

디지털 인증서를 가져오기 위해 VPN 클라이언트 3.x 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[VPN 클라이언트 구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 디지털 인증서를 가져오기 위해 Cisco VPN Client 3.x를 구성하는 방법을 보여 줍니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco VPN Client 3.x를 실행하는 PC를 기반으로 합니다.

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.

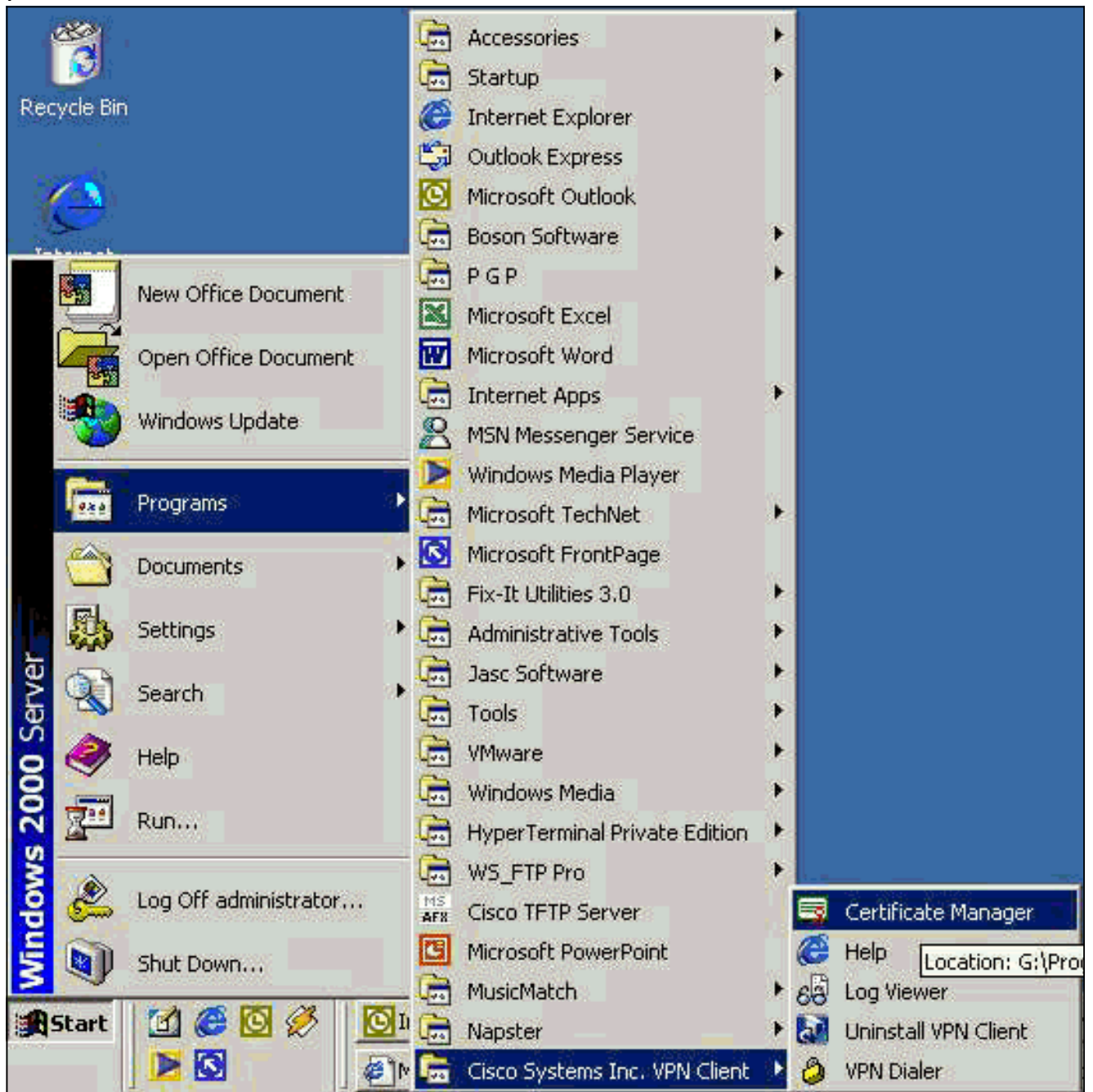
표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 표기 규칙을 참고하십시오.](#)

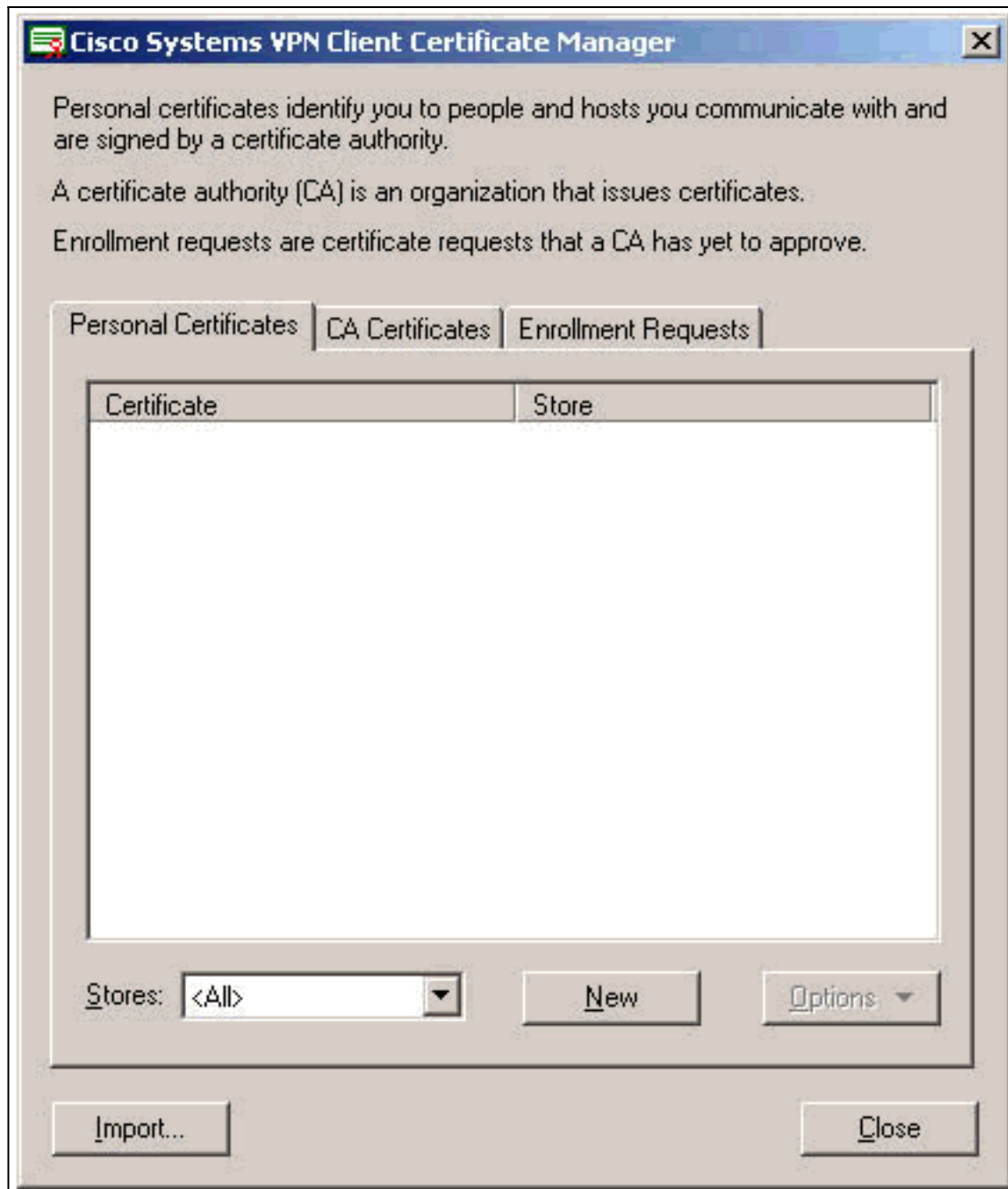
VPN 클라이언트 구성

VPN 클라이언트를 구성하려면 다음 단계를 완료합니다.

1. Start(시작) > Programs(프로그램) > Cisco Systems Inc. VPN client(Cisco Systems Inc. VPN 클라이언트) > Certificate Manager(인증서 관리자)를 선택하여 VPN 클라이언트 인증서 관리자를 시작합니다



2. Personal Certificates(개인 인증서) 탭을 선택하고 New(새로 만들기)를 클릭합니다



참고: VPN

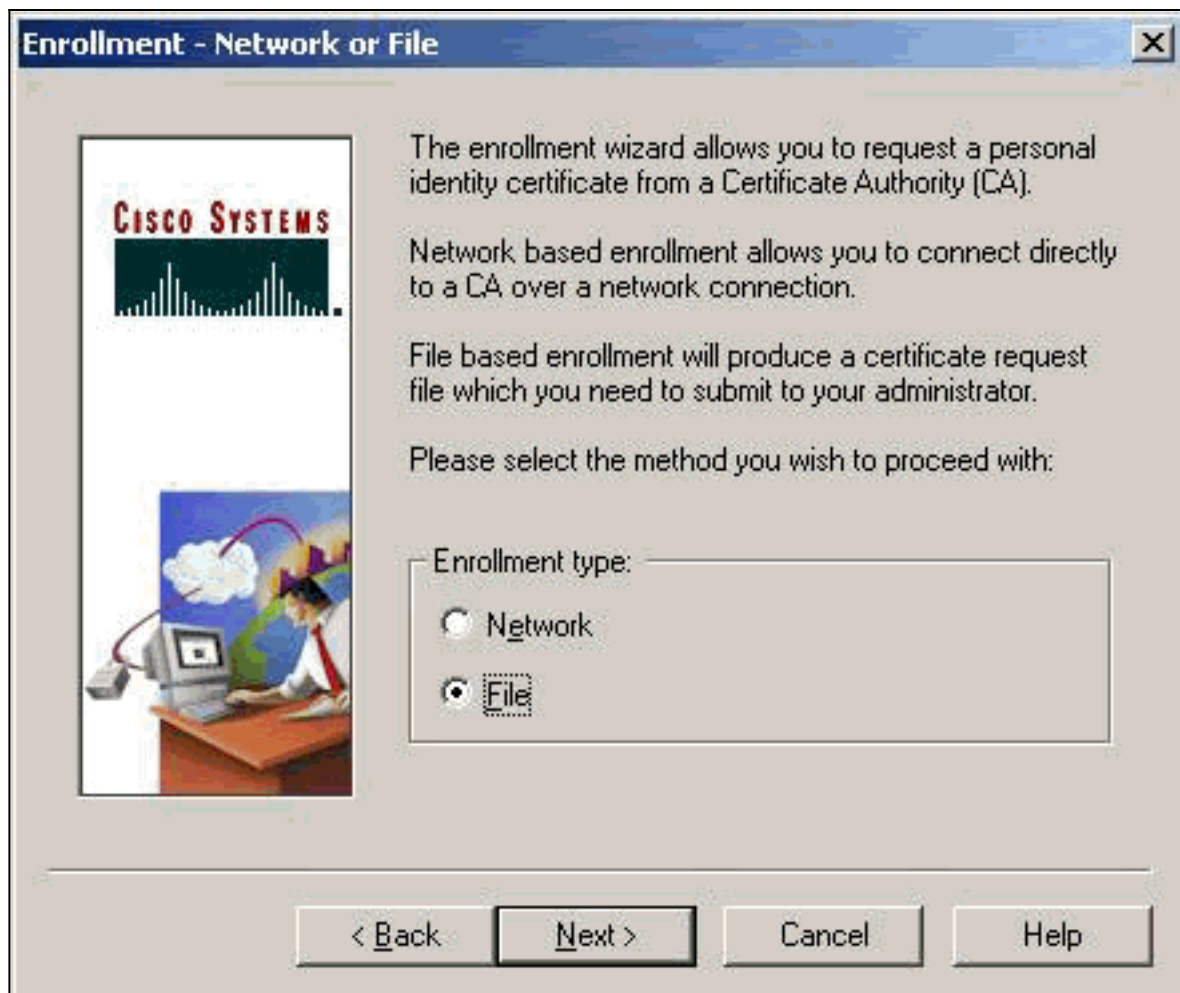
연결을 위해 사용자를 인증하는 시스템 인증서는 IPsec에서 수행할 수 없습니다.

3. VPN 클라이언트에서 비밀번호를 입력하라는 메시지를 표시할 때 인증서를 보호할 비밀번호를 지정합니다. 인증서의 개인 키에 액세스해야 하는 작업을 계속하려면 지정된 암호가 필요

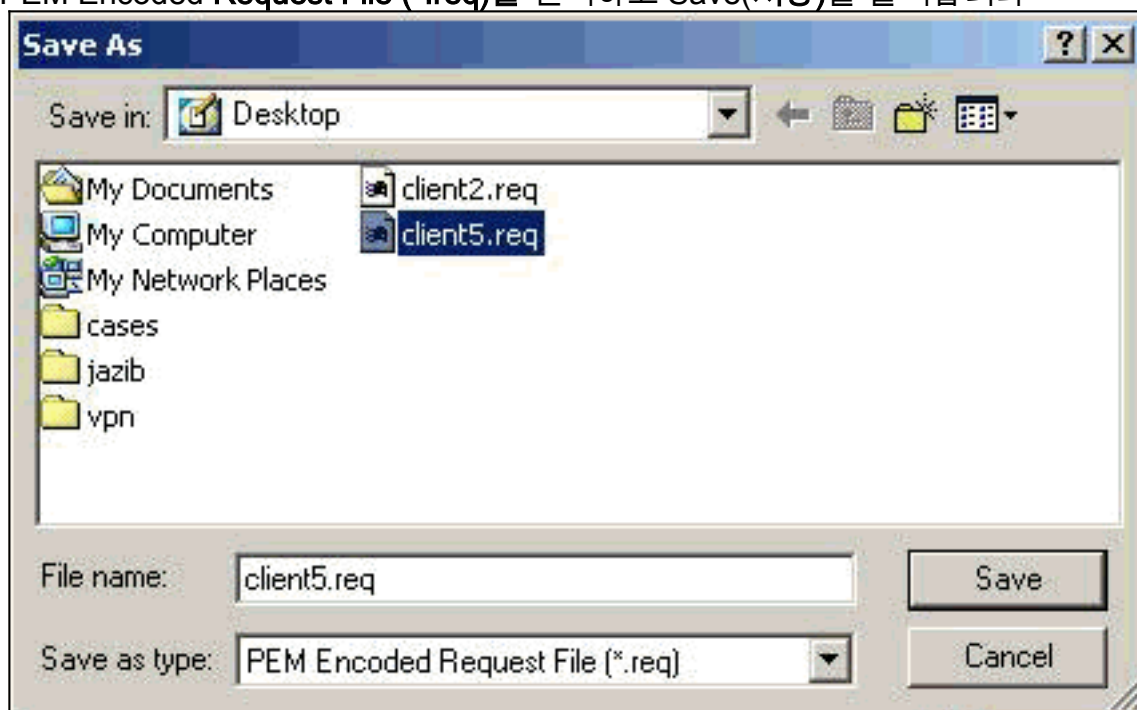


합니다.

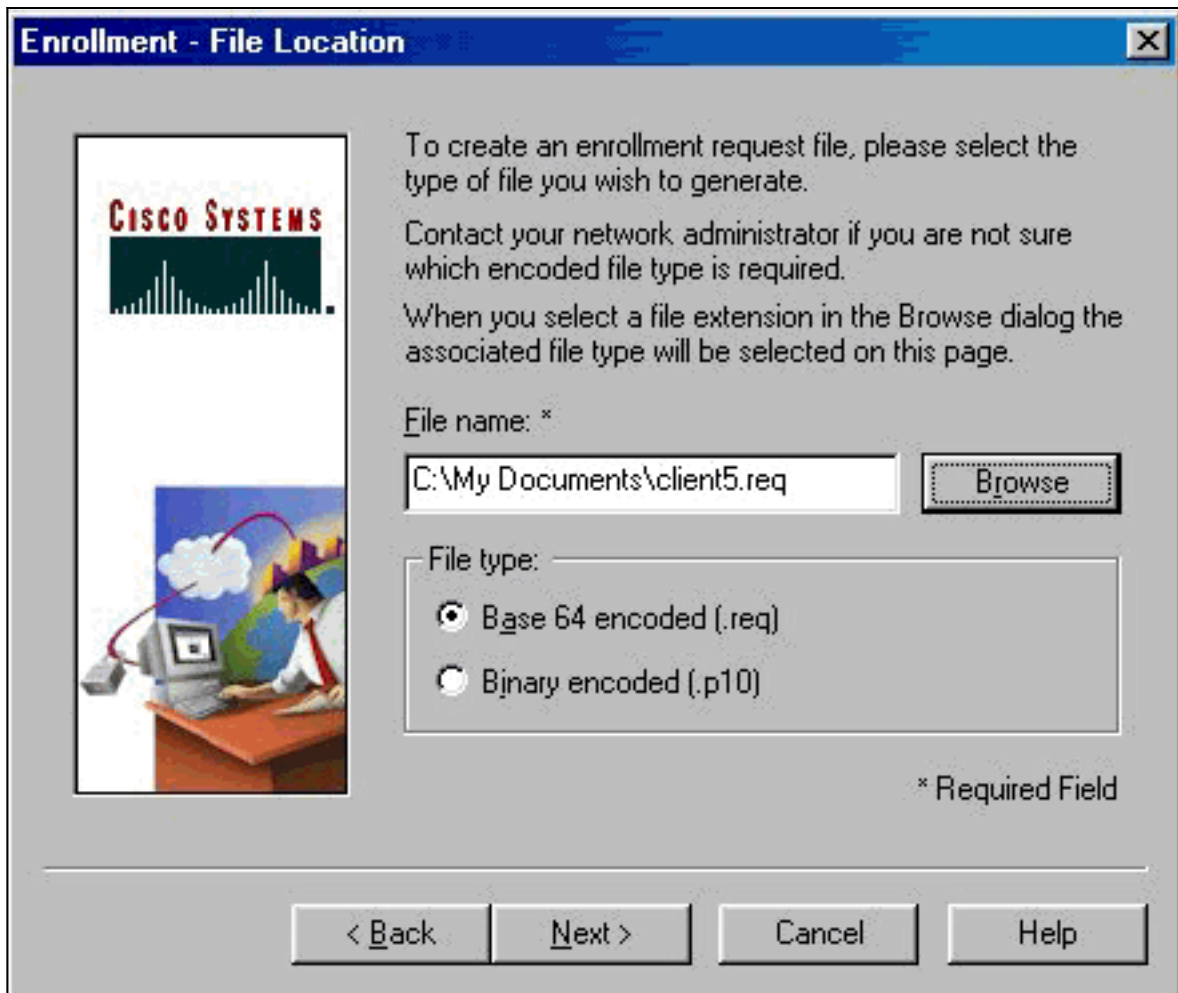
4. Enrollment 페이지에서 PKCS #10 형식을 사용하여 인증서를 요청하려면 File을 선택합니다. 그런 다음 **Next(다음)**를 클릭합니다



5. Browse(찾아보기)를 클릭하고 인증서 요청 파일의 파일 이름을 지정합니다. 파일 유형에서 PEM Encoded Request File (*.req)을 선택하고 Save(저장)를 클릭합니다





6. VPN Client Enrollment 페이지에서 Next를 클릭합니다



7. 등록 양식의 필드를 입력합니다. 다음 예에서는 필드를 보여 줍니다. 일반 이름 = 사용자1부서 = IPSECCERT(VPN 3000 Concentrator의 OU(조직 구성 단위) 및 그룹 이름과 일치해야 합니다.) 회사 = Cisco Systems 주 = 노스캐롤라이나 국가 = 미국 이메일 = User1@email.com IP 주소 = (선택 사항; 인증서 요청에서 IP 주소를 지정하는 데 사용됨) 도메인 = cisco.com 완료되면 **Next**(다음)를 클릭합니다

Enrollment - Form

Enter your certificate enrollment information in the fields provided below.

Common Name (cn):* User1

Department (ou): IPSECCERT

Company (o): Cisco Systems

State (st): NorthCarolina

Country (c): US

Email (e): User1@email.com

IP Address:

Domain: cisco.com

* Required Field

< Back Next > Cancel Help

8. Finish를 클릭하여 등록을 계속 진행합니다

Enrollment - Summary

This is a summary of the information you have provided for this certificate enrollment request.

Select Finish to proceed with the enrollment or Back to make modifications.

Enrollment: File - client5.req

Certificate Store: Cisco

Common Name: User1

Department: IPSECCERT

Company: Cisco Systems

State: NorthCarolina

Country: US

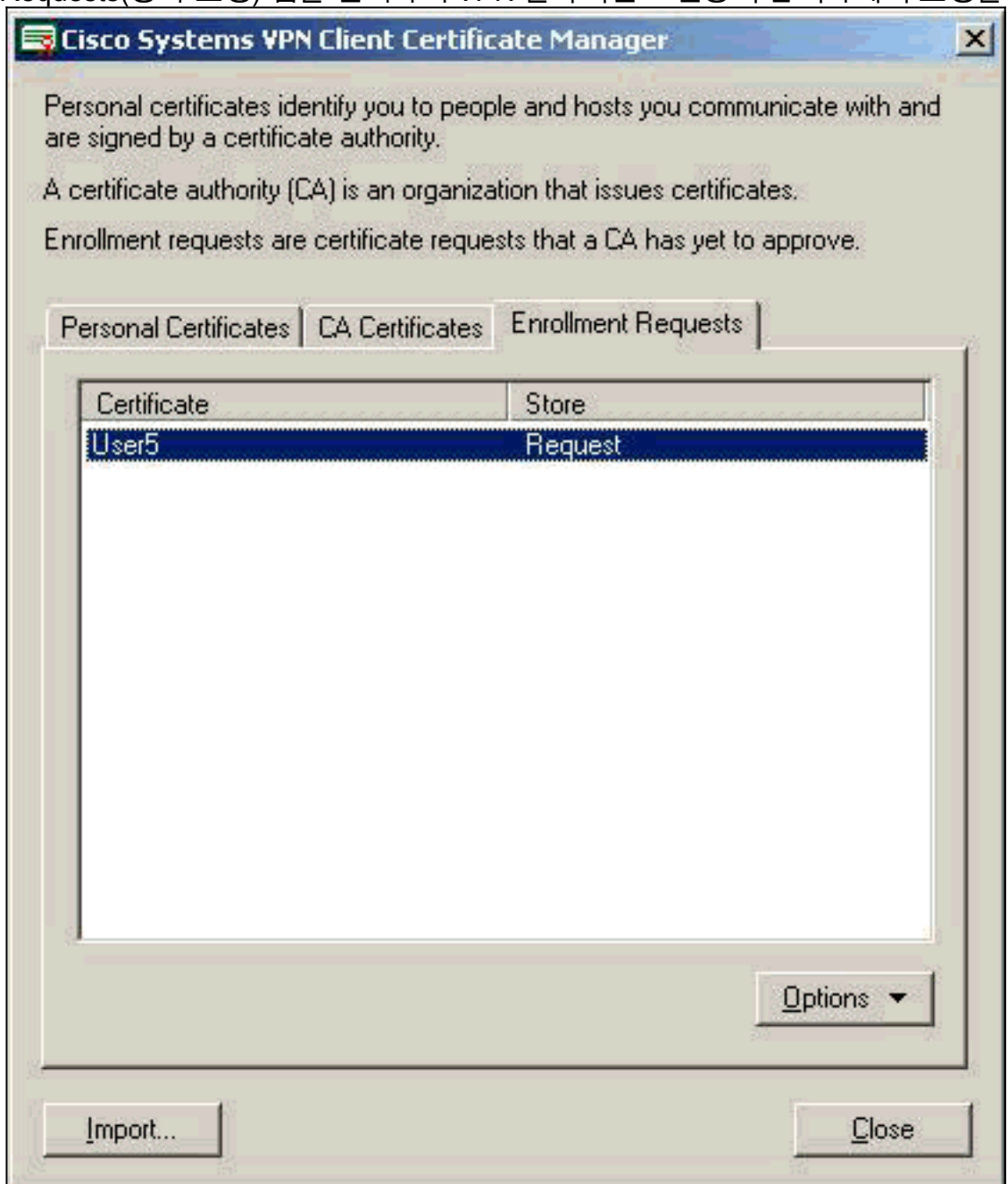
Email: User1@email.com

IP Address:

Domain: cisco.com

< Back Finish Cancel Help

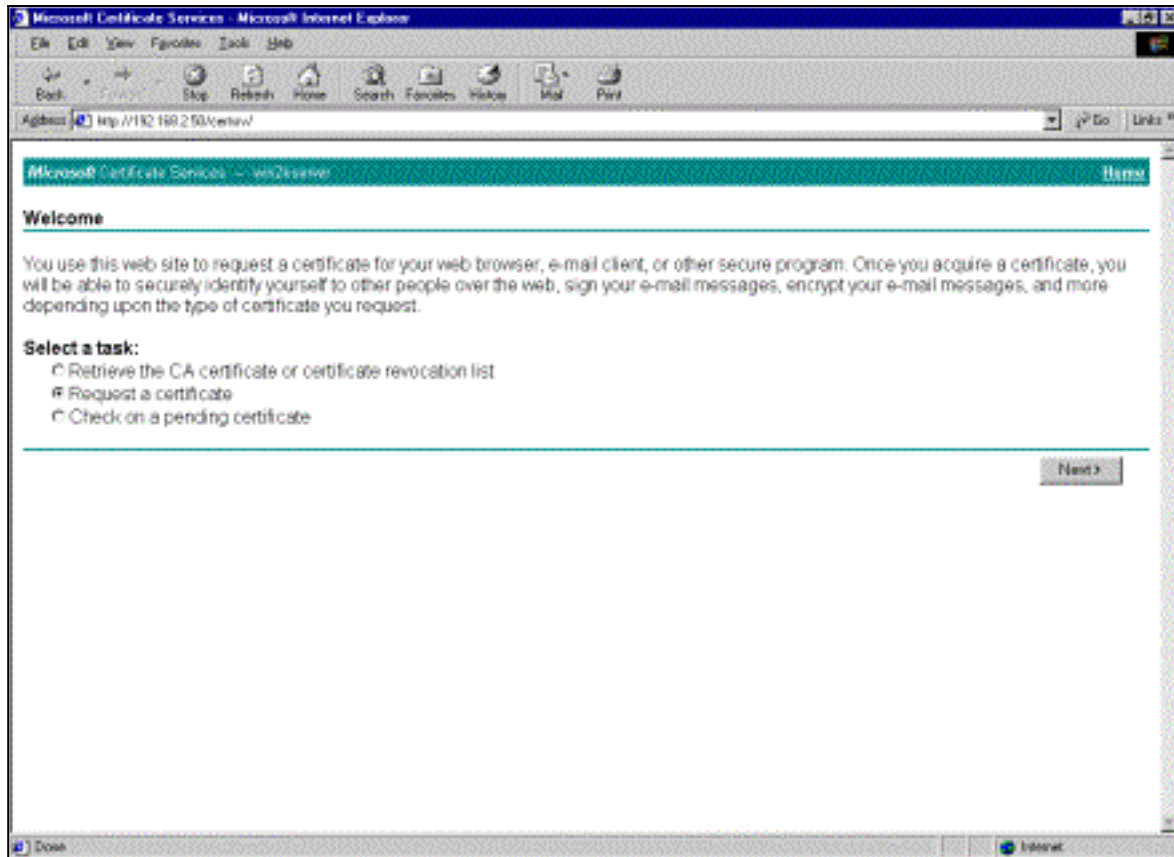
9. Enrollment Requests(등록 요청) 탭을 선택하여 VPN 클라이언트 인증서 관리자에서 요청을



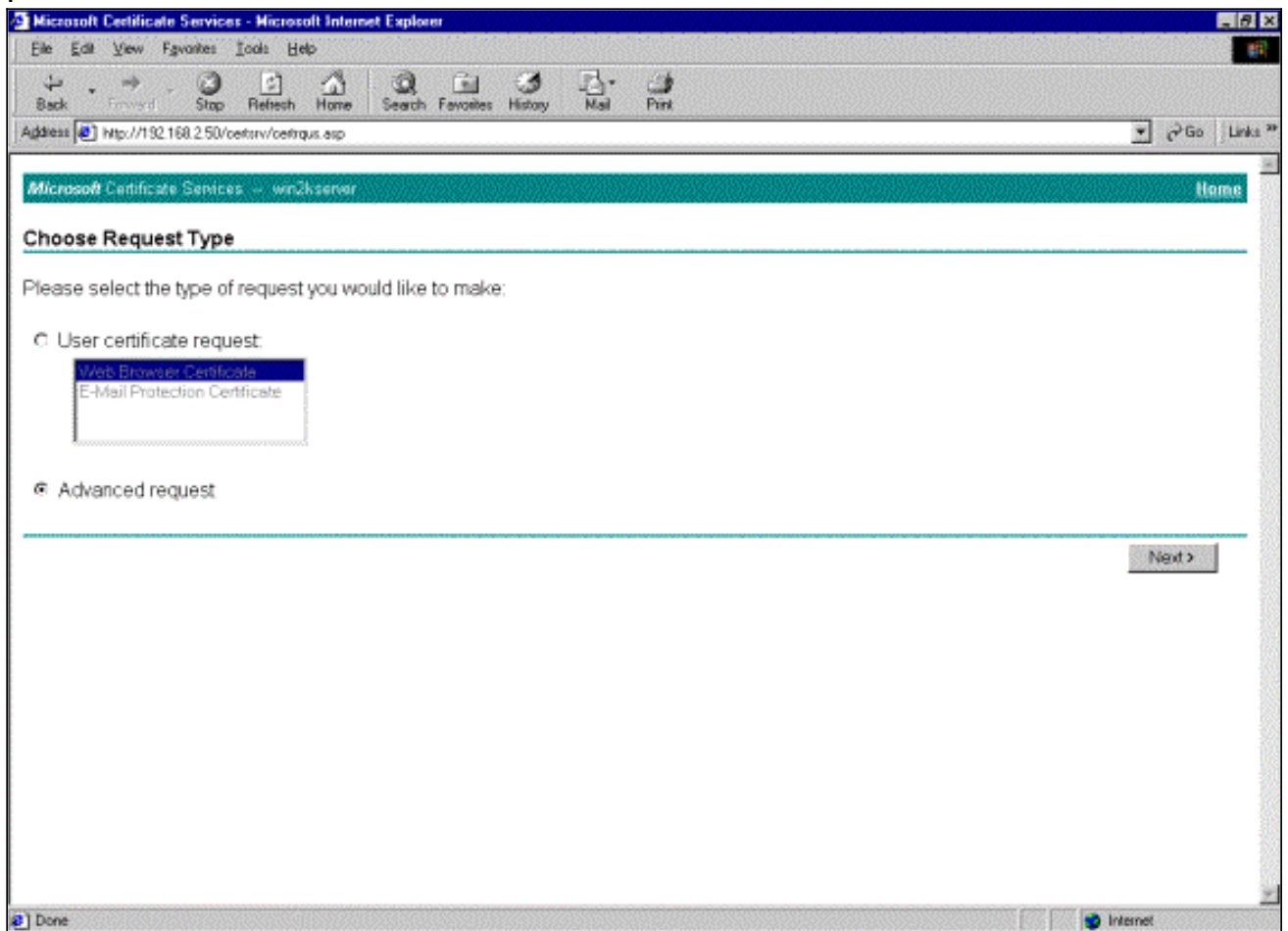
확인합니다.

10. 요청을 제출하려면 CA(Certification Authority) 서버 및 VPN 클라이언트 인터페이스를 동시에 실행합니다.

11. Request a certificate(인증서 요청)를 선택하고 CA 서버에서 Next(다음)를 클릭합니다

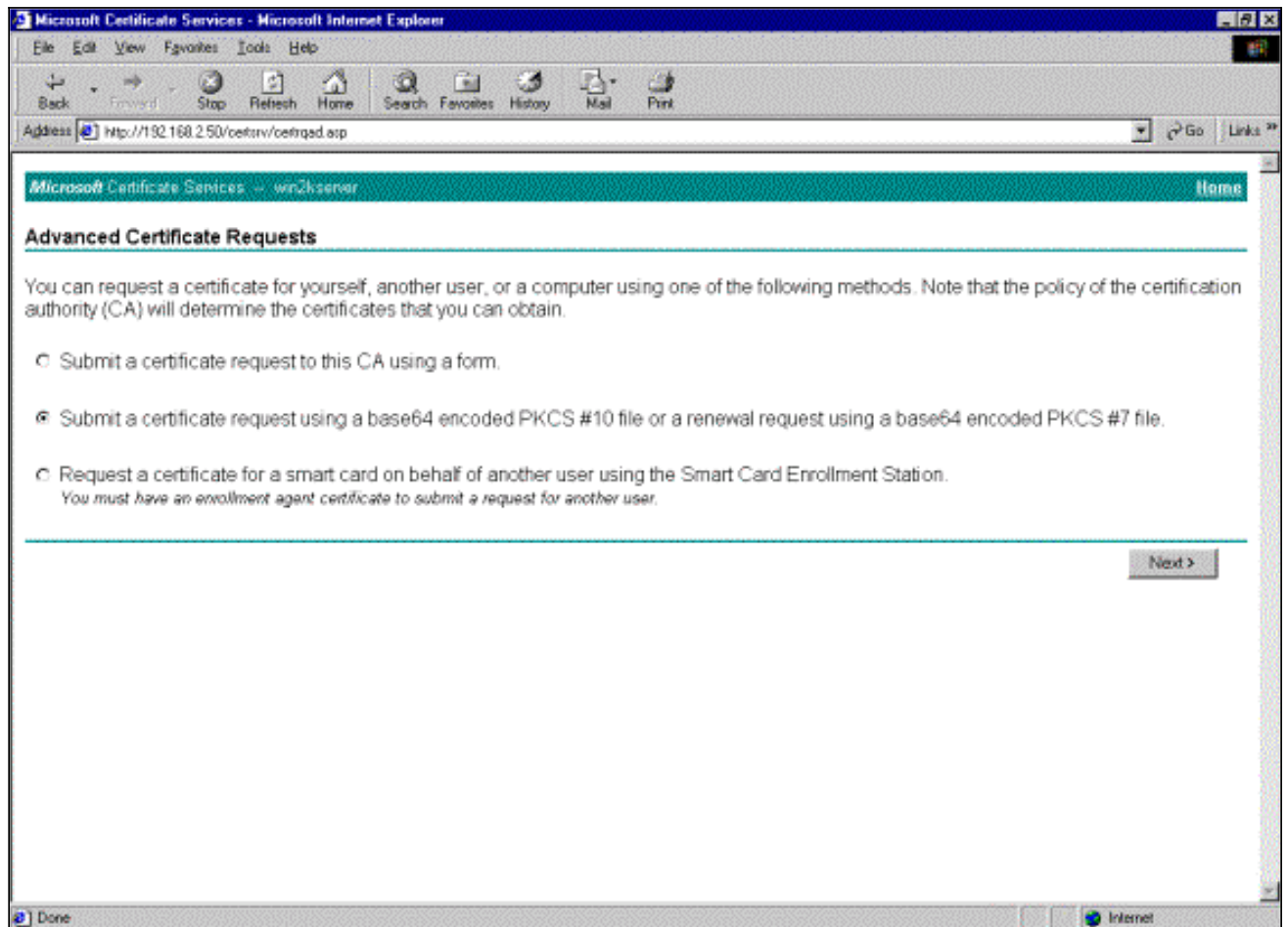


12. 요청 유형에 대해 고급 요청을 선택하고 다음을 클릭합니다

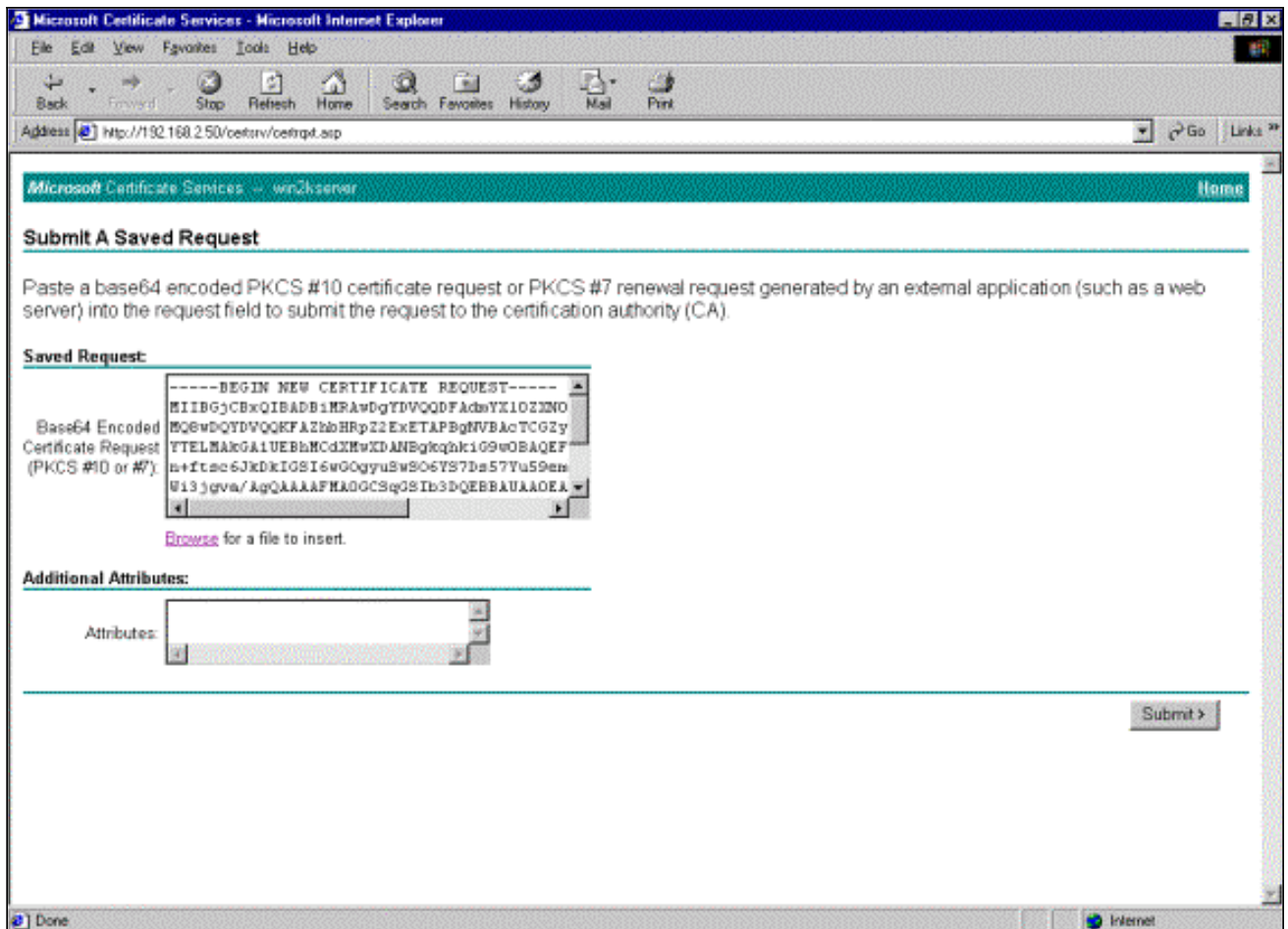


13. Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file(base64 인코딩 PKCS 파일을 사용하는 갱신 요청을 Advanced Certificate Requests(고급 인증서 요청)에서 선택한 다음 Next(다음)를 클릭합니

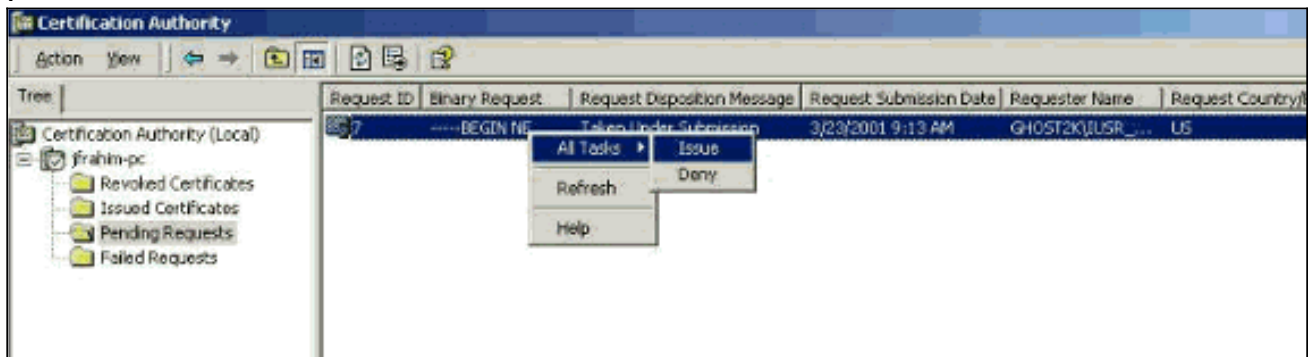
다



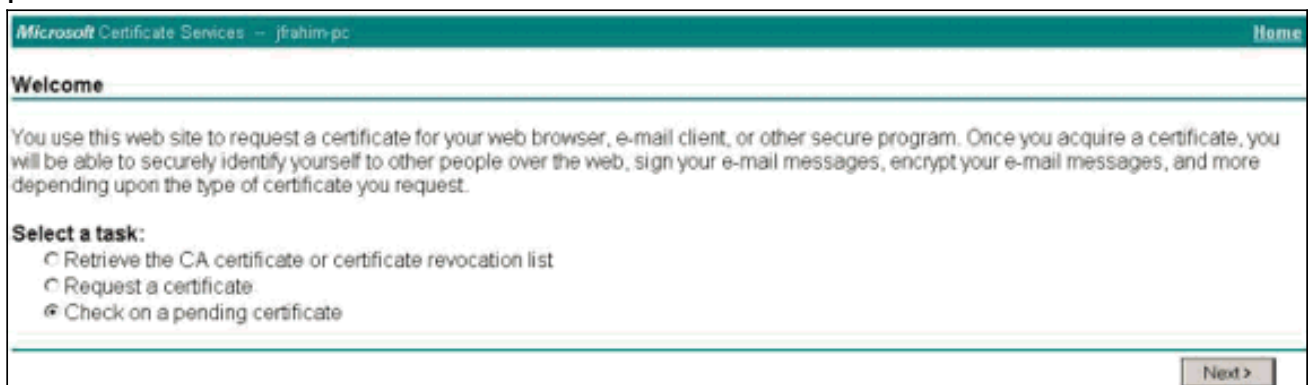
14. VPN Client 요청 파일을 강조 표시하고 Saved Request(저장된 요청)에서 CA 서버에 붙여넣습니다. 그런 다음 **Submit(제출)**을 클릭합니다



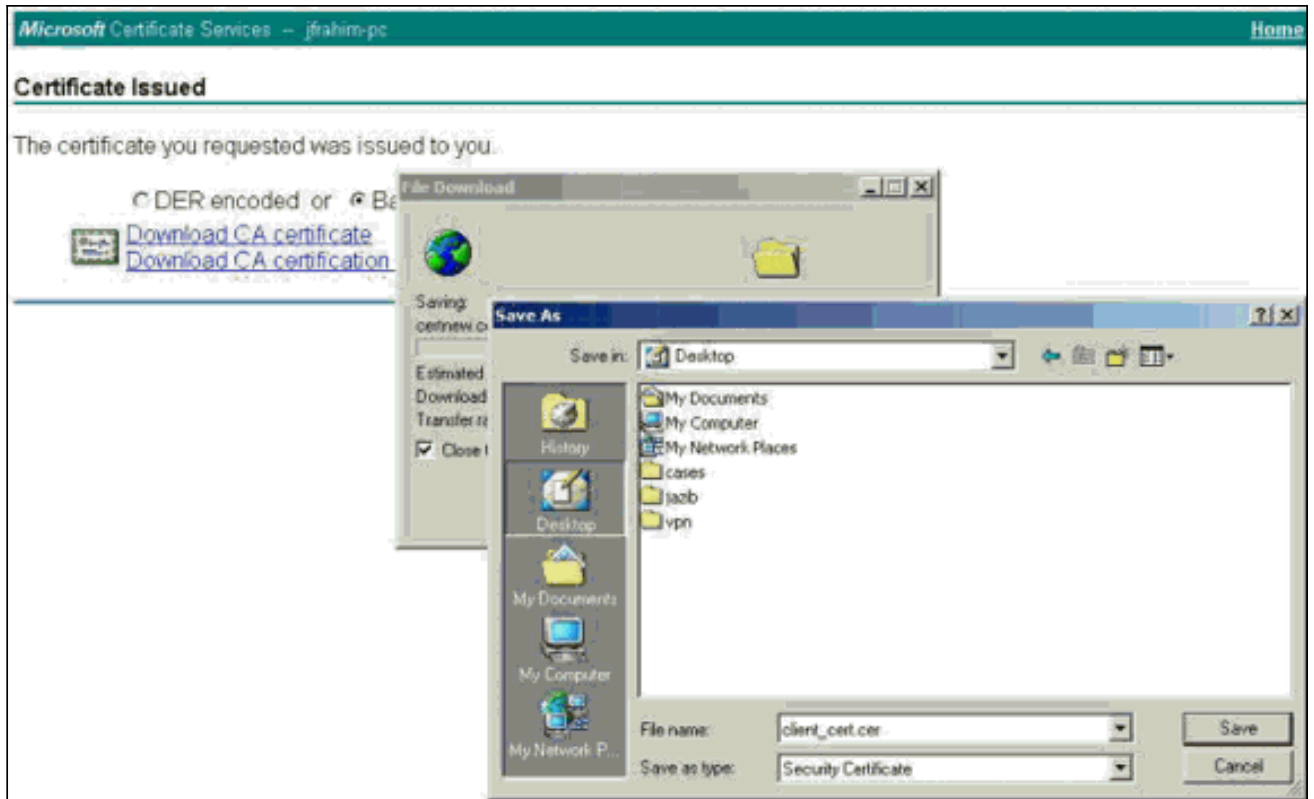
15. CA 서버에서 VPN 클라이언트 요청에 대한 ID 인증서를 발급합니다



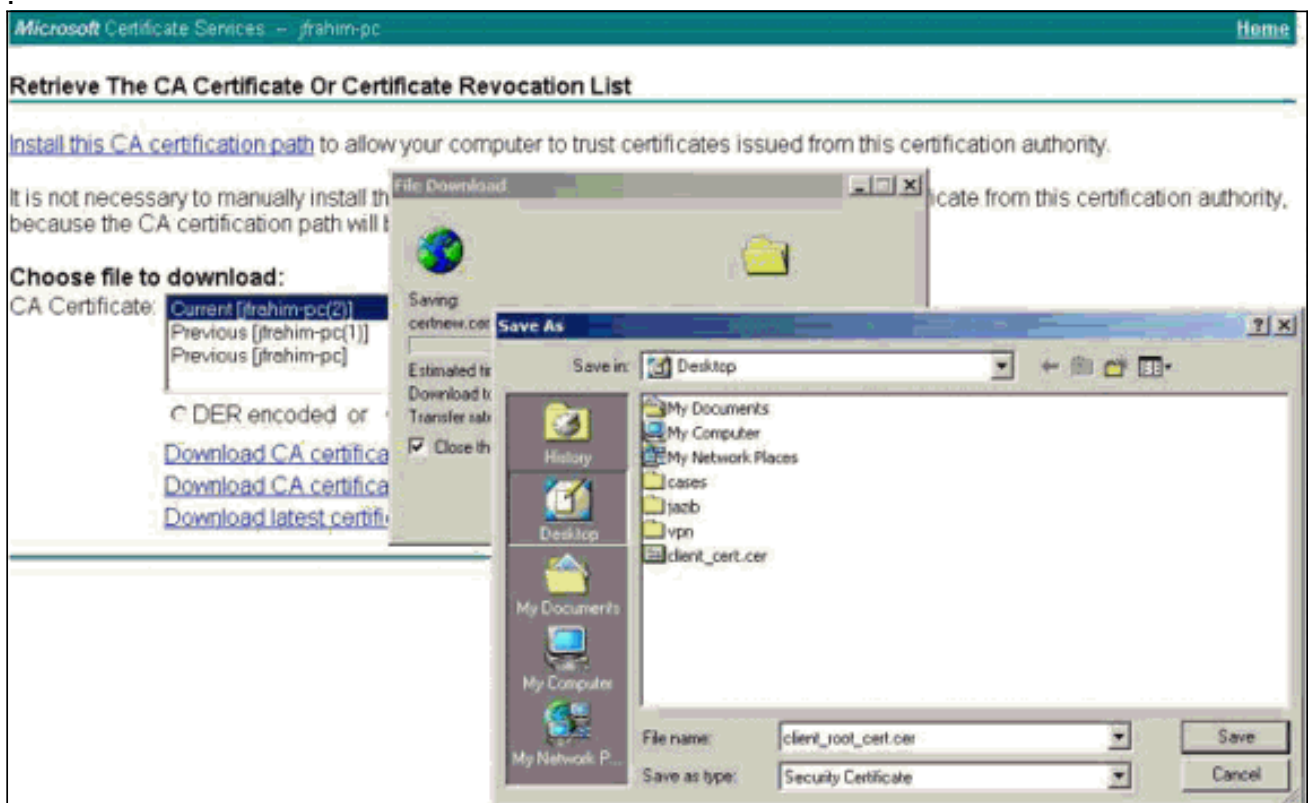
16. VPN 클라이언트에 루트 및 ID 인증서를 다운로드합니다. CA 서버에서 Check on a pending certificate(보류 중인 인증서 확인)를 선택하고 Next(다음)를 클릭합니다



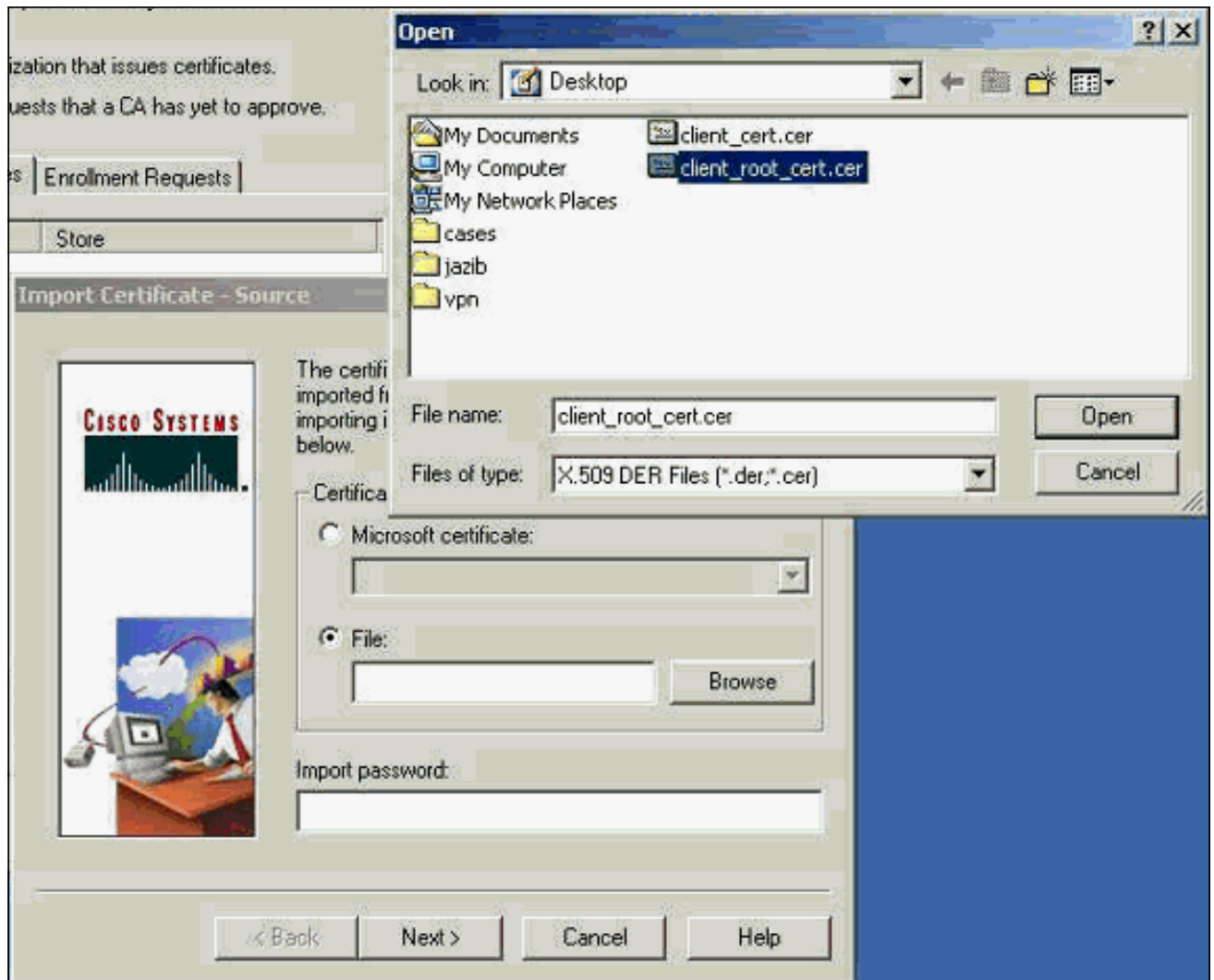
17. Base 64 encoded를 선택합니다. 그런 다음 CA 서버에서 Download CA certificate(CA 인증서 다운로드)를 클릭합니다



18. Retrieve the CA Certificate or Certificate Revocation List 페이지에서 다운로드할 파일을 선택하여 CA 서버에서 루트 인증서를 가져옵니다. 그런 다음 **Next(다음)**를 클릭합니다



19. Certificate Manager > CA Certificate > VPN Client에서 **Import**를 선택한 다음 루트 CA 파일을 선택하여 루트 및 ID 인증서를 설치합니다

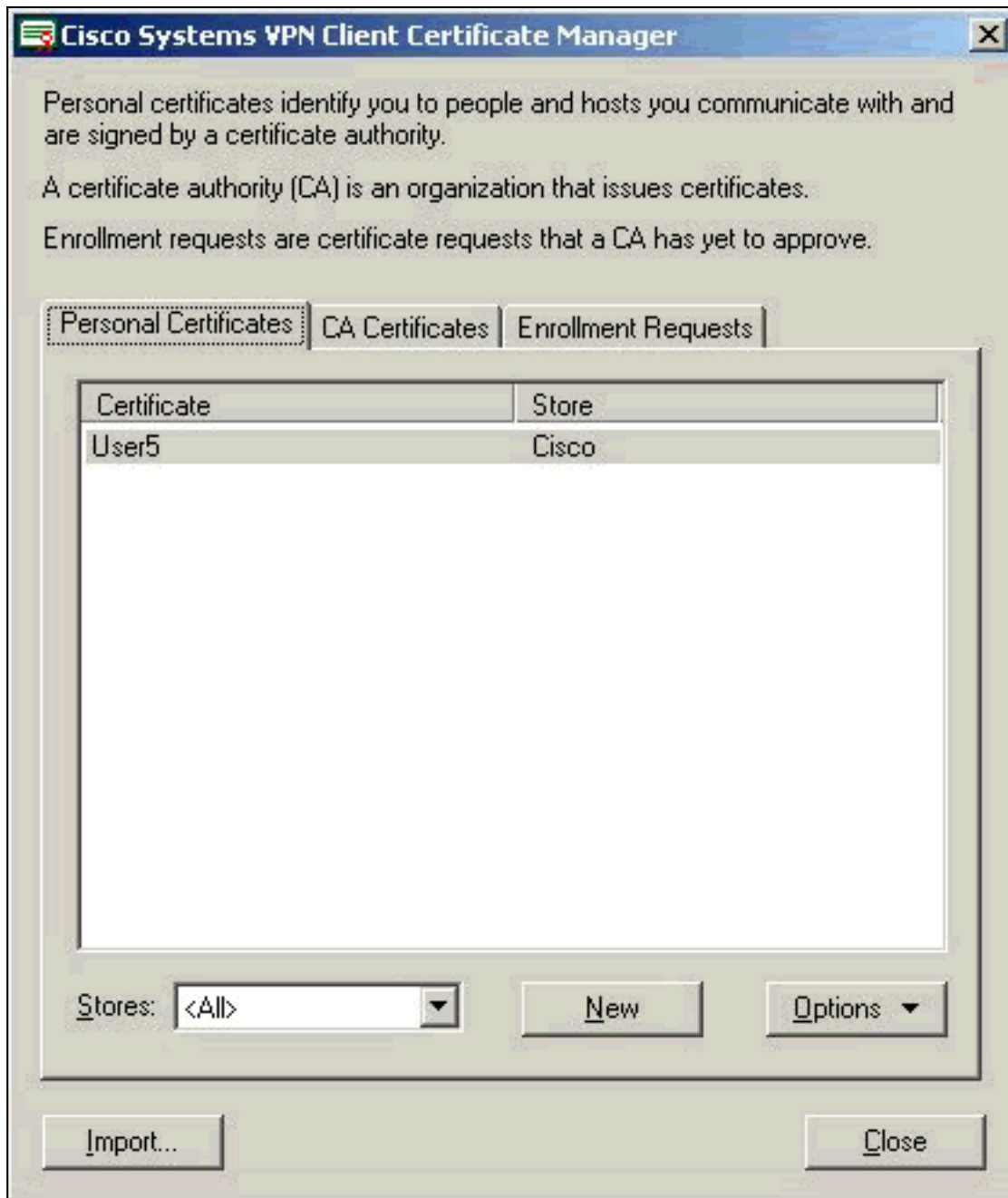


20. Certificate Manager > Personal Certificates > Import를 선택하고 ID 인증서 파일을 선택합니

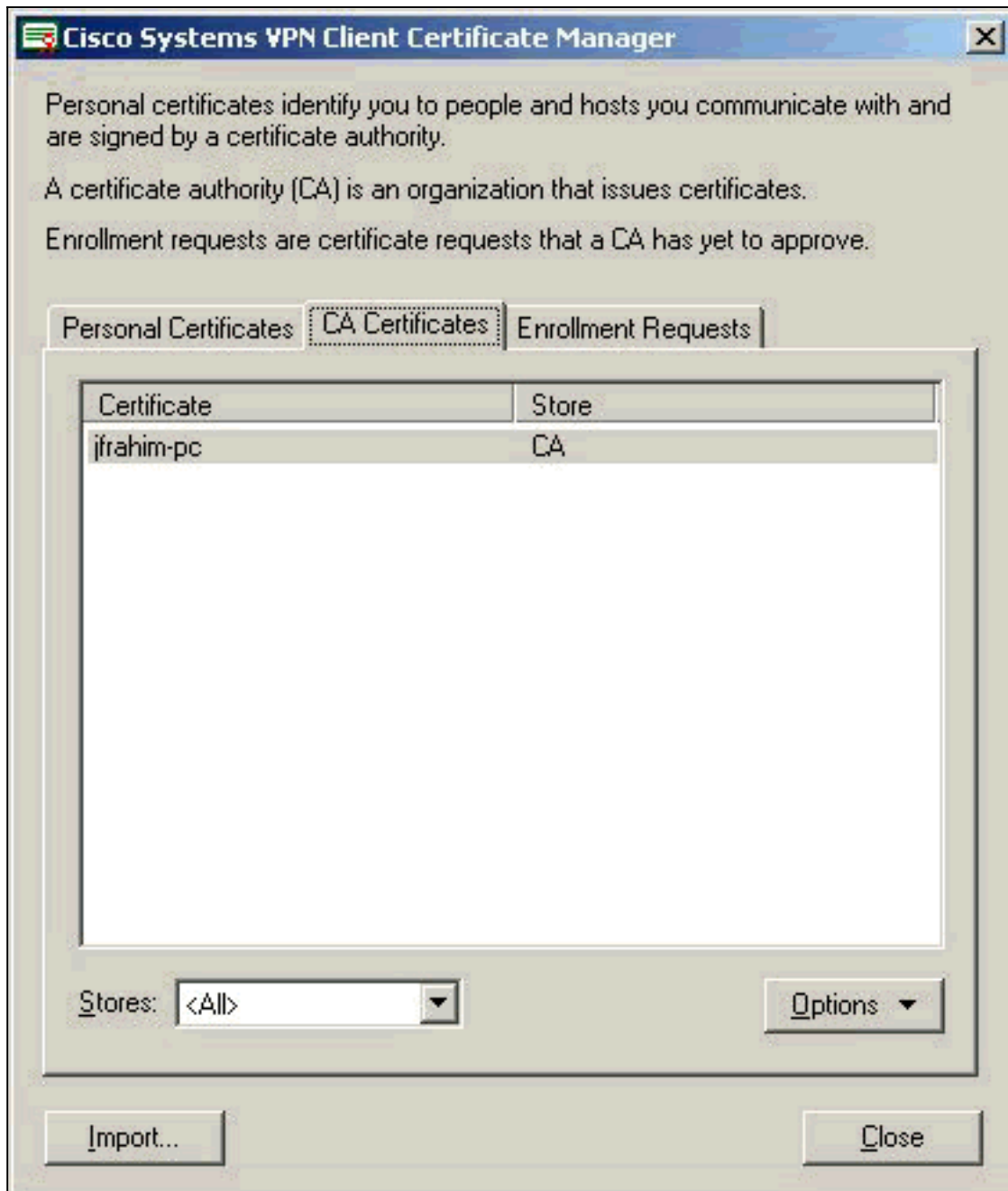


다.

21. Personal Certificates(개인 인증서) 탭 아래에 ID 인증서가 표시되는지 확인합니다



22. 루트 인증서가 CA Certificates(CA 인증서) 탭 아래에 나타나야 합니다



다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

Microsoft CA Server에 등록하려고 하면 이 오류 메시지가 생성될 수 있습니다.

```
Initiating online request
Generating key pair
Generating self-signed Certificate
Initiating online request
Received a response from the CA
Your certificate request was denied
```

이 오류 메시지가 표시되면 자세한 내용은 Microsoft CA 로그를 참조하거나 이러한 리소스를 참조

하십시오.

- [요청을 처리하는 인증 기관을 찾을 수 없습니다.](#)
- [XCCC: "인증서 요청이 거부되었습니다." 오류 메시지는 보안 회의를 위한 인증서를 요청할 때 발생합니다.](#)

[관련 정보](#)

- [IPSec 협상/IKE 프로토콜](#)
- [기술 지원 및 문서 - Cisco Systems](#)