RV32x Series 라우터 인증서 업로드에 대한 해결 방법

요약

디지털 인증서는 인증서의 명명된 주체에 의해 공개 키의 소유권을 인증합니다.이렇게 하면 신뢰 당사자가 인증된 공개 키에 해당하는 개인 키가 만든 서명 또는 어설션에 의존할 수 있습니다.라우터는 네트워크 관리자가 생성한 인증서인 자체 서명 인증서를 생성할 수 있습니다 .또한 디지털 ID 인증서를 신청하기 위해 CA(Certificate Authority)에 요청을 보낼 수 있습니다 .타사 애플리케이션의 합법적인 인증서를 보유하는 것이 중요합니다.

CA가 인증서에 서명하는 방법에는 두 가지가 있습니다.

1. CA는 개인 키를 사용하여 인증서에 서명합니다.

2. RV320/RV325에서 생성된 CSR을 사용하여 인증서에 서명하는 경우

RV320 및 RV325는 .pem 형식 인증서만 지원합니다.두 경우 모두 인증 기관에서 .pem 형식 인증서를 받아야 합니다.다른 형식 인증서를 가져올 경우 직접 형식을 변환하거나 CA에서 .pem 형식 인증서를 다시 요청해야 합니다.

대부분의 상용 인증서 공급업체는 중간 인증서를 사용합니다. 중간 인증서는 신뢰할 수 있는 루트 CA에서 발급되므로 중간 인증서에서 발급한 모든 인증서는 신뢰할 수 있는 루트의 트러스트를 상속합니다. 이는 신뢰 인증 체인과 같습니다.

이 설명서에서는 RV320/RV325에서 Intermediate Certificate Authority에서 발급한 인증서를 가져오는 방법에 대해 설명합니다.

식별된 날짜

2017년 2월 24일

해결된 날짜

해당 없음

영향을 받는 제품

RV320/RV325	1.1.1.06 이상

개인 키를 사용하여 인증서 서명

이 예에서는 서드파티 중간 CA에서 RV320.pem을 가져온 것으로 가정합니다.파일에 다음과 같은 내용이 있습니다.개인 키, 인증서, 루트 CA 인증서, 중간 CA 인증서

참고:하나의 파일 대신 중간 CA에서 여러 파일을 가져오는 것은 선택 사항입니다.하지만 여러 파일에서 4개 이상의 부분을 찾을 수 있습니다.

CA 인증서 파일에 루트 CA 인증서와 중간 인증서가 모두 포함되어 있는지 확인합니다 .RV320/RV325에는 중간 인증서 및 루트 인증서가 CA 번들, 루트 인증서, 중간 인증서 순으로 필요합니다.둘째, RV320/RV325 인증서와 개인 키를 하나의 파일로 결합해야 합니다.

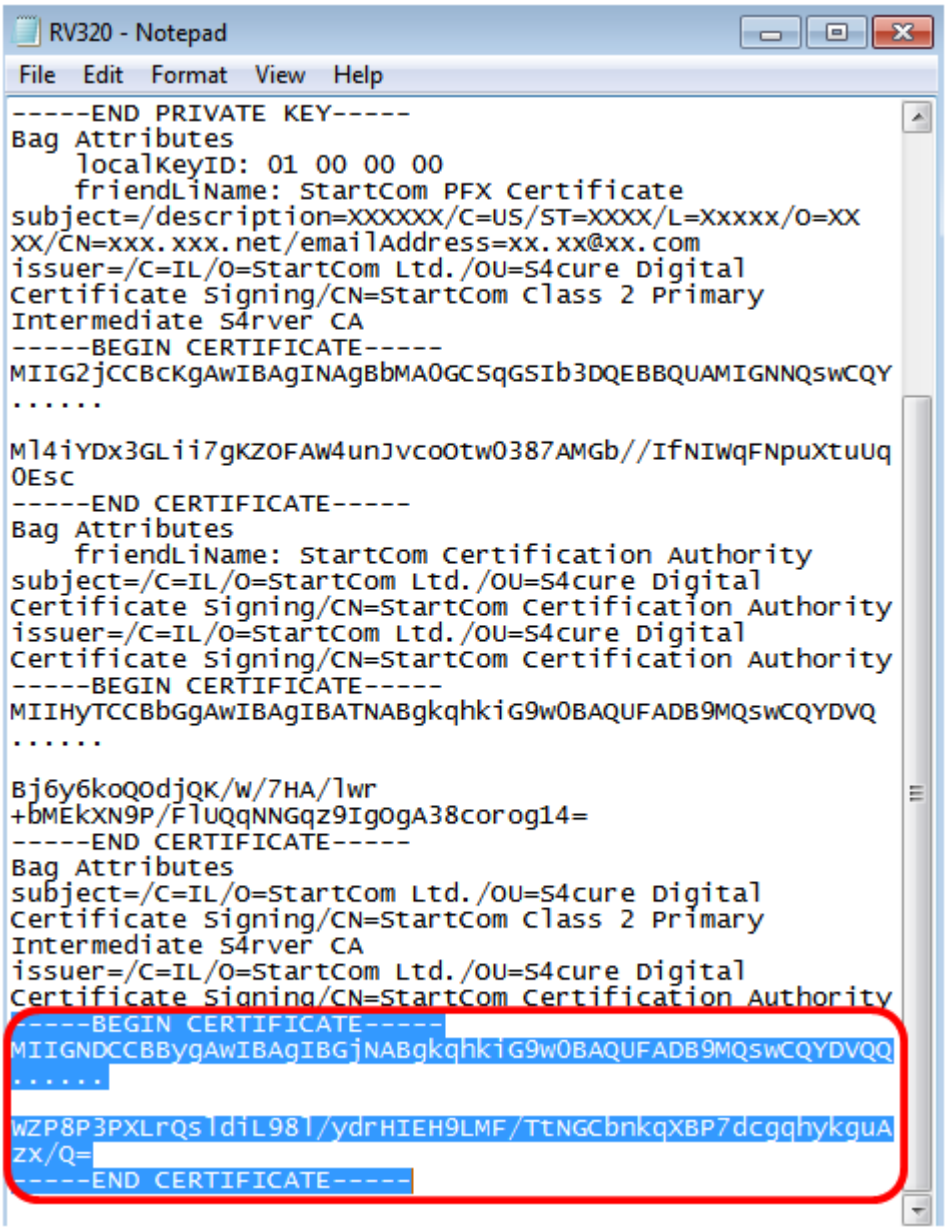
참고:모든 텍스트 편집기를 사용하여 파일을 열고 편집할 수 있습니다.빈 줄, 공백 또는 캐리지 리턴을 추가해도 계획이 예상대로 진행되지 않도록 해야 합니다.

인증서 결합

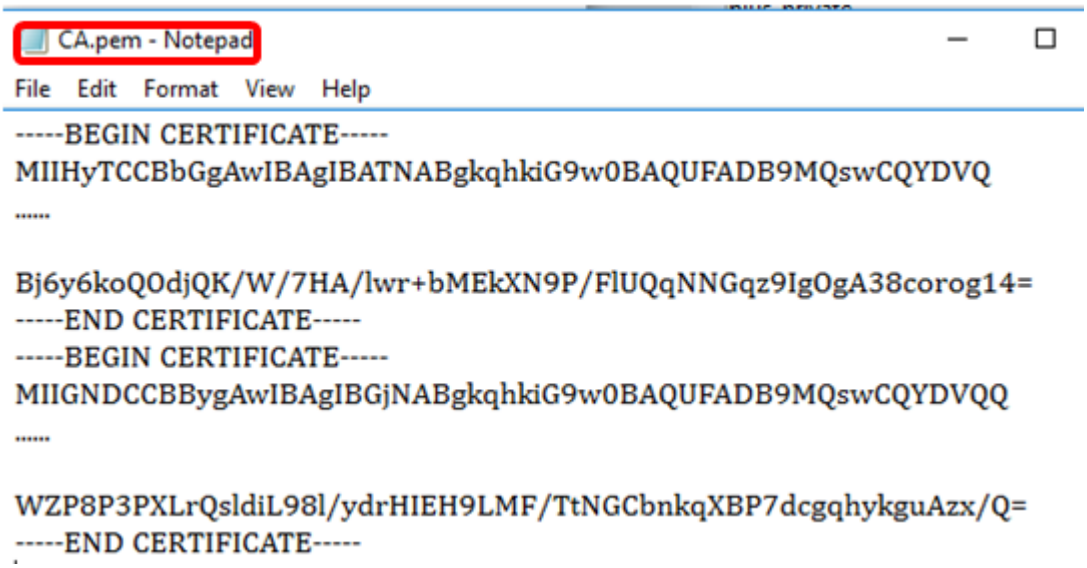
1단계. RV320.pem을 열고 두 번째 인증서(루트 인증서) 및 시작/종료 메시지를 포함한 세 번째 인증서(중간 인증서)를 복사합니다.

참고:이 예에서는 텍스트의 강조 표시 문자열이 루트 인증서입니다.

참고:이 예에서는 강조 표시된 텍스트 문자열이 중간 인증서입니다.

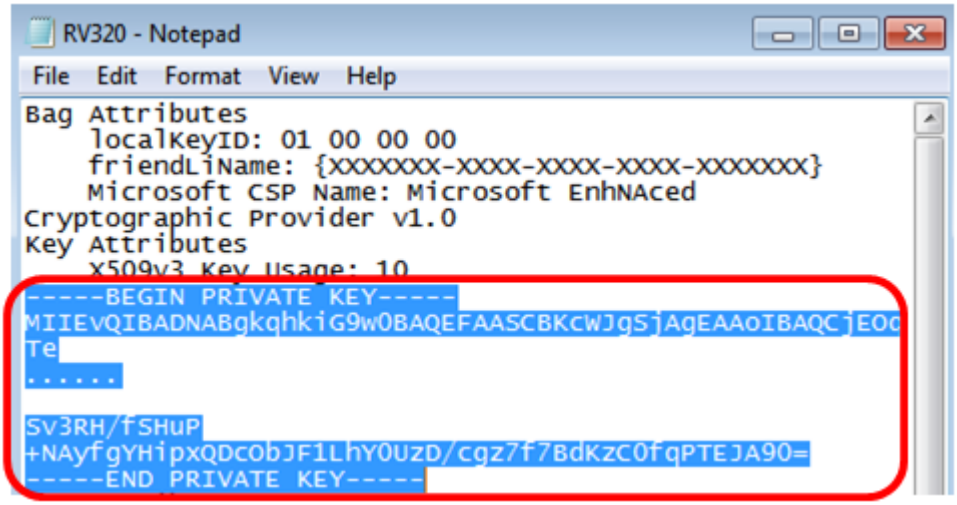


2단계. 새 파일에 내용을 붙여넣고 CA.pem으로 저장합니다.

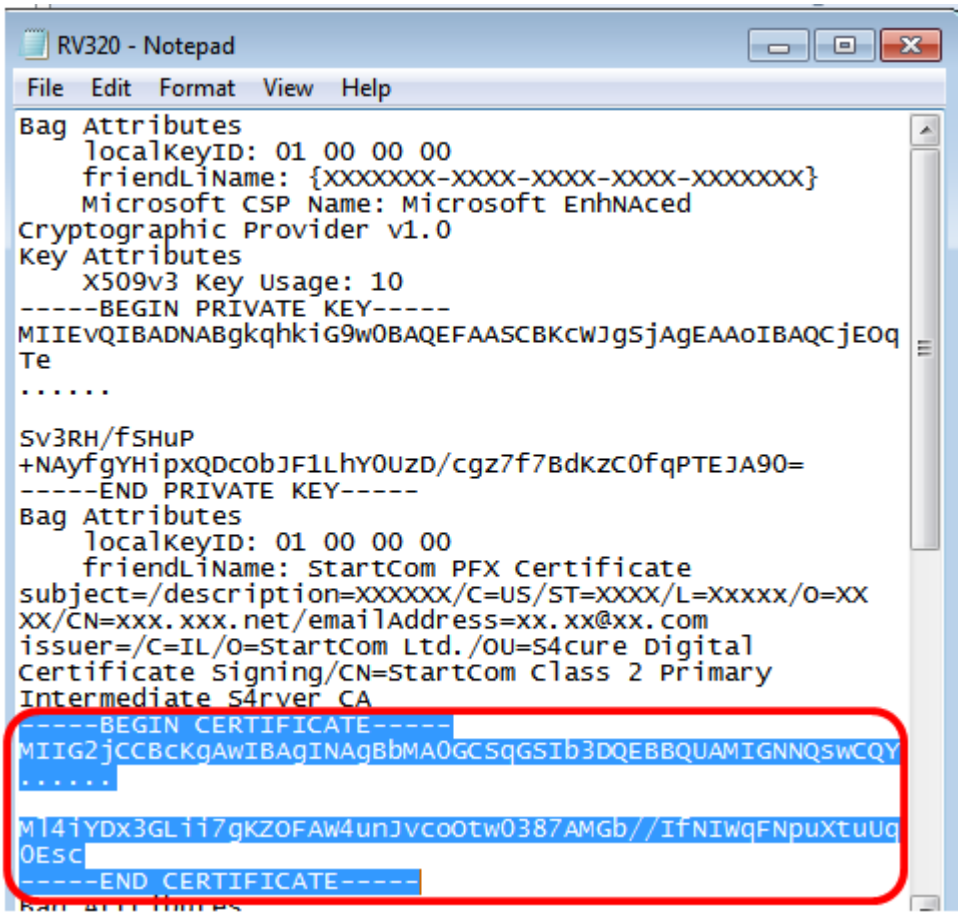


3단계. RV320.pem을 열고 시작/종료 메시지를 포함한 첫 번째 인증서와 개인 키 섹션을 복사합니다.

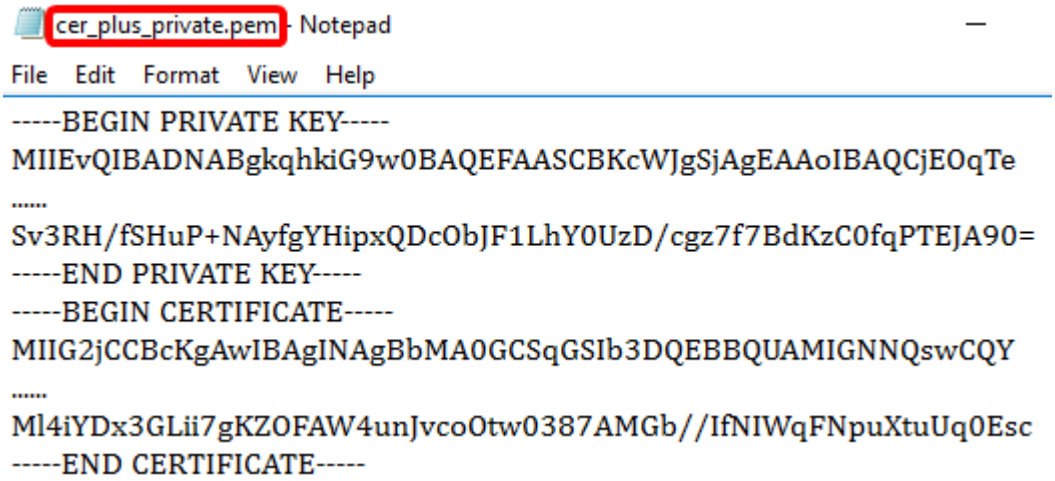
참고:아래 예에서는 강조 표시된 텍스트 문자열이 개인 키 섹션입니다.



참고:아래 예에서는 강조 표시된 텍스트 문자열이 첫 번째 인증서입니다.



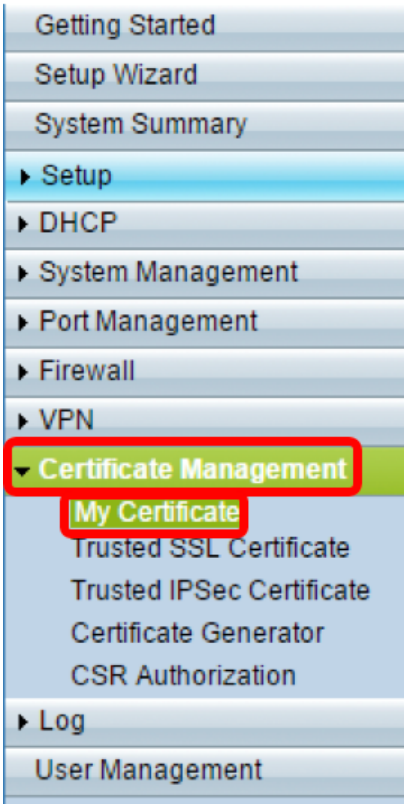
4단계. 새 파일에 내용을 붙여 넣고 cer_plus_private.pem으로 저장합니다.



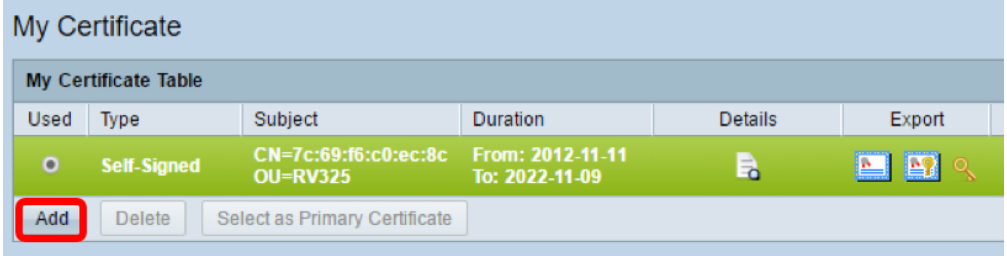
참고:RV320/RV325 펌웨어 버전이 1.1.1.06 미만이면 파일 끝에 두 개의 라인 피드(cer_plus_private.pem)가 있는지 확인합니다. 1.1.1.06 이후 펌웨어에서 라인 피드를 두 개 더 추가할 필요가 없습니다.이 예에서는 단축된 버전의 인증서가 데모용으로만 표시됩니다.

가져오기 CA.pem 및 cer_plus_private.pem RV320으로/RV325

1단계. RV320 또는 RV325의 웹 기반 유틸리티에 로그인하고 **Certificate Management(인증서 관리) > My Certificate(내 인증서)를** 선택합니다.



2단계. **Add**(추가)를 클릭하여 인증서를 가져옵니다.



3단계. *서드파티 인증* 라디오 버튼을 클릭하여 인증서를 가져옵니다.

4단계. Import Full *Certificate Set(전체 인증서 집합 가져오기*) 영역에서 라디오 버튼을 클릭하여 저장된 인증서의 소스를 선택합니다.옵션은 다음과 같습니다.

- *PC에서 가져오기* - 컴퓨터에 파일이 있는 경우 선택합니다.
- *USB에서 가져오기* - 플래시 드라이브에서 파일을 가져오려면 선택합니다.

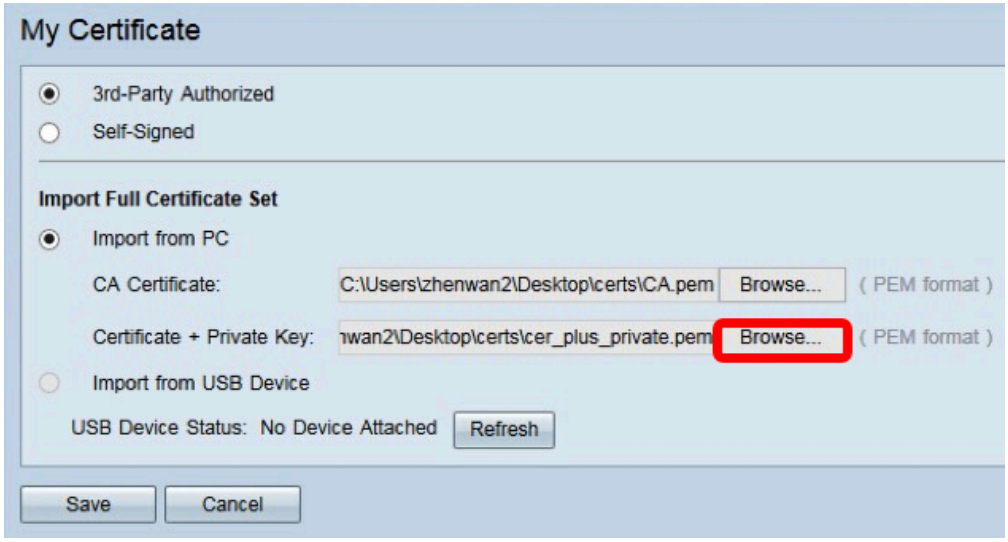
참고:이 예에서는 **PC에서 가져오기**를 선택합니다.

5단계. *CA Certificate*(*CA 인증서*) 영역**에서 Browse..**를 **클릭하고** CA.pem을 찾습니다.파일.

참고:1.1.0.6 이상의 펌웨어를 실행 중인 경우 선택 버튼을 클릭하고 필요한 파일을 찾습니다.

6단계. *Certificate + Private Key*(인증서 + *개인 키*) 영역**에서 Browse...를** 클릭하고 er_plus_private.pem 파일을 찾습니다.

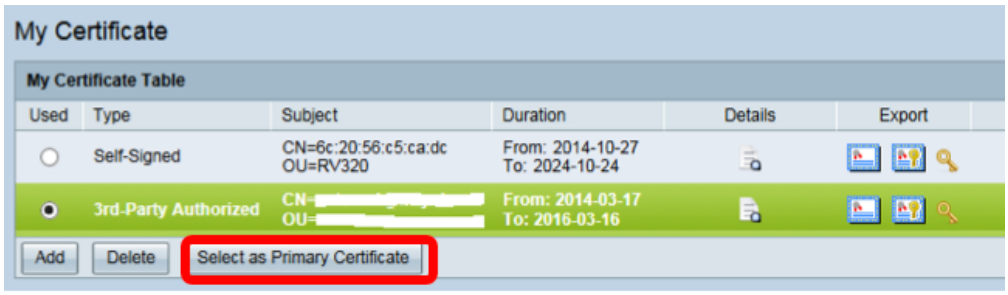
참고:1.1.0.6 이상의 펌웨어를 실행 중인 경우 선택 버튼을 클릭하고 필요한 파일을 찾습니다.



7단계. **저장**을 클릭합니다.

인증서를 가져왔습니다.이제 HTTPS 액세스, SSL VPN 또는 IPSec VPN에 사용할 수 있습니다.

8단계. (선택 사항) HTTPS 또는 SSL VPN에 인증서를 사용하려면 인증서의 라디오 버튼을 클릭하고 **Select as Primary Certificate** 버튼을 클릭합니다.

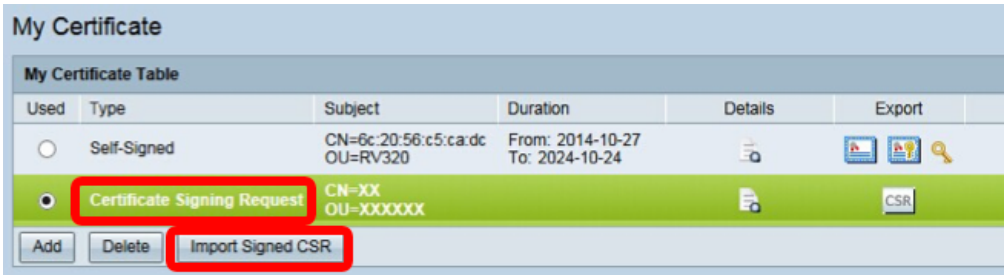


이제 인증서를 성공적으로 가져와야 합니다.

CSR을 사용한 인증서 서명

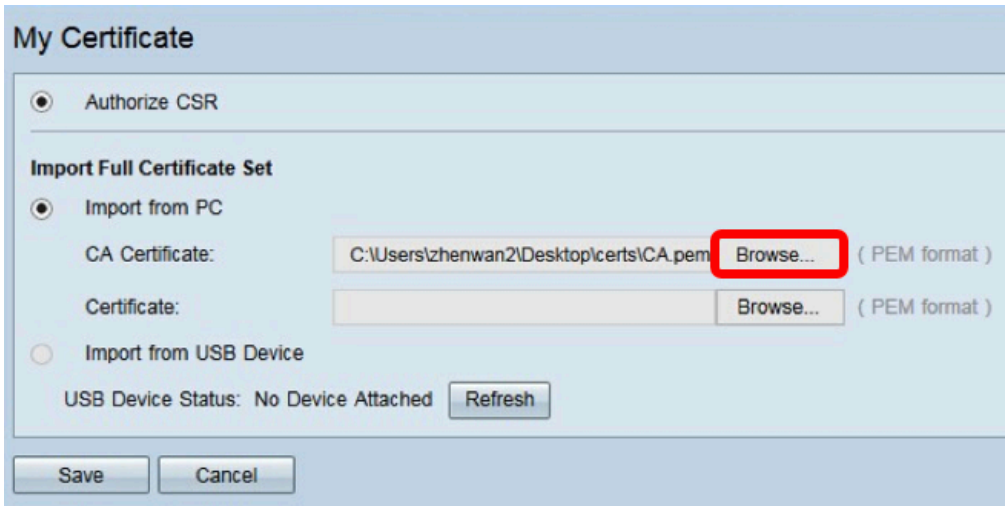
1단계. RV320/RV325에서 CSR(Certificate Signing Request)을 생성합니다. CSR을 생성하는 방법을 알아보려면 여기를 클릭하십시오.

2단계. 인증서를 가져오려면 Certificate **Signing Request(인증서 서명 요청)를** 선택하고 Import Signed CSR(**서명된 CSR 가져오기**)을 **클릭합니다**.

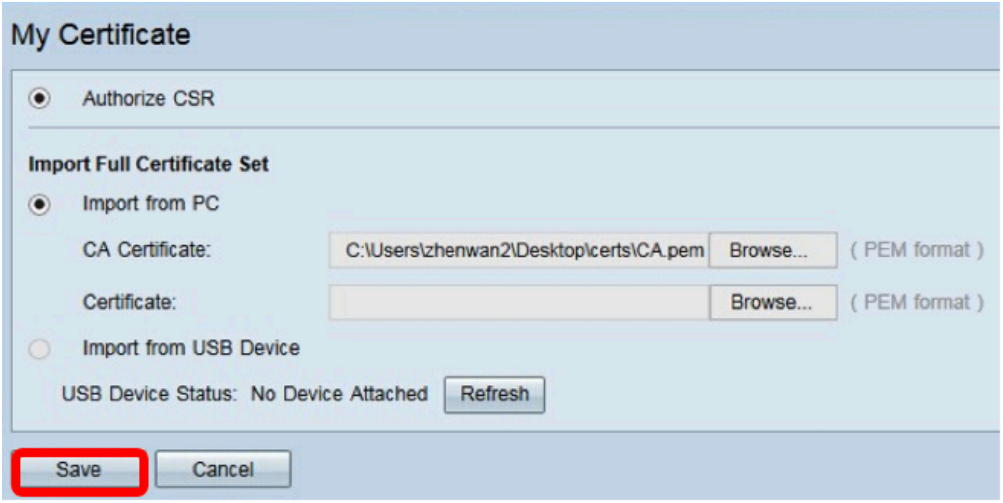


3단계. **Browse...를** 클릭하고 CA 인증서 파일을 선택합니다.여기에는 루트 CA + 중간 CA 인증서가 포함됩니다.

참고:이 예에서는 CSR을 사용하여 인증서가 생성되므로 개인 키가 필요하지 않습니다.



4단계. **저장**을 클릭합니다.



이제 CSR을 사용하여 인증서를 성공적으로 업로드해야 합니다.

부록:

RV320.pem의 내용

백 속성

로컬 키 ID:+ 01 00 00 00

친구 이름:{{XXXXXXX-XXXX-XXXX-XXXX-XXXXXXX}}

Microsoft CSP 이름:Microsoft EnhNAced 암호화 공급자 v1.0

키 특성

X509v3 키 사용:10

—개인 키 시작—

MIIEvQIBADNABgkqhkiG9w0BAQEFAASCBKcWJgSjAgEAAoIBAQCjEOqTe

.....

Sv3RH/fSHuP+NAyfgYHipxQDcObJF1LhY0UzD/cgz7f7BdKzC0fqPTEJA90=

—개인 키 종료—

백 속성

로컬 키 ID:+ 01 00 00 00

친구 이름:StartCom PFX 인증서

subject=/description=XXXXXX/C=US/ST=XXXX/L=Xxxxx/O=XX XX/CN=xxx.xxx.net/emailAddress=xx.xx@xx.com

issuer=/C=IL/O=StartCom Ltd./OU=S4Cure 디지털 인증서 서명/CN=StartCom Class 2 기본 중간 S4서버 CA

—인증서 시작—

MIIG2jCCBcKgAwIBAgInaBbMA0GCSqGSIb3DQEBBQUAMIGNQswCQY

.....

Ml4iYDx3GLii7gKZOAW4unJvcoOtw0387AMGb//IfNIWqFNpuXtuUq0Esc

—인증서 종료—

백 속성

친구 이름:StartCom 인증 기관

subject=/C=IL/O=StartCom Ltd./OU=S4cure 디지털 인증서 서명/CN=StartCom 인증 기관

issuer=/C=IL/O=StartCom Ltd./OU=S4cure 디지털 인증서 서명/CN=StartCom 인증 기관

—인증서 시작—

MIIHyTCCBbGawIBAgIBATNABgkqhkiG9w0BAQUFADB9MQswCQYDVQ

.....

BJ6y6koQOQK/W/7HA/lwr+bMEkXN9P/FlUQqz9IgOgA38corog14=

—인증서 종료—

백 속성

subject=/C=IL/O=StartCom Ltd./OU=S4Cure 디지털 인증서 서명/CN=StartCom Class 2 기본 중간 S4서버 CA

issuer=/C=IL/O=StartCom Ltd./OU=S4cure 디지털 인증서 서명/CN=StartCom 인증 기관

—인증서 시작—

MIIGNDCCBBAwIBAgIBGjNABgkqhkiG9w0BAQUFADB9MQswCQYDVQQ

.....

WZP8P3PXLrQsldiL98l/ydrHIEH9LMF/TtNGCbnkqXBP7dcqhykguAzx/Q=

—인증서 종료—