

RV160和RV260路由器上的OpenVPN

目標

本文的目的是指導您在RV160或RV260路由器上設定OpenVPN，以及在電腦上設定OpenVPN的VPN客戶端。

適用裝置

- RV160
- RV260

軟體版本

- 1.0.00.15

目錄

[在RV160/RV260路由器上設定演示OpenVPN](#)

[在RV160/RV260路由器上設定OpenVPN](#)

[設定演示OpenVPN後使用自簽名證書登入](#)

[電腦上的OpenVPN客戶端設定](#)

簡介

OpenVPN是一個免費的開源應用程式，可以設定並用於虛擬專用網路(VPN)。它使用客戶端 — 伺服器連線，通過網際網路在伺服器和遠端客戶端位置之間提供安全通訊。

OpenVPN使用OpenSSL對UDP進行加密，使用TCP進行流量傳輸。VPN提供安全保護隧道，對通過VPN連線從您的電腦傳送的資料進行加密，因此不易受到駭客攻擊。例如，如果您在公共場所（如機場）使用WiFi，它會使您的資料、事務和查詢不會被其他使用者看到。與HTTPS非常相似，它加密在兩個端點之間傳送的資料。

設定OpenVPN最重要的步驟之一是從證書頒發機構(CA)獲取證書。這用於身份驗證。可以從任意數量的第三方站點購買證書。這是證明您的站點安全的官方方式。實質上，CA是受信任的來源，用於驗證您的企業是否合法以及是否值得信任。對於OpenVPN，您只需要最低成本的較低級證書。您會由CA簽出，他們驗證您的資訊後，會向您頒發證書。此證書可以作為檔案下載到您的電腦上。然後，您可以進入您的路由器（或VPN伺服器）並上傳到那裡。請注意，客戶端不需要證書即可使用OpenVPN，它只是通過路由器進行驗證。

必要條件

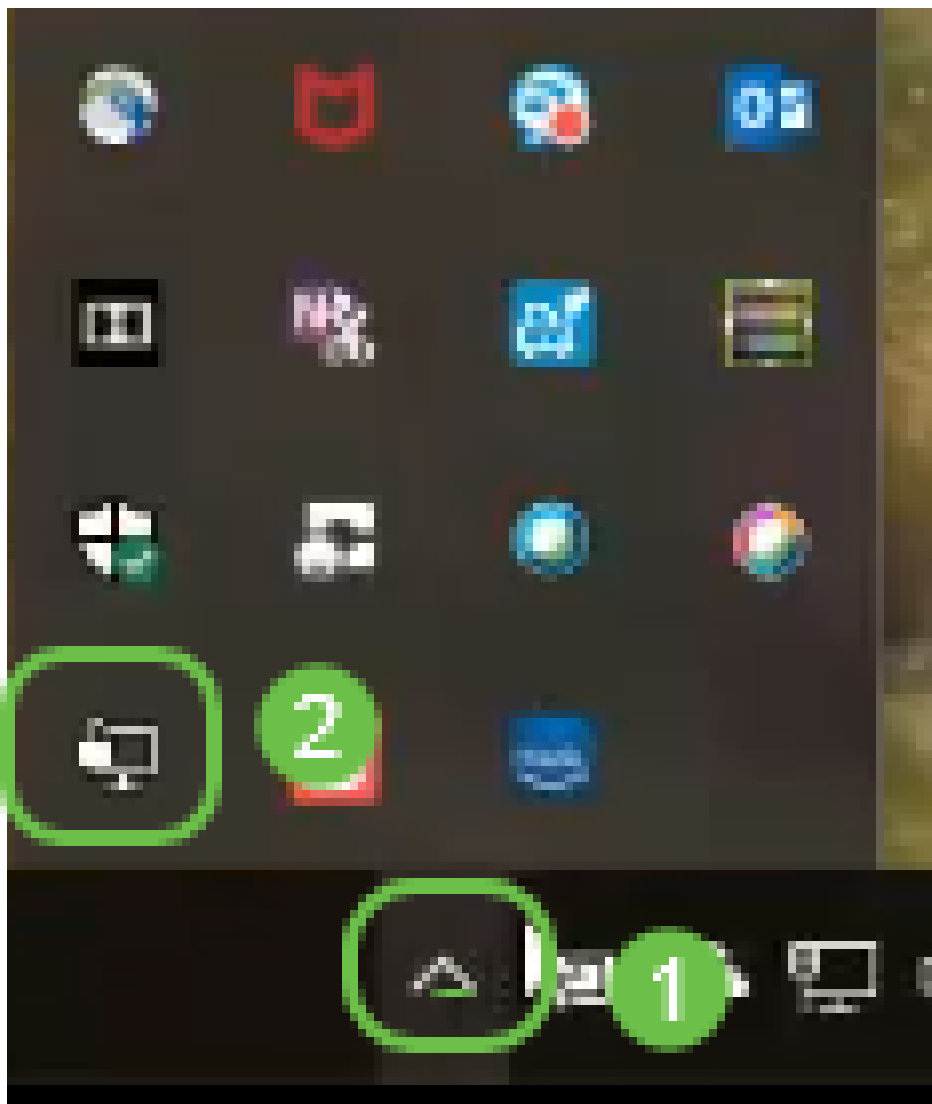
在系統上安裝OpenVPN應用程式。按一下[此處](#)以轉到OpenVPN網站。

有關OpenVPN的詳細資訊以及許多問題的答案，請按一下[此處](#)。

附註：此安裝程式特定於Windows 10。



安裝OpenVPN後，該應用程式應顯示在您的案頭上，或作為小圖示顯示在工作列的右側。OpenVPN客戶端也需要安裝此程式。



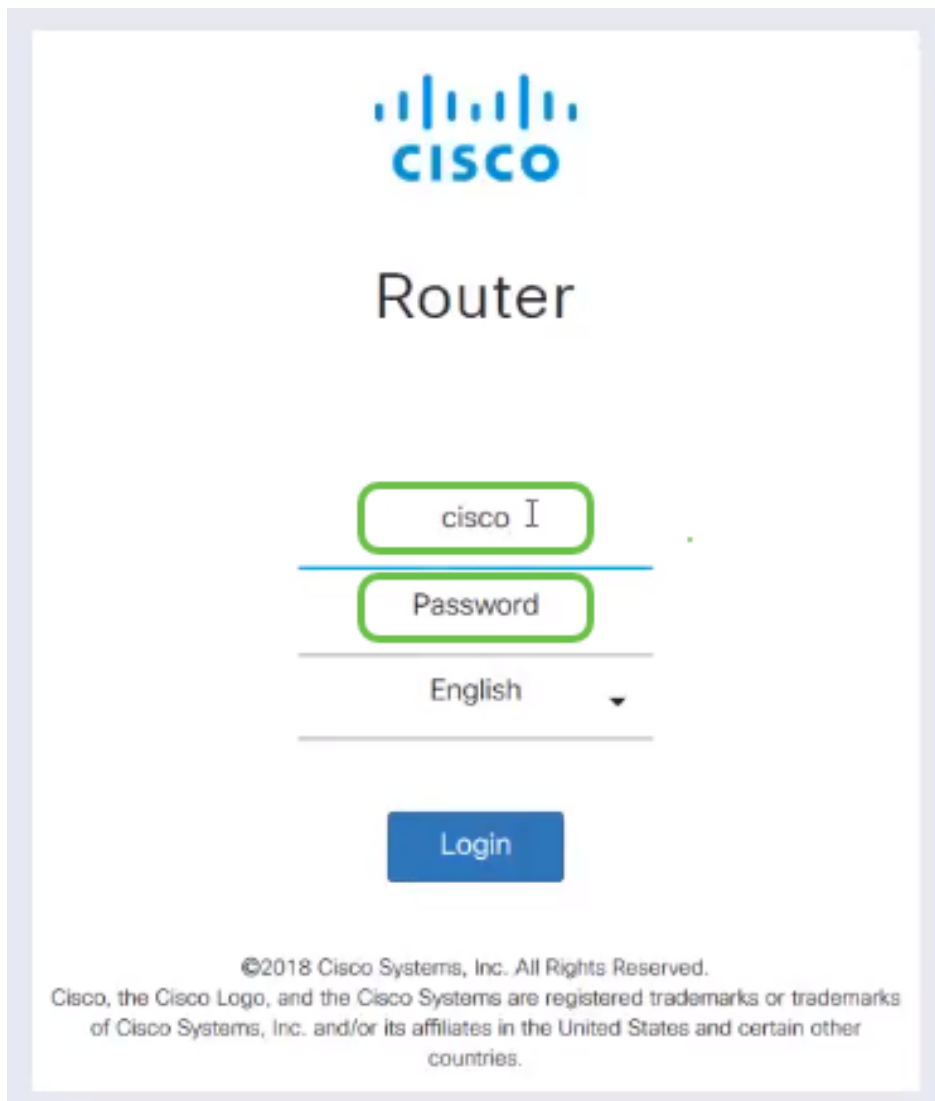
確保在所有裝置上設定了正確的系統時間。建立證書之前，必須在路由器上完全同步正確的系統時間。這通常是自動完成的，但如果您遇到問題，這是一個很好的檢查位置。

在RV160/RV260路由器上設定演示OpenVPN

如果您想在支付CA費用之前嘗試OpenVPN，可以建立自簽名證書。這是一種免費的方法，可以瞭解您是否希望為您的企業部署OpenVPN。如果您已經知道要購買CA，則可以跳過本文此部分，直接轉至[在RV160/RV260路由器上設定OpenVPN](#)。

步驟1.使用您的憑證登入路由器。預設使用者名稱和密碼為cisco。

附註：強烈建議您將所有密碼更改為更複雜的密碼。否則，就像把鎖門的鑰匙留在門口一樣。



步驟2.需要在路由器上取得憑證。導覽至Administration > Certificate > Generate CSR/Certificate... 這是建立憑證請求的方法。



步驟3.請求CA憑證。

- 從下拉選單中選擇 *CA Certificate*
- 輸入證書名稱
- 輸入IP地址、完全限定域名(FQDN)或電子郵件。輸入IP地址是最常見的選擇。
- 輸入您的國家/地區
- 輸入您的州/省
- 輸入您的地區名稱，通常是您的城市
- 輸入組織名稱
- 輸入組織單位名稱
- 輸入您的電子郵件地址
- 輸入金鑰加密長度，建議使用2048

按一下右上角的**Generate**按鈕。

步驟4.您還需要伺服器證書。此CA證書簽名的證書將由您剛建立的CA證書簽名。

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	CertT	-	CA Certificate	Self-Signed	From 2018-Apr-04, 00:00:00 To 2023-Apr-04, 00:00:00		
3	CertImport	NETCONF WebServer RESTCONF	Local Certificate	CiscoTest-DC1-CA	From 2018-Aug-03, 00:00:00 To 2020-Aug-02, 00:00:00		
4	AnthonyRouterIm...	-	Local Certificate	CiscoTest-DC1-CA	From 2018-Sep-18, 00:00:00 To 2020-Sep-17, 00:00:00		

步驟5.請求由CA憑證簽署的憑證。

- 從下拉選單中選擇 *Certificate Signing Request*
- 輸入證書名稱
- 輸入IP地址、完全限定域名(FQDN)或電子郵件。輸入IP地址是最常見的選擇。
- 輸入您的國家/地區
- 輸入您的州/省
- 輸入您的地區名稱，通常是您的城市
- 輸入組織名稱
- 輸入組織單位名稱
- 輸入您的電子郵件地址
- 輸入金鑰加密長度，建議使用2048
- 從下拉選單中選擇適當的證書頒發機構

按一下右上角的**Generate**按鈕。

步驟6.導覽至System Configuration > User Groups。選擇plus圖示以新增新組。

Group	Web Login /NETCONF /RESTCONF	Lobby Ambassa...	802.1x	S2S IPSec VPN	C2S IPSec VPN	OpenVPN	PPTP	Captive Portal
<input type="checkbox"/>	Ambassa...	Disable	Enable	Disable	Disable	Disable	Disable	Enable
<input type="checkbox"/>	admin	Admin	Enable	Enable	Enable	Enable	Enable	Enable
<input type="checkbox"/>	guest	Disable	Disable	Disable	Disable	Disable	Disable	Disable

步驟7.輸入組的名稱，按一下 *On* 單選按鈕開啟OpenVPN。按一下「Apply」。

User Groups

3 Apply Cancel

Group Name: OpenVPN 1

Local User Membership List

+

<input type="checkbox"/>	#	User

* Should have at least one account in the 'admin' group.

Services

Web Login/NETCONF/RESTCONF: Disable Readonly Admin

Site to Site VPN:

+

<input type="checkbox"/>	#	Connection Name

Client to Site VPN:

+

<input type="checkbox"/>	#	Group Name

OpenVPN: 2 On Off

PPTP VPN: On Off

802.1x: On Off

Lobby Ambassador: On Off

步驟8.在System Configuration (系統配置)選單中導航，然後按一下User Accounts。在Local Users下，按一下plus圖示。

- Getting Started
- Status and Statistics
- Administration
- System Configuration
- Initial Router Setup
- System
- Time
- Log
- Email
- User Accounts 1
- User Groups
- IP Address Groups
- SNMP
- Discovery-Bonjour
- LLDP
- Automatic Updates
- Schedules

User Accounts

Apply Cancel

Minimal Password Length: (Range: 0-64, Default: 8)

Minimal Number of Character Classes: (Range: 0-4, Default: 3)

The four classes are: uppercase (A,B,C...), lowercase (a,b,c...), numbers (1,2,3...) and special characters (!@#\$...).

The new password must be different from the current one.: Enabled

Password Aging Time: days (Range: 0-365, 0 means never expires)

Local Users


+

<input type="checkbox"/>	Username	Group
<input type="checkbox"/>	Test_Admin	Ambassador
<input type="checkbox"/>	cisco	admin
<input type="checkbox"/>	guest	guest

* Should have at least one account in the 'admin' group.

步驟9.填寫以下資訊。確保從下拉選單中選擇OpenVPN。按一下「Apply」。

Add user account

 The current minimum requirements are as follows

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

Username:

1

VPN

New Password:

●●●●●●●●

Confirm Password:

●●●●●●●●

Password Strength meter:



Group:

OpenVPN

2

Apply

Cancel

所有依賴項都已完成，現在可以為OpenVPN配置路由器。

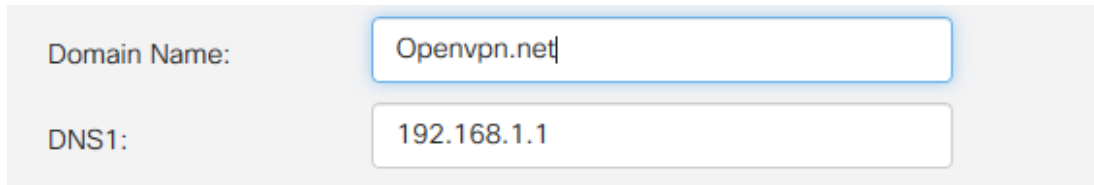
步驟10.導覽至VPN > OpenVPN。開啟OpenVPN頁面。填寫頁面上的每個框，確保從下拉選單中選擇以前建立的證書。

- 選中 *Enable* 框。選擇要允許流量進入的介面。在此案例中為廣域網(WAN)，然後選擇證書頒發機構(CA)證書。
- 從下拉選單中選擇 *CA Certificate*
- 從下拉選單中選擇下載的伺服器證書
- 選擇 *Client Authentication*。如果您選擇「密碼」，他們需要使用密碼進行身份驗證。如果選擇 Password + Certificate，則客戶端還必須具有證書。這樣更安全，但會增加VPN的成

本，因為它們需要購買單獨的CA。

- 輸入 *Client Address Pool*。選擇公司中其他任何位置未使用的網路子網上的IP地址。從保留範圍中選擇一個範圍，並選擇其它任何地方都不使用的範圍。
- 選擇 *Encryption* 的形式。確保加密與客戶端相同。建議不要使用DES和3DES，它們只能用於向後相容。
- 如果只想指定哪些流量通過VPN，請選擇Split tunnel。對於VPN，需要拆分隧道。如果您希望所有客戶端流量通過VPN，則在其他情況下會選擇全通道模式。

步驟11. 向下滾動頁面並填寫 *Domain Name* 和 *DNS1*。



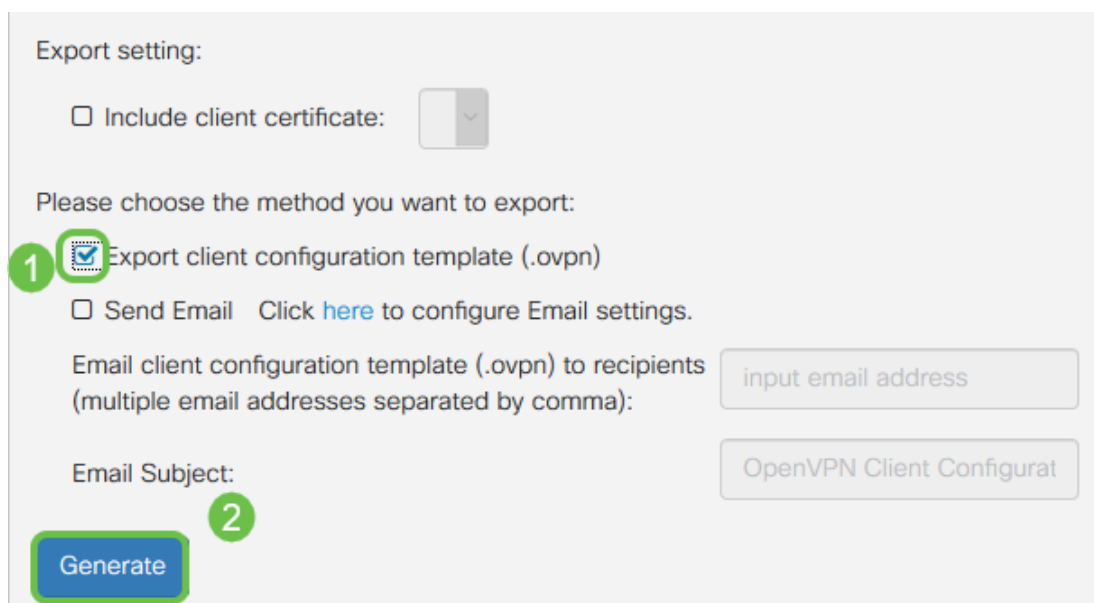
Domain Name:

DNS1:

注意： DNS1 IP地址可以是專用的內部DNS伺服器、網際網路服務提供商(ISP)提供的預設網關的相同IP地址、虛擬機器上的或網際網路上的受信任DNS伺服器。

步驟12. 按一下 **Apply**，在路由器上儲存組態。

步驟13. 停留在同一頁面上，然後進一步滾動。生成要安裝在OpenVPN客戶端上的配置模板。此檔案具有 *.ovpn* 副檔名，將由OpenVPN客戶端使用。選中 *Export client configuration template(.ovpn)* 覈取方塊，然後按一下 **Generate**。這會將檔案下載到您的電腦上。



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

步驟14. 導航到 **Status and Statistics > VPN Status**。您可以向下滾動以獲取更多詳細資訊。

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

本文的下一節將重點複習，因為它說明了如何使用自簽名證書登入。

設定演示OpenVPN後使用自簽名證書登入

使用自簽名證書登入時，在嘗試登入時可能會看到一個警告彈出視窗。您需要點選Advanced、Proceed、Trust或其他選項（取決於您的Web瀏覽器）才能繼續。

此時，您可能會收到警告，表示它不安全。您可以選擇繼續、新增例外或高級。這因網路瀏覽器而異。

在本示例中，Chrome用於Web瀏覽器。出現此消息，請按一下**Advanced**。



Your connection is not private

Attackers might be trying to steal your information from .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

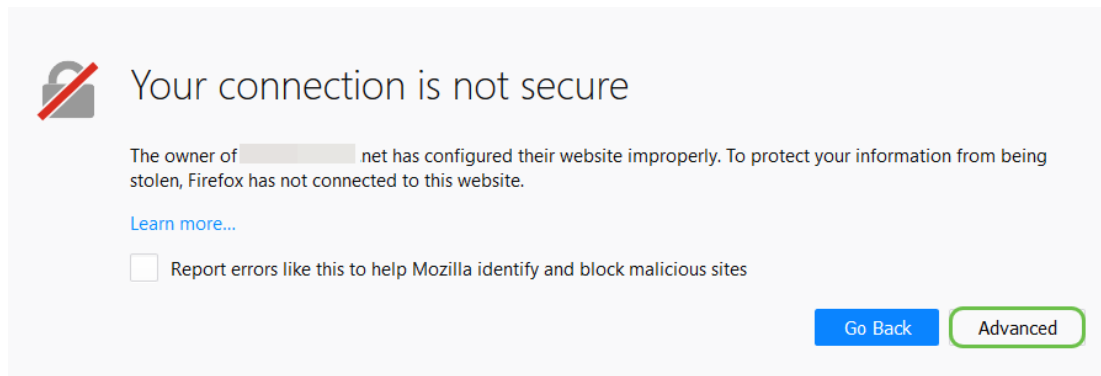
BACK TO SAFETY


將會開啟一個新螢幕，您需要按一下**Proceed to yourwebsite.net(unsafe)**(繼續訪問 (不安全))

This server could not prove that it is .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 .net (unsafe)

以下是使用Firefox作為Web瀏覽器時訪問裝置警告的示例。按一下「Advanced」。



 Your connection is not secure

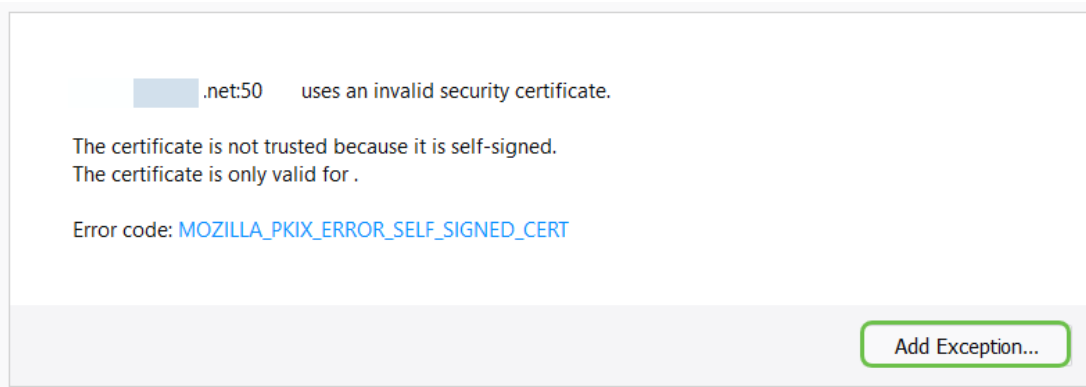
The owner of net has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

[Learn more...](#)

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

[Go Back](#) [Advanced](#)

按一下新增例外.....



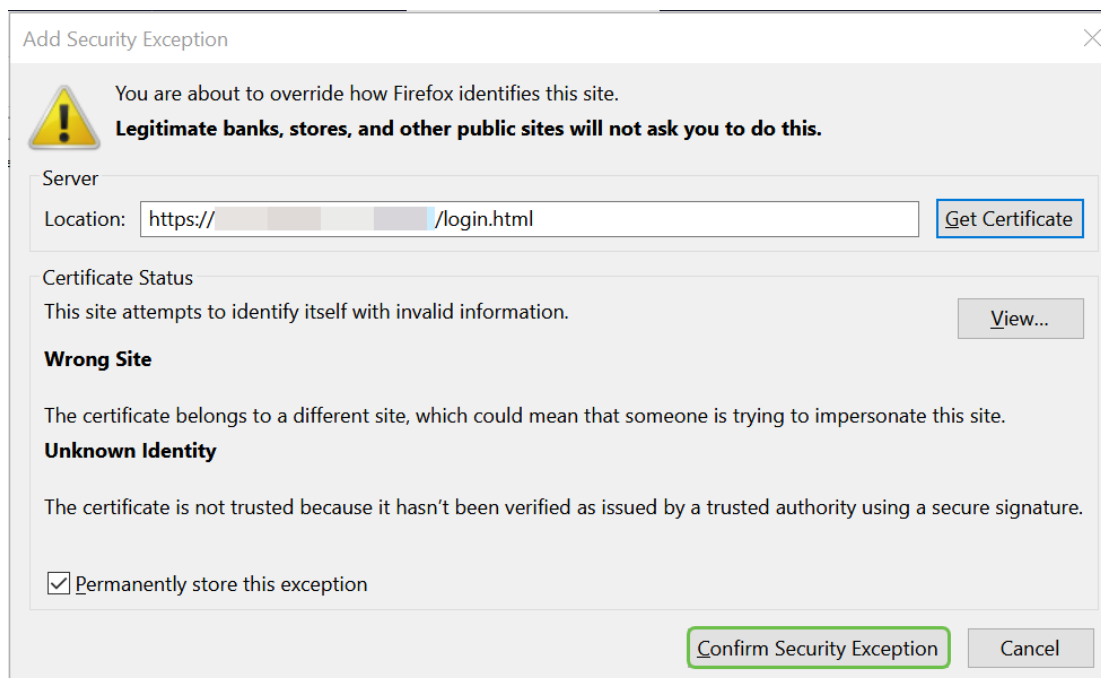
 .net:50 uses an invalid security certificate.

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...](#)

最後，您必須按一下確認安全例外。



Add Security Exception

 You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location: / /login.html"/> [Get Certificate](#)

Certificate Status

This site attempts to identify itself with invalid information. [View...](#)

Wrong Site

The certificate belongs to a different site, which could mean that someone is trying to impersonate this site.

Unknown Identity

The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a secure signature.

Permanently store this exception

[Confirm Security Exception](#) [Cancel](#)

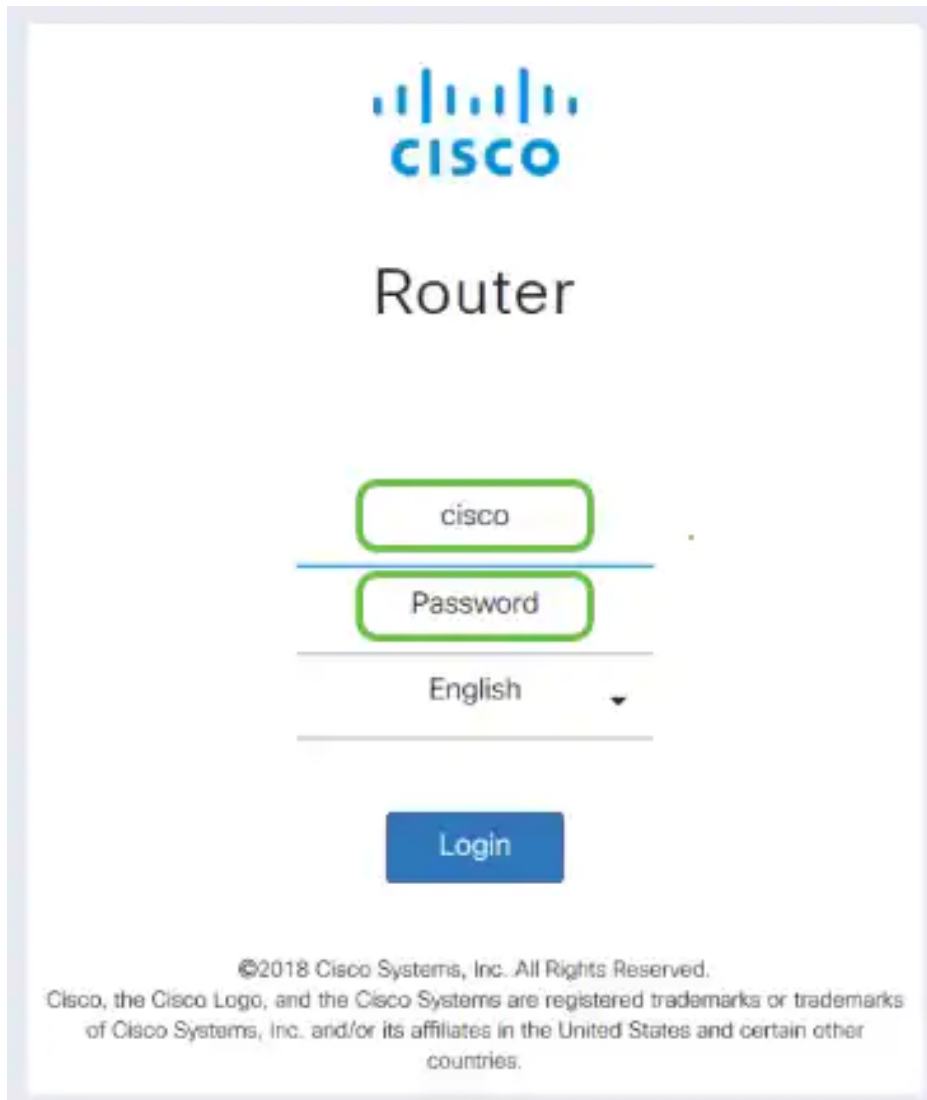
路由器現在配置了支援OpenVPN客戶端連線所需的所有引數。由於您已將客戶端配置模板下載到您的裝置(以.ovpn結尾的裝置)，因此您可以轉到[OpenVPN Client Setup on Computer](#)一節。如果您決定為貴公司部署OpenVPN，可以按照下一節中的步驟操作。

在RV160/RV260路由器上設定OpenVPN

這是一個更為複雜的過程，因為它涉及從第三方獲取CA，而這需要耗費資金。您還需要向所有客戶端傳送VPN客戶端配置模板(以.ovpn結尾)，以便它們可以在自己的裝置上設定。使用者端需要幾種與路由器相同的設定才能進行通訊。最棒的一點是，您和您的員工能夠以最低的成本使用網際網路，更安全地開展業務。

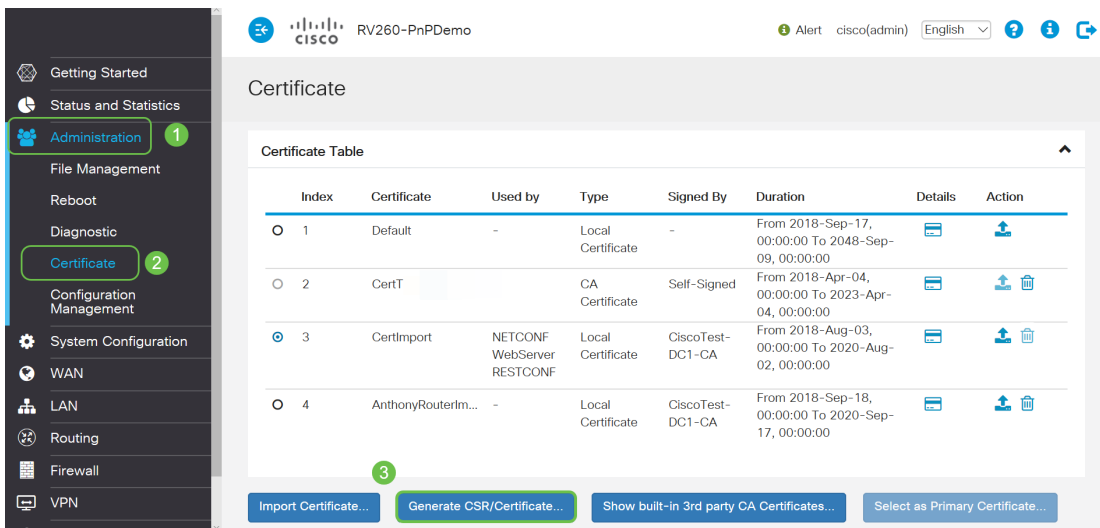
步驟1.使用您的憑證登入路由器。預設使用者名稱和密碼為*cisco*。

附註：強烈建議您將所有密碼更改為更複雜的密碼。否則，就像把鎖門的鑰匙留在門口一樣。

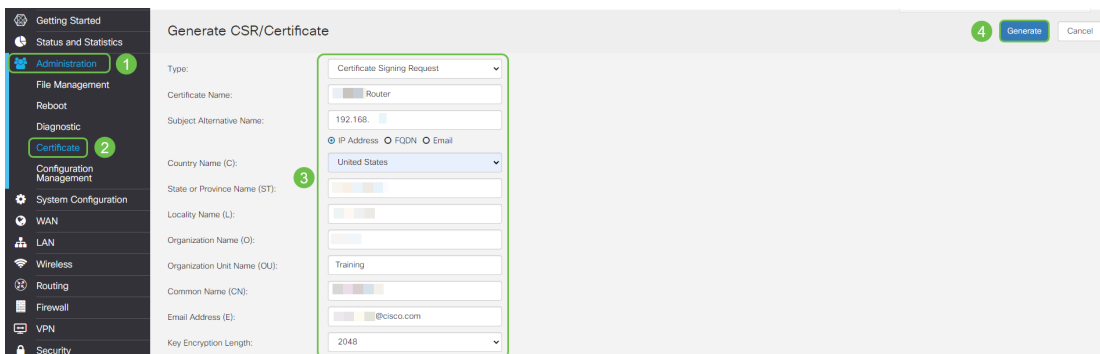


The image shows the login interface for a Cisco Router. At the top is the Cisco logo. Below it, the word "Router" is displayed. There are three input fields: the first contains "cisco", the second is labeled "Password", and the third is labeled "English" with a dropdown arrow. A blue "Login" button is located below the language field. 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."

步驟2.您必須取得憑證。導覽至Administration > Certificate > Generate CSR/Certificate...這是建立憑證請求的方法。



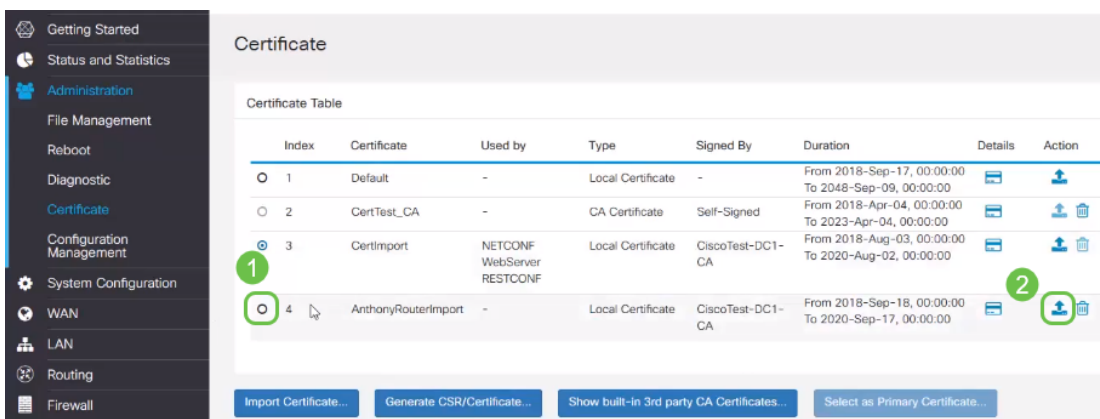
步驟3. 請求由CA憑證簽署的憑證。導覽至Administration > Certificate即可找到此項。



- 從下拉選單中選擇 *Certificate Signing Request*
- 輸入證書名稱
- 輸入IP地址、完全限定域名(FQDN)或電子郵件。輸入IP地址是最常見的選擇。
- 輸入您的國家/地區
- 輸入您的州/省
- 輸入您的地區名稱，通常是您的城市
- 輸入組織名稱
- 輸入組織單位名稱
- 輸入您的電子郵件地址
- 輸入金鑰加密長度，建議使用2048

按一下右上角的「生成」按鈕

步驟4. 按一下「操作」下的向上箭頭選擇以匯出它。



步驟5. 出現此畫面。按一下「Export」。

Export Certificate

Export as PEM format

Export to:

PC USB 

Export

Cancel

步驟6.從下拉選單中選擇開啟方式和記事本（預設）。按一下「OK」（確定）。

Opening AnthonyRouter.pem

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

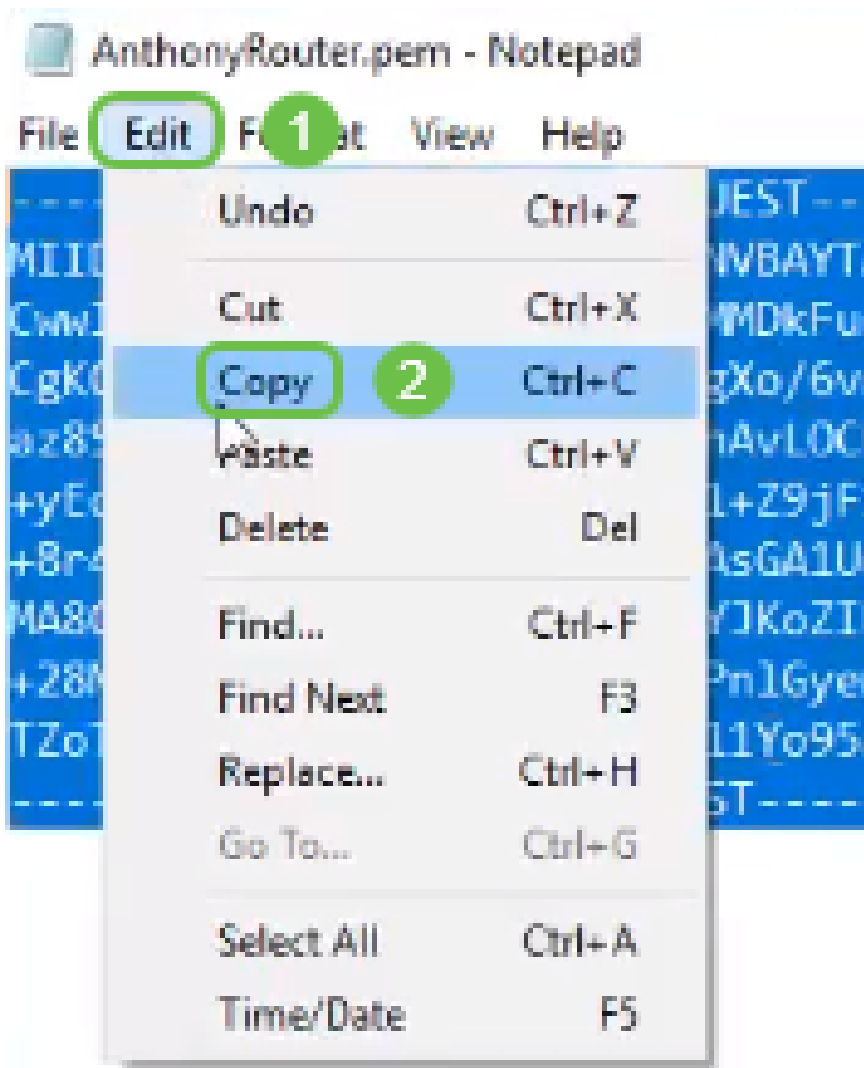
Cancel

步驟7.開啟XML檔案。

```
AnthonyRouter.pem - Notepad
File Edit Format View Help
-----BEGIN CERTIFICATE REQUEST-----
MIIDYTCBAkCAQAwZCcxZzA3BjgNBAYTA1VTRUwEwYDQVQIDAAxTb3V0aCBEYwtdGEwFDASBgWBAcMC1Npb3V4IEZhbGxzMQ4wDAYDVQQKDAVDAWJjZERMMA8GA1UE
CwV: GvbnkgUw91dGVyYWRwYXQzKoZihvcIAQkBFhBhcmVubGJw8BAQEFAADCAQIB
CgkCAQEApZLPhuMow2IgsVh7b1gXo/6vnp1BYn1HKMDkjnlZzfcCroCdqerCEjEe17XYGLsR9LXt61F1JGkaQ0rRpl.Yz7n11jRoL0BSzAeVJ0/bFDwOFF6X1Dx0peAyNS
az8So3RgkIoCyrghWUjIyEE91ThAvL0CEpd+BPjFpyE5Jj JdkrBDL47n9rv4MM9dWl./hXPD5tVxLw23+vfMtDh821tZgyJ9Z1HVb3dFZ42yZFEw+xjWU/N
+eF51bVH1P6TyqK2b0DeS1xs1+Z9Jf1ac3Gw6CFDYXg09C8ja8x1qgBasGcrwnJaycF+MBOL5s41UfWIDAQABoIGDMIGABgkqhk1G9w0BCQ4xczBxPMAkGA1UdEwQCMAMwIQYDVR00BBEYFFI
+B4zZePCPInbvS4HYDdPQcwz0MAsGA1UdDwQEAwIF4DAnBgIwH5UEIDAeBgggrBgEFBQcDAQYIKwYBBQUHwIGCCsGAQUFCAIC
MA8GA1UdEQQIMAAHBMcoASgUdQYJKoZIhvcIAQELBQADggEBAF2+aVr 44sZy0N0WnTawM49GnKChXMI3wFUXyYVvsGo0wN1XY5nUzmD0gJ5jE1
+28MBtJ0YuthSLMMAtbic6zUzHPnIGyemQz+JRjN/RNq5NHSL70sd8jwad0ZXXp6XpZ+mK5pm6vA1e0ef3mdJ/R+rP2Ahb+11RWmqQ0wh5f3swRS2HEon4
TzoTKfIXBcMTWpCh1jPFyALeNH811Yo95aB02WX2e+9vH0T5xgVae2wFomPHBBSUvcUNT4jUzYnysV7XkrREz7oY1PF5T2W9KzA1oZw8aQbNUqNTxJqFbM41F01cMUYs73q06M2M-
-----END CERTIFICATE REQUEST-----
```

附註：確保BEGIN CERTIFICATE REQUEST和END CERTIFICATE REQUEST分別位於各自的行上，如上所示。

步驟8.在螢幕頂部按一下Edit，然後從下拉選單中選擇Copy。



步驟9.選擇信譽良好的第三方站點進行證書請求。您需要將複製的XML檔案貼上為請求的一部分。

附註：如果您的網路上有內部憑證伺服器，可以使用該伺服器，但是這並不常見。

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  
cUNT4jUzYNyaV7XkREz7oY1PF5TZW9KzzAIo2W8a  
3qO6K2M=  
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Web Server

Additional Attributes:

Attributes:

Submit >

步驟10.驗證之後，您可以選擇 *Download certificate*。

Certificate Issued

The certificate you requested was issued to you.

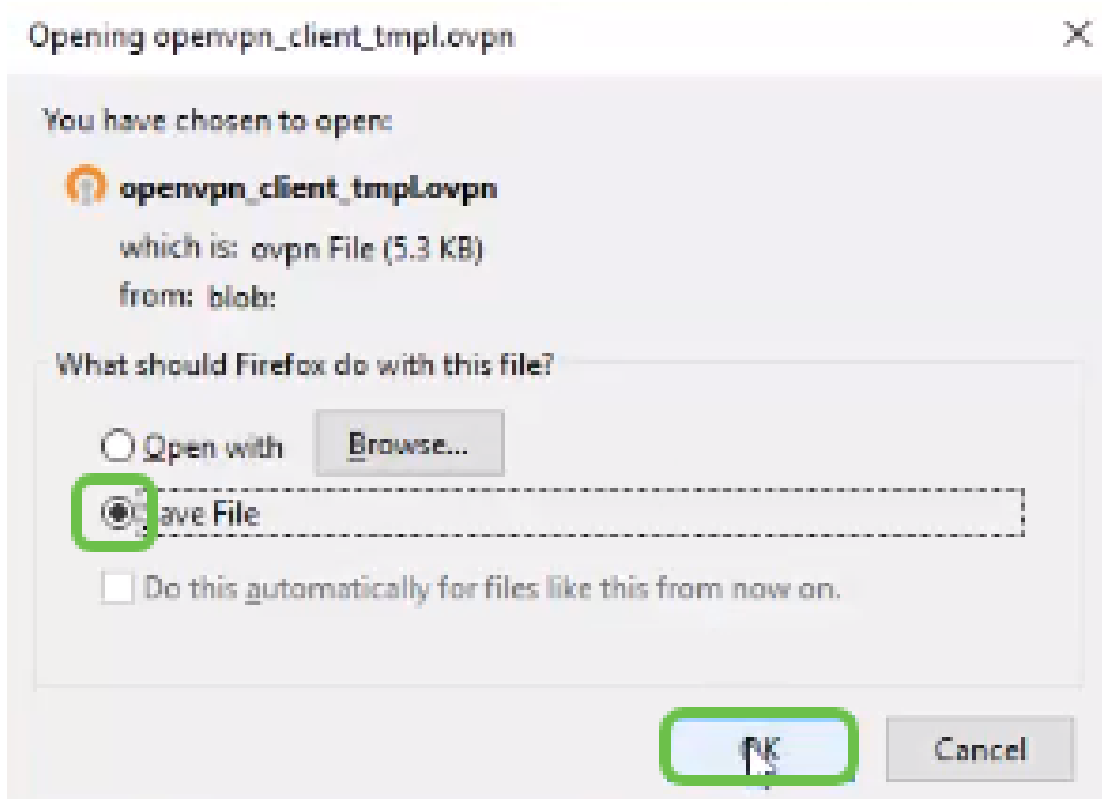
DER encoded or Base 64 encoded



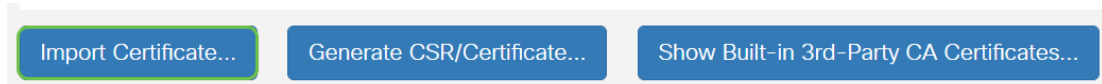
[Download certificate](#)

[Download certificate chain](#)

步驟11.按一下單選按鈕 *Save File*，然後按一下OK。



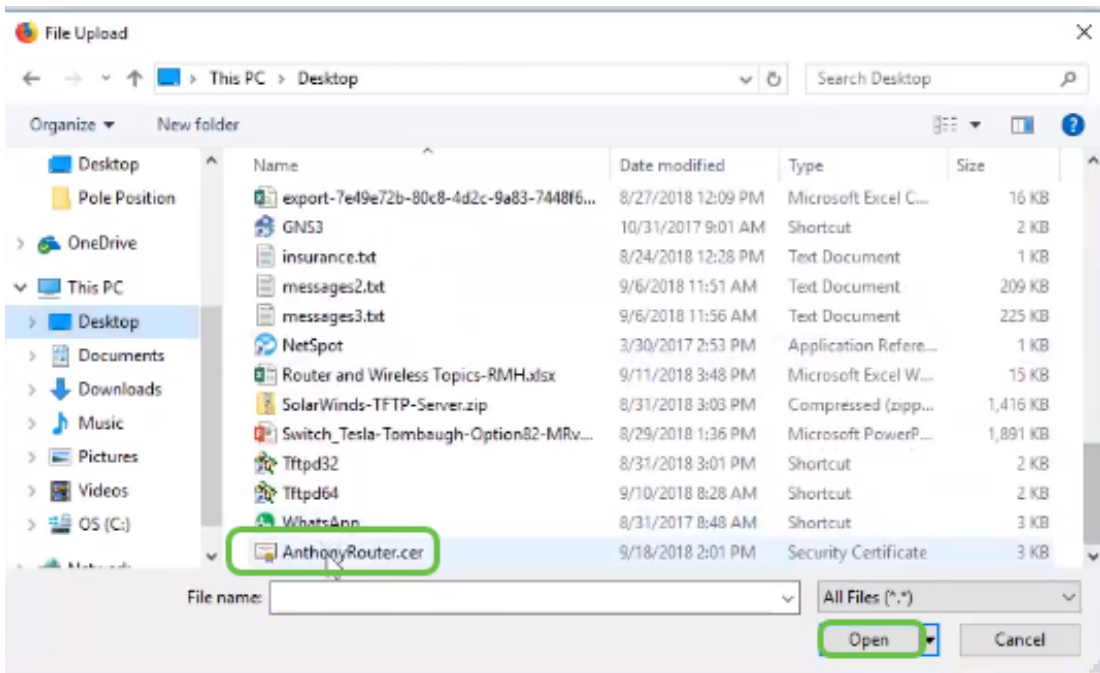
步驟12.儲存後，選擇該證書的單選按鈕，然後按一下箭頭圖標。



步驟13.將開啟此螢幕。選擇瀏覽.....



步驟14.選擇憑證檔案，然後按一下Open。



步驟15.輸入要匯入的Certificate Name，然後按一下Upload。

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

步驟16.您將收到證書已成功匯入的通知。按一下「OK」（確定）。

Information

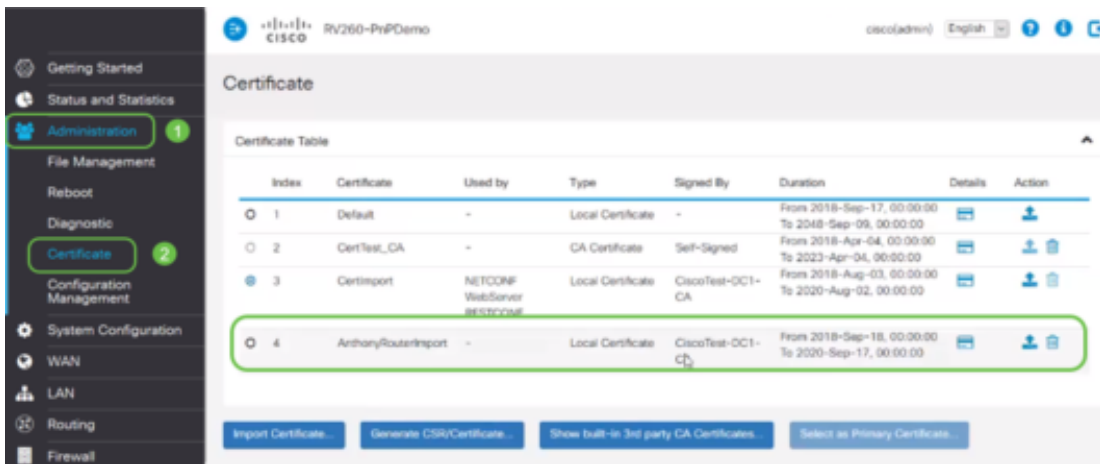


Import certificate successfully!

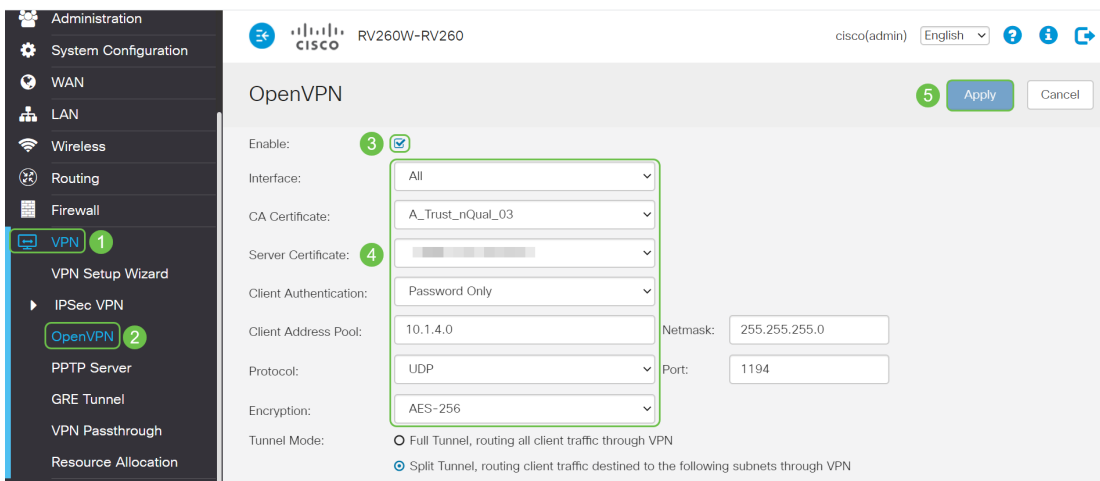
OK

步驟17.導覽至Administration > Certificate。已載入證書。

附註：在本示例中，使用了本地證書伺服器。



步驟18.導覽至VPN > OpenVPN。開啟OpenVPN頁面。使用您的資訊完成以下操作。



- 選中 *Enable* 框。選擇要允許流量進入的介面。在此案例中為廣域網(WAN)，然後選擇證書頒發機構(CA)證書
- 從下拉選單中選擇 *CA Certificate*
- 從下拉選單中選擇 *Server Certificate*
- 選擇 *Client Authentication*。如果您選擇「密碼」，他們需要使用密碼進行身份驗證。如果選擇 Password + Certificate，則客戶端還必須具有證書。這樣更安全，但會增加VPN的成本，因為它們需要購買單獨的CA。
- 輸入 *Client Address Pool*。選擇公司中其他任何位置未使用的網路子網上的IP地址。從保留範圍中選擇一個範圍，並選擇其它任何地方都不使用的範圍。
- 選擇 *Encryption* 的形式。確保加密與客戶端相同。建議不要使用DES和3DES，它們只能用於向後相容。
- 如果要讓所有客戶端流量通過VPN，請選擇 *Full Tunnel Mode*；如果要指定哪些流量通過VPN，請選擇 *Split tunnel*
- *DNS1* IP地址可以是專用的內部DNS伺服器、網際網路服務提供商(ISP)在虛擬機器上提供的與預設網關相同的IP地址，也可以是網際網路上提供的受信任DNS伺服器。

按一下「**Apply**」以儲存組態。

步驟19 (選項1)。您可以將此配置通過電子郵件傳送給客戶端。選中 *Send Email* 覈取方塊。輸入電子郵件地址。為電子郵件新增主題標題。按一下「**Generate**」。

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@ciscom

Email Subject: OpenVPN Client Config

4 **Generate**

步驟20. (選項2)。 選擇 *Export client configuration template(.ovpn)* , 然後按一下 **Generate**。

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**

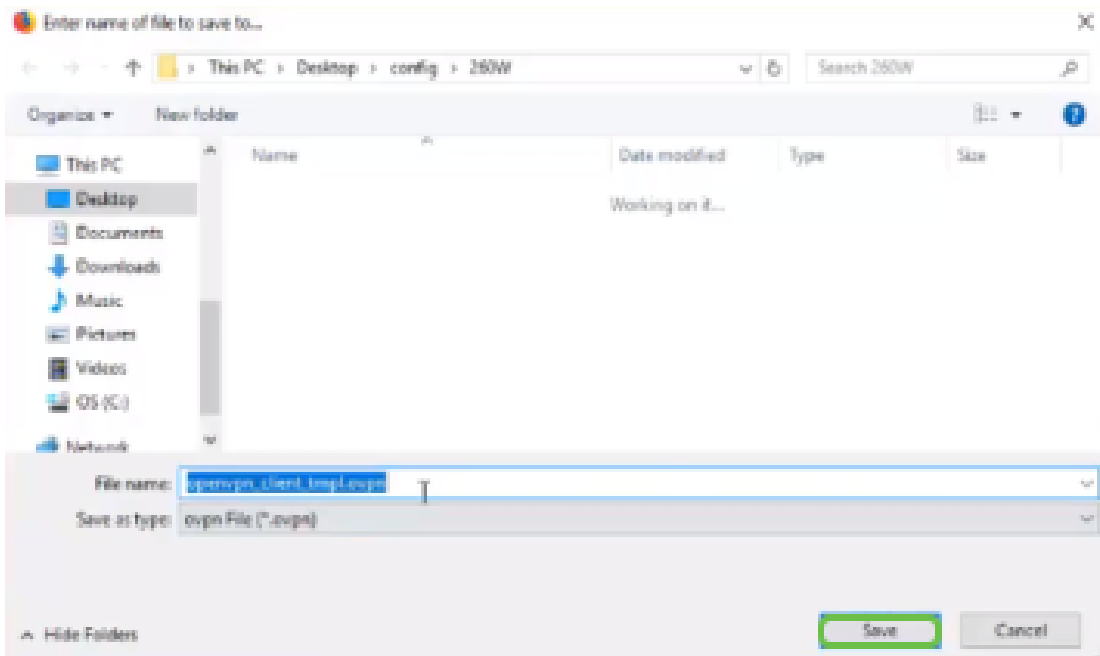
步驟21.您將收到成功的確認。按一下「OK」(確定)。

Information

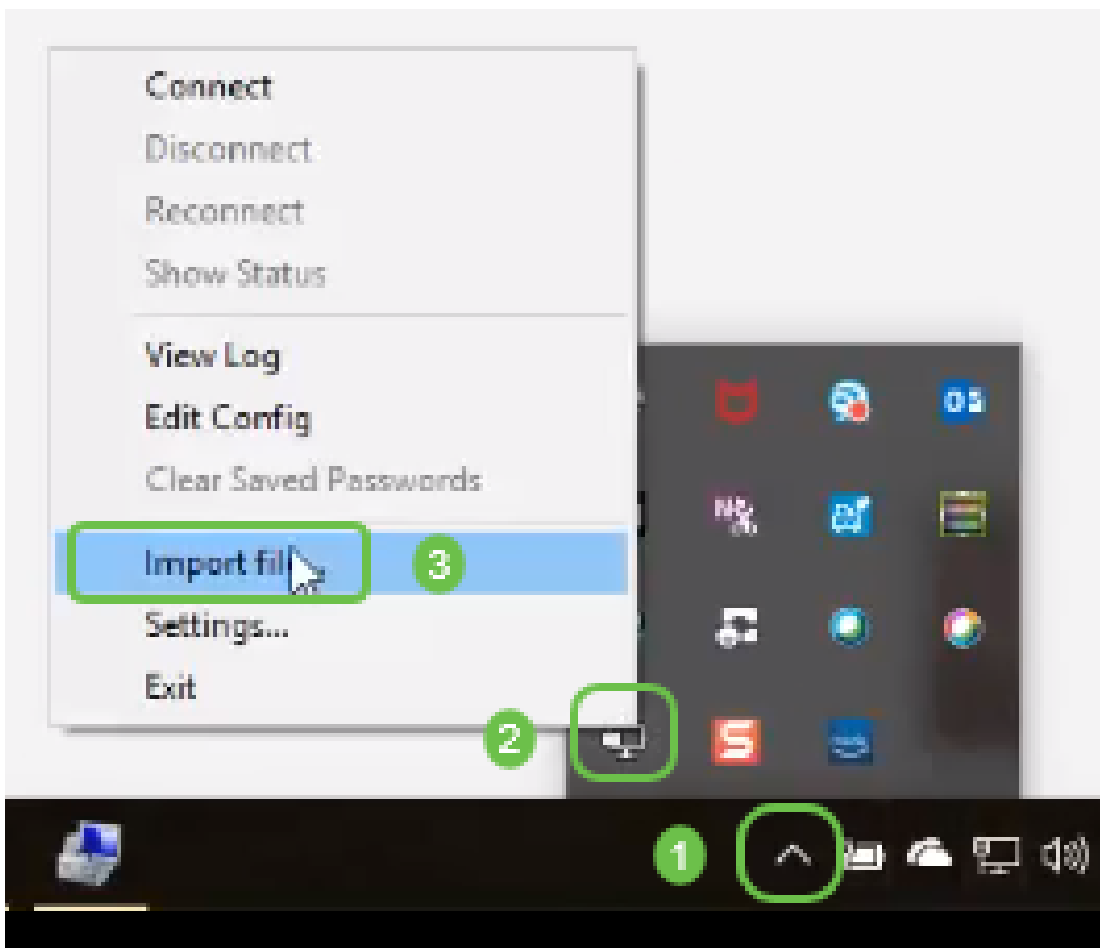
i Export client configuration template downloaded successfully!

OK

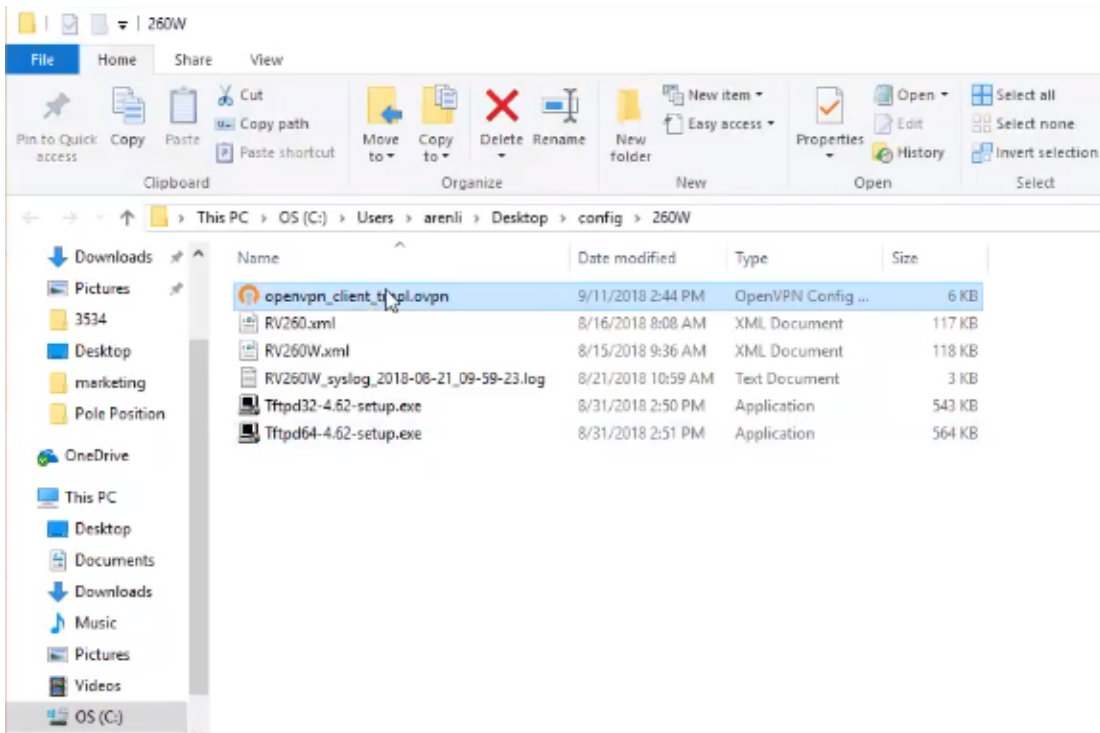
步驟22.按一下「Save」。



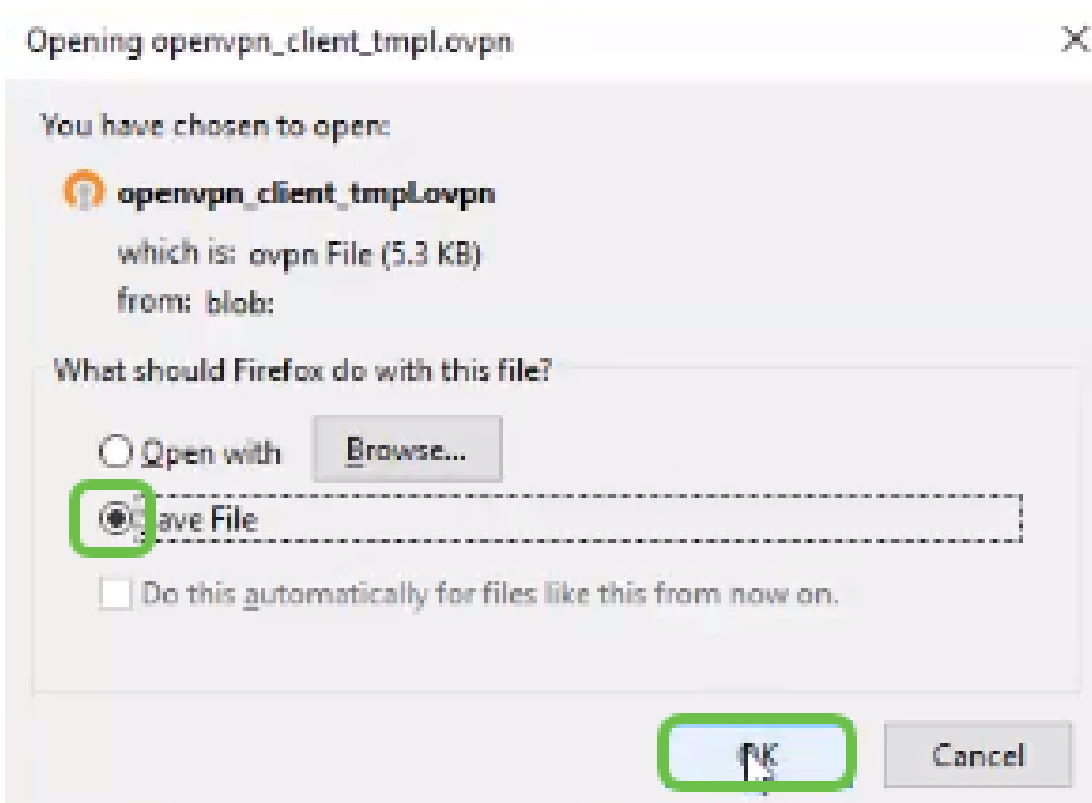
步驟23.在案頭右下方，按一下以開啟OpenVPN。按一下右鍵以開啟下拉選單。按一下「Import File」。



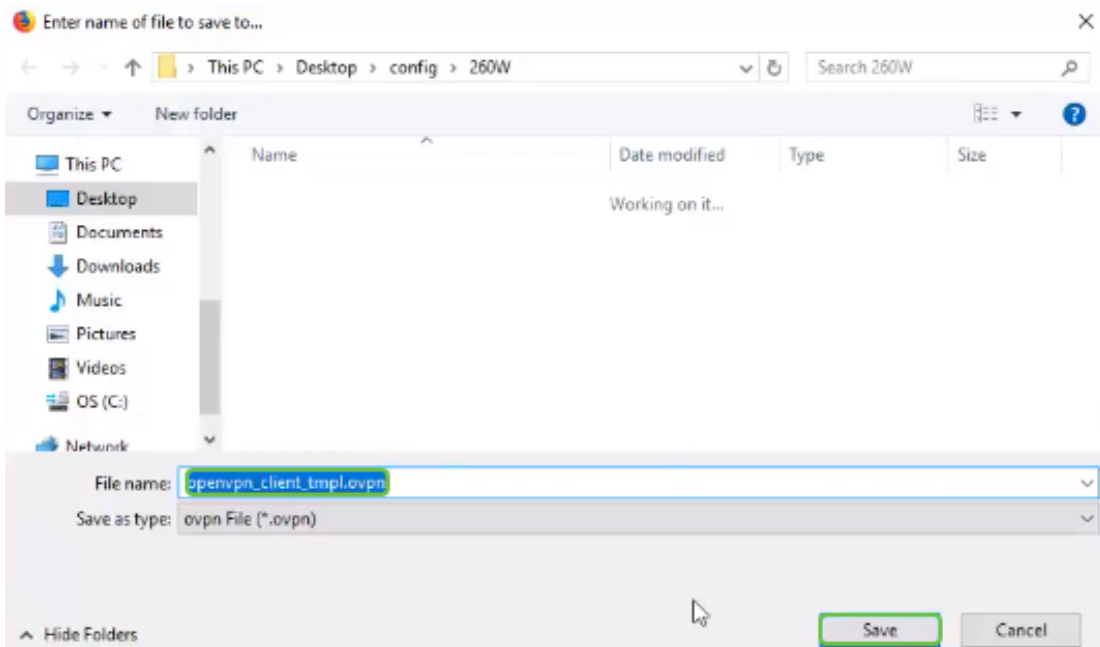
步驟24.選擇以.ovpn結尾的OpenVPN檔案。



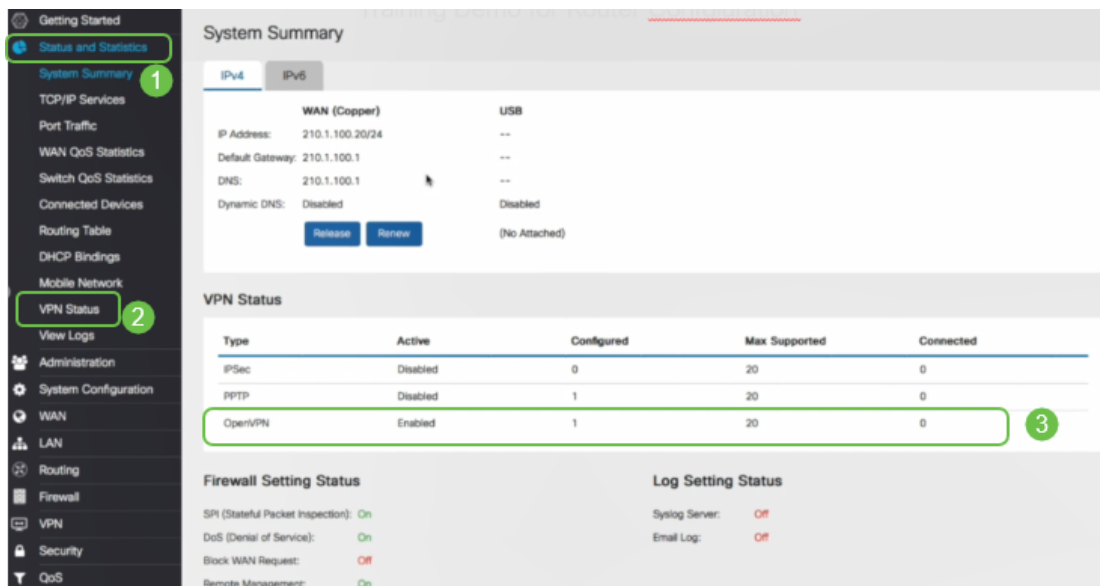
步驟25.按一下 *Save File* 單選按鈕，然後按一下OK。



步驟26.如果您選擇，請更改檔名，但保留檔名末尾的.ovpn。按一下「**Save**」。



步驟27.導覽至Status and Statistics > VPN Status。您可以向下滾動以獲取更多詳細資訊。



現在，路由器已配置支援個人試用版的OpenVPN客戶端連線所需的所有引數。

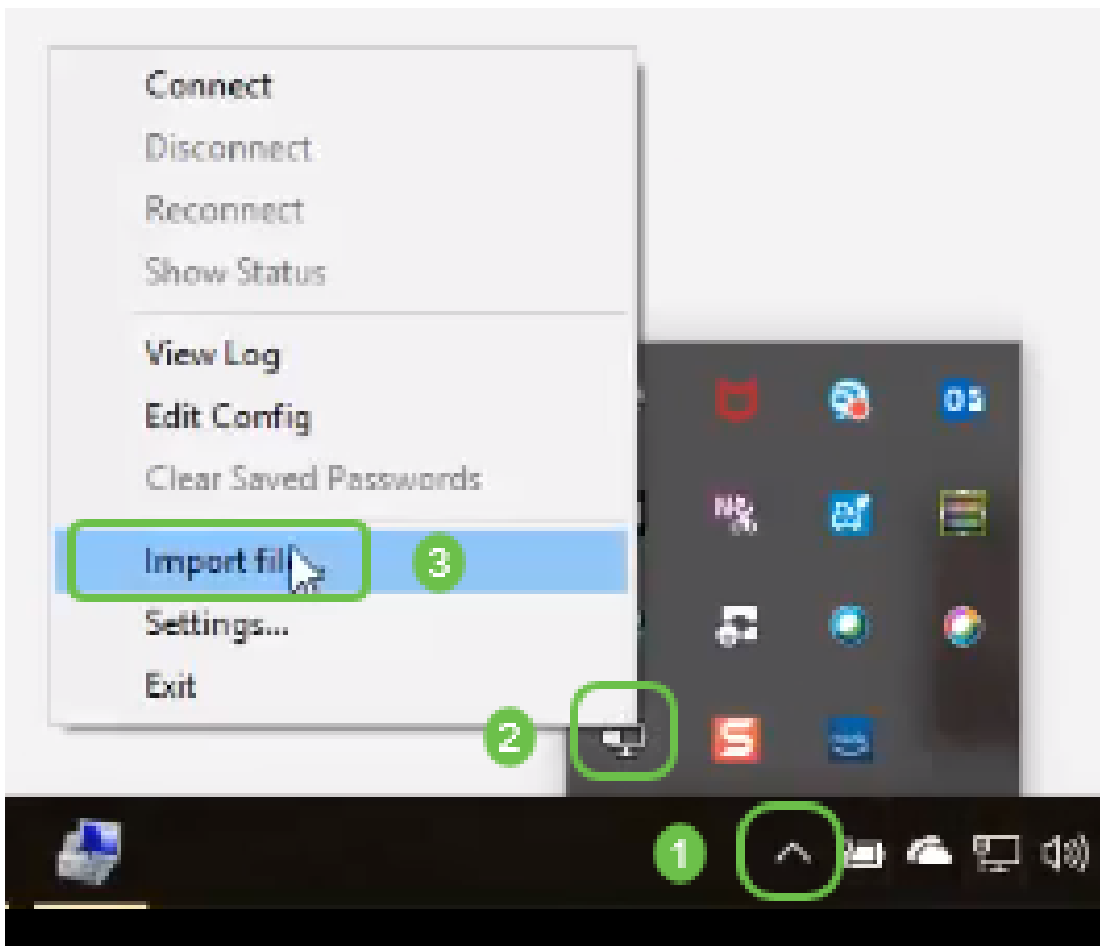
電腦上的OpenVPN客戶端設定

作為先決條件，每個OpenVPN客戶端都需要執行以下任務：

- 在裝置上下載OpenVPN應用程式。
- 開啟並儲存上一節的步驟19-22中傳送的配置檔案。配置檔案以.ovpn結尾。

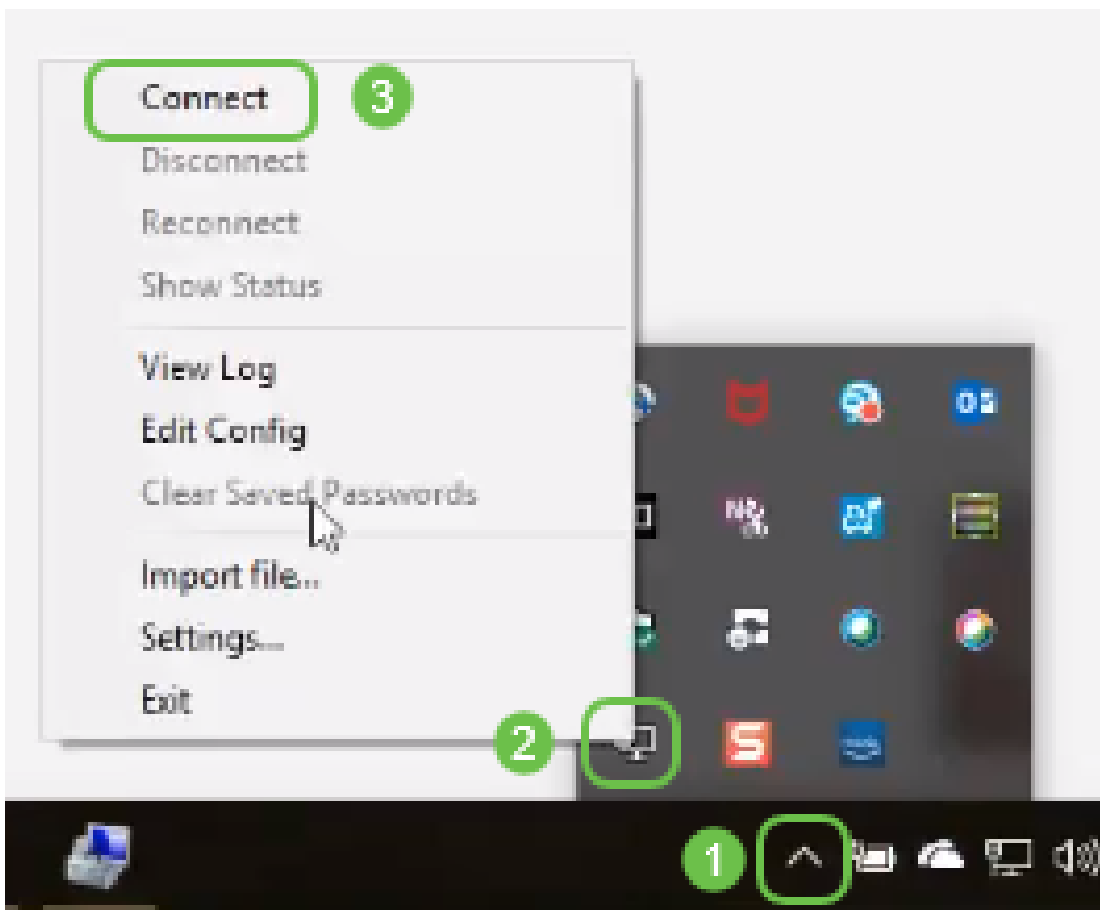
附註：此安裝程式專門用於Windows 10。

步驟1.導航至案頭右下方的箭頭圖示，然後按一下開啟OpenVPN圖示。按一下右鍵並選擇匯入檔案。

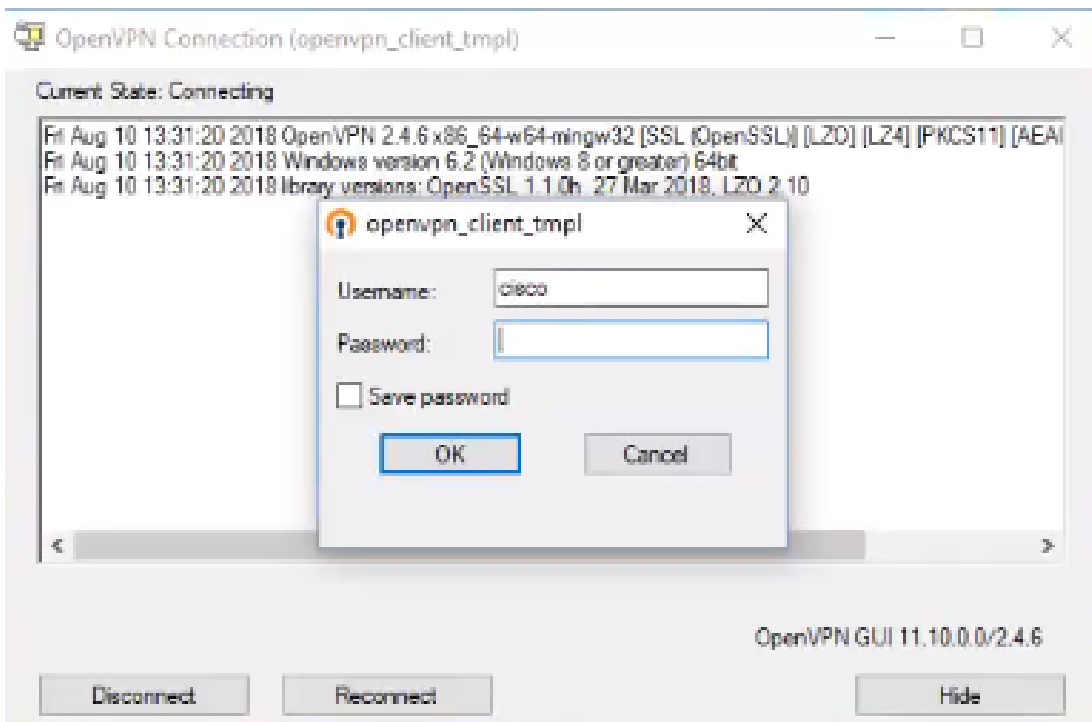


附註：圖示為黑白色，表示當前未運行。運行後，圖示將以顏色顯示。

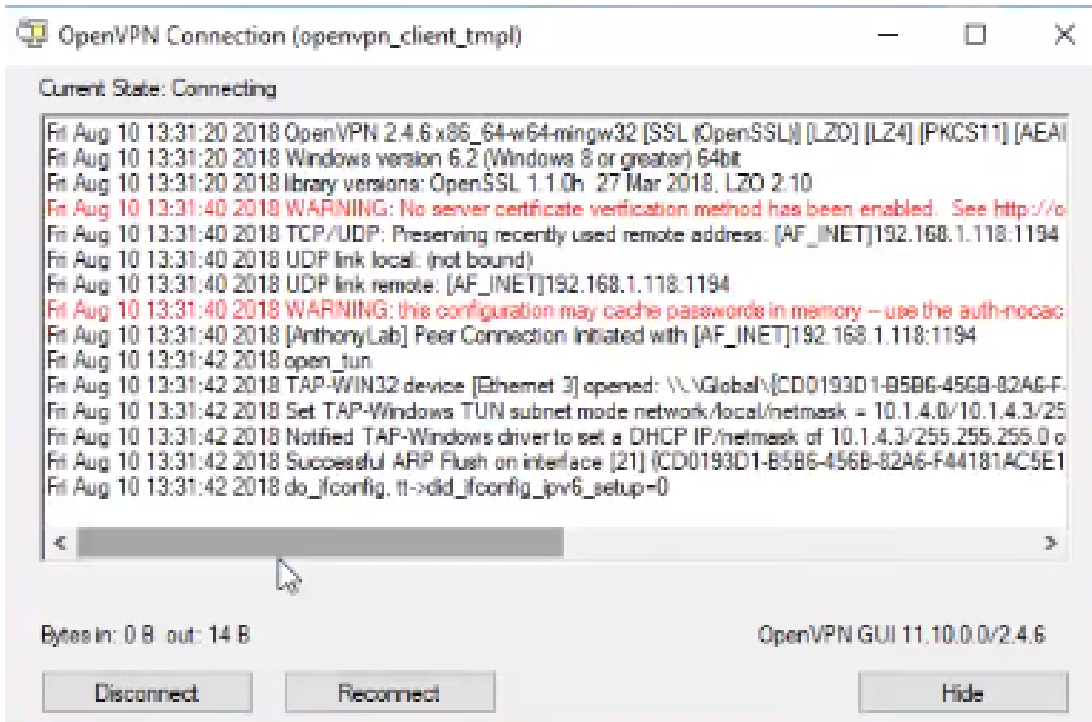
步驟2.按一下上箭頭。按一下OpenVPN圖示。按一下右鍵並從下拉選單中選擇連線。



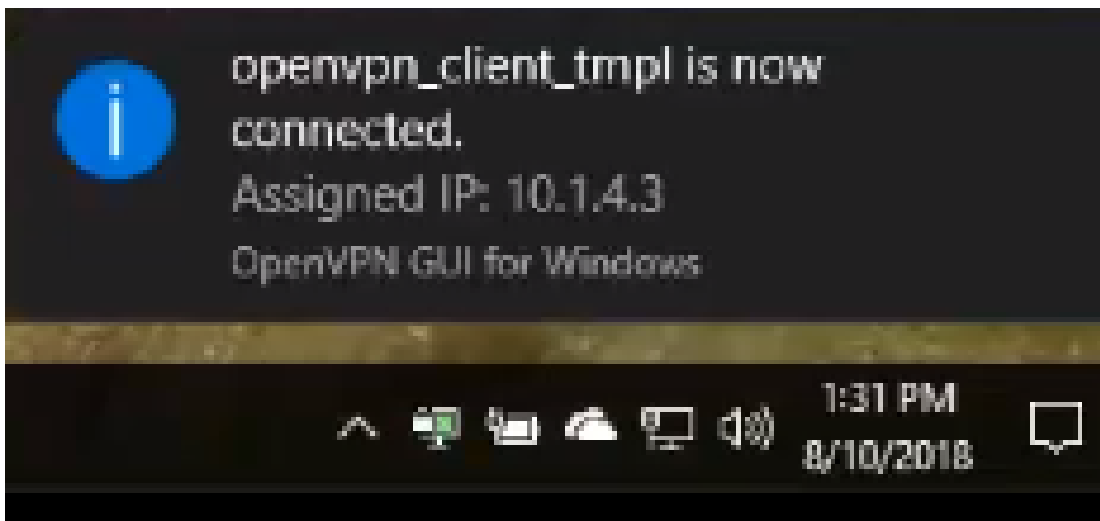
步驟3.輸入Username和Password。



步驟4.視窗將顯示OpenVPN連線以及一些日誌資料。

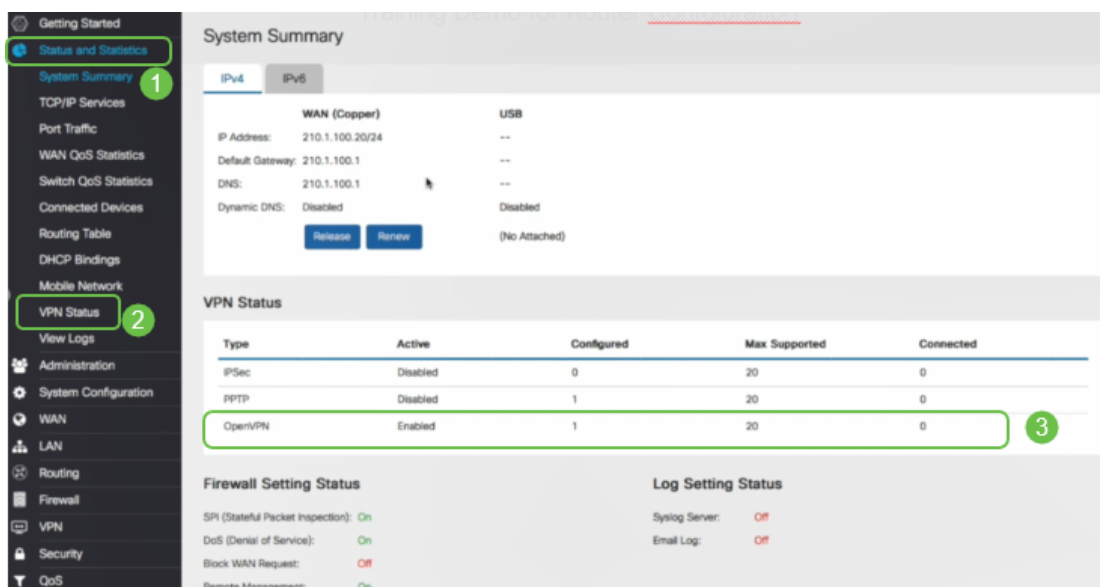


步驟5.系統日誌應發出連線警報。



步驟6. VPN客戶端應該能夠安全地通過OpenVPN隧道傳輸傳入和傳出資訊。可在OpenVPN設定中將此設定為自動連線。

步驟7. 管理員可以通過在路由器上導航到**Status and Statistics > VPN Status**來確認VPN狀態。



結論

現在，您應該已經在RV160或RV260路由器和VPN客戶端站點成功安裝了OpenVPN。

有關OpenVPN的社群討論，請點選此處，然後搜尋OpenVPN。

檢視與本文相關的影片.....

[按一下此處檢視思科的其他技術對話](#)