# EAP-TLS 머신 인증을 사용하는 Windows v3.2용 보안 ACS

## 목차



## 소개

이 문서에서는 Windows 버전 3.2용 Cisco ACS(Secure Access Control System)를 사용하여 EAP-TLS(Extensible Authentication Protocol-Transport Layer Security)를 구성하는 방법에 대해 설명합니다.

**참고:** 컴퓨터 인증은 Novell CA(Certificate Authority)에서 지원되지 않습니다.ACS는 EAP-TLS를 사용하여 Microsoft Windows Active Directory에 대한 머신 인증을 지원할 수 있습니다.최종 사용자 클라이언트는 사용자 인증을 위한 프로토콜을 머신 인증에 사용되는 동일한 프로토콜로 제한할 수 있습니다.즉, 머신 인증에 EAP-TLS를 사용하려면 사용자 인증에 EAP-TLS를 사용해야 할 수 있습니다.시스템 인증에 대한 자세한 내용은 *Cisco Secure Access Control Server 4.1용 사용 설명서*의 [시스템 인증](#) *섹션을* 참조하십시오.

**참고:** EAP-TLS를 통해 시스템을 인증하도록 ACS를 설정하고 ACS가 시스템 인증을 위해 설정된 경우, 클라이언트는 머신 인증만 하도록 구성해야 합니다.자세한 내용은 Windows Vista, Windows Server 2008 및 Windows XP 서비스 팩 3에서 802.1X 기반 네트워크에 대한 컴퓨터 전용 인증을 활성화하는 방법을 참조하십시오.

# 사전 요구 사항

## 요구 사항

이 문서에 대한 특정 요건이 없습니다.

## 사용되는 구성 요소

이 문서의 정보는 아래 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Secure ACS for Windows 버전 3.2
- Microsoft 인증서 서비스(엔터프라이즈 루트 CA(Certificate Authority)로 설치됨)**참고:** 자세한 내용은 인증 기관 설정 단계별 가이드를 참조하십시오.
- Windows 2000 Server 서비스 팩 3 및 핫픽스 323172를 사용하는 DNS 서비스**참고:** CA 서버 문제가 발생하면 핫픽스 323172를 설치합니다.Windows 2000 SP3 클라이언트에는 IEEE 802.1x 인증을 활성화하려면 핫픽스 313664 가 필요합니다.
- Cisco Aironet 1200 Series Wireless Access Point 12.01T
- Windows XP Professional 서비스 팩 1을 실행하는 IBM ThinkPad T30

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.라이브 네트워크에서 작업하는 경우, 사용하기 전에 모든 명령의 잠재적인 영향을 이해해야 합니다.

## 배경 이론

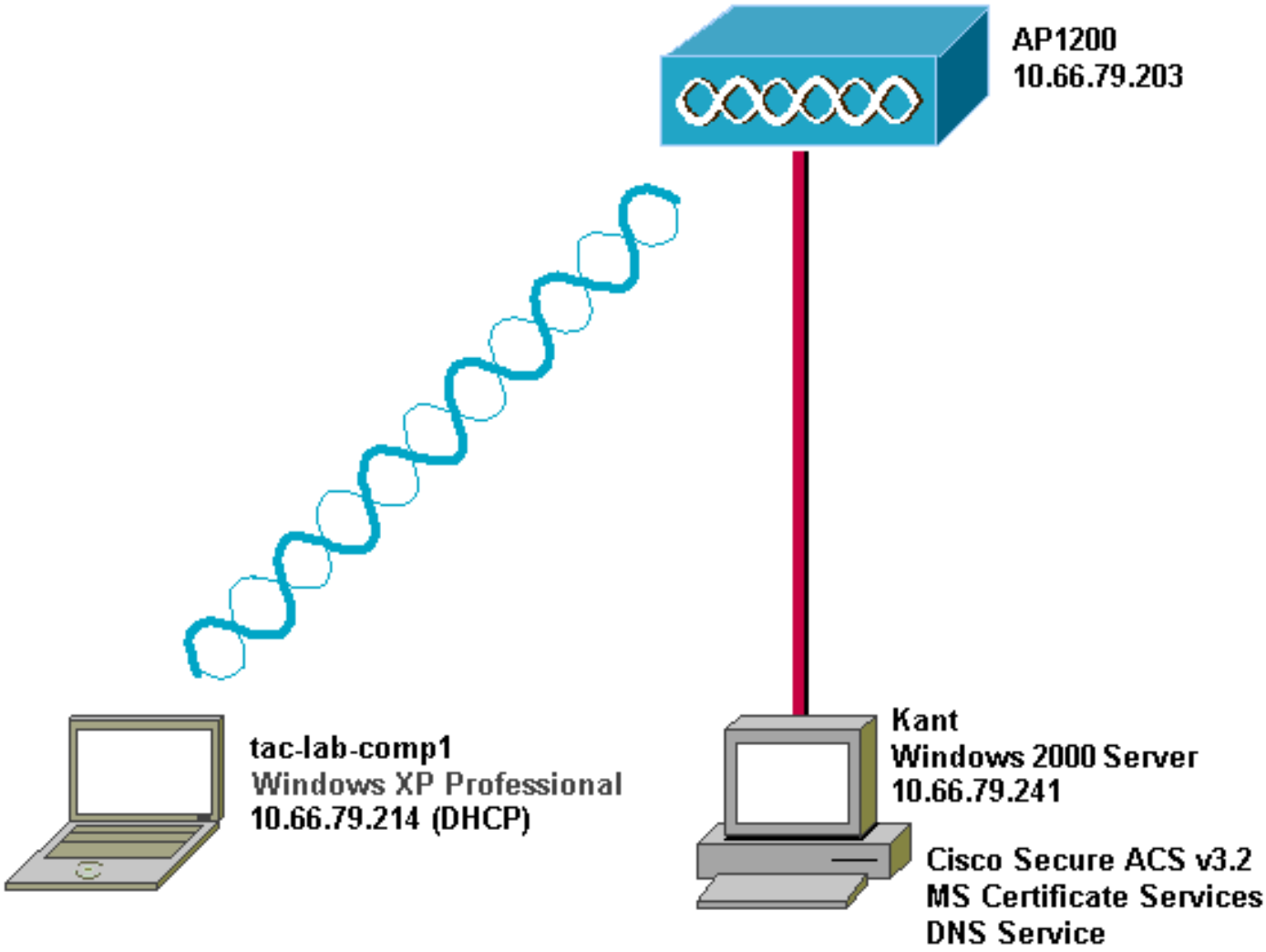
EAP-TLS 및 PEAP(Protected Extensible Authentication Protocol) 모두 TLS/SSL(Secure Socket Layer) 터널을 구축하고 사용합니다.EAP-TLS는 ACS(인증, 권한 부여 및 계정 관리[AAA]) 서버 및 클라이언트가 인증서를 가지고 있고 서로 ID를 증명하는 상호 인증을 사용합니다.그러나 PEAP는 서버측 인증만 사용합니다.서버만 인증서를 가지고 있으며 클라이언트의 ID를 확인합니다.

## 표기 규칙

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

## 네트워크 다이어그램

이 문서에서는 아래 다이어그램에 표시된 네트워크 설정을 사용합니다.




# Windows v3.2용 Cisco Secure ACS 구성

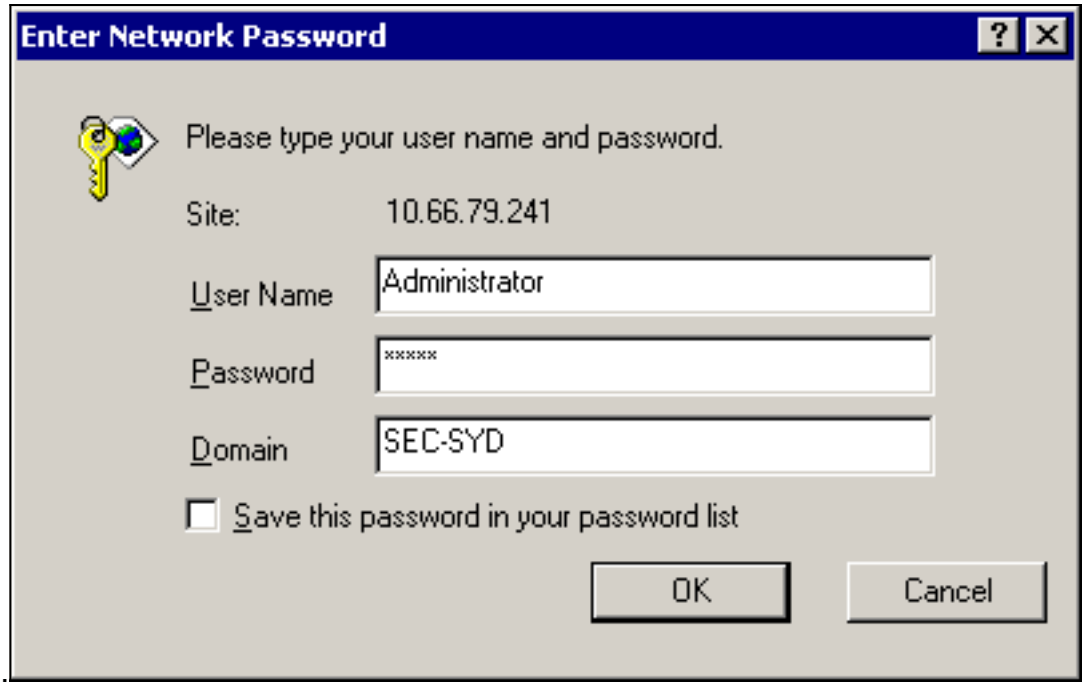
ACS 3.2를 구성하려면 다음 단계를 수행합니다.

1. ACS 서버의 인증서를 가져옵니다.
2. 저장소에서 인증서를 사용하도록 ACS를 구성합니다.
3. ACS에서 신뢰해야 하는 추가 인증 기관을 지정합니다.
4. 서비스를 다시 시작하고 ACS에서 PEAP 설정을 구성합니다.
5. 액세스 포인트를 AAA 클라이언트로 지정하고 구성합니다.
6. 외부 사용자 데이터베이스를 구성합니다.
7. 서비스를 다시 시작합니다.

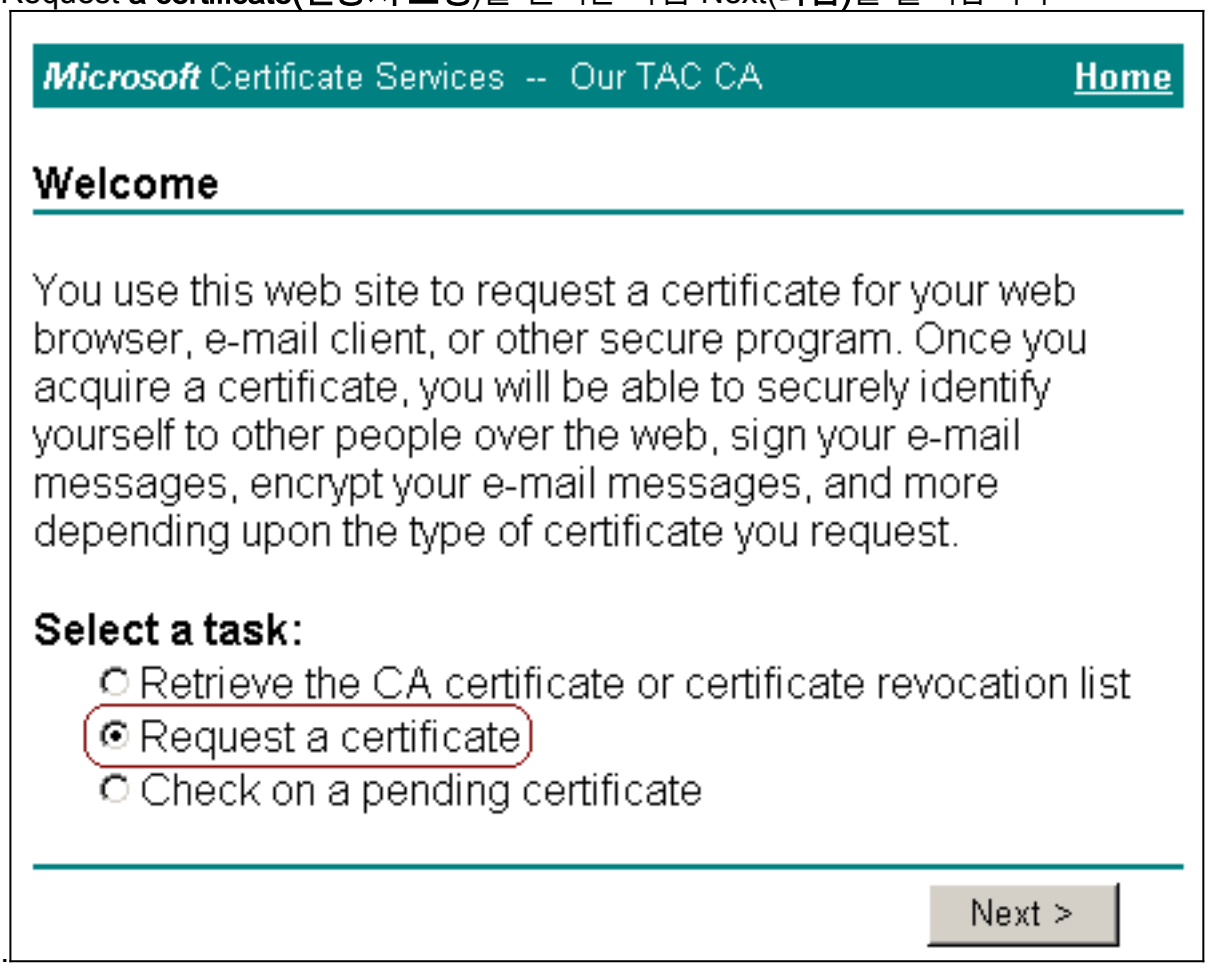
## ACS 서버의 인증서 가져오기

인증서를 얻으려면 다음 단계를 수행합니다.

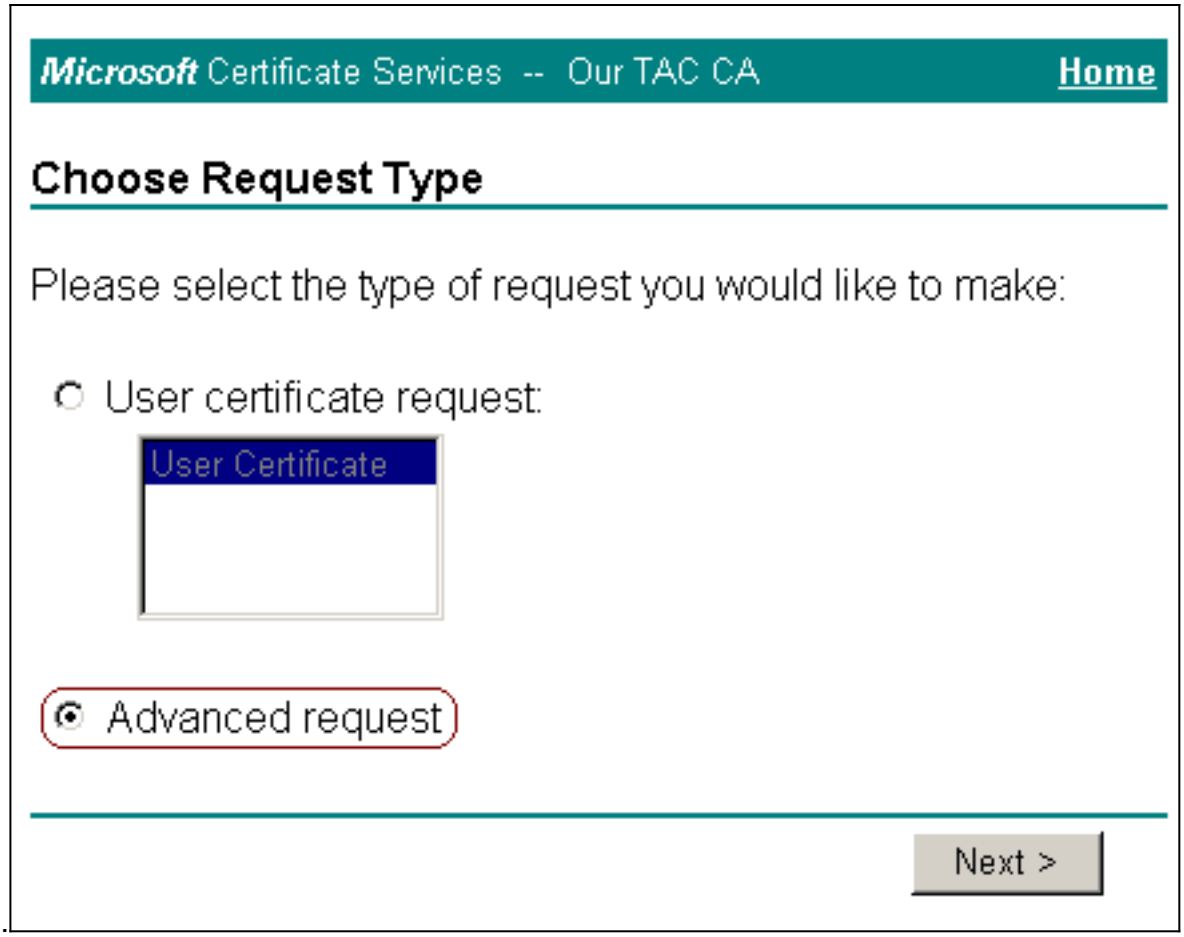
1. ACS 서버에서 웹 브라우저를 열고 **http://*CA-ip-address*/certsrv**를 입력하여 CA 서버에 액세스합니다.
2. 도메인에 관리자로 로그인합니다



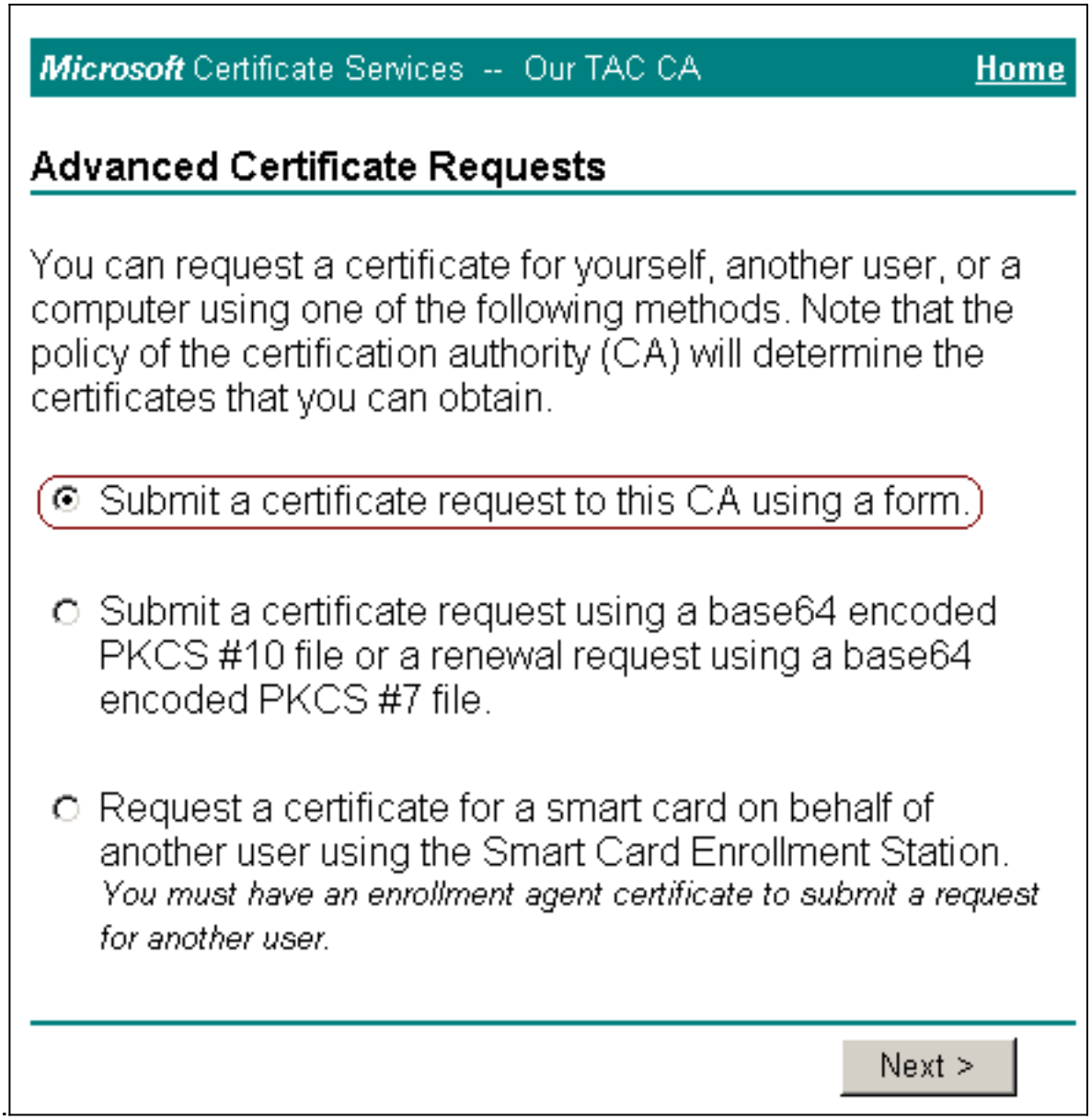

3. Request **a certificate(인증서 요청)**를 선택한 다음 Next(**다음)**를 클릭합니다



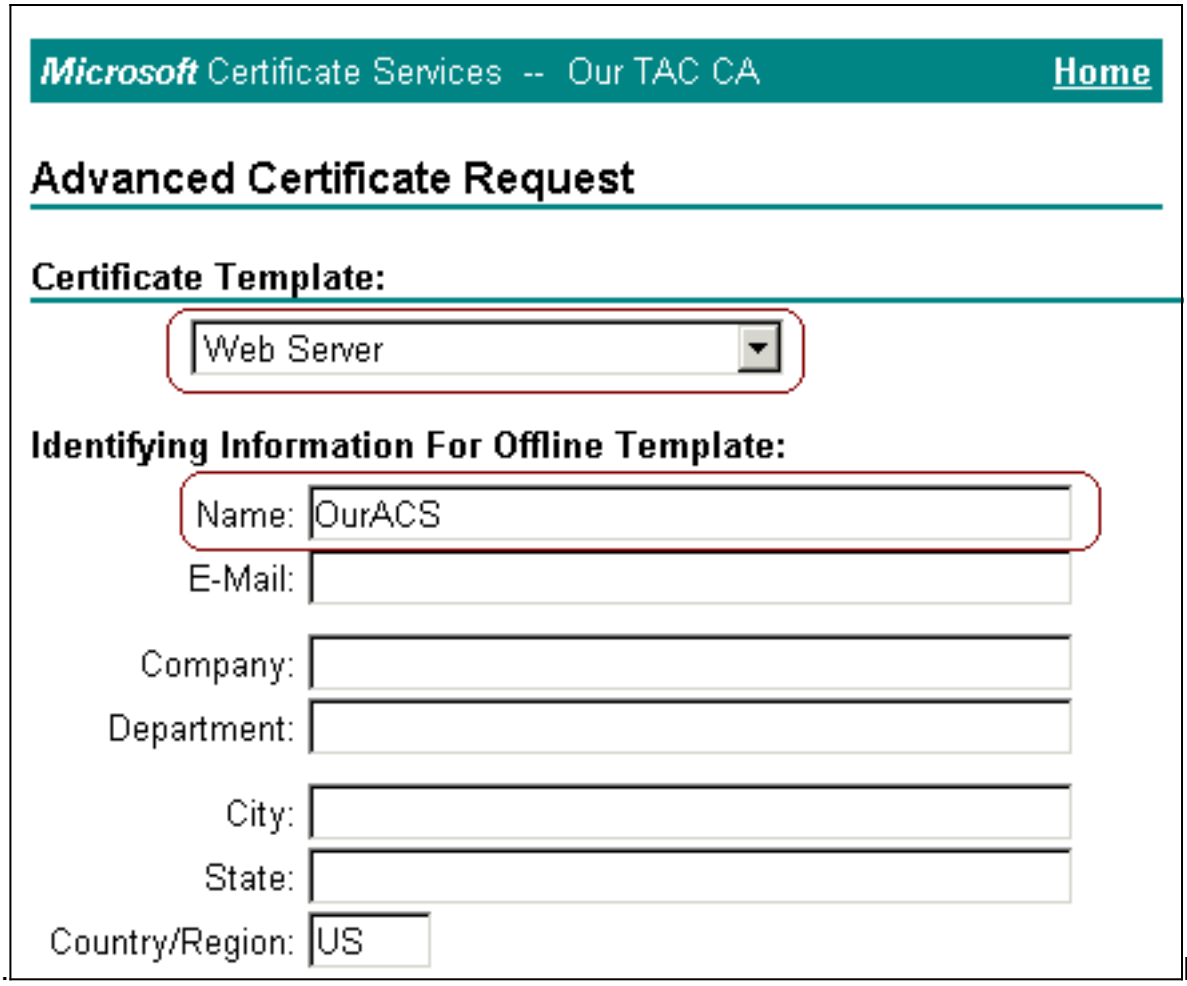

4. 고급 **요청**을 선택한 다음 **다음**을 클릭합니다



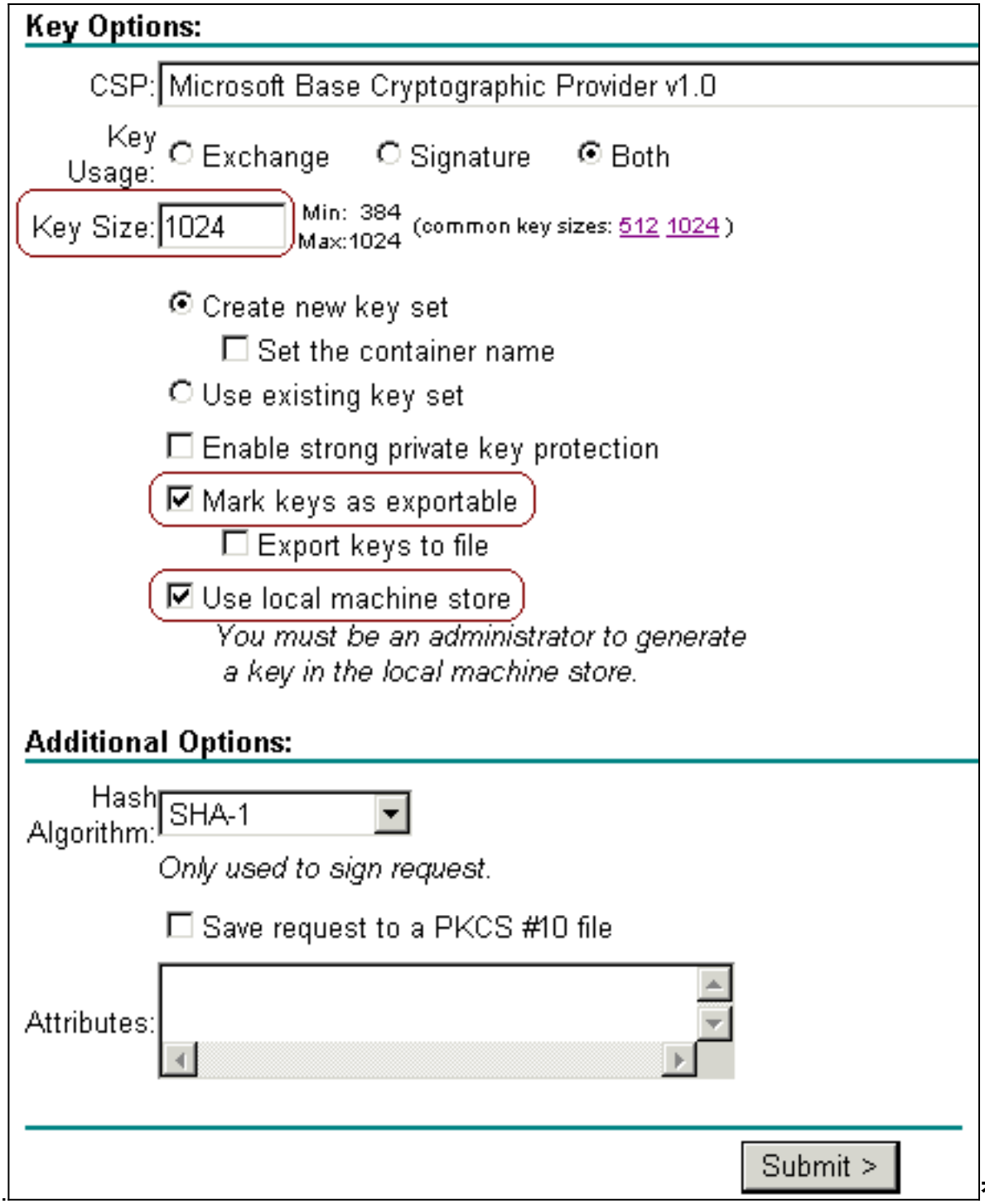

5. Submit **a certificate request to this CA using a form(양식을 사용하여 이 CA에 인증서 요청 제출)을** 선택한 다음 Next(**다음**)를 클릭합니다




6. 인증서 옵션을 구성합니다.인증서 템플릿으로 **웹 서버**를 선택하고 ACS 서버의 이름을 입력합

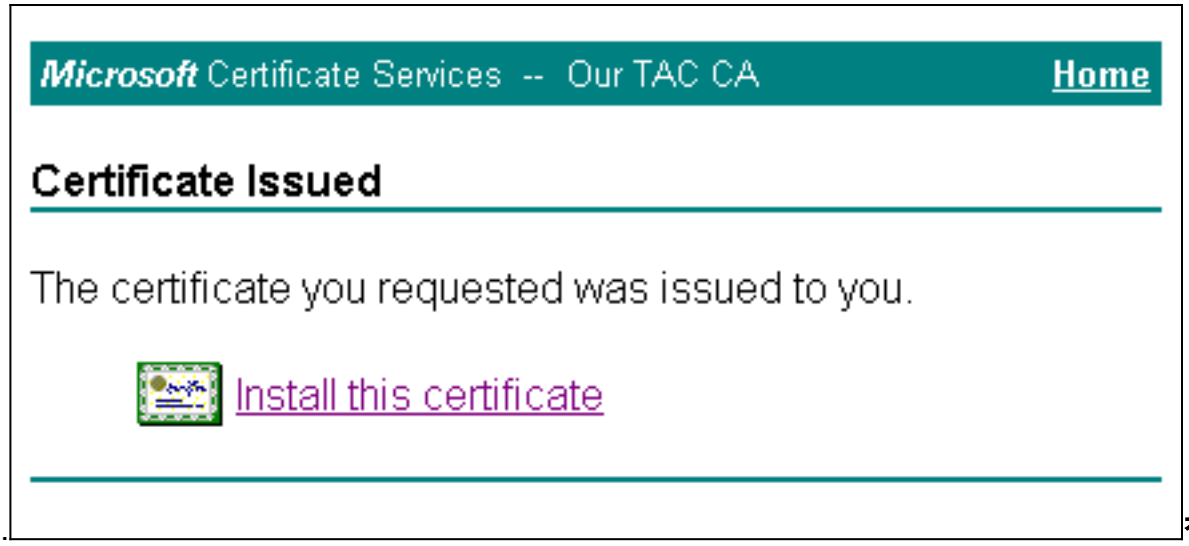



니다.Key Size(키 크기) 필드에 **1024를** 입력하고 **Mark keys as exportable(키를 내보낼 수** 있는 것으로 표시) 및 **Use local machine store(로컬 머신 저장소 사용**) 확인란을 선택합니다.필요에 따라 다른 옵션을 구성한 다음 Submit(제출)을 **클릭합니다**

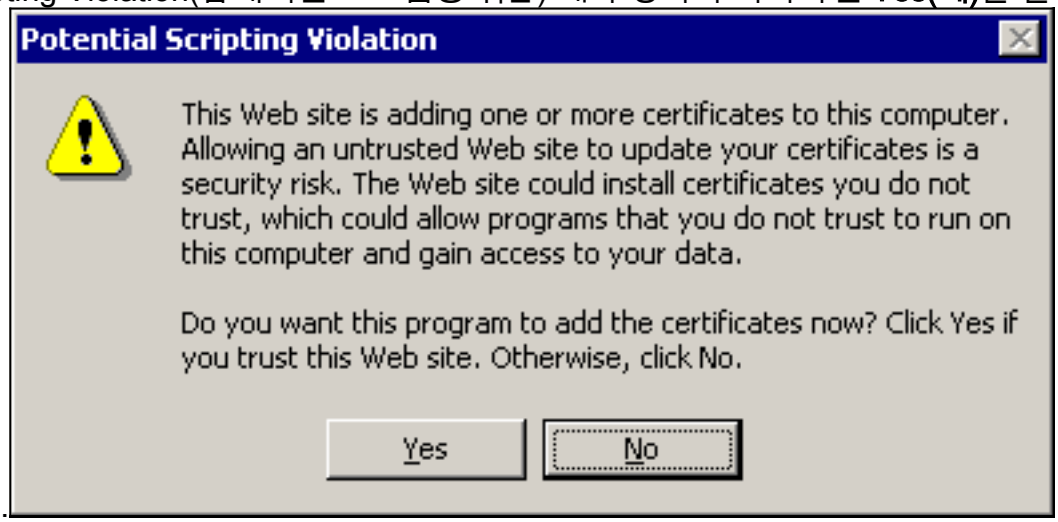



**참고:** Potential Scripting Violation(잠재적인 스크립팅 위반) 대화 상자가 나타나면 **Yes(예)**를 클릭하여 계속합니다.

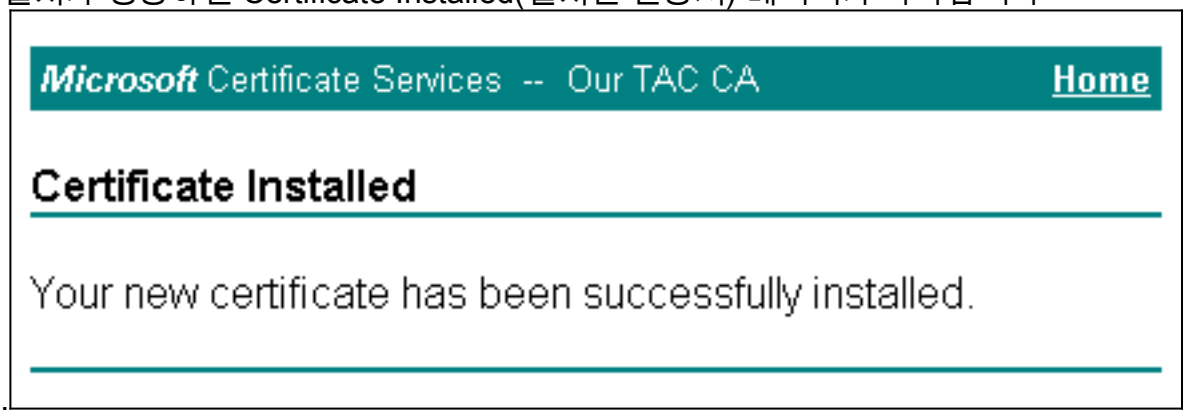

7. **이 인증서 설치를 클릭합니다**




**참고:** Potential Scripting Violation(잠재적인 스크립팅 위반) 대화 상자가 나타나면 **Yes(예)**를 클릭하여 계속합니다.




8. 설치가 성공하면 Certificate Installed(설치된 인증서) 메시지가 나타납니다



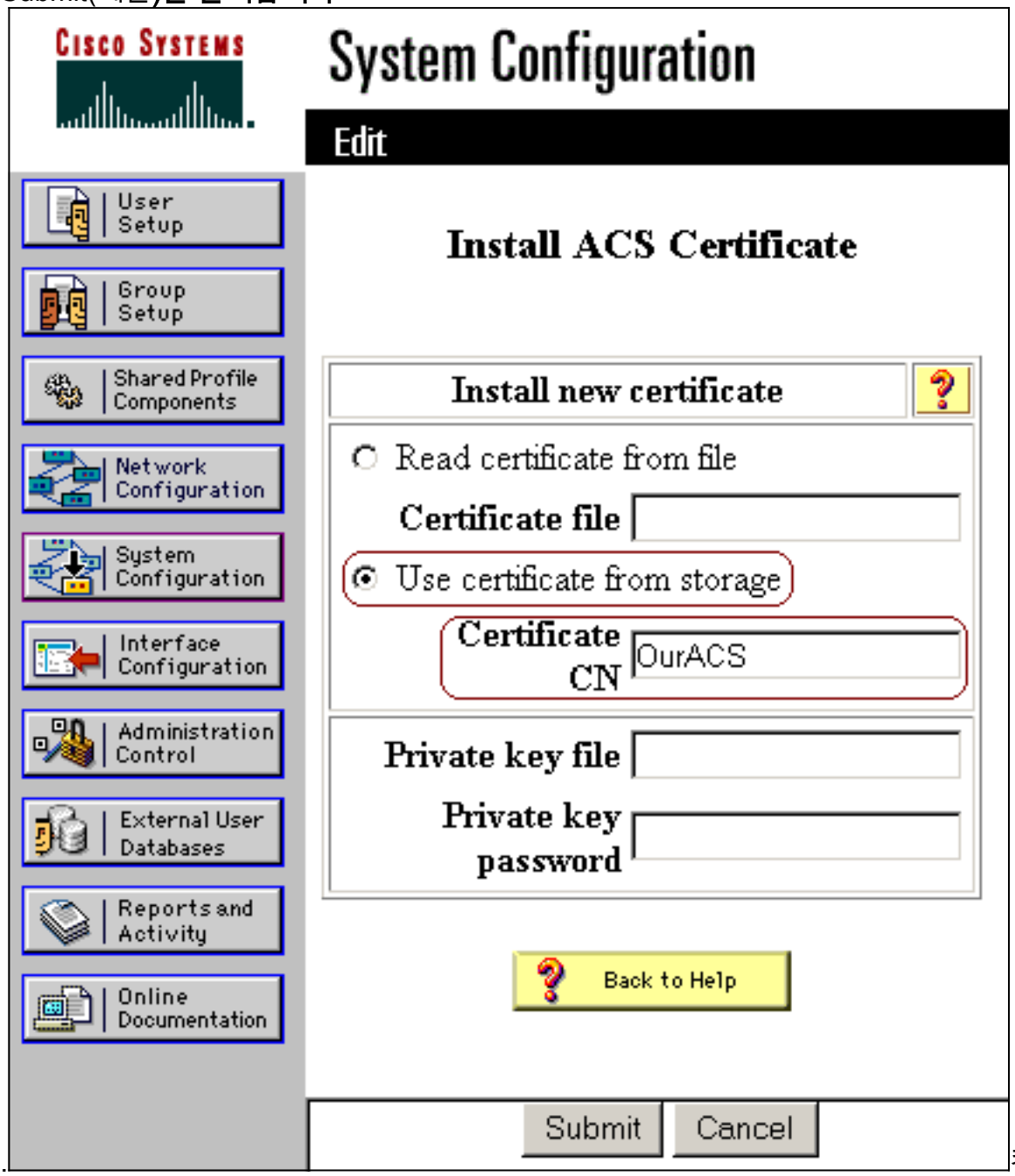

## 저장소에서 인증서를 사용하도록 ACS 구성

ACS가 저장소에서 인증서를 사용하도록 구성하려면 다음 단계를 완료합니다.

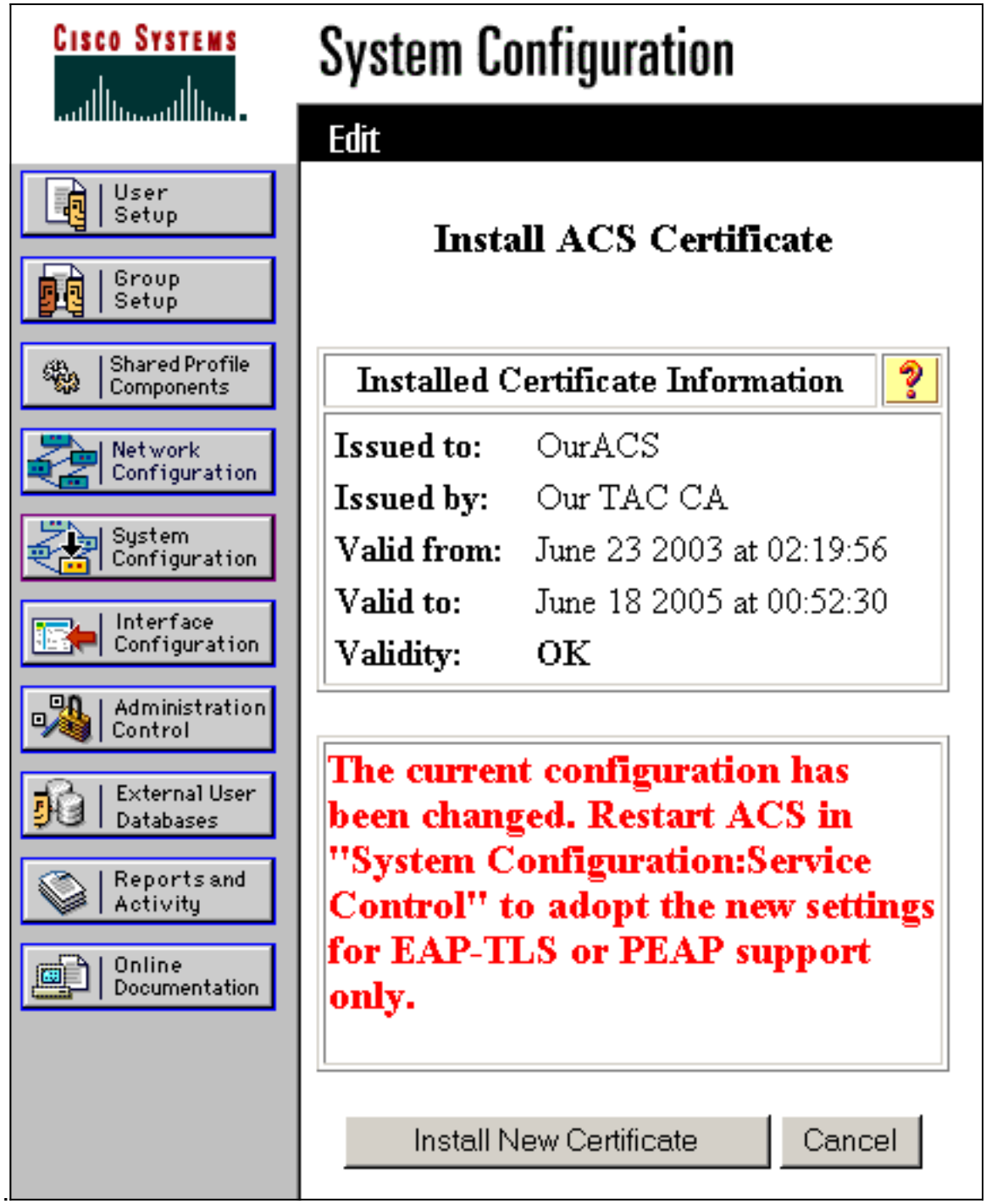
1. 웹 브라우저를 열고 **http://*ACS-ip-address*:2002/를 입력하여** ACS 서버에 액세스합니다.
2. System **Configuration(시스템 컨피그레이션)**을 클릭한 다음 **ACS Certificate Setup(ACS 인증서 설정)을 클릭합니다**.
3. Install **ACS Certificate(ACS 인증서 설치)를 클릭합니다**.
4. **Use certificate from storage** 라디오 버튼을 클릭합니다.
5. Certificate CN(인증서 CN) 필드에 이 문서의 ACS 서버에서 인증서 가져오기 섹션의 5a 단계

에서 할당한 인증서의 이름을 입력합니다.

6. Submit(제출)**을 클릭합니다**



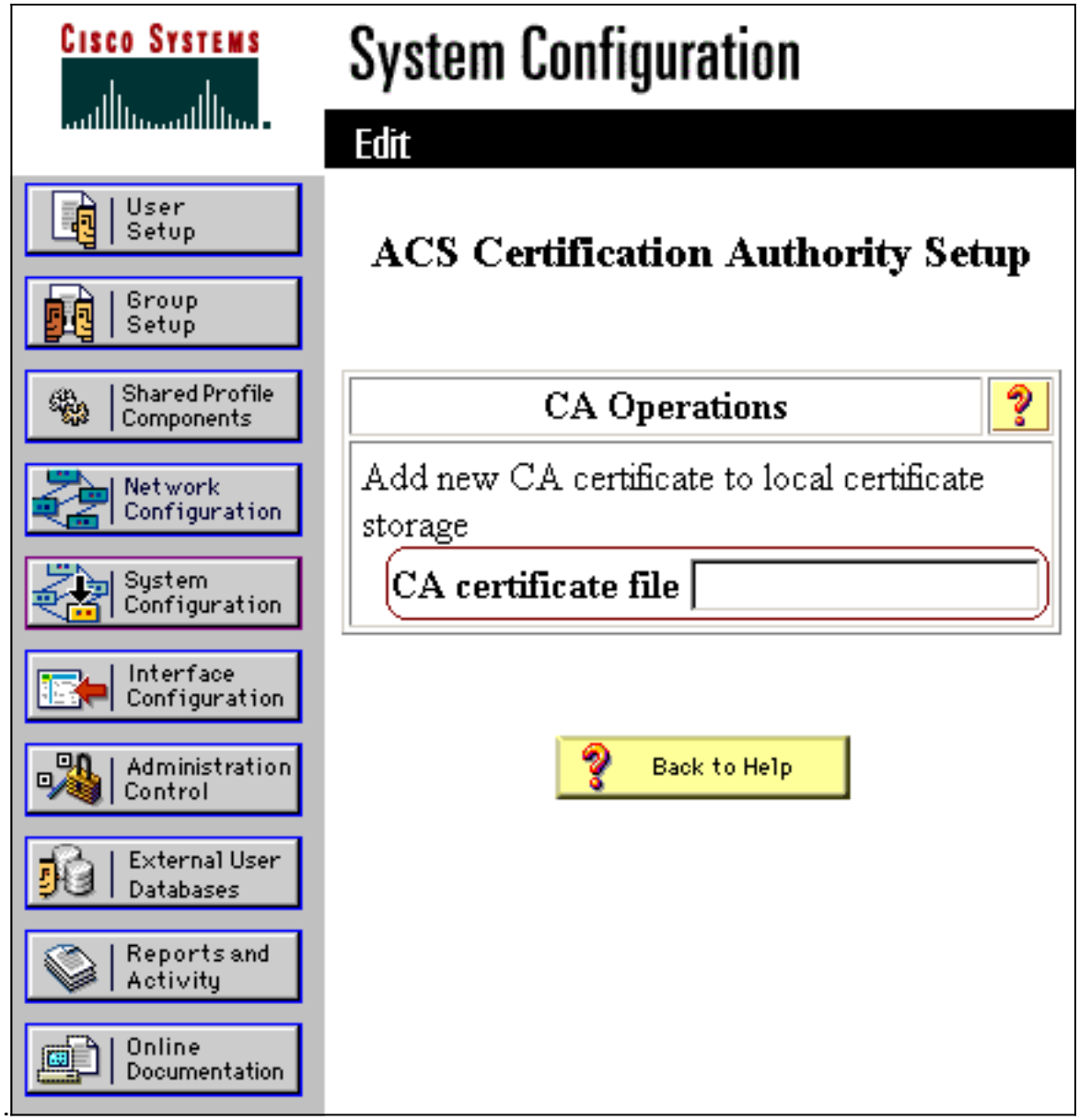

. 컨피그레이션이 완료되면 ACS 서버의 컨피그레이션이 변경되었음을 나타내는 확인 메시지가 나타납니다.**참고:** 지금은 ACS를 다시 시작할 필요가 없습니다



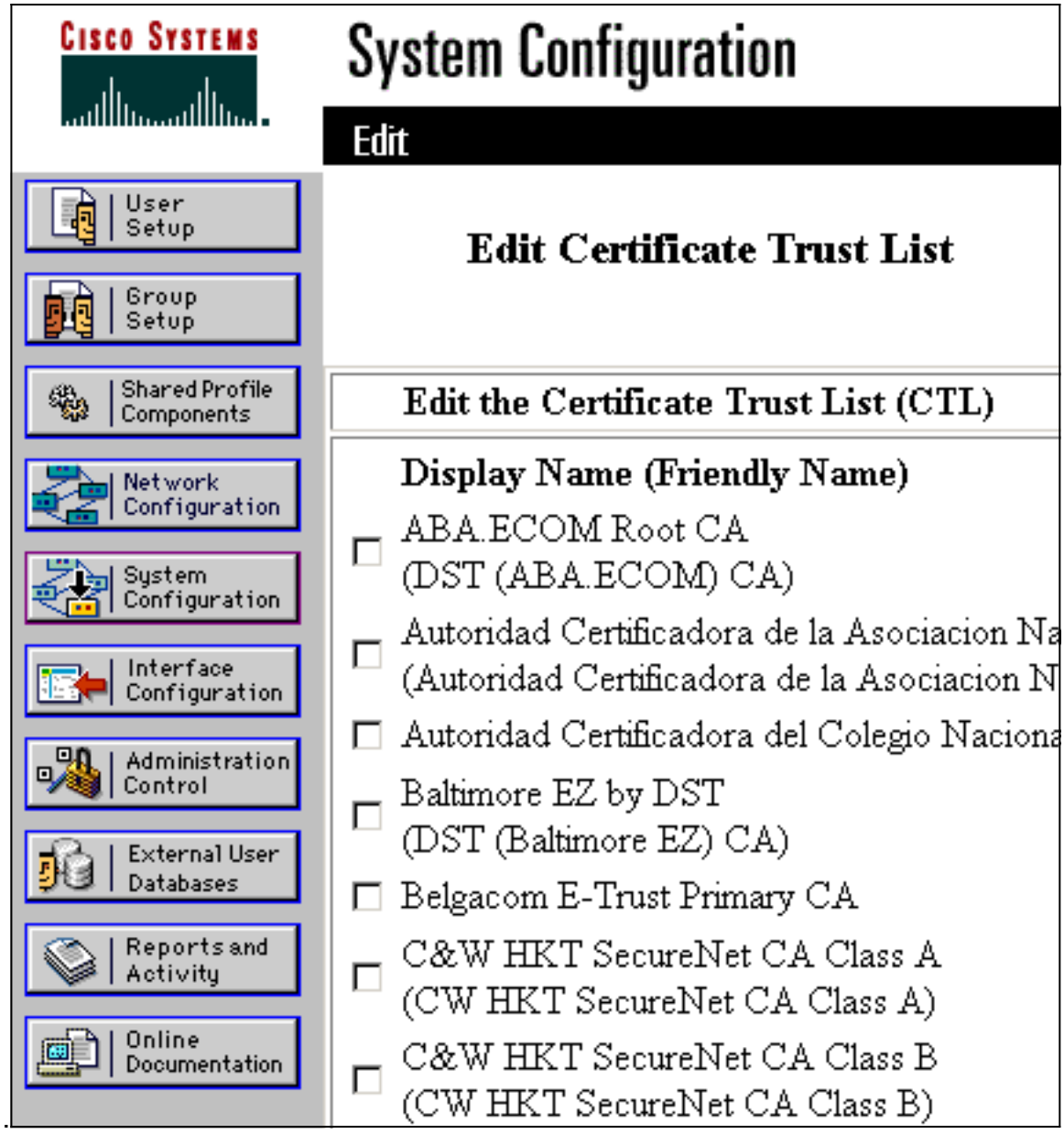

## ACS에서 신뢰해야 하는 추가 인증 기관 지정

ACS는 자체 인증서를 발급한 CA를 자동으로 신뢰합니다.추가 CA에서 클라이언트 인증서를 발급한 경우 다음 단계를 완료해야 합니다.

1. System **Configuration(시스템 컨피그레이션)**을 클릭한 다음 **ACS Certificate Setup(ACS 인증서 설정)을 클릭합니다**.
2. ACS **Certificate Authority Setup(ACS 인증 기관 설정)**을 클릭하여 CA를 신뢰할 수 있는 인증서 목록에 추가합니다.
3. CA 인증서 파일의 필드에 인증서의 위치를 입력한 다음 Submit(제출)을 **클릭합니다**




4. Edit **Certificate Trust List를 클릭합니다**.
5. ACS에서 신뢰해야 하는 모든 CA를 선택하고 ACS에서 신뢰하지 않아야 하는 모든 CA의 선택을 취소합니다.
6. Submit(제출)**을 클릭합니다**




## 서비스를 다시 시작하고 ACS에서 EAP-TLS 설정 구성

서비스를 다시 시작하고 EAP-TLS 설정을 구성하려면 다음 단계를 완료합니다.

1. System **Configuration(시스템 컨피그레이션)**을 클릭한 다음 **Service Control(서비스 제어)**을 클릭합니다.
2. 서비스를 다시 시작하려면 Restart를 클릭합니다.
3. EAP-TLS 설정을 구성하려면 **System Configuration(시스템 컨피그레이션)**을 클릭한 다음 **Global Authentication Setup(전역 인증 설정)을 클릭합니다**.
4. Allow **EAP-TLS(EAP-TLS 허용)**를 선택한 다음 하나 이상의 인증서 비교를 확인합니다.
5. Submit(제출)**을 클릭합니다**