

# AnyConnect:安裝自簽名證書作為受信任的來源

## 目標

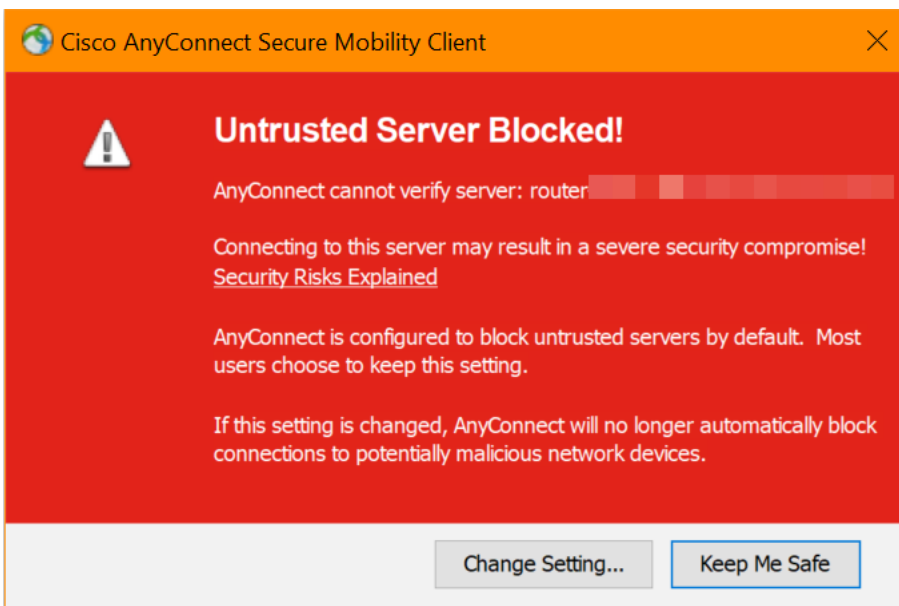
本文的目的是指導您在Windows電腦上建立和安裝自簽名證書作為受信任源。這將消除AnyConnect中的「不受信任的伺服器」警告。

## 簡介

Cisco AnyConnect Virtual Private Network(VPN)Mobility Client為遠端使用者提供安全的VPN連線。它提供思科安全套接字層(SSL)VPN客戶端的優點，並支援基於瀏覽器的SSL VPN連線無法使用的應用程式和功能。AnyConnect VPN通常由遠端工作人員使用，它使員工可以像在辦公室那樣連線到公司網路基礎設施，即使他們不在辦公室也是如此。這提高了員工的靈活性、移動性和工作效率。

證書在通訊過程中非常重要，用於驗證個人或裝置的身份、驗證服務或加密檔案。自簽名證書是由其自己的建立者簽名的SSL證書。

首次連線到AnyConnect VPN移動客戶端時，使用者可能會遇到「Untrusted Server (不受信任的伺服器)」警告，如下圖所示。



按照本文中的步驟在Windows電腦上安裝自簽名證書作為受信任源，以消除此問題。

應用匯出的證書時，請確保將其放在安裝了Anyconnect的客戶端PC上。

## AnyConnect軟體版本

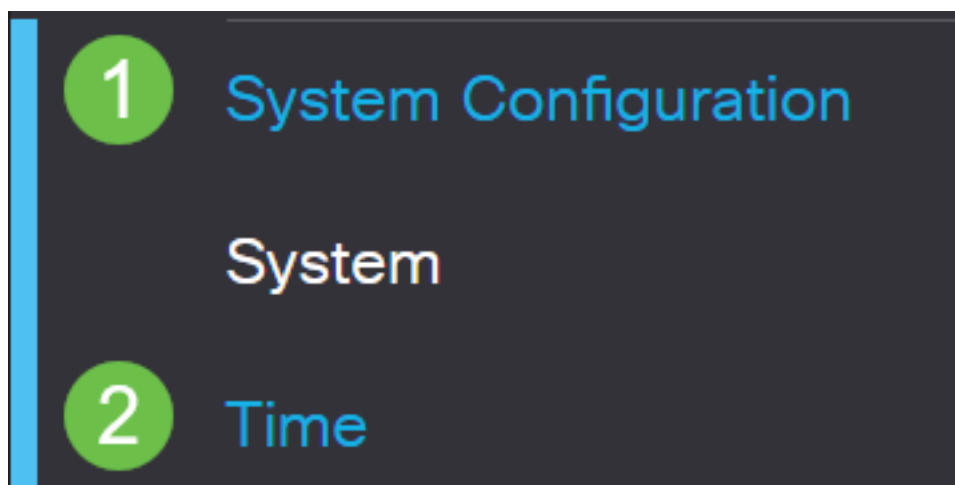
- AnyConnect - v4.9.x(下載[最新版](#))

## 檢查時間設定

作為前提條件，您需要確保您的路由器具有正確的時間設定，包括時區和夏令時設定。

## 步驟1

導覽至System Configuration > Time。



## 步驟2


確保一切設定正確。

### Time

Current Date and Time: 2019-Oct-21, 10:51:21 PST

Time Zone: (UTC -08:00) Pacific Time (US & Canada) ▼

Set Date and Time:  Auto  Manual

Enter Date and Time: 2019-10-21  (yyyy-mm-dd)

10 ▼ : 51 ▼ : 10 ▼ (24hh:mm:ss)

Daylight Saving Time:

Daylight Saving Mode:  By Date  Recurring

From: Month 3 ▼ Day 10 ▼ Time 02 ▼ : 00 ▼ (24hh:mm)

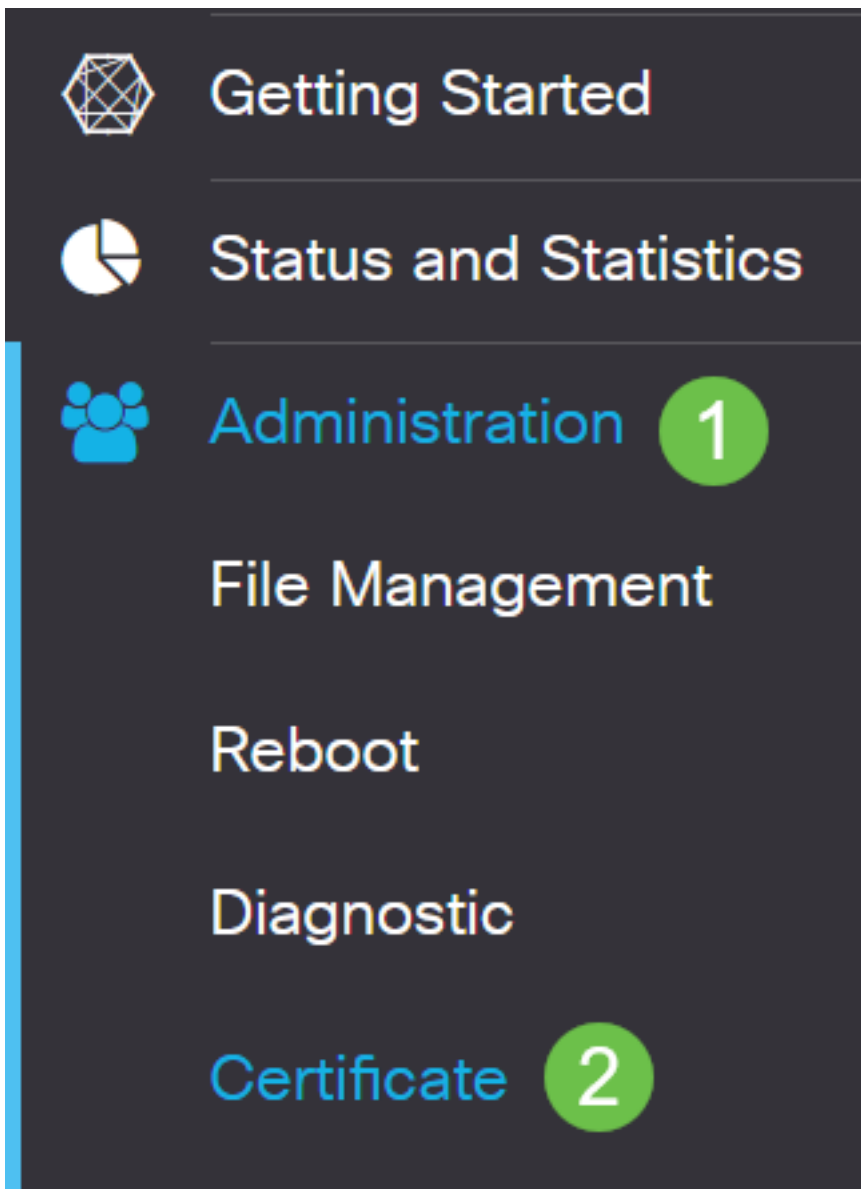
To: Month 11 ▼ Day 03 ▼ Time 02 ▼ : 00 ▼ (24hh:mm)

Daylight Saving Offset: +60 ▼ Minutes

## 建立自簽名證書

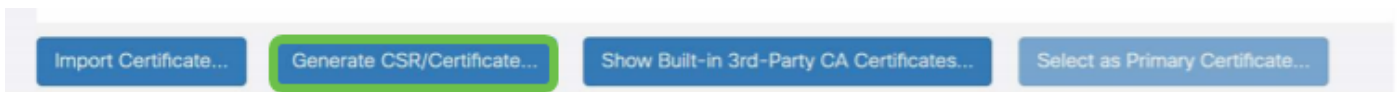
## 步驟1

登入到RV34x系列路由器，然後導航到Administration > Certificate。



## 步驟2

按一下「Generate CSR/Certificate」。



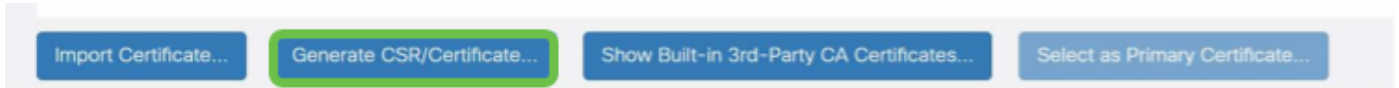
## 步驟3

填寫以下資訊：

- Type: 自簽名證書
- 證書名稱：（ 您選擇的任何名稱 ）
- 使用者替代名稱：如果要在WAN埠上使用IP地址，請在框下選擇IP Address，如果要使用完全限定的域名，請選擇FQDN。在框中，輸入WAN埠的IP地址或FQDN。
- 國家/地區名稱(C): 選擇裝置所在的國家/地區

- 省或州名稱(ST):選擇裝置所在的州或省
- 地區名稱(L): ( 可選 ) 選擇裝置所在的位置。這可能是一個城鎮、城市等等。
- 組織名稱(O): ( 選用 )
- 組織單位名稱(OU):公司名稱
- 一般名稱(CN):此名稱必須與設定為主題備用名稱的內容匹配
- 電子郵件地址(E): ( 選用 )
- 金鑰加密長度：2048
- 有效持續時間：這是證書的有效時間。預設值為360天。您可以將此值調整為任意值，最長為10,950天或30年。

按一下**Generate**。

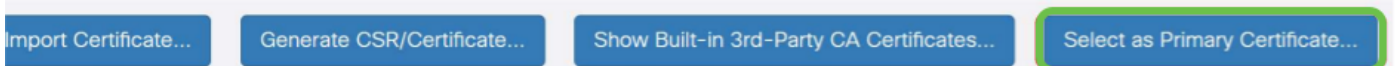


#### 步驟4

選擇剛建立的證書，然後按一下**選擇為主要證書**。

#### Certificate Table

<input type="checkbox"/>	Index ↕	Certificate ↕	Used By ↕	Type ↕	Signed By ↕	Duration ↕	Details	Action
<input type="checkbox"/>	1	Default	WebServer, ...	Local Certifi...	Self Signed	From 2012-Jul-12, 00:00:00 PST To 2042-Jul-05, 00:00:00 PST		
<input checked="" type="checkbox"/>	2	SEAR	-	Local Certifi...	Self Signed	From 2019-Oct-21, 00:00:00 PS To 2029-Aug-29, 00:00:00 PST		



#### 步驟5

刷新Web使用者介面(UI)。由於它是新證書，因此需要重新登入。登入後，請轉至VPN > SSL VPN。

1

VPN

VPN Status

IPSec Profiles

Site-to-Site

Client-to-Site

Teleworker VPN Client

PPTP Server

L2TP Server

GRE Tunnel

2

SSL VPN

步驟6

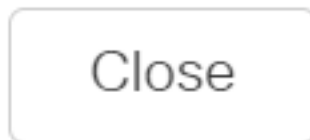
將Certificate File變更為新建立的憑證。

# Mandatory Gateway Settings

Gateway Interface:	<input type="text" value="WAN1"/>	
Gateway Port:	<input type="text" value="8443"/>	(Range: 1-65535)
Certificate File:	<input type="text" value="SEAR"/>	
Client Address Pool:	<input type="text" value="10.10.10.0"/>	
Client Netmask:	<input type="text" value="255.255.255.0"/>	
Client Domain:	<input type="text" value="yourdomain.com"/>	
Login Banner:	<input type="text" value="Hello, welcome!"/>	

## 第7步

按一下「Apply」。

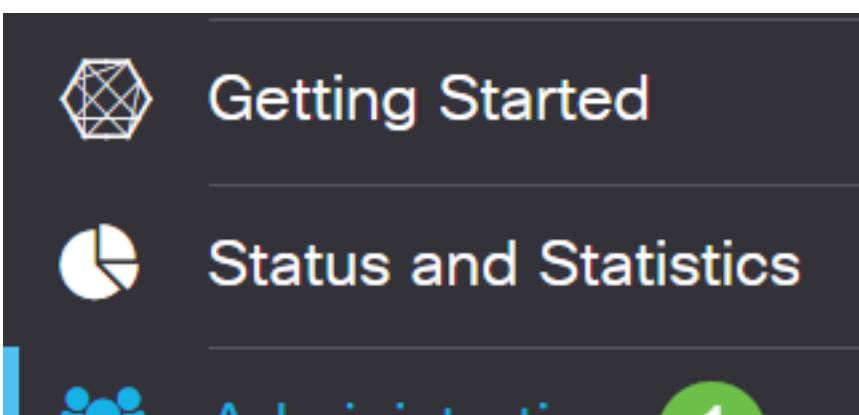


## 安裝自簽名證書

要在Windows電腦上安裝自簽名證書作為受信任的源，消除AnyConnect中的「不受信任的伺服器」警告，請執行以下步驟：

## 步驟1

登入到RV34x系列路由器，然後導航到Administration > Certificate。



## 步驟2

選擇預設自簽名證書，然後按一下**Export**按鈕下載證書。

Certificate

Certificate Table

<input checked="" type="checkbox"/>	Index	Certificate	Used By	Type	Signed By	Duration	Details	Action
<input checked="" type="checkbox"/>	1	Default	WebServer, ...	Local Certifi...	Self Signed	From 2019-Feb-22, 00:00:00 GM To 2049-Feb-14, 00:00:00 GMT		

## 步驟3

在「*Export Certificate*」視窗中，輸入憑證的密碼。在 *Confirm Password* 欄位中重新輸入密碼，然後按一下**Export**。

Export Certificate

Export as PKCS#12 format

Enter Password  1

Confirm Password  2

Export as PEM format

Select Destination to Export:

PC

3

**Export** Cancel

## 步驟4

您將看到一個彈出視窗，通知已成功下載證書。按一下「**OK**」（確定）。

# Information

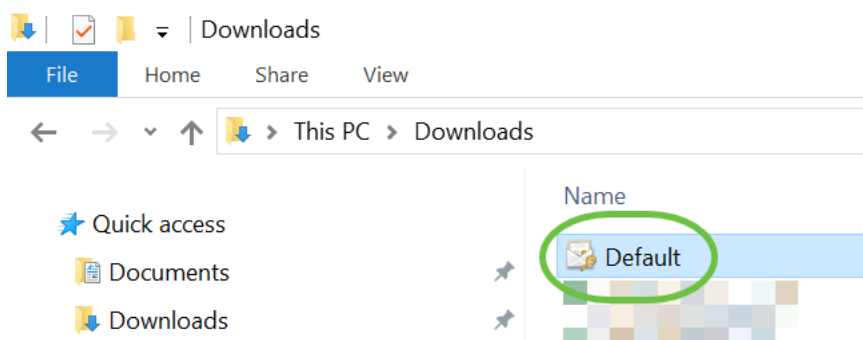


Success

Ok

## 步驟5

將證書下載到PC後，找到該檔案，然後按兩下該檔案。



## 步驟6

將會出現「*Certificate Import Wizard*」視窗。對於 *Store Location*，選擇 **Local Machine**。按「**Next**」（下一步）。



## Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

1

Store Location

Current User

Local Machine

To continue, click Next.

2

### 第7步

將在以下螢幕上顯示證書位置和資訊。按「Next」（下一步）。

**File to Import**

Specify the file you want to import.

File name:

Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

**步驟8**

輸入您為憑證選擇的 *Password* ，然後按一下 **Next**。

### Private key protection

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

1

•••••

Display Password

Import options:

- Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
- Mark this key as exportable. This will allow you to back up or transport your keys at a later time.
- Protect private key using virtualized-based security(Non-exportable)
- Include all extended properties.

2

Next

Cancel

### 步驟9

在下一個螢幕上，選擇Place all certificates in the following store，然後按一下Browse。

### Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

Automatically select the certificate store based on the type of certificate

1

Place all certificates in the following store

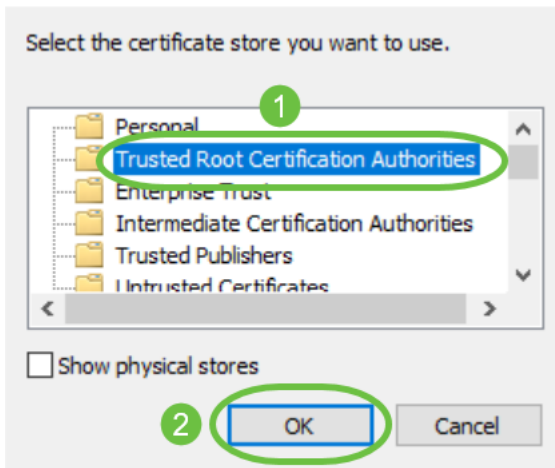
Certificate store:

2

Browse...


### 步驟10

選擇Trusted Root Certification Authorities，然後按一下OK。



### 步驟11

按「Next」（下一步）。

←  Certificate Import Wizard

#### Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

- Automatically select the certificate store based on the type of certificate
- Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities

Browse...

Next

Cancel

### 步驟12

將顯示設定的摘要。按一下Finish匯入證書。

## Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	PFX
File Name	C:\Users\██████\Downloads\Default.p12

Finish

Cancel

### 步驟13

您將看到證書已成功匯入的確認。按一下「OK」（確定）。

Certificate Import Wizard



The import was successful.

OK

### 步驟14

開啟Cisco AnyConnect並再次嘗試連線。不應再看到不受信任的伺服器警告。

## 結論

你拿到了！現在，您已成功學習了在Windows電腦上安裝自簽名證書作為受信任源的步驟，從而消除AnyConnect中的「不受信任的伺服器」警告。

## 其他資源

[基本故障排除](#) [AnyConnect管理員指南4.9版](#) [AnyConnect發行說明](#) — [4.9 思科業務VPN概述和最佳實踐](#)