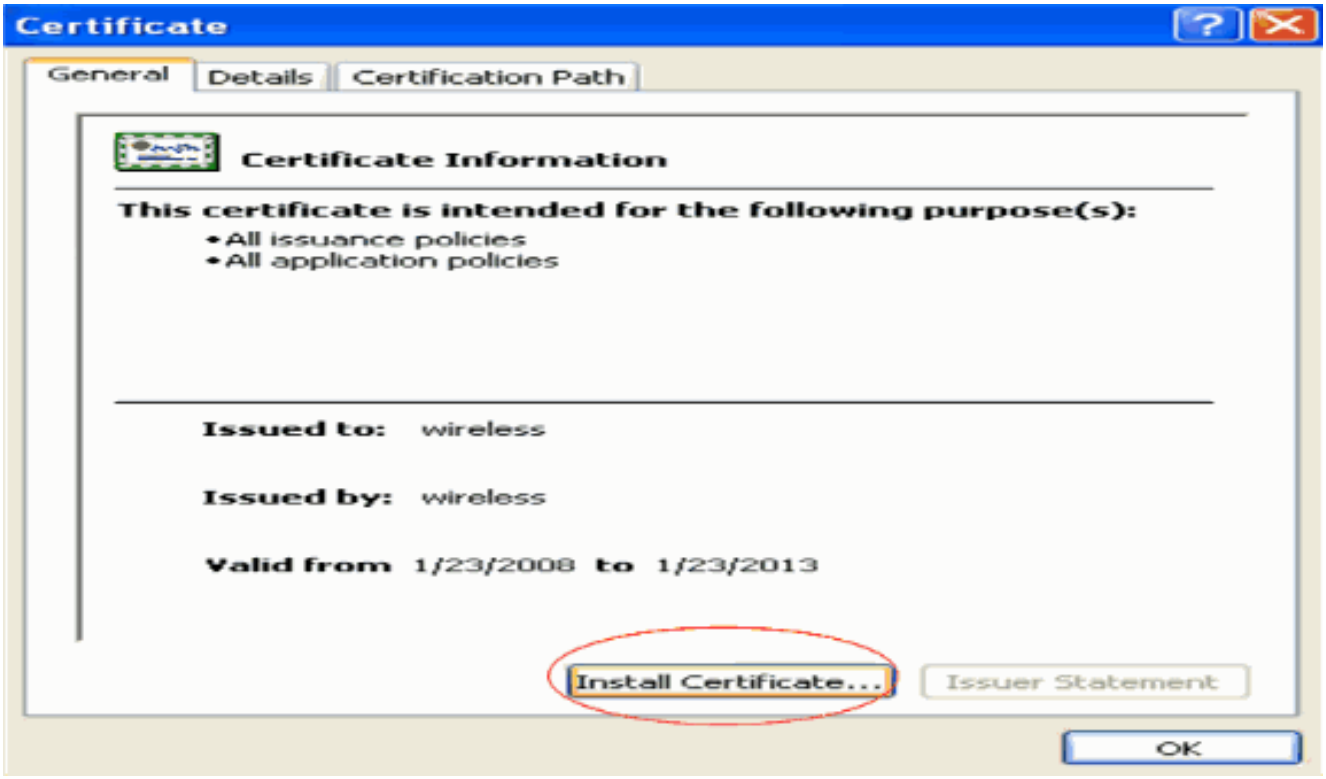
2. 결과 페이지에서 CA 서버에서 사용 가능한 현재 CA 인증서를 CA **인증서** 상자 아래에 볼 수 있습니다. 인코딩 **방법**으로 **Base 64**를 선택합니다. 그런 다음 **Download CA certificate(CA 인증서 다운로드)**를 클릭하고 클라이언트 PC에 파일을 **.cer 파일로** 저장합니다. 이 예에서는 **rootca.cer**을 파일 이름으로 사용합니다

   .



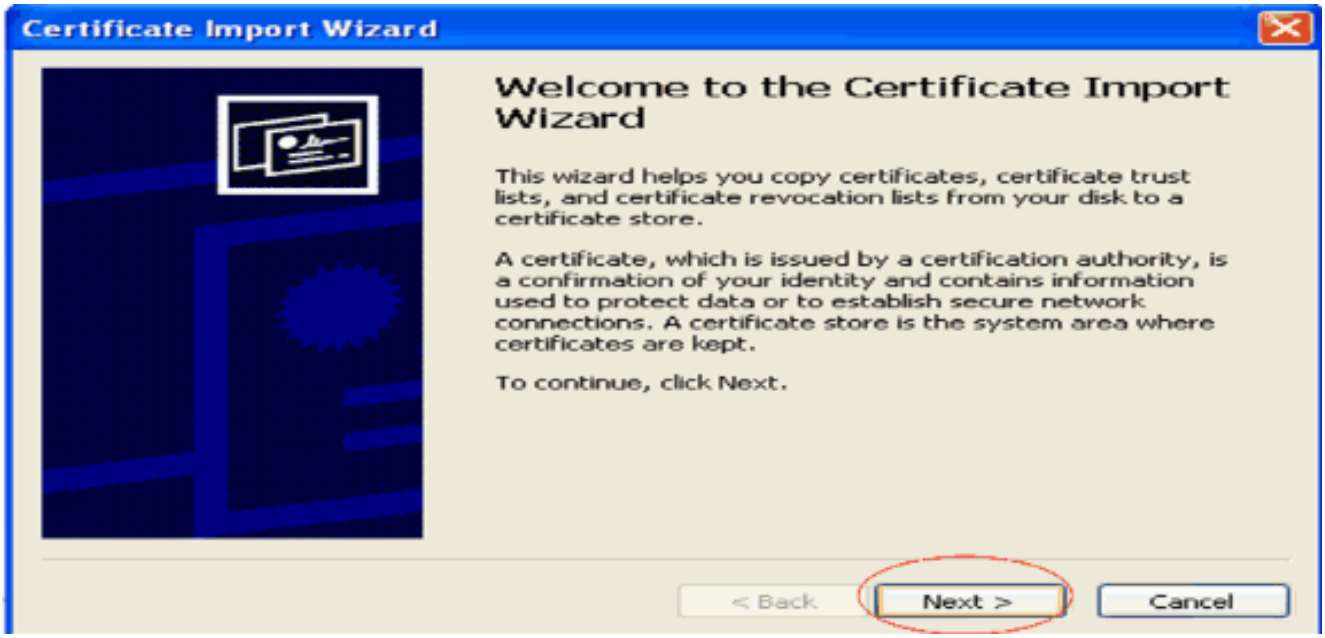
3. 그런 다음 .cer 형식으로 저장된 CA 인증서를 클라이언트의 인증서 저장소에 설치합니다. rootca.cer 파일을 두 번 클릭하고 **Install Certificate(인증서 설치)**를 클릭합니다

   .



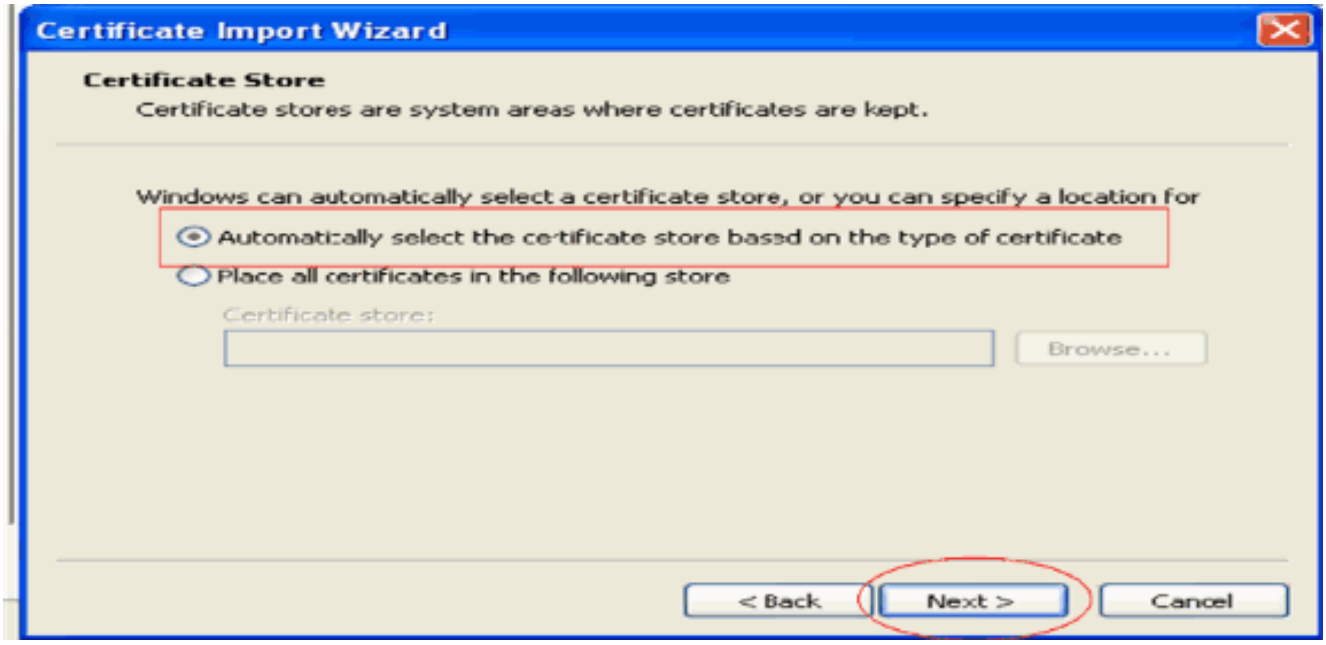
4. 클라이언트의 하드 디스크에서 인증서 저장소로 인증서를 가져오려면 **Next(다음)**를 클릭합니다

.



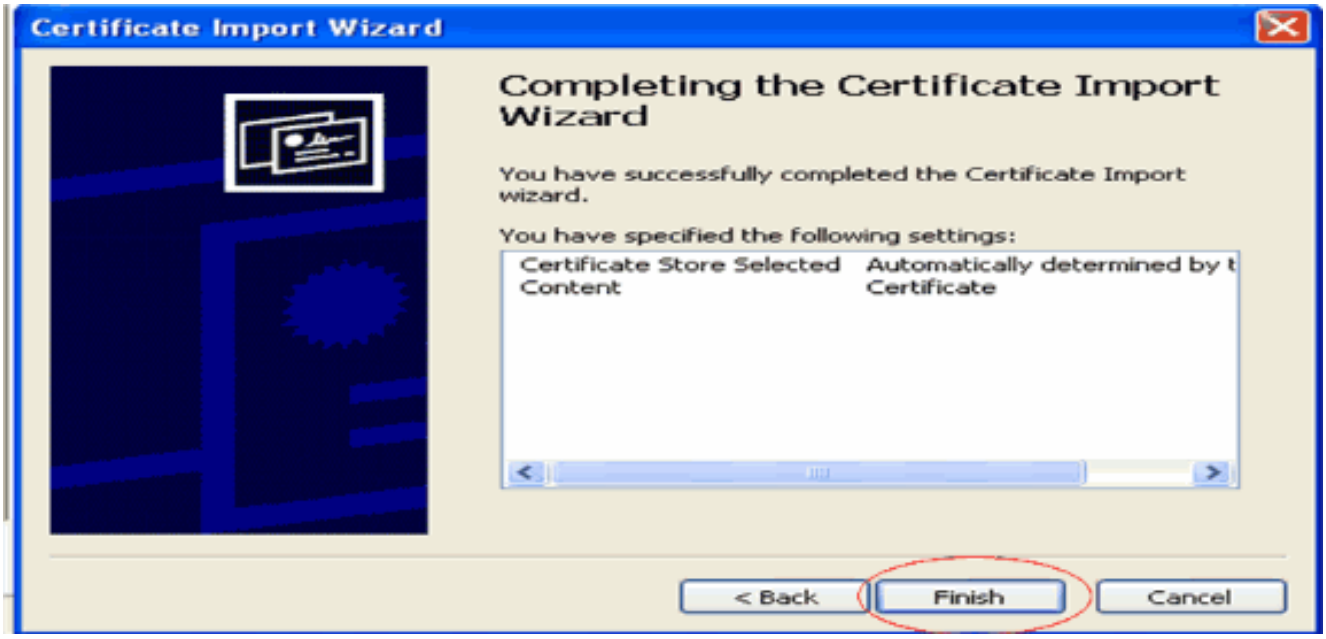
5. Automatically **select the certificate based on the type of certificate(인증서 유형에 따라 자동으로 인증서 저장소 선택)를 선택하고 Next(다음)**를 클릭합니다

.



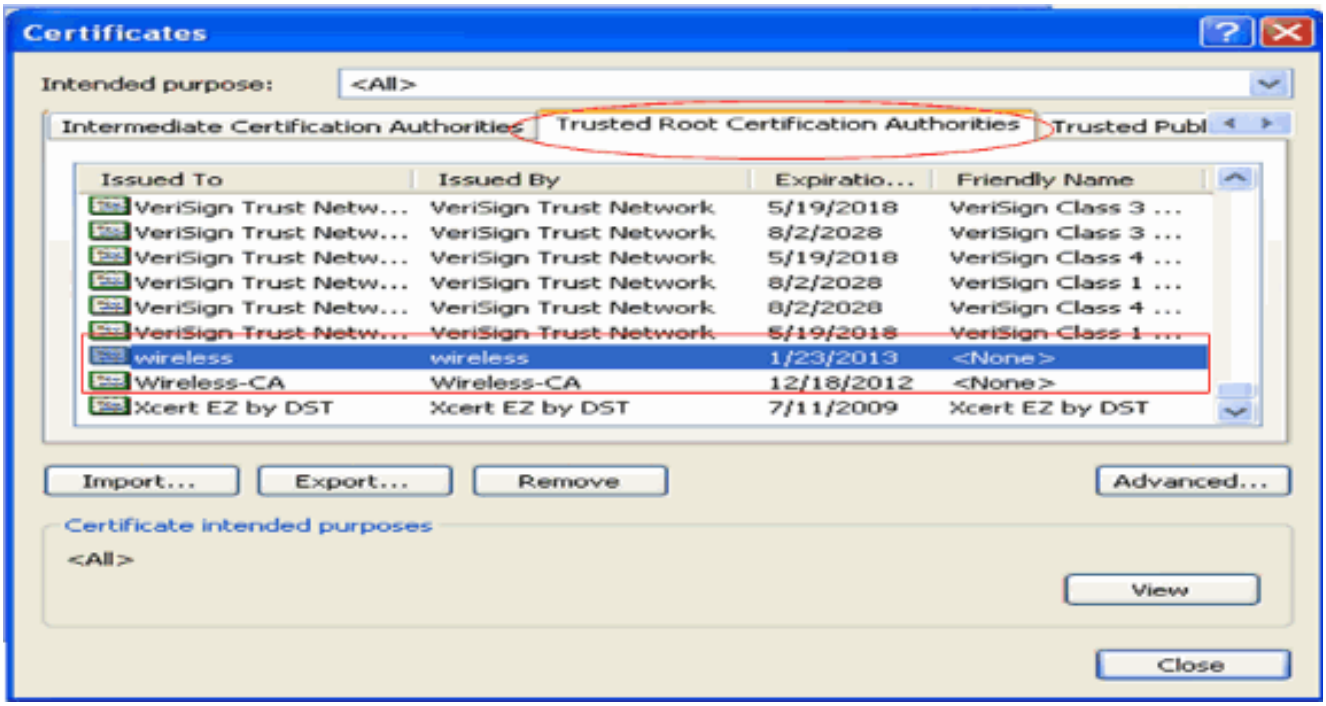
6. Finish(**마침**)를 클릭하여 가져오기 프로세스를 완료합니다

.



7. 기본적으로 CA 인증서는 클라이언트 IE 브라우저의 Tools(**툴**) **> Internet Options(인터넷 옵션) > Content(콘텐츠) > Certificates(인증서)**에서 Trusted Root Certification Authorities(신뢰할 수 있는 루트 인증 기관) 목록 아래에 설치됩니다. 예를 들면 다음과 같습니다

.



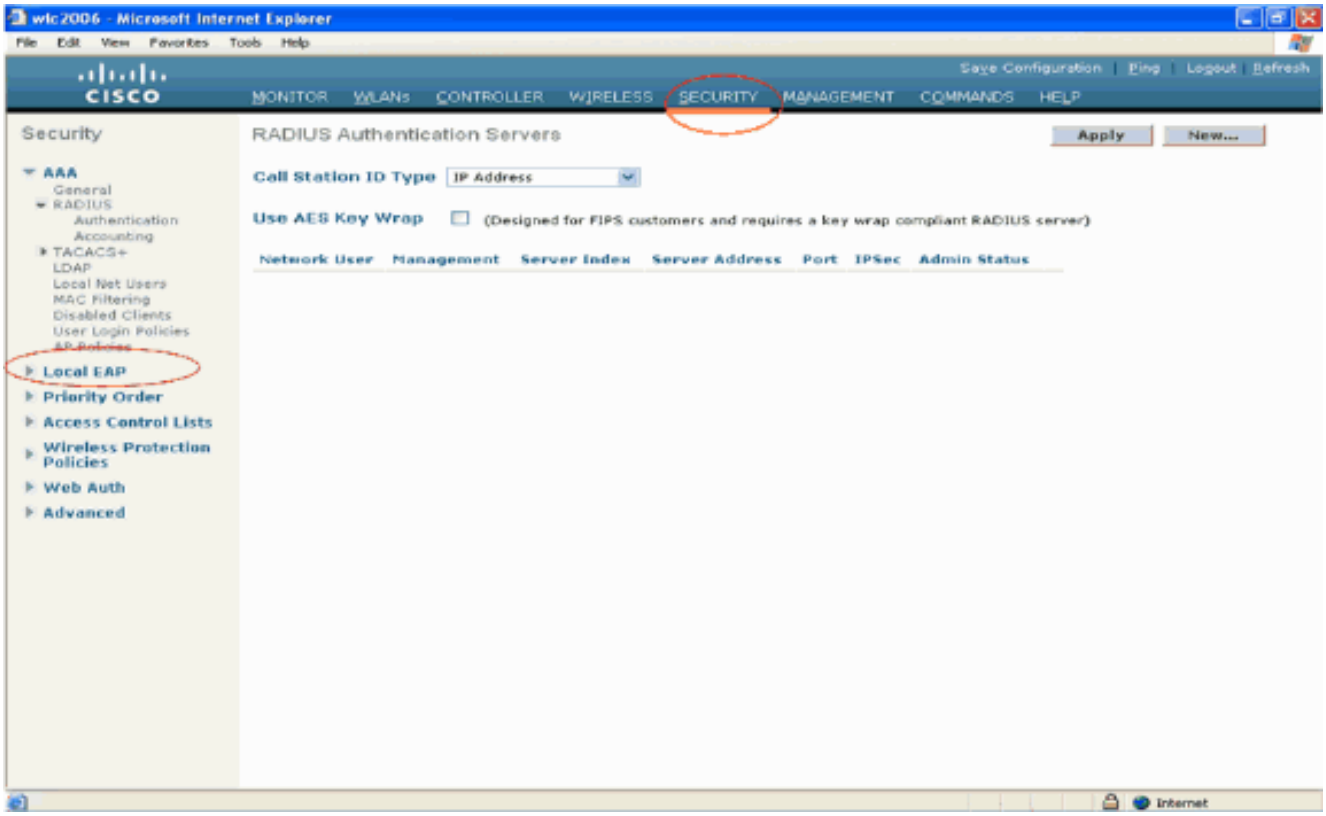
필요한 모든 인증서는 WLC뿐만 아니라 EAP-FAST 로컬 EAP 인증을 위한 클라이언트에 설치됩니다. 다음 단계는 로컬 EAP 인증을 위해 WLC를 구성하는 것입니다.

WLC에서 로컬 EAP 구성

WLC에서 로컬 **EAP 인증을** 구성하려면 WLC **GUI** 모드에서 다음 단계를 완료합니다.

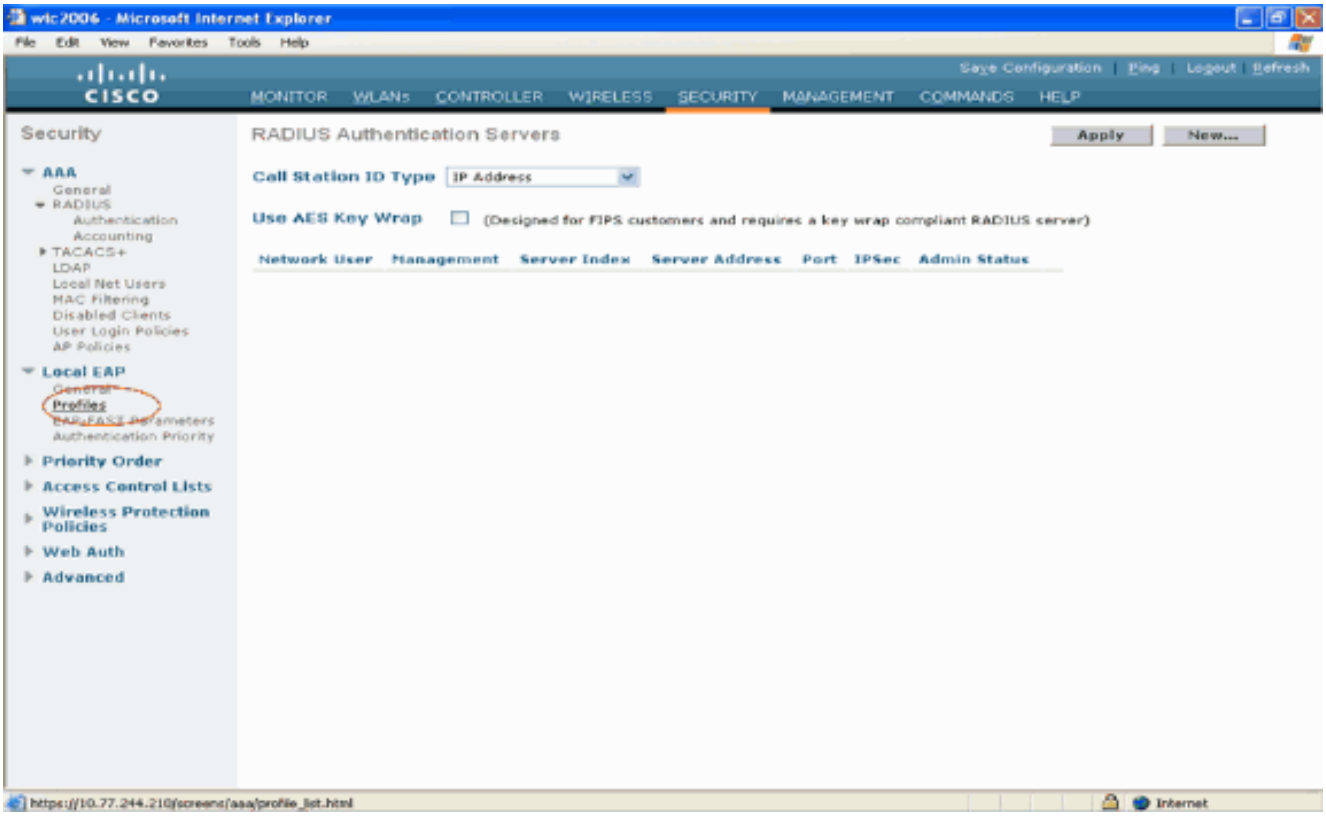
1. Security(**보안) > Local EAP(로컬 EAP)를 클릭합니다**

.



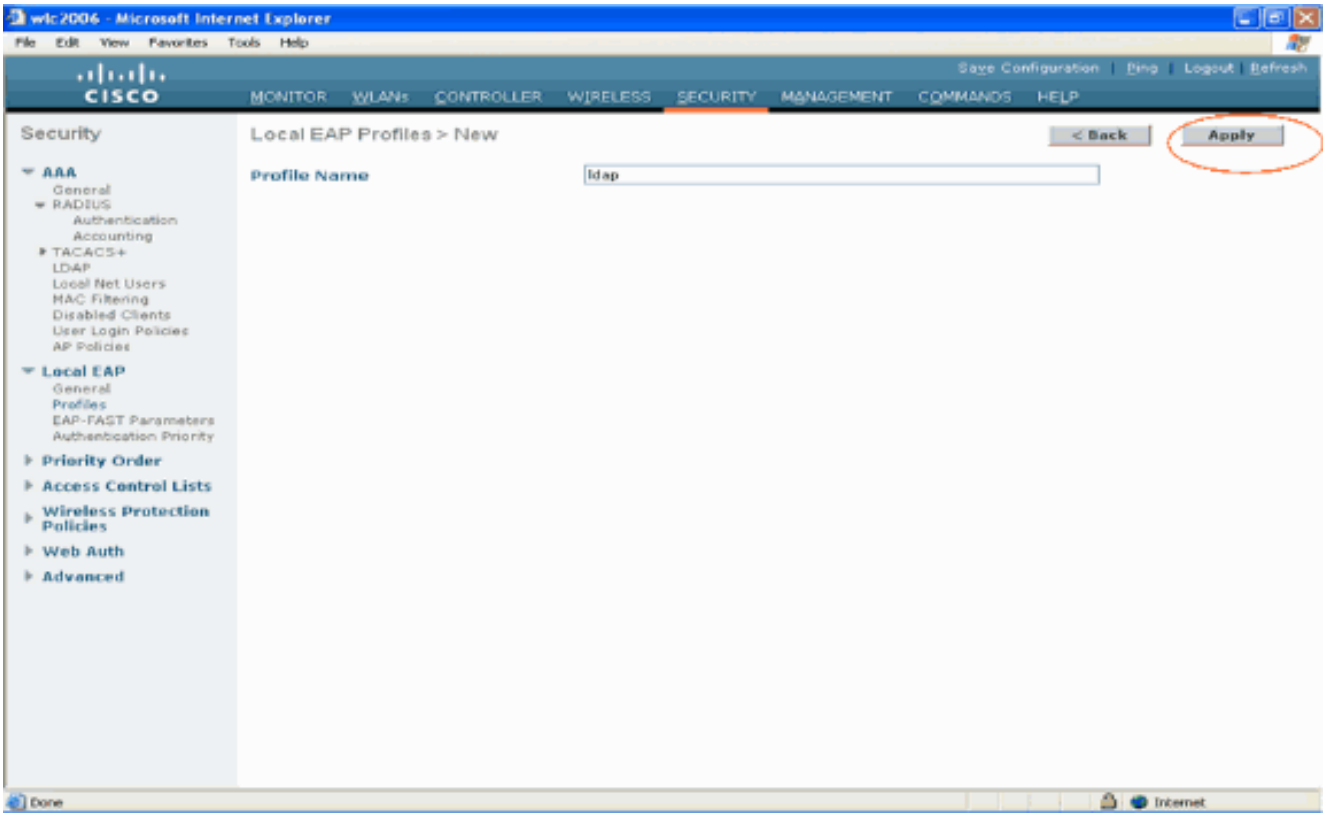
2. Local EAP(로컬 EAP)에서 **Profiles(**프로파일)를 클릭하여 로컬 EAP 프로파일을 구성합니다

.



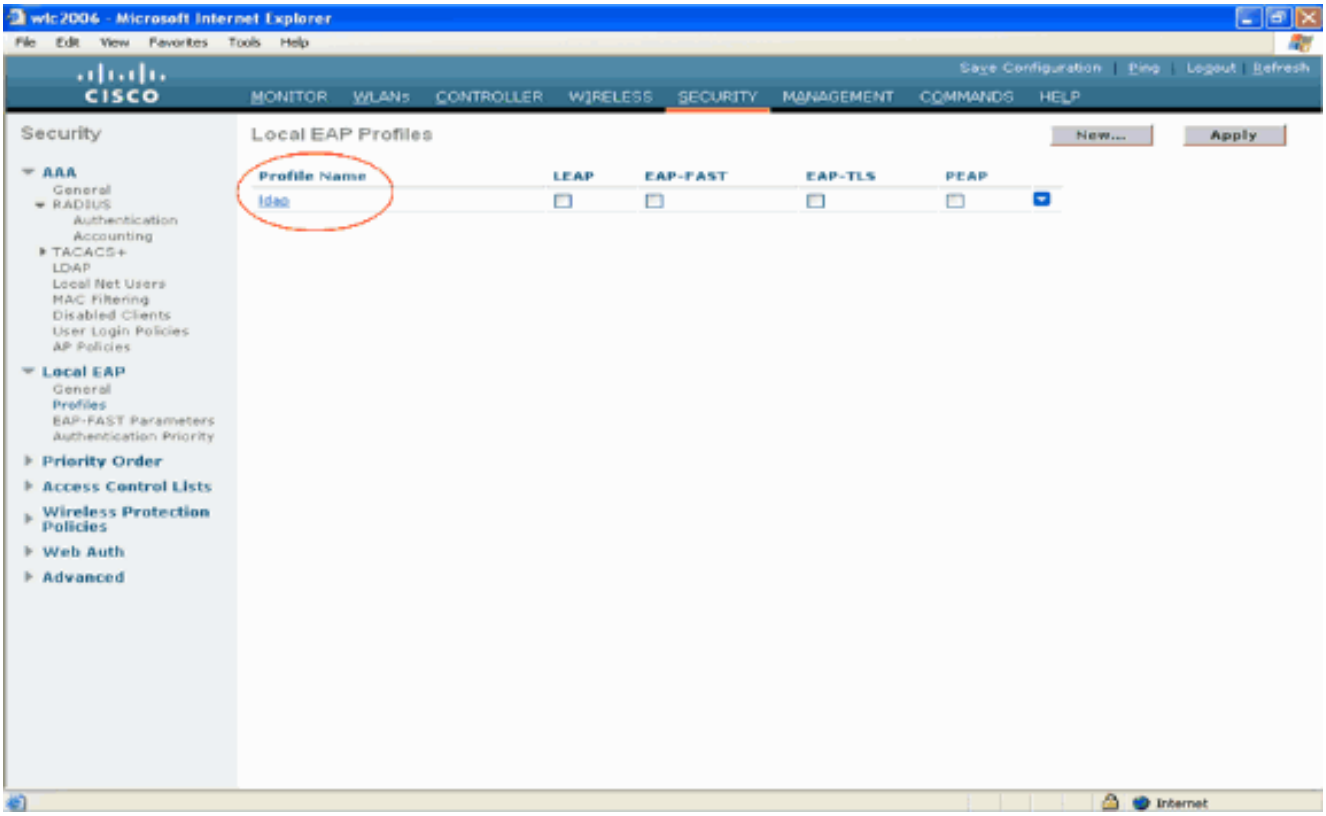
3. 새 **로컬** EAP 프로파일을 생성하려면 New(새로 만들기)를 클릭합니다.
4. 이 프로필의 이름을 구성하고 Apply를 **클릭합니다**. 이 예에서 프로파일 이름은 **ldap입니다**. 이렇게 하면 WLC에서 생성된 로컬 EAP 프로필로 이동합니다

.



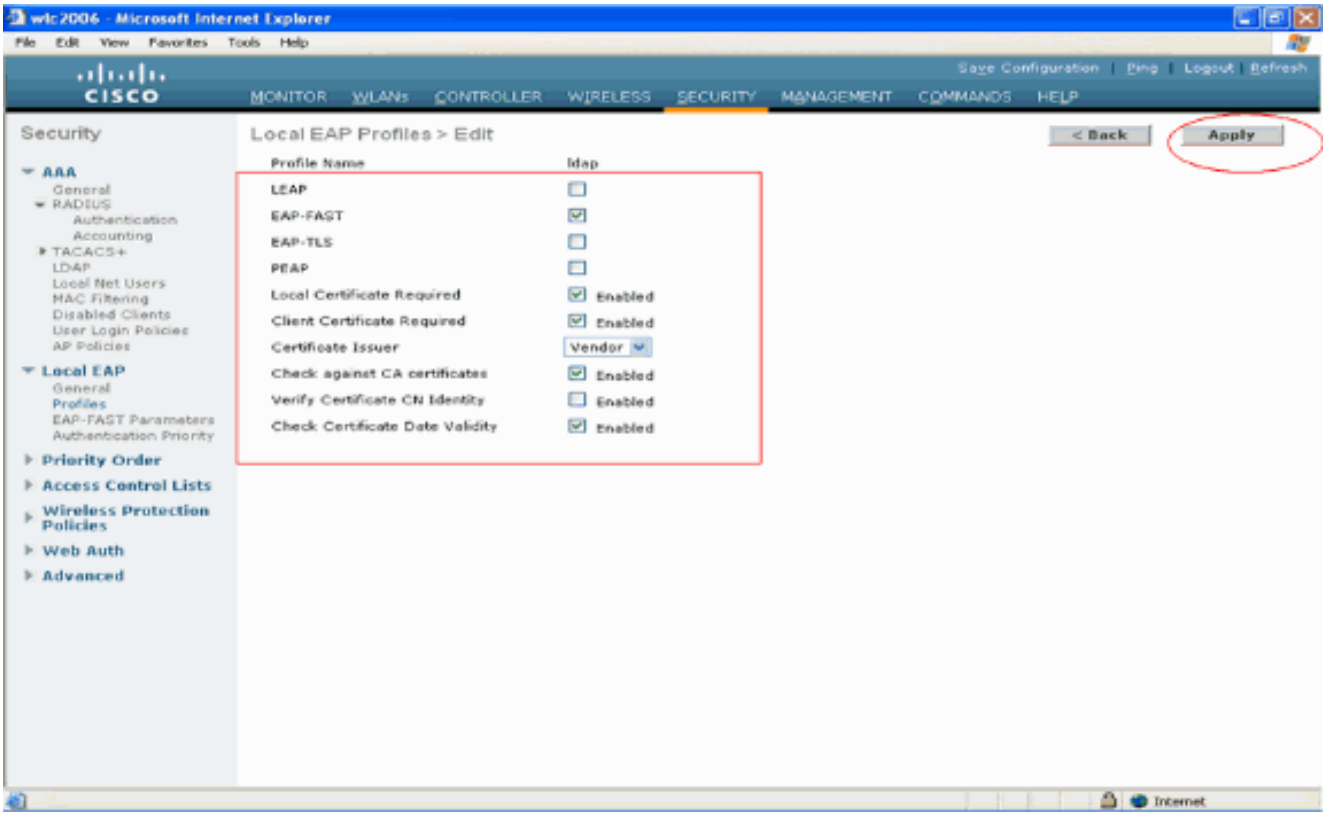
5. Local EAP **Profiles**(로컬 EAP 프로파일) 페이지의 Profile Name(프로파일 이름) 필드 아래에 나타나는 방금 생성한 LDAP 프로파일을 클릭합니다. 그러면 Local EAP Profiles(로컬 EAP **프로파일) > Edit(수정) 페이지로** 이동합니다

.



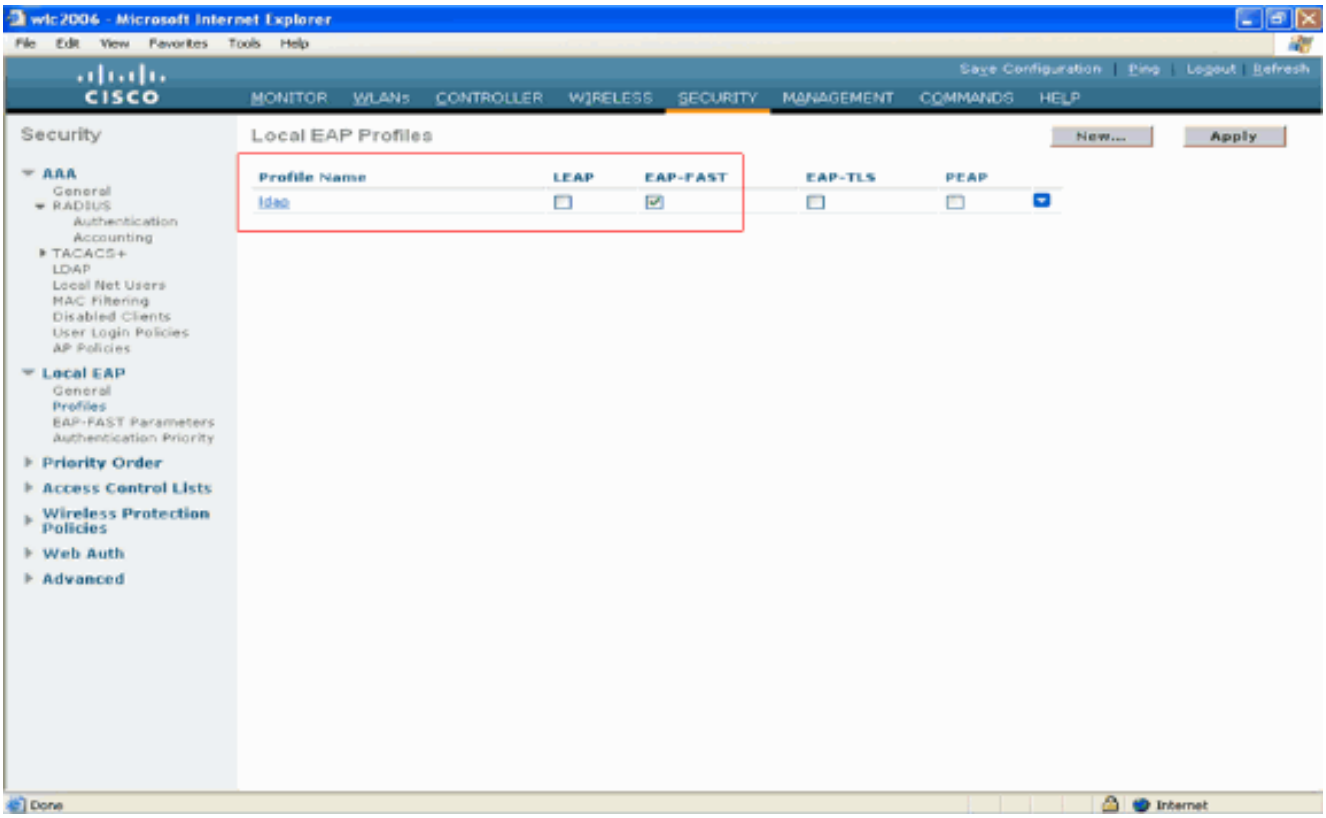
6. Local EAP Profiles(로컬 EAP 프로파일) **> Edit(편집) 페이지에서** 이 **프로파일에** 특정한 **매개 변수를** 구성합니다.로컬 **EAP** 인증 방법으로 EAP-FAST를 선택합니다.Local Certificate Required(로컬 인증서 필요) **및 Client Certificate Required(클라이언트 인증서 필요) 옆**의 **확인란을 활성화합니다**.이 **문서**는 서드파티 CA 서버를 사용하므로 Vendor(벤더)를 Certificate Issuer(인증서 발급자)로 선택합니다.클라이언트의 수신 인증서가 컨트롤러**의 CA 인증서**에 대해 검증되도록 하려면 Check against CA certificates 옆에 있는 확인란을 활성화합니다.수신 인증서의 CN(Common Name)을 컨트롤러의 CA 인증서 CN에 대해 검증하려면 **Verify Certificate CN Identity 확인란**을 선택합니다. 기본 설정은 비활성화되어 있습니다. 컨트롤러에서 수신 장치 인증서가 여전히 유효하고 만료되지 않았는지 확인할 수 있도록 하려면 Check Certificate Date Validity(인증서 **날짜 유효성 확인) 확인란**을 선택합니다.**참고:** 인증서 날짜 유효성은 컨트롤러에 구성된 현재 UTC(GMT) 시간을 기준으로 확인됩니다. 표준 시간대 오프셋은 무시됩니다.Apply를 **클릭합니다**

.



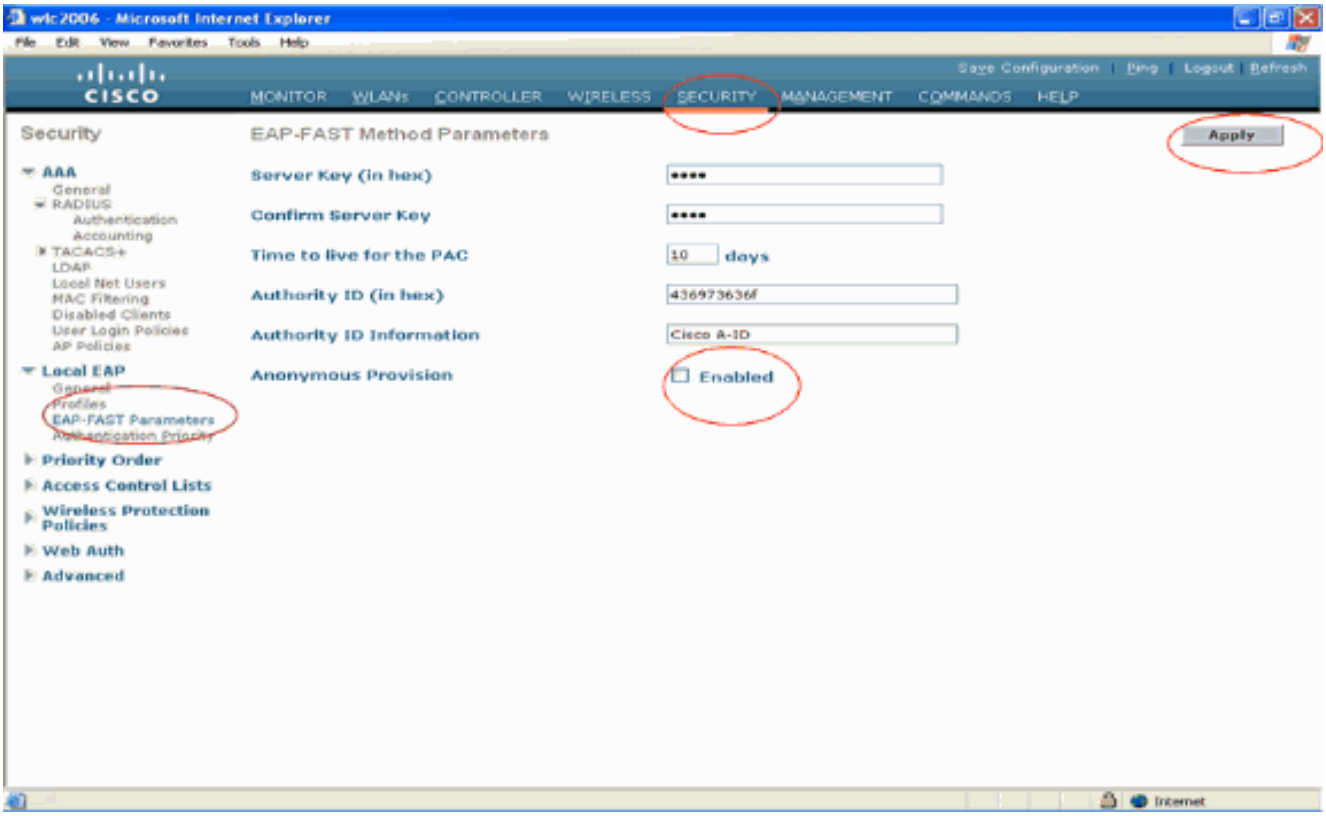
7. 이제 EAP-FAST 인증을 사용하는 로컬 EAP 프로파일이 WLC에 생성됩니다

.



8. 다음 단계는 WLC에서 EAP-FAST 관련 매개변수를 구성하는 것입니다. WLC Security(WLC 보안) 페이지에서 **Local EAP(로컬 EAP) > EAP-FAST Parameters(EAP-**FAST 매개변수)를 클릭하여 EAP-FAST Method Parameters(EAP-FAST 방법 매개변수) 페이지로 이동합니다.이 예에서는 **인증서를** 사용하는 EAP-FAST에 대해 설명하므로 Anonymous Provision(익명 프로비저닝) 확인란의 선택을 취소합니다. 다른 모든 매개변수는 기본값으로 둡니다. Apply를 **클릭합니다**

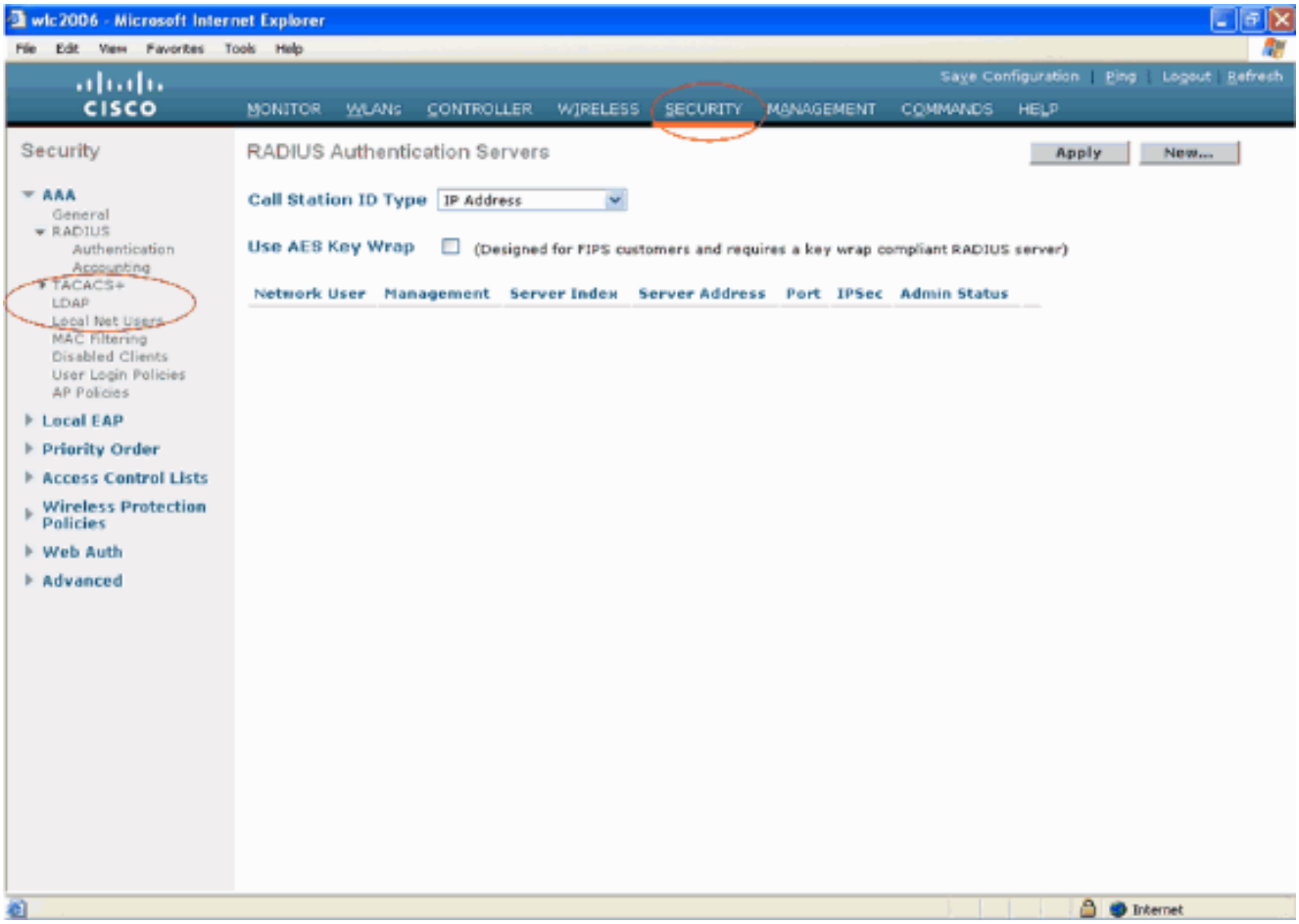
.



LDAP 서버 세부 정보로 WLC 구성

이제 WLC가 로컬 EAP 프로파일 및 관련 정보로 구성되었으므로 다음 단계는 LDAP 서버의 세부사항으로 WLC를 구성하는 것입니다. WLC에서 다음 단계를 완료합니다.

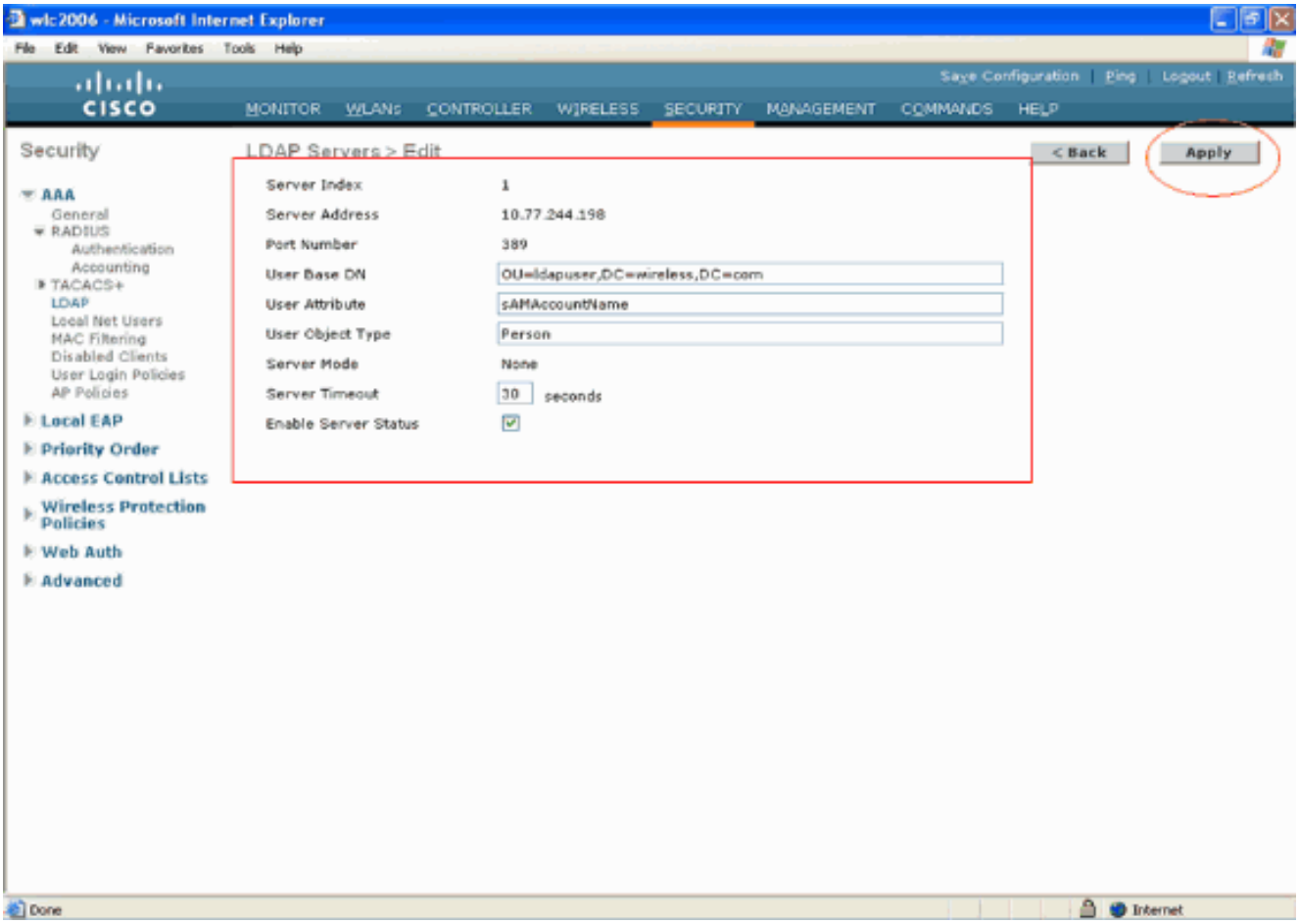
1. WLC의 **Security(보안)** 페이지에서 왼쪽 작업창에서 **AAA > LDAP**를 선택하여 LDAP 서버 컨피그레이션 페이지로 이동합니다. LDAP 서버를 추가하려면 New(새로 만들기)를 **클릭합니다**. LDAP **Servers(LDAP 서버) > New(새)** 페이지가 나타납니다
.



2. LDAP Servers Edit(LDAP 서버 수정) 페이지에서 LDAP 서버의 IP 주소, Port Number(포트 번호), Enable Server status(서버 활성화 상태) 등과 같은 LDAP 서버의 세부 정보를 지정합니다 .**Server Index (Priority)(서버 인덱스(우선순위))** 드롭다운 상자에서 숫자를 선택하여 구성된 다른 LDAP 서버와 관련하여 이 서버의 우선순위를 지정합니다. 최대 17개의 서버를 구성할 수 있습니다. 컨트롤러가 첫 번째 서버에 도달할 수 없는 경우 목록의 두 번째 서버에 연결하는 등의 작업을 시도합니다.Server IP Address 필드에 LDAP 서버의 **IP 주소를** 입력합니다.Port Number(포트 번호) 필드에 LDAP 서버의 TCP **포트 번호를** 입력합니다. 유효한 범위는 1~65535이며 기본값은 **389**입니다.**User Base DN** 필드에서 모든 사용자 목록이 포함된 LDAP 서버에 있는 하위 트리의 DN(Distinguished Name)을 입력합니다. 예를 들어, ou=조직 단위, .ou=다음 조직 단위 및 o=corporation.com입니다. 사용자를 포함하는 트리가 기본 DN인 경우 o=corporation.com 또는 dc=corporation, dc=com을 입력합니다.이 예에서 사용자는 OU(Organizational Unit) **ldapuser**에 있으며, 이 OU는 **Wireless.com 도메인**의 일부로 생성됩니다.사용자 기본 DN은 사용자 정보(EAP-FAST 인증 방법에 따른 사용자 자격 증명)가 있는 전체 경로를 가리켜야 합니다. 이 예에서 사용자는 기본 DN OU=ldapuser, DC=Wireless, DC=com 아래에 있습니다.OU와 사용자 구성에 대한 자세한 내용은 이 문서의 도메인 컨트롤러에서 사용자 만들기 섹션에서 설명합니다.**User Attribute(사용자 특성)** 필드에 사용자 이름이 포함된 사용자 레코드의 특성 이름을 입력합니다.레코드를 **사용자로** 식별하는 LDAP objectType 특성의 값을 User Object Type 필드에 입력합니다. 사용자 레코드에는 objectType 특성에 대한 여러 값이 있는 경우가 많습니다. 그중 일부는 사용자에게 고유하고 일부는 다른 객체 유형과 공유됩니다.**참고:** Windows 2003 지원 도구의 일부로 제공되는 LDAP 브라우저 유틸리티를 사용하여 디렉토리 서버에서 이 두 필드의 값을 가져올 수 있습니다. **이 Microsoft LDAP 브라우저 도구를 LDP라고 합니다.** 이 도구를 사용하면 이 특정 사용자의 User Base DN, User Attribute 및 User Object Type 필드를 알 수 있습니다. LDP를 사용하여 이러한 사용자별 특성을 아는 방법에 대한 자세한 내용은 이 문서의 LDP를 사용하여 사용자 특성 식별 섹션에서 설명합니다.모든 **LDAP 트랜잭션**에서 보안 TLS 터널을 사용하려면 Server Mode(서버 모드) 드롭다운 상자에서 Secure(보안)를 선택합니다. 그렇지 않은 경우 기본 설정인 **None**을

선택합니다.**Server** Timeout(**서버 시간 제한**) 필드에 재전송 간격(초)을 입력합니다. 유효한 범위는 2~30초이며 기본값은 2초입니다.Enable **Server Status(서버 상태 활성화**) 확인란을 선택하여 이 LDAP 서버를 활성화하거나 선택을 취소하여 비활성화합니다. 기본값은 disabled입니다.Apply(**적용**)를 클릭하여 변경 사항을 커밋합니다.이 정보로 이미 구성된 예는 다음과 같습니다

.



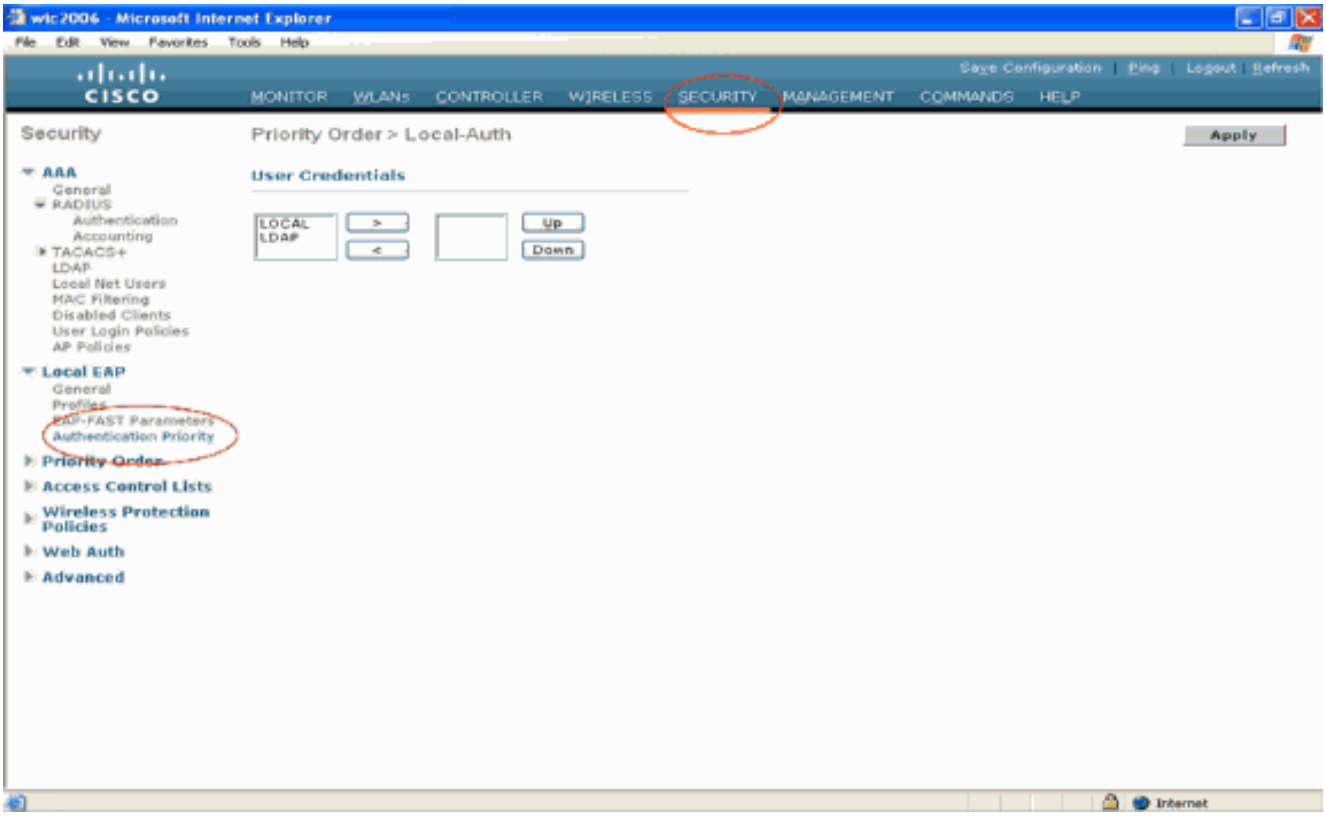
LDAP 서버에 대한 세부 정보가 WLC에 구성되었으므로, 다음 단계는 LDAP를 우선 순위 백엔드 데이터베이스로 구성하여 WLC가 먼저 LDAP 데이터베이스에서 다른 데이터베이스가 아닌 사용자 자격 증명을 찾도록 하는 것입니다.

LDAP를 우선순위 백엔드 데이터베이스로 구성

LDAP를 우선순위 백엔드 데이터베이스로 구성하려면 WLC에서 다음 단계를 완료합니다.

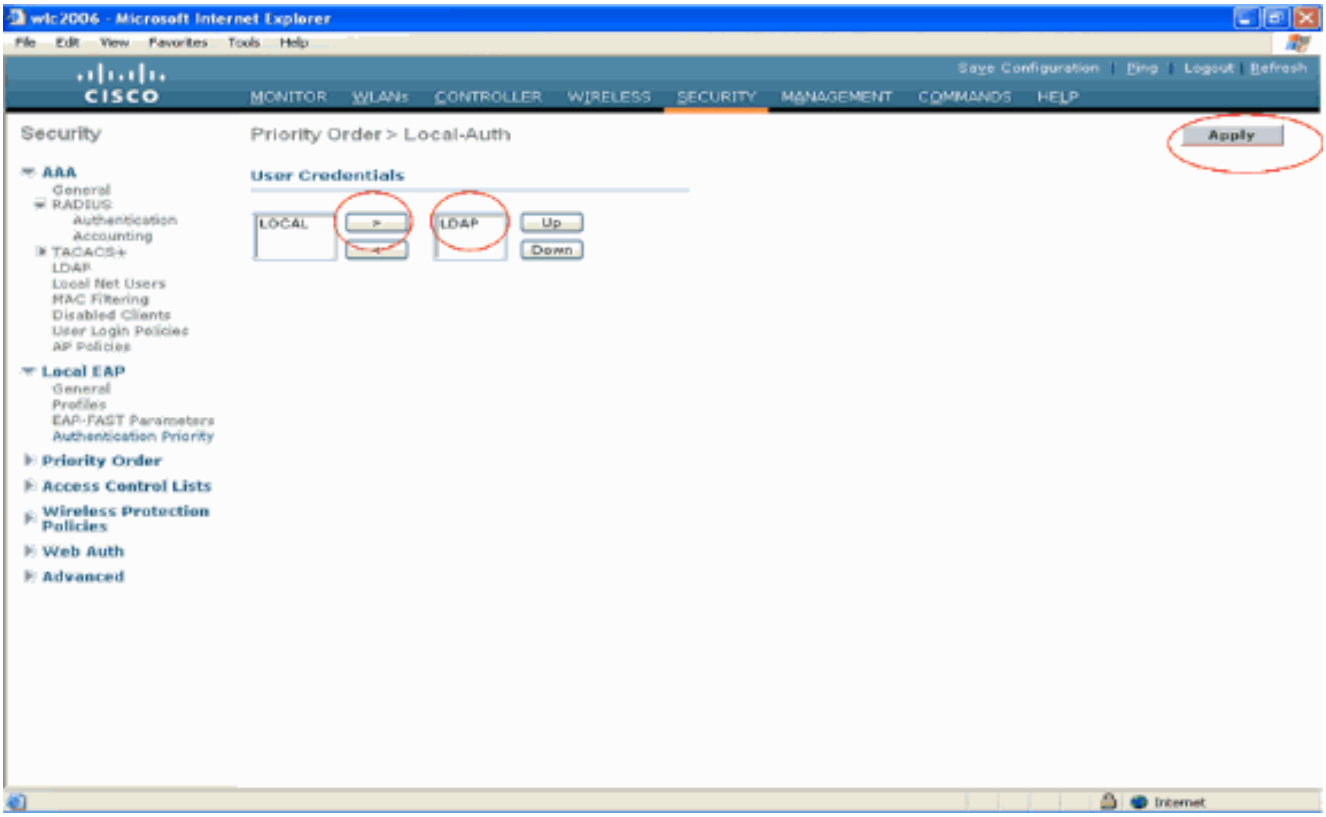
1. Security(보안) 페이지에서 Local EAP(**로컬 EAP) > Authentication Priority(인증 우선순위)를 클릭합니다**. Priority Order(우선순위) > Local-Auth(로컬 인증) 페이지에서 사용자 자격 증명을 저장할 수 있는 두 개의 데이터베이스(로컬 및 LDAP)를 찾을 수 있습니다.LDAP를 우선순위 데이터베이스로 만들려면 왼쪽 사용자 자격 증명 상자에서 LDAP를 선택하고 **> 버튼**을 클릭하여 LDAP를 오른쪽의 우선순위 순서 상자로 이동합니다

.



2. 이 예에서는 왼쪽 상자에서 LDAP가 선택되고 **>** 버튼이 선택된 **것**을 명확하게 보여줍니다. 따라서 LDAP가 우선순위를 결정하는 오른쪽 상자로 이동합니다. LDAP 데이터베이스가 인증 우선순위 데이터베이스로 선택됩니다.Apply를 **클릭합니다**

.



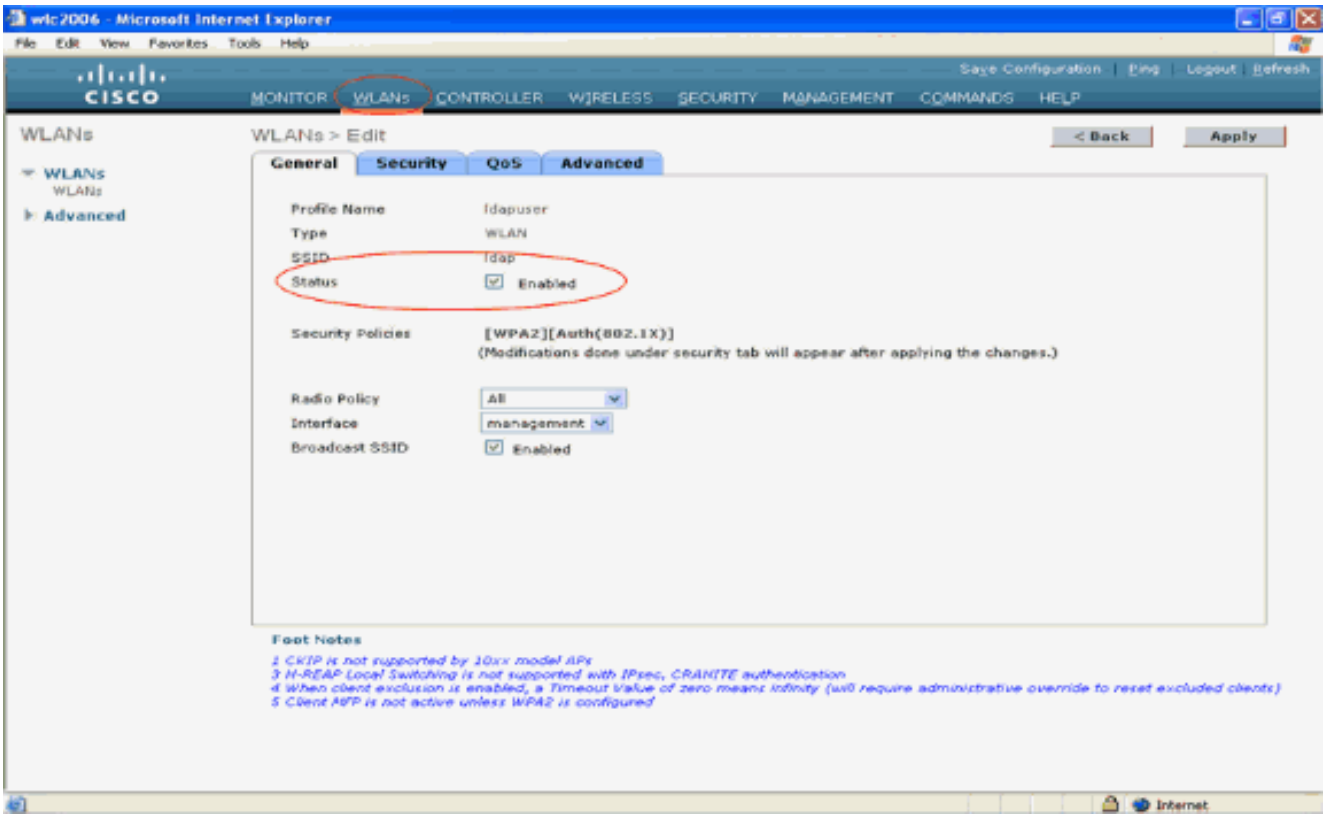
참고: 오른쪽 User Credentials(사용자 자격 증명) 상자에 LDAP와 LOCAL이 모두 표시되고 맨 위에 LDAP가 표시되고 맨 아래에 LOCAL이 표시될 경우, 로컬 EAP는 LDAP 백엔드 데이터베이스를 사용하여 클라이언트를 인증하려고 시도하며 LDAP 서버에 연결할 수 없는 경우 로컬 사용자 데이터베이스로 장애 조치합니다. 사용자를 찾을 수 없는 경우 인증 시도가 거부됩니다. LOCAL이 맨 위에 있는 경우 로컬 EAP는 로컬 사용자 데이터베이스만 사용하여 인증을 시도합니다. LDAP 백엔드 데이터베이스로 장애 조치하지 않습니다.

로컬 EAP 인증을 사용하여 WLC에 WLAN 구성

WLC의 마지막 단계는 로컬 EAP를 인증 방법으로 사용하고 LDAP를 백엔드 데이터베이스로 사용하는 WLAN을 구성하는 것입니다. 다음 단계를 수행합니다.

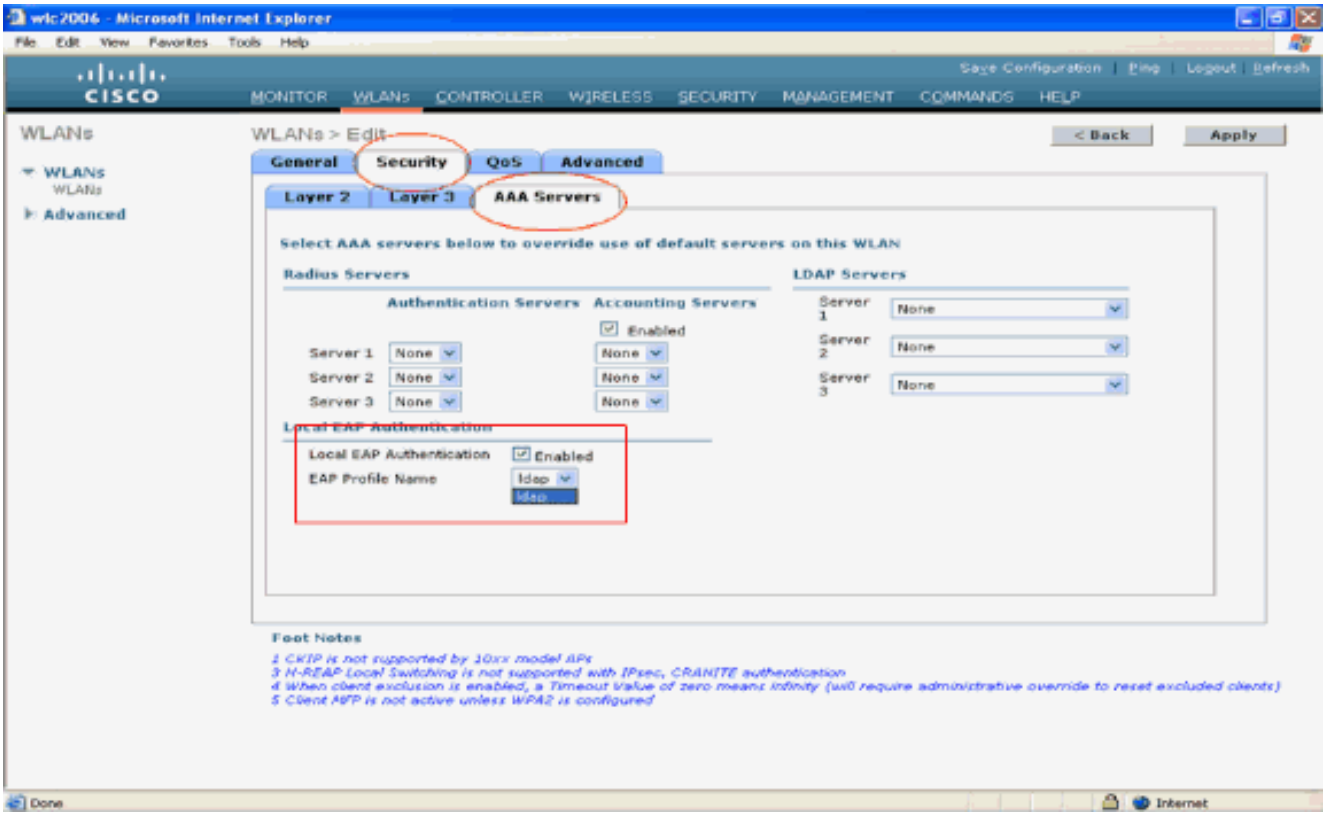
1. Controller Main(컨트롤러 주) 메뉴에서 **WLANs(**WLAN)를 클릭하여 WLANs 컨피그레이션 페이지로 이동합니다. WLANs(WLAN) 페이지에서 **New(새로** 만들기)를 클릭하여 새 WLAN을 생성합니다. 이 예에서는 새 WLAN ldap를 **생성합니다**.Apply(**적용**)를 클릭합니다. 다음 단계는 WLANs(WLAN) > Edit(수정) 페이지에서 WLAN 매개변수를 구성하는 것입니다.
2. WLAN edit(WLAN 수정) 페이지에서 이 WLAN의 상태를 활성화합니다. 기타 필요한 모든 매개변수를 구성합니다

.



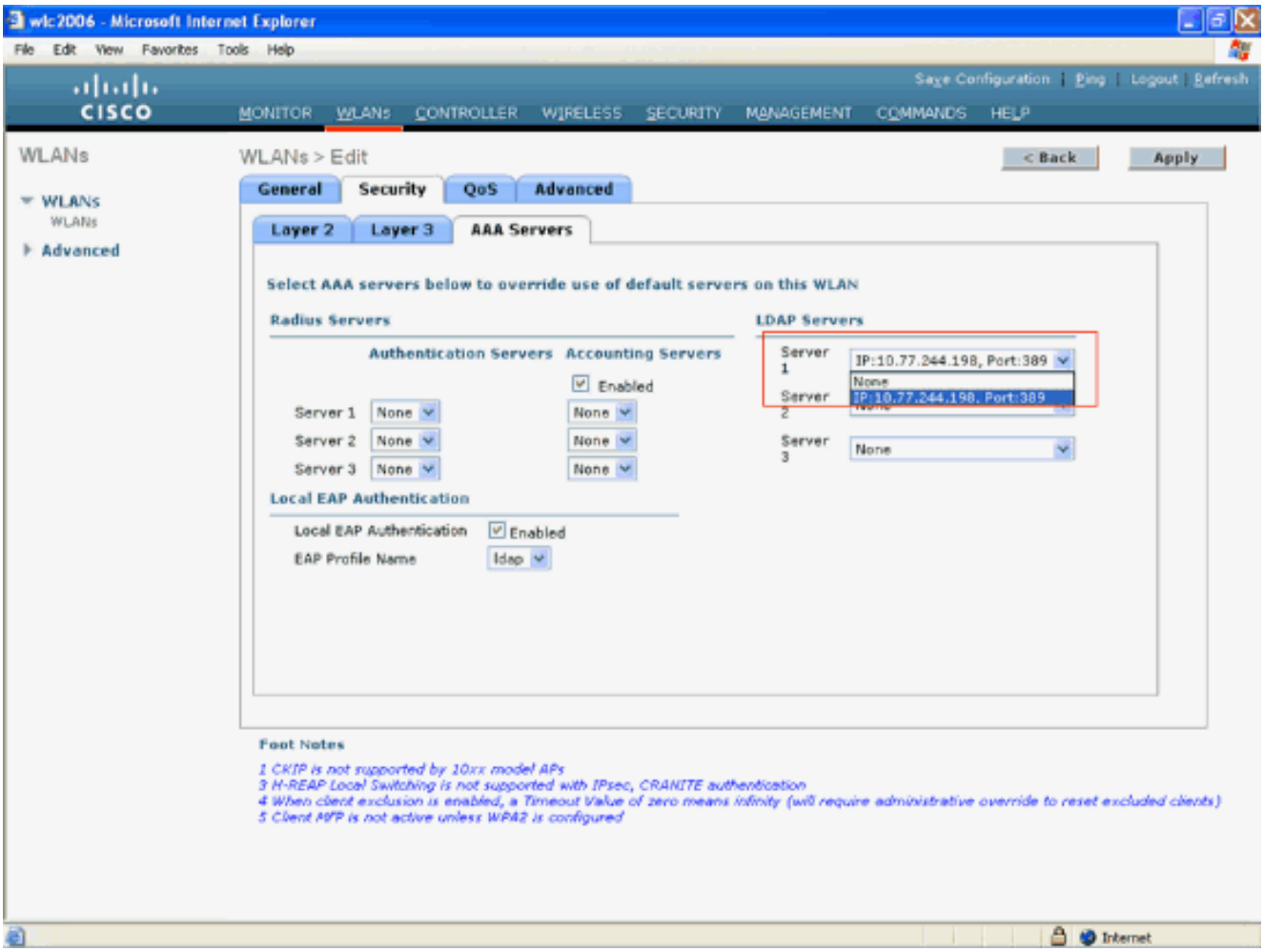
3. 이 **WLAN**에 대한 보안 관련 매개변수를 구성하려면 Security(보안)를 클릭합니다. 이 예에서는 104비트 동적 WEP를 사용하는 802.1x로 레이어 2 보안을 사용합니다.**참고:** 이 문서에서는 동적 WEP가 포함된 802.1x를 예로 사용합니다. WPA/WPA2와 같이 보다 안전한 인증 방법을 사용하는 것이 좋습니다.
4. WLAN Security configuration(WLAN 보안 컨피그레이션) 페이지에서 **AAA servers(AAA 서버) 탭을** 클릭합니다. AAA servers(AAA 서버) 페이지에서 Local EAP Authentication(로컬 EAP 인증) 방법을 활성화하고 EAP Profile Name(EAP 프로파일 이름) 매개변수에 해당하는 드롭다운 상자에서 ldap를 선택합니다. 이 예에서 생성된 로컬 EAP 프로필입니다

.



5. 드롭다운 상자에서 이전에 WLC에 구성된 LDAP 서버를 선택합니다. WLC에서 LDAP 서버에 연결할 수 있는지 확인합니다.Apply를 **클릭합니다**

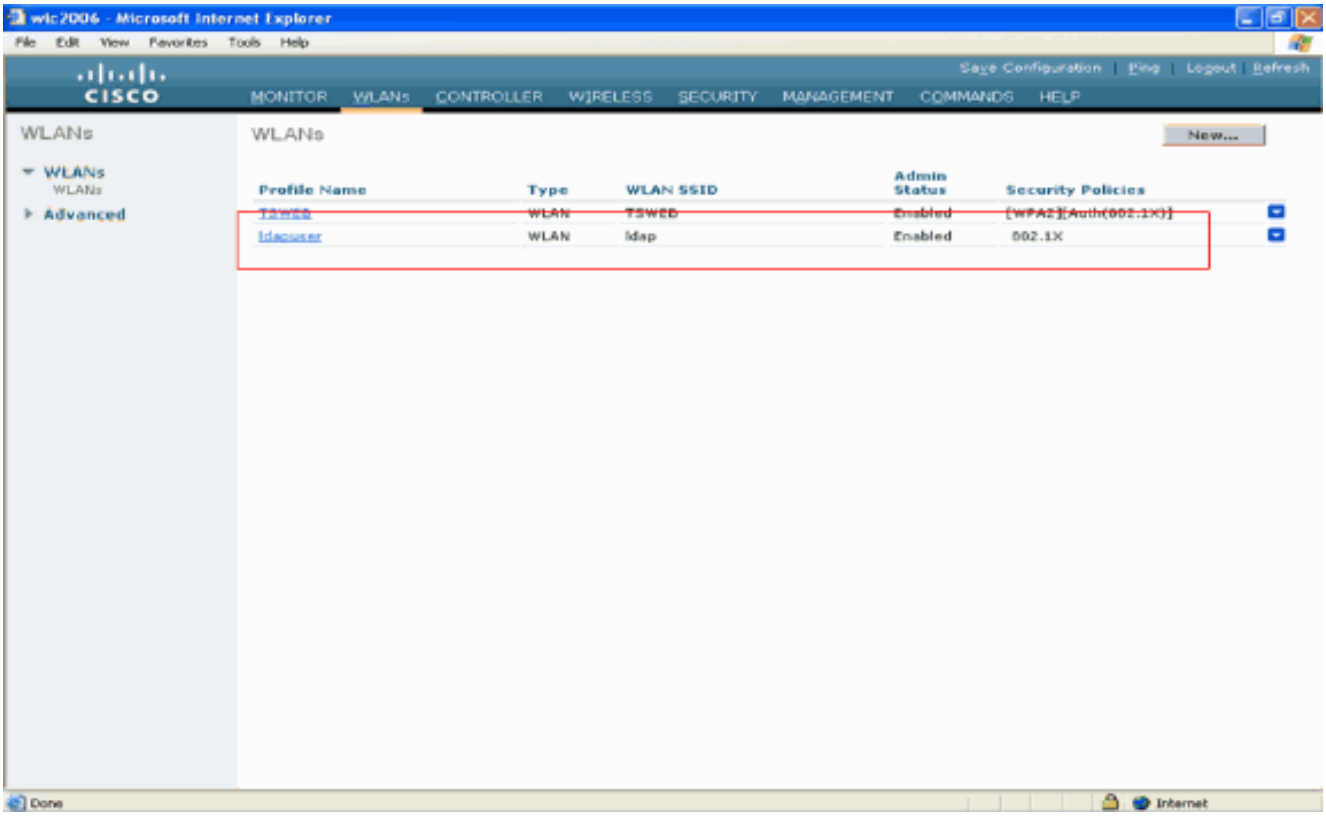
.



6. 새 WLAN Ldap가 WLC에 구성되었습니다. 이 WLAN은 로컬 EAP 인증(이 경우 EAP-FAST)으로 클라이언트를 인증하고 클라이언트 자격 증명 검증을 위해 LDAP 백엔드 데이터베이스를

쿼리합니다

.



LDAP 서버 구성

이제 로컬 EAP가 WLC에 구성되었으므로 다음 단계는 인증서 검증에 성공할 때 무선 클라이언트를 인증하기 위해 백엔드 데이터베이스 역할을 하는 LDAP 서버를 구성하는 것입니다.

LDAP 서버를 구성하는 첫 번째 단계는 WLC가 이 데이터베이스에 쿼리하여 사용자를 인증할 수 있도록 LDAP 서버에 사용자 데이터베이스를 만드는 것입니다.

도메인 컨트롤러에서 사용자 생성

이 예에서는 새 OU **ldapuser**가 생성되고 이 OU 아래에 user **2**가 생성됩니다. LDAP 액세스를 위해 이 사용자를 구성하면 WLC는 사용자 인증을 위해 이 LDAP 데이터베이스에 쿼리할 수 있습니다.

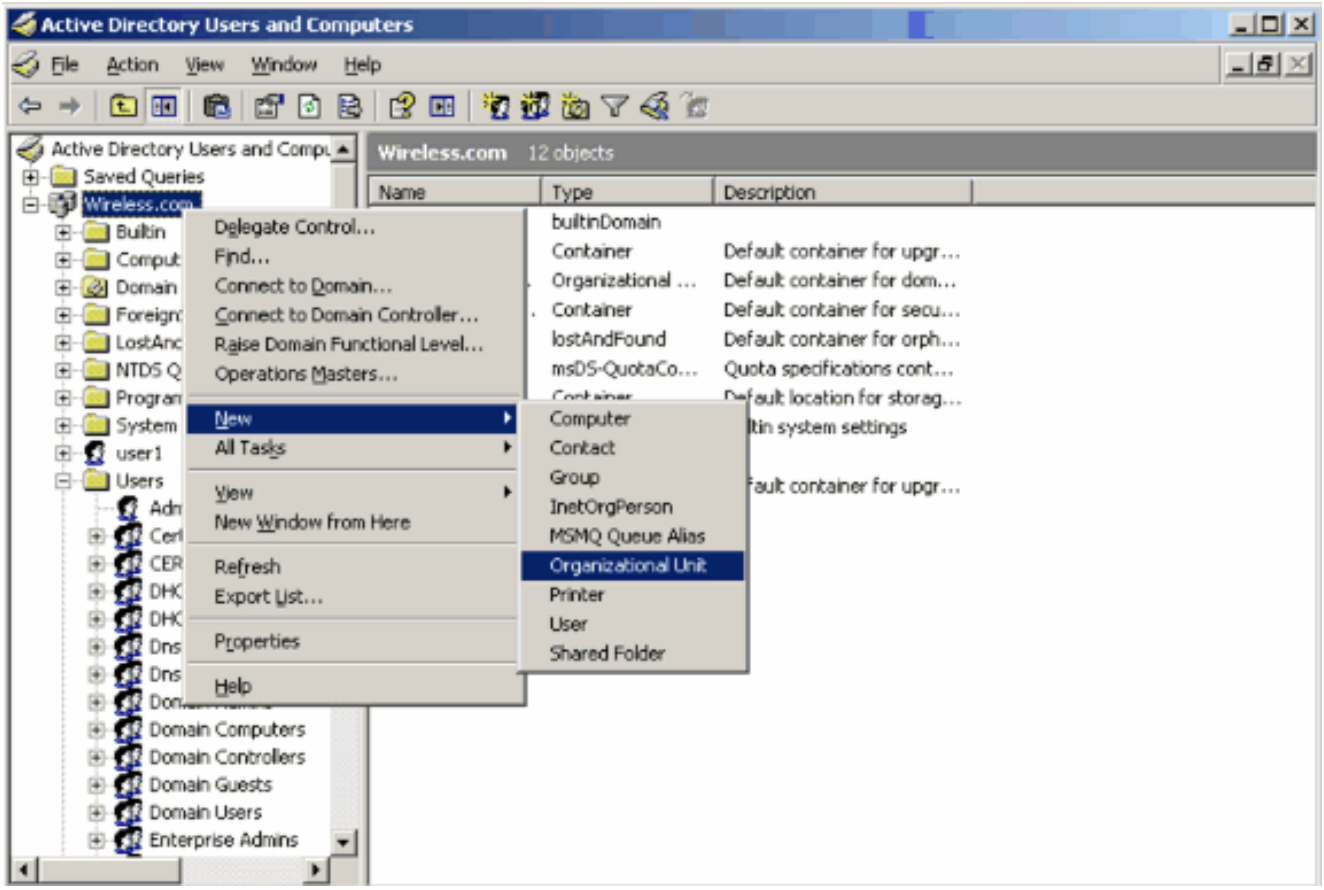
이 예에서 사용되는 도메인은 **wireless.com입니다**.

OU에서 사용자 데이터베이스 만들기

이 섹션에서는 도메인에 새 OU를 만들고 이 OU에 새 사용자를 만드는 방법에 대해 설명합니다.

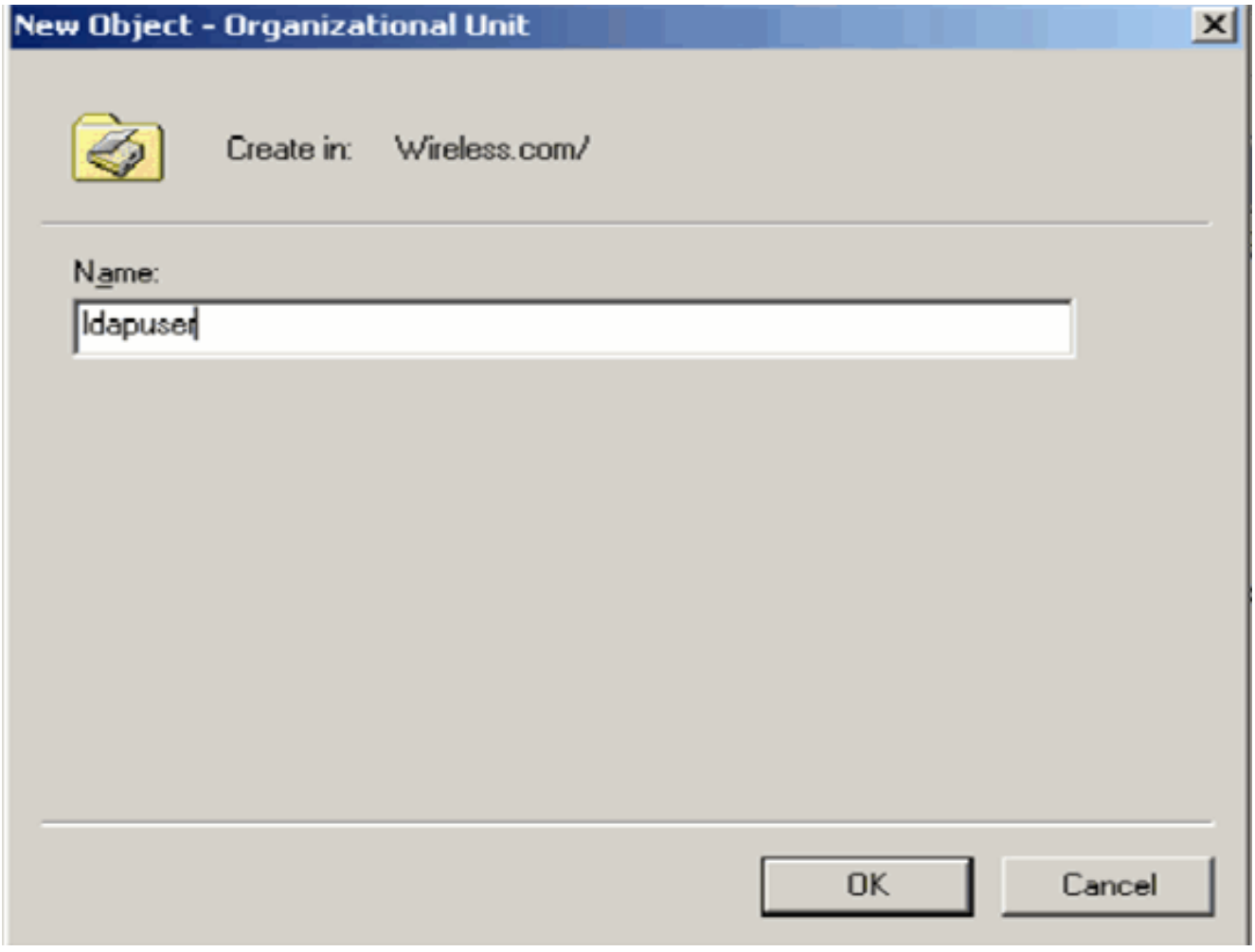
1. 도메인 컨트롤러에서 **시작 > 프로그램 > 관리 도구 > Active Directory 사용자 및 컴퓨터**를 클릭하여 **Active Directory 사용자 및 컴퓨터** 관리 콘솔을 시작합니다.
2. 도메인 이름(이 예에서는 wireless.com)을 마우스 오른쪽 단추로 클릭한 다음 컨텍스트 메뉴에서 **새로 만들기 > 조직 구성 단위**를 선택하여 새 OU를 만듭니다

.



3. 이 OU에 이름을 지정하고 **OK**(확인)를 클릭합니다

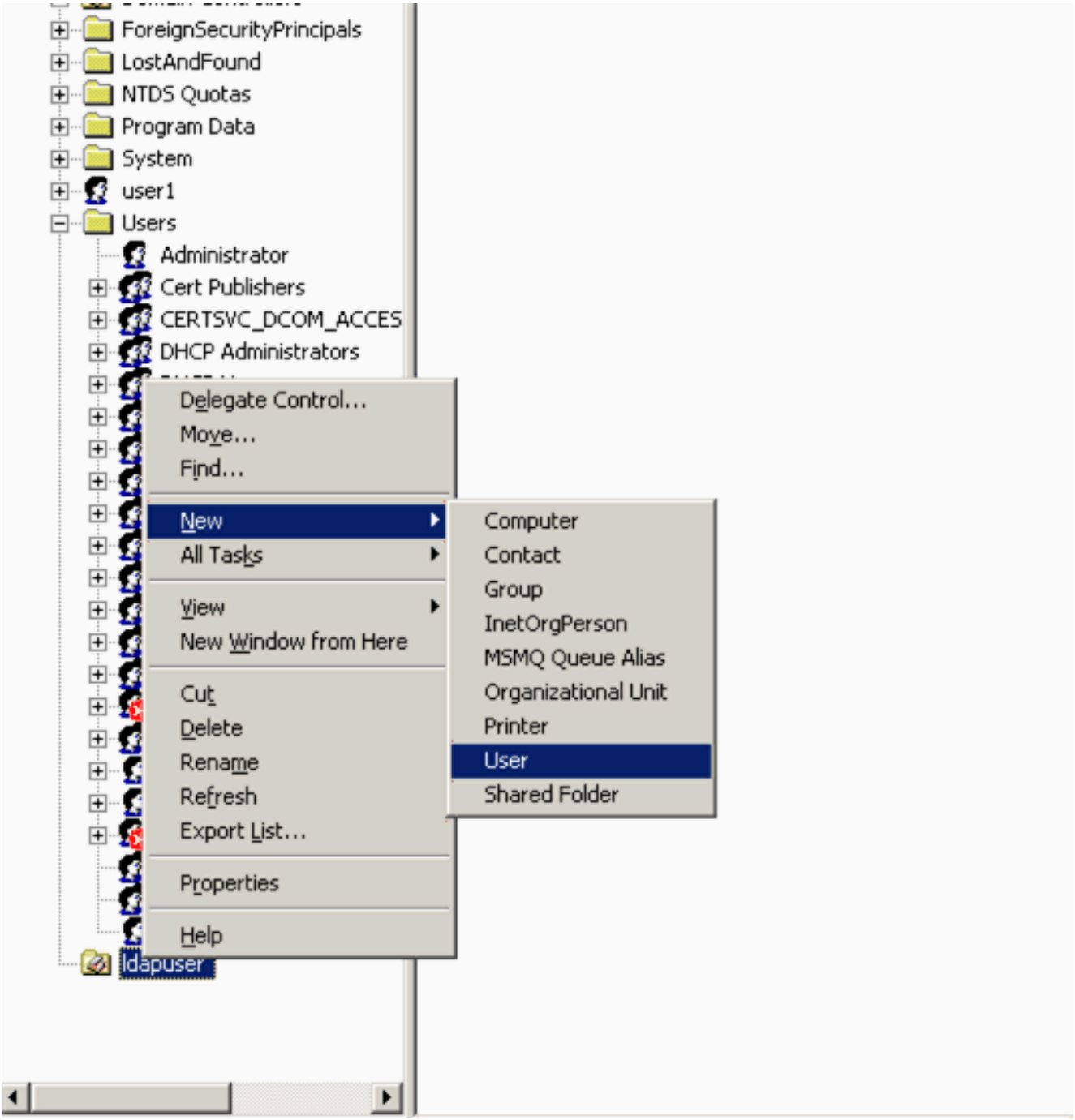
.



새 OU ldapuser가 **LDAP** 서버에 생성되었으므로 다음 단계는 이 OU 아래에 user **user2**를 생성하는 것입니다. 이를 위해 다음 단계를 완료하십시오.

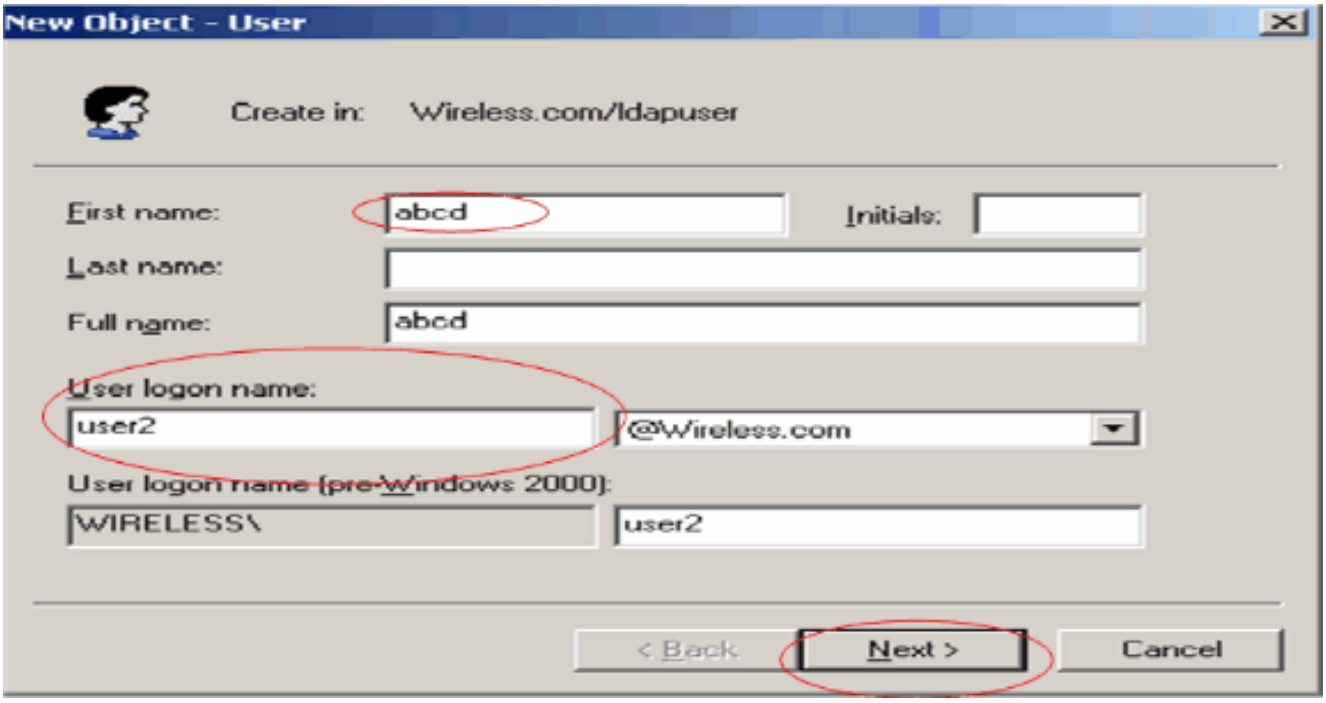
1. 생성된 새 OU를 마우스 오른쪽 버튼으로 클릭합니다. 결과 컨텍스트 **메뉴**에서 **새로 만들기 > 사용자**를 선택하여 새 사용자를 생성합니다

.



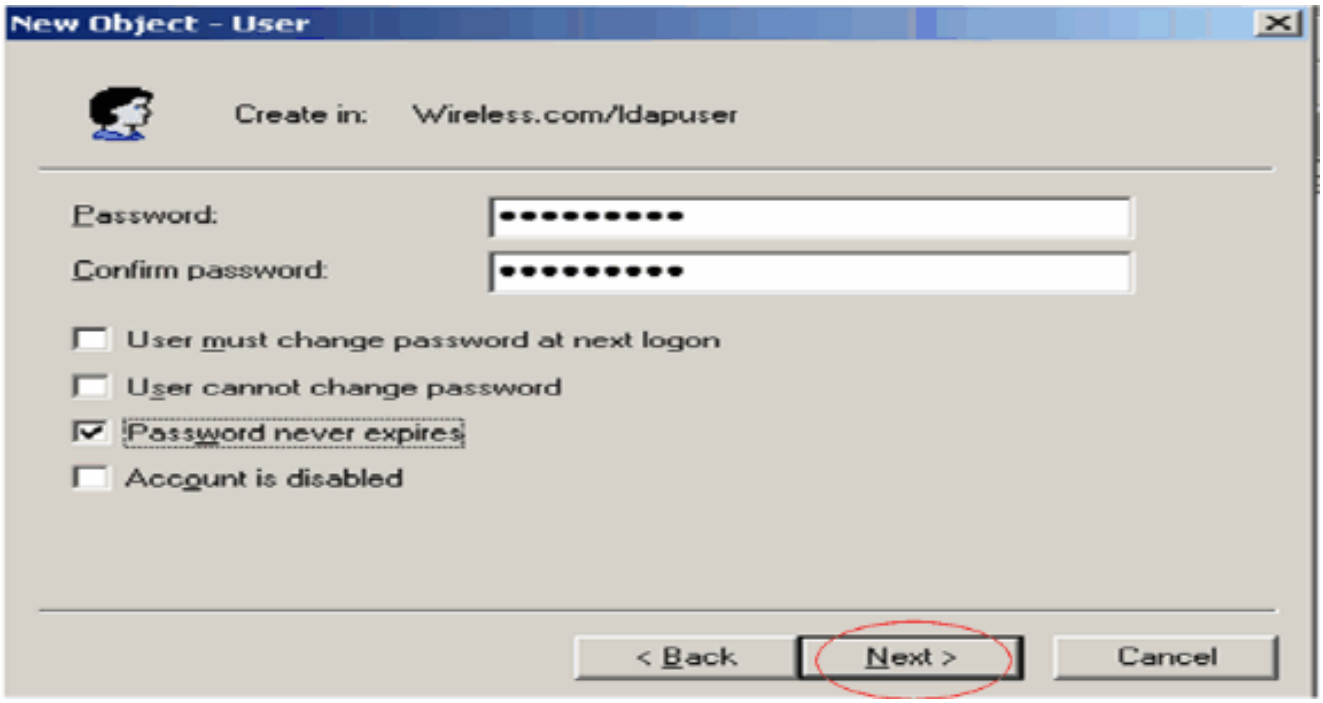
2. User setup(사용자 설정) 페이지에서 이 예에 표시된 대로 필수 필드를 입력합니다. 이 예에서는 **user2**를 사용자 로그온 이름으로 사용합니다.클라이언트 인증을 위해 LDAP 데이터베이스에서 확인되는 사용자 이름입니다. 이 예에서는 **abcd**를 이름과 성으로 사용합니다. **Next(다음)**를 클릭합니다

.

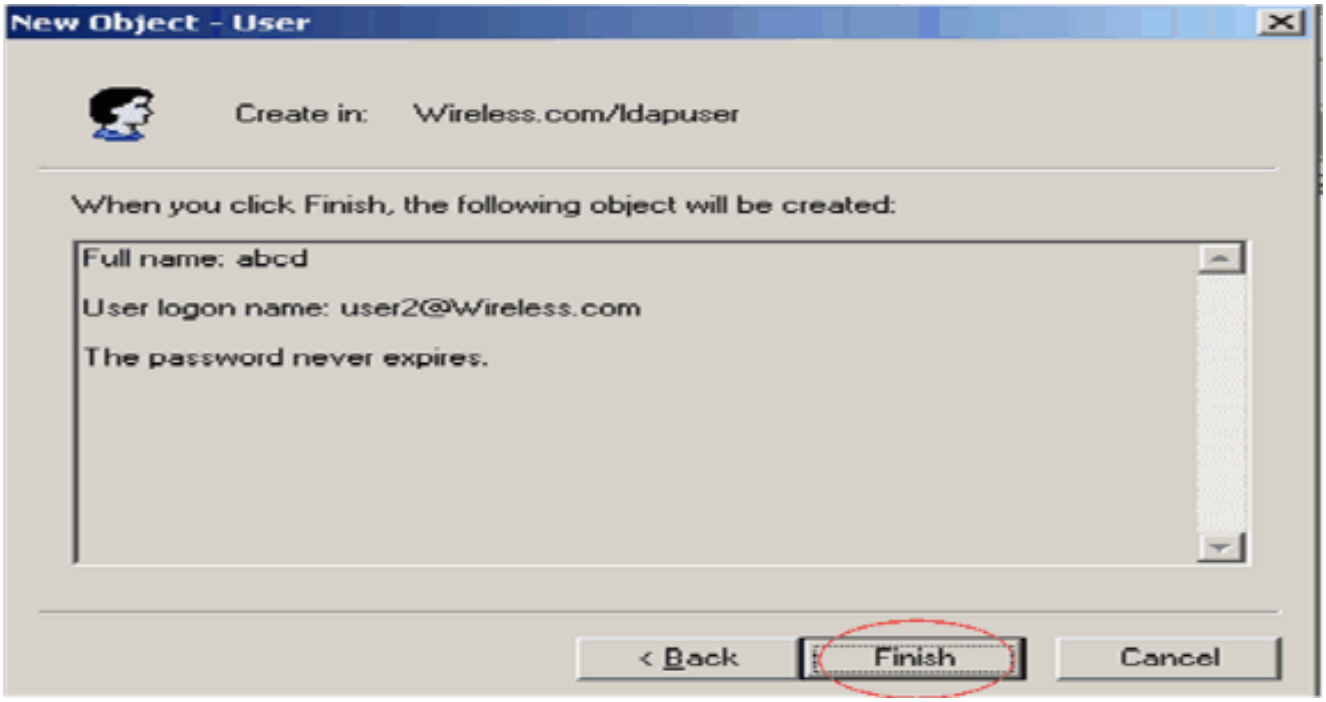


3. 비밀번호를 입력하고 비밀번호를 확인합니다. Password never expires(**비밀번호 만료되지 않음) 옵션**을 선택하고 Next(**다음)**를 클릭합니다

.



4. Finish(마침)를 클릭합니다.새 사용자 **user2**가 OU ldapuser 아래에 **생성됩니다**. 사용자 자격 증명은 다음과 같습니다.사용자 이름: **user2**암호: **Laptop123**



이제 OU의 사용자가 생성되었으므로 다음 단계는 LDAP 액세스를 위해 이 사용자를 구성하는 것입니다.

LDAP 액세스를 위한 사용자 구성

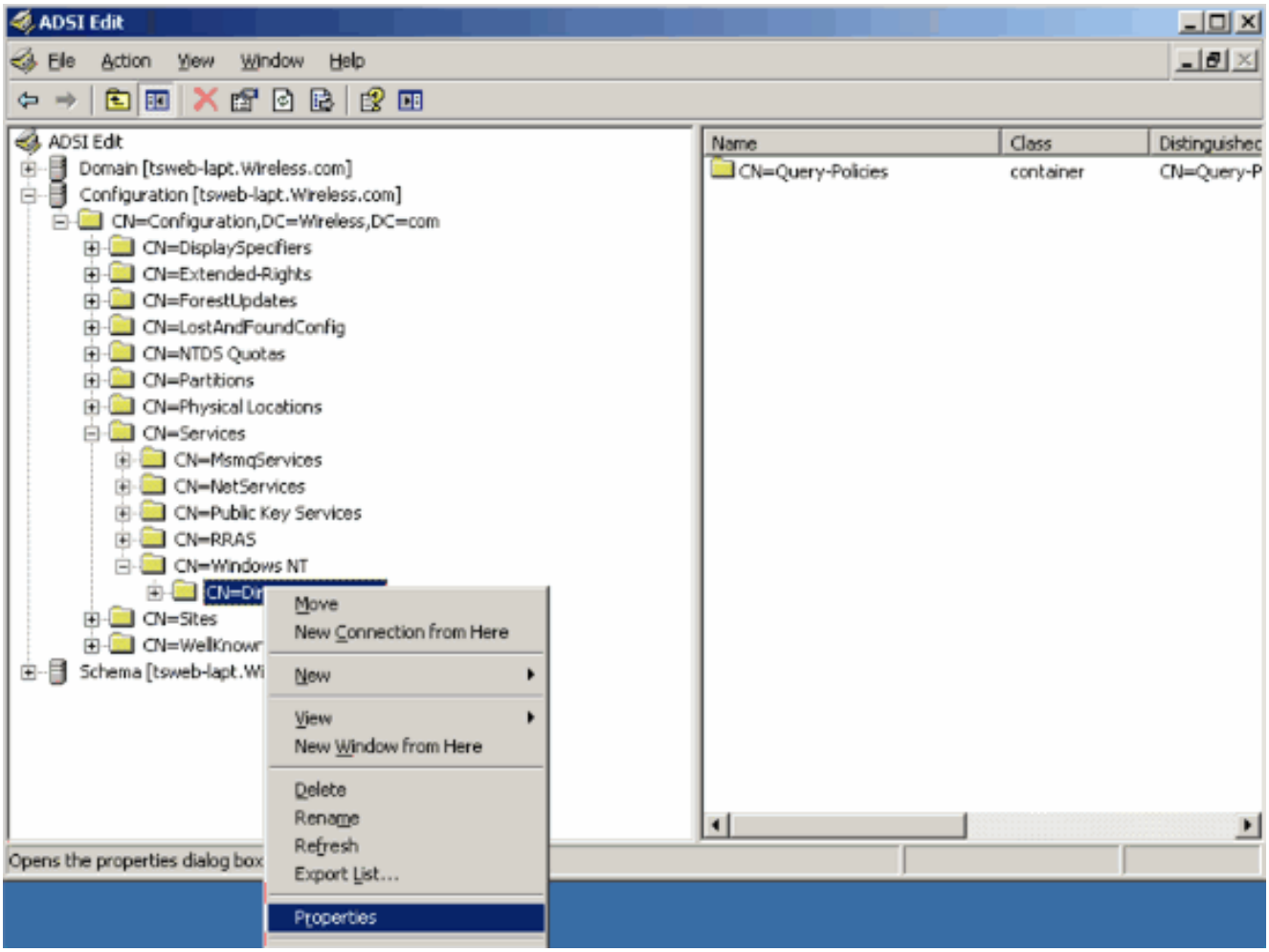
LDAP 액세스를 위한 사용자를 구성하려면 이 섹션의 단계를 수행합니다.

Windows 2003 Server에서 익명 바인딩 기능 사용

서드파티 애플리케이션이 LDAP에서 Windows 2003 AD에 액세스하려면 Windows 2003에서 익명 바인딩 기능을 활성화해야 합니다. 기본적으로 익명 LDAP 작업은 Windows 2003 도메인 컨트롤러에서 허용되지 않습니다.

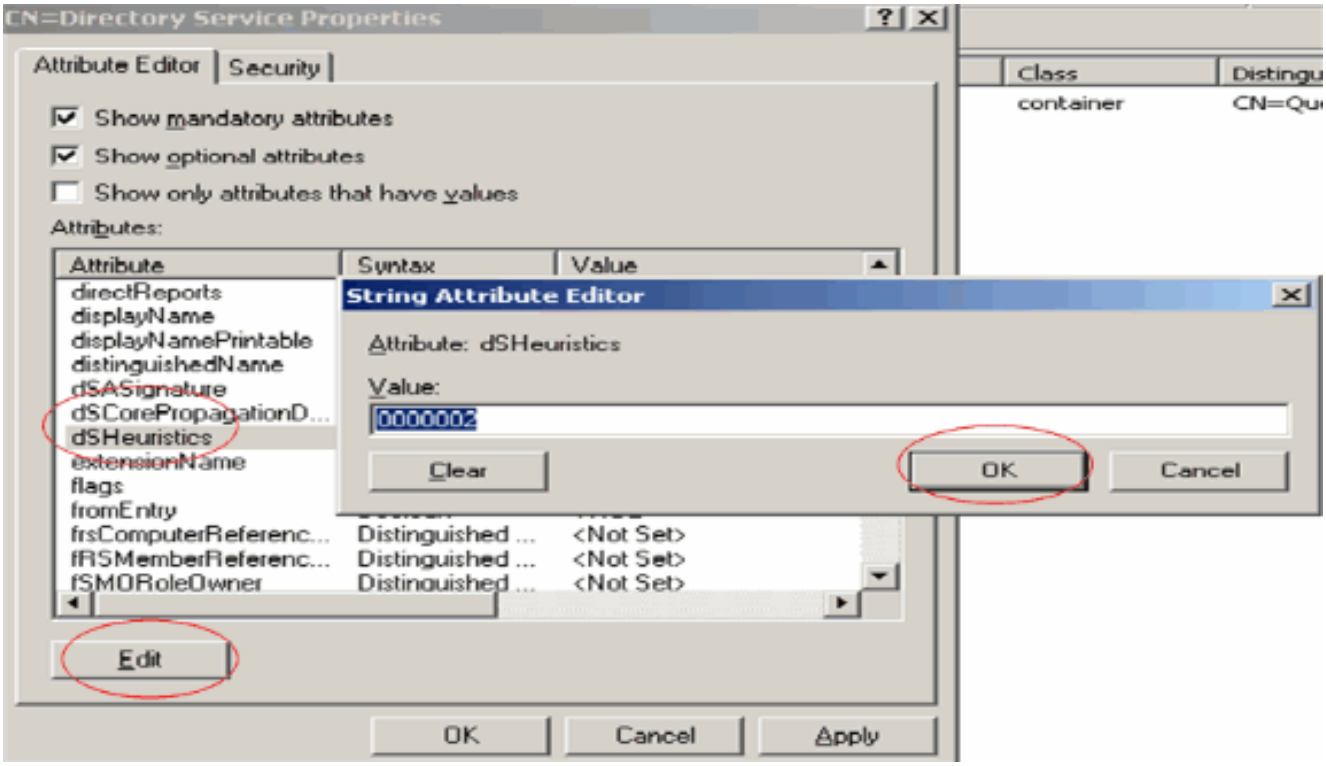
익명 바인딩 기능을 활성화하려면 다음 단계를 수행합니다.

1. 시작 > 실행 > 유형: ADSI Edit.**msc** 위치에서 ADSI 편집 **도구를 시작합니다**. 이 도구는 Windows 2003 지원 도구의 일부입니다.
2. ADSI Edit(ADSI 편집) 창에서 Root(루트) 도메인(Configuration(컨피그레이션) [tsweb-lapt.Wireless.com])을 확장합니다.**CN=Services(CN=서비스) > CN=Windows NT > CN=Directory Service(CN=디렉토리 서비스)를** 확장합니다. **CN=Directory Service** 컨테이너를 마우스 오른쪽 단추로 클릭하고 상황에 맞는 **메뉴**에서 속성을 선택합니다
.



3. **CN=Directory Service Properties(CN=디렉토리 서비스 속성)** 창에서 Attribute(특성) 필드 **아래**의 dsHeuristics(dsHeuristics) 특성을 클릭하고 Edit(**편집**)를 **선택합니다**. 이 속성의 **String Attribute** Editor(문자열 속성 편집기) 창에 값 **000002**를 입력하고 Apply(적용) 및 **OK(확인)를** 클릭합니다. 익명 바인딩 기능은 Windows 2003 서버에서 사용할 수 있습니다.**참고:** 마지막 (7번째) 문자는 LDAP 서비스에 바인딩할 수 있는 방법을 제어하는 문자입니다. "0" 또는 7번째 문자가 없으면 익명 LDAP 작업이 비활성화됨을 의미합니다. **일곱 번째 문자를 "2"로 설정하면 익명 바인드 기능이 활성화됩니다**

.

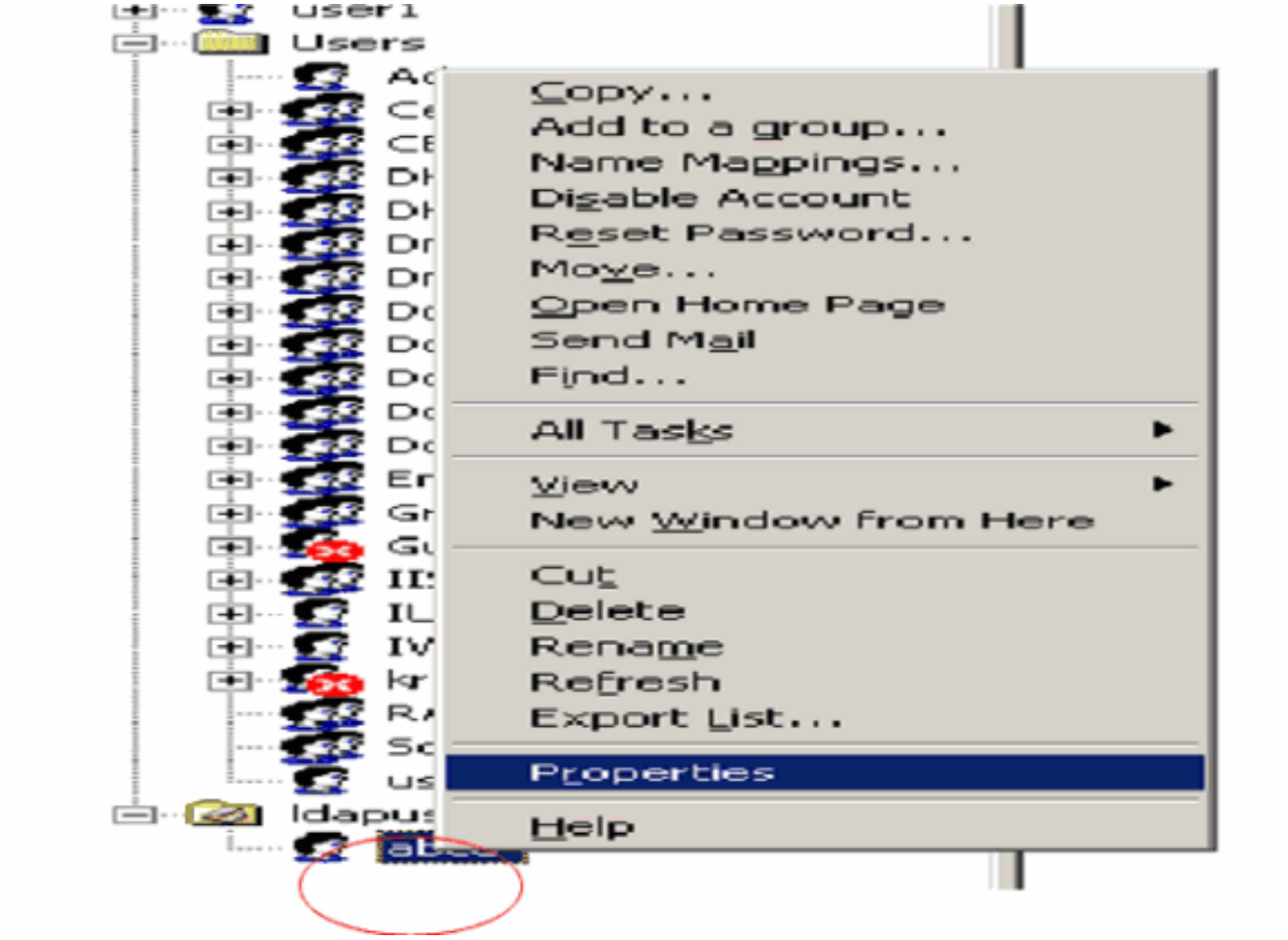


참고: 이 속성에 이미 값이 있는 경우 왼쪽의 7번째 문자만 변경해야 합니다. 익명 바인딩을 활성화하려면 이 문자만 변경해야 합니다. 예를 들어 현재 값이 "0010000"이면 "0010002"로 변경해야 합니다. 현재 값이 7자 미만이면 사용하지 않는 위치에 0을 입력해야 합니다. "001"은 "0010002"이 됩니다.

사용자 "user2"에게 익명 로그온 액세스 권한 부여

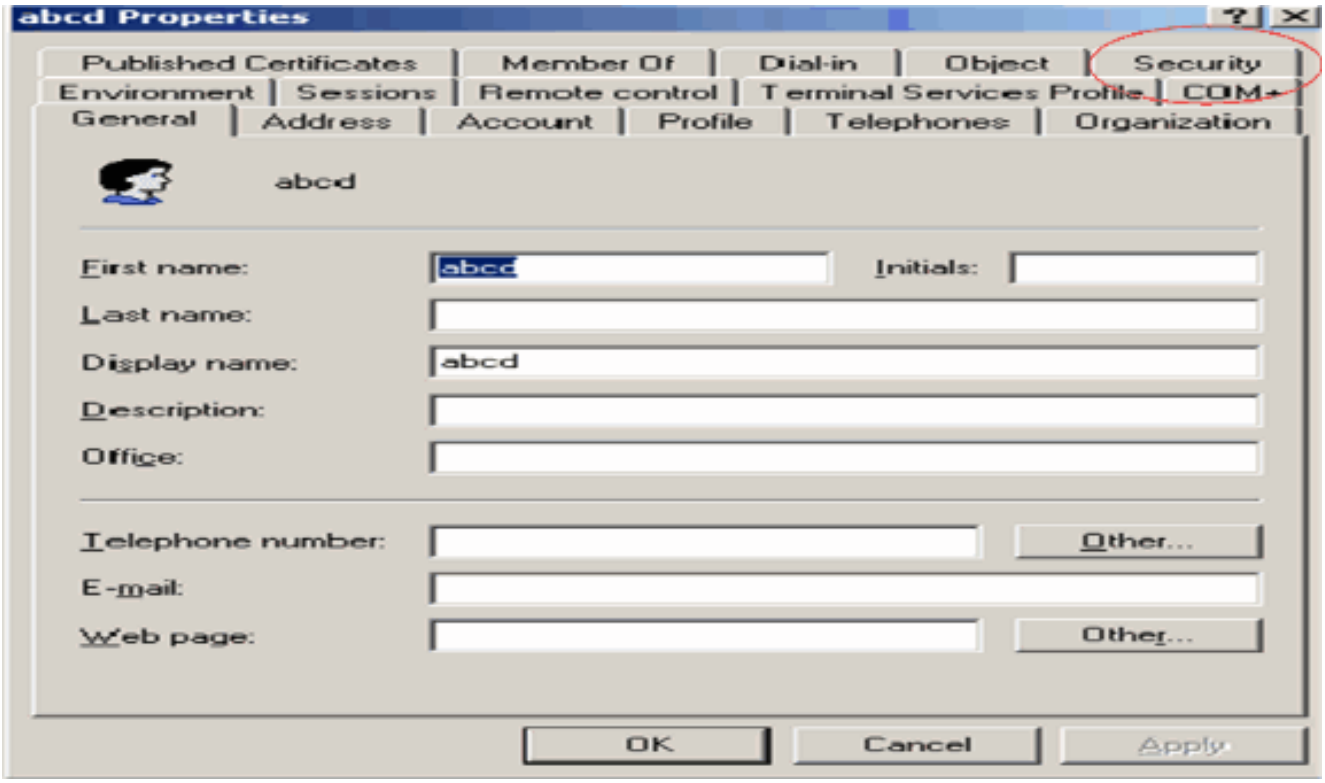
다음 단계는 사용자 **user2**에게 **ANONYMOUS LOGON** 액세스 권한을 부여하는 **것입니다**. 이를 위해 다음 단계를 완료하십시오.

1. **Active Directory 사용자** 및 컴퓨터**를** 엽니다.
2. View **Advanced Features(고급 기능 보기)**가 선택되었는지 확인합니다.
3. 사용자 user2로 **이동하여** 마우스 오른쪽 버튼을 클릭합니다. 컨텍스트 **메뉴**에서 등록 정보를 선택합니다. 이 사용자는 "abcd"라는 이름으로 식별됩니다
.



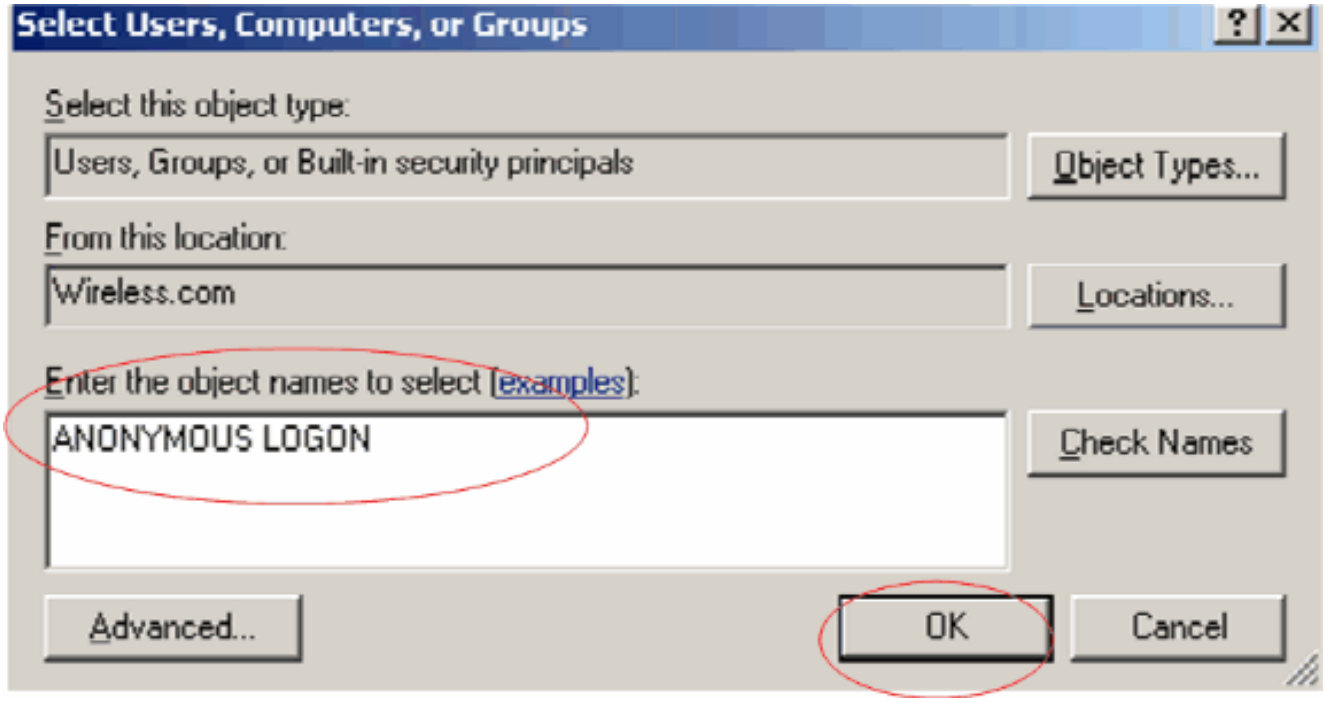
4. 속성 창에서 **보안**으로 이동합니다

.



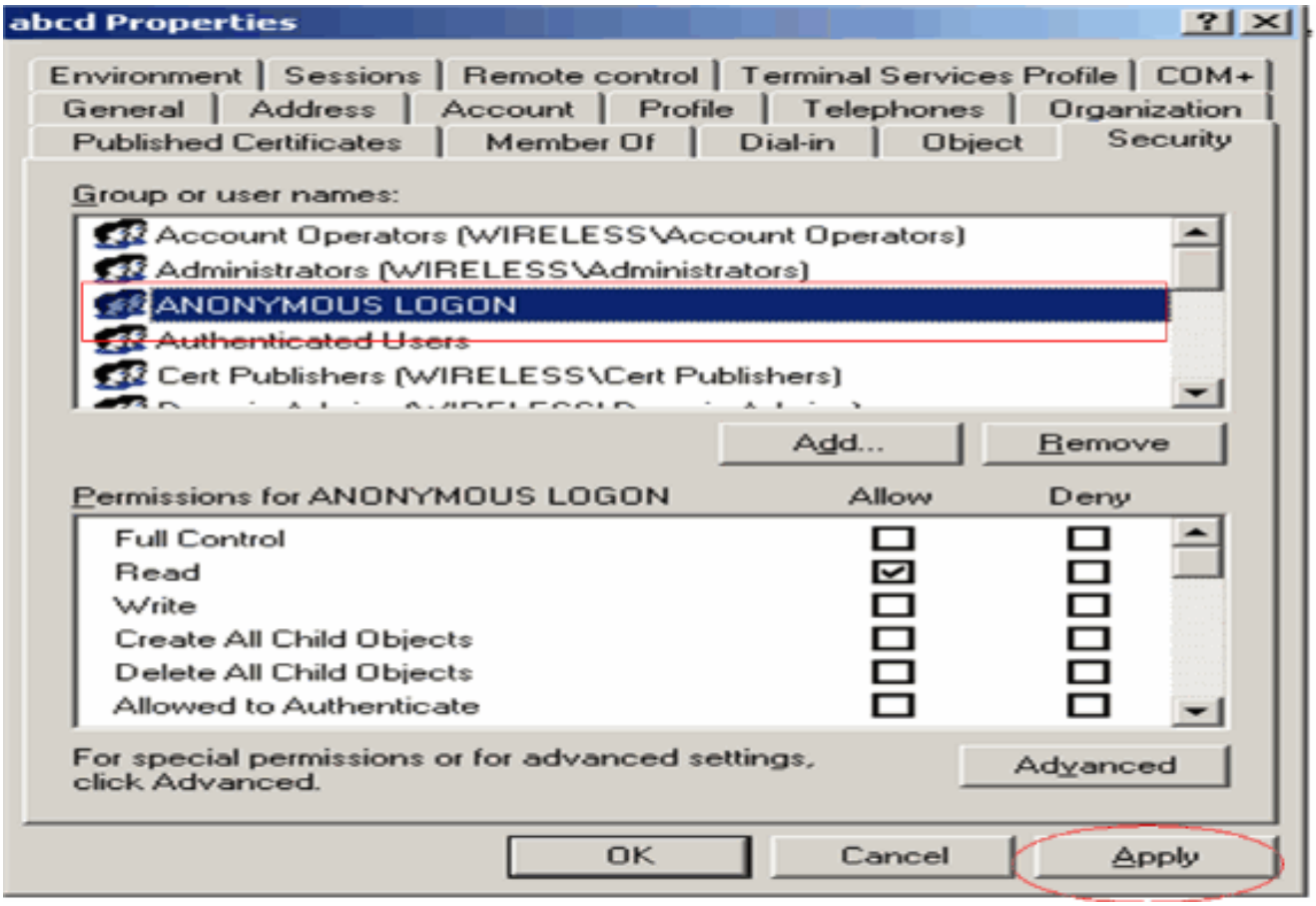
5. 결과 **창**에서 Add를 클릭합니다.
6. 선택할 **개체 이름 입력** 상자에 **ANONYMOUS LOGON**을 입력하고 대화 상자를 승인합니다

.



7. ACL에서 ANONYMOUS LOGON이 사용자의 일부 속성 **집합**에 액세스할 수 있음을 알 수 있습니다. **OK(확인)**를 클릭합니다. 이 사용자에게는 ANONYMOUS LOGON 액세스 권한이 부여됩니다

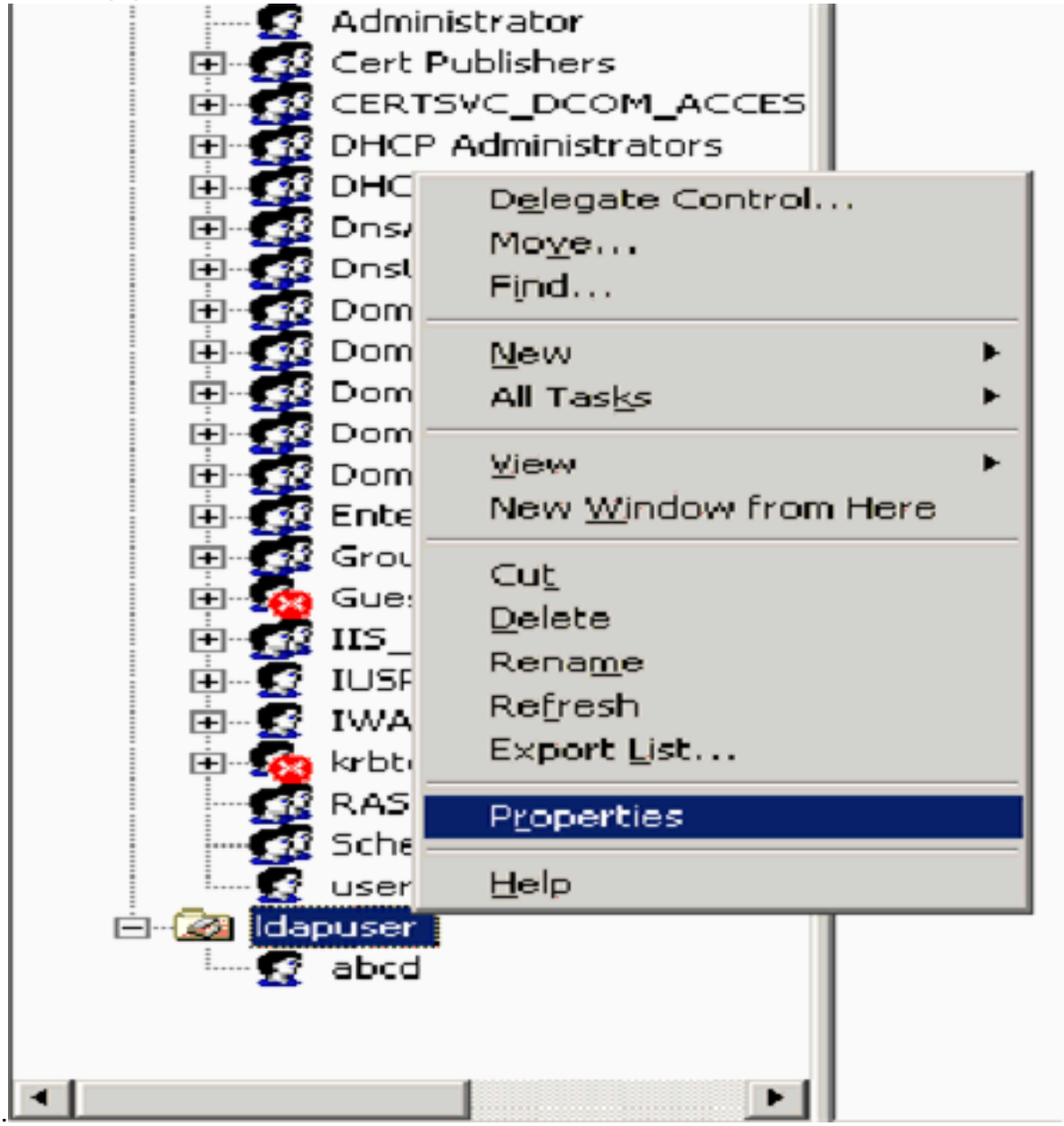
.



OU에 대한 목록 내용 권한 부여

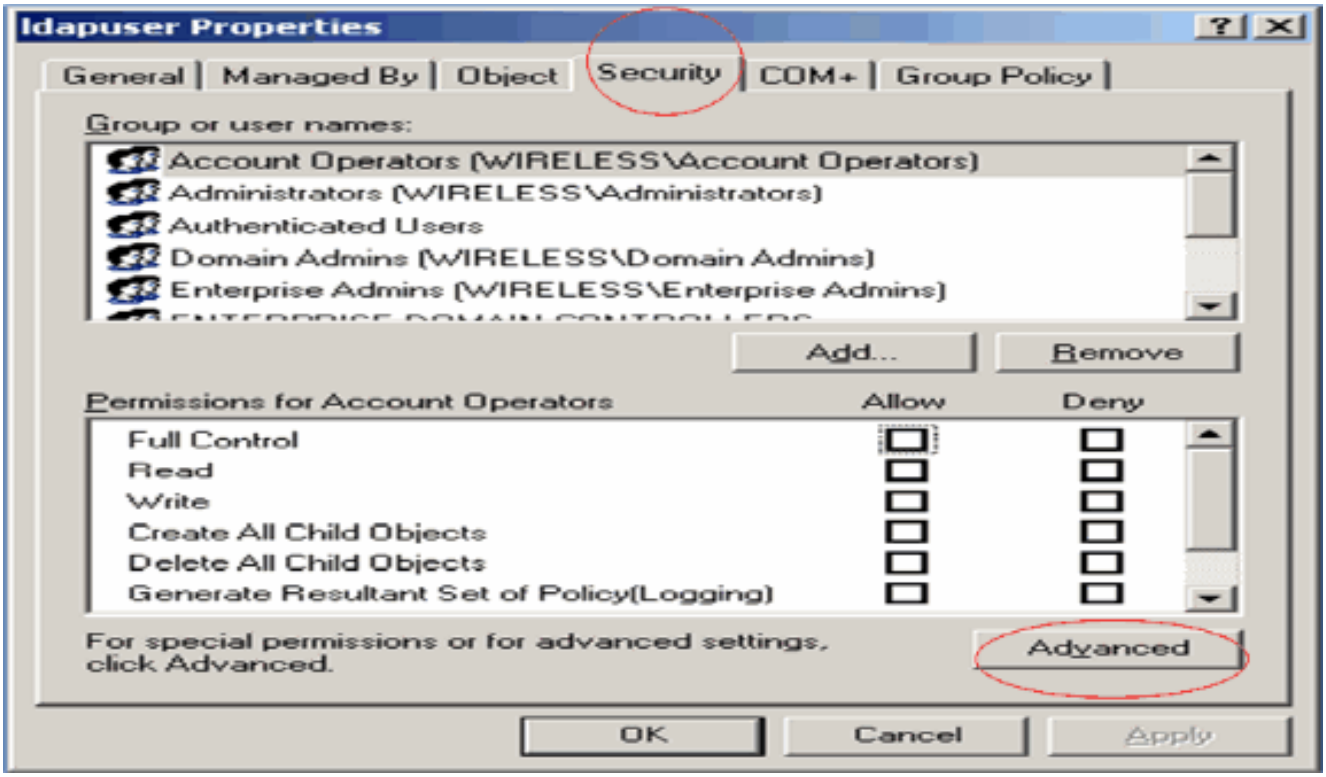
다음 단계는 사용자가 있는 OU의 **ANONYMOUS LOGON**에 최소 목록 **콘텐츠** 권한을 부여하는 것입니다. 이 예에서 "user2"는 OU "ldapuser"에 있습니다. 이를 위해 다음 단계를 완료하십시오.

1. Active Directory 사용자 및 컴퓨터에서 OU ldapuser를 마우스 오른쪽 단추로 클릭하고 **속성**을 **선택합니다**



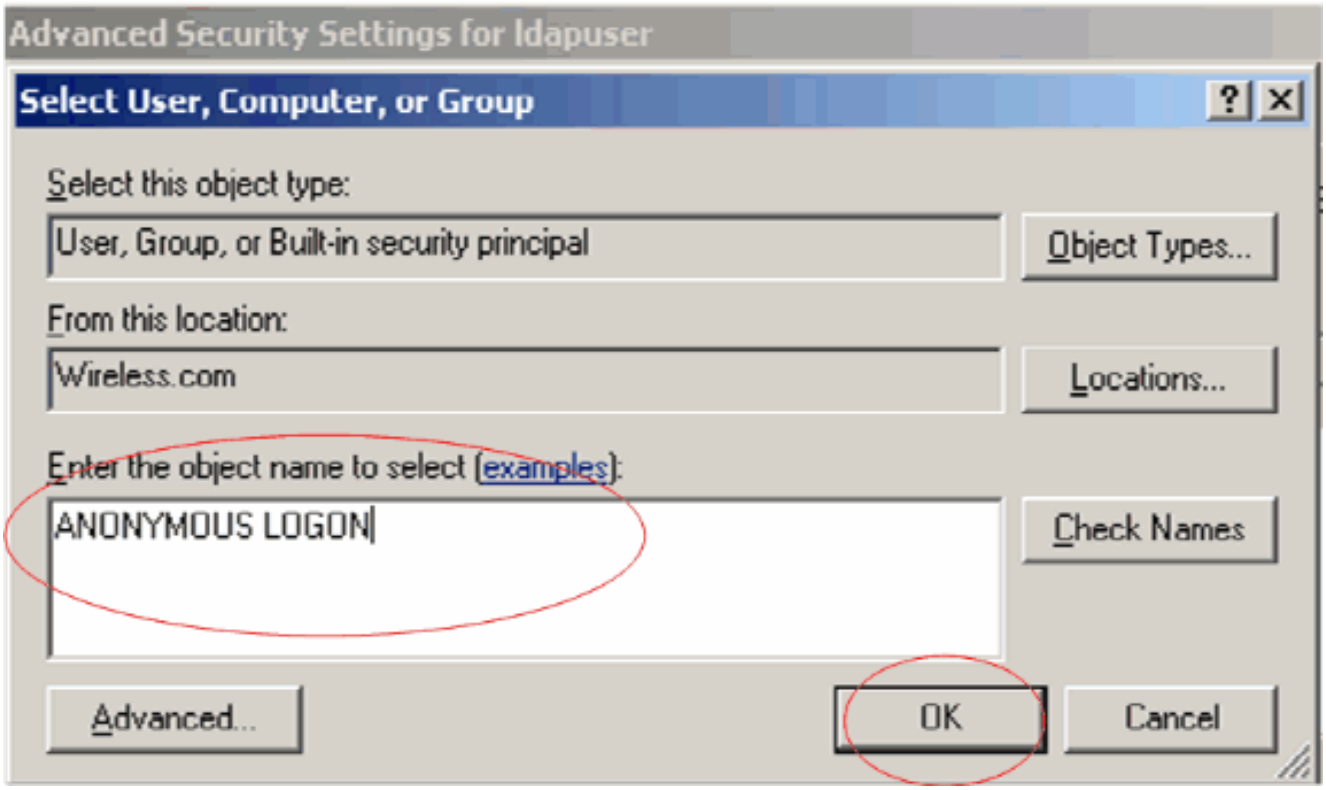
2. Security(**보안**)를 클릭한 다음 Advanced(**고급**)**를 클릭합니다**

.



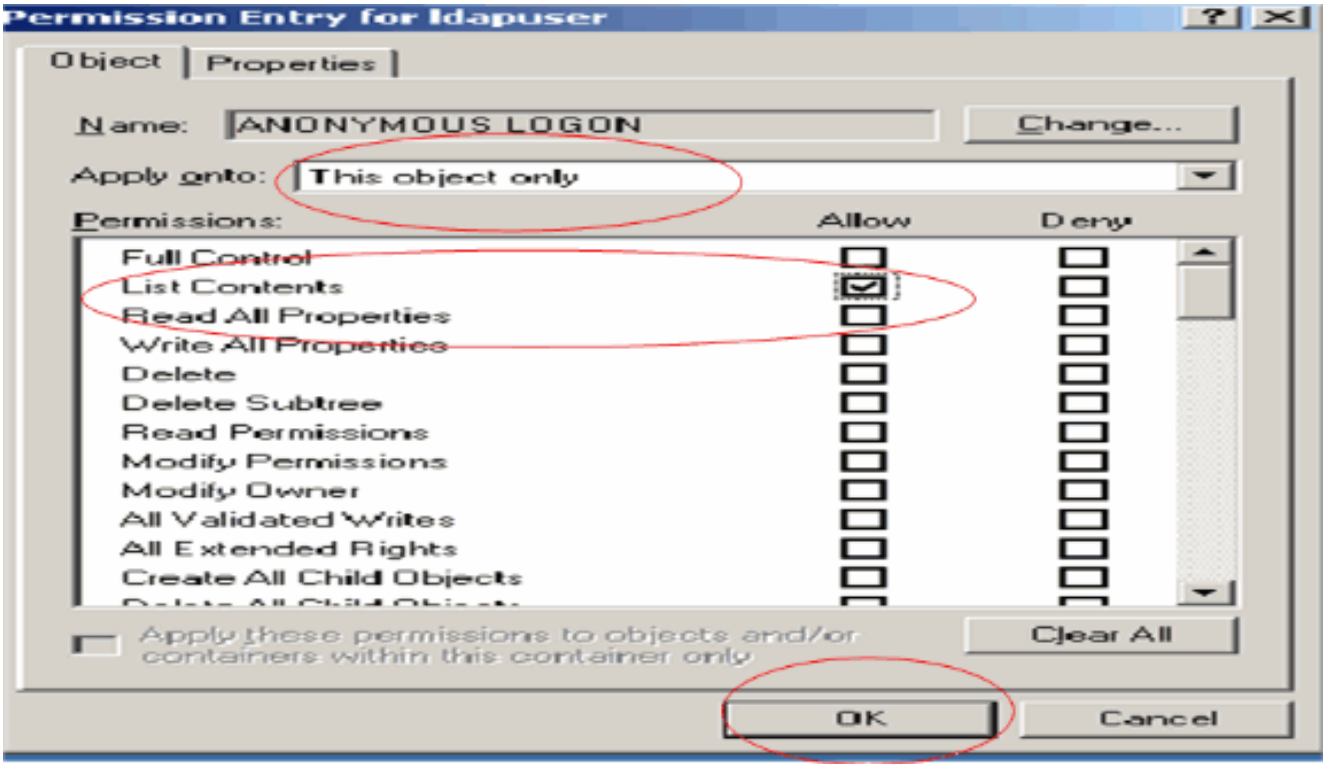
3. **Add(추가)**를 클릭합니다. 대화 상자가 열리면 ANONYMOUS LOGON**을 입력합니다**

.



4. 대화 상자를 승인합니다. 그러면 새 대화 상자 창이 열립니다.
5. 적용 **대상** 드롭다운 **상자**에서 **이 객체만**을 선택하고 **내용** 허용 나열 **확인란**을 활성화합니다

.



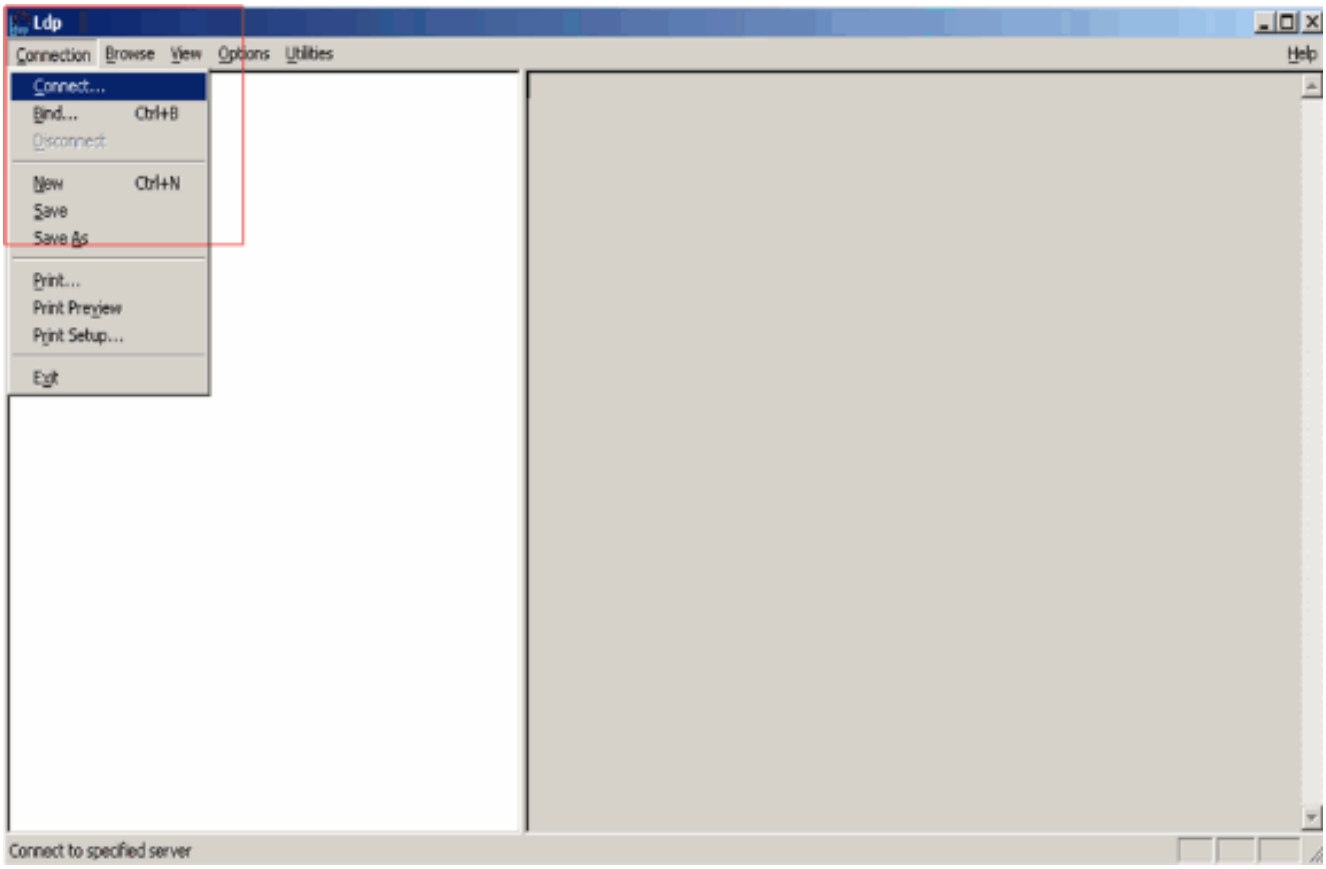
LDP를 사용하여 사용자 특성 식별

이 GUI 도구는 사용자가 Active Directory와 같은 LDAP 호환 디렉토리에 대해 작업(예: 연결, 바인딩, 검색, 수정, 추가, 삭제)을 수행할 수 있도록 하는 LDAP 클라이언트입니다. LDP는 보안 설명자 및 복제 메타데이터와 같은 메타데이터와 함께 Active Directory에 저장된 개체를 보는 데 사용됩니다.

LDP GUI 도구는 제품 CD에서 Windows Server 2003 지원 도구를 설치할 때 포함됩니다. 이 섹션에서는 LDP 유틸리티를 사용하여 사용자 user2와 연결된 특정 속성을 식별하는 방법에 대해 **설명합니다**. 이러한 특성 중 일부는 WLC의 LDAP 서버 컨피그레이션 매개변수(예: User Attribute type 및 User Object type)를 채우는 데 사용됩니다.

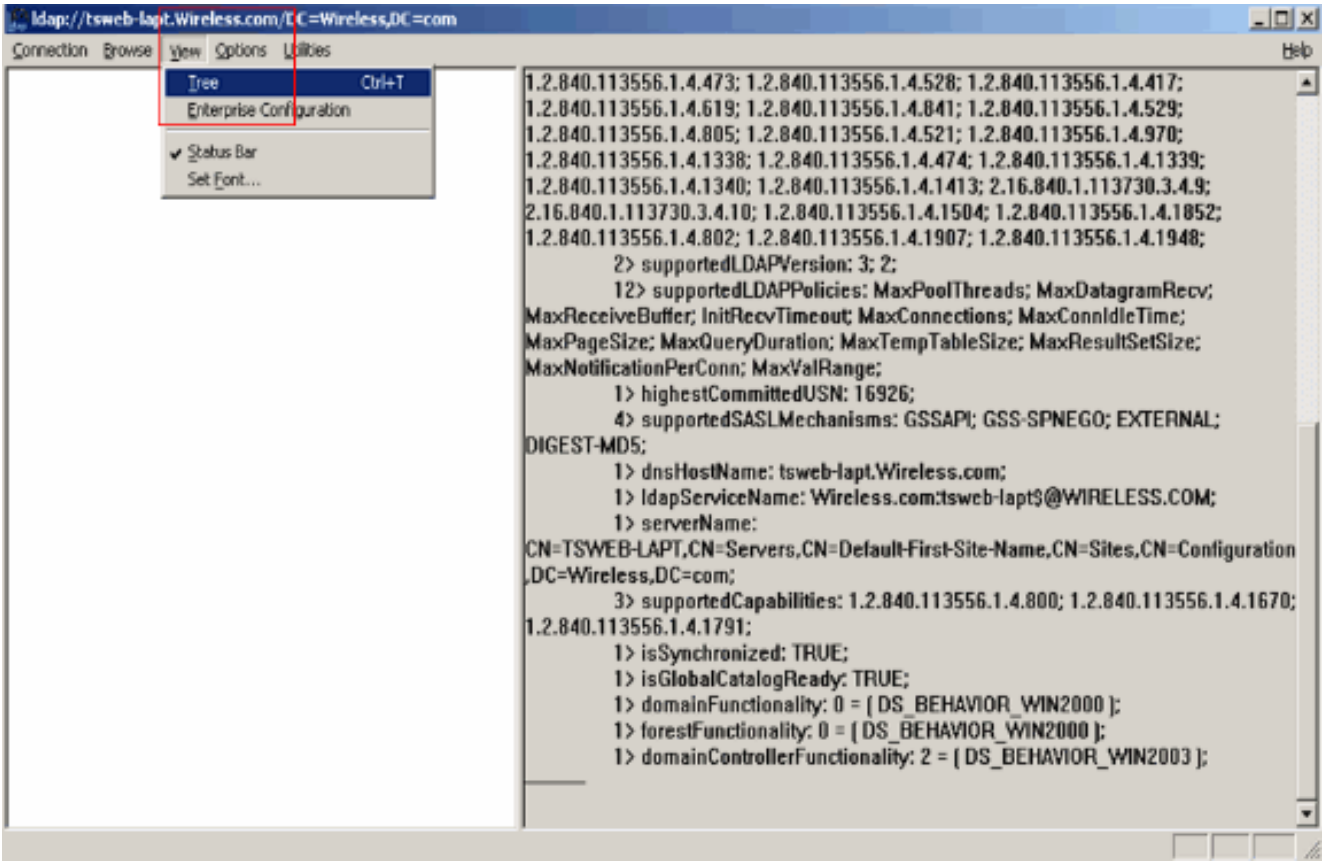
1. Windows 2003 서버(동일한 LDAP 서버에서도)에서 **시작 > 실행**을 클릭하고 **LDP**를 입력하여 LDP 브라우저에 액세스합니다.
2. LDP 기본 창에서 **Connection(연결) > Connect(연결)**를 클릭하고 LDAP 서버의 IP 주소를 입력하여 LDAP 서버에 연결합니다

   .



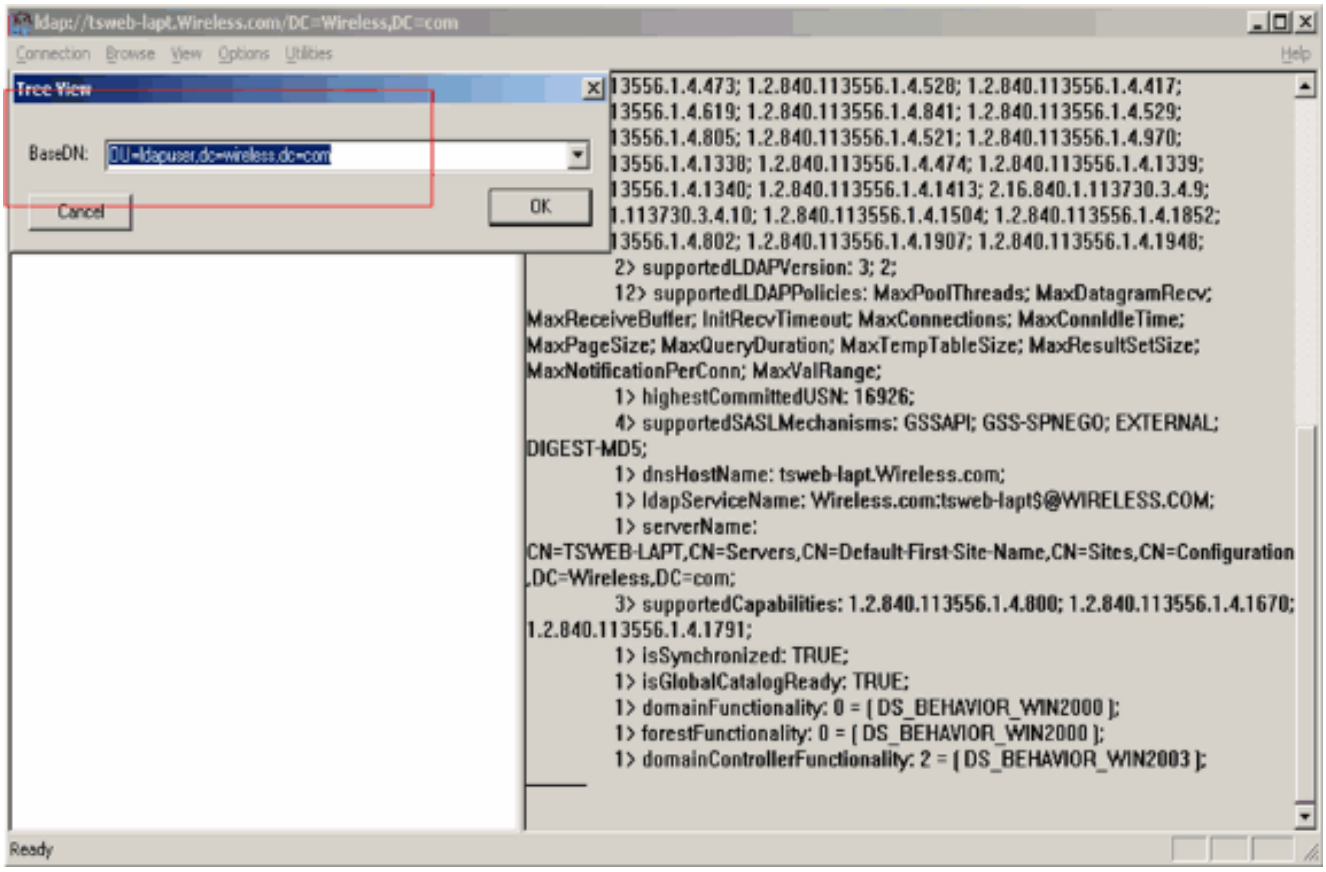
3. LDAP 서버에 연결되면 주 메뉴에서 **View**를 선택하고 Tree를 **클릭합니다**

.



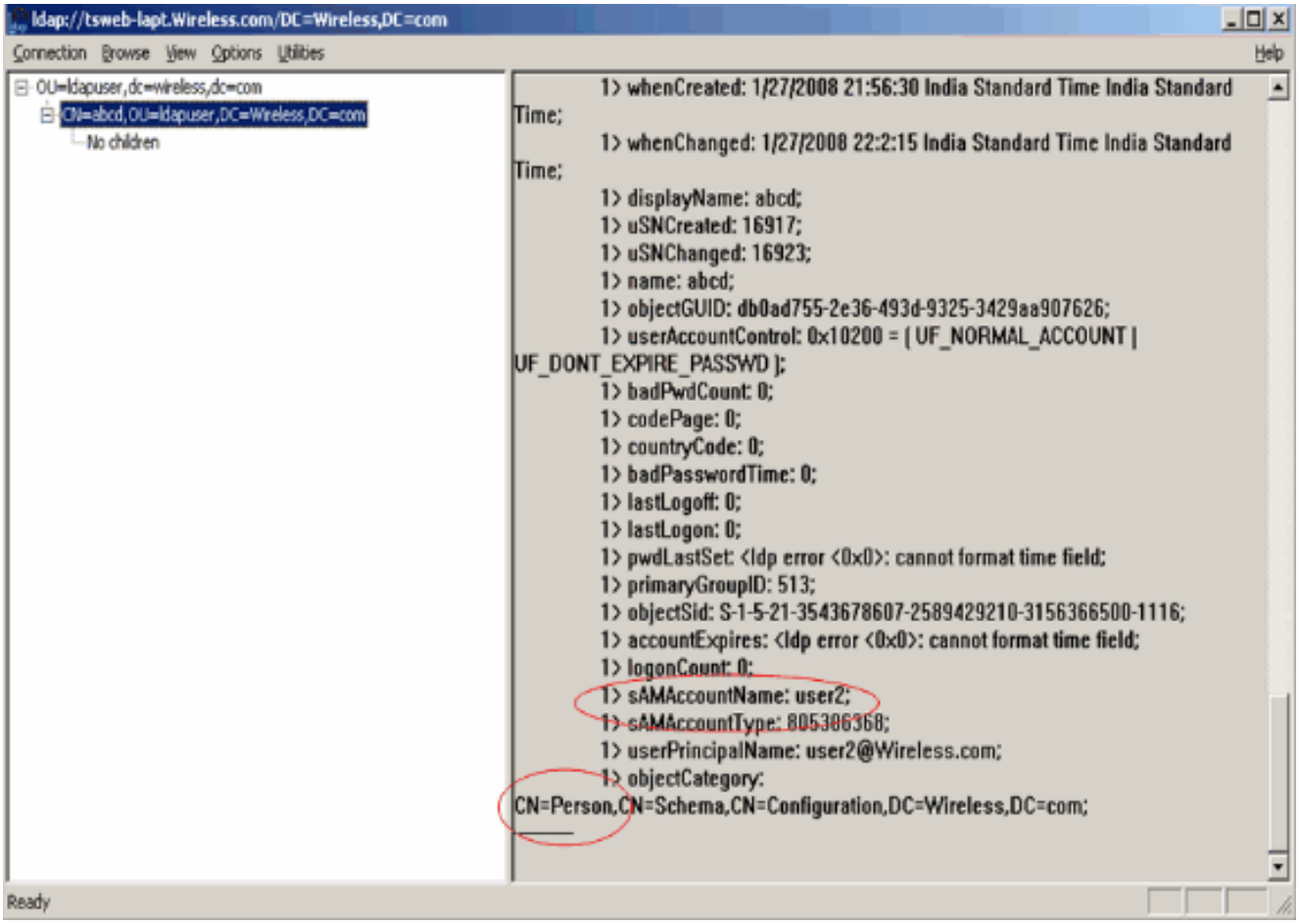
4. 결과 트리 보기 창에서 사용자의 BaseDN을 입력합니다. 이 예에서 **user2는 Wireless.com 도메인 아래의 OU "ldapuser" 아래에 있습니다**. 따라서 user2의 BaseDN은 **OU=ldapuser, dc=wireless, dc=com입니다**. **OK(확인)**를 클릭합니다

.



5. LDP 브라우저의 왼쪽에는 지정된 BaseDN(**OU=ldapuser, dc=wireless, dc=com**) 아래에 나타나는 전체 트리가 표시됩니다. 사용자 user2를 찾으려면 트리를 **확장합니다**. 이 사용자는 사용자의 이름을 나타내는 CN 값으로 식별될 수 있습니다. 이 예에서는 **CN=abcd입니다**. **CN=abcd**를 두 번 클릭합니다. LDP 브라우저의 오른쪽 창에서 LDP는 **user2와 연결된 모든 특성을 표시합니다**. 다음 예에서는 이 단계를 설명합니다

.



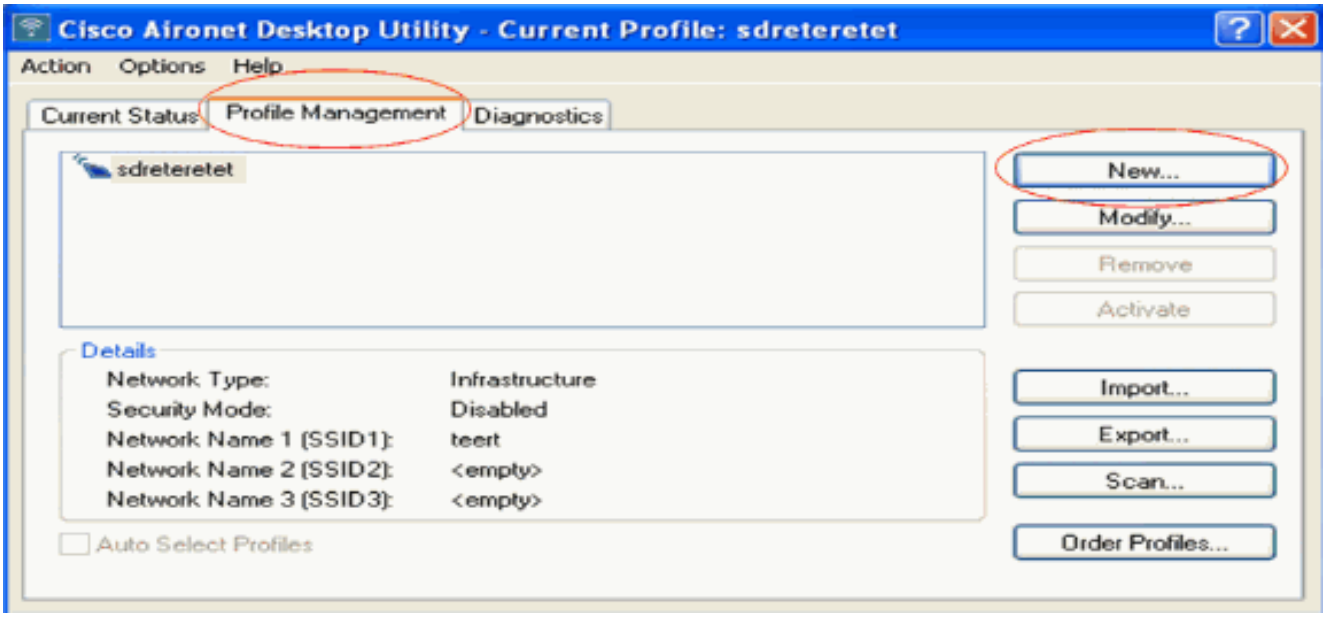
이 예에서는 오른쪽의 둘러싸인 필드를 관찰합니다.

6. 이 문서의 Configure WLC with Details of LDAP Server(LDAP 서버 세부사항으로 WLC 구성) 섹션에서 설명한 대로 **User Attribute(사용자 특성) 필드**에 사용자 이름이 포함된 사용자 레코드의 특성 이름을 입력합니다.이 LDP 출력에서 sAMAccountName이 사용자 이름 "user2"를 포함하는 하나의 특성임을 알 수 있습니다. 따라서 WLC의 **User Attribute** 필드에 해당하는 **sAMAccountName** 특성을 입력합니다.
7. 레코드를 **사용자로** 식별하는 LDAP objectType 특성의 값을 User Object Type 필드에 입력합니다. 사용자 레코드에는 objectType 특성에 대한 여러 값이 있는 경우가 많습니다. 그중 일부는 사용자에게 고유하고 일부는 다른 객체 유형과 공유됩니다.LDP 출력에서 **CN=Person**은 레코드를 사용자로 식별하는 하나의 값입니다. 따라서 WLC에서 **User Object Type 특성**으로 Person을 지정합니다.

무선 클라이언트 구성

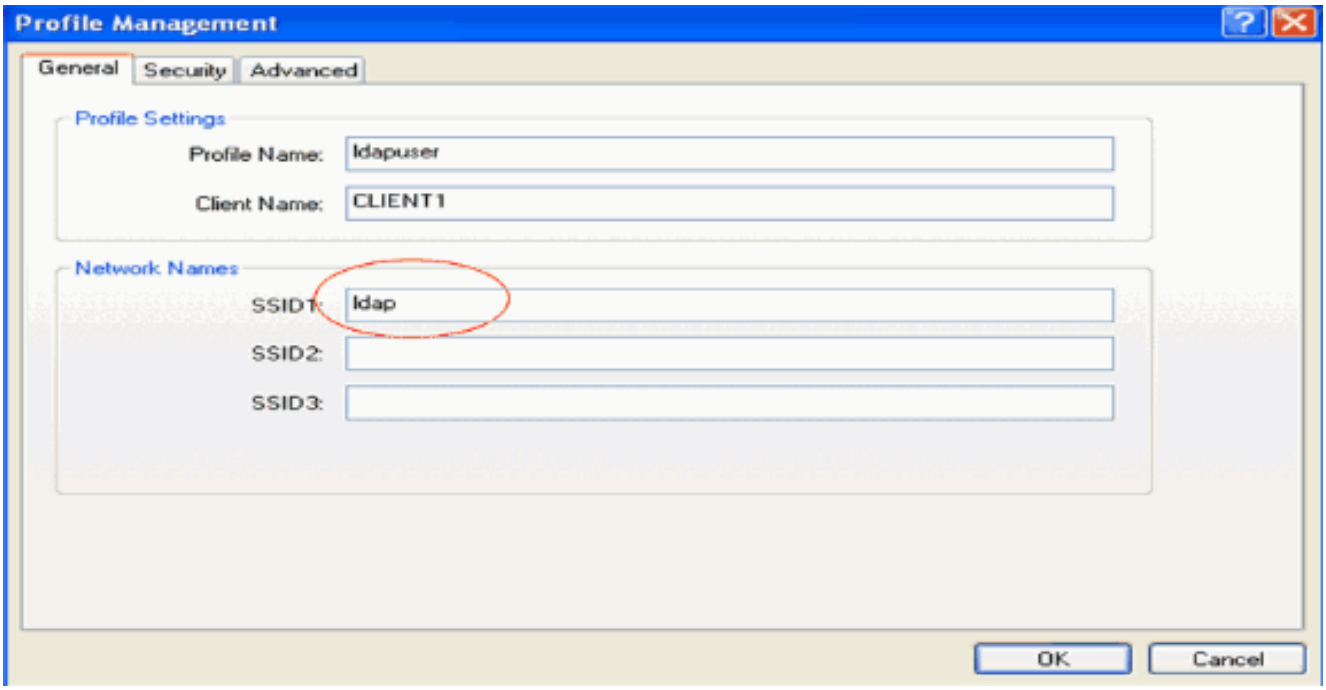
마지막 단계는 클라이언트 및 서버 인증서를 사용하여 EAP-FAST 인증을 위한 무선 클라이언트를 구성하는 것입니다. 이를 위해 다음 단계를 완료하십시오.

1. **Cisco** Aironet **Desktop Utility**(ADU)를 시작합니다. 새 무선 클라이언트 프로파일을 생성하려면 ADU 기본 **창**에서 **Profile Management(프로파일 관리)** > New(새로 만들기)를 클릭합니다.



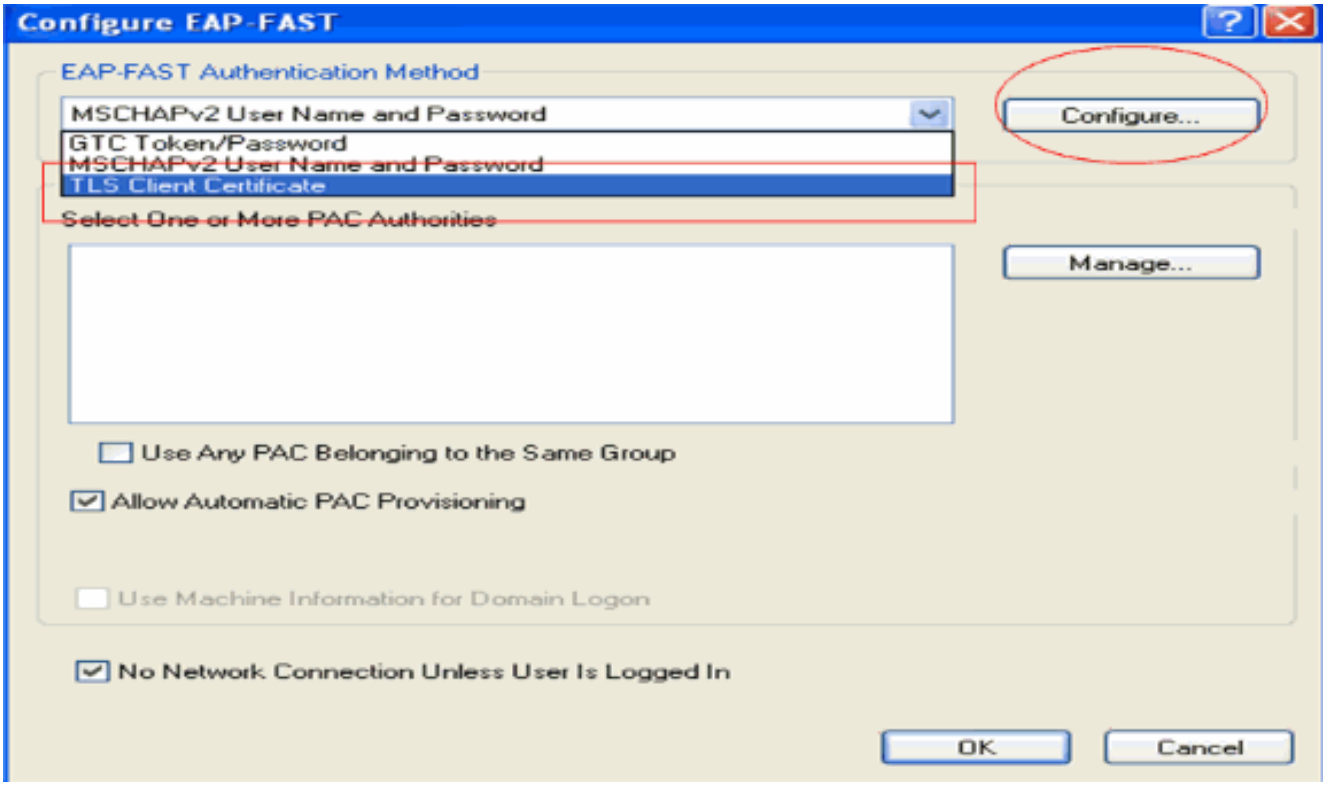
2. 프로파일 이름을 지정하고 이 프로파일에 SSID 이름을 할당합니다. 이 SSID 이름은 WLC에 구성된 것과 동일해야 합니다. 이 예에서 SSID 이름은 ldap**입니다**

.



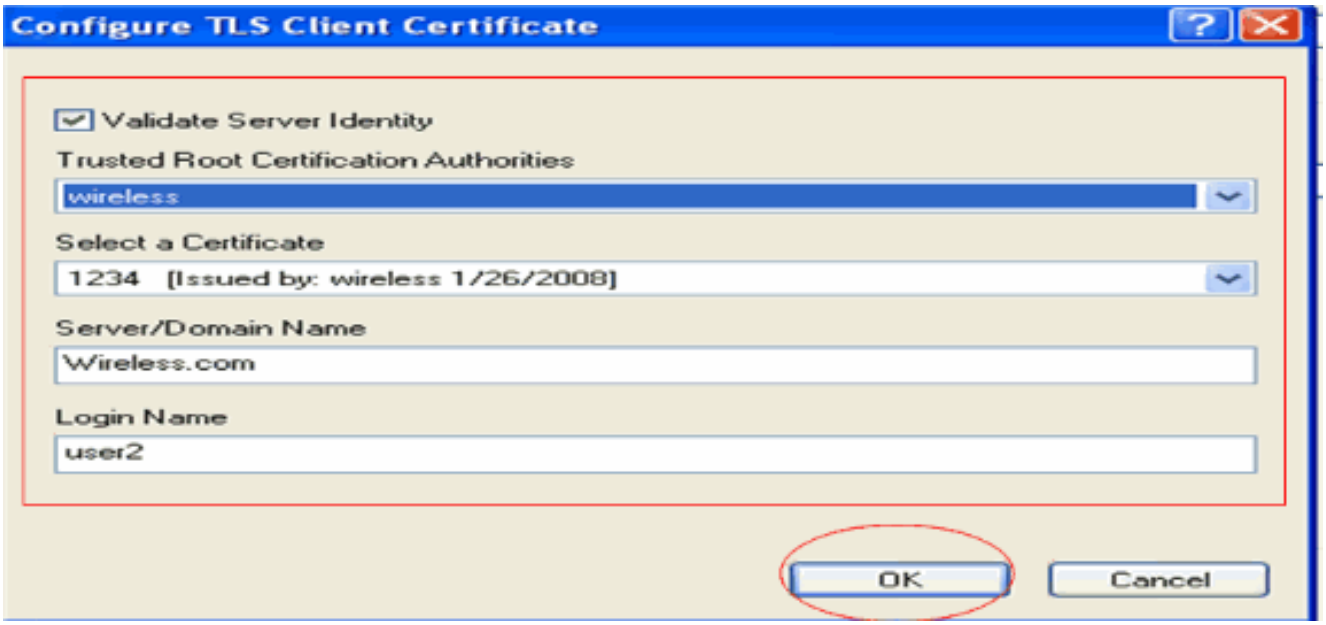
3. **Security(보안) 탭**을 클릭하고 **802.1x/EAP를** Layer 2 Security(레이어 2 보안)로 선택합니다. EAP **방법으로 EAP-**FAST를 선택하고 Configure를 **클릭합니다**.
4. EAP-FAST 구성 페이지의 EAP-FAST 인증 방법 드롭다운 상자에서 TLS **클라이언트 인증서**를 선택하고 구성을 **클릭합니다**

.



5. TLS Client certificate configuration(TLS 클라이언트 인증서 컨피그레이션) 창에서Validate **Server Identity(서버 ID 검증**) 확인란을 활성화하고 클라이언트에 설치된 CA 인증서(이 문서의 클라이언트에 대한 루트 CA 인증서 생성 섹션 참조)를 신뢰할 수 있는 루트 인증 기관으로 선택합니다.클라이언트에 설치된 디바이스 인증서(이 문서의 클라이언트에 대한 디바이스 인증서 생성 섹션에서 설명)를 클라이언트 인증서로 선택합니다.**OK(확인)**를 클릭합니다.다음 예에서는 이 단계를 설명합니다

.



무선 클라이언트 프로파일이 생성됩니다.

다음을 확인합니다.

컨피그레이션이 제대로 작동하는지 확인하려면 다음 단계를 수행하십시오.

1. ADU에서 **ldap** SSID를 활성화합니다.
2. 다음 창에서 **Yes(예)** 또는 **OK(확인)**를 클릭합니다. ADU에서 성공하려면 클라이언트 인증의

모든 단계 및 연결을 볼 수 있어야 합니다.

설정이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오. WLC CLI 모드를 사용합니다.

- WLC가 LDAP 서버와 통신할 수 있는지 확인하고 사용자를 찾으려면 WLC CLI에서 debug aaa ldap **enable** 명령을 지정합니다. 다음 예에서는 성공적인 통신 LDAP 프로세스에 대해 설명합니다.**참고:** 이 섹션의 출력 중 일부는 공간을 고려하여 두 번째 행으로 이동되었습니다.(Cisco 컨트롤러) **>debug aaa ldap enable**

```
Sun Jan 27 09:23:46 2008: AuthenticationRequest: 0xba96514
Sun Jan 27 09:23:46 2008:       Callback.....................................0x8
344900
Sun Jan 27 09:23:46 2008:       protocolType.................................0x0
0100002
Sun Jan 27 09:23:46 2008:       proxyState...................................00:
40:96:AC:E6:57-00:00
Sun Jan 27 09:23:46 2008:       Packet contains 2 AVPs (not shown)
Sun Jan 27 09:23:46 2008: ldapTask [1] received msg 'REQUEST' (2) in state 'IDLE' (1)
Sun Jan 27 09:23:46 2008: LDAP server 1 changed state to INIT
Sun Jan 27 09:23:46 2008: ldapInitAndBind [1] called lcapi_init (rc = 0 - Success)
Sun Jan 27 09:23:46 2008: ldapInitAndBind [1] called lcapi_bind (rc = 0 - Success)
Sun Jan 27 09:23:46 2008: LDAP server 1 changed state to CONNECTED
Sun Jan 27 09:23:46 2008: LDAP server 1 now active
Sun Jan 27 09:23:46 2008: LDAP_CLIENT: UID Search (base=OU=ldapuser,DC=wireless,
DC=com, pattern=(&(objectclass=Person)(sAMAccountName=user2))
Sun Jan 27 09:23:46 2008: LDAP_CLIENT: Returned msg type 0x64
Sun Jan 27 09:23:46 2008: ldapAuthRequest [1] called lcapi_query base="OU=ldapus
er,DC=wireless,DC=com" type="Person" attr="sAMAccountName" user="user2" (rc = 0
- Success)
Sun Jan 27 09:23:46 2008: LDAP ATTR> dn = CN=abcd,OU=ldapuser,DC=Wireless,DC=com
 (size 38)
Sun Jan 27 09:23:46 2008: Handling LDAP response Success
```

이 디버그 출력에서 강조 표시된 정보를 보면 WLC에서 WLC에 지정된 사용자 특성을 사용하여 LDAP 서버를 쿼리하고 LDAP 프로세스가 성공했음을 알 수 있습니다.

- 로컬 EAP 인증이 성공적인지 확인하려면 WLC CLI에서 **debug aaa local-auth eap method events enable** 명령을 지정합니다. 예를 들면 다음과 같습니다.(Cisco 컨트롤러) **>debug aaa local-auth eap method events enable**

```
Sun Jan 27 09:38:28 2008: eap_fast.c-EVENT: New context
(EAP handle = 0x1B000009)

Sun Jan 27 09:38:28 2008: eap_fast.c-EVENT: Allocated new EAP-FAST context
(handle = 0x22000009)

Sun Jan 27 09:38:28 2008: eap_fast_auth.c-AUTH-EVENT: Process Response
(EAP handle = 0x1B000009)

Sun Jan 27 09:38:28 2008: eap_fast_auth.c-AUTH-EVENT: Received Identity

Sun Jan 27 09:38:28 2008: eap_fast_tlv.c-AUTH-EVENT: Adding PAC A-ID TLV
(436973636f000000000000000000000)

Sun Jan 27 09:38:28 2008: eap_fast_auth.c-AUTH-EVENT: Sending Start

Sun Jan 27 09:38:29 2008: eap_fast.c-AUTH-EVENT: Process Response, type: 0x2b

Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Process Response
(EAP handle = 0x1B000009)

Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT:
Received TLS record type: Handshake in state: Start
```

Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Local certificate found

Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Reading Client Hello handshake

Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT:
TLS_DHE_RSA_AES_128_CBC_SHA proposed...

Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: Proposed ciphersuite(s):

Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: TLS_DHE_RSA_WITH_AES_128_CBC_SHA

Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: TLS_RSA_WITH_AES_128_CBC_SHA

Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: TLS_RSA_WITH_RC4_128_SHA

Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: Selected ciphersuite:

Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: TLS_DHE_RSA_WITH_AES_128_CBC_SHA

Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Building Provisioning Server Hello

**Sun Jan 27 09:38:29 2008: eap_fast_crypto.c-EVENT:
Starting Diffie Hellman phase 1 ...**

**Sun Jan 27 09:38:30 2008: eap_fast_crypto.c-EVENT:
Diffie Hellman phase 1 complete**

Sun Jan 27 09:38:30 2008: eap_fast_auth.c-AUTH-EVENT: DH signature length = 128

Sun Jan 27 09:38:30 2008: eap_fast_auth.c-AUTH-EVENT: Sending Provisioning Serving Hello

Sun Jan 27 09:38:30 2008: eap_fast.c-EVENT: Tx packet fragmentation required

Sun Jan 27 09:38:30 2008: eap_fast.c-AUTH-EVENT: eap_fast_rx_packet():
EAP Fast NoData (0x2b)

Sun Jan 27 09:38:30 2008: eap_fast.c-AUTH-EVENT: eap_fast_rx_packet():
EAP Fast NoData (0x2b)

Sun Jan 27 09:38:30 2008: eap_fast.c-AUTH-EVENT: eap_fast_rx_packet():
EAP Fast NoData (0x2b)

Sun Jan 27 09:38:32 2008: eap_fast.c-AUTH-EVENT: Process Response, type: 0x2b

Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Reassembling TLS record

Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Sending EAP-FAST Ack

.....

.....

.....

**Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT:
Received TLS record type: Handshake in state: Sent provisioning Server Hello**

**Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT:
Reading Client Certificate handshake**

Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Added certificate 1 to chain

Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Added certificate 2 to chain

Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Successfully validated received certificate

Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT: Rx'd I-ID:
"EAP-FAST I-ID" from Peer Cert

Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT:
Reading Client Key Exchange handshake

Sun Jan 27 09:38:32 2008: eap_fast_crypto.c-EVENT:
Starting Diffie Hellman phase 2 ...

Sun Jan 27 09:38:32 2008: eap_fast_crypto.c-EVENT:
Diffie Hellman phase 2 complete.

Sun **Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT:**
Reading Client Certificate Verify handshake

Sun Jan 27 09:38:32 2008: eap_fast_crypto.c-EVENT:
Sign certificate verify succeeded (compare)

.....

.....

.....

.....
.

- debug **aaa local-auth db enable** 명령도 매우 유용합니다. 예를 들면 다음과 같습니다.(Cisco 컨트롤러) **>debug aaa local-auth db enable**

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: EAP: Received an auth request

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Creating new context

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Local auth profile name for context 'ldapuser'

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Created new context eap session handle fb000007

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: (EAP:8) Sending the Rxd EAP packet
(id 2) to EAP subsys

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Found matching context for id - 8

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: (EAP) Sending user credential
request username 'user2' to LDAP

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Found context matching MAC address - 8

.....

.....

.....

.....

Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) Sending the Rxd EAP packet
(id 12) to EAP subsys

Sun Jan 27 09:35:36 2008: LOCAL_AUTH: Found matching context for id - 8

```
Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) ---> [KEY AVAIL] send_len 64, recv_len 0

Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) received keys waiting for success

Sun Jan 27 09:35:36 2008: LOCAL_AUTH: Found matching context for id - 8

Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) Received success event

Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) Processing keys success
```

- 로컬 인증에 사용할 WLC에 설치된 인증서를 보려면 WLC CLI에서 **show local-auth certificates** 명령을 실행합니다. 예를 들면 다음과 같습니다.(Cisco Controller) **>show local-auth certificates**

```
Certificates available for Local EAP authentication:


Certificate issuer ............................. vendor

  CA certificate:

    Subject: DC=com, DC=Wireless, CN=wireless

     Issuer: DC=com, DC=Wireless, CN=wireless

      Valid: 2008 Jan 23rd, 15:50:27 GMT to 2013 Jan 23rd, 15:50:27 GMT

  Device certificate:

    Subject: O=cisco, CN=ciscowlc123

     Issuer: DC=com, DC=Wireless, CN=wireless

      Valid: 2008 Jan 24th, 12:18:31 GMT to 2010 Jan 23rd, 12:18:31 GMT


Certificate issuer ............................. cisco

  CA certificate:

    Subject: O=Cisco Systems, CN=Cisco Manufacturing CA

     Issuer: O=Cisco Systems, CN=Cisco Root CA 2048

      Valid: 2005 Jun 10th, 22:16:01 GMT to 2029 May 14th, 20:25:42 GMT

   Device certificate:

            Not installed.
```

- CLI 모드에서 WLC의 로컬 인증 컨피그레이션을 보려면 **show local-auth config 명령을** 실행합니다. 예를 들면 다음과 같습니다.(Cisco Controller) **>show local-auth config**

```
User credentials database search order:

    Primary ..................................... LDAP


Timer:

    Active timeout ............................. 300
```

```
Configured EAP profiles:

    Name ..................................... ldapuser

      Certificate issuer ..................... vendor

      Peer verification options:

        Check against CA certificates ........... Enabled

        Verify certificate CN identity .......... Disabled

        Check certificate date validity ......... Disabled

      EAP-FAST configuration:

        Local certificate required .............. Yes

        Client certificate required ............. Yes

      Enabled methods ......................... fast

      Configured on WLANs ..................... 2


EAP Method configuration:

    EAP-FAST:

--More-- or (q)uit

      Server key .............................. <hidden>

      TTL for the PAC ......................... 10

      Anonymous provision allowed ............. No

      ........................................

      ........................................

      Authority Information ................... Cisco A-ID
```

문제 해결

다음 명령을 사용하여 컨피그레이션의 문제를 해결할 수 있습니다.

- **debug aaa local-auth eap method events enable**
- **debug aaa all enable**
- **debug dot1x packet enable**

관련 정보

- 무선 LAN 컨트롤러 및 외부 RADIUS 서버 컨피그레이션을 통한 EAP-FAST 인증 예
- Microsoft IAS(Internet Authentication Service)를 사용하는 Unified Wireless Networks에서

PEAP
- ACS를 기반으로 한 WLC를 통한 동적 VLAN 할당 - Active Directory 그룹 매핑 컨피그레이션 예
- Cisco Wireless LAN Controller 컨피그레이션 가이드 - 보안 솔루션 구성
- Cisco Wireless LAN Controller 컨피그레이션 가이드 - 컨트롤러 소프트웨어 및 컨피그레이션 관리
- WLAN 컨트롤러(WLC)를 사용한 EAP 인증 컨피그레이션 예
- WLC(Wireless LAN Controller) 설계 및 기능 FAQ
- EAP-FAST 인증을 사용하는 Cisco Secure Services Client
- 무선 LAN 컨트롤러(WLC)에 대한 FAQ
- 컨트롤러 WLC(Wireless LAN Controller) 오류 및 시스템 메시지 FAQ
- 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.