

# AnyConnect: Een zelfondertekend certificaat installeren als een betrouwbare bron

## Doel

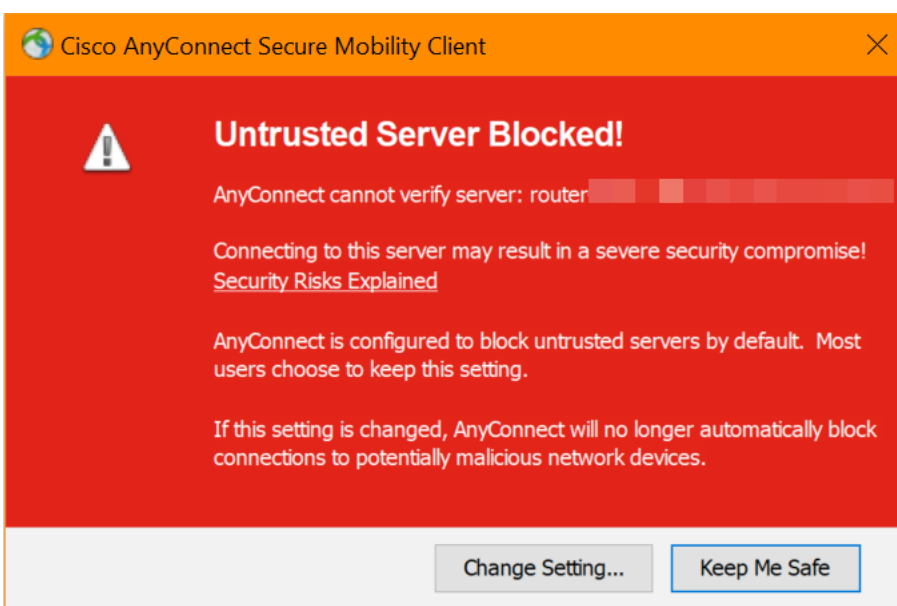
Het doel van dit artikel is om u door het maken en installeren van een zelfondertekend certificaat als een vertrouwde bron op een Windows-machine te begeleiden. Hierdoor wordt de waarschuwing "Onvertrouwde server" in AnyConnect verwijderd.

## Inleiding

De Cisco AnyConnect Virtual Private Network (VPN) Mobiliteitsclient biedt externe gebruikers een beveiligde VPN-verbinding. Het biedt de voordelen van een Cisco Secure Socket Layer (SSL) VPN-client en ondersteunt toepassingen en functies die niet beschikbaar zijn voor een browser-gebaseerde SSL VPN-verbinding. Gebruikt door externe medewerkers laat AnyConnect VPN-medewerkers zich aansluiten op de netwerkinfrastructuur van het bedrijf alsof ze fysiek op het kantoor aanwezig zijn, zelfs wanneer dit niet het geval is. Dit voegt toe aan de flexibiliteit, mobiliteit en productiviteit van je werknemers.

Certificaten zijn belangrijk in het communicatieproces en worden gebruikt om de identiteit van een persoon of apparaat te controleren, een service te controleren of bestanden te versleutelen. Een zelfondertekend certificaat is een SSL-certificaat dat door de eigen maker is ondertekend.

Wanneer gebruikers voor het eerst verbinding maken met AnyConnect VPN Mobility Client, kunnen zij een waarschuwing "Onvertrouwde server" krijgen zoals in de onderstaande afbeelding wordt weergegeven.



Volg de stappen in dit artikel om een zelfondertekend certificaat als een vertrouwde bron op een Windows-machine te installeren, om dit probleem op te lossen.

Wanneer u het geëxporteerde certificaat toepast, dient u er zeker van te zijn dat het op de client-PC is geplaatst terwijl AnyConnect is geïnstalleerd.

## AnyConnect-softwareversie

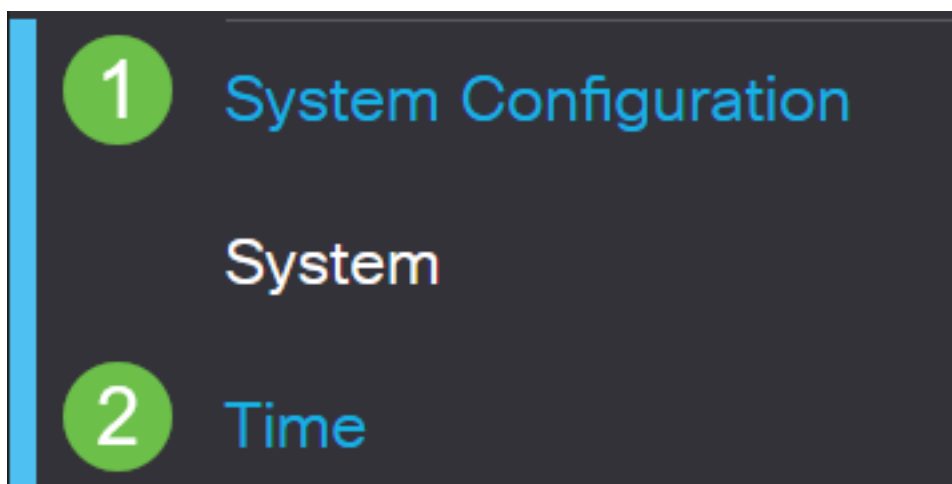
- AnyConnect - v4.9.x ([laatste download](#))

## Instellingen tijd controleren

Als voorwaarde, moet u ervoor zorgen dat uw router de juiste tijdreeks heeft, inclusief de instellingen voor de tijd en de zomertijd.

### Stap 1

Navigeer naar **stelselconfiguratie > Tijd**.



### Stap 2

Zorg ervoor dat alles correct is ingesteld.

# 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

## Een zelfondertekend certificaat maken

### Stap 1

Meld u aan bij de RV34x-router en navigeer naar **Administratie > Certificaat**.



Getting Started



Status and Statistics



Administration

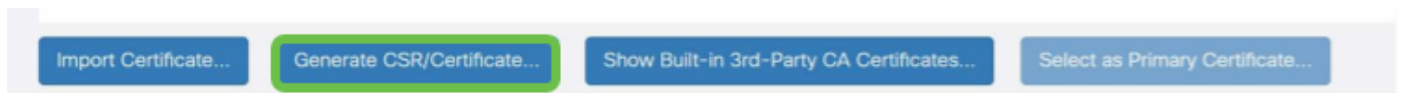
1

File Management

Reboot

## Stap 2

Klik op **Generate CSR/certificaat**.

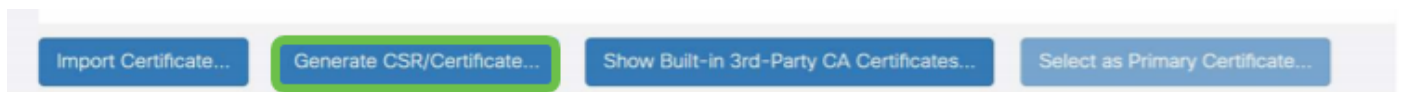


## Stap 3

Vul de volgende informatie in:

- Type: Zelfondertekend certificaat
- certificaatnaam: (Elke naam die u kiest)
- Onderwerp Alternatieve naam: Als een IP-adres op de WAN-poort zal worden gebruikt, selecteert u **IP-adres** onder het vakje of **FQDN** als u de Full Qualified Domain Name gebruikt. Voer in het vak het IP-adres of FQDN van de WAN-poort in.
- Naam land (C): Selecteer het land waar het apparaat zich bevindt
- Naam van de staat of provincie (ST): Selecteer de staat of provincie waar het apparaat zich bevindt
- Naam lokaliteit (L): (Optioneel) Selecteer de locatie waar het apparaat zich bevindt. Dit kan een stad zijn, een stad, enz.
- Naam organisatie (o): (optioneel)
- Naam organisatie-eenheid (OU): Bedrijfsnaam
- Gecombineerde benaming (GN): Dit **MOET** overeenkomen met de handelsnaam voor het alternatief onderwerp
- E-mailadres: (optioneel)
- Lengte belangrijke encryptie: 2048
- Geldige duur: Zo lang is het certificaat geldig. De standaard is 360 dagen. Je kunt dit aanpassen op elke waarde die je wilt, tot 10.950 dagen of 30 jaar.

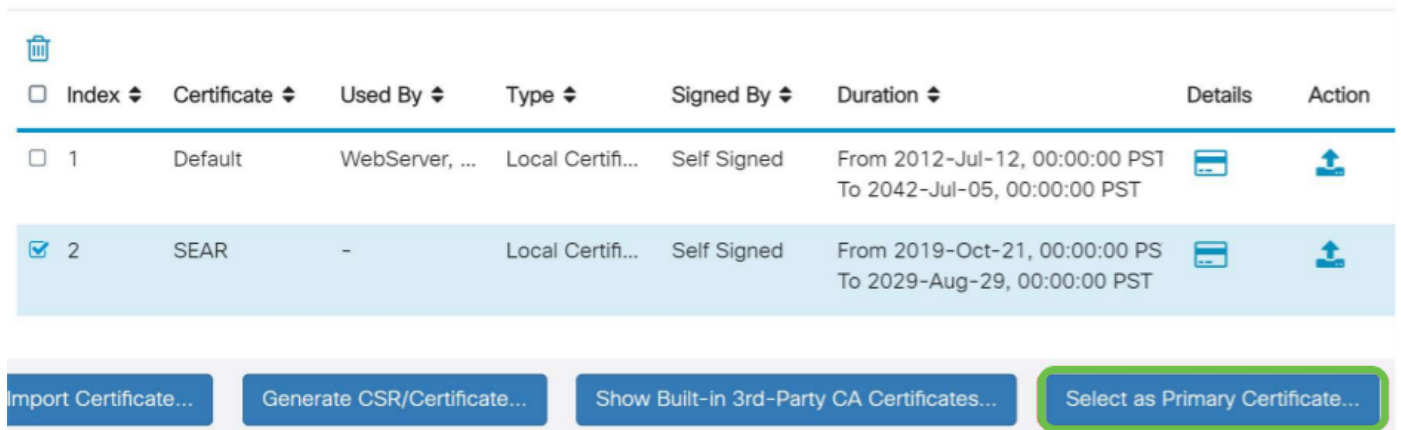
Klik op **Generate**.



## Stap 4

Selecteer het certificaat dat zojuist is gemaakt en klik op **Selecteren als Primair certificaat**.

## 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		

Import Certificate...   Generate CSR/Certificate...   Show Built-in 3rd-Party CA Certificates...   **Select as Primary Certificate...**

### Stap 5

Verfris het Web User Interface (UI). Aangezien het een nieuw certificaat is, moet u opnieuw inloggen. Nadat u hebt aangemeld, gaat u naar **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

Stap 6

Verander **certificaatbestand** in het nieuwe certificaat.

# 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!"/>	

## Stap 7

Klik op **Apply** (Toepassen).

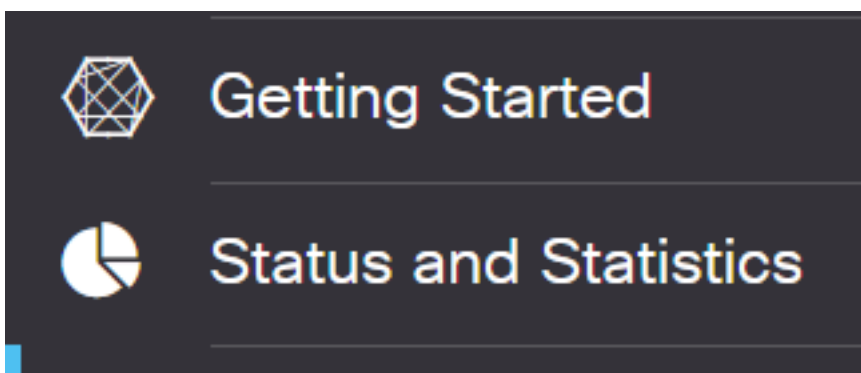


## Een zelfondertekend certificaat installeren

Om een zichzelf ondertekend certificaat als een vertrouwde bron op een Windows-machine te installeren, dient u de waarschuwing "Onvertrouwde server" in AnyConnect te verwijderen en de volgende stappen te volgen:


## Stap 1

Meld u aan bij de RV34x-router en navigeer naar **Administratie > Certificaat**.



## Stap 2

Selecteer het standaard zelfgetekende certificaat en klik op de knop **Exporteren** om uw certificaat te downloaden.

Certificate							
Certificate Table							
<input checked="" type="checkbox"/>	Index	Certificate	Used By	Type	Signed By	Duration	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	

## Stap 3

Voer in het venster *Exportcertificaat* een wachtwoord in voor het certificaat. Voer het wachtwoord opnieuw in het veld *Wachtwoord bevestigen* en klik vervolgens op **Exporteren**.

### 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

## Stap 4

U ziet een pop-upvenster om aan te geven dat het certificaat is gedownload. Klik op **OK**.



# Information

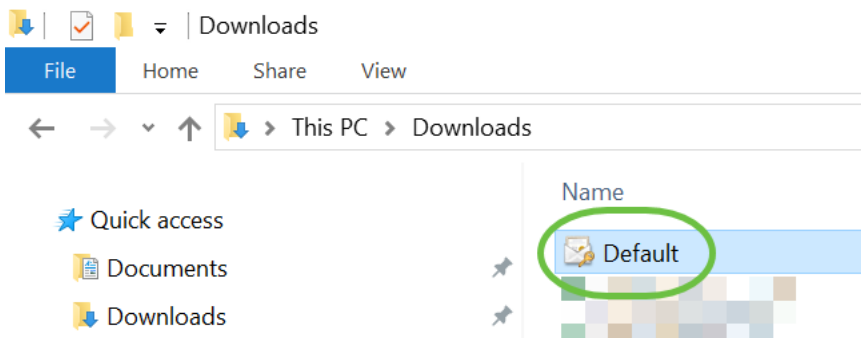


Success



## Stap 5

Nadat het Certificaat naar uw PC is gedownload, kunt u het bestand vinden en erop dubbelklikken.



## Stap 6

Het venster *Wizard Certificaat importeren* verschijnt. Selecteer voor de *opslaglocatie* de optie **Local Machine**. Klik op **Volgende**.

## 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.

Store Location

Current User

1  Local Machine

To continue, click Next.

2

 Next

Cancel

### Stap 7

Op het volgende scherm worden de locatie van het certificaat en de informatie weergegeven. Klik op **Volgende**.

**File to Import**

Specify the file you want to import.

File name:

C:\Users\k... \Downloads\Default.p12

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)

**Stap 8**

Typ het *wachtwoord* dat u voor het certificaat hebt geselecteerd en klik op **Volgende**.

### 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

### Stap 9

Selecteer in het volgende scherm **alle certificaten in de volgende winkel plaatsen** en klik vervolgens op **Bladeren**.

### 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

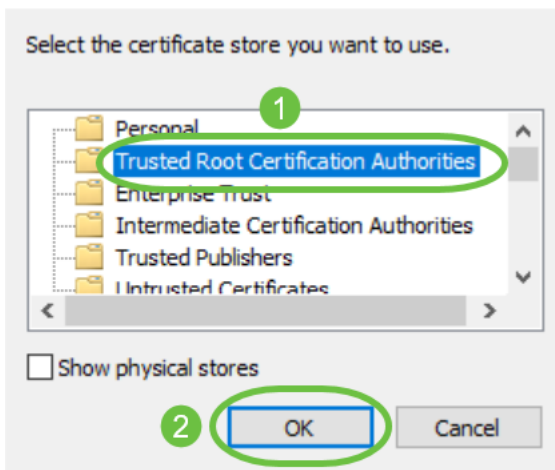
Certificate store:

2

Browse...


### Stap 10

Selecteer **Trusted Root-certificeringsinstanties** en klik op **OK**.



## Stap 11

Klik op **Volgende**.

←  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

## Stap 12

Er wordt een samenvatting van de instellingen weergegeven. Klik op **Voltooien** om het certificaat te importeren.

## 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

### Stap 13

U ziet een bevestiging dat het Certificaat met succes is ingevoerd. Klik op OK.

Certificate Import Wizard



The import was successful.

OK

### Stap 14

Open Cisco AnyConnect en probeer opnieuw verbinding te maken. U dient de waarschuwing Onvertrouwde servers niet langer te zien.

## Conclusie

Daar heb je het! U hebt nu met succes de stappen geleerd om een zelf-ondertekend certificaat als een vertrouwde bron op een Windows-machine te installeren, om de waarschuwing "Onvertrouwde server" in AnyConnect te verwijderen.

## Aanvullende bronnen

[Basisprobleemoplossing AnyConnect-beheerdershandleiding release 4.9 AnyConnect release Notes - 4.9 Cisco Business VPN - Overzicht en beste praktijken](#)