

# RV320 및 RV325 VPN 라우터에서 내 인증서 구성

## 목표

인증서는 개인 또는 장치의 ID를 확인하거나, 서비스를 인증하거나, 파일을 암호화하는 데 사용됩니다. RV320에서는 자체 서명 또는 타사 권한 부여를 통해 최대 50개의 인증서를 추가할 수 있습니다. 클라이언트 또는 관리자용 인증서를 내보내고 PC 또는 USB 장치에 저장한 다음 가져올 수 있습니다.

이 문서의 목적은 기본 인증서를 선택하고, 인증서를 내보내고, RV32x Series VPN 라우터에서 인증서를 가져오는 방법을 보여 주는 것입니다.

## 적용 가능한 디바이스

- RV320 Dual WAN VPN Router
- RV325 Gigabit Dual WAN VPN Router

## 소프트웨어 버전

·v1.1.0.09

## 내 인증서

1단계. 웹 구성 유틸리티에 로그인하고 **Certificate Management(인증서 관리) > My Certificate(내 인증서)**를 선택합니다. *My Certificate(내 인증서)* 페이지가 열립니다.



My Certificate					
My Certificate Table					
Used	Type	Subject	Duration	Details	Export
<input checked="" type="radio"/>	Self-Signed	CN=6c:20:56:c6:16:52 OU=RV320	From: 2013-Apr-08 To: 2023-Apr-06		
<input type="radio"/>	Certificate Signing Request	CN=com OU=so			
<input type="radio"/>	Self-Signed	CN=jwdnkf OU=jdnd	From: 2013-Apr-29 To: 2013-May-29		

Buttons: Add, Delete, Select as Primary Certificate

인증서에는 두 가지 유형이 있습니다.

· 자체 서명 — 자체 작성자가 서명한 SSL(Secure Socket Layer) 인증서입니다. 이 유형은 공격자에 의해 개인 키가 손상된 경우 취소할 수 없으므로 안전하지 않습니다.

· 인증서 서명 요청 — PKI(Public Key Infrastructure)로서 디지털 ID 인증서를 신청하기 위해 인증 기관에 전송됩니다. 개인 키는 비밀로 유지되므로 자체 서명보다 안전합니다.

2단계. *My Certificate Table(내 인증서 테이블)*에서 원하는 라디오 버튼을 클릭하여 인증서를 선택합니다.

3단계. **Select as Primary Certificate(기본 인증서로 선택)**를 클릭하여 선택한 인증서를 기본 인증서로 만듭니다.

4단계. (선택 사항) 인증서에 대한 자세한 정보를 보려면 **Details** 아이콘을 클릭합니다.

My Certificate					
My Certificate Table					
Used	Type	Subject	Duration	Details	Export
<input checked="" type="radio"/>	Self-Signed	CN=6c:20:56:c6:16:52 OU=RV320	From: 2013-Apr-08 To: 2023-Apr-06		
<input type="radio"/>	Certificate Signing Request	CN=com OU=so			
<input type="radio"/>	Self-Signed	CN=jwdnkf OU=jdnd	From: 2013-Apr-29 To: 2013-May-29		

Certificate *Details*(인증서 세부사항) 창이 열립니다.

Certificate Details	
<b>Certificate Information</b>	
Version:	3
Serial Number:	D8 AF 62 26 26 36 5D D1
<b>Subject Information</b>	
Subject:	CN=6c:20:56:c6:16:52 OU=RV320 O=Cisco Systems, Inc. L=Irvine C=US ST=California
Public Key Algorithm:	rsaEncryption -
Subject Key Identifier:	2D E3 89 6D FC 43 76 2B AF 1D AC 2B F1 EB 11 D3 19 FE AD 63
<b>Issuer Information</b>	
Issuer:	CN=6c:20:56:c6:16:52 OU=RV320 O=Cisco Systems, Inc. L=Irvine C=US ST=California
Valid From:	Apr 8 19:12:48 2013 GMT
Valid Through:	Apr 6 19:12:48 2023 GMT
Signature Algorithm:	sha1WithRSAEncryption
Authority Key Identifier:	2D E3 89 6D FC 43 76 2B AF 1D AC 2B F1 EB 11 D3 19 FE AD 63
Fingerprint:	33 C4 E6 40 7D DD 1F 44 32 57 18 A9 AA D1 66 FB 5A B2 CD 36

5단계. (선택 사항) 인증서를 삭제하려면 삭제할 인증서의 라디오 버튼을 클릭한 다음 삭제를 클릭합니다.

6단계. **저장**을 클릭하여 설정을 저장합니다.

## 자체 서명 인증서 내보내기

1단계. 자체 서명 인증서를 내보내려면 **내보내기** 열에서 원하는 아이콘 단추를 클릭합니다.



My Certificate					
My Certificate Table					
Used	Type	Subject	Duration	Details	Export
<input checked="" type="radio"/>	Self-Signed	CN=6c:20:56:c6:16:52 OU=RV320	From: 2013-Apr-08 To: 2023-Apr-06		
<input type="radio"/>	Certificate Signing Request	CN=com OU=so			
<input type="radio"/>	Self-Signed	CN=jwdnkf OU=jdnd	From: 2013-Apr-29 To: 2013-May-29		

사용 가능한 아이콘 단추는 다음과 같이 정의됩니다.

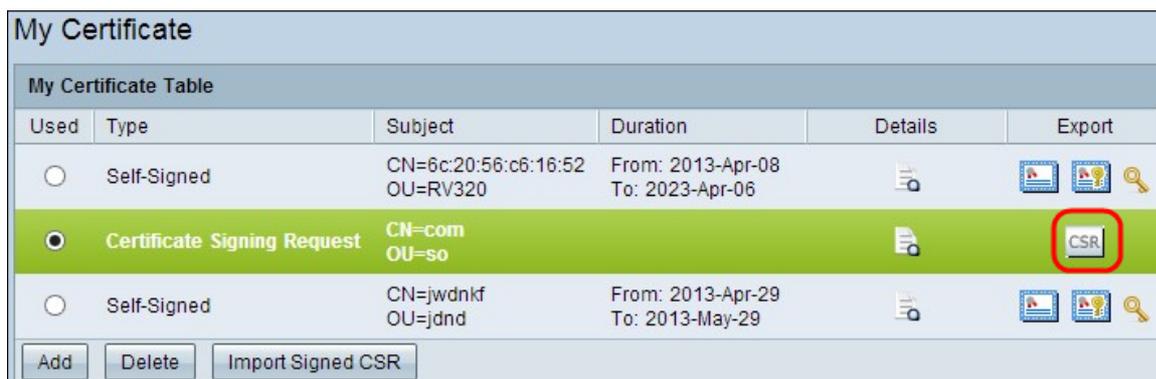
- 클라이언트용 인증서 내보내기 — 클라이언트를 VPN(Virtual Private Network)에 연결하는데 사용되는 클라이언트 인증서를 내보냅니다.
- 관리자를 위한 인증서 내보내기 — 관리자 인증서를 내보냅니다.개인 키가 생성되고 복사본을 백업용으로 보관합니다.
- Export Private Key(개인 키 내보내기) - VPN 연결을 위해 별도의 자격 증명이 필요한 VPN 클라이언트 소프트웨어의 개인 키를 내보냅니다.

2단계. 열기를 클릭하여 키를 봅니다.

3단계. 저장을 클릭하여 키를 저장합니다.

## 인증서 서명 요청 내보내기

1단계. CSR(Export Certificate Signing Request)을 클릭합니다.



My Certificate					
My Certificate Table					
Used	Type	Subject	Duration	Details	Export
<input type="radio"/>	Self-Signed	CN=6c:20:56:c6:16:52 OU=RV320	From: 2013-Apr-08 To: 2023-Apr-06		
<input checked="" type="radio"/>	Certificate Signing Request	CN=com OU=so			
<input type="radio"/>	Self-Signed	CN=jwdnkf OU=jdnd	From: 2013-Apr-29 To: 2013-May-29		

2단계. 열기를 클릭하여 확인합니다.

3단계. Save(저장)를 클릭하여 PC 또는 USB에 키를 저장합니다.

## 인증서 가져오기

1단계. Add(추가)를 클릭하여 인증서를 가져옵니다.

**My Certificate**

**My Certificate Table**

Used	Type	Subject	Duration	Details	Export
<input type="radio"/>	Self-Signed	CN=6c:20:56:c6:16:52 OU=RV320	From: 2013-Apr-08 To: 2023-Apr-06		
<input checked="" type="radio"/>	Certificate Signing Request	CN=com OU=so			
<input type="radio"/>	Self-Signed	CN=jwdnkf OU=jdnd	From: 2013-Apr-29 To: 2013-May-29		

다음 창이 나타납니다.

**My Certificate**

3rd-Party Authorized  
 Self-Signed

---

**Import Full Certificate Set**

Import from PC

CA Certificate:  No file chosen ( PEM format )

Certificate + Private Key:  No file chosen ( PEM format )

Import from USB Device

USB Device Status: No Device Attached

2단계. 원하는 라디오 버튼을 클릭하여 가져올 인증서의 유형을 정의합니다.

**My Certificate**

3rd-Party Authorized  
 Self-Signed

---

**Import Full Certificate Set**

Import from PC

CA Certificate:  No file chosen ( PEM format )

Certificate + Private Key:  No file chosen ( PEM format )

Import from USB Device

USB Device Status: No Device Attached

- 서드파티 공인 — 인증 기관이 디지털 서명을 제공하는 PKI(Public Key Infrastructure)
- 자체 서명 — 자체 작성자가 서명한 SSL(Secure Socket Layer) 인증서입니다.

3단계. 원하는 라디오 버튼을 클릭하여 인증서를 가져올 방법을 선택합니다.

My Certificate

3rd-Party Authorized  
 Self-Signed

Import Full Certificate Set

Import from PC  
CA Certificate:  No file chosen ( PEM format )  
Certificate + Private Key:  No file chosen ( PEM format )  
 Import from USB Device

·PC에서 가져오기 — 인증서를 저장한 PC에서 가져옵니다.

·USB에서 가져오기 — USB 드라이브에서 인증서를 가져옵니다.

## PC에서 인증서 가져오기

1단계. 타사 공인 인증서를 가져오는 경우 **CA 인증서 옆에 있는 파일 선택**을 클릭하여 파일 위치를 찾아 선택합니다.

2단계. **Certificate + Private Key** 옆에 있는 **Choose File**(파일 선택)을 클릭하여 파일 위치를 찾아 선택합니다.

4단계. **저장**을 클릭하여 설정을 저장합니다.가져온 인증서가 **내 인증서 테이블**에 나타납니다.

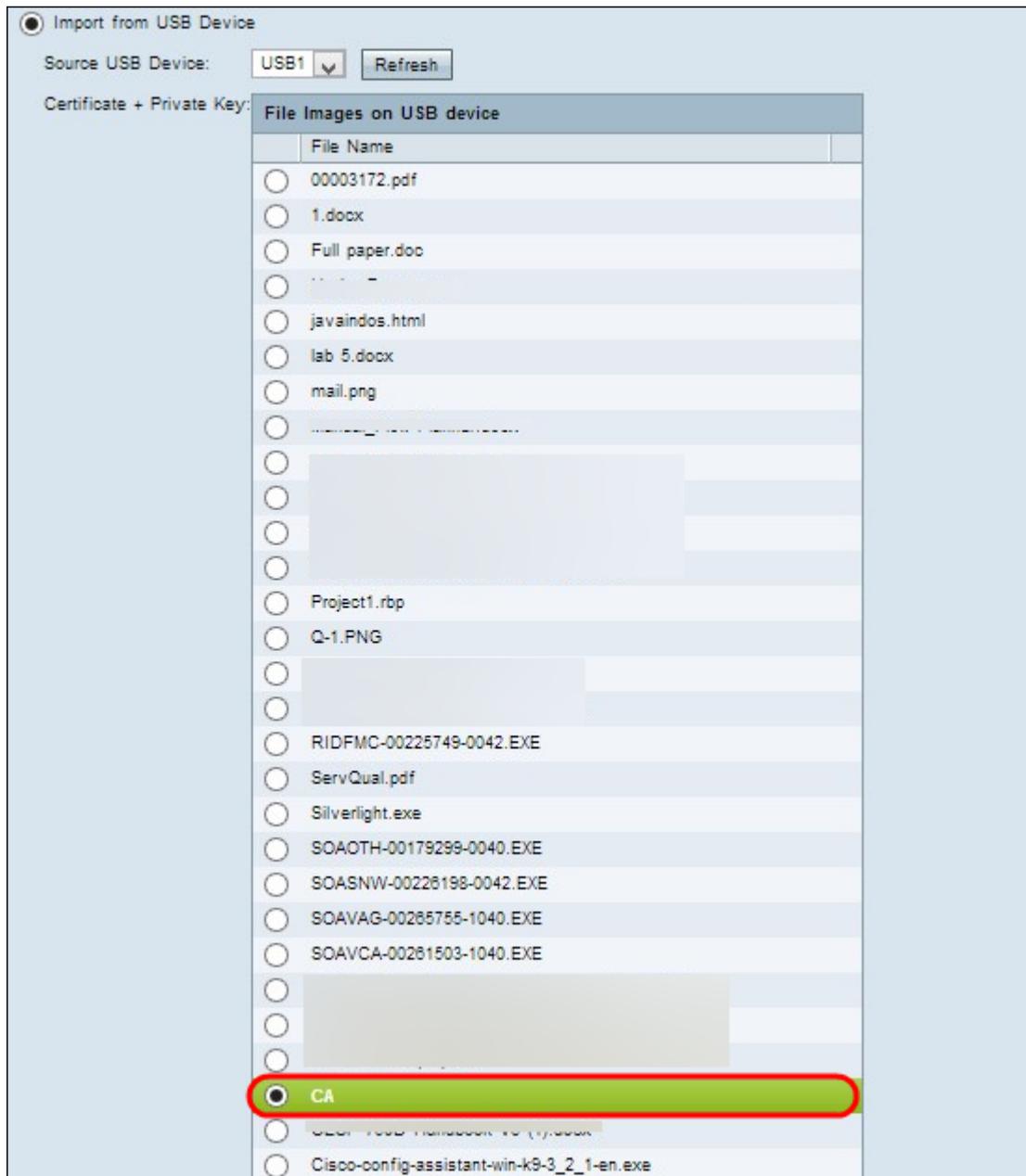
My Certificate

My Certificate Table

Used	Type	Subject	Duration	Details	Export
<input checked="" type="radio"/>	Self-Signed	CN=6c:20:56:c6:16:52 OU=RV320	From: 2013-Apr-08 To: 2023-Apr-06		
<input type="radio"/>	Certificate Signing Request	CN=com OU=so			CSR
<input type="radio"/>	Self-Signed	CN=jwdnkf OU=jdnd	From: 2013-Apr-29 To: 2013-May-29		
<input type="radio"/>	Self-Signed	CN= OU=			

## USB에서 인증서 가져오기

1단계. *Source USB Device* 드롭다운 목록에서 적절한 USB 장치를 선택합니다.



2단계. 타사 공인 인증서를 가져오는 경우 해당 라디오 버튼을 클릭하여 USB에 저장한 CA 인증서를 가져옵니다.

3단계. 적절한 라디오 버튼을 선택하여 USB에 저장한 인증서 + 개인 키를 가져옵니다.

4단계. **저장**을 클릭하여 설정을 저장합니다. 가져온 인증서가 **내 인증서 테이블**에 나타납니다

## My Certificate

My Certificate Table					
Used	Type	Subject	Duration	Details	Export
<input checked="" type="radio"/>	Self-Signed	CN=6c:20:56:c6:16:52 OU=RV320	From: 2013-Apr-08 To: 2023-Apr-06		  
<input type="radio"/>	Certificate Signing Request	CN=com OU=so			 CSR
<input type="radio"/>	Self-Signed	CN=jwdnkf OU=jdnd	From: 2013-Apr-29 To: 2013-May-29		  
<input type="radio"/>	Self-Signed	CN= OU=			  