

RV160 및 RV260 라우터의 OpenVPN

목표

이 문서의 목적은 RV160 또는 RV260 라우터에 OpenVPN을 설정하는 방법과 컴퓨터에 OpenVPN의 VPN 클라이언트 설정을 안내하는 것입니다.

적용 가능한 디바이스

- RV160
- RV260

소프트웨어 버전

- 1.0.00.15

목차

[RV160/RV260 라우터에서 데모 OpenVPN 설정](#)

[RV160/RV260 라우터에서 OpenVPN 설정](#)

[데모 OpenVPN 설정 후 자체 서명 인증서로 로그인](#)

[컴퓨터에 OpenVPN 클라이언트 설정](#)

소개

OpenVPN은 VPN(Virtual Private Network)에 설정 및 사용할 수 있는 무료 오픈 소스 애플리케이션입니다. 클라이언트-서버 연결을 사용하여 인터넷을 통해 서버와 원격 클라이언트 위치 간에 안전한 통신을 제공합니다.

OpenVPN은 트래픽 전송에 UDP 및 TCP의 암호화에 OpenSSL을 사용합니다.VPN은 안전한 보호 터널을 제공하여 VPN 연결을 통해 컴퓨터에서 보낸 데이터를 암호화하기 때문에 해커에게 덜 취약합니다.예를 들어, 공항 등의 공공 장소에서 WiFi를 사용하는 경우 다른 사용자가 데이터, 트랜잭션 및 쿼리를 볼 수 없게 됩니다.HTTPS와 마찬가지로, 두 엔드포인트 간에 전송되는 데이터를 암호화합니다.

OpenVPN을 설정하는 가장 중요한 단계 중 하나는 CA(Certificate Authority)로부터 인증서를 받는 것입니다. 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.OpenVPN의 경우 최소 비용으로 더 낮은 수준의 인증서만 있으면 됩니다.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.클라이언트는 OpenVPN을 사용하기 위한 인증서가 필요하지 않습니다. 이는 라우터를 통한 확인용입니다.

사전 요구 사항

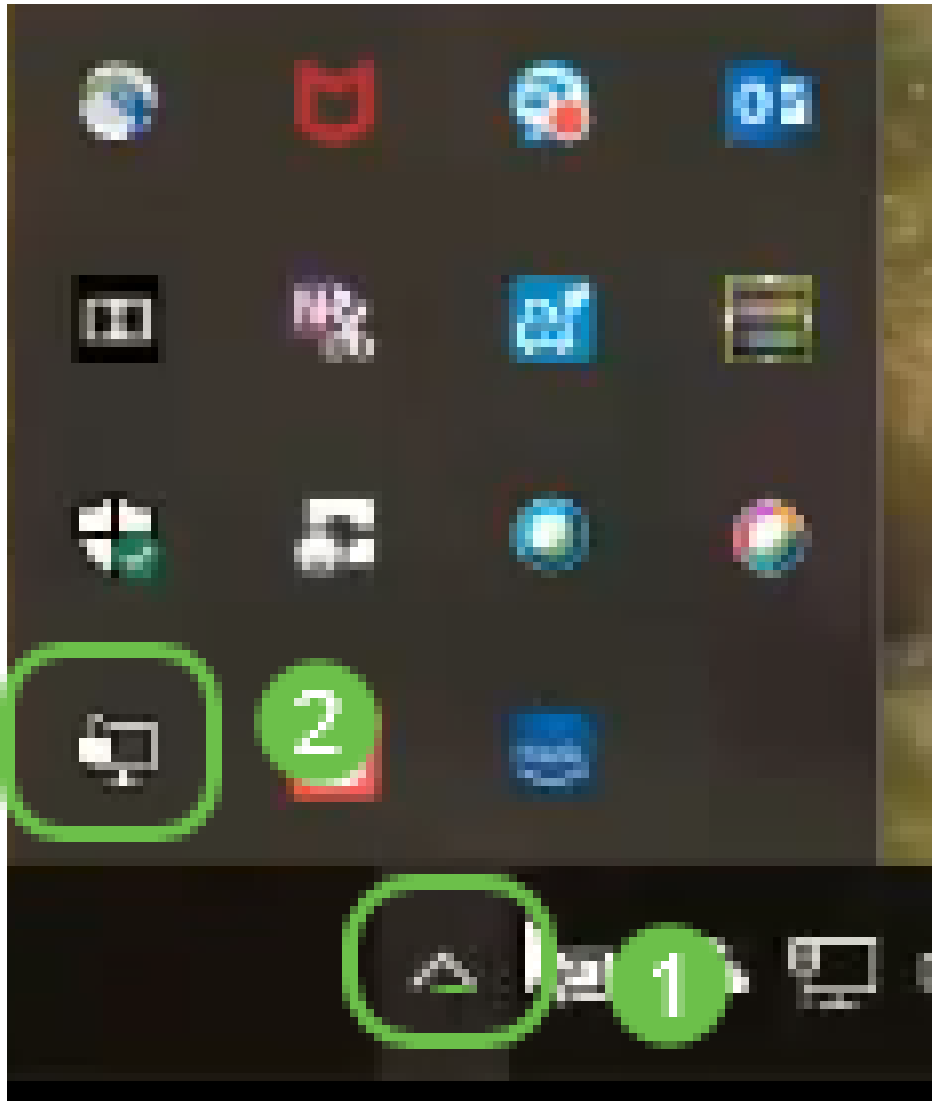
시스템에 OpenVPN 애플리케이션을 설치합니다. OpenVPN 웹 사이트로 이동하려면 [여기](#)를 클릭하십시오.

OpenVPN에 대한 자세한 내용 및 여러 질문에 대한 답변을 보려면 [여기](#)를 클릭하십시오.

참고: 이 설정은 Windows 10에만 적용됩니다.



OpenVPN을 설치한 후에는 애플리케이션이 데스크톱에 나타나거나 작업 표시줄 오른쪽에 작은 아이콘으로 나타나야 합니다. OpenVPN 클라이언트도 이 설치가 필요합니다.



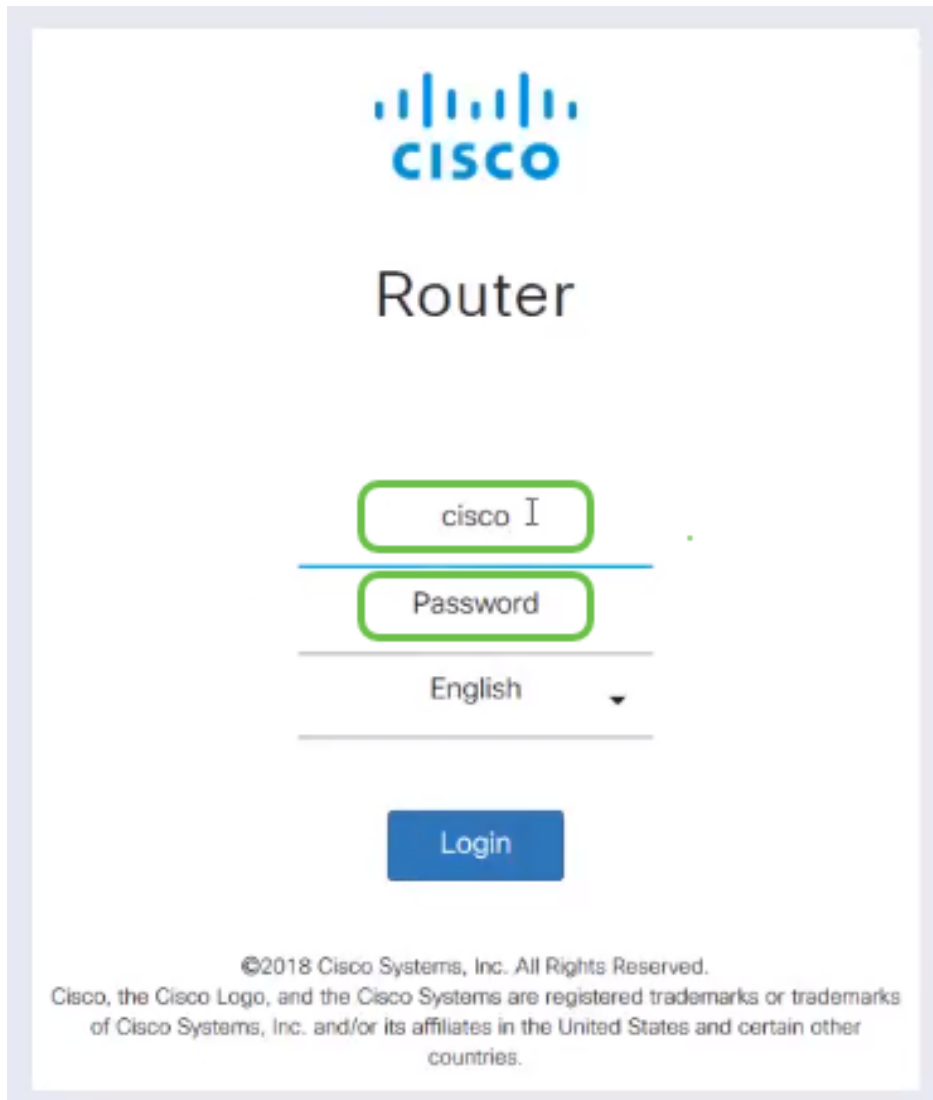
모든 디바이스에서 적절한 시스템 시간을 설정해야 합니다. 인증서를 생성하기 전에 라우터에서 적절한 시스템 시간을 완전히 동기화해야 합니다. 이 작업은 종종 자동으로 수행되지만 문제가 발생할 경우 이 옵션을 선택하면 됩니다.

RV160/RV260 라우터에서 데모 OpenVPN 설정

CA에 대한 비용을 지불하기 전에 OpenVPN을 시도하려는 경우 자체 서명 인증서를 생성할 수 있습니다. 이를 통해 OpenVPN이 비즈니스에 구축하고자 하는 것인지 비용 없이 확인할 수 있습니다. CA를 구매하려는 경우 문서의 이 섹션을 건너뛰고 [RV160/RV260 라우터에서 OpenVPN 설정으로](#) 직접 이동할 수 있습니다.

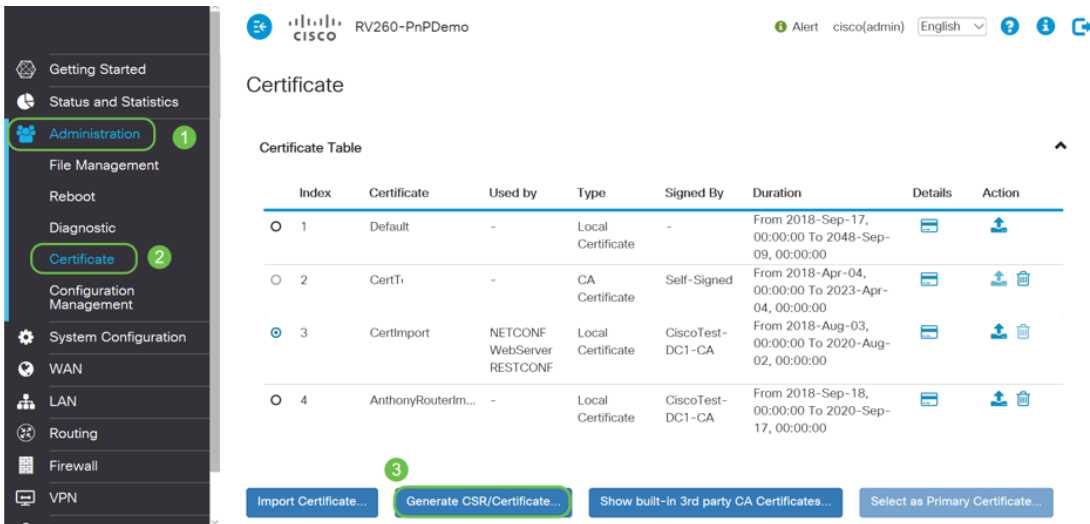
1단계. 자격 증명을 사용하여 라우터에 로그인합니다. 기본 사용자 이름과 비밀번호는 *cisco*입니다.

참고: 모든 비밀번호를 좀 더 복잡한 것으로 변경하는 것이 좋습니다. 그렇지 않으면 문을 잠그지 않은 문 앞에 놓고 가는 것과 같습니다.

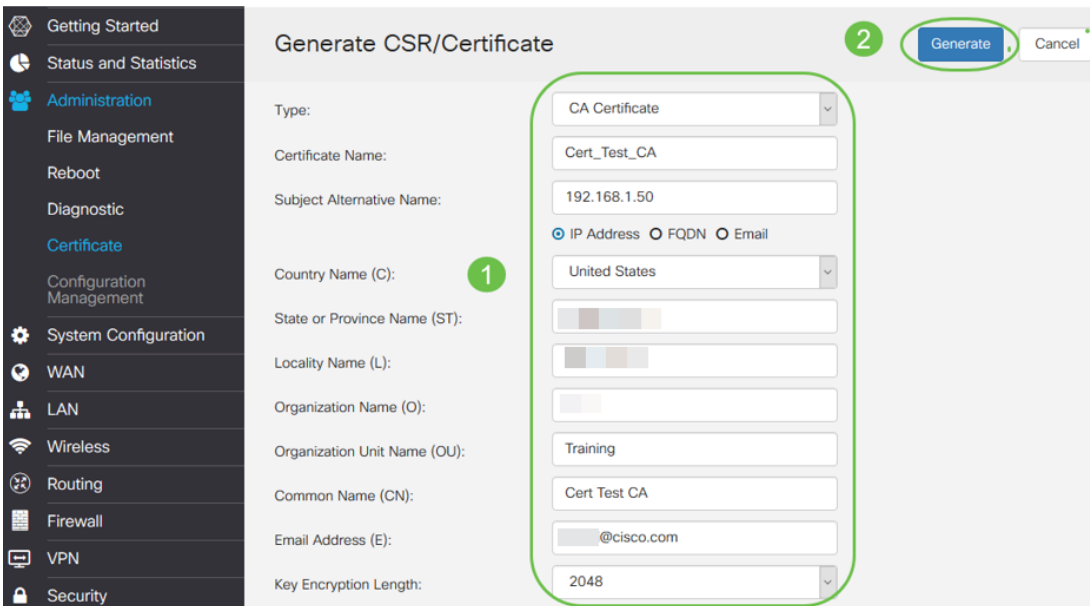


The screenshot shows the Cisco Router login interface. At the top is the Cisco logo. Below it, the word "Router" is displayed. There are three input fields: "Username" containing "cisco", "Password", and "Language" set to "English". A blue "Login" button is located below the fields. At the bottom, there is a copyright notice: "©2018 Cisco Systems, Inc. All Rights Reserved. Cisco, the Cisco Logo, and the Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries."

2단계. 라우터에서 인증서를 받아야 합니다. Administration(관리) > Certificate(인증서) > Generate CSR/Certificate...(CSR/인증서 생성...)로 이동합니다. 이는 인증서에 대한 요청을 생성하는 방법입니다.



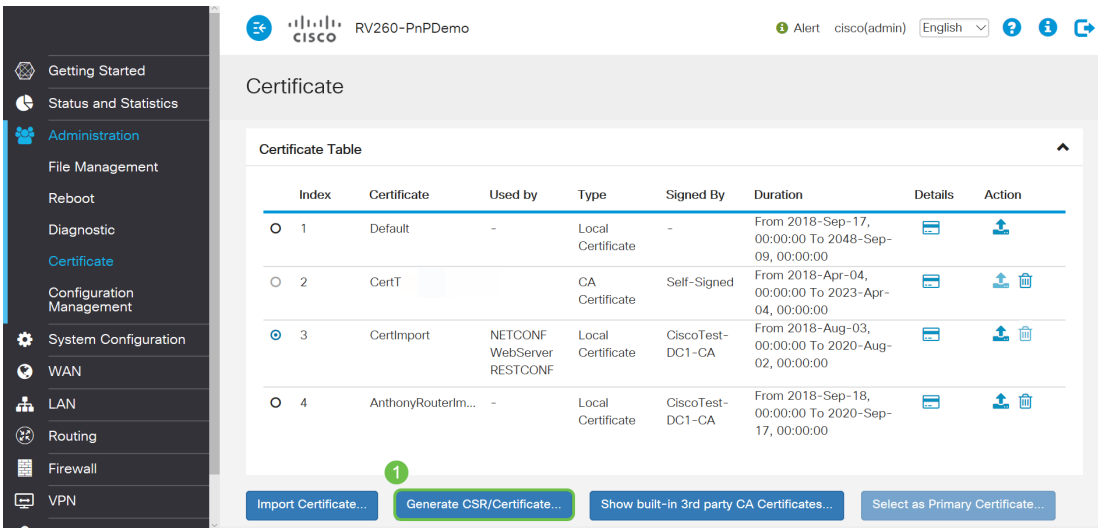
3단계. CA 인증서를 요청합니다.



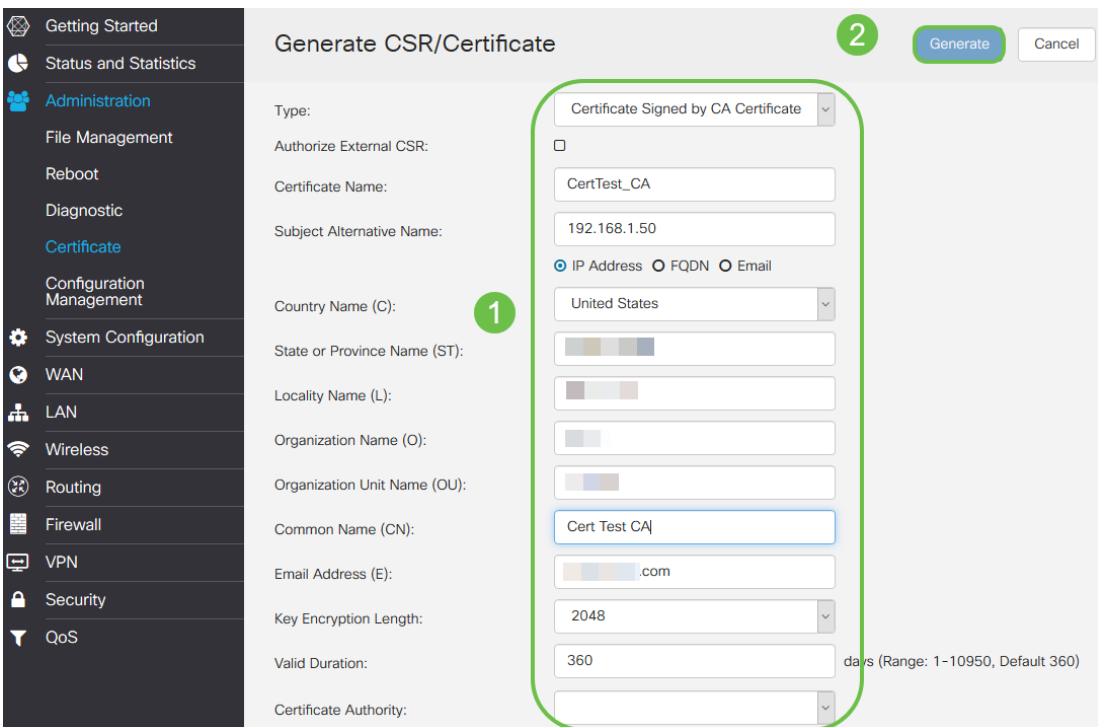
- 드롭다운 메뉴에서 CA Certificate(CA 인증서)를 선택합니다.
- 인증서 이름 입력
- IP 주소, FQDN(Fully Qualified Domain Name) 또는 이메일을 입력합니다.IP 주소를 입력하는 것이 가장 일반적인 선택입니다.
- 국가 입력
- 상태 입력
- 구/군/시 이름 입력
- 조직 이름 입력
- 조직 단위 이름 입력
- 이메일 주소 입력
- Enter Key Encryption Length, 2048을 사용하는 것이 좋습니다.

오른쪽 위의 **Generate** 버튼을 클릭합니다.

4단계. 서버 인증서도 필요합니다.CA 인증서에서 서명한 이 인증서는 방금 생성한 CA 인증서에서 서명됩니다.



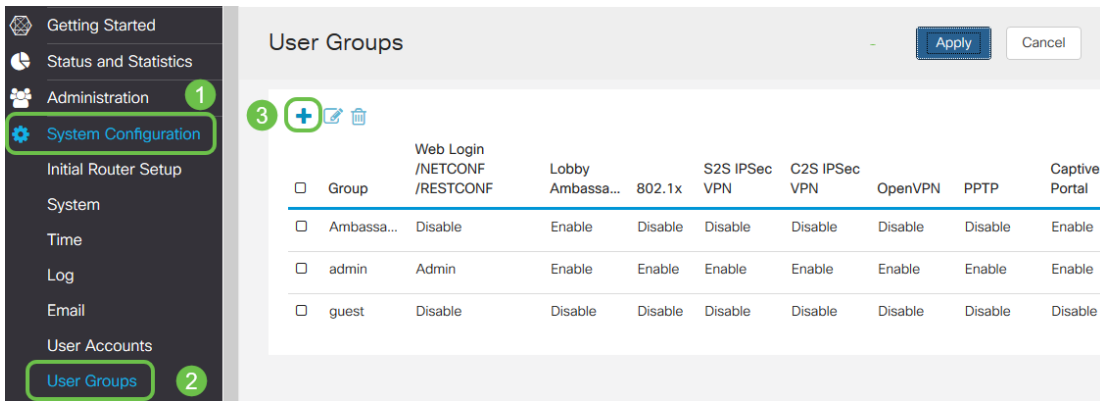
5단계. CA 인증서에서 서명한 인증서를 요청합니다.



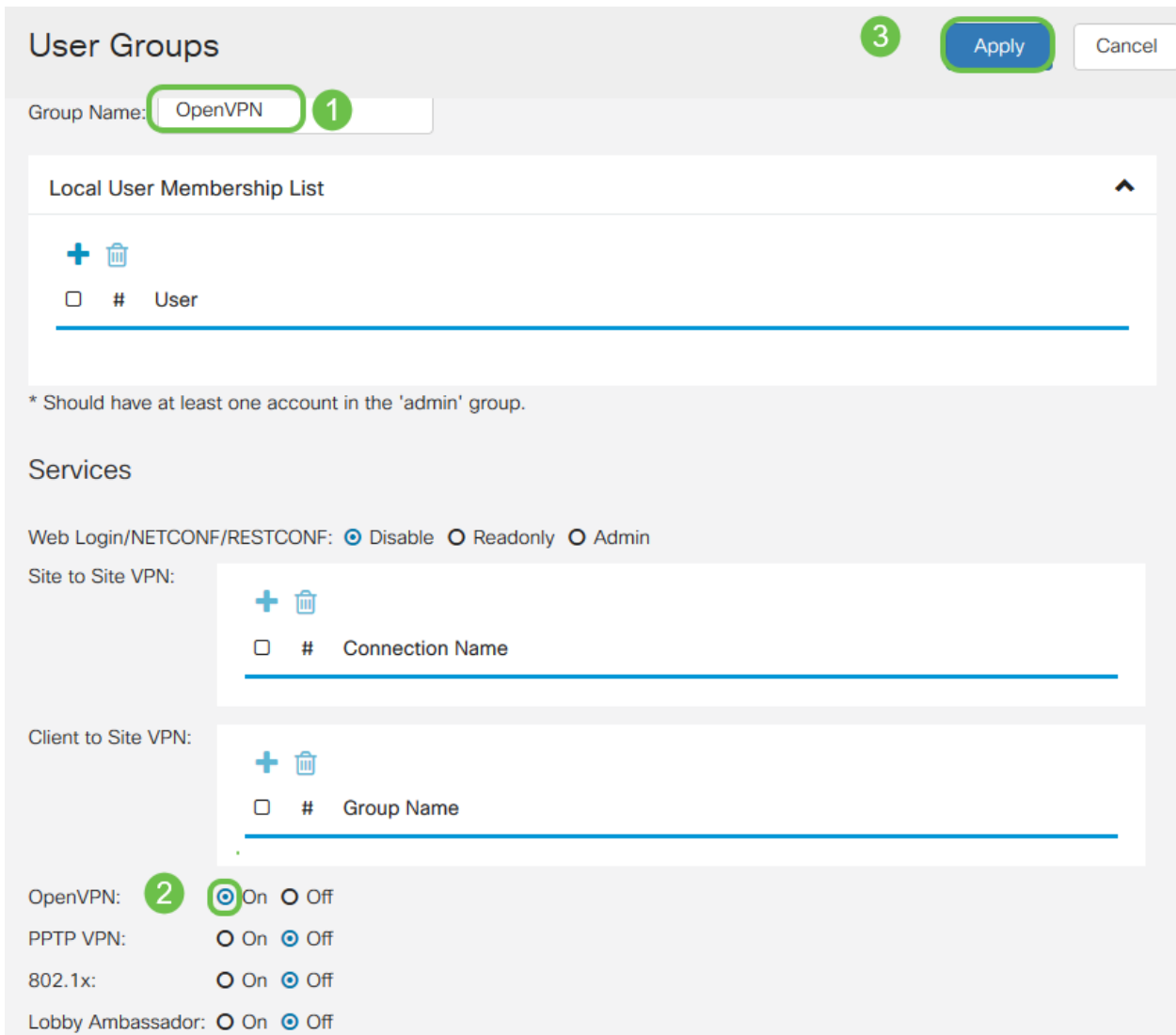
- 드롭다운 메뉴에서 Certificate Signing Request를 선택합니다.
- 인증서 이름 입력
- IP 주소, FQDN(Fully Qualified Domain Name) 또는 이메일을 입력합니다. IP 주소를 입력하는 것이 가장 일반적인 선택입니다.
- 국가 입력
- 상태 입력
- 구/군/시 이름 입력
- 조직 이름 입력
- 조직 단위 이름 입력
- 이메일 주소 입력
- Enter Key Encryption Length, 2048을 사용하는 것이 좋습니다.
- 드롭다운 메뉴에서 적절한 인증 기관을 선택합니다.

오른쪽 위의 **Generate** 버튼을 클릭합니다.

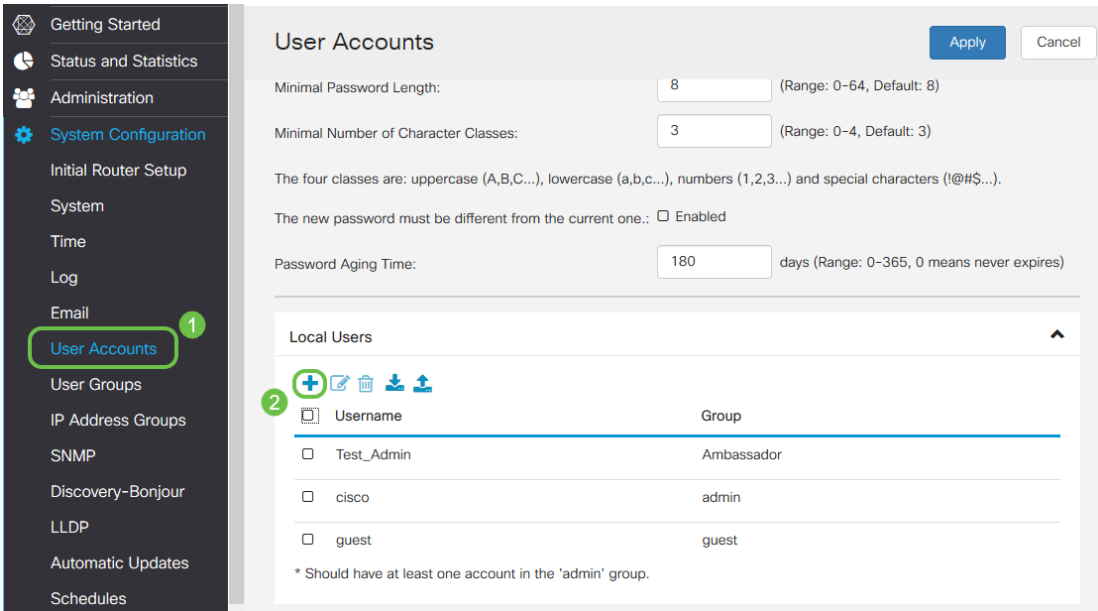
6단계. **System Configuration(시스템 컨피그레이션) > User Groups(사용자 그룹)**로 이동합니다. 더하기 아이콘을 선택하여 새 그룹을 추가합니다.



7단계. 그룹 이름을 입력하고 OpenVPN을 켜려면 라디오 버튼을 클릭 합니다.Apply를 클릭합니다.



8단계. System Configuration(시스템 컨피그레이션) 메뉴에서 User Accounts(사용자 계정)를 클릭 합니다.Local Users(로컬 사용자)에서 더하기 아이콘을 클릭합니다.



9단계. 아래 정보를 입력합니다.드롭다운 메뉴에서 OpenVPN을 선택해야 합니다.Apply를 클릭합니다.

Add user account

⚠ The current minimum requirements are as follows

- * Minimal Password Length: 8
- * Minimal Number of Character Classes: 3

Username: **1**

New Password:

Confirm Password:

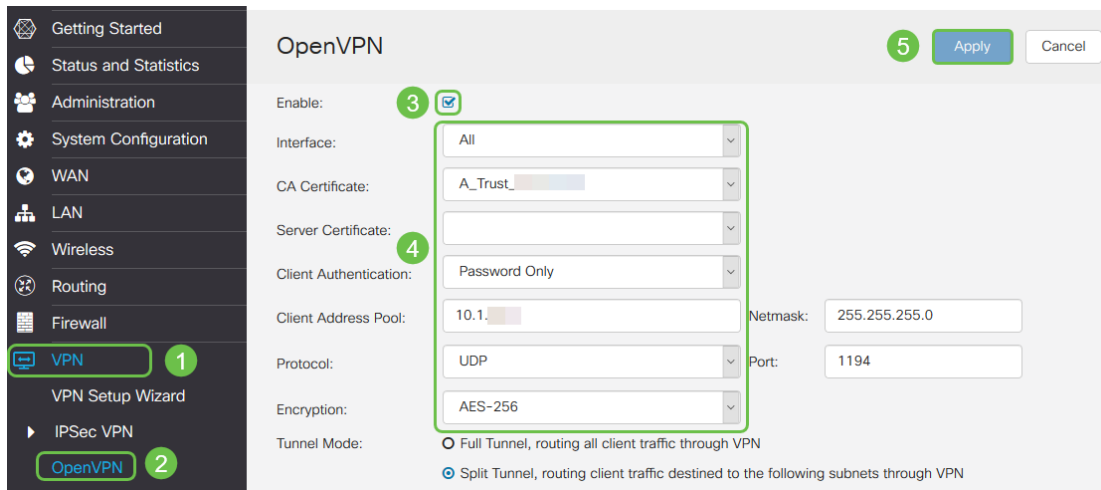
Password Strength meter:

Group:

2

모든 종속성이 완료되었으며 이제 OpenVPN에 대해 라우터를 구성할 수 있습니다.

10단계. **VPN > OpenVPN으로 이동합니다.**OpenVPN 페이지가 열립니다.드롭다운 메뉴에서 이전에 만든 인증서를 선택하여 페이지의 각 상자를 완료합니다.



- Enable(활성화) 상자를 선택합니다. 트래픽에서 허용할 인터페이스를 선택합니다. 이 경우 WAN(Wide Area Network)을 선택하고 CA(Certificate Authority) 인증서를 선택합니다.
- 드롭다운 메뉴에서 CA 인증서를 선택합니다.
- 드롭다운 메뉴에서 다운로드한 서버 인증서를 선택합니다.
- Client Authentication을 선택합니다. Password(비밀번호)를 선택하면 비밀번호로 인증해야 합니다. Password + Certificate를 선택하는 경우 클라이언트에도 인증서가 있어야 합니다. 이는 더 안전하지만 별도의 CA를 구매해야 하므로 VPN 비용이 추가됩니다.
- 클라이언트 주소 풀을 입력합니다. 회사 내 다른 곳에서 사용되지 않는 네트워크 서브넷의 IP 주소를 선택합니다. 예약된 범위 중에서 선택하고 다른 곳에서 사용되지 않는 범위를 선택합니다.
- 암호화 형식을 선택합니다. 암호화가 클라이언트와 동일한지 확인합니다. DES 및 3DES는 권장되지 않으며 이전 버전과의 호환성에만 사용해야 합니다.
- VPN을 통과하는 트래픽만 지정하려면 Split tunnel을 선택합니다. VPN의 경우 스플릿 터널이 필요합니다. 모든 클라이언트 트래픽이 VPN을 통과하도록 하려는 다른 상황에서는 전체 터널 모드가 선택됩니다.

11단계. 페이지를 아래로 스크롤하여 도메인 이름 및 DNS1을 입력합니다.

Domain Name:	Openvpn.net
DNS1:	192.168.1.1

참고: DNS1 IP 주소는 전용 내부 DNS 서버, ISP(인터넷 서비스 공급자)가 제공한 기본 게이트웨이의 동일한 IP 주소, 가상 머신 또는 인터넷의 신뢰할 수 있는 DNS 서버일 수 있습니다.

12단계. Apply를 클릭하여 라우터에 컨피그레이션을 저장합니다.

13단계. 동일한 페이지에 그대로 두고 더 스크롤합니다. OpenVPN 클라이언트에 설치할 구성 템플릿을 생성합니다. 이 파일은 .ovpn 확장명을 가지며 OpenVPN 클라이언트에서 사용됩니다. Export client configuration template (.ovpn)(클라이언트 컨피그레이션 템플릿 내보내기)을 선택하고 Generate(생성)를 클릭합니다. 이렇게 하면 파일이 컴퓨터에 다운로드됩니다.

Export setting:

Include client certificate:

Please choose the method you want to export:

1 Export client configuration template (.ovpn)

Send Email [Click here](#) to configure Email settings.

Email client configuration template (.ovpn) to recipients (multiple email addresses separated by comma):

Email Subject:

2

14단계. Status and Statistics(상태 및 통계) > VPN Status(VPN 상태)로 이동합니다.아래로 스크롤 하여 자세한 정보를 확인할 수 있습니다.

System Summary

IPv4 IPv6

WAN (Copper) USB

IP Address: 210.1.100.20/24 --

Default Gateway: 210.1.100.1 --

DNS: 210.1.100.1 --

Dynamic DNS: Disabled Disabled

(No Attached)

VPN Status

Type	Active	Configured	Max Supported	Connected
IPSec	Disabled	0	20	0
PPTP	Disabled	1	20	0
OpenVPN	Enabled	1	20	0

3

Firewall Setting Status

SPI (Stateful Packet Inspection): On

DoS (Denial of Service): On

Block WAN Request: Off

Remote Management: On

Log Setting Status

Syslog Server: Off

Email Log: Off

이 문서의 다음 섹션에서는 자체 서명 인증서를 사용하여 로그인하는 방법을 설명하므로 이 내용을 검토해야 합니다.

데모 OpenVPN 설정 후 자체 서명 인증서로 로그인

자체 서명 인증서를 사용하여 로그인하면 로그인을 시도할 때 경고 팝업이 표시될 수 있습니다.계속하려면 웹 브라우저에 따라 Advanced(고급), Proceed(진행), Trust(신뢰) 또는 다른 옵션을 클릭해야 합니다.

이 시점에서는 안전하지 않다는 경고를 받을 수 있습니다.계속, 예외 추가 또는 고급으로 선택할 수 있습니다.이는 웹 브라우저에 따라 달라집니다.

이 예에서 Chrome은 웹 브라우저에 사용되었습니다.이 메시지가 나타나면 **Advanced**를 클릭합니다.



Your connection is not private

Attackers might be trying to steal your information from [redacted].net (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_AUTHORITY_INVALID

Help improve Safe Browsing by sending some [system information and page content](#) to Google. [Privacy policy](#)

ADVANCED

BACK TO SAFETY

새 화면이 열리고 Proceed to yourwebsite.net (unsafe)(웹 사이트로 진행(unsafe))을 클릭해야 합니다.

This server could not prove that it is [redacted].net; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to [redacted].net (unsafe)

다음은 Firefox를 웹 브라우저로 사용할 때 디바이스 경고에 액세스하는 예입니다. Advanced(고급)를 클릭합니다.



Your connection is not secure

The owner of [redacted].net has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

[Learn more...](#)

Report errors like this to help Mozilla identify and block malicious sites

Go Back

Advanced

예외 추가...를 클릭합니다.

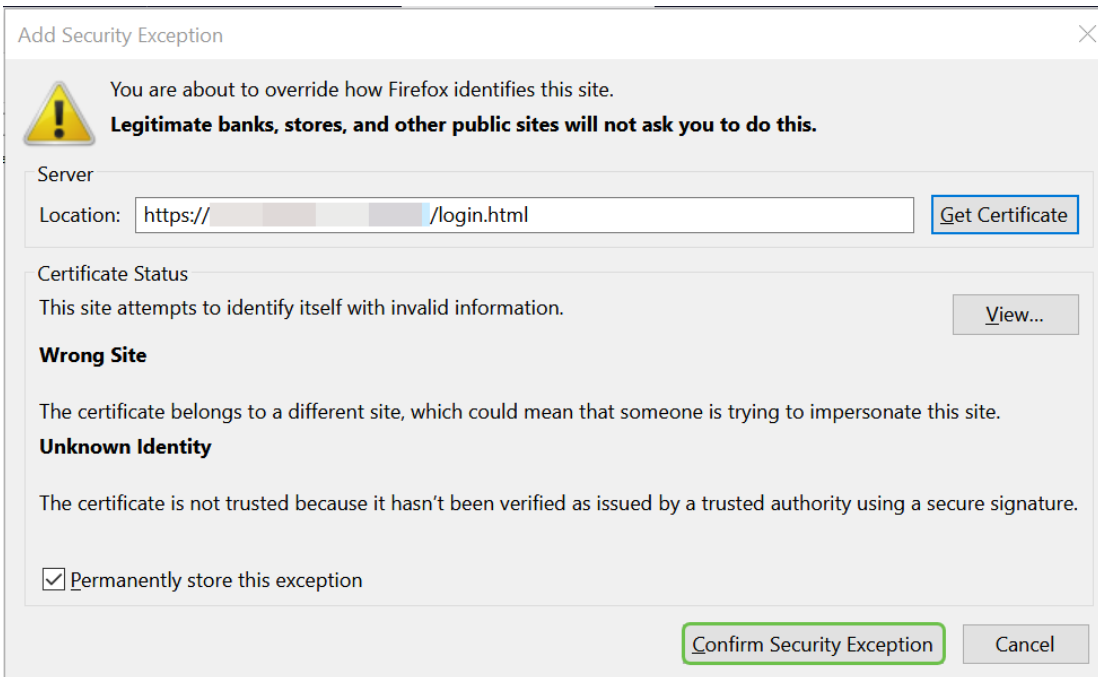
[redacted].net:50 uses an invalid security certificate.

The certificate is not trusted because it is self-signed.
The certificate is only valid for .

Error code: [MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT](#)

Add Exception...

마지막으로 Confirm Security Exception(보안 예외 확인)을 클릭해야 합니다.



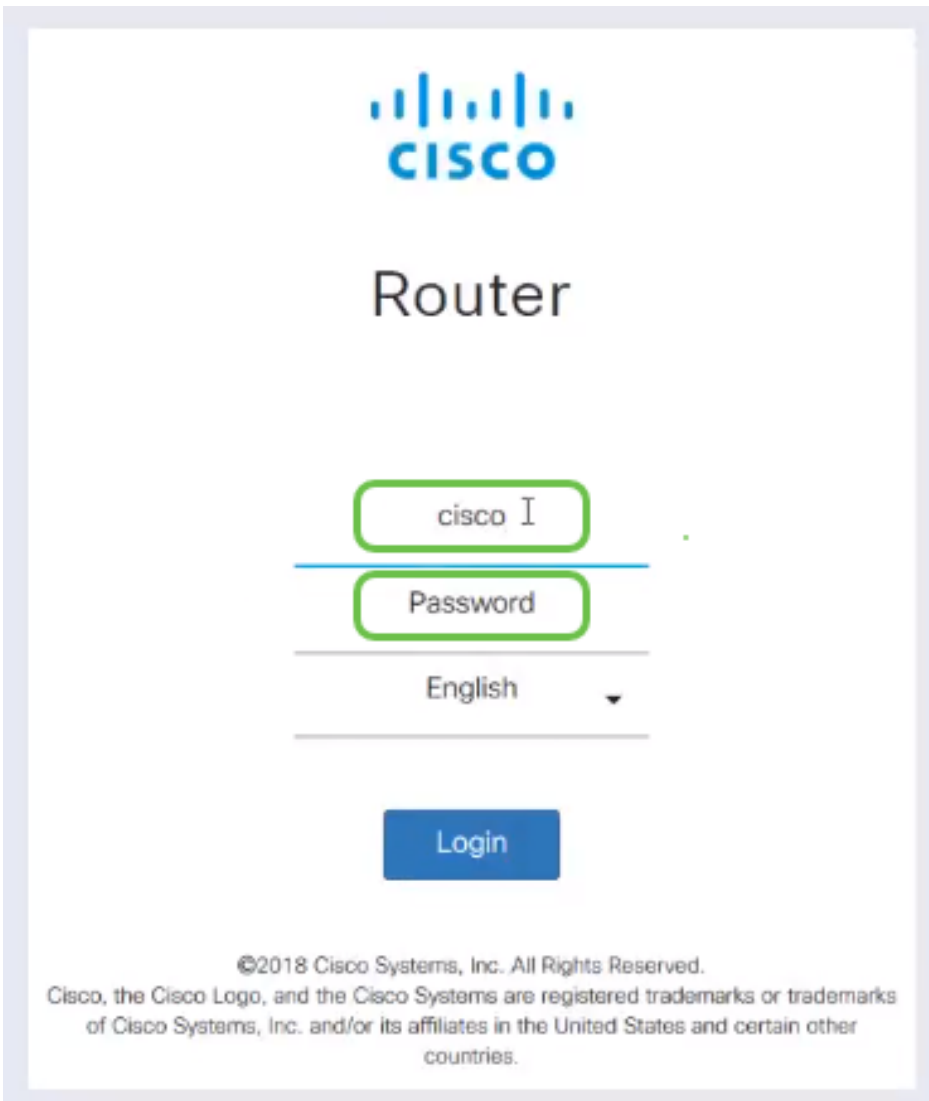
이제 라우터가 OpenVPN 클라이언트 연결을 지원하는 데 필요한 모든 매개변수로 구성됩니다. 클라이언트 컨피그레이션 템플릿을 디바이스에 이미 다운로드했으므로 이 템플릿은 *.ovpn*으로 끝납니다. 이제 [컴퓨터](#)의 OpenVPN [Client Setup](#) 섹션으로 이동할 수 있습니다. 회사에 OpenVPN을 구축하기로 결정한 경우 다음 섹션의 단계를 수행할 수 있습니다.

RV160/RV260 라우터에서 OpenVPN 설정

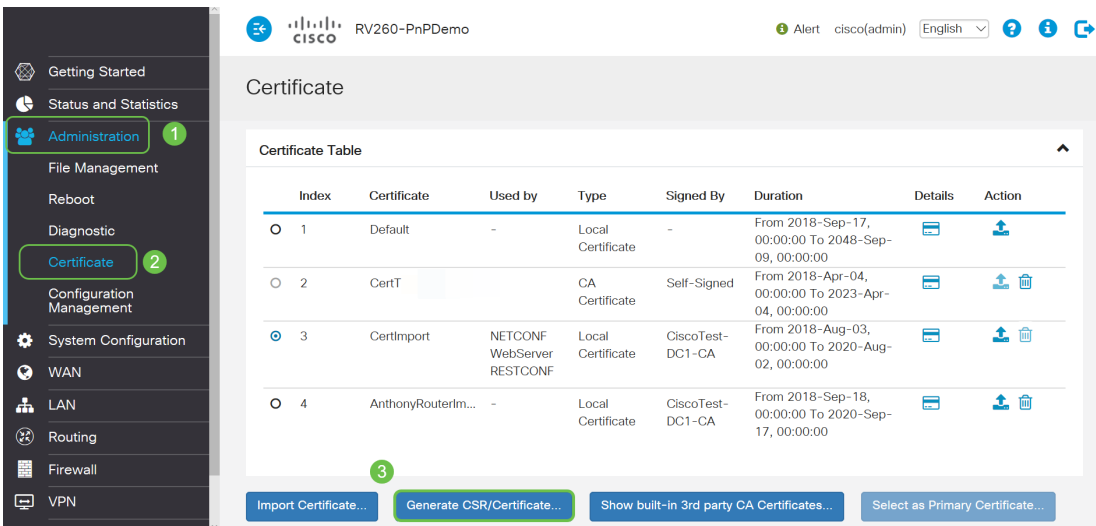
이것은 비용이 드는 제3자로부터 CA를 받는 것과 관련이 있기 때문에 더 복잡한 프로세스입니다. 또한 VPN 클라이언트 컨피그레이션 템플릿을 *.ovpn*으로 모든 클라이언트에 전송하여 해당 디바이스에서 설정할 수 있어야 합니다. 클라이언트가 통신하려면 라우터와 동일한 여러 설정이 필요합니다. 가장 좋은 점은 최소한의 비용으로 여러분과 직원들이 인터넷을 사용하고 더 안전하게 비즈니스를 수행할 수 있다는 것입니다.

1단계. 자격 증명을 사용하여 라우터에 로그인합니다. 기본 사용자 이름과 비밀번호는 *cisco*입니다.

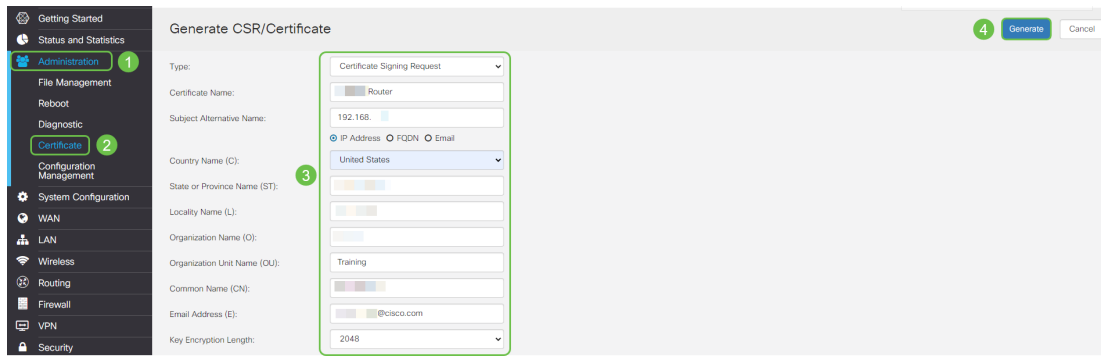
참고: 모든 비밀번호를 좀 더 복잡한 것으로 변경하는 것이 좋습니다. 그렇지 않으면 문을 잠그지 않은 문 앞에 놓고 가는 것과 같습니다.



2단계. 인증서를 받아야 합니다. Administration(관리) > Certificate(인증서) > Generate CSR/Certificate...(CSR/인증서 생성...)로 이동합니다. 이는 인증서에 대한 요청을 생성하는 방법입니다.



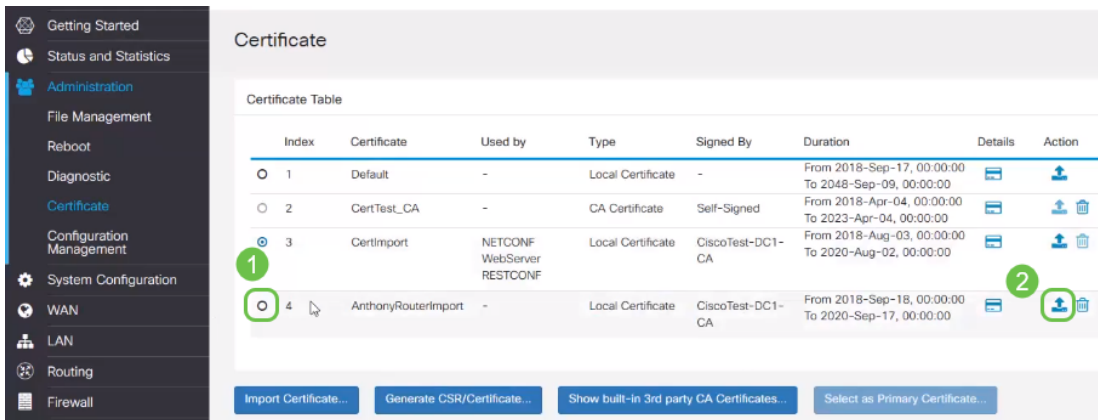
3단계. CA 인증서에서 서명한 인증서를 요청합니다. 이 정보는 Administration(관리) > Certificate(인증서)로 이동하여 찾을 수 있습니다.



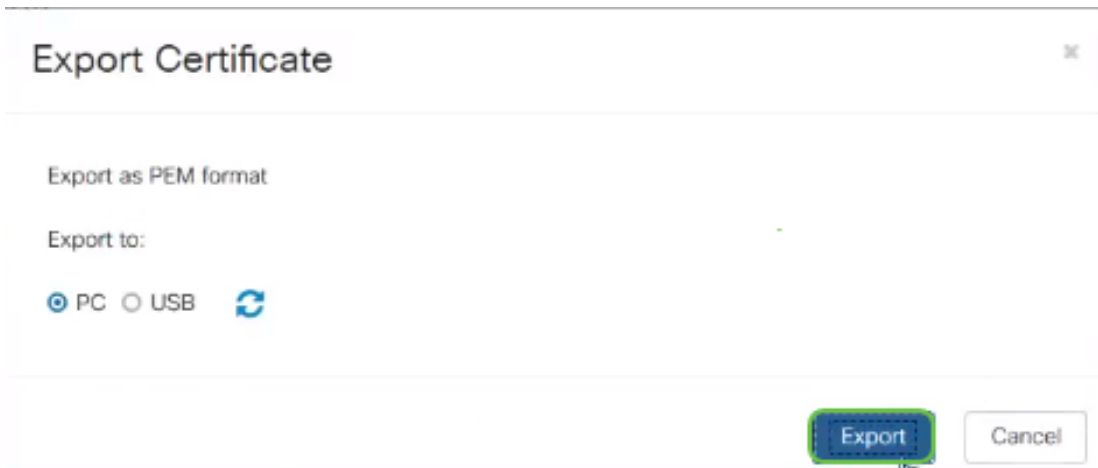
- 드롭다운 메뉴에서 Certificate Signing Request를 선택합니다.
- 인증서 이름 입력
- IP 주소, FQDN(Fully Qualified Domain Name) 또는 이메일을 입력합니다.IP 주소를 입력하는 것이 가장 일반적인 선택입니다.
- 국가 입력
- 상태 입력
- 구/군/시 이름 입력
- 조직 이름 입력
- 조직 단위 이름 입력
- 이메일 주소 입력
- Enter Key Encryption Length, 2048을 사용하는 것이 좋습니다.

오른쪽 위의 **Generate** 버튼을 클릭합니다.

4단계. 작업 아래의 위쪽 화살표를 클릭하여 내보내려면 선택합니다.



5단계. 이 화면이 나타납니다.Export(내보내기)를 클릭합니다.



6단계. 드롭다운 메뉴에서 *Open with*(열기)와 *Notepad*(메모장)(기본값)를 선택합니다.확인을 클릭합니다.

You have chosen to open:

 AnthonyRouter.pem

which is: PEM file (1.2 KB)

from: blob:

What should Firefox do with this file?

Open with: Notepad (default)

Save File

Do this automatically for files like this from now on.

OK

Cancel

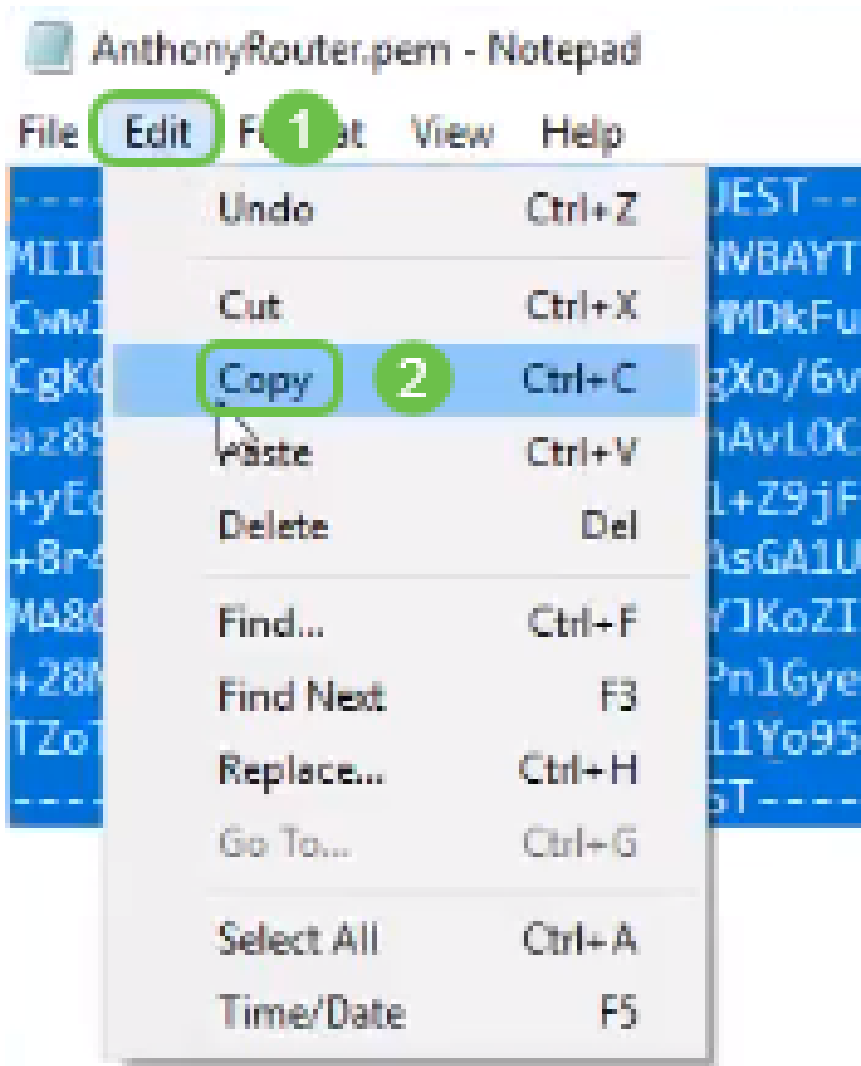
7단계. XML 파일이 열립니다.



```
AnthonyRouter.pem - Notepad
File Edit Format View Help
-----BEGIN CERTIFICATE REQUEST-----
MIIDYTCBAAkCAQAwZ2cxZ2c3ZjBhbnVAYTA1VTMRUWVwYDQVQ0IDAxTb3V0aCBEYWtvdGExFDASBgNVBACMC1Npb3V4IEZhbGxzMQ4wDAYDVQQKDAVkaXJibzERMhMGA1UE
Cw:GhvbGkU91dGVyMR8wHQYjKoZIHvcIAQkBFHhcmVubGJw0BAQEFAAOCAQ8AMIIB
CgKCAQEApZLPhuMow2Ig5vM7b1gXo/6vnp1BYn1HKMDkcnLz#CroCdqRcEjEe17XYGLsR9LXt61F1JGkaQOrRpLyz7n11jRoLOBsZaeV30/bFDW0FF6X1DxOpeAyNs
az85o3RgkIoCyrngNWUj1yEE91ThAvLOCepd+BPjFpyE5j]akrBDL47n9rv4M9dNL/WXPD5tVxLw23+vFntDh821tzyJ921hVb3dfZ42yZfEw+xjWln/N
+yEd51bVH1P6TyqK2bD0eEs1xs1+Z9jF1ac3Gw6CFDYXg09C0ja8x1qgBasGcrwnJaycF+WB0LSs41UrwIDAQABoIGDMIGABgkqhkiG9w0BCQ4xcccBxMakGA1UdEwQCMwHqQDVROB0BBYEFFPI
+8r4zePCPInbvS4HYdDpQcwz0MAsGA1UdDwQEAwIF4DAnBgIvH5UEID0AeBgggrBGF8QcDAQYIKwYBBQUHwIICCSsGAQUFCAIC
MhMGA1UdEQQIMAAhBMCoASgwDQYKoZIHvcIAQELBQ40ggEBAF2+aV44sZy0N0MntaMj49GnKChXMI3wFUXYYVsgo0wN1XY5nUzmDQg15jE1
+28MBtJ0YuThSLMpatb1c6zUzPn1GyemQz+JRjN/RNq5NH5L70sd8jwad0ZXXp6XpZ+mK5pm6vA1e0ef3mdJ/R+rP2AHb+1iRVWrrqq0wh5f]swRS2HEon4
TZoTKf0XBcMTWpCh1jPFyALeMhB11Yo95aB02WX2e+9vI0T5xgVae2wFomPHB0sUvcUNT4jUzYnlyS7XkREz7oY1PF5TZn9KzAIoZn8aQbNUqNtXJqFm41F01cMUys73q0GM2M=
-----END CERTIFICATE REQUEST-----
```

참고:BEGIN CERTIFICATE REQUEST(인증서 요청 시작) 및 END CERTIFICATE REQUEST(인증서 요청 종료)가 각각 위에 나와 있는 것과 같은 고유한 행에 있는지 확인합니다.

8단계. 화면 상단에서 **Edit(편집)**를 클릭하고 드롭다운 메뉴에서 **Copy(복사)**를 선택합니다.



9단계. 인증서 요청을 위해 신뢰할 수 있는 서드파티 사이트를 선택합니다. 복사한 XML 파일을 요청의 일부로 붙여넣어야 합니다.

참고: 네트워크에 내부 인증서 서버가 있는 경우 이를 대신 사용할 수 있지만 이는 일반적이지 않습니다.

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
TZoTKHXBcMTWpCh1jPFyALeNH811Yo95aBO2WX2e  
cUNT4jUzYNYsV7XkREz7oY1PF5TZW9KzzAIoZW8a  
3qO6K2H=  
  
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Web Server

Additional Attributes:

Attributes:

Submit >

10단계. 확인되면 **인증서 다운로드**를 선택할 수 있습니다.

Certificate Issued

The certificate you requested was issued to you.

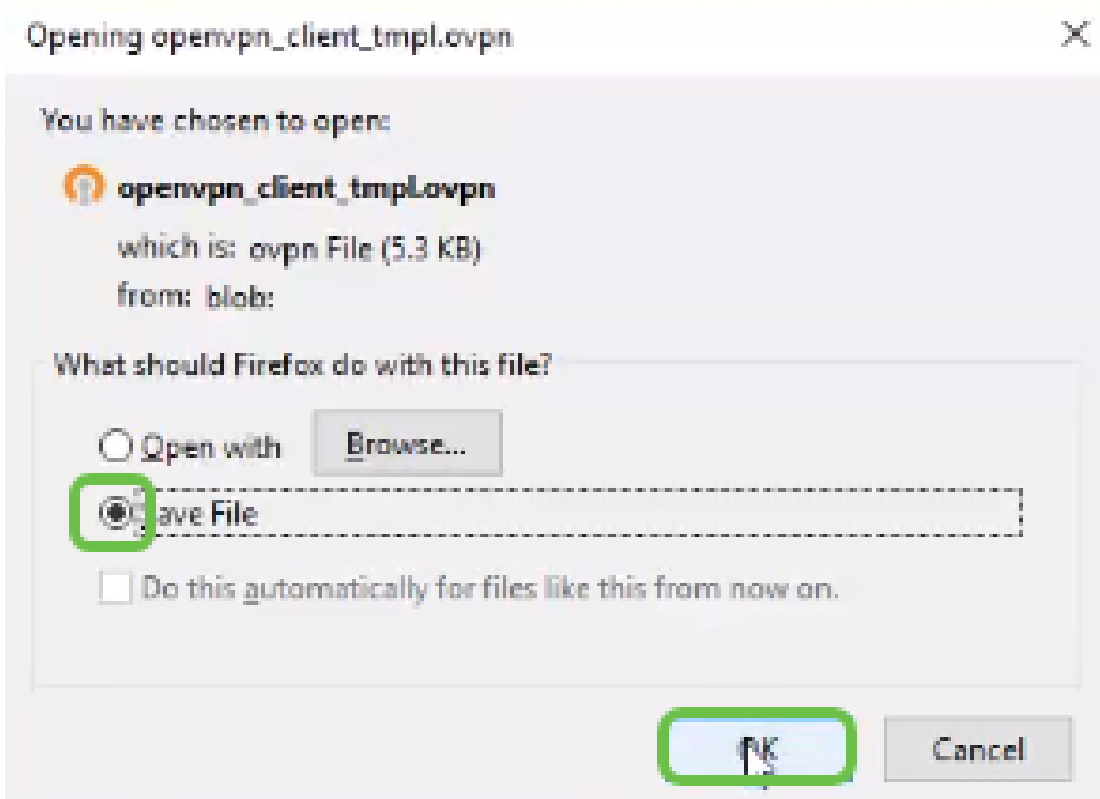
DER encoded or Base 64 encoded



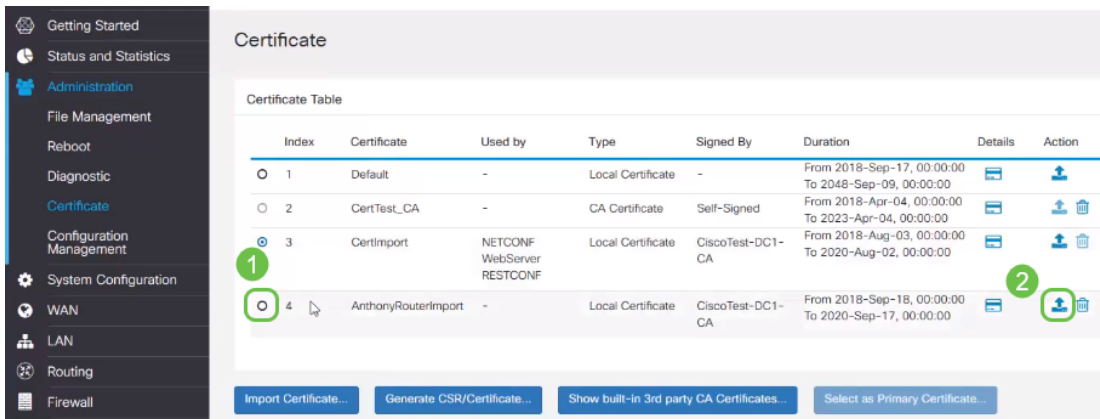
[Download certificate](#)

[Download certificate chain](#)

11단계. 라디오 버튼을 클릭하여 **파일을 저장하고 확인**을 클릭합니다.



12단계. 저장된 후에는 해당 인증서의 라디오 버튼을 선택하고 아래쪽 화살표 아이콘을 클릭합니다



13단계. 이 화면이 열립니다. 찾아보기 선택....

Import Signed-Certificate



Type: Local Certificate

Certificate Name:

Upload Certificate file

Import from PC

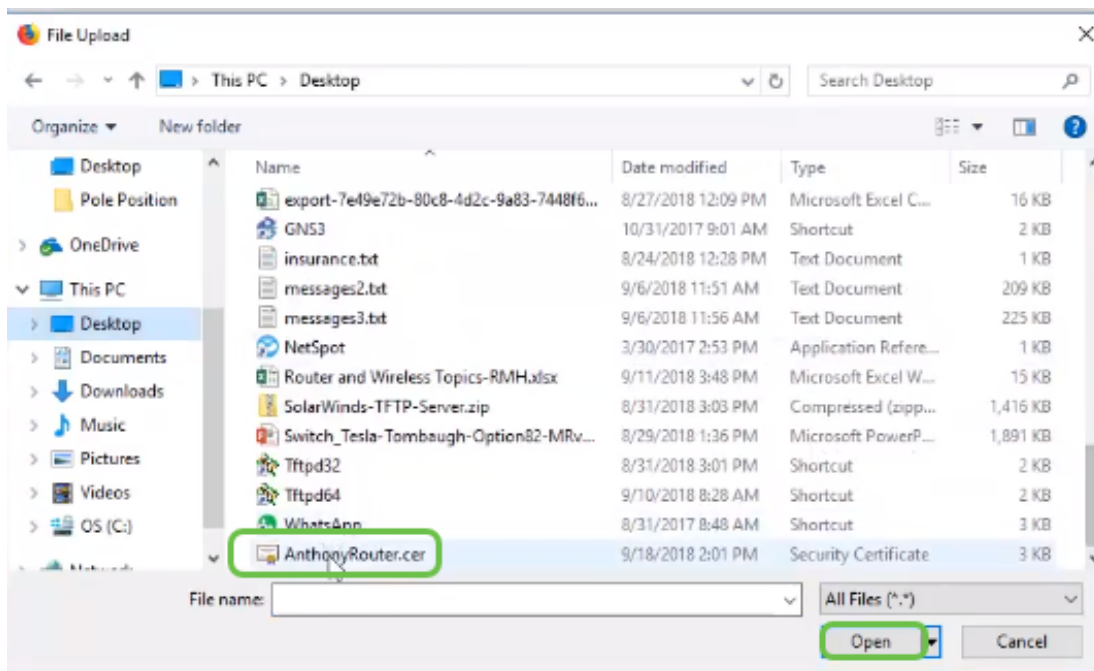
No file is selected

Import from USB



No file is selected

14단계. 인증서의 파일을 선택하고 열기를 클릭합니다.



15단계. 가져올 인증서 이름을 입력하고 업로드를 클릭합니다.

Import Signed-Certificate

Type: Local Certificate

Certificate Name: AnthonyRouterImport

Upload Certificate file

Import from PC

Browse...

AnthonyRouter.cer

Import from USB



Browse...

No file is selected

Upload

Cancel

16단계. 인증서를 성공적으로 가져왔다는 알림을 받게 됩니다. 확인을 클릭합니다.

Information

Import certificate successfully!

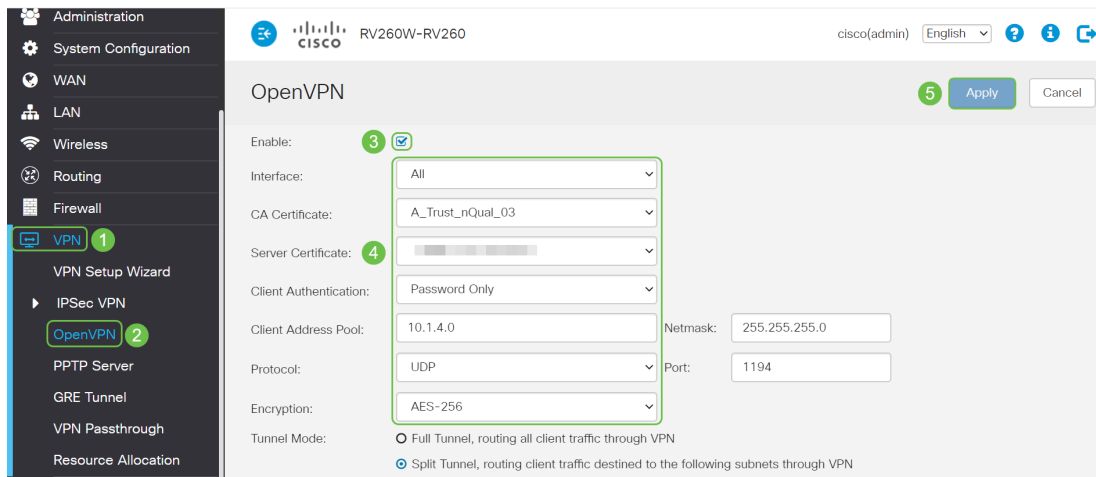
OK

17단계. Administration(관리) > Certificate(인증서)로 이동합니다. 인증서가 로드되었습니다.

참고: 이 예에서는 로컬 인증서 서버가 사용되었습니다.

Index	Certificate	Used by	Type	Signed By	Duration	Details	Action
1	Default	-	Local Certificate	-	From 2018-Sep-17, 00:00:00 To 2048-Sep-09, 00:00:00		
2	CertTest_CA	-	CA Certificate	Self-Signed	From 2018-Apr-04, 00:00:00 To 2023-Apr-04, 00:00:00		
3	Certimport	NETCOM WebServer (823004)	Local Certificate	CiscoTest-OC1-CA	From 2018-Aug-03, 00:00:00 To 2020-Aug-02, 00:00:00		
4	AnthonyRouterImport	-	Local Certificate	CiscoTest-OC1-CA	From 2018-Sep-18, 00:00:00 To 2020-Sep-17, 00:00:00		

18단계. VPN > OpenVPN으로 이동합니다. OpenVPN 페이지가 열립니다. 다음 정보를 입력합니다.



- Enable(활성화) 상자를 선택합니다.트래픽에서 허용할 인터페이스를 선택합니다.이 경우 WAN(Wide Area Network)에서 CA(Certificate Authority) 인증서를 선택합니다.
- 드롭다운 메뉴에서 CA 인증서를 선택합니다.
- 드롭다운 메뉴에서 다운로드한 서버 인증서를 선택합니다.
- Client Authentication을 선택합니다.Password(비밀번호)를 선택하면 비밀번호로 인증해야 합니다.Password + Certificate를 선택하는 경우 클라이언트에도 인증서가 있어야 합니다.이는 더 안전하지만 별도의 CA를 구매해야 하므로 VPN 비용이 추가됩니다.
- 클라이언트 주소 풀을 입력합니다.회사 내 다른 곳에서 사용되지 않는 네트워크 서브넷의 IP 주소를 선택합니다.예약된 범위 중에서 선택하고 다른 곳에서 사용되지 않는 범위를 선택합니다.
- 암호화 형식을 선택합니다.암호화가 클라이언트와 동일한지 확인합니다.DES 및 3DES는 권장되지 않으며 이전 버전과의 호환성에만 사용해야 합니다.
- VPN을 통과하는 트래픽만 지정하려면 모든 클라이언트 트래픽이 VPN 또는 Split 터널을 통과하도록 하려면 Full Tunnel Mode(전체 터널 모드)를 선택합니다.
- DNS 1 IP 주소는 전용 내부 DNS 서버, ISP(인터넷 서비스 공급자)가 제공한 기본 게이트웨이의 동일한 IP 주소, 가상 컴퓨터 또는 인터넷의 신뢰할 수 있는 DNS 서버가 될 수 있습니다.

Apply(적용)를 클릭하여 컨피그레이션을 저장합니다.

19단계(옵션 1). 이 컨피그레이션을 클라이언트에 이메일로 보낼 수 있습니다.Send Email(이메일 보내기) 확인란을 선택합니다.이메일 주소를 입력합니다.이메일의 제목 제목을 추가합니다 .Generate를 클릭합니다.

Export setting:

Include client certificate: AnthonyRouterImport

Please choose the method you want to export:

1 Export client configuration template (.ovpn)

Send Email Click [here](#) to configure Email settings.

Email client configuration template (.ovpn) to recipients (multiple email addresses separated by comma): nick@cisico.com

Email Subject: OpenVPN Client Config

4 Generate

20단계(옵션 2). Export *client configuration template (.ovpn)*(클라이언트 컨피그레이션 템플릿 내보내기(.ovpn))를 선택하고 Generate(생성)를 클릭합니다.

Export setting:

Include client certificate:

Please choose the method you want to export:

1 Export client configuration template (.ovpn)

Send Email Click [here](#) to configure Email settings.

Email client configuration template (.ovpn) to recipients (multiple email addresses separated by comma): input email address

Email Subject: OpenVPN Client Configurat

2 Generate

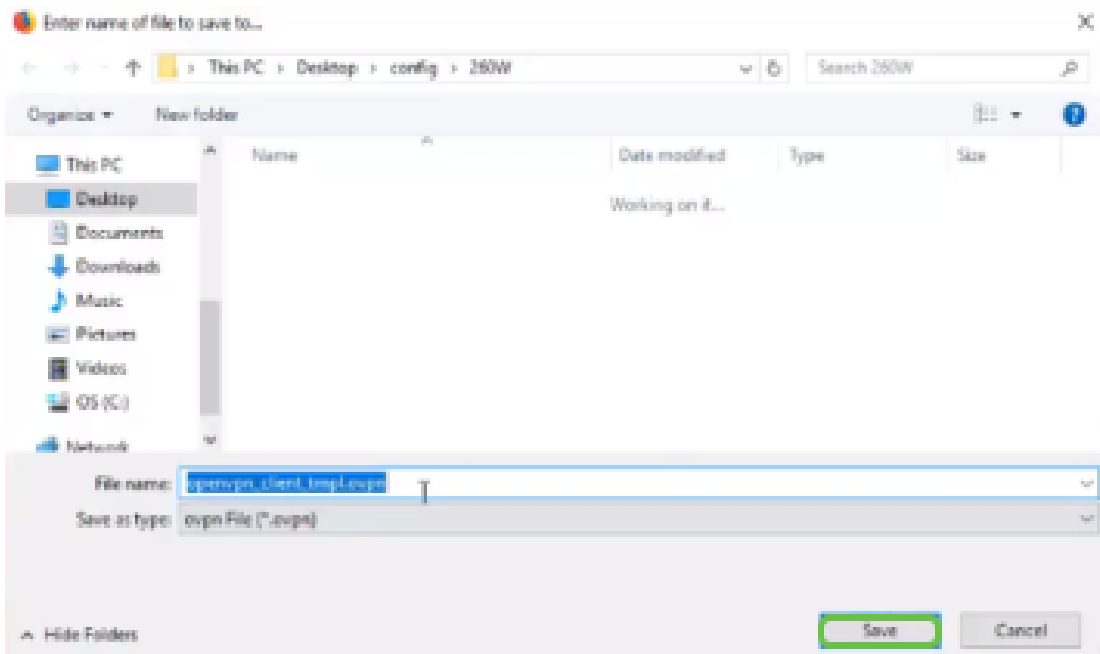
21단계. 성공적으로 확인되었습니다.확인을 클릭합니다.

Information

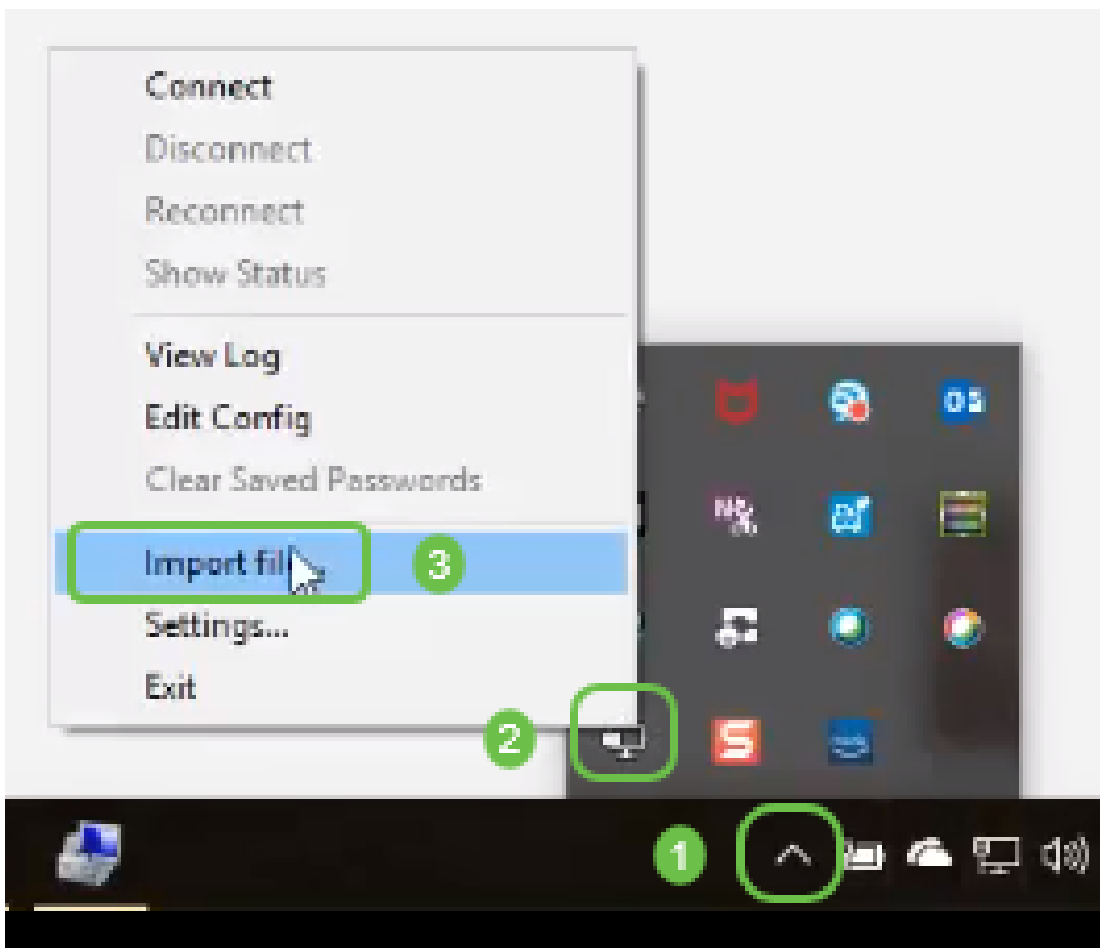
 Export client configuration template downloaded successfully!

OK

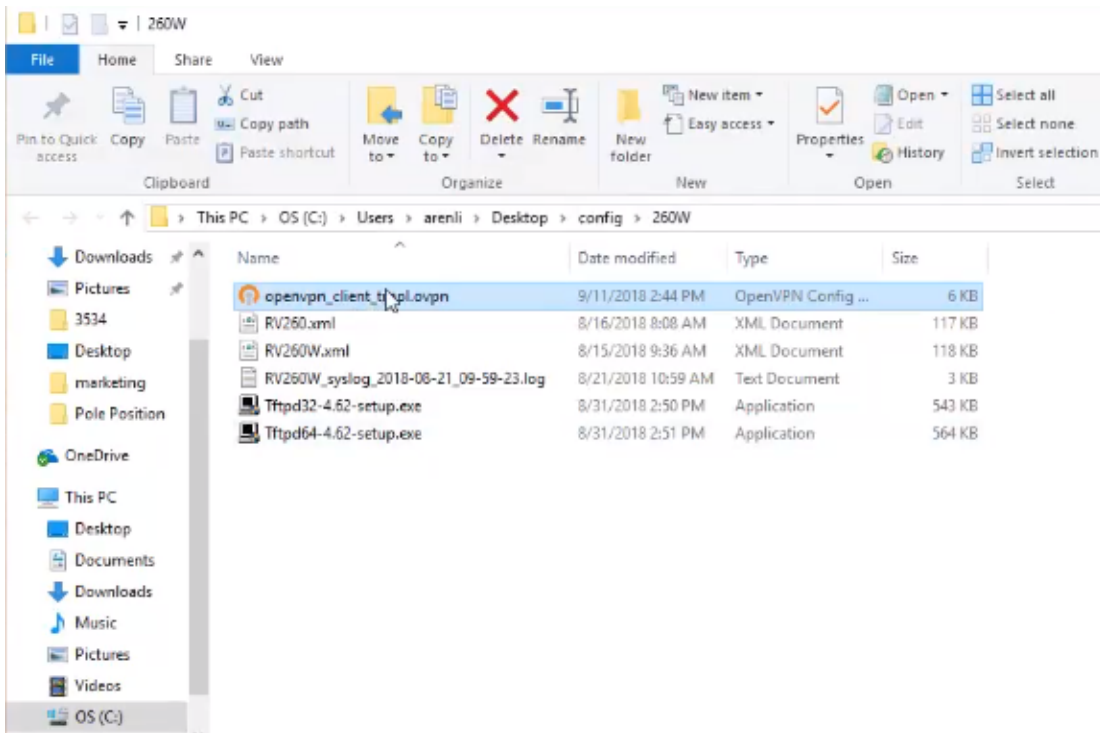
22단계. 저장을 클릭합니다.



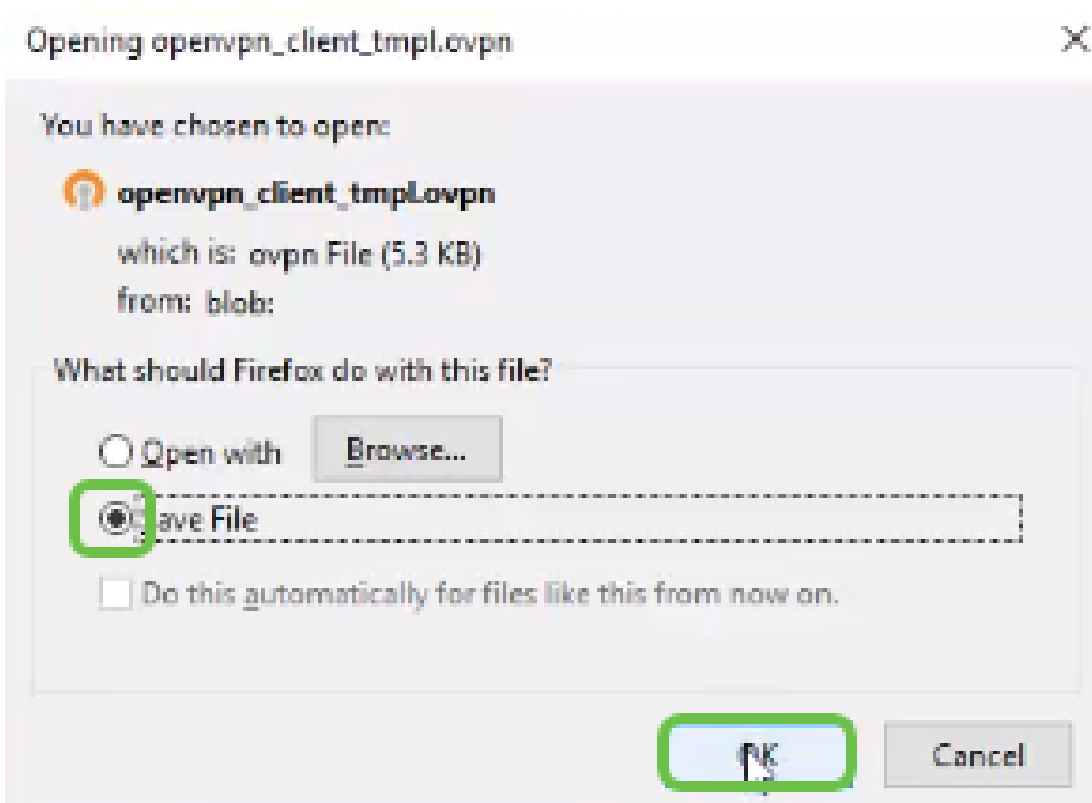
23단계. 바탕 화면 오른쪽 하단에서 OpenVPN을 열려면 클릭합니다.마우스 오른쪽 버튼을 클릭하여 드롭다운 메뉴를 엽니다.Import File을 클릭합니다.



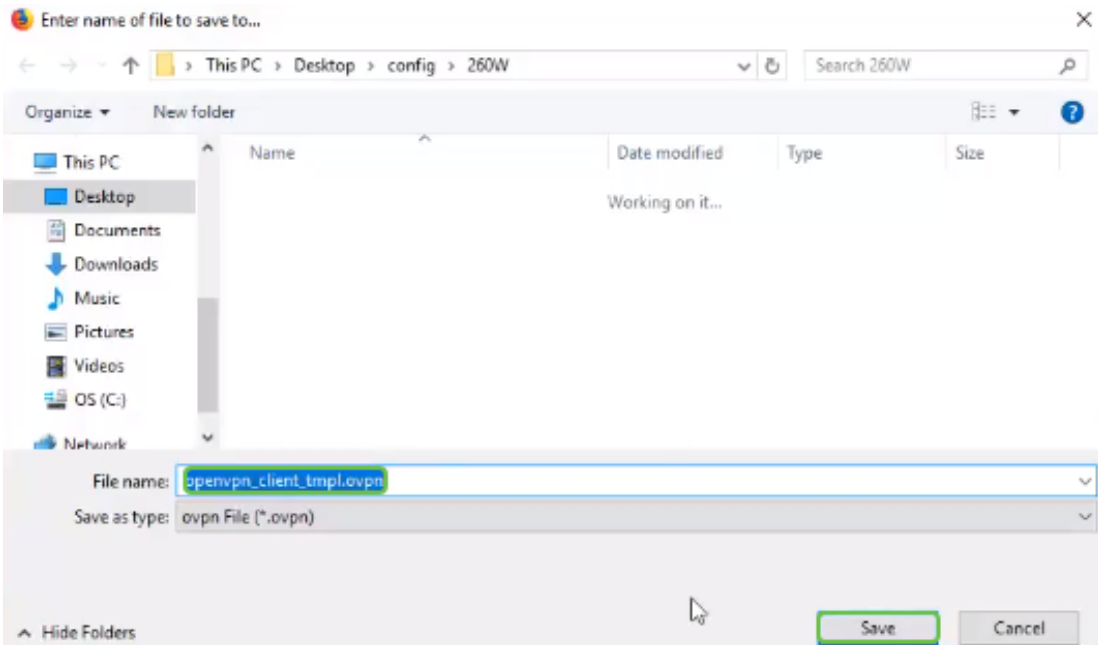
24단계. .ovpn으로 끝나는 OpenVPN 파일을 선택합니다.



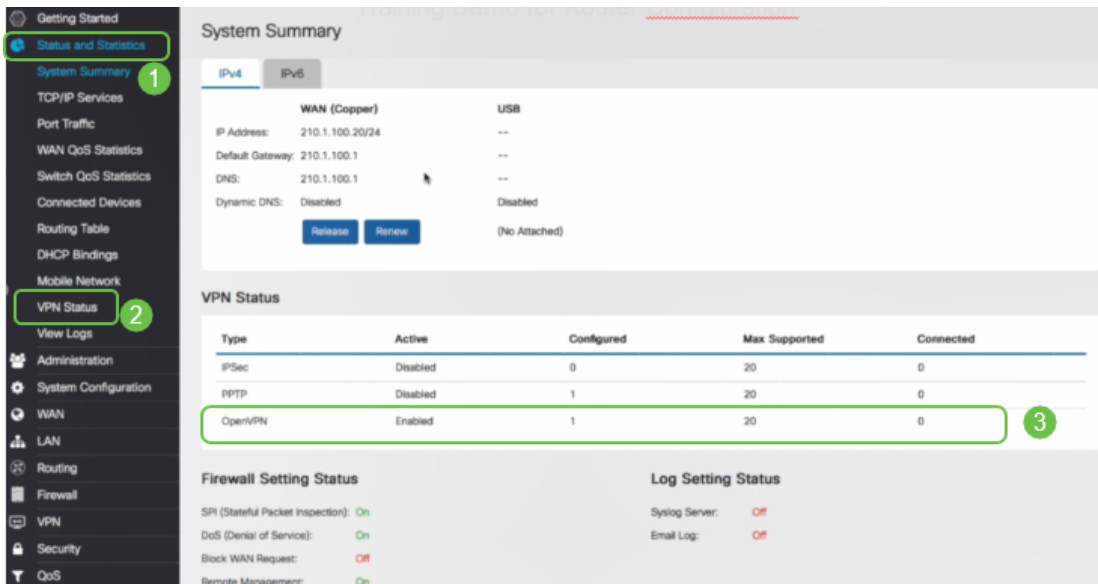
25단계. 파일 저장 라디오 버튼을 클릭하고 확인을 클릭합니다.



26단계. 선택한 경우 파일 이름을 변경하고 .ovpn을 파일 이름 끝에 둡니다.저장을 클릭합니다.



27단계. Status and Statistics(상태 및 통계) > VPN Status(VPN 상태)로 이동합니다.아래로 스크롤 하여 자세한 정보를 확인할 수 있습니다.



이제 라우터가 개인 평가판의 OpenVPN 클라이언트 연결을 지원하는 데 필요한 모든 매개 변수로 구성됩니다.

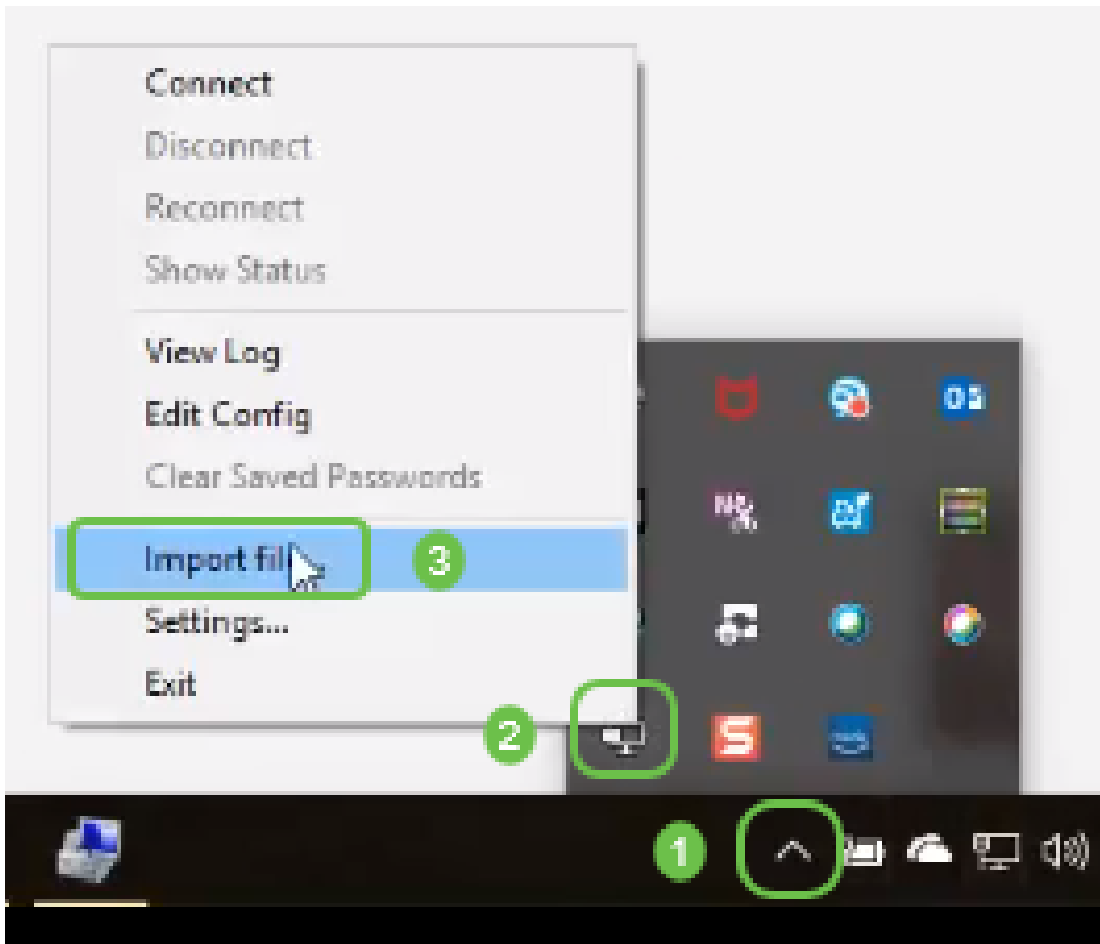
컴퓨터에 OpenVPN 클라이언트 설정

각 OpenVPN 클라이언트는 사전 요구 사항으로 다음 작업을 수행해야 합니다.

- 디바이스에서 OpenVPN 애플리케이션을 다운로드합니다.
- 이전 섹션의 19-22단계에서 전송된 구성 파일을 열고 저장합니다.구성 파일이 .ovpn으로 끝납니다.

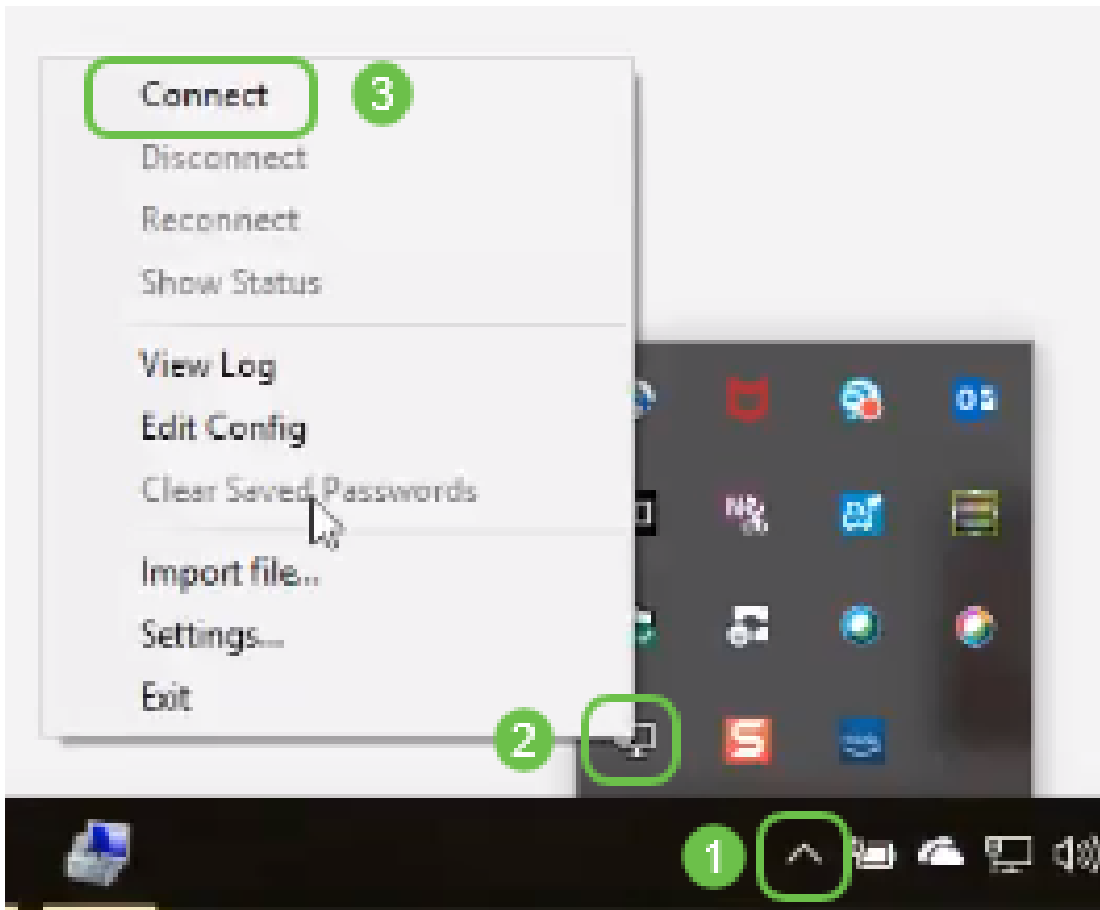
참고:이 설정은 Windows 10용으로 특별히 사용됩니다.

1단계. 바탕 화면 오른쪽 하단에 있는 화살표 아이콘으로 이동한 다음 클릭하여 OpenVPN 아이콘을 엽니다.마우스 오른쪽 버튼을 클릭하고 **파일 가져오기**를 선택합니다.

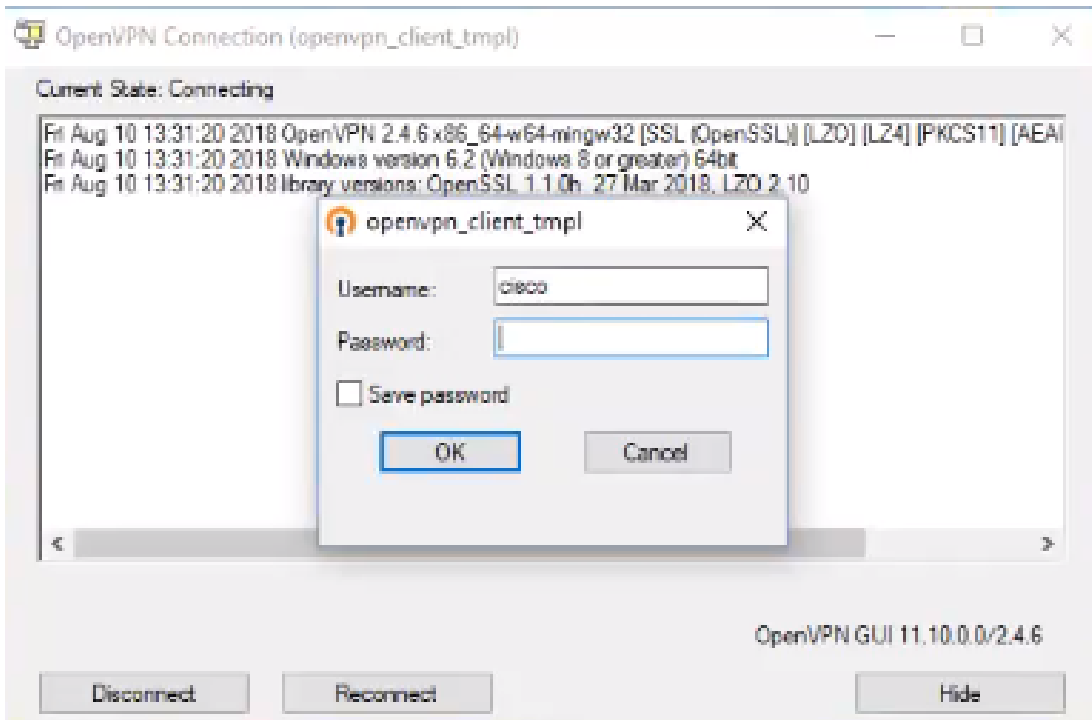


참고:아이콘은 현재 실행되고 있지 않음을 나타내는 흑백입니다.아이콘을 실행하면 색상이 표시됩니다.

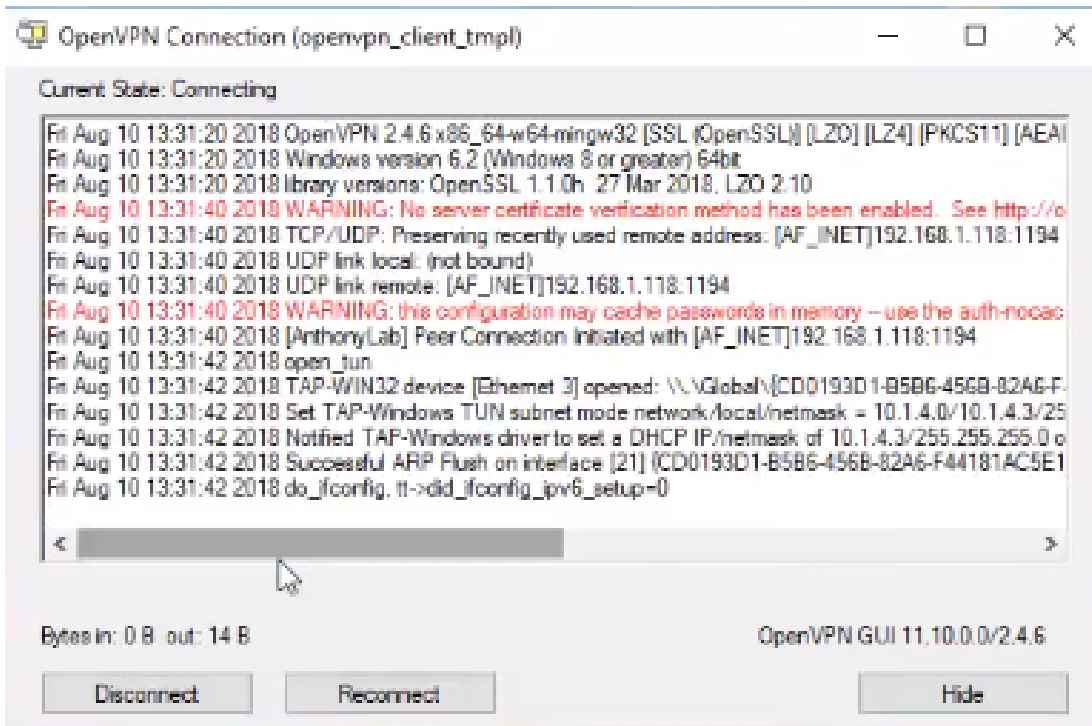
2단계. 위쪽 화살표를 클릭합니다.OpenVPN 아이콘을 클릭합니다.마우스 오른쪽 버튼을 클릭하고 드롭다운 메뉴에서 Connect를 선택합니다.



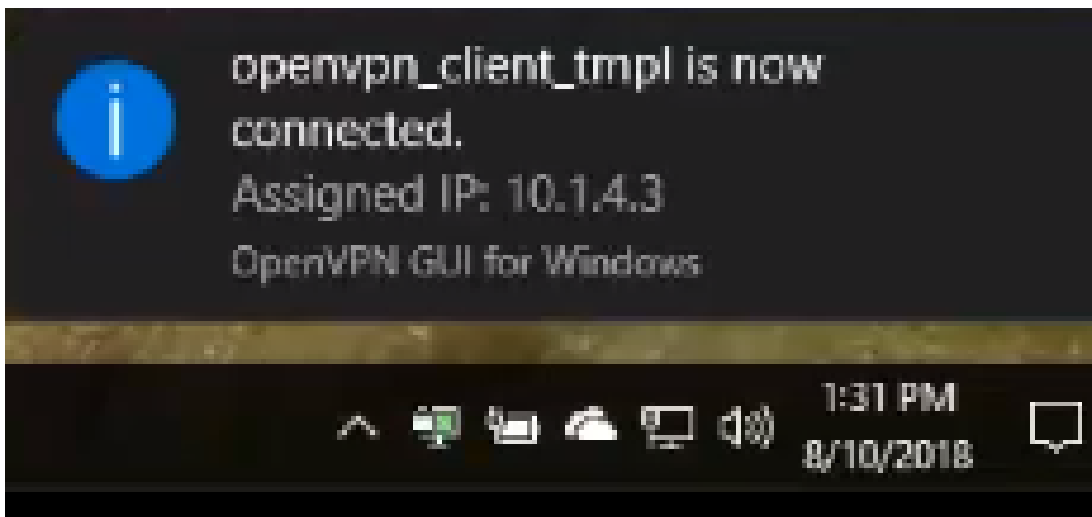
3단계. 사용자 이름 및 비밀번호를 입력합니다.



4단계. 창에 일부 로그 데이터와 함께 연결된 OpenVPN이 표시됩니다.

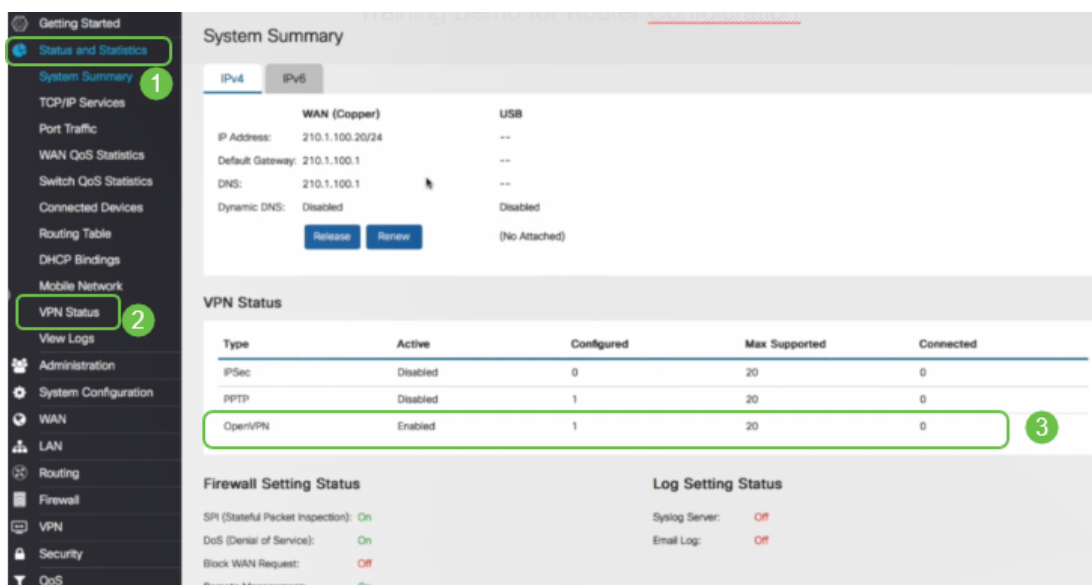


5단계. 시스템 로그에 연결이 있음을 알려야 합니다.



6단계. VPN 클라이언트는 OpenVPN을 통해 수신 및 발신 정보를 안전하게 터널링할 수 있어야 합니다. OpenVPN 설정에서 자동으로 연결하도록 설정할 수 있습니다.

7단계. 관리자는 라우터에서 **Status and Statistics(상태 및 통계) > VPN Status(VPN 상태)**로 이동하여 VPN Status(VPN 상태)를 확인할 수 있습니다.



결론

이제 RV160 또는 RV260 라우터와 VPN 클라이언트 사이트에 OpenVPN을 성공적으로 설치해야 합니다.

OpenVPN에 대한 커뮤니티 토론을 보려면 [여기](#)를 클릭하고 OpenVPN을 검색합니다.

이 문서와 관련된 비디오 보기...

[여기를 클릭하여 Cisco의 다른 기술 대화를 확인하십시오.](#)