

RV34x Series 라우터의 인증서 관리

목표

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.

CA(Certificate Authority)에서 인증서를 가져오는 방법에 대해 살펴보겠습니다.CA는 인증에 사용됩니다.인증서는 다양한 서드파티 사이트에서 구매합니다.이는 귀하의 사이트가 안전하다는 것을 증명하는 공식적인 방법입니다.기본적으로 CA는 신뢰할 수 있는 소스이며, 사용자가 합법적인 비즈니스인지 확인하고 신뢰할 수 있는지 확인합니다.필요에 따라 최소한의 비용으로 인증서를 생성합니다.CA에서 체크 아웃한 후, 해당 정보가 확인되면 사용자에게 인증서를 발급합니다.이 인증서는 컴퓨터에서 파일로 다운로드할 수 있습니다.그런 다음 라우터(또는 VPN 서버)로 이동하여 업로드할 수 있습니다.

이 문서의 목적은 RV34x Series 라우터에서 인증서를 생성, 내보내기 및 가져오는 방법을 보여 주는 것입니다.

적용 가능한 디바이스 | 소프트웨어 버전

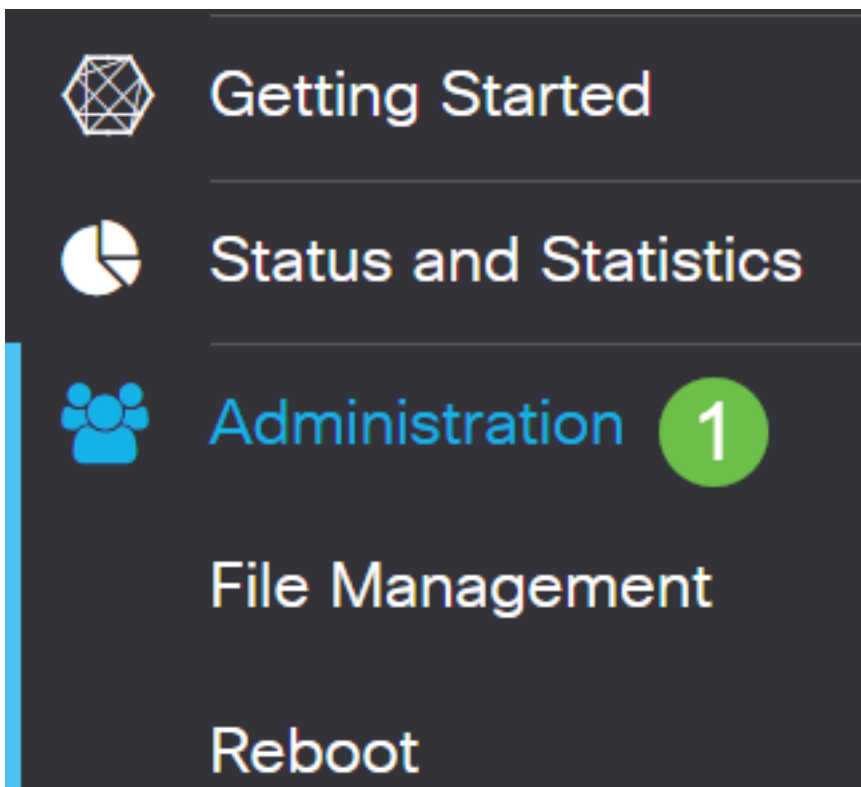
- RV34x 시리즈 | 1.0.03.20

라우터에서 인증서 관리

CSR/인증서 생성

1단계

라우터의 웹 기반 유틸리티에 로그인하고 Administration(관리) > Certificate(인증서)를 선택합니다.



2단계

Generate **CSR/Certificate**를 클릭합니다.CSR/인증서 생성 페이지로 이동합니다.

Import Certificate...

Generate CSR/Certificate...

Show Built-in 3rd-Party CA Certificates...

3단계

상자에 다음을 입력합니다.

- 적절한 인증서 유형 선택
 - 자체 서명 인증서 — 자체 작성자가 서명한 SSL(Secure Socket Layer) 인증서입니다.이 인증서는 신뢰할 수 없습니다. 개인 키가 공격자에 의해 보안된 경우 취소할 수 없습니다.
 - Certified Signing Request — PKI(Public Key Infrastructure)로서 디지털 ID 인증서를 신청하기 위해 인증 기관에 전송됩니다.개인 키가 비밀로 유지되므로 자체 서명보다 안전합니다.
- 인증서 이름 필드에 인증서 이름을 입력하여 요청을 식별합니다.이 필드는 공백이거나 공백과 특수 문자를 포함할 수 없습니다.
- (선택 사항) Subject Alternative Name(주체 대체 이름) 영역에서 라디오 버튼을 클릭합니다.옵션은 다음과 같습니다.
 - IP 주소 — 인터넷 프로토콜(IP) 주소를 입력합니다.
 - FQDN — FQDN(정규화된 도메인 이름)을 입력합니다.
 - 이메일 — 이메일 주소를 입력합니다.
- Subject Alternative Name 필드에 FQDN을 입력합니다.
- Country Name(국가 이름) 드롭다운 목록에서 귀하의 조직이 합법적으로 등록된 국가 이름을 선택합니다.
- 조직이 있는 주, 도, 지역 또는 지역의 이름이나 약어를 주/도 이름(ST) 필드에 입력합니다.
- 조직이 등록되거나 Locality Name(구/군/시) 필드에 위치한 구/군/시의 이름을 입력합니다.
- 사업체가 법적으로 등록된 이름을 입력합니다.소기업 또는 단독 소유자로 등록하는 경우 Organization Name 필드에 인증서 요청자의 이름을 입력합니다.특수 문자는 사용할 수 없습니다.
- 조직 단위 이름 필드에 이름을 입력하여 조직 내 부서 간에 구분합니다.
- Common Name 필드에 이름을 입력합니다.이 이름은 인증서를 사용하는 웹 사이트의 정규화된 도메인 이름이어야 합니다.
- 인증서를 생성하려는 사람의 이메일 주소를 입력합니다.
- Key Encryption Length 드롭다운 목록에서 키 길이를 선택합니다.옵션은 512, 1024 및 2048입니다.키 길이가 클수록 인증서의 보안이 강화됩니다.
- Valid Duration 필드에 인증서가 유효한 일 수를 입력합니다.기본값은 360입니다.
- Generate를 클릭합니다.

Certificate

2

Generate

Cancel

Generate CSR/Certificate

Type:

Certificate Name:

Subject Alternative Name:

IP Address FQDN Email

Country Name(C):

State or Province Name(ST):

Locality Name(L):

Organization Name(O):

Organization Unit Name(OU):

Common Name(CN):

Email Address(E):

Key Encryption Length:

Valid Duration:

1

days (Range: 1-10950, Default: 360)

참고: 생성된 인증서가 이제 인증서 테이블에 나타납니다.

Certificate Table

Index	Certificate	Used By	Type	Signed By	Duration	Details	Action
1	Default	WebServ...	Local ...	Self Signed	From 2012-Jul-12, 00:00:00 GM To 2042-Jul-05, 00:00:00 GMT		
2	TestCACert...	-	CA C...	Self Signed	From 2018-Apr-04, 00:00:00 GM To 2023-Apr-04, 00:00:00 GMT		
3	Router	-	Local ...	CiscoTest-...	From 2020-Oct-01, 00:00:00 GM To 2022-Oct-01, 00:00:00 GMT		
4	TestCACert...	-	Local ...	Self Signed	From 2020-Nov-19, 00:00:00 GM To 2021-Nov-14, 00:00:00 GMT		

이제 RV345P 라우터에 인증서를 생성했습니다.

인증서 내보내기

1단계

Certificate Table(인증서 테이블)에서 내보낼 인증서의 확인란을 선택하고 내보내기 아이콘을 클릭합니다.

Certificate Table

Index	Certificate	Used By	Type	Signed By	Duration	Details	Action
1	Default	WebServ...	Local ...	Self Signed	From 2012-Jul-12, 00:00:00 GM To 2042-Jul-05, 00:00:00 GMT		
2	TestCACert...	-	CA C...	Self Signed	From 2018-Apr-04, 00:00:00 GM To 2023-Apr-04, 00:00:00 GMT		
3	Router	-	Local ...	CiscoTest-...	From 2020-Oct-01, 00:00:00 GM To 2022-Oct-01, 00:00:00 GMT		
<input checked="" type="checkbox"/> 1	TestCACert...	-	Local ...	Self Signed	From 2020-Nov-19, 00:00:00 GM To 2021-Nov-14, 00:00:00 GMT		2

2단계

- 인증서를 내보내려면 형식을 클릭합니다. 옵션은 다음과 같습니다.
 - PKCS #12 — PKCS(Public Key Cryptography Standards) #12은 .p12 확장자로 제공되는 내보낸 인증서입니다. 내보내기, 가져오기 및 삭제되는 파일을 보호하기 위해 파일을 암호화하려면 암호가 필요합니다.

- PEM — PEM(Privacy Enhanced Mail)은 메모장과 같은 간단한 텍스트 편집기를 사용하여 쉽게 읽을 수 있는 데이터로 변환할 수 있도록 웹 서버에 자주 사용됩니다.
- PEM을 선택한 경우 Export(내보내기)를 **클릭합니다**.
- Enter Password(비밀번호 입력) 필드에 내보낼 파일을 보호하기 위한 비밀번호를 입력합니다.
- 비밀번호 확인 필드에 비밀번호를 *다시* 입력합니다.
- Select Destination(대상 선택) 영역에서 PC가 선택되었으며 현재 사용 가능한 유일한 옵션입니다.
- Export(내보내기)를 **클릭합니다**.

Export Certificate

1

Export as PKCS#12 format

Enter Password

.....

2

Confirm Password

.....

Export as PEM format

Select Destination to Export:

PC

3

4

Export

Cancel

3단계

다운로드가 성공했음을 알리는 메시지가 다운로드 버튼 아래에 나타납니다. 브라우저에서 파일이 다운로드되기 시작합니다. **확인**을 클릭합니다.



Success



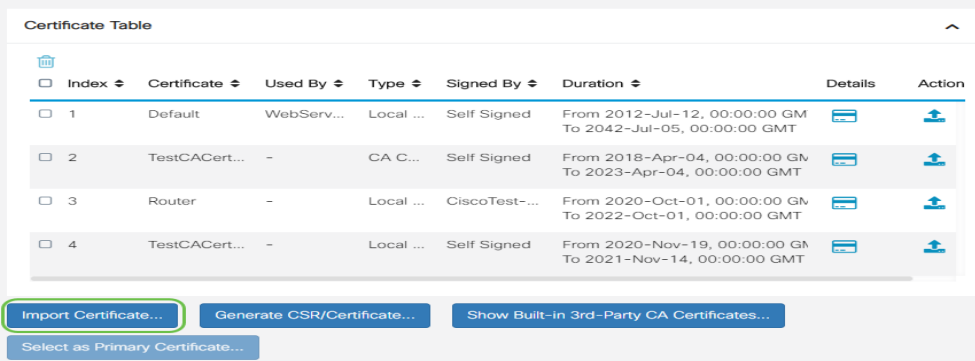
Ok

이제 Rv34x Series 라우터에서 인증서를 성공적으로 내보냈어야 합니다.

인증서 가져오기

1단계

Import Certificate..(인증서 가져오기..)를 클릭합니다..



Index	Certificate	Used By	Type	Signed By	Duration	Details	Action
1	Default	WebServ...	Local ...	Self Signed	From 2012-Jul-12, 00:00:00 GM To 2042-Jul-05, 00:00:00 GMT		
2	TestCACert...	-	CA C...	Self Signed	From 2018-Apr-04, 00:00:00 GM To 2023-Apr-04, 00:00:00 GMT		
3	Router	-	Local ...	CiscoTest-...	From 2020-Oct-01, 00:00:00 GM To 2022-Oct-01, 00:00:00 GMT		
4	TestCACert...	-	Local ...	Self Signed	From 2020-Nov-19, 00:00:00 GN To 2021-Nov-14, 00:00:00 GMT		

2단계

- 드롭다운 목록에서 가져올 인증서의 유형을 선택합니다. 옵션은 다음과 같습니다.
 - 로컬 인증서 — 라우터에서 생성된 인증서.
 - CA 인증서 — 신뢰할 수 있는 서드파티 기관에서 인증한 인증서로서 인증서에 포함된 정보가 정확함을 확인했습니다.
 - PKCS #12 Encoded 파일 — PKCS(Public Key Cryptography Standards) #12은 서버 인증서를 저장하는 형식입니다.
- *Certificate Name* 필드에 인증서 이름을 입력합니다.
- PKCS #12을 선택한 경우 Import Password(비밀번호 가져오기) 필드에 파일의 비밀번호를 입력합니다. 그렇지 않으면 3단계로 건너뛵니다.
- 인증서를 가져오려면 소스를 클릭합니다. 옵션은 다음과 같습니다.
 - PC에서 가져오기
 - USB에서 가져오기
- 라우터에서 USB 드라이브를 탐지하지 못하면 Import from USB(USB에서 가져오기) 옵션이 회색으로 표시됩니다.
- Import From USB(USB에서 가져오기)를 선택했는데 라우터에서 USB를 인식하지 못하는 경우 Refresh(새로 고침)를 클릭합니다.
- Choose File(파일 선택) 버튼을 클릭하고 적절한 파일을 선택합니다.
- Upload(업로드)를 클릭합니다.

Certificate

3 Upload Cancel

Import Certificate

Type: PKCS#12 encoded file

Certificate Name: cisco 1

Import Password:

Upload certificate file

Import From PC

2 Browse... TestCACertificate

Import From USB

성공하면 자동으로 기본 Certificate 페이지로 이동합니다. 인증서 테이블이 최근에 가져온 인증서로 채워집니다.

Certificate Table

Index	Certificate	Used By	Type	Signed By	Duration	Details	Action
1	Default	WebServ...	Local ...	Self Signed	From 2012-Jul-12, 00:00:00 GM To 2042-Jul-05, 00:00:00 GMT		
2	TestCACert...	-	CA C...	Self Signed	From 2018-Apr-04, 00:00:00 GM To 2023-Apr-04, 00:00:00 GMT		
3	Router	-	Local ...	CiscoTest-...	From 2020-Oct-01, 00:00:00 GM To 2022-Oct-01, 00:00:00 GMT		
4	TestCACert...	-	Local ...	Self Signed	From 2020-Nov-19, 00:00:00 GM To 2021-Nov-14, 00:00:00 GMT		

이제 RV34x Series 라우터에서 인증서를 성공적으로 가져와야 합니다.