AnyConnect:신뢰할 수 있는 소스로 자체 서명 인증서 설치

목표

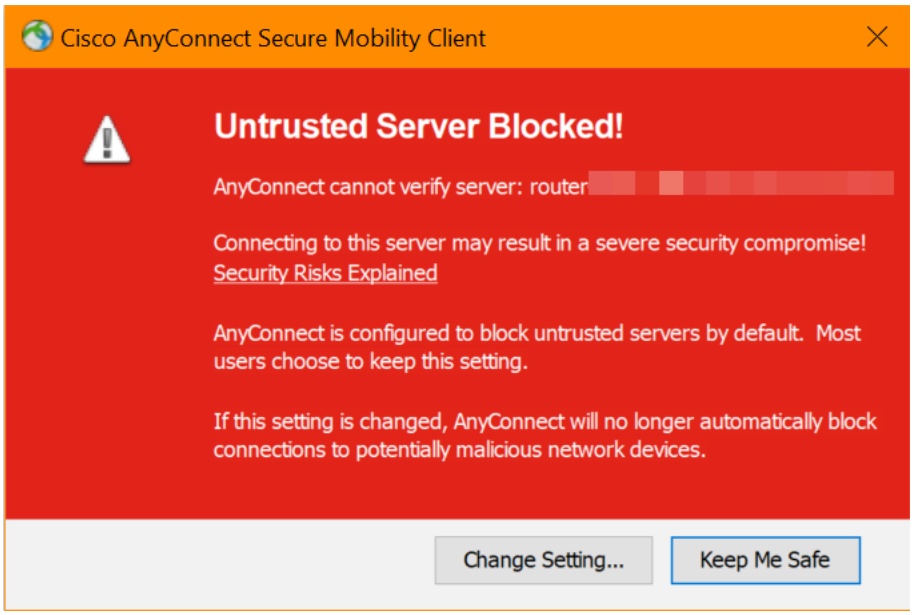
이 문서의 목적은 Windows 컴퓨터에 신뢰할 수 있는 원본으로 자체 서명된 인증서를 만들고 설치하는 과정을 안내하는 것입니다.그러면 AnyConnect에서 "신뢰할 수 없는 서버" 경고가 사라집니다.

소개

Cisco AnyConnect VPN(Virtual Private Network) Mobility Client는 원격 사용자에게 보안 VPN 연결을 제공합니다.Cisco SSL(Secure Sockets Layer) VPN 클라이언트의 이점을 제공하며 브라우저 기반 SSL VPN 연결에서 사용할 수 없는 애플리케이션 및 기능을 지원합니다.원격 근무자가 일반적으로 사용하는 AnyConnect VPN을 사용하면 직원이 사무실에 물리적으로 있는 것처럼, 그렇지 않은 경우에도 회사 네트워크 인프라에 연결할 수 있습니다.이를 통해 직원들의 유연성, 이동성 및 생산성이 향상됩니다.

인증서는 통신 프로세스에서 중요하며 개인 또는 장치의 ID를 확인하거나 서비스를 인증하거나 파일을 암호화하는 데 사용됩니다.자체 서명 인증서는 자체 작성자가 서명한 SSL 인증서입니다.

AnyConnect VPN Mobility Client에 처음 연결할 때 아래 이미지에 표시된 것처럼 사용자에게 "Untrusted Server(신뢰할 수 없는 서버)" 경고가 발생할 수 있습니다.



이 문제를 해결하려면 이 문서의 단계에 따라 Windows 시스템에 신뢰할 수 있는 원본으로 자체 서명된 인증서를 설치하십시오.

내보낸 인증서를 적용할 때 AnyConnect가 설치된 클라이언트 PC에 저장되어야 합니다.

AnyConnect 소프트웨어 버전

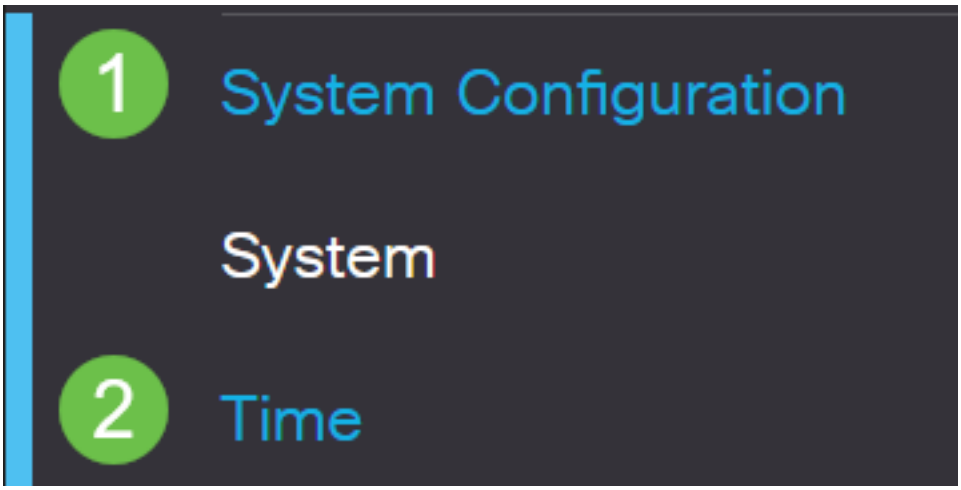
- AnyConnect - v4.9.x(최신 다운로드)

확인 시간 설정

사전 요구 사항으로 표준 시간대 및 일광 절약 시간 설정을 포함하여 라우터에 올바른 시간 집합이 있는지 확인해야 합니다.

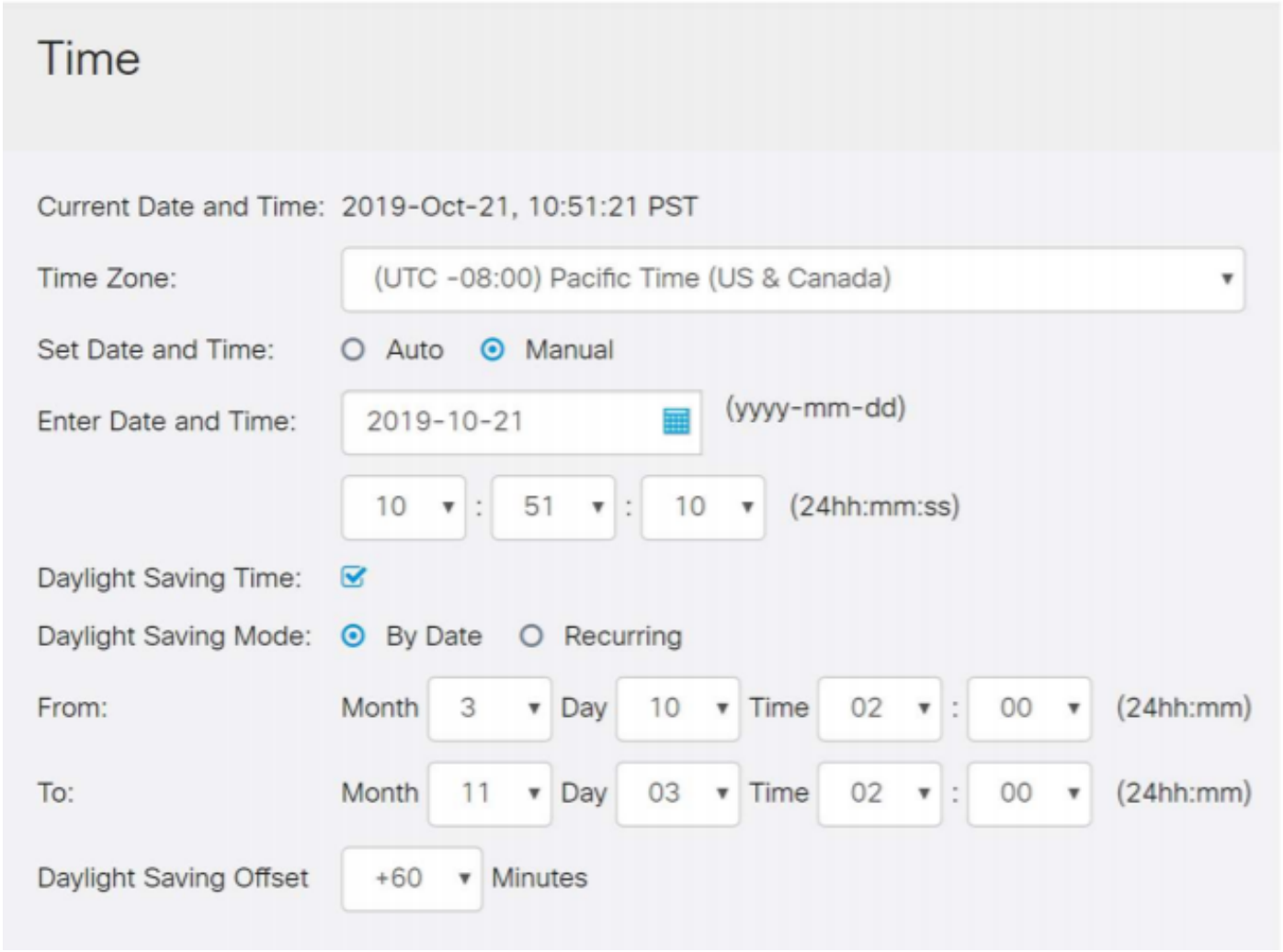
1단계

System Configuration(**시스템 컨피그레이션) > Time(시간)으로 이동합니다**.



2단계

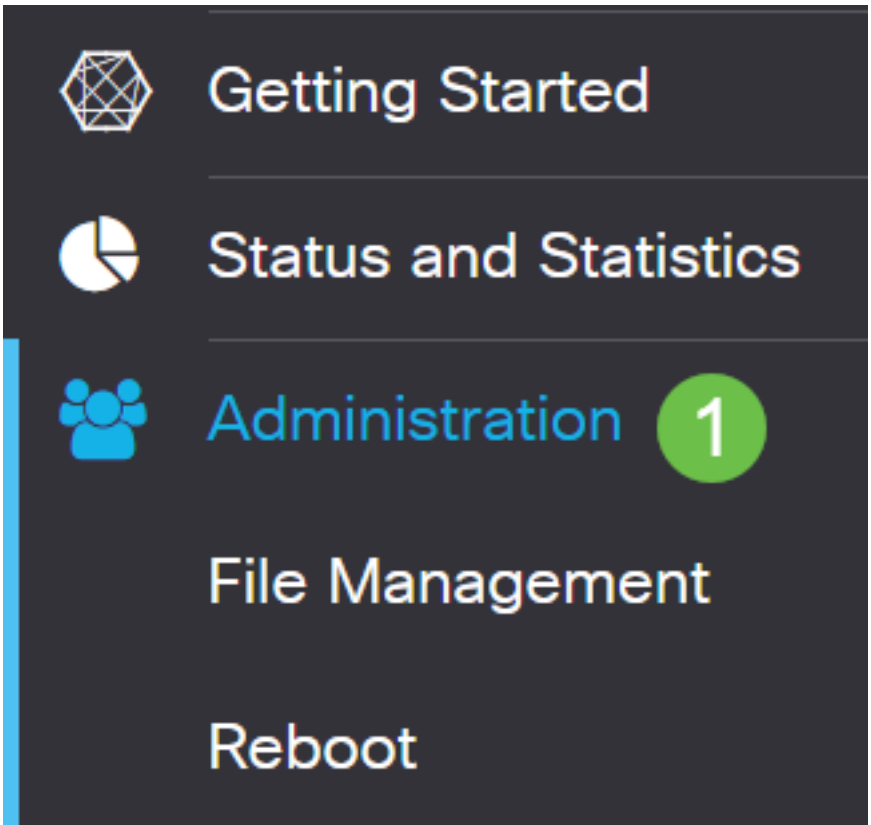
모든 것이 올바르게 설정되었는지 확인합니다.



자체 서명 인증서 생성

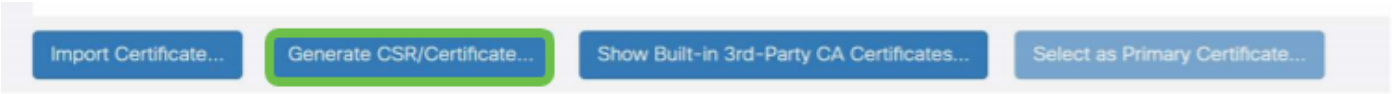
1단계

RV34x 시리즈 라우터에 로그인하고 Administration(관리) **> Certificate(인증서)로 이동합니다**.



2단계

Generate CSR/**Certificate(CSR/인증서 생성)를 클릭합니다**.

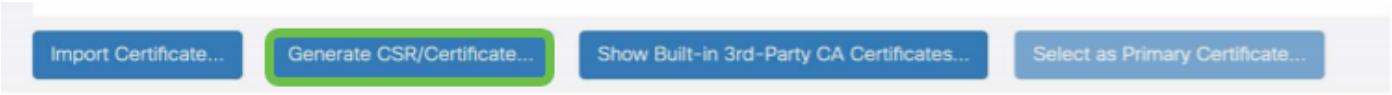


3단계

다음 정보를 입력합니다.

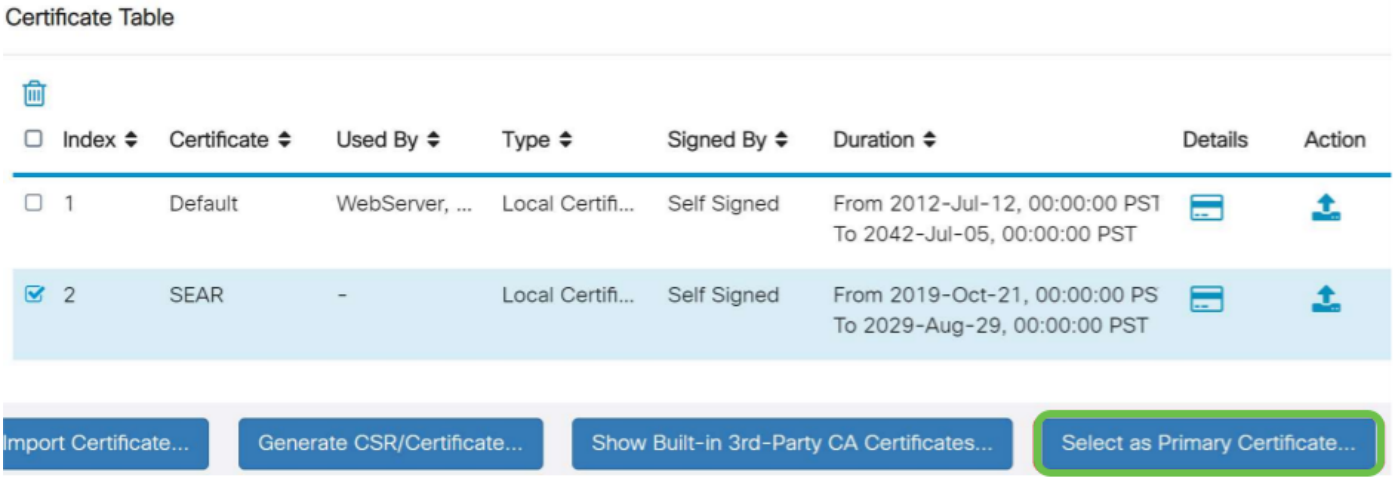
- 유형:자체 서명 인증서
- 인증서 이름:(선택한 모든 이름)
- 주체 대체 이름:WAN 포트에서 IP 주소를 사용할 경우 상자 아래**의 IP 주소**를 선택하거나 FQDN(Fully Qualified Domain Name)을 사용할 경우 **FQDN**을 선택합니다.상자에 WAN 포트의 IP 주소 또는 FQDN을 입력합니다.
- 국가 이름(C):장치가 있는 국가 선택
- 시/도 이름(ST):디바이스가 있는 시/도를 선택합니다.
- 지역 이름(L):(선택 사항) 디바이스가 있는 Locality를 선택합니다.도시, 도시 등이 될 수 있습니다.
- 조직 이름(O):(선택 사항)
- 조직 단위 이름(OU):회사 이름
- 일반 이름(CN):이는 주체 대체 이름으로 설정된 것과 일치해야 합니다.
- 이메일 주소(E):(선택 사항)
- 키 암호화 길이:2048
- 유효한 기간:인증서가 유효한 기간입니다.기본값은 360일입니다.최대 10,950일 또는 30년까지 원하는 값으로 조정할 수 있습니다.

Generate(생성)를 **클릭합니다**.



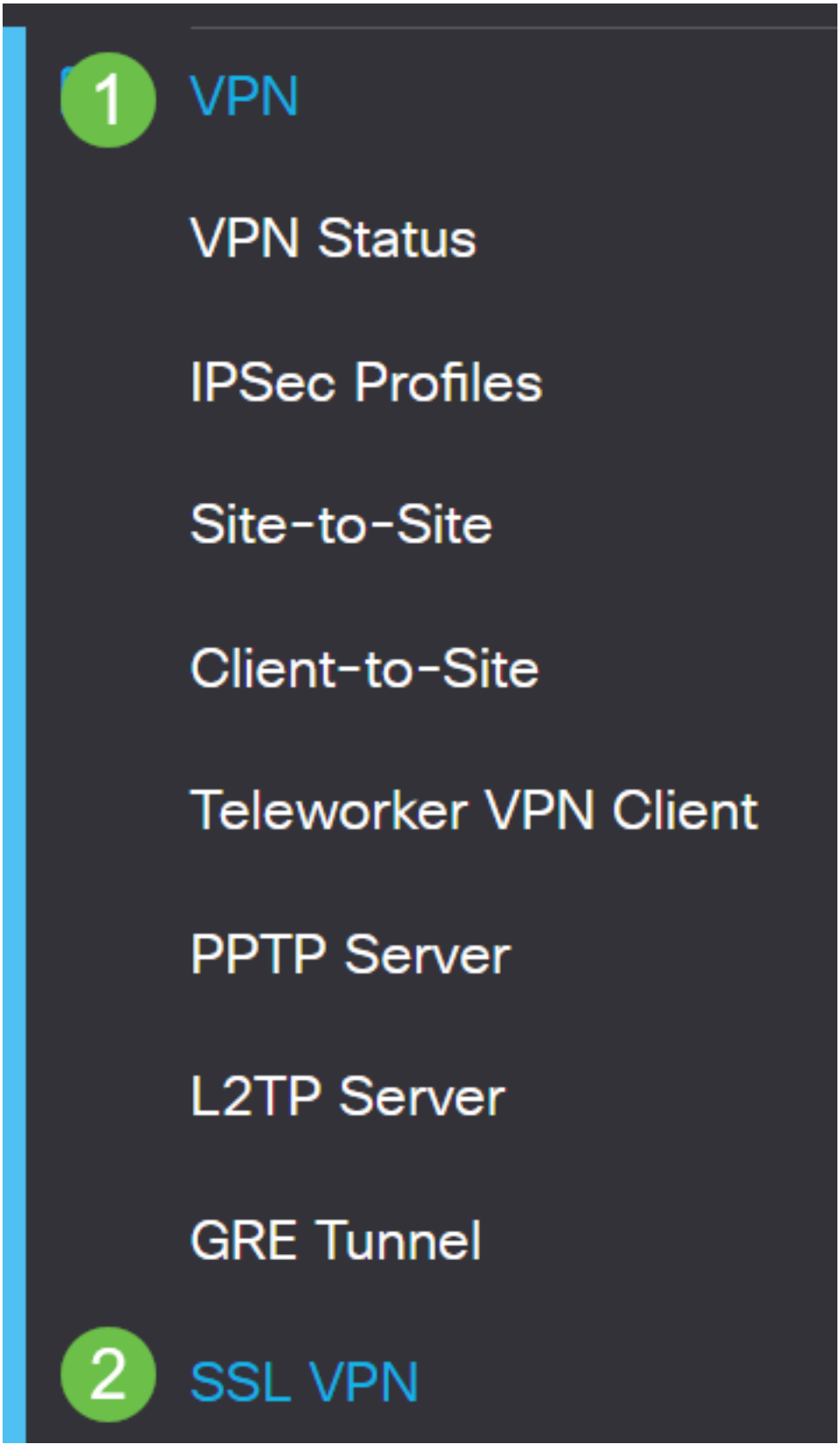
4단계

방금 생성한 인증서를 선택하고 Select as Primary **Certificate를** 클릭합니다**.**



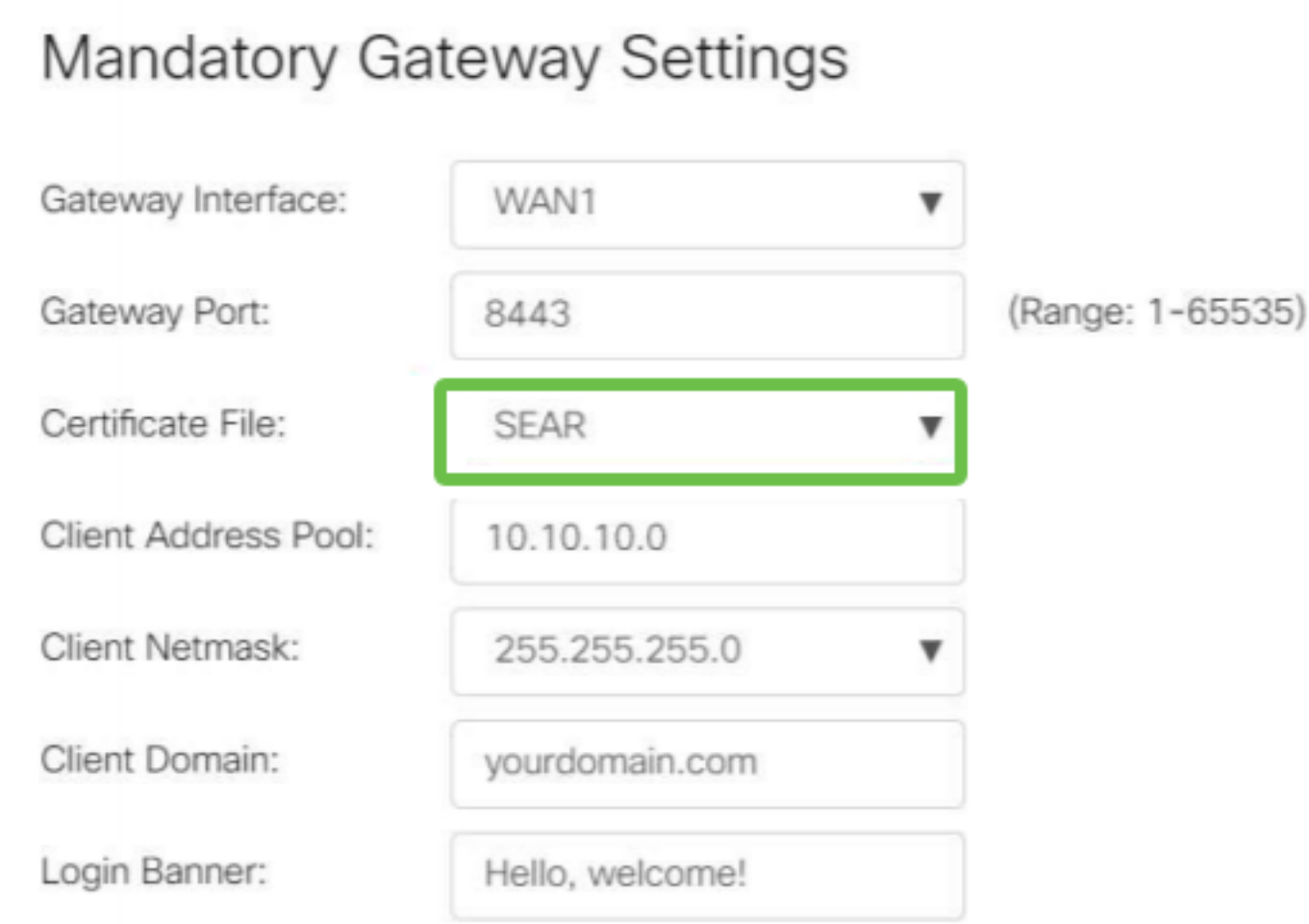
5단계

웹 사용자 인터페이스(UI)를 새로 고칩니다. 새 인증서이므로 다시 로그인해야 합니다 .로그인했으면 **VPN > SSL VPN으로 이동합니다**.



6단계

인증서 **파일**을 새로 만든 인증서로 변경합니다.



7단계

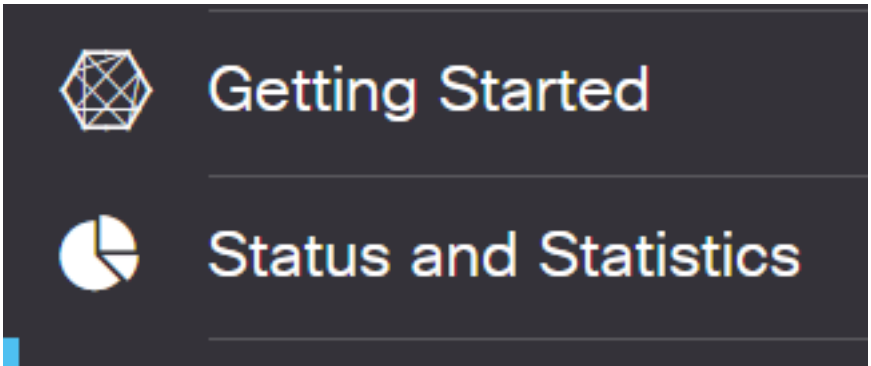
Apply를 **클릭합니다**.

자체 서명 인증서 설치

Windows 시스템에 신뢰할 수 있는 소스로 자체 서명된 인증서를 설치하려면 AnyConnect에서 "신뢰할 수 없는 서버" 경고를 제거하려면 다음 단계를 수행합니다.

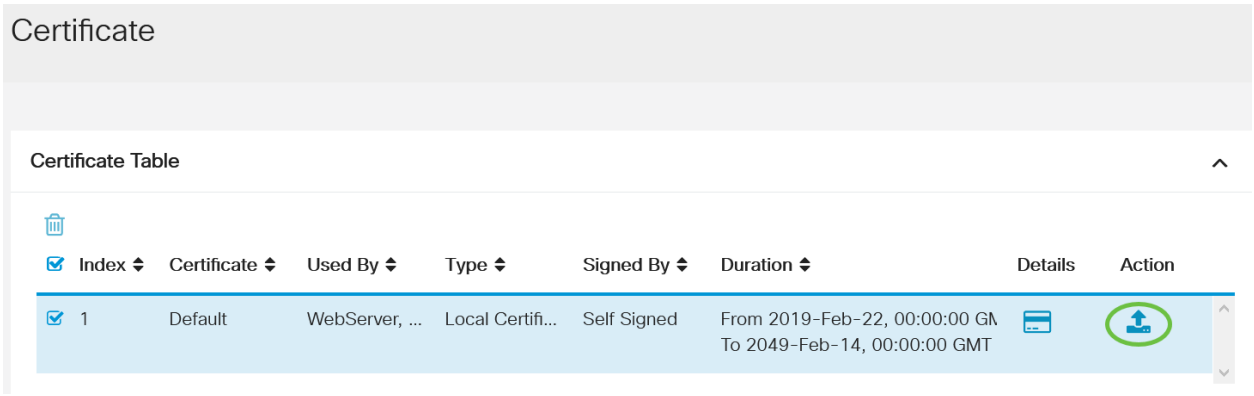
1단계

RV34x 시리즈 라우터에 로그인하고 Administration(관리) **> Certificate(인증서)로 이동합니다**.



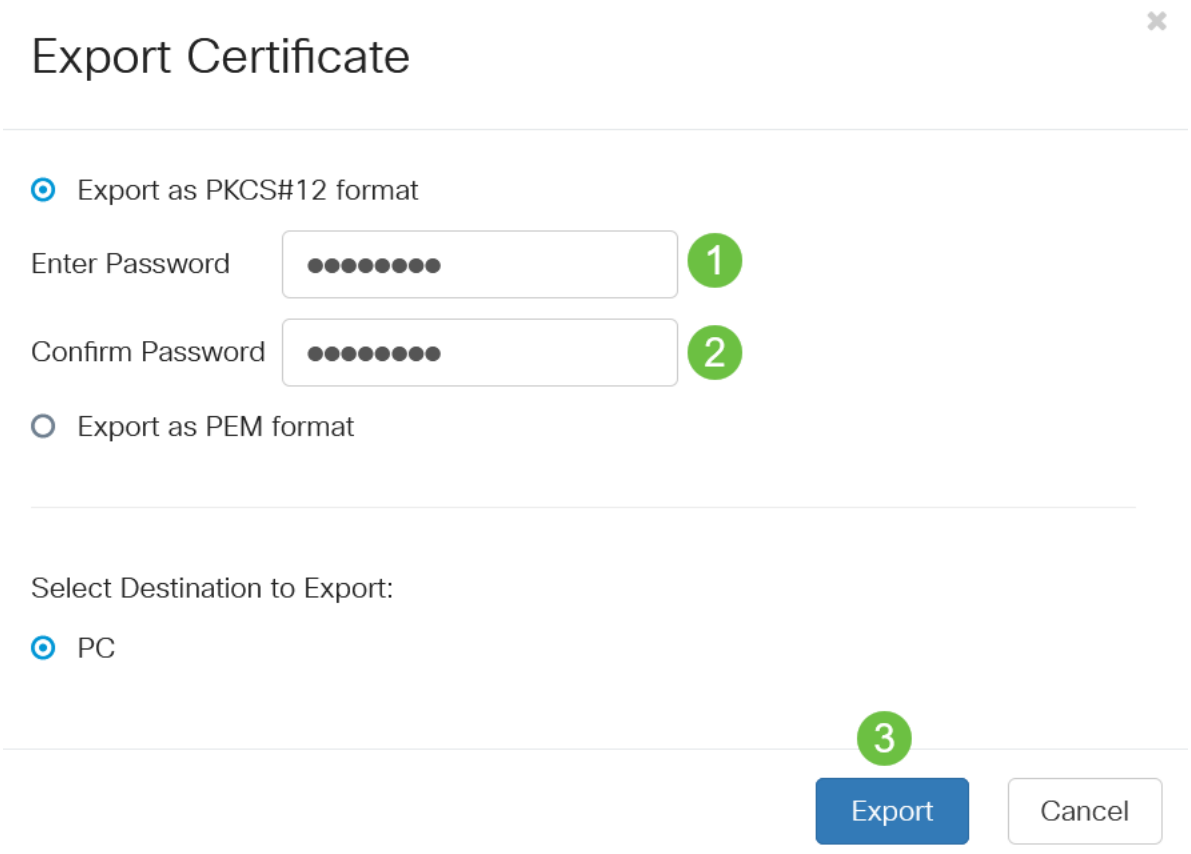
2단계

기본 자체 서명 인증서를 선택하고 Export(내보내기) 버튼을 클릭하여 인증서를 다운로드합니다.



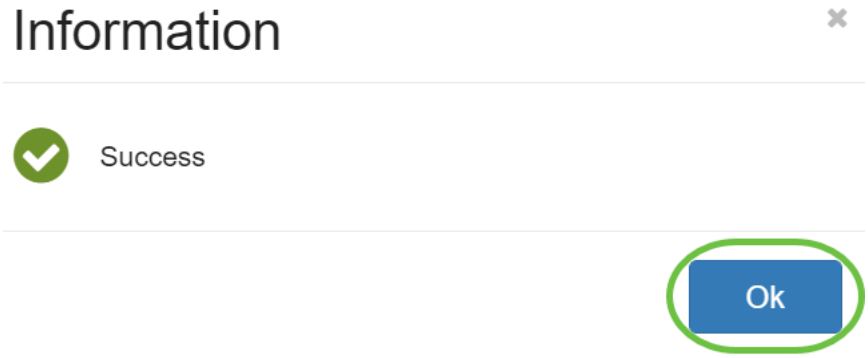
3단계

Export *Certificate(인증서 내보내기)* 창에서 인증서 비밀번호를 입력합니다.Confirm Password(비밀번호 확인) 필드에 비밀번호*를 다시* 입력한 다음 Export(내보내기)를 **클릭합니다.**



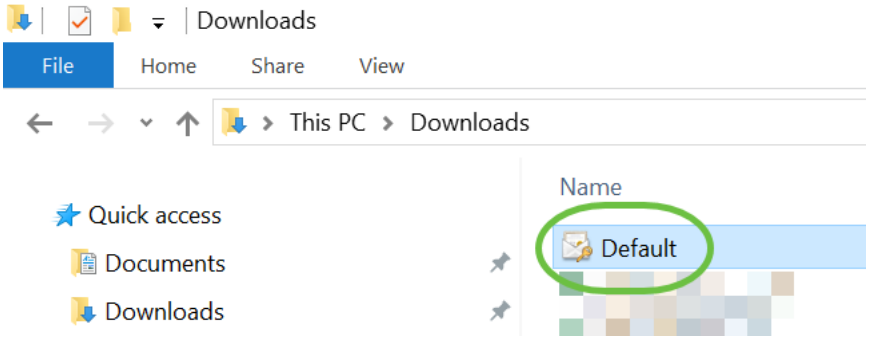
4단계

인증서가 성공적으로 다운로드되었음을 알리는 팝업 창이 표시됩니다.**확인**을 **클릭합니다**.



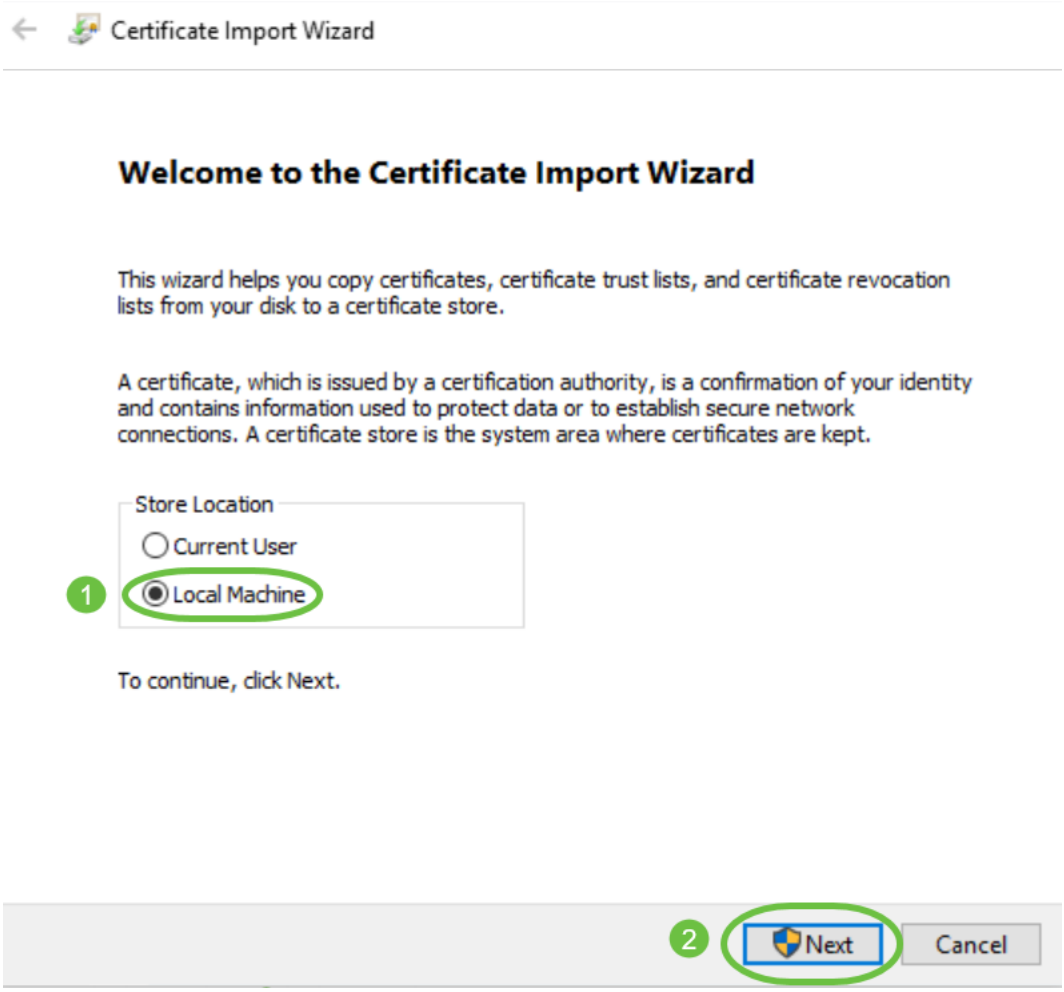
5단계

인증서가 PC에 다운로드되면 파일을 찾아 두 번 클릭합니다.



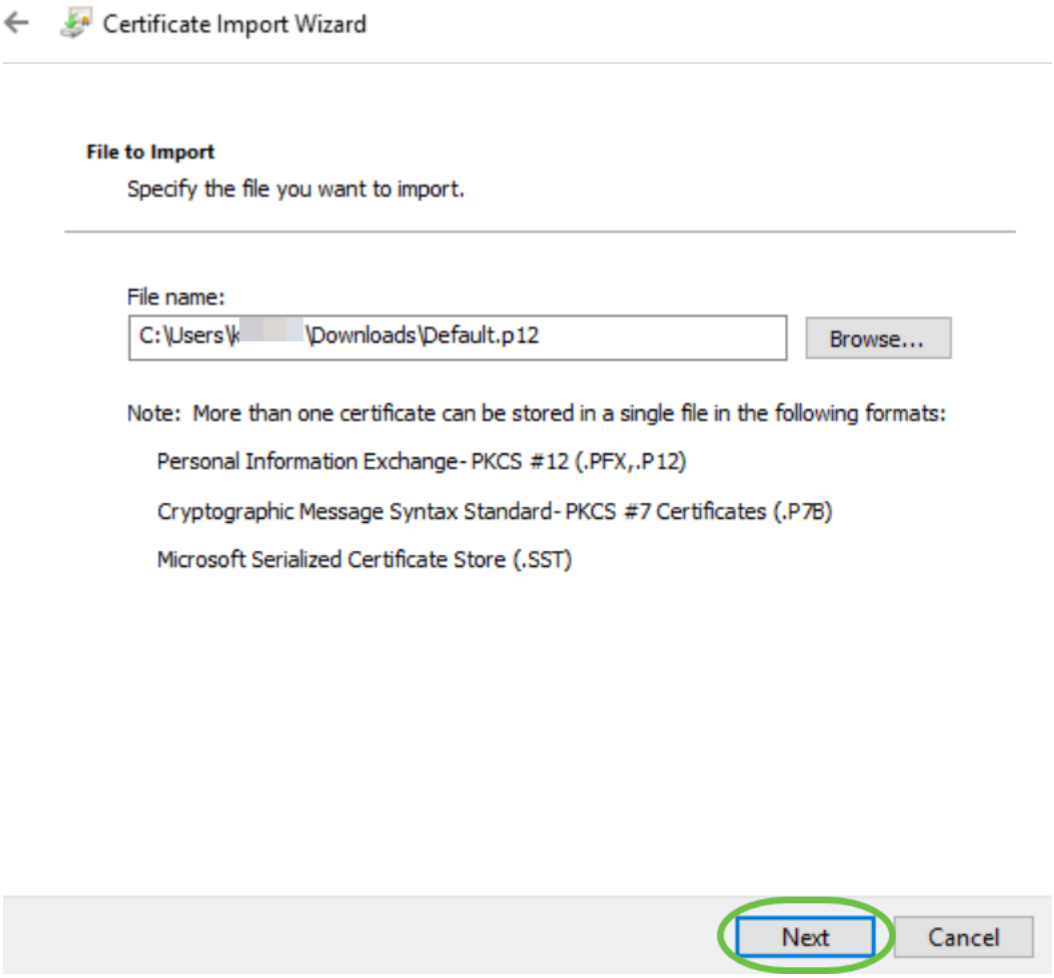
6단계

Certificate *Import Wizard* 창이 나타납니다.Store Location(*저장소 위치*)에서 Local Machine(**로컬 머신)을 선택합니다**.Next(**다음)를 클릭합니다**.



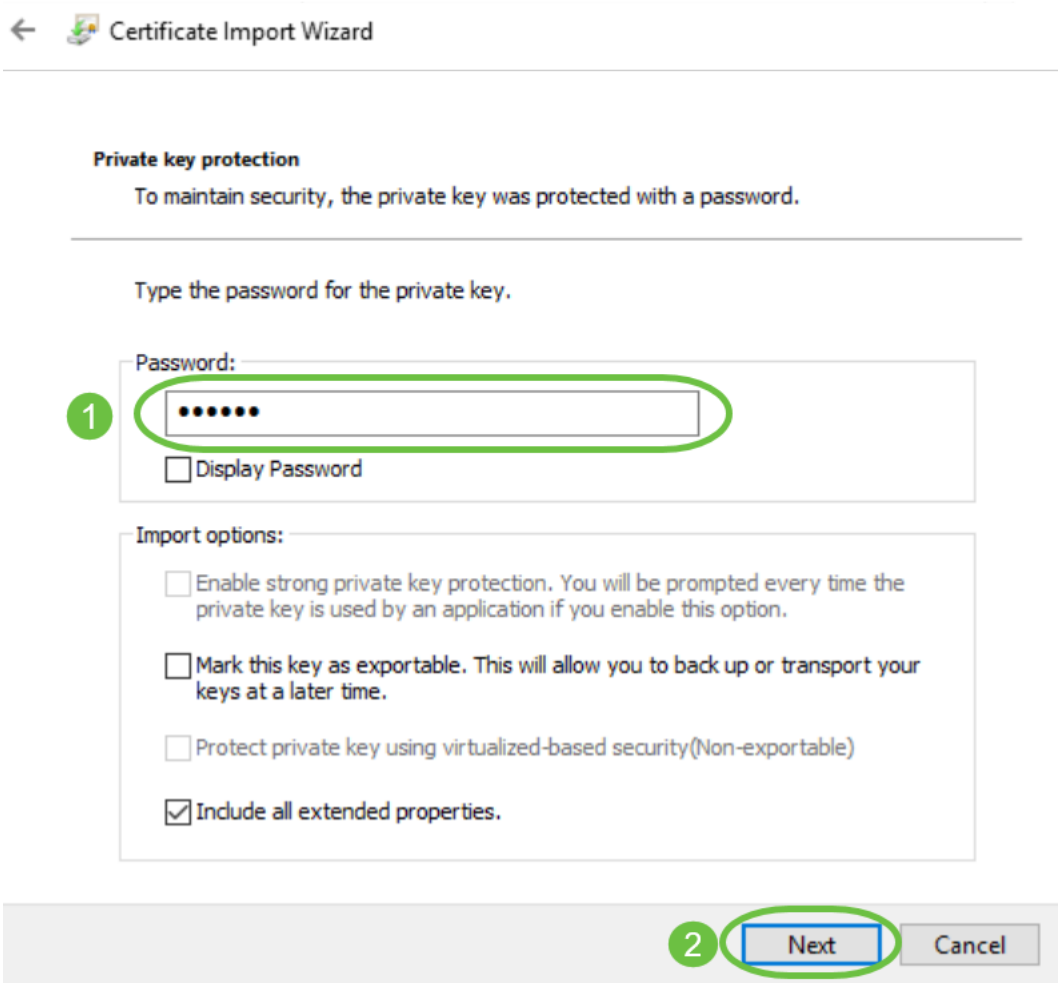
7단계

다음 화면에 인증서 위치 및 정보가 표시됩니다.Next(**다음)를 클릭합니다**.



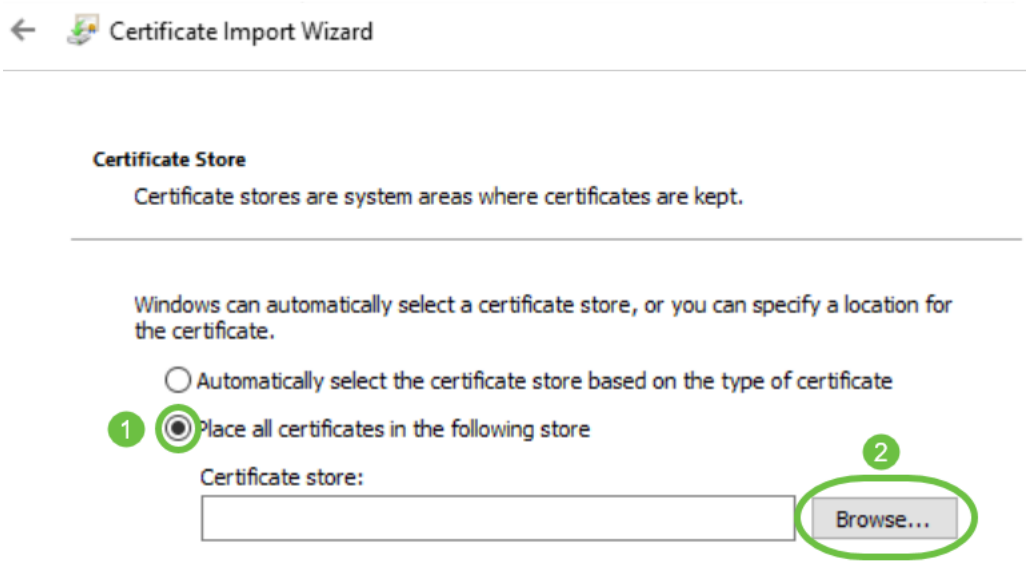
8단계

인증서에 대해 선택한 *비밀번호*를 입력하고 **Next**를 클릭합니다.



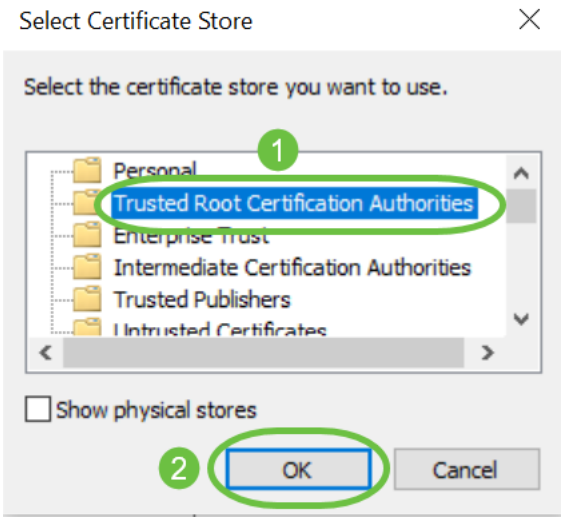
9단계

다음 화면에서 **Place all certificates in the following store(다음 저장소에 모든 인증서 배치)**를 선택한 다음 Browse(찾아보기)를 **클릭합니다**.



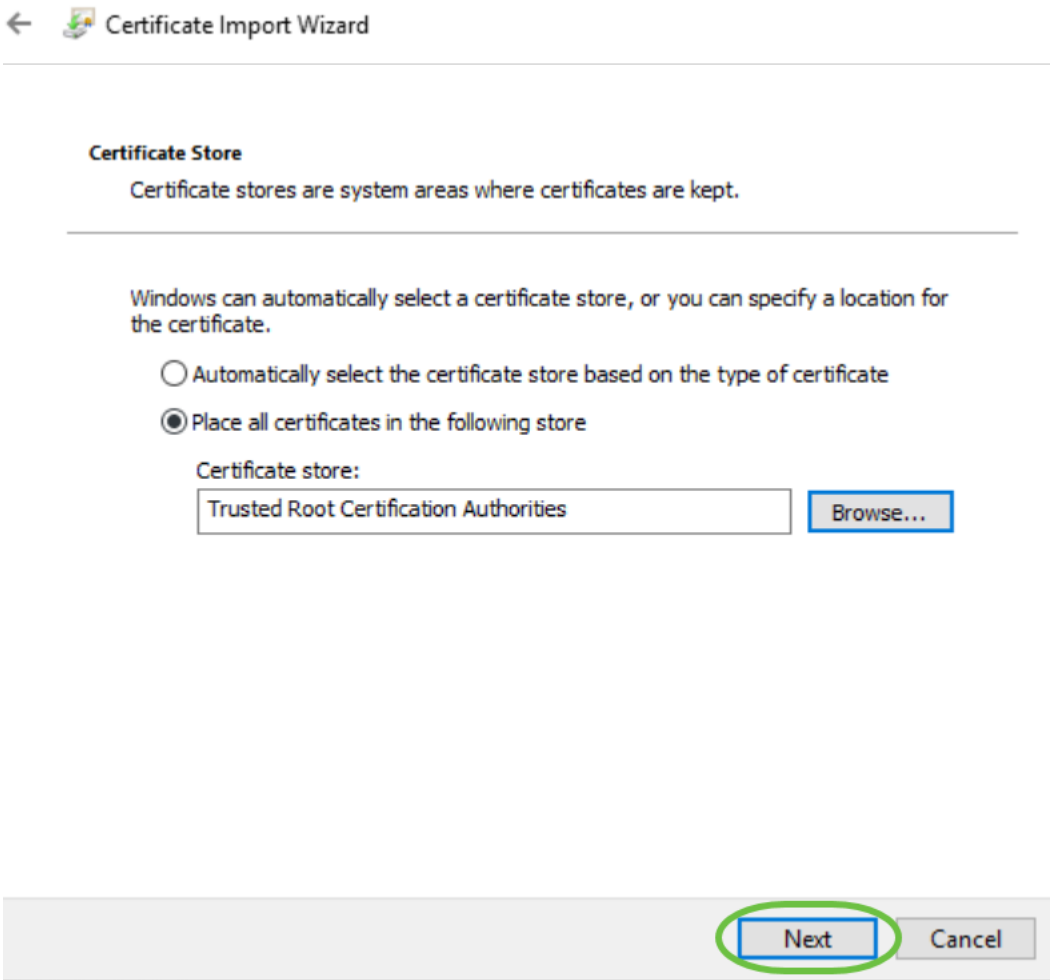
10단계

Trusted **Root Certification Authorities(신뢰할 수 있는 루트 인증 기관)**를 선택하고 **OK(확인)**를 클릭합니다.



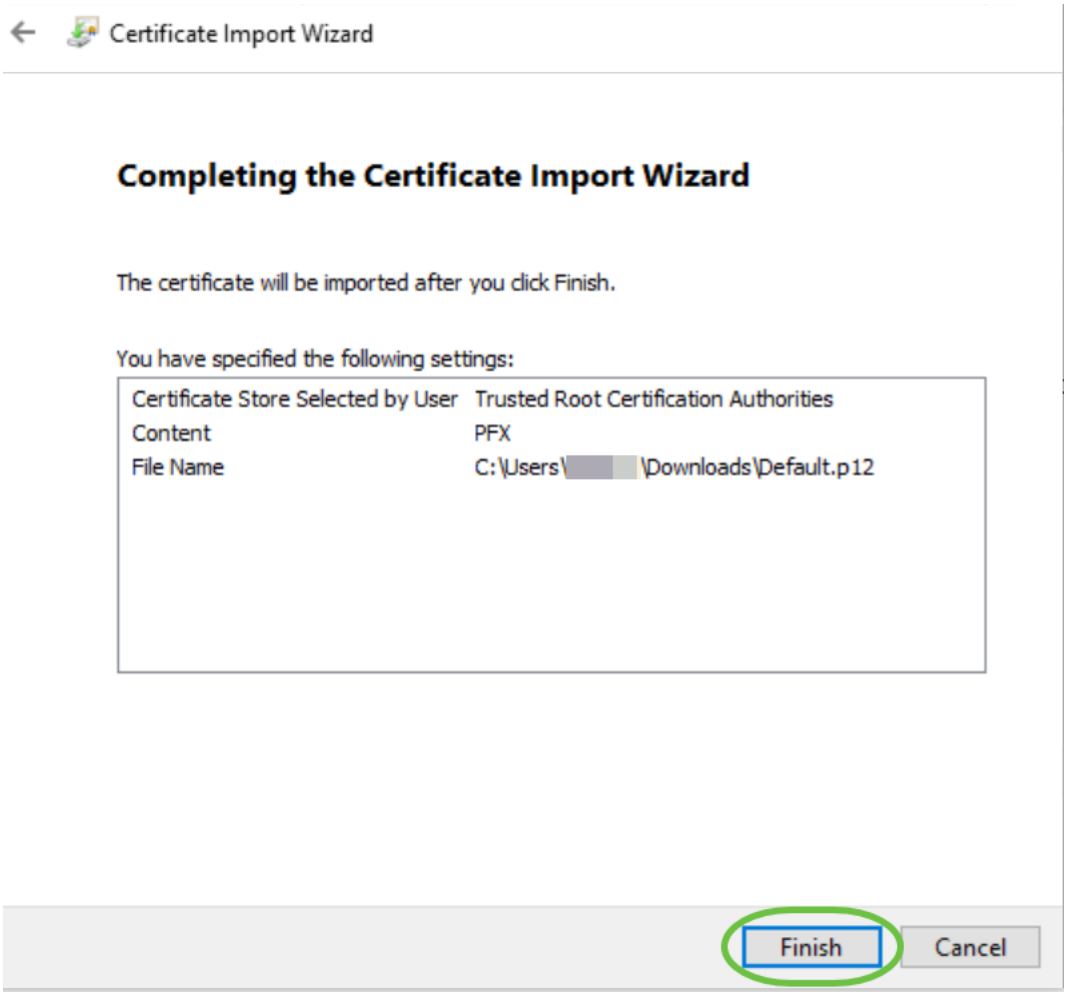
11단계

Next(**다음**)**를 클릭합니다**.



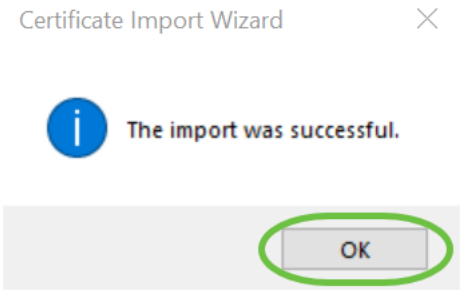
12단계

설정에 대한 요약이 표시됩니다.Finish(**마침**)를 클릭하여 인증서를 가져옵니다.



13단계

인증서를 성공적으로 가져왔다는 확인 메시지가 표시됩니다.**확인**을 **클릭합니다**.



14단계

Cisco AnyConnect를 열고 다시 연결해 보십시오.신뢰할 수 없는 서버 경고가 더 이상 표시되지 않아야 합니다.

결론

여기 있습니다!이제 AnyConnect에서 "Untrusted Server(신뢰할 수 없는 서버)" 경고를 제거하기 위해 Windows 시스템에 신뢰할 수 있는 소스로 자체 서명된 인증서를 설치하는 단계를 성공적으로 학습했습니다.

추가 리소스

기본 문제 해결 AnyConnect 관리자 가이드 릴리스 4.9 AnyConnect 릴리스 노트 - 4.9 Cisco Business VPN 개요 및 모범 사례