Unified Wireless Network 로컬 EAP 서버 컨피그레이션 예

목차

소개

이 문서에서는 무선 사용자 인증을 위한 Cisco WLC(Wireless LAN Controller)의 로컬 EAP(Extensible Authentication Protocol) 서버 컨피그레이션에 대해 설명합니다.

로컬 EAP는 사용자 및 무선 클라이언트가 로컬로 인증될 수 있도록 하는 인증 방법입니다.백엔드 시스템이 중단되거나 외부 인증 서버가 다운될 때 무선 클라이언트와의 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 로컬 사용자 데이터베이스 또는 LDAP(Lightweight Directory Access Protocol) 백엔드 데이터베이스에서 사용자 자격 증명을 검색하여 사용자를 인증합니다.로컬 EAP는 LEAP(Lightweight EAP), EAP-FAST(Flexible Authentication via Secure Tunneling), 컨트롤러와 무선 클라이언트 간의 EAP-TLS(Transport Layer Security) 인증을 지원합니다.

WLC에 전역 외부 RADIUS 서버 컨피그레이션이 있는 경우 로컬 EAP 서버를 사용할 수 없습니다.모든 인증 요청은 로컬 EAP 서버를 사용할 수 있을 때까지 전역 외부 RADIUS로 전달됩니다.WLC가 외부 RADIUS 서버에 대한 연결을 끊으면 로컬 EAP 서버가 활성화됩니다.전역 RADIUS 서버 컨피그레이션이 없는 경우 로컬 EAP 서버가 즉시 활성 상태가 됩니다.다른 WLC에 연결된 클

라이언트를 인증하는 데 로컬 EAP 서버를 사용할 수 없습니다.즉, 하나의 WLC가 인증을 위해 다른 WLC에 EAP 요청을 전달할 수 없습니다.모든 WLC에는 고유한 로컬 EAP 서버 및 개별 데이터베이스가 있어야 합니다.

참고: WLC가 외부 RADIUS 서버로 요청을 보내는 것을 중지하려면 다음 명령을 사용합니다.

```
config wlan disable
        config wlan radius_server auth disable
        config wlan enable
```

로컬 EAP 서버는 4.1.171.0 소프트웨어 릴리스 이상에서 다음 프로토콜을 지원합니다.

- LEAP
- EAP-FAST(사용자 이름/비밀번호 및 인증서 모두)
- EAP-TLS

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 기본 운영을 위해 WLC 및 LAP(Lightweight Access Point)를 구성하는 방법에 대한 지식
- LWAPP(Lightweight Access Point Protocol) 및 무선 보안 방법에 대한 지식
- 로컬 EAP 인증에 대한 기본 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Windows XP with CB21AG Adapter Card and Cisco Secure Services Client Version 4.05
- Cisco 4400 Wireless LAN Controller 4.1.171.0
- Windows 2000 서버의 Microsoft 인증 기관

표기 규칙

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

Cisco Wireless LAN Controller에서 로컬 EAP 구성

이 문서에서는 WLC의 기본 컨피그레이션이 이미 완료된 것으로 가정합니다.

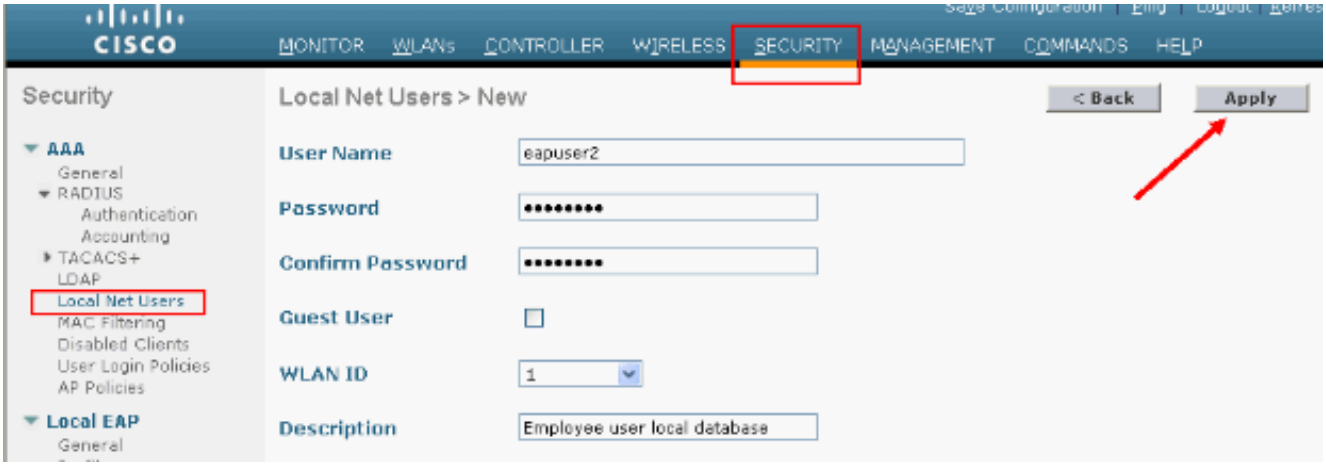
로컬 EAP 컨피그레이션

로컬 EAP를 구성하려면 다음 단계를 완료합니다.

1. 로컬 네트 사용자 추가:GUI에서 **Security(보안) > Local Net Users(로컬 네트워크 사용자) > New(새로 만들기)를** 선택하고 User Name(사용자 이름), Password(비밀번호), Guest User(게

스트 사용자), WLAN ID 및 Description(설명)을 입력하고 **Apply(적용)를** 클릭합니다

.

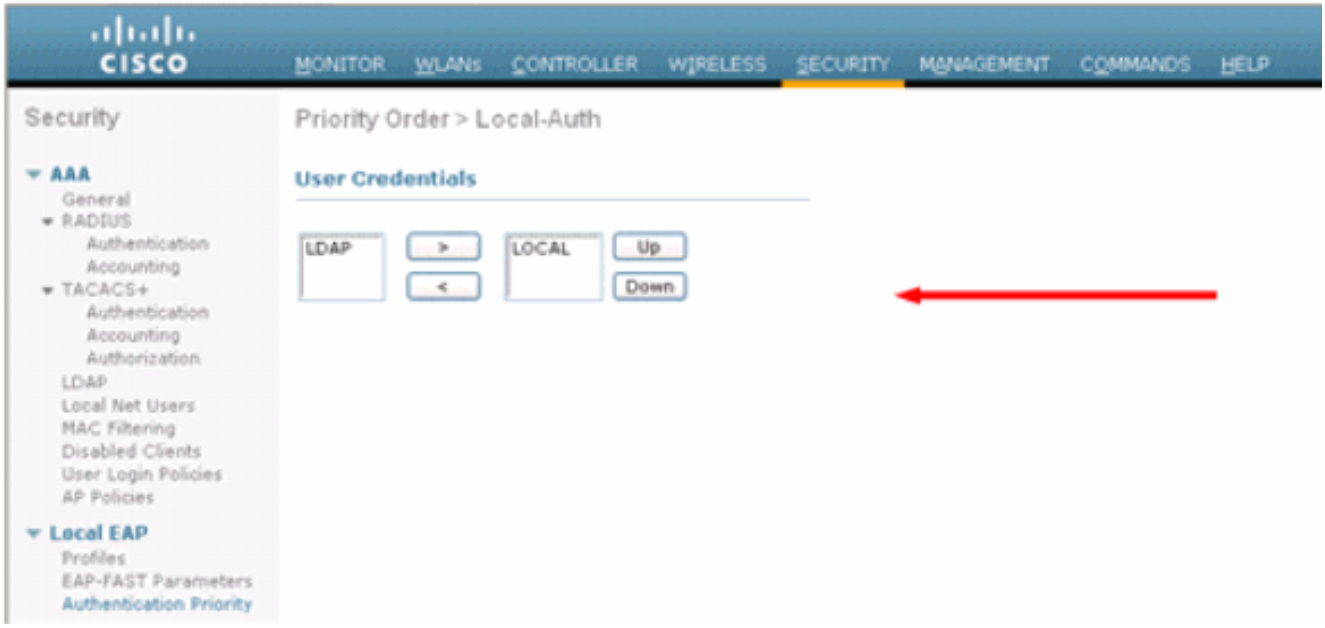


CLI에서 config netuser **add <*username*><password><WLAN id><*description*> 명령을** 사용할 수 있습니다.**참고:** 공간 이유로 이 명령이 두 번째 줄로 내려갔습니다.

```
(Cisco Controller) >config netuser add eapuser2 cisco123 1 Employee user local database
```

2. 사용자 자격 증명 검색 순서를 지정합니다.GUI에서 Security(보안) **> Local EAP(로컬 EAP) > Authentication Priority(인증 우선순위)를** 선택합니다.그런 다음 LDAP를 선택하고 "<" 버튼을 클릭하고 **Apply**(적용)를 클릭합니다.이렇게 하면 먼저 로컬 데이터베이스에 사용자 자격 증명이 저장됩니다

.

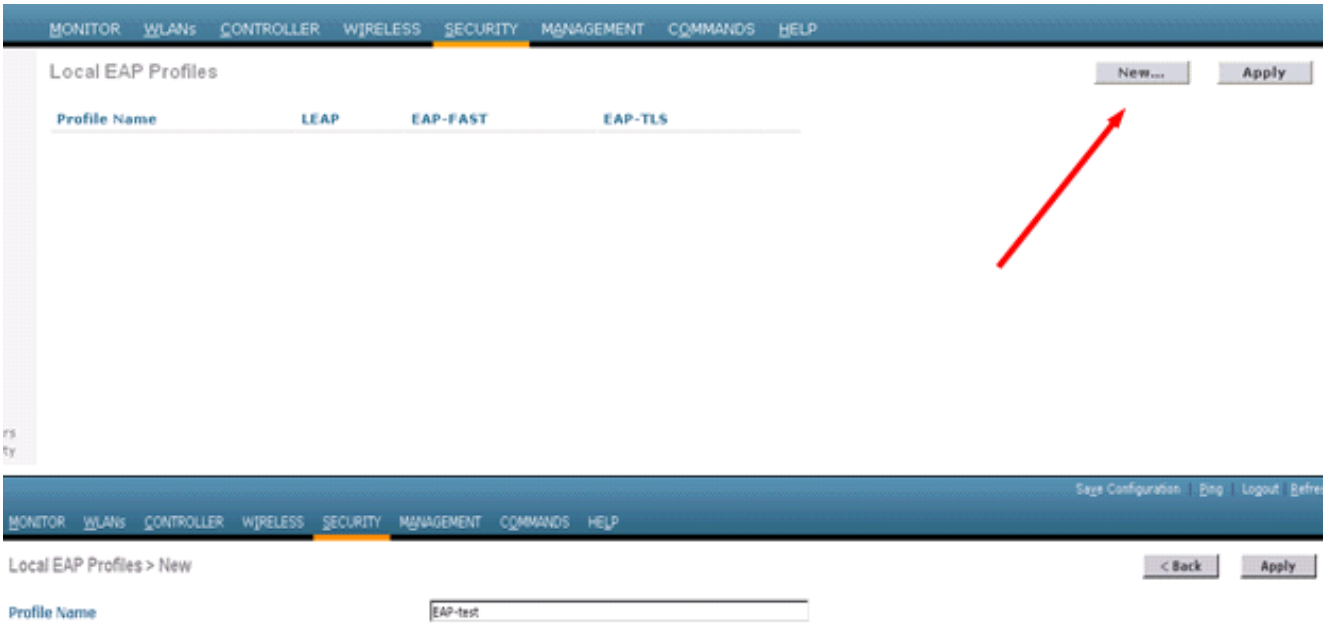


CLI에서 다음을 수행합니다.

```
(Cisco Controller) >config local-auth user-credentials local
```

3. EAP 프로파일 추가:GUI에서 이 작업을 수행하려면 **Security(보안) > Local EAP(로컬 EAP) > Profiles(프로파일)를** 선택하고 **New(새로 만들기)**를 클릭합니다.새 창이 나타나면 프로파일 이름을 입력하고 **적용**을 클릭합니다

.

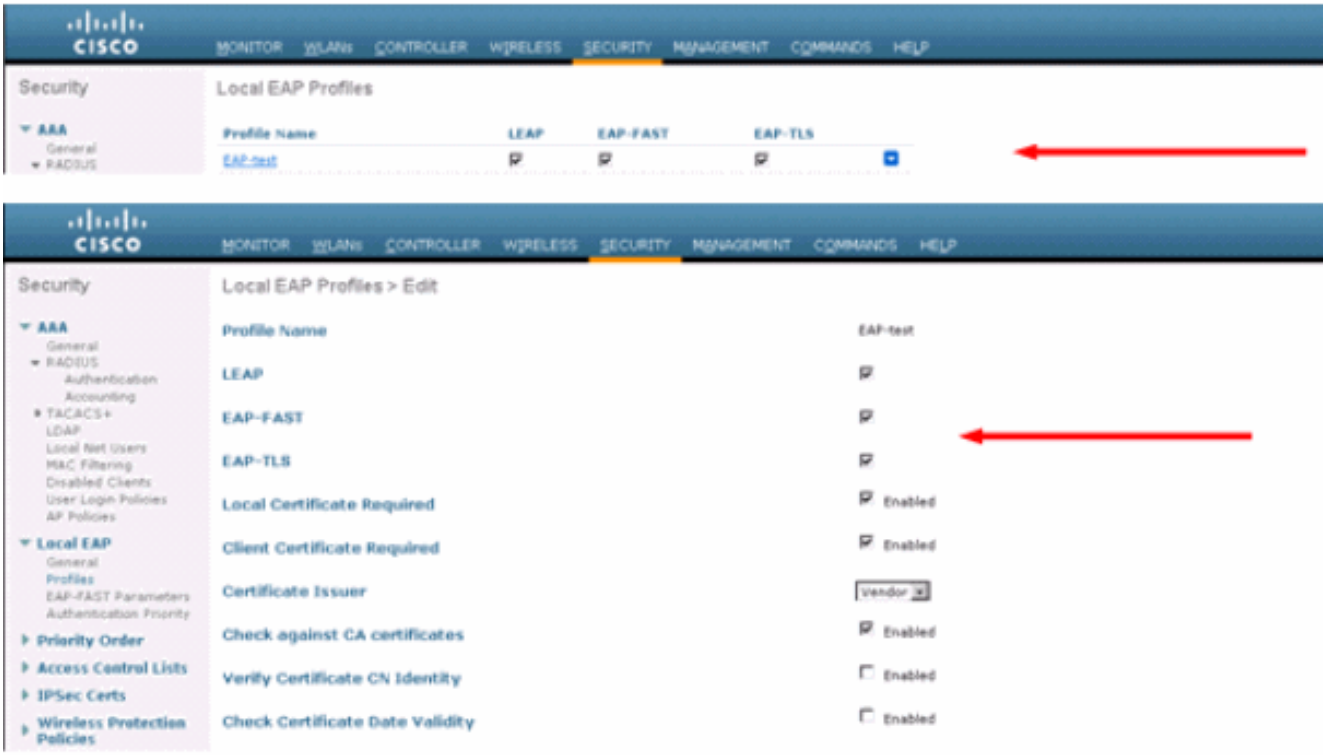


CLI 명령 config local-auth eap-**profile add** *<profile-name>* **를** 사용하여 이 **작업을** 수행할 수도 있습니다. 이 예에서 프로파일 이름은 *EAP-test입니다*.

```
(Cisco Controller) >config local-auth eap-profile add EAP-test
```

4. EAP 프로파일에 방법을 추가합니다.GUI에서 **Security(보안) > Local EAP(로컬 EAP) > Profiles(프로파일)를** 선택하고 인증 방법을 추가할 프로파일 이름을 클릭합니다.이 예에서는 LEAP, EAP-FAST 및 EAP-TLS를 사용합니다.**적용**을 클릭하여 방법을 설정합니다

.

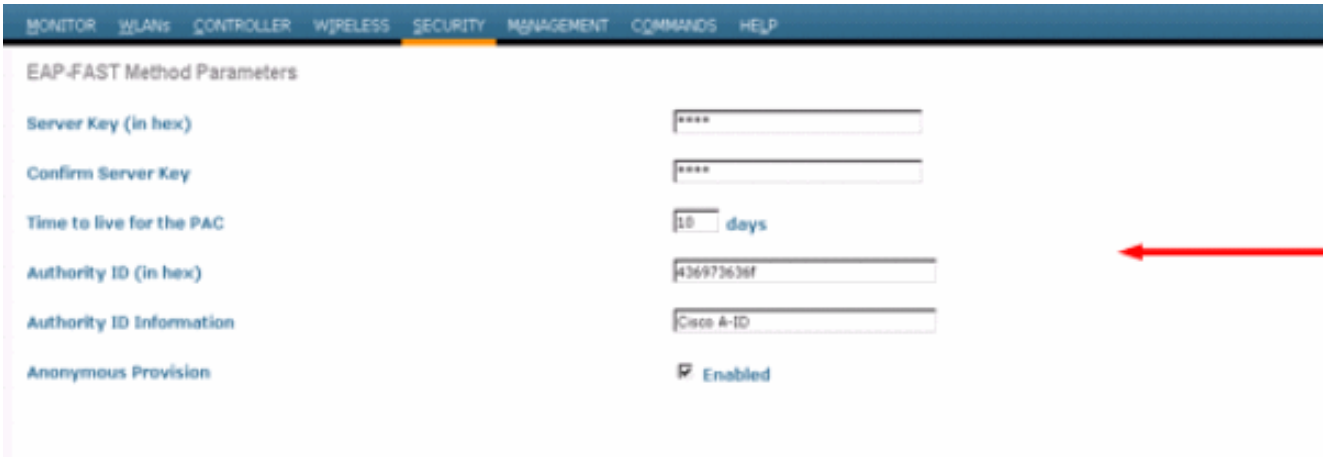


또한 CLI 명령 **config local-auth eap-profile method add** *<method-name>*<profile-*name>을* 사용할 수 있습니다.예제 컨피그레이션에서는 프로파일 EAP-test에 세 가지 방법을 추가합니다.방법 이름은 각각 *leap, fast* 및 *tls*인 LEAP, EAP-FAST 및 EAP-TLS입니다.이 출력은 CLI 컨피그레이션 명령을 보여줍니다.

```
(Cisco Controller) >config local-auth eap-profile method add leap EAP-test
(Cisco Controller) >config local-auth eap-profile method add fast EAP-test
(Cisco Controller) >config local-auth eap-profile method add tls EAP-test
```

5. EAP 방법의 매개변수를 구성합니다.EAP-FAST에만 사용됩니다.구성할 매개변수는 다음과 같습니다.**Server Key (server-key)**—PAC(Protected Access Credentials)를 암호화/해독하기 위한 서버 키(16진수).**Time to Live for PAC (pac-ttl)** - PAC에 대한 Time to Live를 설정합니다 .**Authority ID (authority-id)(권한 ID(authority-id))** - 권한 식별자를 설정합니다.**Anonymous Provision (anonymous-provision)** - 익명 프로비저닝을 허용할지 여부를 구성합니다.기본적으로 활성화되어 있습니다.GUI를 통한 컨피그레이션의 경우 **Security(보안) > Local EAP(로컬 EAP) > EAP-FAST Parameters(EAP-FAST 매개변수)**를 선택하고 Server key(서버 키), Time to live for the PAC, authority ID(16진수) 및 Authority ID Information(권한 ID 정보) 값을 입력합니다

.

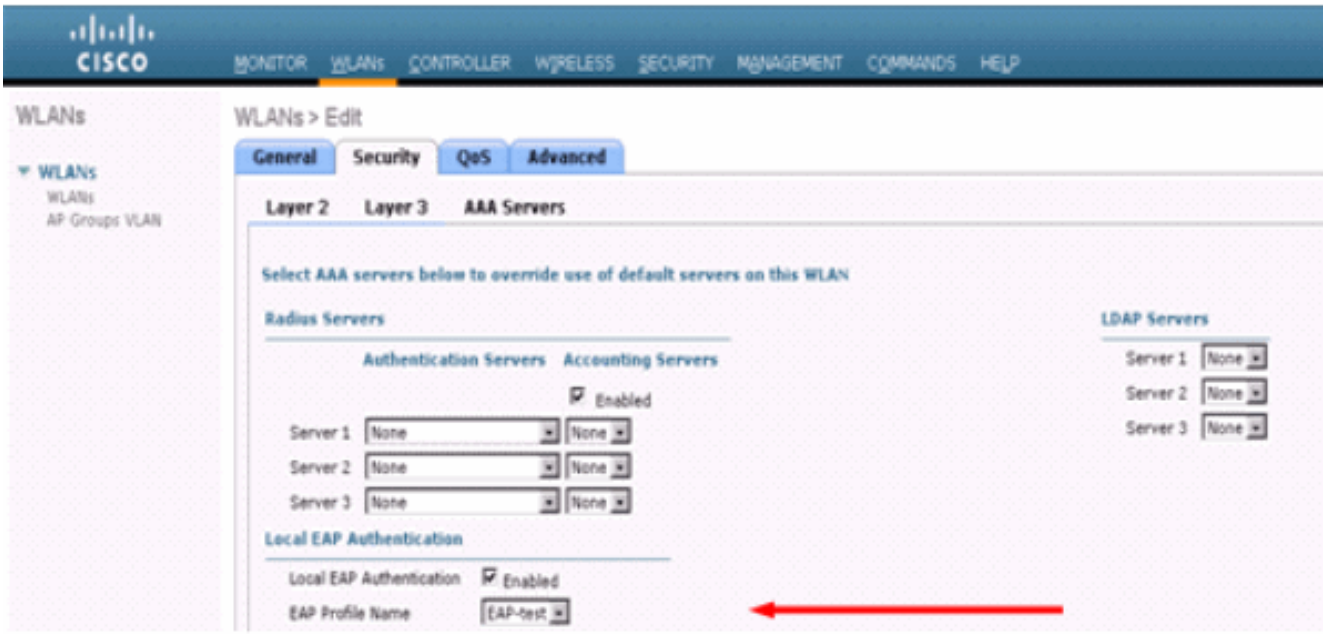


다음은 EAP-FAST에 대해 이러한 매개변수를 설정하기 위해 사용할 CLI 컨피그레이션 명령입니다.

```
(Cisco Controller) >config local-auth method fast server-key 12345678
(Cisco Controller) >config local-auth method fast authority-id 43697369f1 CiscoA-ID
(Cisco Controller) >config local-auth method fast pac-ttl 10
```

6. WLAN당 로컬 인증 활성화:GUI에서 상단 메뉴에서 WLANs를 선택하고 로컬 인증을 구성할 WLAN을 선택합니다.새 창이 나타납니다.Security(**보안) > AAA 탭을** 클릭합니다.로컬 **EAP 인증**을 선택하고 다음 예와 같이 풀다운 메뉴에서 올바른 EAP 프로파일 이름을 선택합니다

.



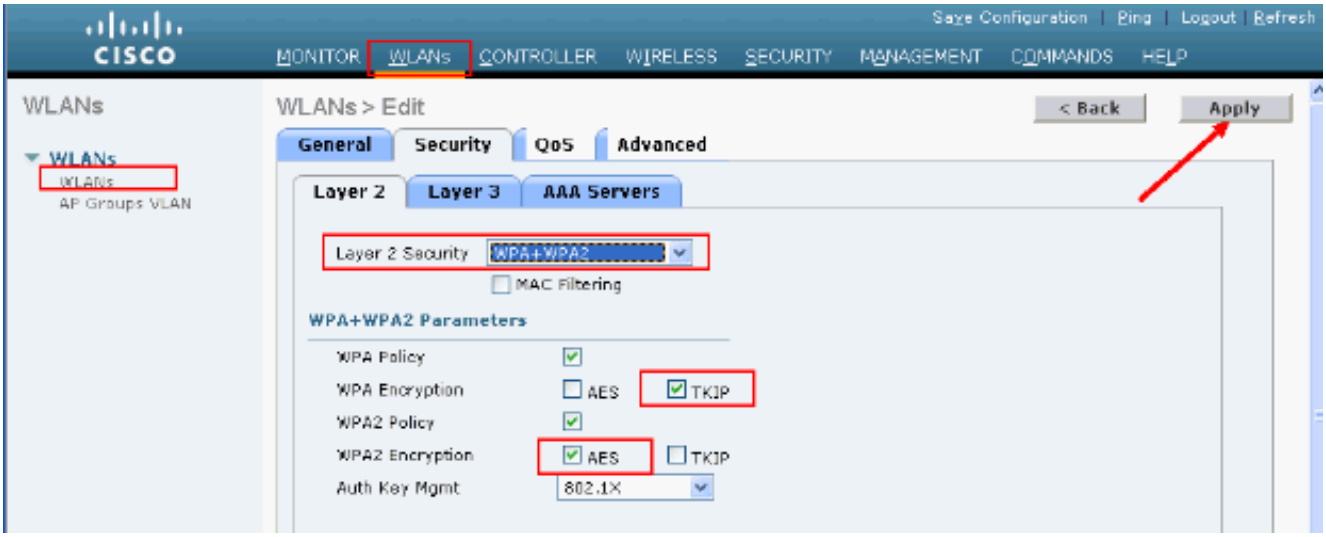
CLI config wlan local-**auth enable *<profile-name> <wlan-id>* 컨피그레이션 명령도** 여기에 나

와 있습니다.

```
(Cisco Controller) >config wlan local-auth enable EAP-test 1
```

7. 레이어 2 보안 매개변수를 설정합니다.GUI 인터페이스에서 WLAN Edit(WLAN 편집) 창의 **Security(보안) > Layer 2(레이어 2)** 탭으로 이동하여 Layer 2 Security(레이어 2 보안) 풀다운 메뉴에서 WPA+WPA2를 선택합니다.WPA+WPA2 매개변수 섹션에서 WPA 암호화를 TKIP 및 WPA2 암호화 AES로 **설정합니다**.그런 다음 **Apply를** 클릭합니다

.



CLI에서 다음 명령을 사용합니다.

```
(Cisco Controller) >config wlan security wpa enable 1
(Cisco Controller) >config wlan security wpa wpa1 ciphers tkip enable 1
(Cisco Controller) >config wlan security wpa wpa2 ciphers aes enable 1
```

8. 구성을 확인합니다.

```
(Cisco Controller) >show local-auth config

User credentials database search order:
    Primary ..................................... Local DB

Timer:
    Active timeout .............................. Undefined

Configured EAP profiles:
    Name ........................................ EAP-test
      Certificate issuer ........................ cisco
      Peer verification options:
        Check against CA certificates ........... Enabled
        Verify certificate CN identity .......... Disabled
        Check certificate date validity ......... Enabled
      EAP-FAST configuration:
        Local certificate required .............. No
        Client certificate required ............. No
      Enabled methods ........................... leap fast tls
      Configured on WLANs ....................... 1

EAP Method configuration:
    EAP-FAST:
--More-- or (q)uit
      Server key ................................ <hidden>
      TTL for the PAC ........................... 10
      Anonymous provision allowed ............... Yes
      Authority ID .............................. 43697369f1000000000000000000
      Authority Information ..................... CiscoA-ID
```

show wlan *<wlan id>* 명령을 사용하여 wlan 1의 특정 매개변수를 확인할 수 있습니다.

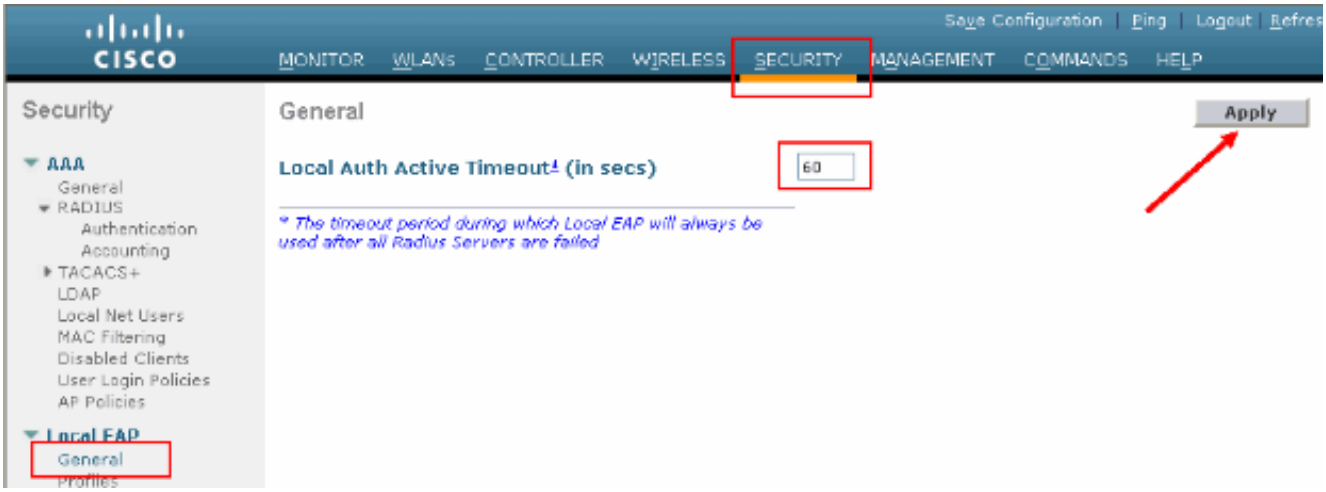
```
(Cisco Controller) >show wlan 1
```

```
WLAN Identifier.................................. 1
Profile Name..................................... austinlab
Network Name (SSID).............................. austinlab
Status........................................... Disabled
MAC Filtering.................................... Disabled
Broadcast SSID................................... Enabled
AAA Policy Override.............................. Disabled
Number of Active Clients......................... 0
Exclusionlist Timeout............................ 60 seconds
Session Timeout.................................. 1800 seconds
Interface........................................ management
WLAN ACL......................................... unconfigured
DHCP Server...................................... Default
DHCP Address Assignment Required................. Disabled
Quality of Service............................... Silver (best effort)
WMM.............................................. Disabled
CCX - AironetIe Support.......................... Enabled
CCX - Gratuitous ProbeResponse (GPR)............. Disabled
Dot11-Phone Mode (7920).......................... Disabled
Wired Protocol................................... None
--More-- or (q)uit
IPv6 Support..................................... Disabled
Radio Policy..................................... All
Local EAP Authentication......................... Enabled (Profile 'EAP-test')
Security

   802.11 Authentication:........................ Open System
   Static WEP Keys............................... Disabled
   802.1X........................................ Disabled
   Wi-Fi Protected Access (WPA/WPA2)............. Enabled
      WPA (SSN IE)............................... Enabled
         TKIP Cipher............................. Enabled
         AES Cipher.............................. Disabled
      WPA2 (RSN IE)............................... Enabled
         TKIP Cipher............................. Disabled
         AES Cipher.............................. Enabled
                                                        Auth Key Management
         802.1x.................................. Enabled
         PSK..................................... Disabled
         CCKM.................................... Disabled
   CKIP ........................................... Disabled
   IP Security..................................... Disabled
   IP Security Passthru............................ Disabled
   Web Based Authentication........................ Disabled
--More-- or (q)uit
   Web-Passthrough................................. Disabled
   Conditional Web Redirect........................ Disabled
   Auto Anchor..................................... Disabled
   Cranite Passthru................................ Disabled
   Fortress Passthru............................... Disabled
   H-REAP Local Switching.......................... Disabled
   Infrastructure MFP protection................... Enabled
                                             (Global Infrastructure MFP Disabled)
   Client MFP...................................... Optional
   Tkip MIC Countermeasure Hold-down Timer....... 60

 Mobility Anchor List
 WLAN ID     IP Address       Status
```

구성할 수 있는 다른 로컬 인증 매개변수, 특히 활성 시간 초과 타이머가 있습니다.이 타이머는 모든 RADIUS 서버가 실패한 후 로컬 EAP가 사용되는 기간을 구성합니다.GUI에서 **Security(보안) > Local EAP(로컬 EAP) > General(일반)을** 선택하고 시간 값을 설정합니다.그

런 다음 **Apply**를 클릭합니다

.



CLI에서 다음 명령을 실행합니다.

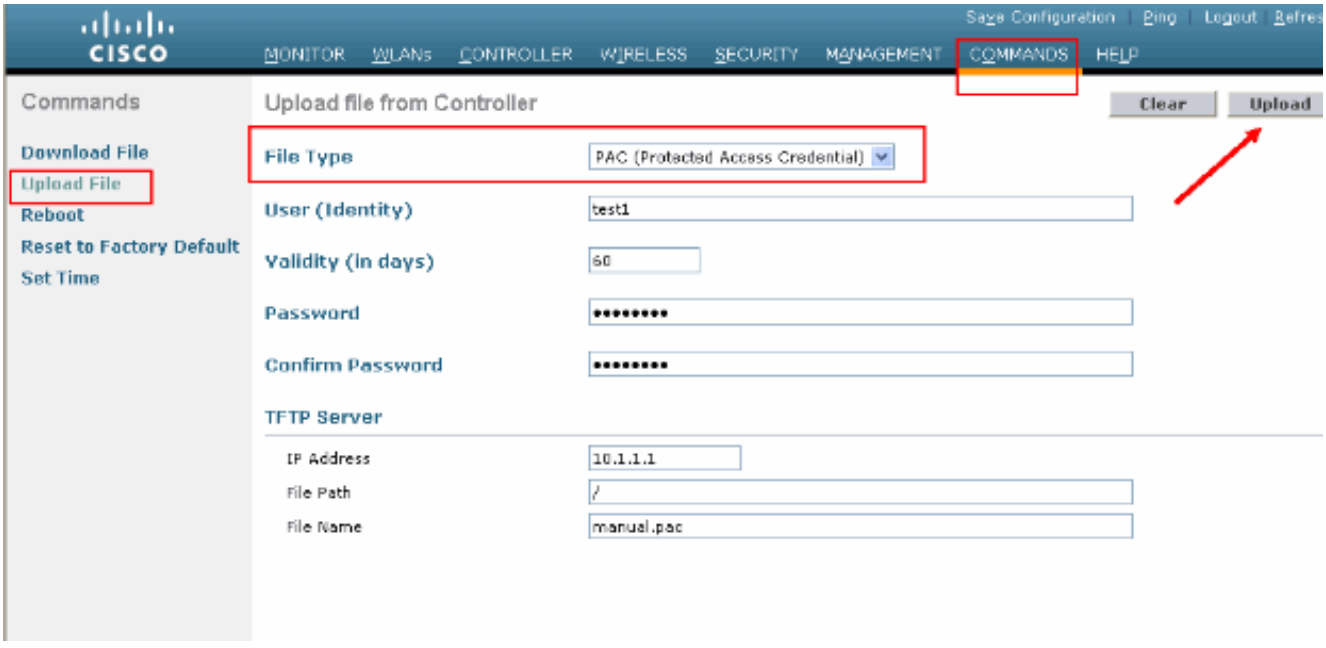
```
(Cisco Controller) >config local-auth active-timeout ?
<1 to 3600> Enter the timeout period for the Local EAP to remain active,
in seconds.
(Cisco Controller) >config local-auth active-timeout 60
```

show local-auth config 명령을 실행할 때 이 타이머가 설정된 값을 확인할 수 있습니다.

```
(Cisco Controller) >show local-auth config

User credentials database search order:
    Primary ..................................... Local DB

Timer:
    Active timeout ............................... 60

Configured EAP profiles:
    Name ........................................ EAP-test
... Skip
```

9. 수동 PAC를 생성하고 로드해야 하는 경우 GUI 또는 CLI를 사용할 수 있습니다.GUI의 상단 메뉴에서 **COMMANDS**를 선택하고 오른쪽 목록에서 **Upload File**을 선택합니다.File **Type(파일 유형)** 풀다운 메뉴에서 PAC(Protected Access Credential)를 선택합니다.모든 매개변수를 입력하고 Upload(업로드)를 **클릭합니다**

.



CLI에서 다음 명령을 입력합니다.

```
(Cisco Controller) >transfer upload datatype pac
(Cisco Controller) >transfer upload pac ?

username     Enter the user (identity) of the PAC

 (Cisco Controller) >transfer upload pac test1 ?

<validity>     Enter the PAC validity period (days)

(Cisco Controller) >transfer upload pac test1 60 ?

<password>     Enter a password to protect the PAC

 (Cisco Controller) >transfer upload pac test1 60 cisco123

(Cisco Controller) >transfer upload serverip 10.1.1.1

(Cisco Controller) >transfer upload filename manual.pac

(Cisco Controller) >transfer upload start

Mode..................................................... TFTP
TFTP Server IP........................................... 10.1.1.1
TFTP Path................................................ /
TFTP Filename............................................ manual.pac
Data Type................................................ PAC
PAC User................................................. test1
PAC Validity............................................. 60 days
PAC Password............................................. cisco123

Are you sure you want to start? (y/N) y
PAC transfer starting.
File transfer operation completed successfully.
```

Microsoft 인증 기관

EAP-FAST 버전 2 및 EAP-TLS 인증을 사용하려면 WLC 및 모든 클라이언트 장치에 유효한 인증서가 있어야 하며 인증 기관의 공개 인증서도 알아야 합니다.

설치

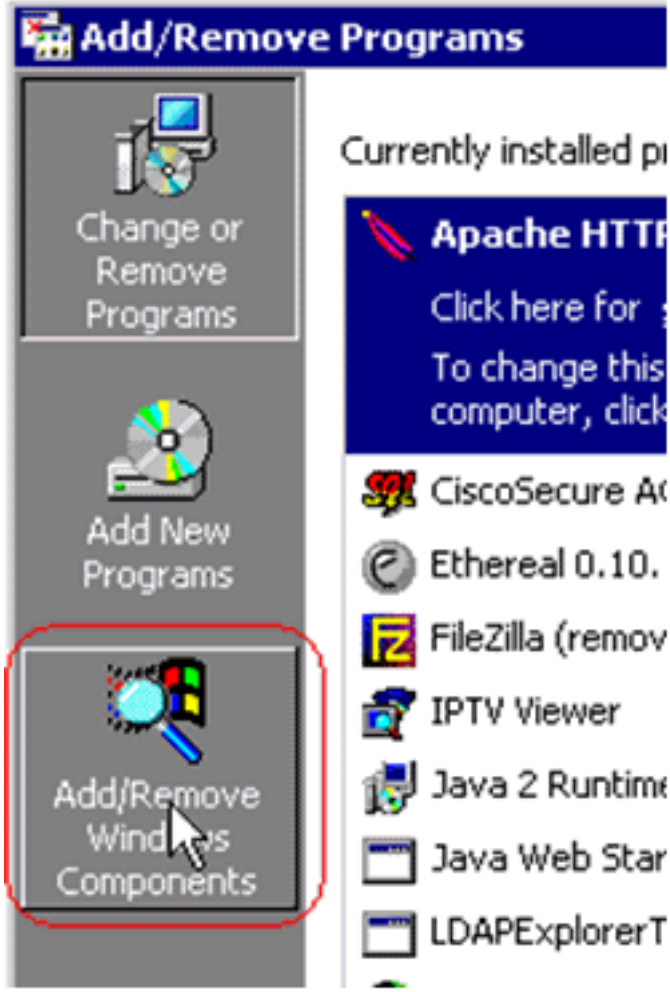
Windows 2000 Server에 인증 기관 서비스가 설치되어 있지 않으면 설치해야 합니다.

Windows 2000 Server에서 Microsoft 인증 기관을 활성화하려면 다음 단계를 완료하십시오.

1. 제어판에서 프로그램 **추가/제거**를 선택합니다

.:

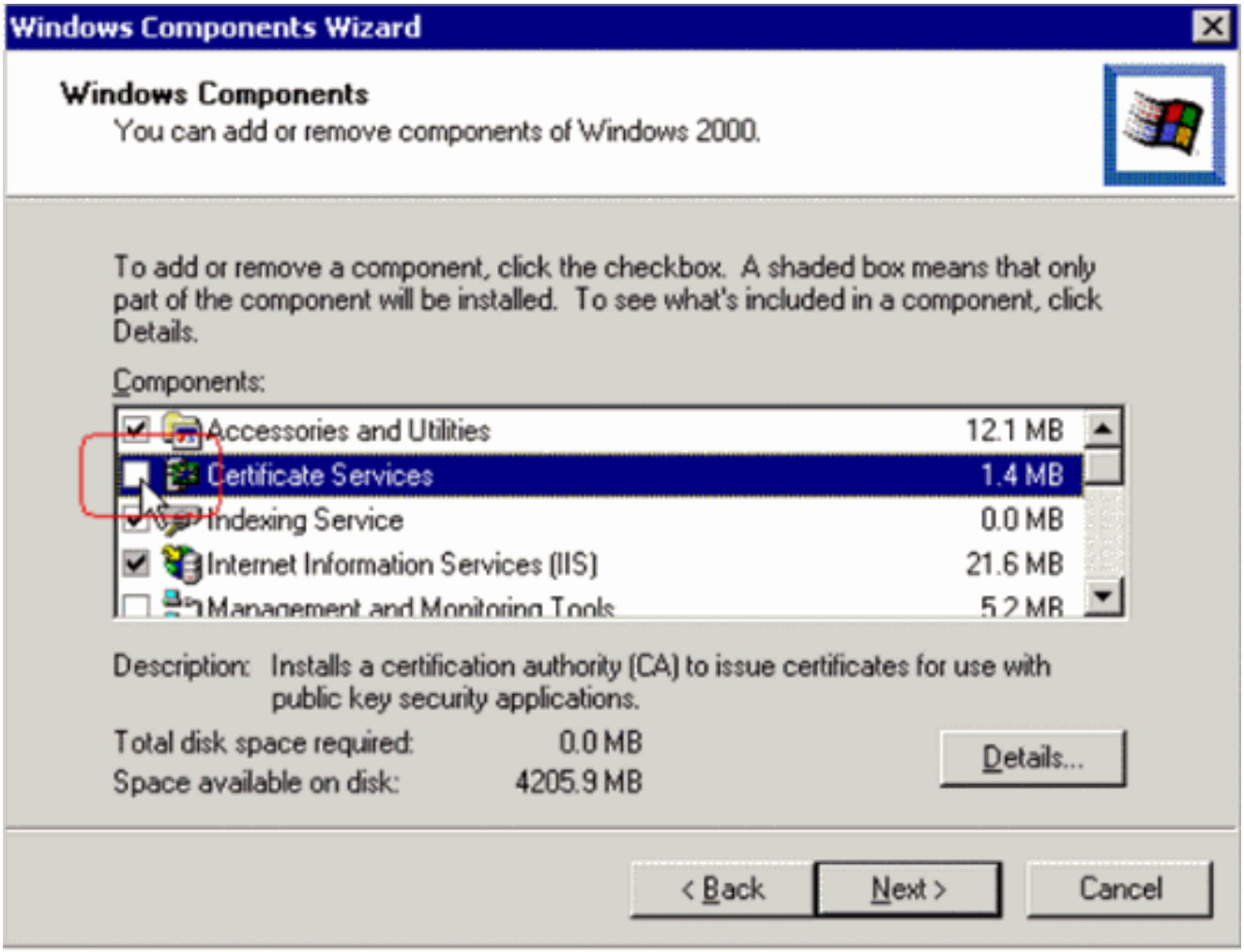
2. 왼쪽에서 **Windows 구성 요소 추가/제거**를 선택합니다



.

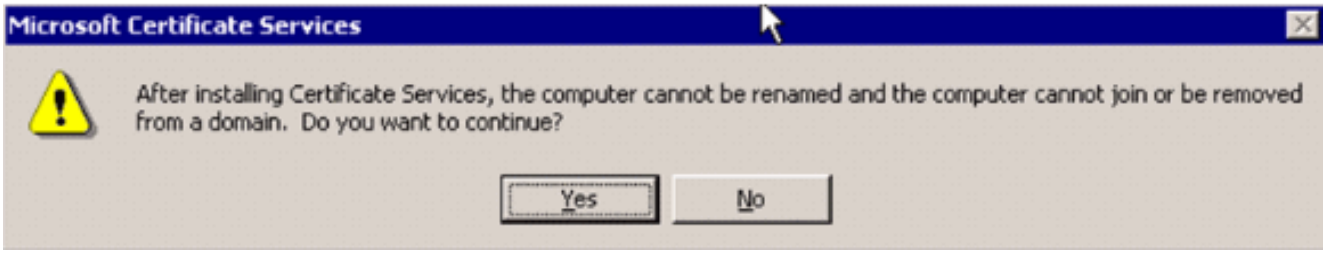
3. 인증서 **서비스를 확인합니다**

.



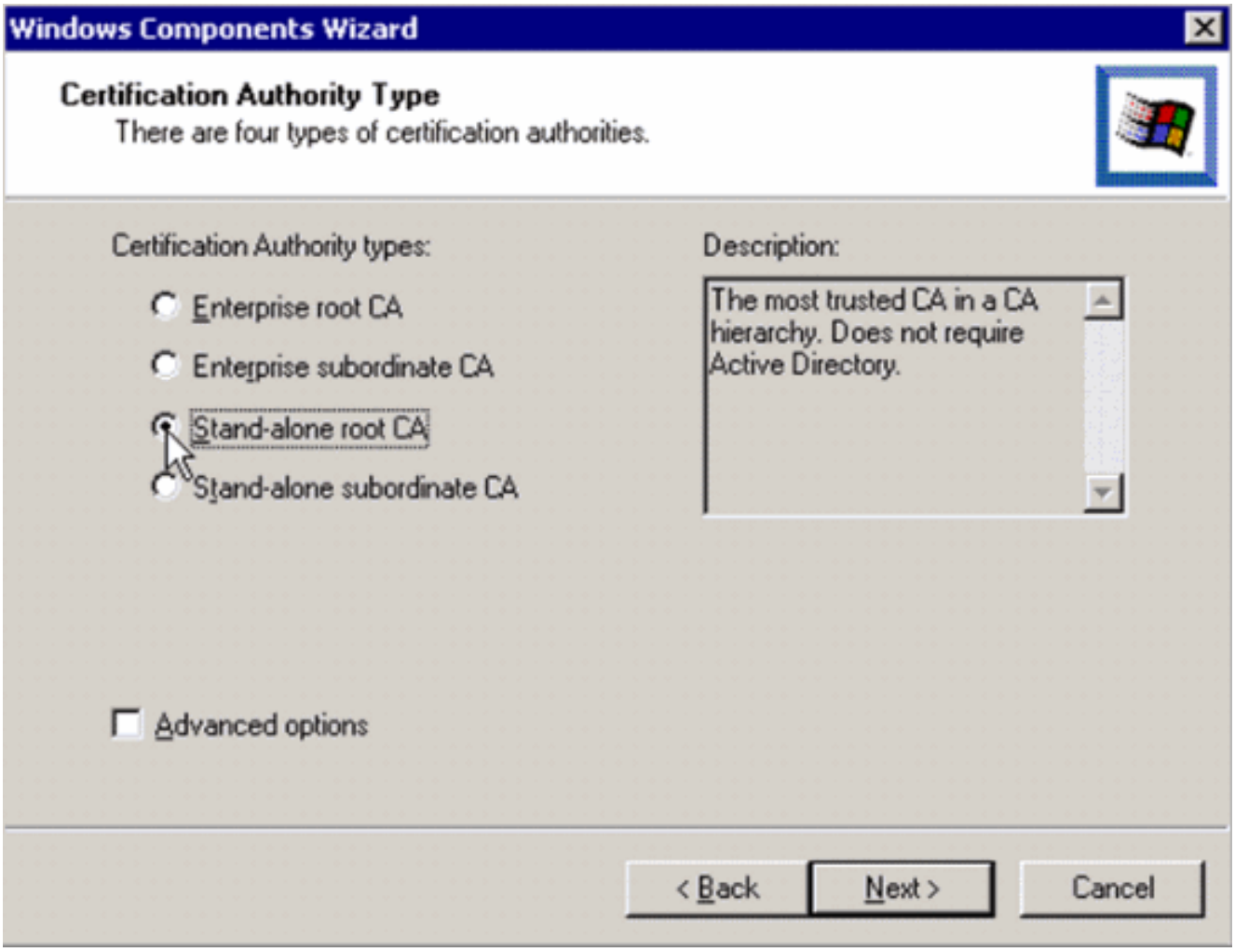
계속하기 전에 이 경고를 검토하십시오

.

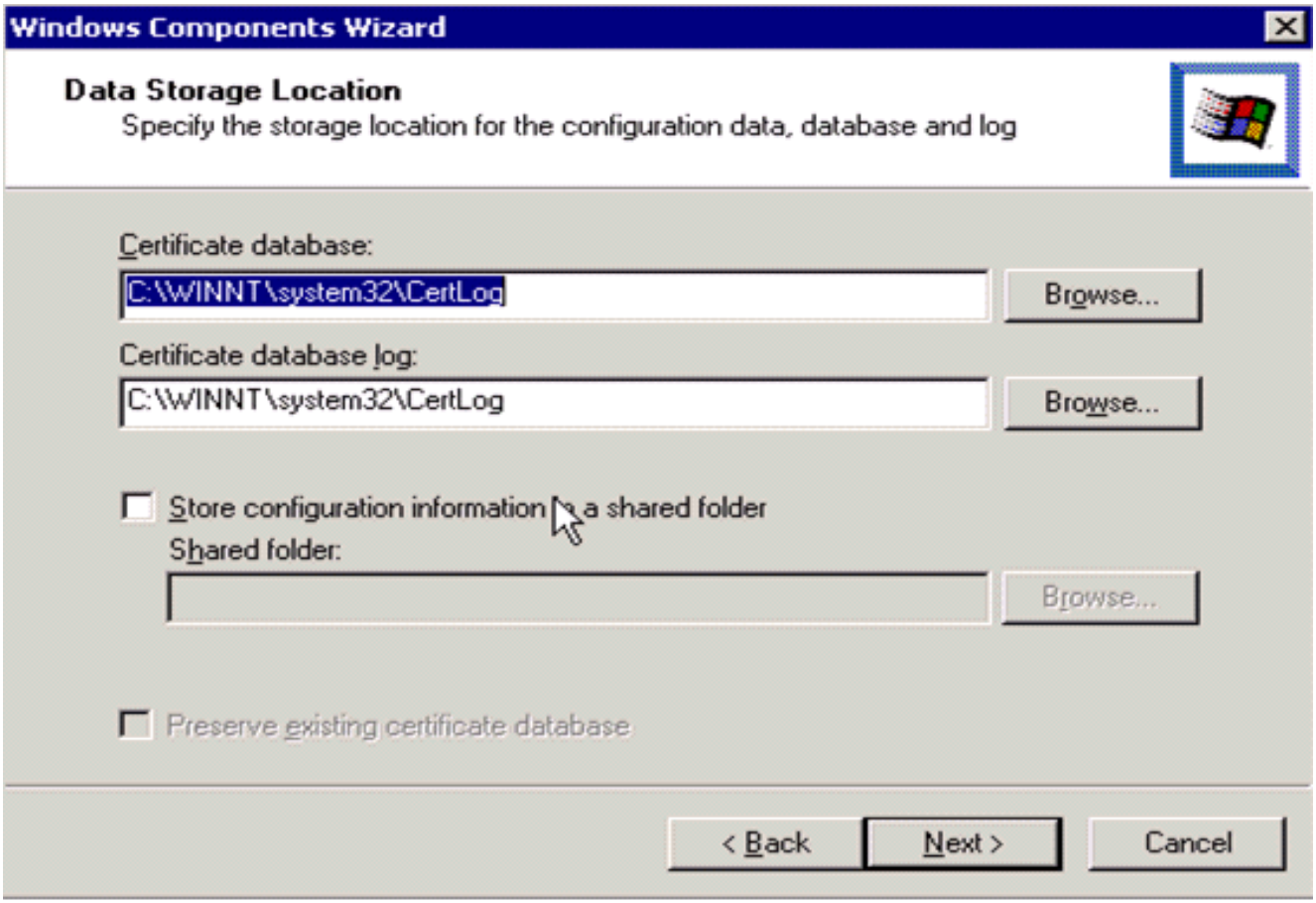


4. 설치할 인증 기관 유형을 선택합니다.간단한 독립형 권한을 생성하려면 독립형 **루트 CA**를 선택합니다

.

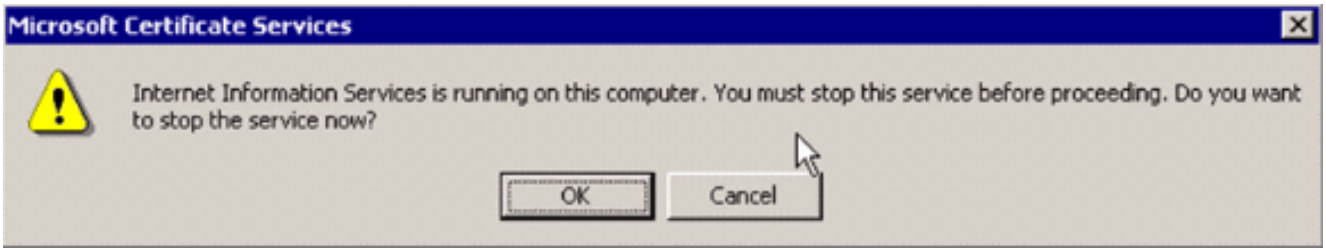


5. 인증 기관에 필요한 정보를 입력합니다.이 정보는 인증 기관에 대한 자체 서명 인증서를 생성합니다.사용하는 CA 이름을 기억하십시오.인증 기관은 인증서를 데이터베이스에 저장합니다.이 예에서는 Microsoft에서 제안하는 기본 설정을 사용합니다
.



6. Microsoft 인증 기관 서비스는 클라이언트 및 서버 인증서를 만들고 관리하기 위해 IIS Microsoft 웹 서버를 사용합니다.다음에 대한 IIS 서비스를 다시 시작해야 합니다

.



이제 Microsoft Windows 2000 Server가 새 서비스를 설치합니다.새 Windows 구성 요소를 설치하려면 Windows 2000 Server 설치 CD가 있어야 합니다.인증 기관이 설치되었습니다.

Cisco Wireless LAN Controller에 인증서 설치

Cisco Wireless LAN Controller의 로컬 EAP 서버에서 EAP-FAST 버전 2 및 EAP-TLS를 사용하려면 다음 3단계를 수행하십시오.

1. 무선 LAN 컨트롤러에 장치 인증서를 설치합니다.
2. Wireless LAN Controller에 공급업체 CA 인증서를 다운로드합니다.
3. EAP-TLS를 사용하도록 무선 LAN 컨트롤러를 구성합니다.

이 문서에 표시된 예에서 ACS(Access Control Server)는 Microsoft Active Directory 및 Microsoft Certification Authority와 동일한 호스트에 설치되지만, ACS 서버가 다른 서버에 있는 경우에는 구성이 동일해야 합니다.

무선 LAN 컨트롤러에 장치 인증서 설치

다음 단계를 완료하십시오.

1. .WLC로 가져올 인증서를 생성하려면 다음 단계를 완료합니다.http://**<serverIpAddr>/certsrv로 이동합니다**.Request **a Certificate(인증서 요청)를** 선택하고 **Next(다음)**를 클릭합니다 .Advanced **Request(고급 요청)**를 선택하고 **Next(다음)**를 클릭합니다.Submit **a certificate request to this CA using a form(양식을 사용하여 이 CA에 인증서 요청 제출)을 선택하고 Next(다음**)를 클릭합니다.Certificate **Template(**인증서 템플릿)에 대한 웹 서버를 선택하고 관련 정보를 입력합니다.그런 다음 키를 내보낼 수 있는 것으로 **표시합니다**.이제 시스템에 설치해야 하는 인증서를 받습니다.
2. PC에서 인증서를 검색하려면 다음 단계를 완료합니다.Internet Explorer 브라우저를 열고 **도구 > 인터넷 옵션 > 콘텐츠를** 선택합니다.Certificates(**인증서)를 클릭합니다**.풀다운 메뉴에서 새로 설치된 인증서를 선택합니다.Export(내보내기)를 **클릭합니다**.Next(**다음)**를 두 번 클릭하고 **Yes export the private key(개인 키 내보내기 예)를 선택합니다**.이 형식은 PKCS#12(.PFX 형식)입니다.Enable **strong protection(강력한 보호 활성화)을 선택합니다**.비밀번호를 입력합니다.<tme2.pfx> 파일에 저장합니다.
3. PKCS#12 형식의 인증서를 PEM 형식으로 변환하기 위해 OpenssI이 설치된 컴퓨터에 복사합니다.

```
openssl pkcs12 -in tme2.pfx -out tme2.pem
!--- The command to be given, -in Enter Import Password: !--- Enter the password given
previously, from step 2g. MAC verified OK Enter PEM pass phrase: !--- Enter a phrase.
Verifying - Enter PEM pass phrase:
```

4. 변환된 PEM 형식 장치 인증서를 WLC에 다운로드합니다.

```
(Cisco Controller) >transfer download datatype eapdevcert

(Cisco Controller) >transfer download certpassword password
!--- From step 3. Setting password to <cisco123> (Cisco Controller) >transfer download
filename tme2.pem

(Cisco Controller) >transfer download start

Mode..................................................... TFTP
Data Type................................................ Vendor Dev Cert
TFTP Server IP........................................... 10.1.1.12
TFTP Packet Timeout...................................... 6
TFTP Max Retries......................................... 10
TFTP Path................................................ /
TFTP Filename............................................ tme2.pem

This may take some time.
Are you sure you want to start? (y/N) y

TFTP EAP Dev cert transfer starting.

Certificate installed.
  Reboot the switch to use new certificate.
```

5. 재부팅되면 인증서를 확인합니다.

```
(Cisco Controller) >show local-auth certificates

Certificates available for Local EAP authentication:

Certificate issuer ..................... vendor
  CA certificate:
    Subject: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme
     Issuer: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme
      Valid: 2007 Feb 28th, 19:35:21 GMT to 2012 Feb 28th, 19:44:44 GMT
  Device certificate:
    Subject: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme2
     Issuer: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme
```

```
        Valid: 2007 Mar 28th, 23:08:39 GMT to 2009 Mar 27th, 23:08:39 GMT
```

무선 LAN 컨트롤러에 공급업체 CA 인증서 다운로드

다음 단계를 완료하십시오.

1. 판매업체 CA 인증서를 검색하려면 다음 단계를 완료합니다.http://**<serverIpAddr>/certsrv로 이동합니다**.Retrieve **the CA Certificate(CA 인증서 검색)를** 선택하고 **Next(다음)**를 클릭합니다.CA 인증서를 선택합니다.DER encoded**를 클릭합니다**.Download **CA certificate(CA 인증서 다운로드)**를 클릭하고 인증서를 rootca.cer로 **저장합니다**.
2. 공급업체 CA를 DER 형식에서 PEM 형식으로 변환하고 openssl **x509 -in rootca.cer -inform DER -out rootca.pem -outform PEM** 명령**을 사용합니다**.출력 파일은 PEM 형식의 rootca.pem입니다.
3. 공급업체 CA 인증서 다운로드:

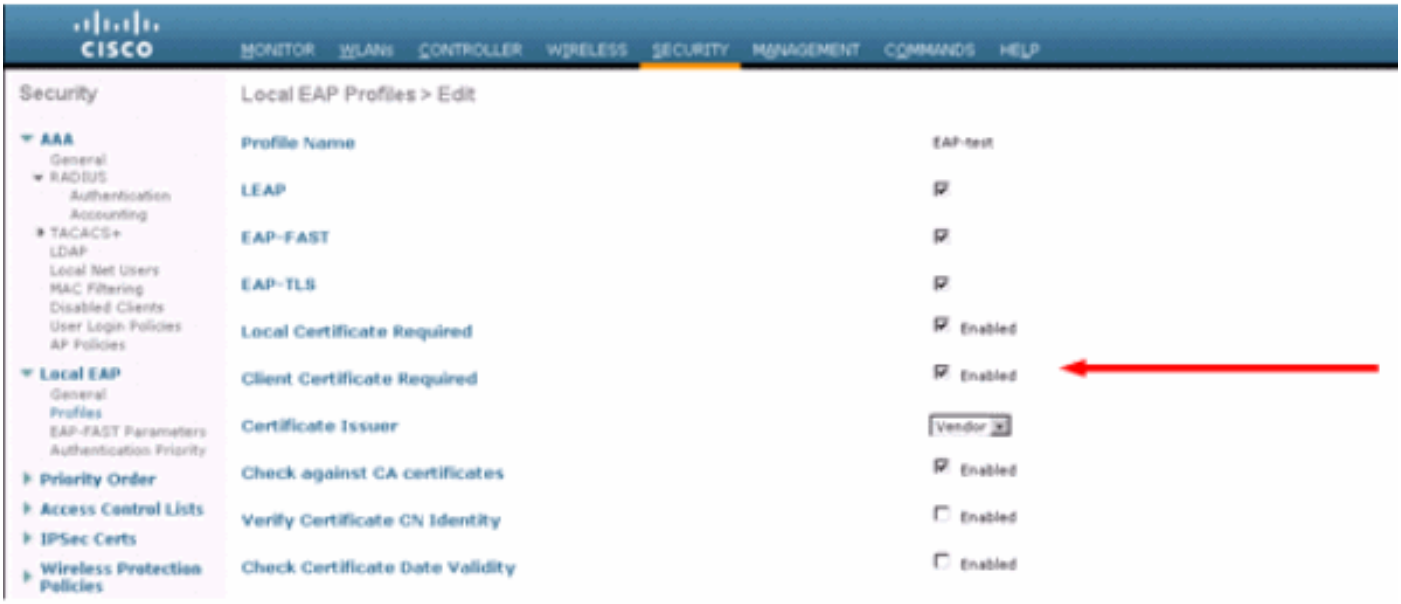
```
(Cisco Controller) >transfer download datatype eapcacert

(Cisco Controller) >transfer download filename ?

<filename>     Enter filename up to 16 alphanumeric characters.

(Cisco Controller) >transfer download filename rootca.pem

(Cisco Controller) >transfer download start ?

(Cisco Controller) >transfer download start

Mode..................................................... TFTP
Data Type................................................ Vendor CA Cert
TFTP Server IP........................................... 10.1.1.12
TFTP Packet Timeout...................................... 6
TFTP Max Retries......................................... 10
TFTP Path................................................ /
TFTP Filename............................................ rootca.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 new certificate.
```

EAP-TLS를 사용하도록 무선 LAN 컨트롤러 구성

다음 단계를 완료하십시오.

GUI에서 **Security(보안) > Local EAP(로컬 EAP) > Profiles(프로파일)**를 선택하고 프로파일을 선택하고 다음 설정을 확인합니다.

- Local Certificate Required(로컬 인증서 필요)가 활성화되어 있습니다.
- Client Certificate Required(필요한 클라이언트 인증서)가 활성화되어 있습니다.
- 인증서 발급자가 공급업체입니다.
- CA 인증서에 대한 확인이 활성화되었습니다.



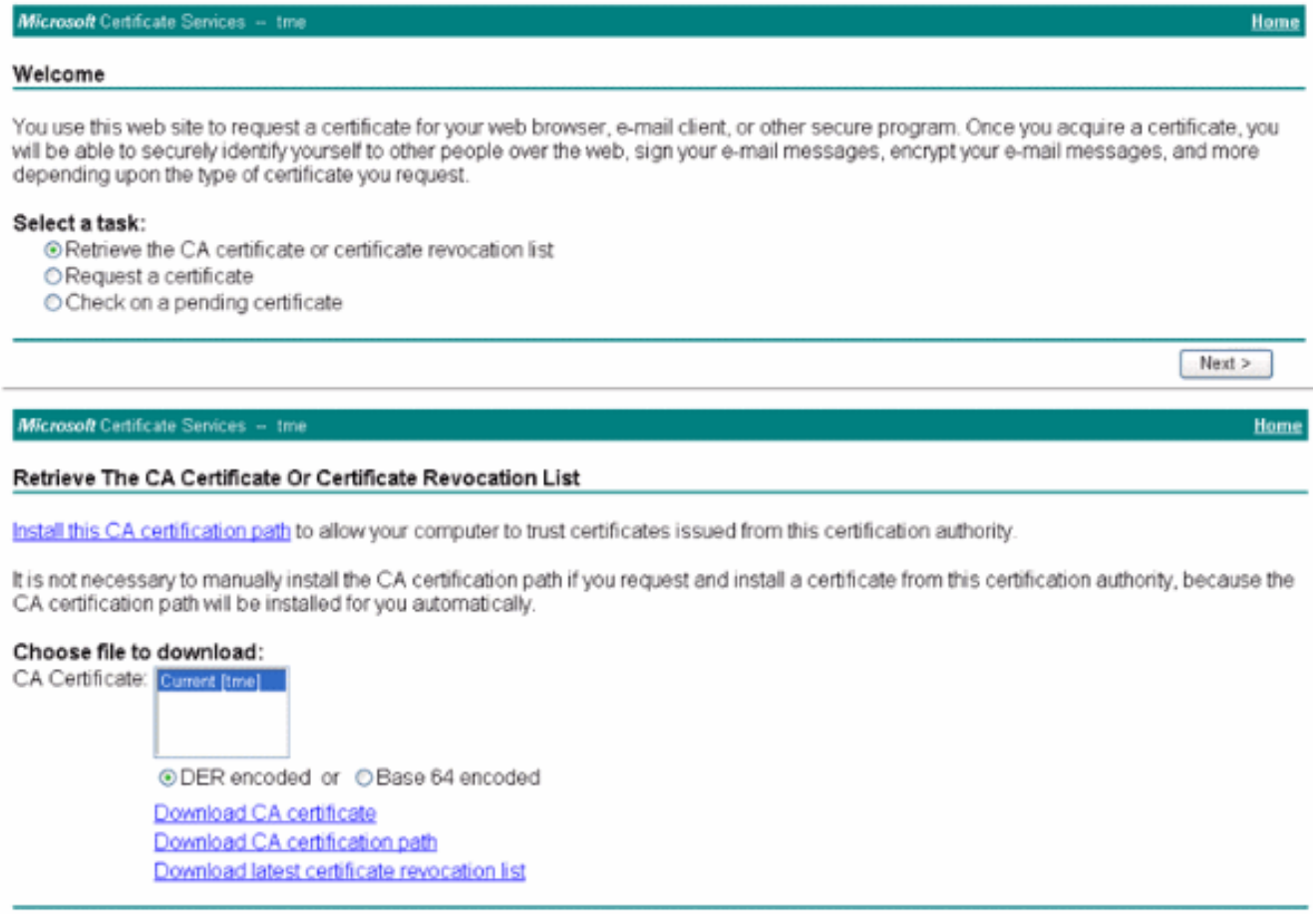
클라이언트 장치에 인증 기관 인증서 설치

클라이언트용 루트 CA 인증서 다운로드 및 설치

클라이언트는 인증 기관 서버에서 루트 CA 인증서를 가져와야 합니다.클라이언트 인증서를 가져와서 Windows XP 시스템에 설치하는 데 사용할 수 있는 몇 가지 방법이 있습니다.유효한 인증서를 얻으려면 Windows XP 사용자가 사용자 ID를 사용하여 로그인해야 하며 네트워크에 연결되어 있어야 합니다.

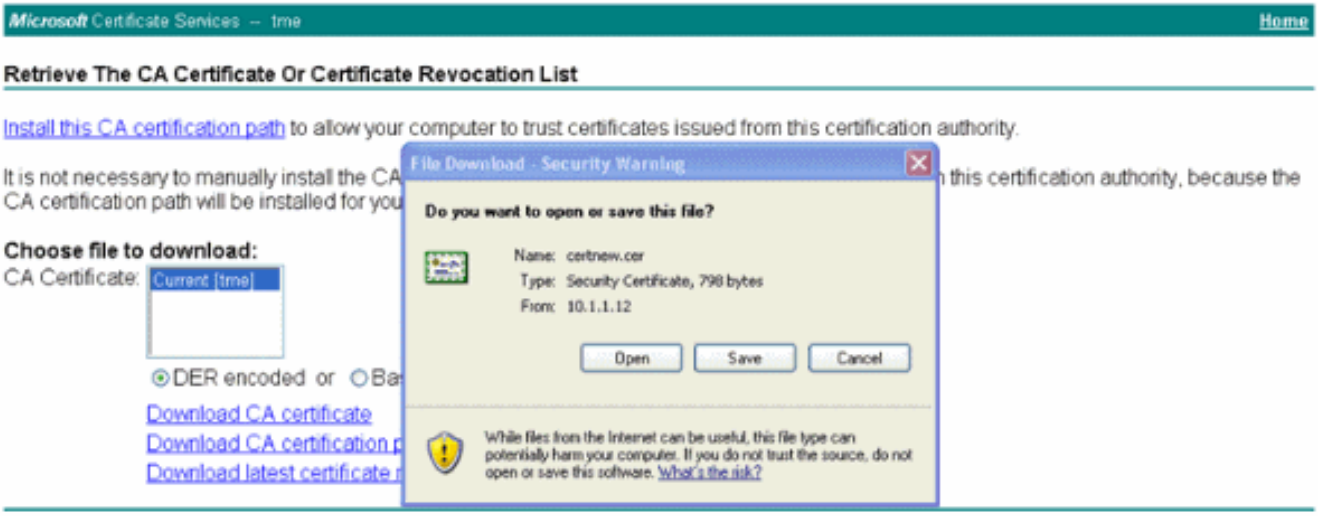
Windows XP 클라이언트의 웹 브라우저 및 네트워크에 대한 유선 연결은 개인 루트 인증 기관 서버에서 클라이언트 인증서를 가져오는 데 사용되었습니다.이 절차는 Microsoft 인증 기관 서버에서 클라이언트 인증서를 가져오는 데 사용됩니다.

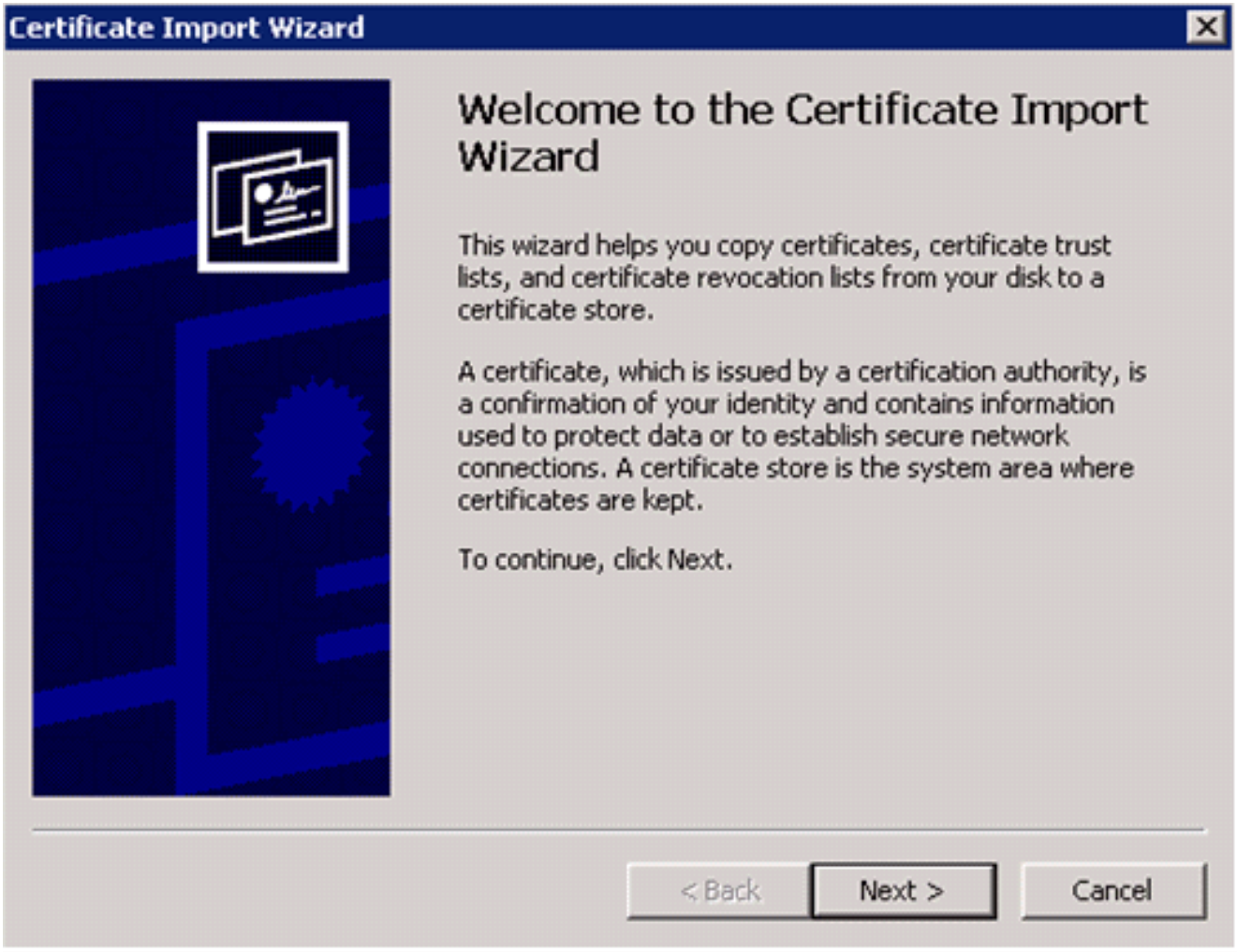
1. 클라이언트에서 웹 브라우저를 사용하고 브라우저를 인증 기관 서버로 가리킵니다.이렇게 하려면 http://IP-address-of-Root-CA/certsrv을 **입력합니다**.
2. **Domain_Name\user_name**을 사용하여 **로그인합니다**.XP 클라이언트를 사용할 개인의 사용자 이름을 사용하여 로그인해야 합니다.
3. Welcome(시작) 창에서 Retrieve a **CA certificate(CA 인증서 검색)를** 선택하고 **Next(다음)**를 클릭합니다.
4. Base**64 Encoding** and **Download CA certificate를 선택합니다**.
5. Certificate Issued(인증서 발급됨) 창에서 **Install this certificate(이 인증서 설치)**를 클릭하고 **Next(다음)**를 클릭합니다.
6. Automatically **select the certificate store(인증서 저장소 자동 선택)**를 선택하고 **Next(다음)**를 클릭하여 성공적인 가져오기 메시지를 확인합니다.
7. 인증 기관에 연결하여 인증 기관 인증서를 검색합니다
   .

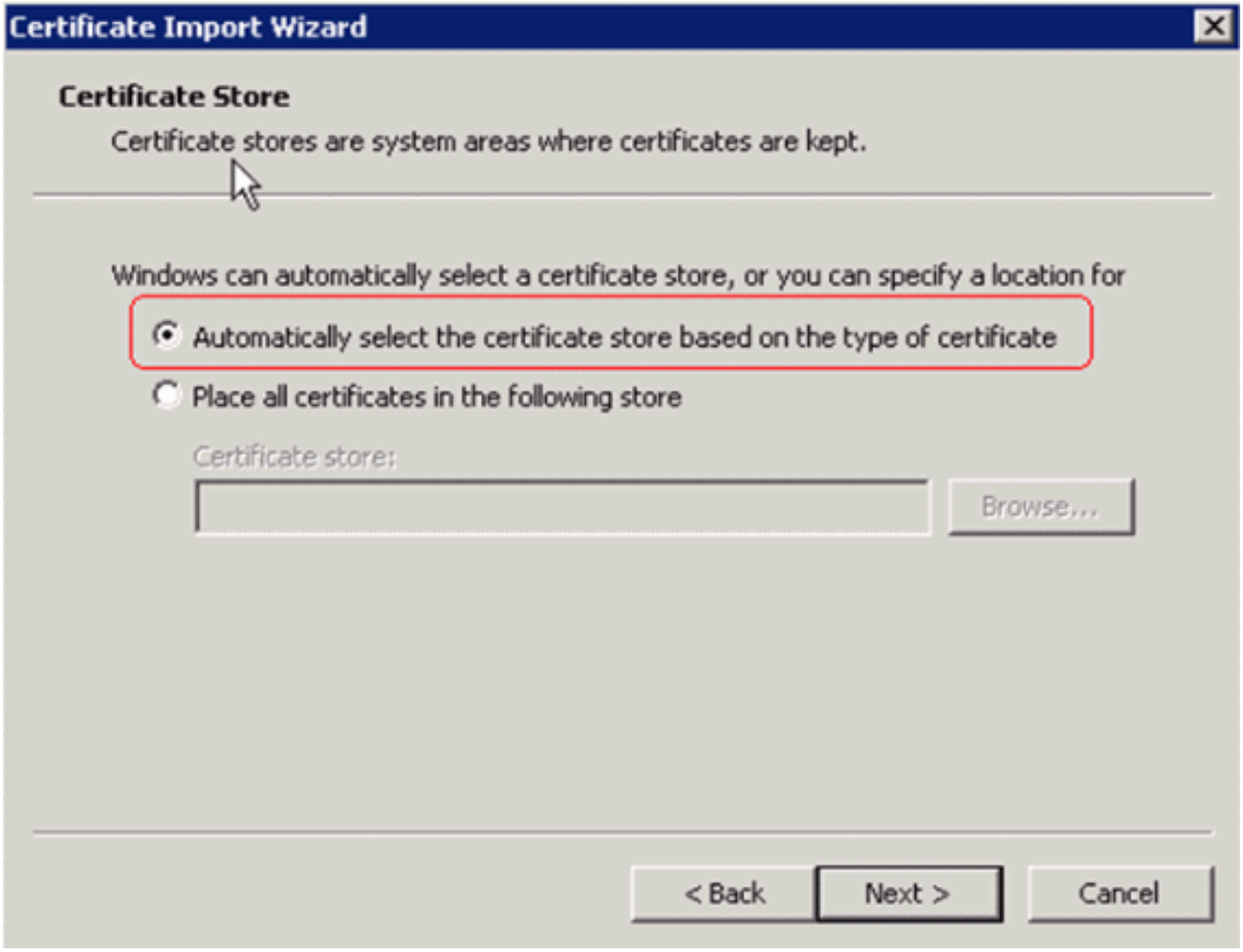


8. Download **CA certificate(CA 인증서 다운로드)를 클릭합니다**

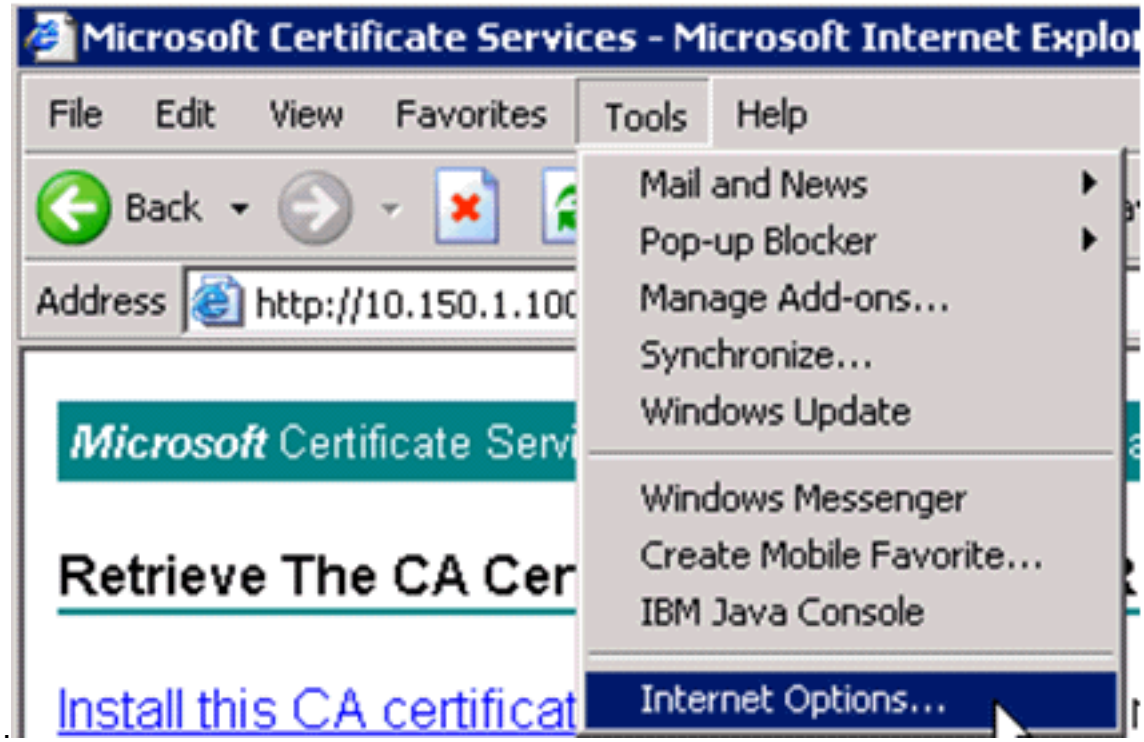
.

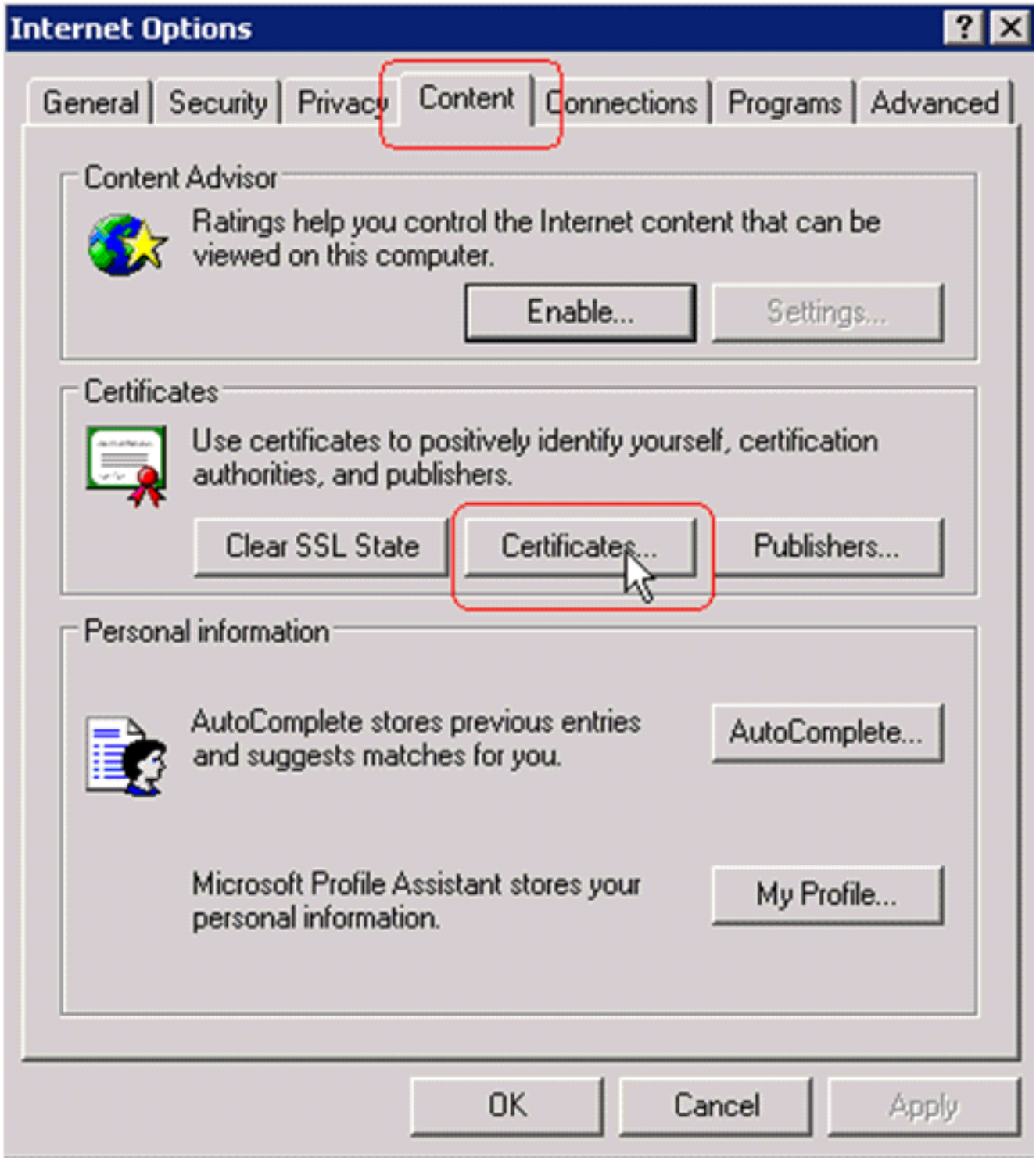



Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
To continue, click Next.
< Back
Next >
Cancel


Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Browse...
< Back
Next >
Cancel

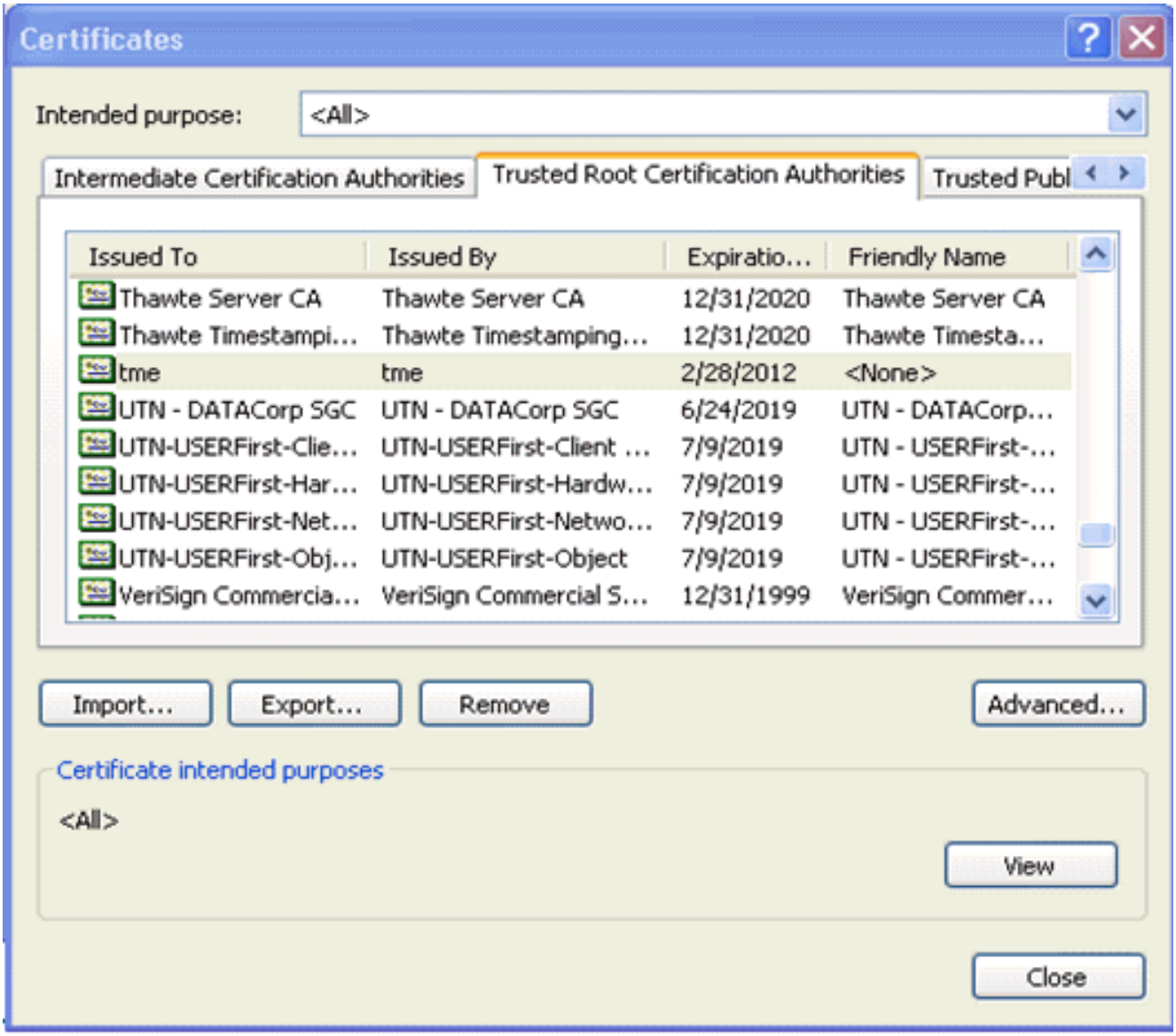
9. 인증 기관 인증서가 올바르게 설치되었는지 확인하려면 Internet Explorer를 열고 **도구 > 인터넷 옵션 > 콘텐츠 > 인증서**를 선택합니다





신뢰할 수 있는 루트 인증 기관에서 새로 설치된 인증 기관을 확인해야 합니다

.



클라이언트 장치에 대한 클라이언트 인증서 생성

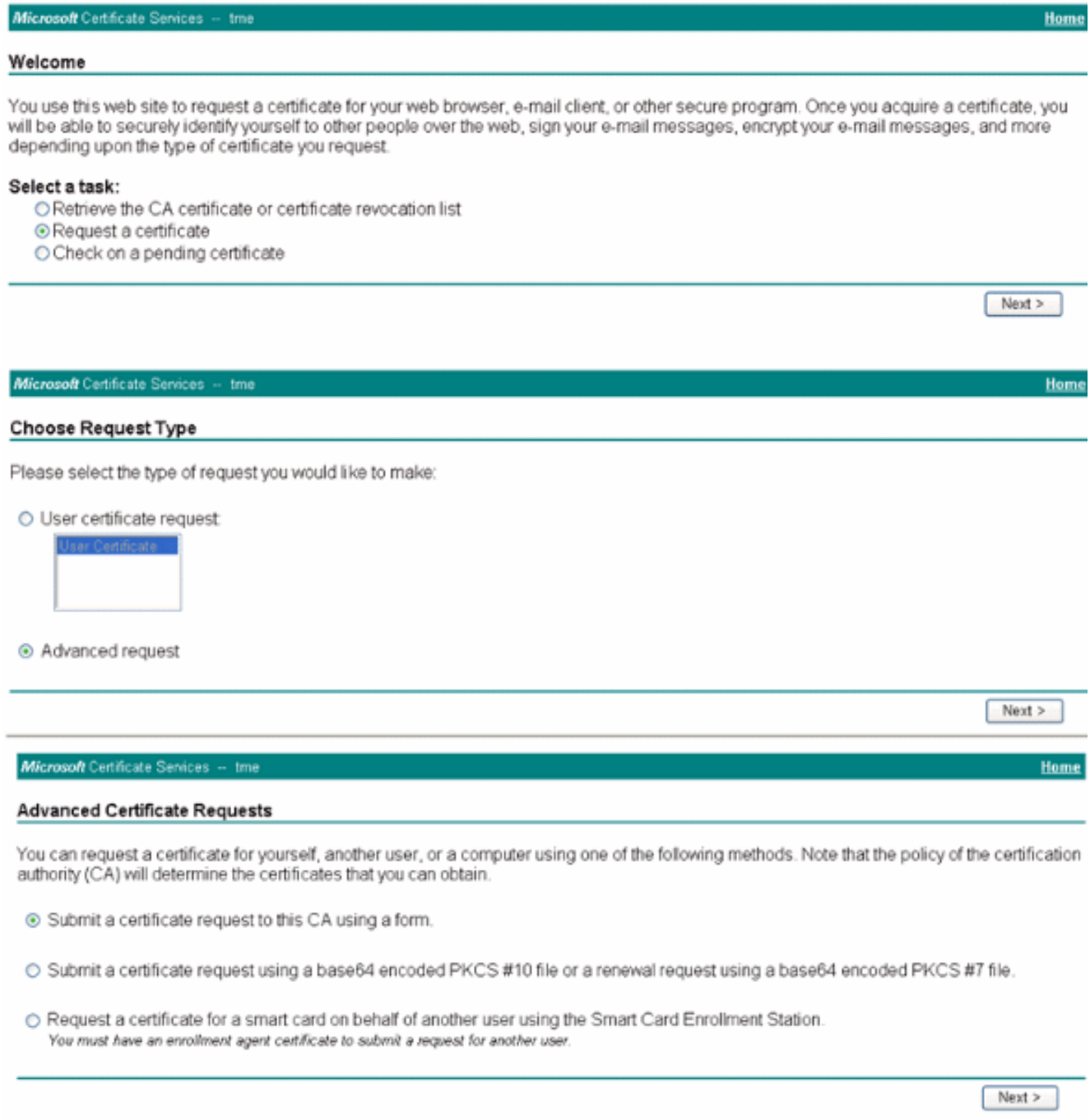
클라이언트는 WLAN EAP-TLS 클라이언트를 인증하려면 WLC에 대한 인증 기관 서버에서 인증서를 받아야 합니다.클라이언트 인증서를 가져와서 Windows XP 시스템에 설치하는 데 사용할 수 있는 몇 가지 방법이 있습니다.유효한 인증서를 취득하려면 Windows XP 사용자는 사용자 ID를 사용하여 로그인해야 하며 네트워크 연결(유선 연결 또는 802.1x 보안을 사용하는 WLAN 연결 사용 안 함)이 있어야 합니다.

Windows XP 클라이언트의 웹 브라우저 및 네트워크에 대한 유선 연결은 개인 루트 인증 기관 서버에서 클라이언트 인증서를 가져오는 데 사용됩니다.이 절차는 Microsoft 인증 기관 서버에서 클라이언트 인증서를 가져오는 데 사용됩니다.

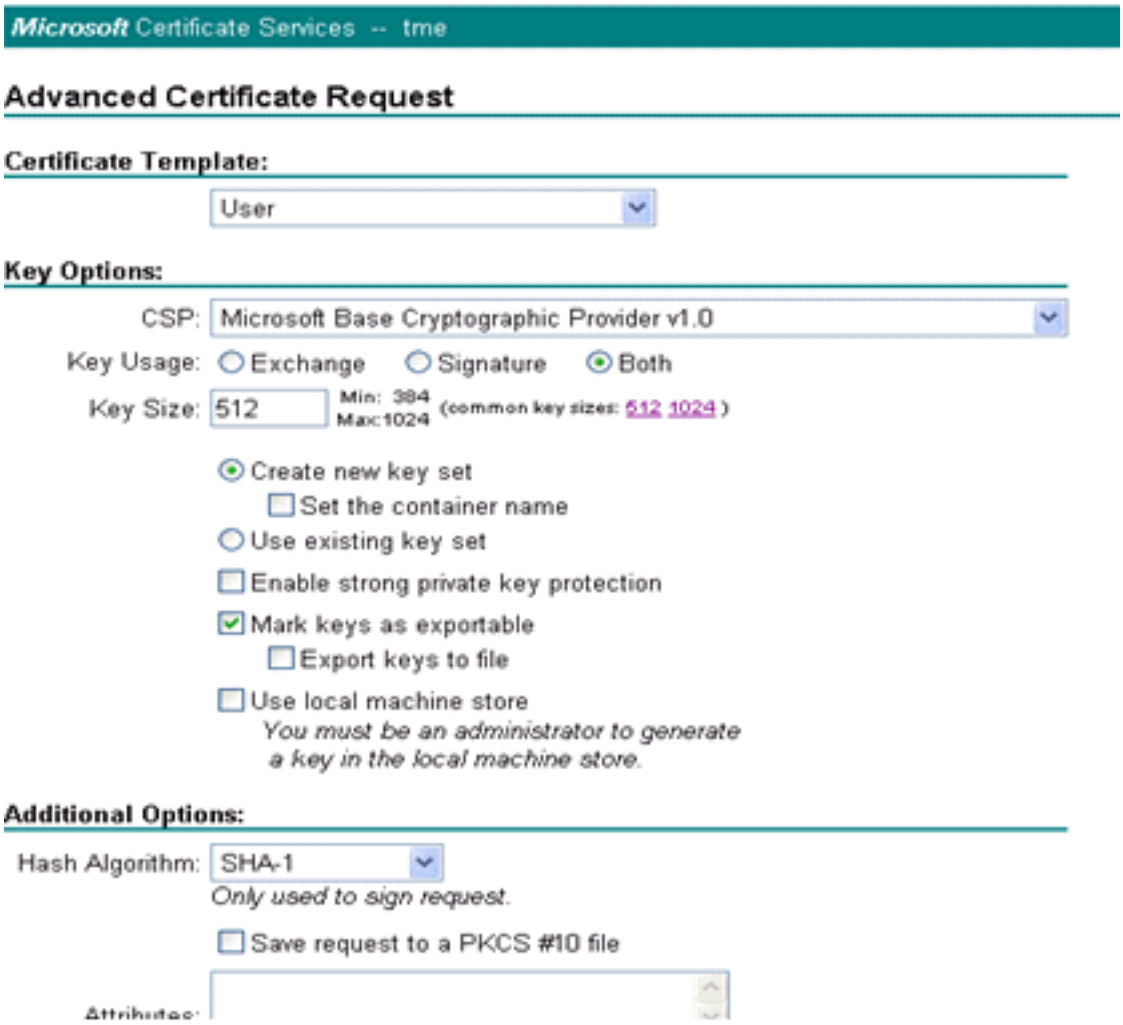
1. 클라이언트에서 웹 브라우저를 사용하고 브라우저를 인증 기관 서버로 가리킵니다.이렇게 하려면 http://IP-address-of-Root-CA/certsrv을 **입력합니다**.
2. **Domain_Name\user_name**을 사용하여 **로그인합니다**.XP 클라이언트를 사용하는 개인의 사용자 이름을 사용하여 로그인해야 합니다.(사용자 이름은 클라이언트 인증서에 포함됩니다.)
3. 시작 창에서 **인증서 요청**을 선택하고 **다음**을 클릭합니다.
4. Advanced **request(고급 요청)**를 선택하고 Next(**다음)**를 클릭합니다.
5. Submit **a certificate request to this CA using a form(양식을 사용하여 이 CA에 인증서 요청 제출)을 선택하고 Next(다음)**를 클릭합니다.

6. Advanced Certificate Request(고급 인증서 요청) 양식에서 Certificate Template as **User(사용자**로 인증서 템플릿)를 선택하고 Key Size(키 크기)를 **1024로** 지정하고 Submit(제출)을 **클릭합니다**.
7. Certificate Issued(인증서 발급) 창에서 **Install this certificate(이 인증서 설치)를** 클릭합니다.그러면 Windows XP 클라이언트에 클라이언트 인증서를 성공적으로 설치할 수 있습니다

.



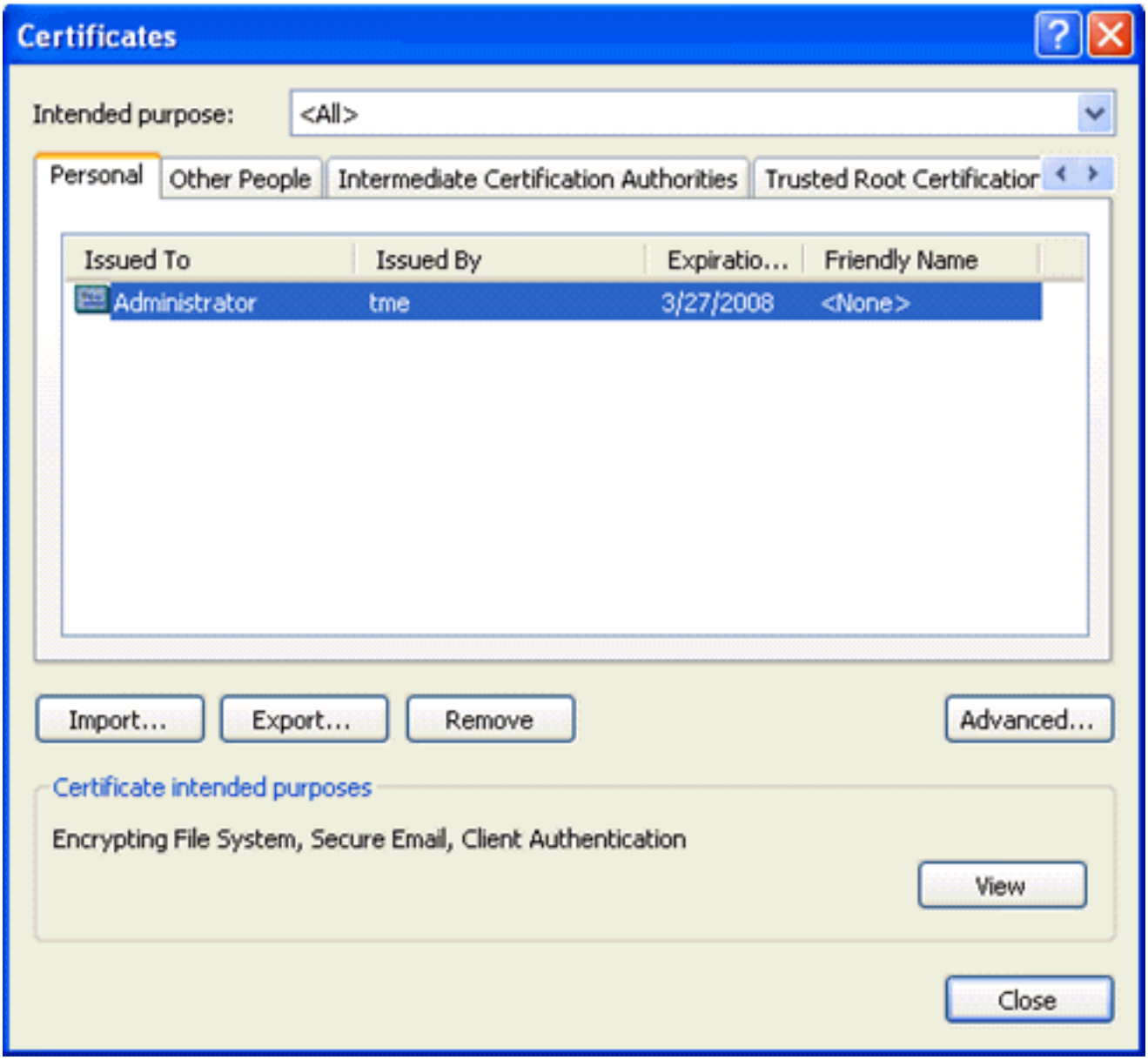
8. Client **Authentication Certificate를 선택합니다**



. 이제 클라이언트 인증서가 생성됩니다.

9. 인증서가 설치되어 있는지 확인하려면 Internet Explorer로 이동하여 **도구 > 인터넷 옵션 > 콘텐츠 > 인증서**를 선택합니다.개인 탭에서 인증서를 확인해야 합니다

.

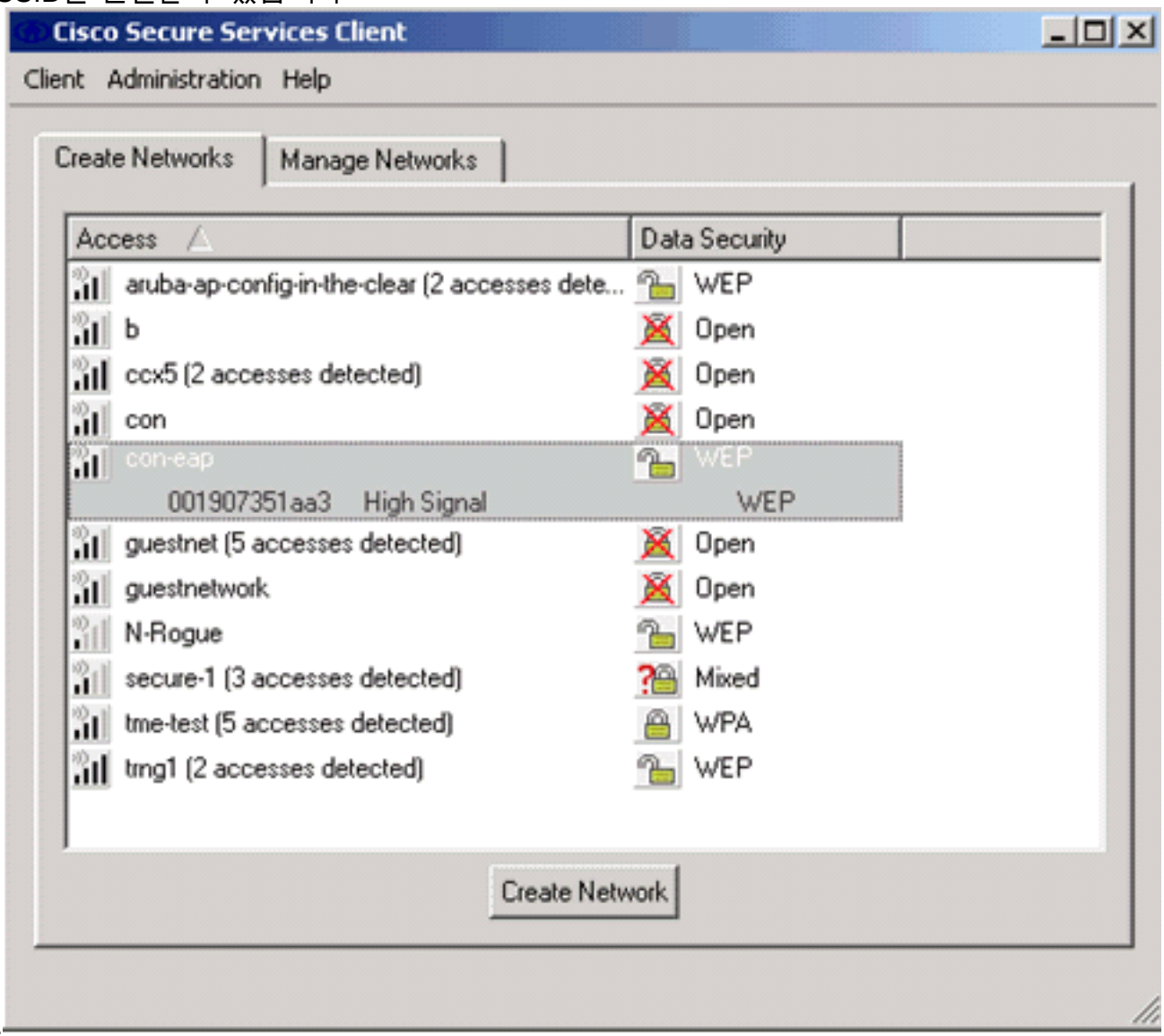


클라이언트 디바이스에서 Cisco Secure Services Client를 사용하는 EAP-TLS

다음 단계를 완료하십시오.

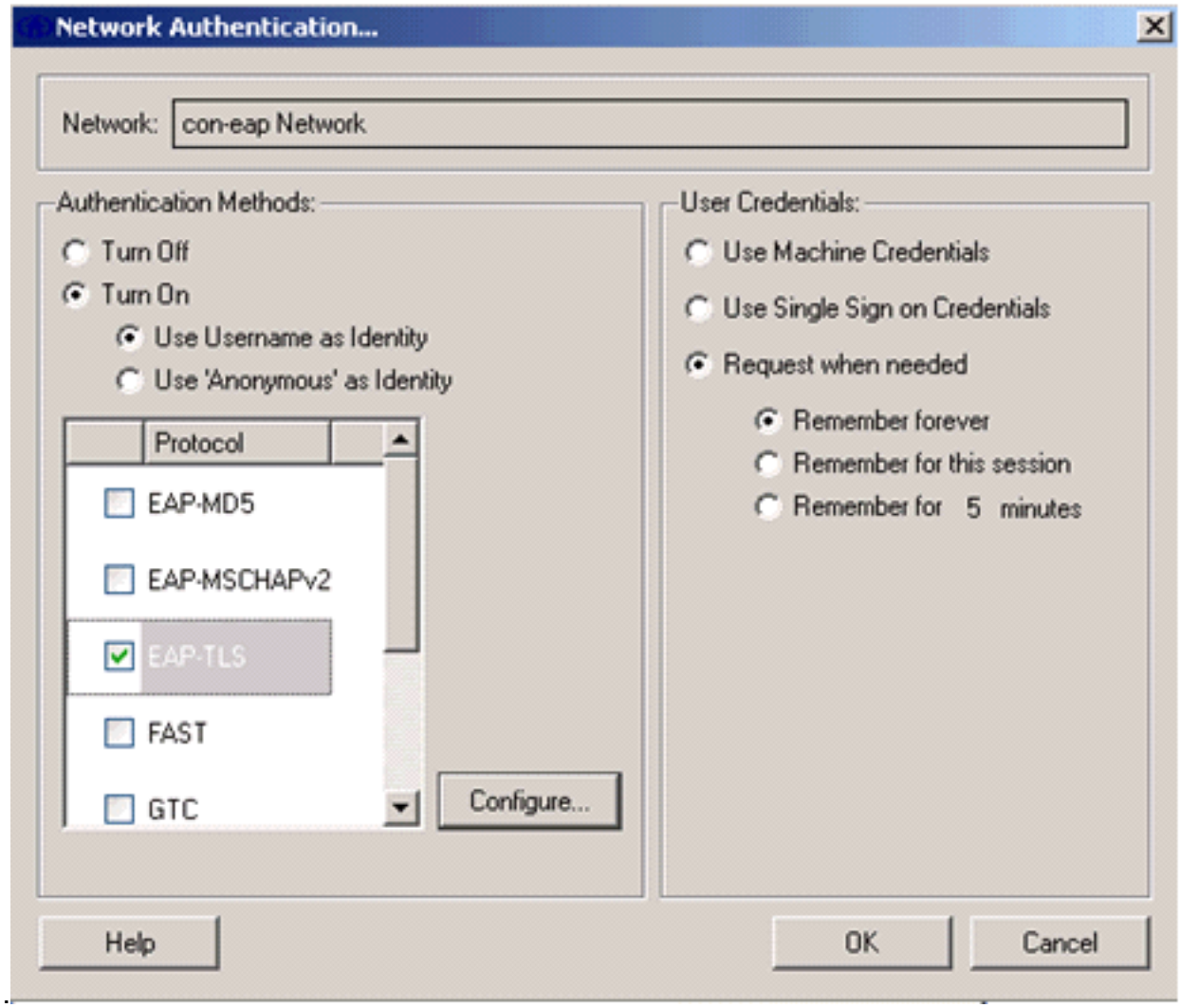
1. WLC는 기본적으로 SSID를 브로드캐스트하므로 스캔된 SSID의 Create Networks 목록에 표시됩니다.네트워크 프로파일을 생성하려면 목록(엔터프라이즈)에서 SSID를 클릭하고 Create **Network**(네트워크 생성)를 클릭할 수 있습니다.WLAN 인프라가 브로드캐스트 SSID를 비활성화하여 구성된 경우 SSID를 수동으로 추가해야 합니다.이렇게 하려면 Access Devices(액세스 디바이스) 아래에서 **Add(추가)**를 클릭하고 적절한 SSID(예: Enterprise)를 수동으로 입력합니다. 클라이언트에 대한 활성 프로브 동작을 구성합니다.즉, 클라이언트가 구성된 SSID에 대해 적극적으로 프로브합니다.Add **Access Device(액세스 디바이스 추가)** 창에서 SSID를 입력한 후 Actively search for this access device(이 액세스 디바이스**를** 적극적으로 검색)를 지정합니다.**참고:** EAP 인증 설정이 먼저 프로파일에 대해 구성되지 않은 경우 포트 설정은 엔터프라이즈 모드(802.1X)를 허용하지 않습니다.
2. Create **Network(네트워크** 생성)를 클릭하여 Network Profile(네트워크 프로파일) 창을 실행합니다. 그러면 선택한(또는 구성된) SSID를 인증 메커니즘과 연결할 수 있습니다.프로필에 대한 설명 이름을 지정합니다.**참고:** 이 인증 프로파일에서 여러 WLAN 보안 유형 및/또는

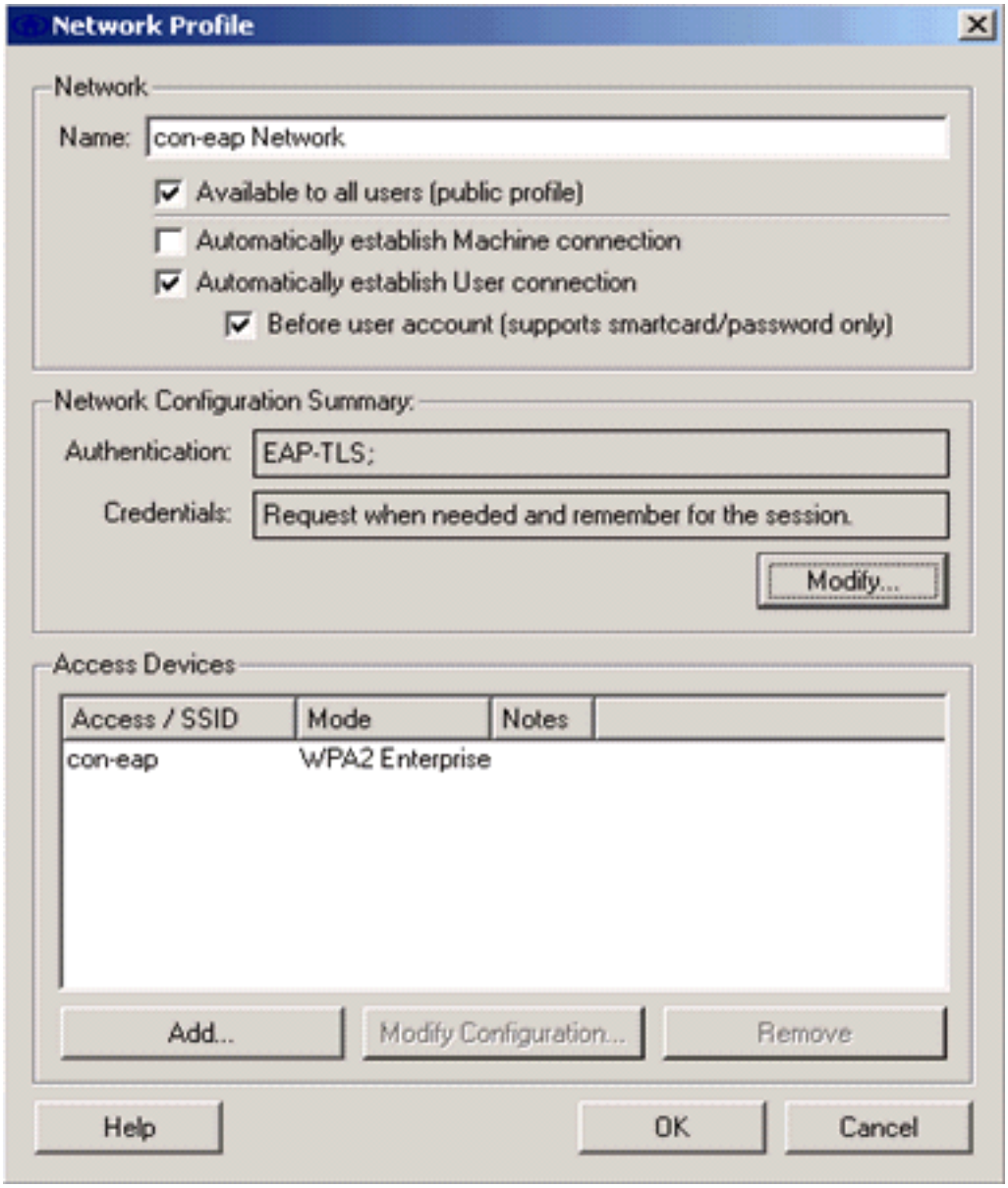
SSID를 연결할 수 있습니다



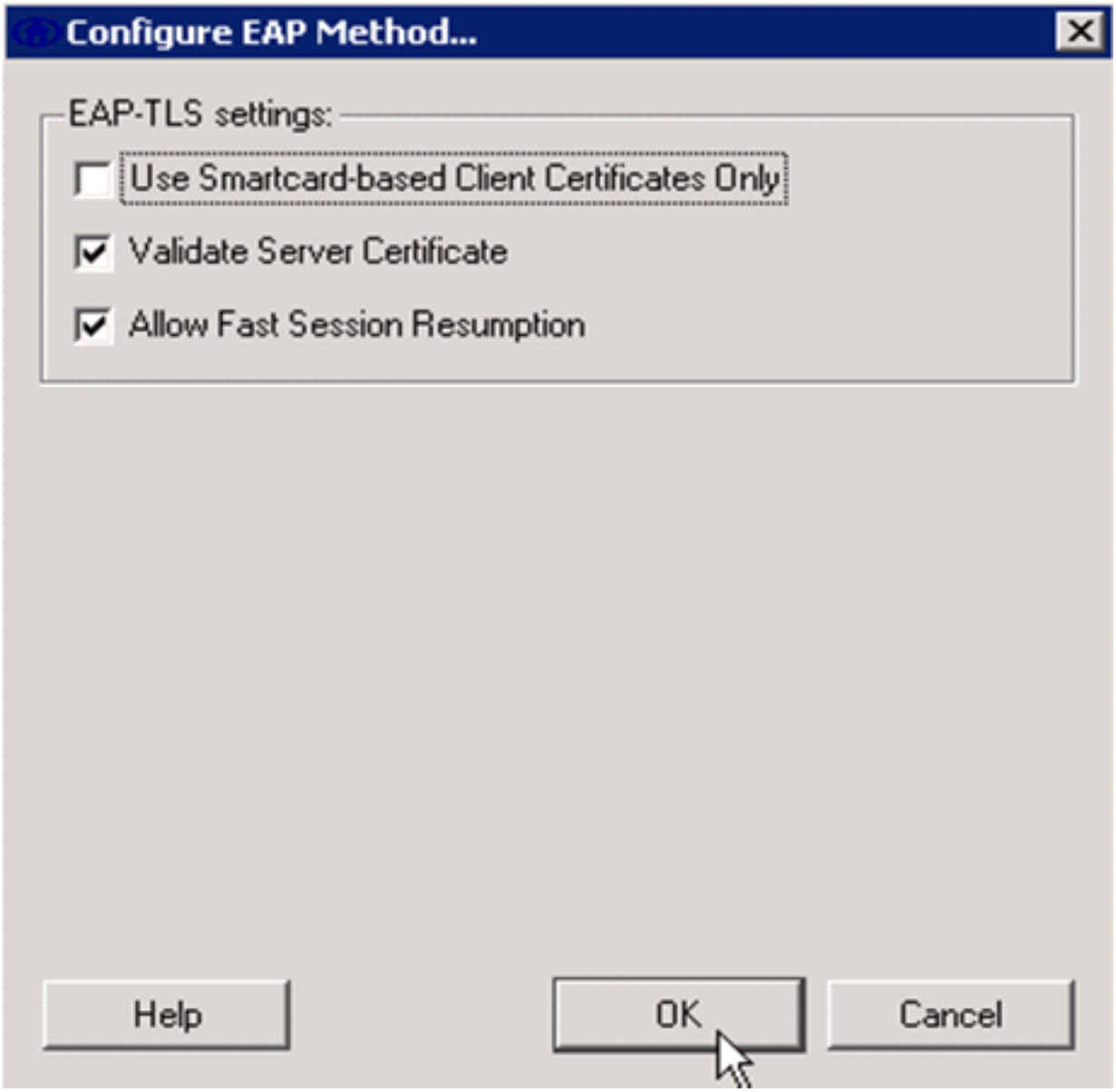
.

3. 인증을 켜고 EAP-TLS 방법을 확인합니다.그런 다음 **Configure(구성)**를 클릭하여 EAP-TLS 속성을 구성합니다.
4. Network Configuration Summary(네트워크 컨피그레이션 요약)에서 **Modify(수정)**를 클릭하여 EAP/자격 증명 설정을 구성합니다.
5. Turn **On Authentication(인증 켜기)**을 지정하고 **Protocol(프로토콜)**에서 EAP-TLS를 선택하고 **Username(사용자 이름)**을 ID로 선택합니다.
6. 네트워크 인증에 로그온 자격 증명을 사용하려면 Use Single Sign-on Credentials를 지정합니다.EAP-TLS 매개변수를 설정하려면 Configure를 클릭합니다

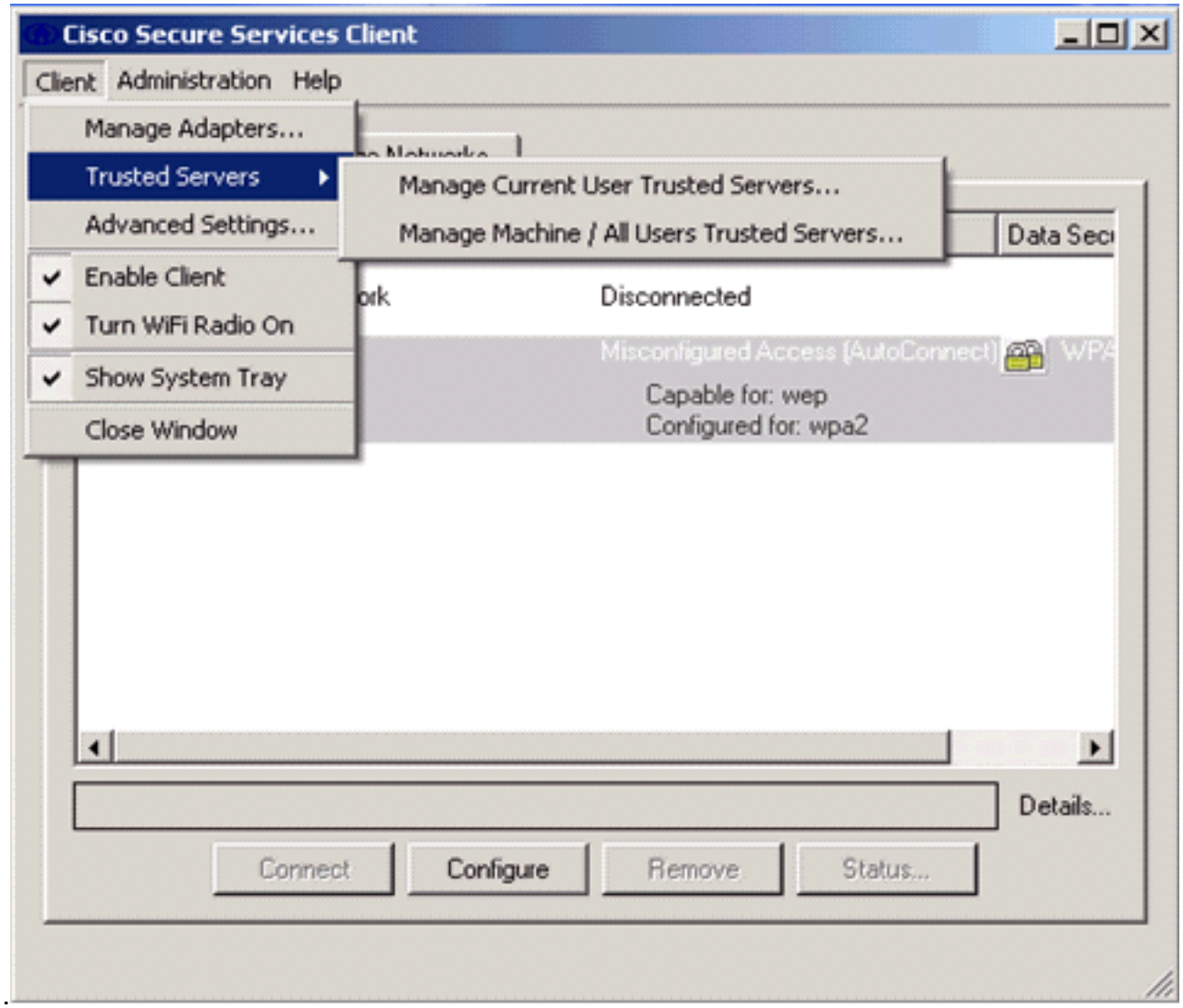

Network Authentication...
Network:
con-eap Network
Authentication Methods:
Turn Off
Turn On
Use Username as Identity
Use 'Anonymous' as Identity
Protocol
EAP-MD5
EAP-MSCHAPv2
EAP-TLS
FAST
GTC
Configure...
User Credentials:
Use Machine Credentials
Use Single Sign on Credentials
Request when needed
Remember forever
Remember for this session
Remember for 5 minutes
Help
OK
Cancel

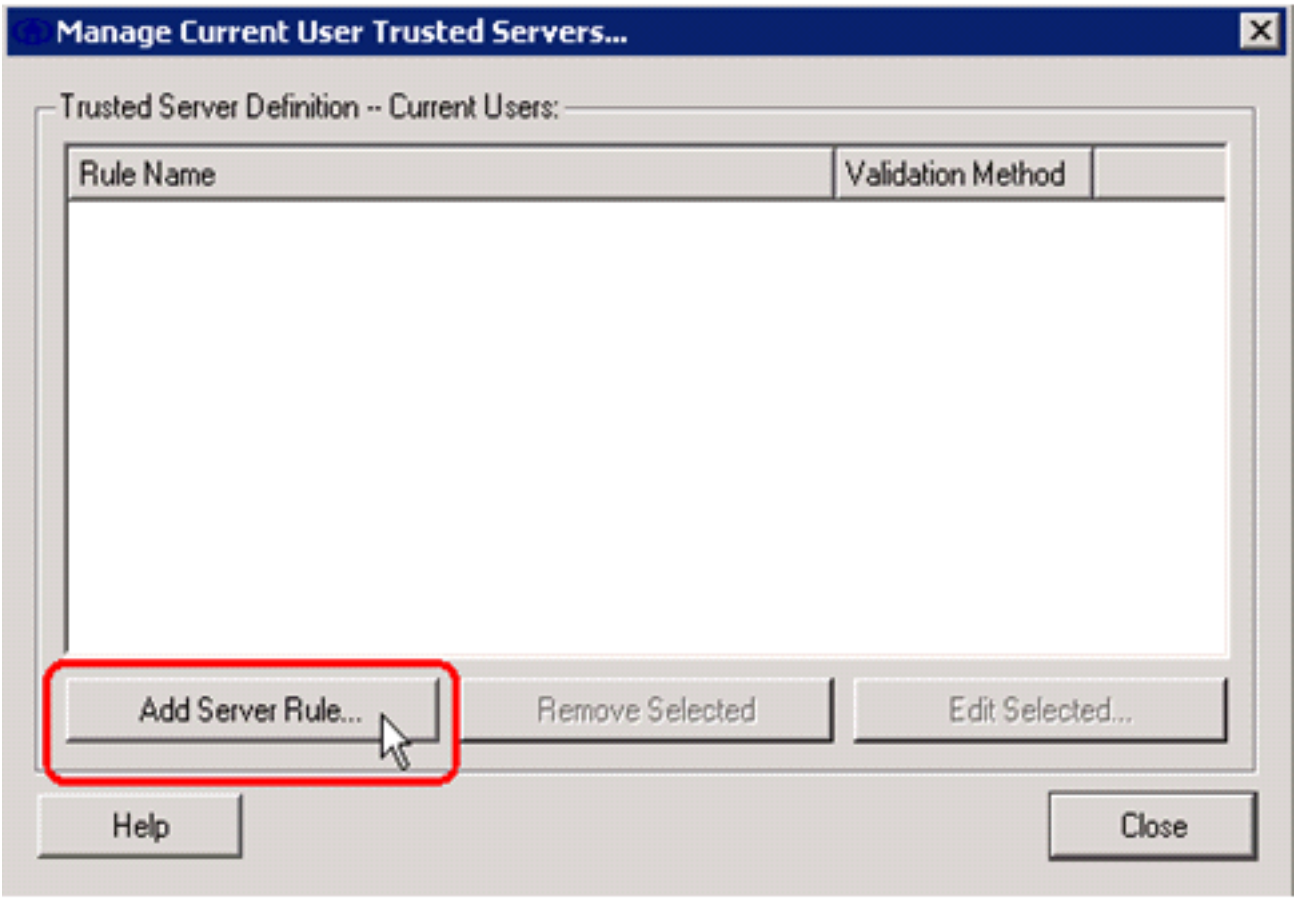


7. 보안 EAP-TLS 컨피그레이션을 사용하려면 RADIUS 서버 인증서를 확인해야 합니다.이렇게 하려면 Validate **Server Certificate**를 선택합니다



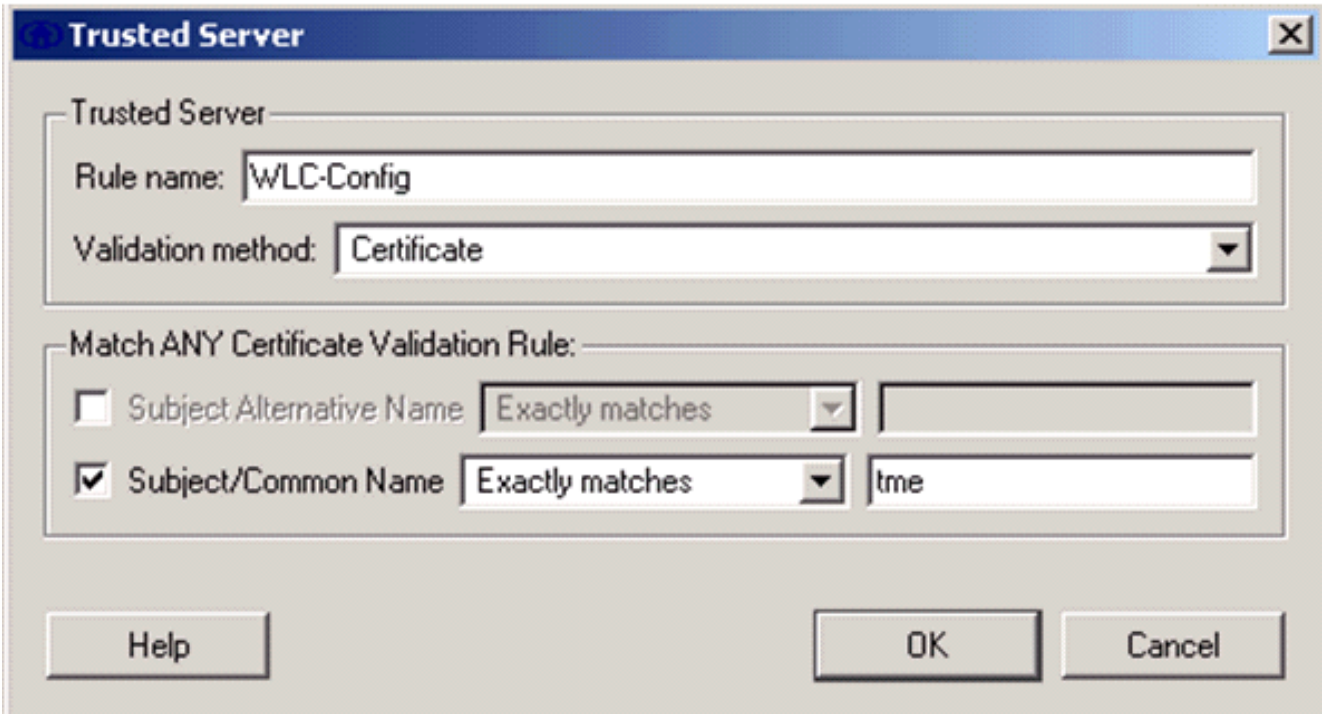
8. RADIUS 서버 인증서를 검증하려면 올바른 인증서만 수락하려면 Cisco Secure Services Client 정보를 제공해야 합니다.Client(**클라이언트) > Trusted Servers(신뢰할 수 있는 서버) > Manage Current User Trusted Servers(현재 사용자 신뢰할 수 있는 서버 관리)를 선택합니다**





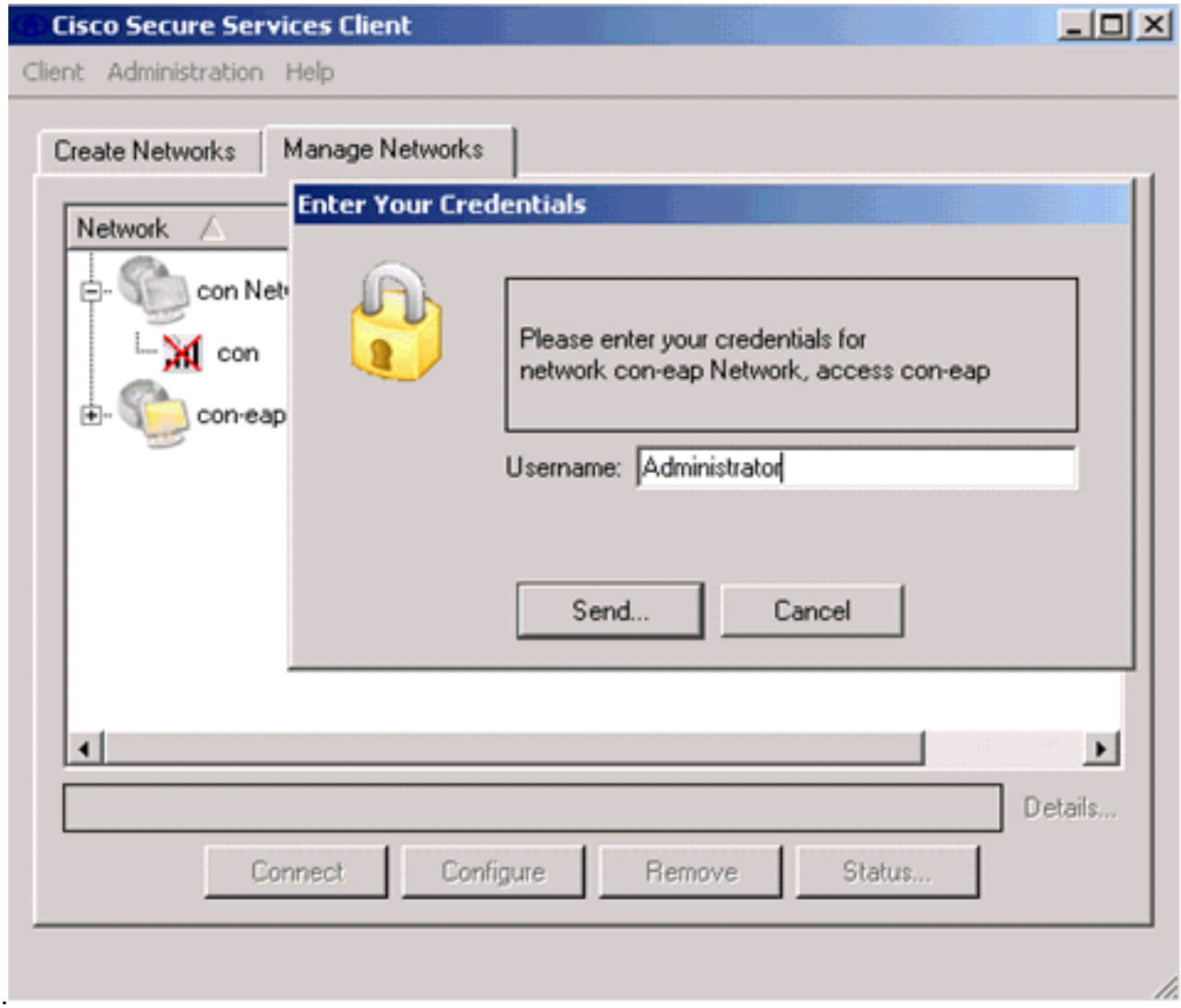
9. 규칙의 이름을 지정하고 서버 인증서의 이름을 확인합니다

.



EAP-TLS 컨피그레이션이 완료되었습니다.

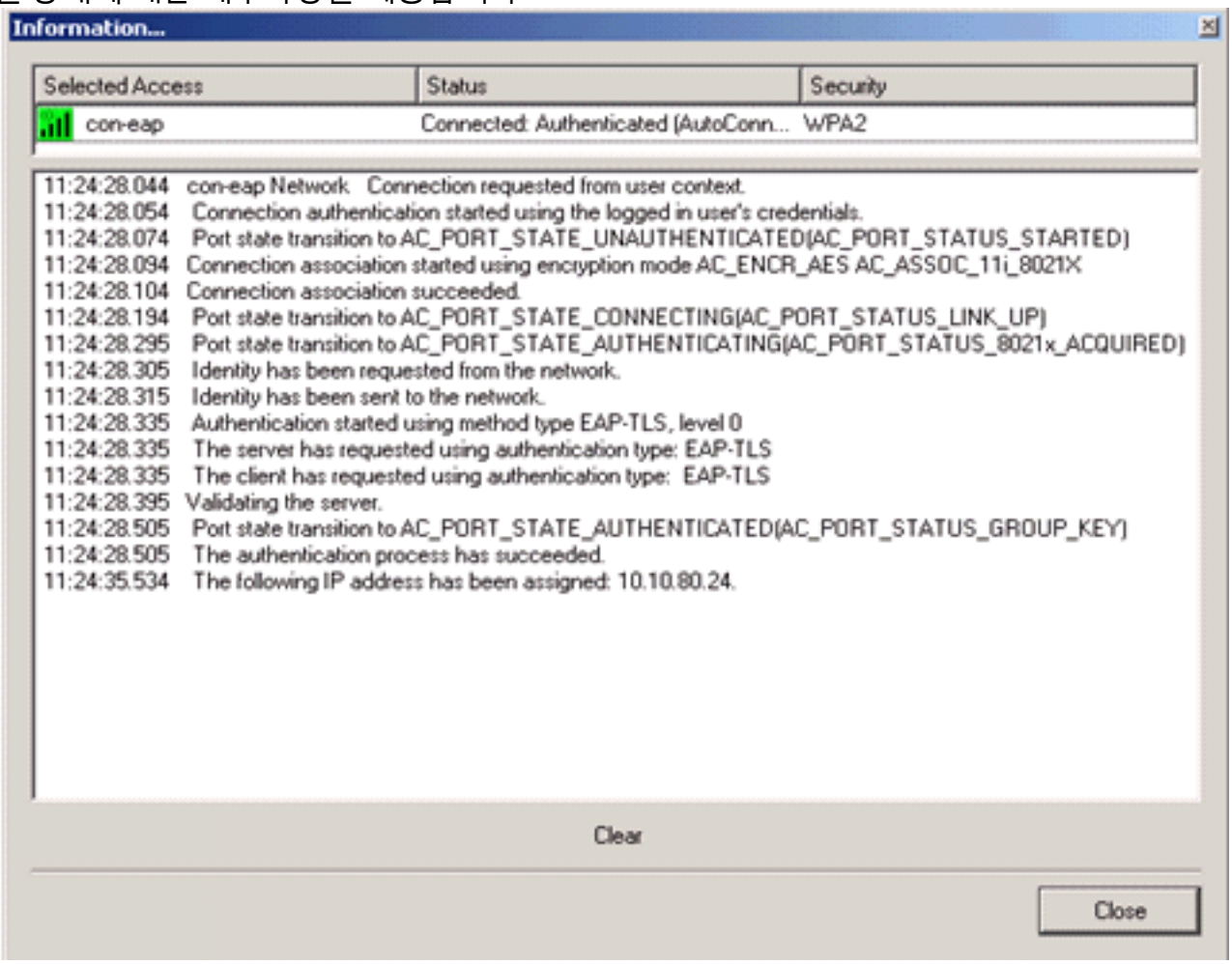
10. 무선 네트워크 프로파일에 연결합니다.Cisco Secure Services Client가 사용자 로그인을 요청합니다



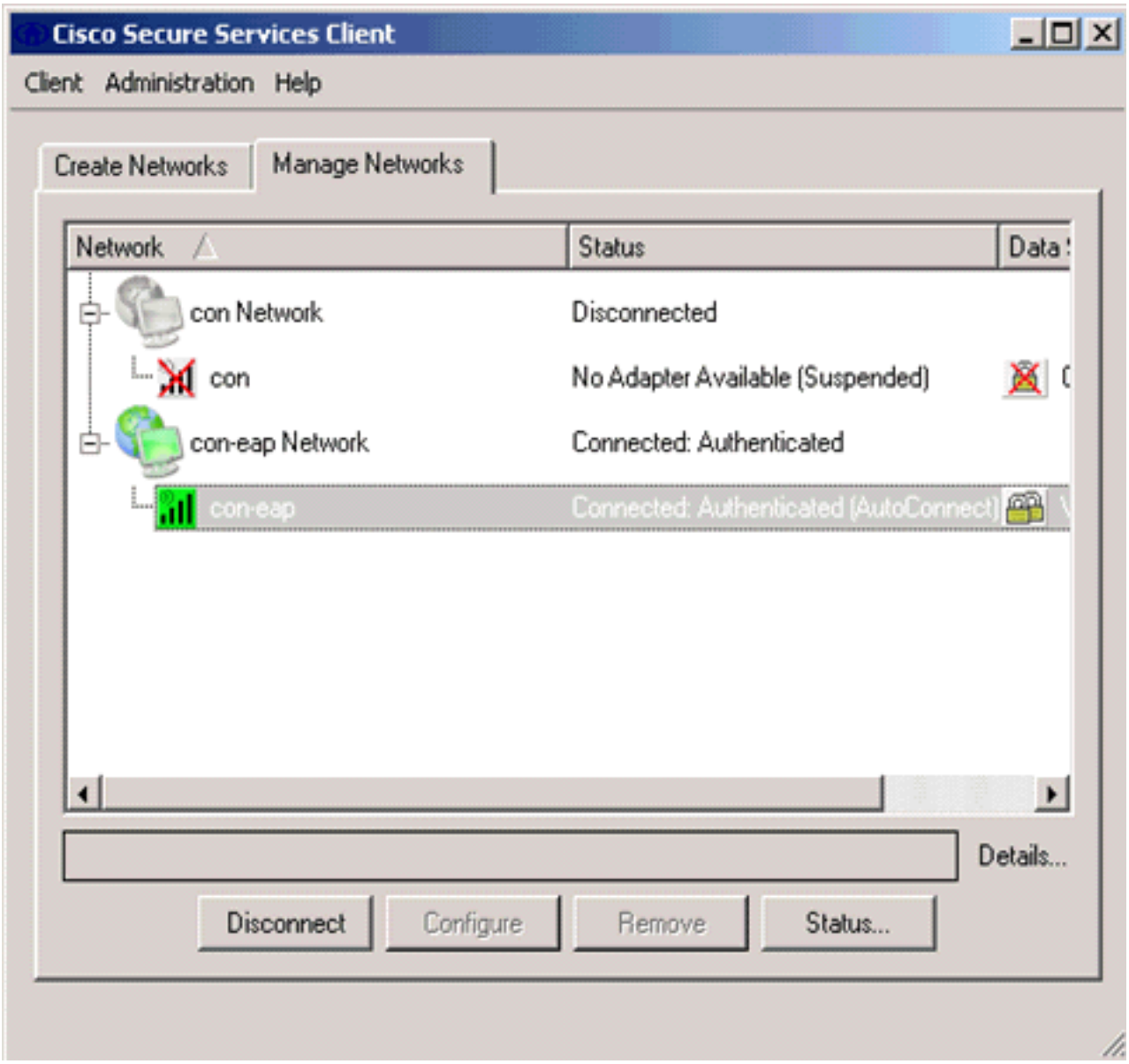
. Cisco Secure Services Client는 서버 인증서를 수신하고 이를 확인합니다(구성된 규칙과 인증

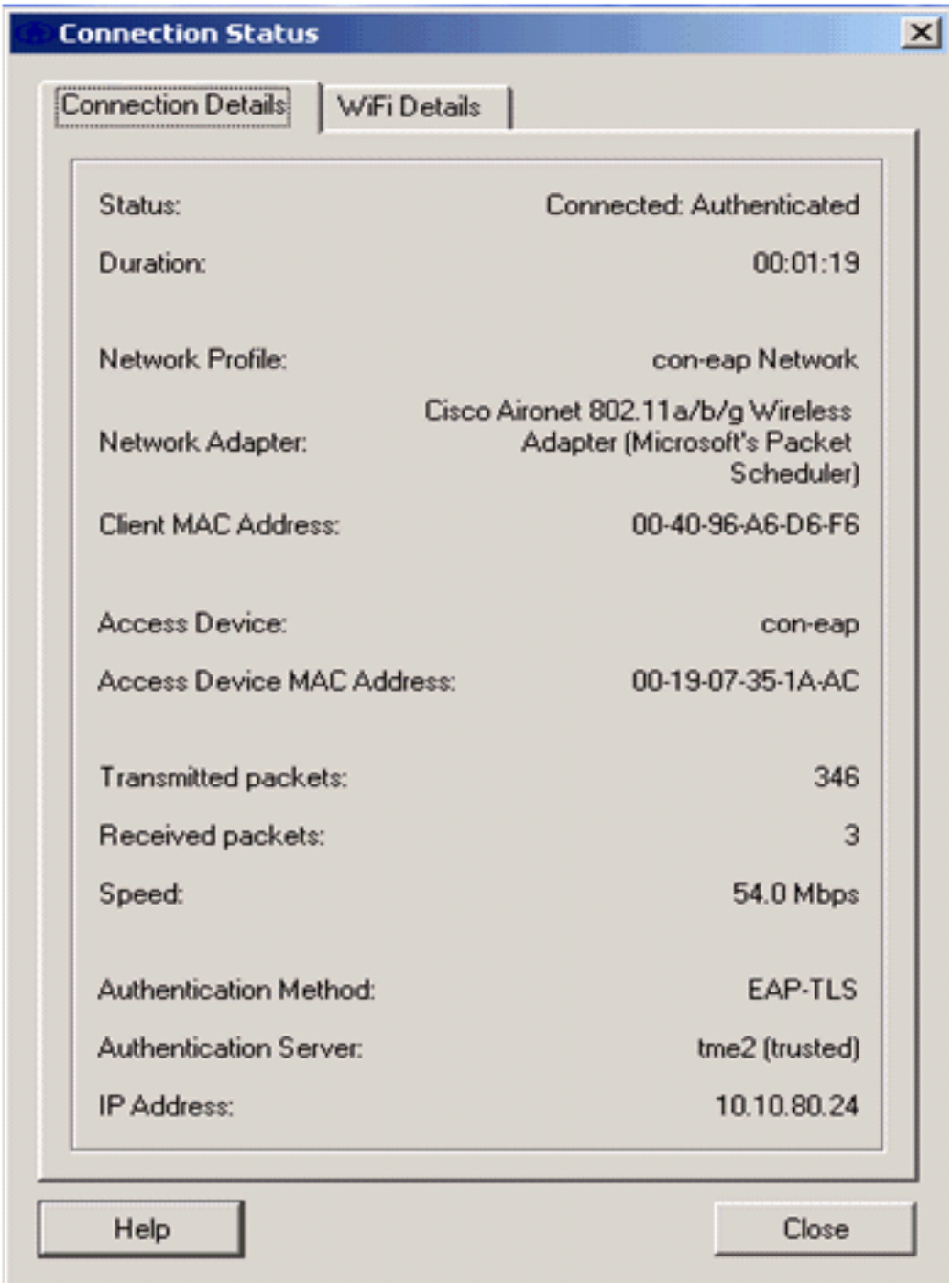
기관이 설치되어 있음). 그런 다음 사용자에게 사용할 인증서를 요청합니다.

11. 클라이언트가 인증되면 Manage Networks(네트워크 관리) 탭의 Profile(프로파일) 아래에서 **SSID**를 선택하고 **Status(상태)를** 클릭하여 연결 세부사항을 쿼리합니다.Connection Details(연결 세부사항) 창은 클라이언트 디바이스, 연결 상태 및 통계, 인증 방법에 대한 정보를 제공합니다.WiFi 세부사항 탭은 RSSI, 802.11 채널 및 인증/암호화를 포함하는 802.11 연결 상태에 대한 세부사항을 제공합니다



.


Cisco Secure Services Client
Client
Administration
Help
Create Networks
Manage Networks
Network
Status
Data
con Network
Disconnected
con
No Adapter Available (Suspended)
con-eap Network
Connected: Authenticated
con-eap
Connected: Authenticated (AutoConnect)
Details...
Disconnect
Configure
Remove
Status...



디버그 명령

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

참고: debug **명령**을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

이러한 debug 명령은 WLC에서 사용하여 인증 교환의 진행 상황을 모니터링할 수 있습니다.

- **디버그 aaa 이벤트 활성화**
- **디버그 aaa detail enable**
- **debug dot1x 이벤트 활성화**
- **디버그 dot1x 상태 활성화**
- **디버그 aaa local-auth eap 이벤트 활성화**또는

- 디버그 aaa all 활성화

관련 정보

- Cisco Wireless LAN Controller 컨피그레이션 가이드, 릴리스 4.1
- WLAN 기술 지원
- 기술 지원 및 문서 – Cisco Systems