

AnyConnect : Installation d'un certificat auto-signé en tant que source fiable

Objectif

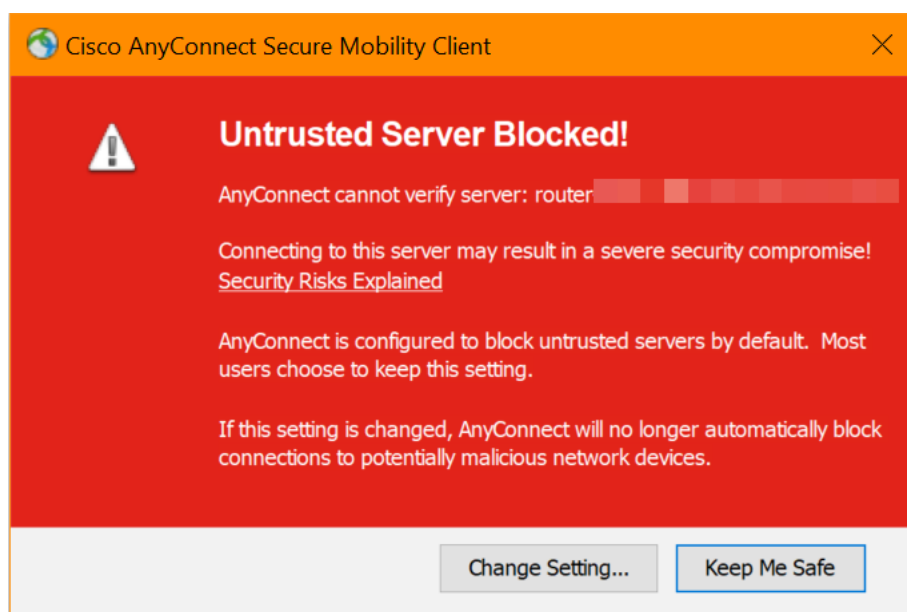
L'objectif de cet article est de vous guider dans la création et l'installation d'un certificat auto-signé en tant que source fiable sur un ordinateur Windows. Cela éliminera l'avertissement " Untrust Server " dans AnyConnect.

Introduction

Le client de mobilité VPN (Virtual Private Network) Cisco AnyConnect fournit aux utilisateurs distants une connexion VPN sécurisée. Il fournit les avantages d'un client VPN SSL (Secure Sockets Layer) de Cisco et prend en charge les applications et fonctions non disponibles pour une connexion VPN SSL basée sur navigateur. Généralement utilisé par les travailleurs distants, AnyConnect VPN permet aux employés de se connecter à l'infrastructure réseau de l'entreprise comme s'ils se trouvaient physiquement au bureau, même lorsqu'ils ne le sont pas. Cela ajoute à la flexibilité, à la mobilité et à la productivité de vos employés.

Les certificats sont importants dans le processus de communication et sont utilisés pour vérifier l'identité d'une personne ou d'un périphérique, authentifier un service ou chiffrer des fichiers. Le certificat auto-signé est un certificat SSL qui est signé par son propre créateur.

Lors de la première connexion au client AnyConnect VPN Mobility, les utilisateurs peuvent rencontrer un " de serveur non approuvé ", comme l'illustre l'image ci-dessous.



Suivez les étapes de cet article pour installer un certificat auto-signé en tant que source fiable sur un ordinateur Windows, afin d'éliminer ce problème.

Lors de l'application du certificat exporté, assurez-vous qu'il est placé sur le PC client avec

Anyconnect installé.

Version du logiciel AnyConnect

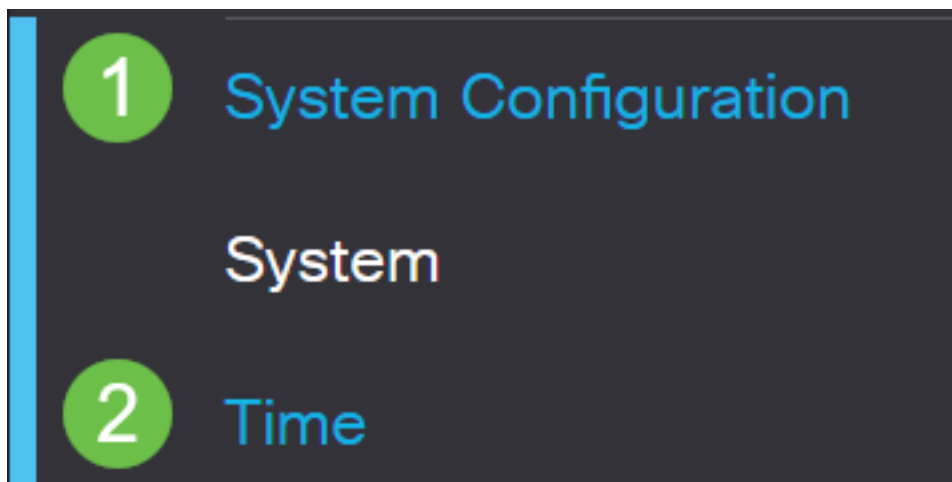
- AnyConnect - v4.9.x ([Télécharger la dernière version](#))

Vérifier les paramètres de temps

En tant que condition préalable, vous devez vous assurer que votre routeur dispose de l'heure correcte, y compris les paramètres de fuseau horaire et d'heure d'été.

Étape 1

Accédez à **Configuration système > Heure**.



Étape 2

Assurez-vous que tout est réglé correctement.

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

Créer un certificat auto-signé

Étape 1

Connectez-vous au routeur de la gamme RV34x et accédez à **Administration > Certificate**.



Getting Started



Status and Statistics



Administration

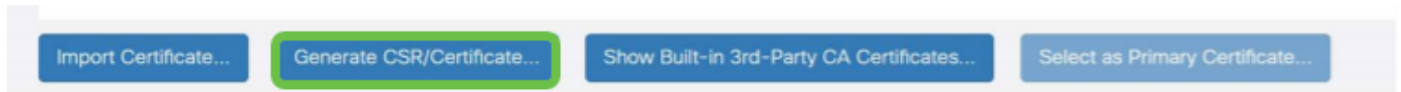
1

File Management

Reboot

Étape 2

Cliquez sur **Generate CSR/Certificate**.

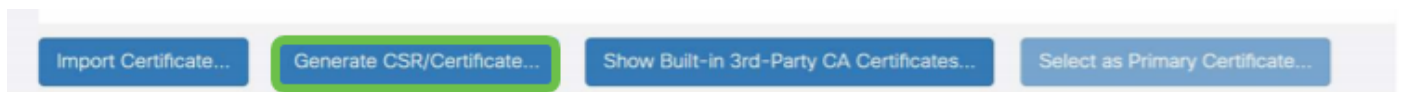


Étape 3

Complétez les informations suivantes :

- type : Certificat auto-signé
- Nom du certificat : (Tout nom que vous choisissez)
- Autre nom du sujet : Si une adresse IP est utilisée sur le port WAN, sélectionnez **IP Address** sous la zone ou **FQDN** si vous utilisez le nom de domaine complet. Dans la zone, saisissez l'adresse IP ou le nom de domaine complet du port WAN.
- Nom du pays (C) : Sélectionnez le pays où se trouve le périphérique
- Nom de l'État ou de la province (ST) : Sélectionnez l'État ou la province où se trouve le périphérique
- Nom de la localité (L) : (Facultatif) Sélectionnez la localité où se trouve le périphérique. Il peut s'agir d'une ville, d'une ville, etc.
- Nom de l'organisation (O) : (Facultatif)
- Nom de l'unité d'organisation : Nom de la société
- Nom commun (CN) : Cette valeur DOIT correspondre à celle définie comme nom alternatif de l'objet
- Adresse e-mail (E) : (Facultatif)
- Longueur du chiffrement de clé : 2048
- Durée valide : C'est la durée de validité du certificat. La valeur par défaut est 360 jours. Vous pouvez l'ajuster à n'importe quelle valeur, jusqu'à 10 950 jours ou 30 ans.

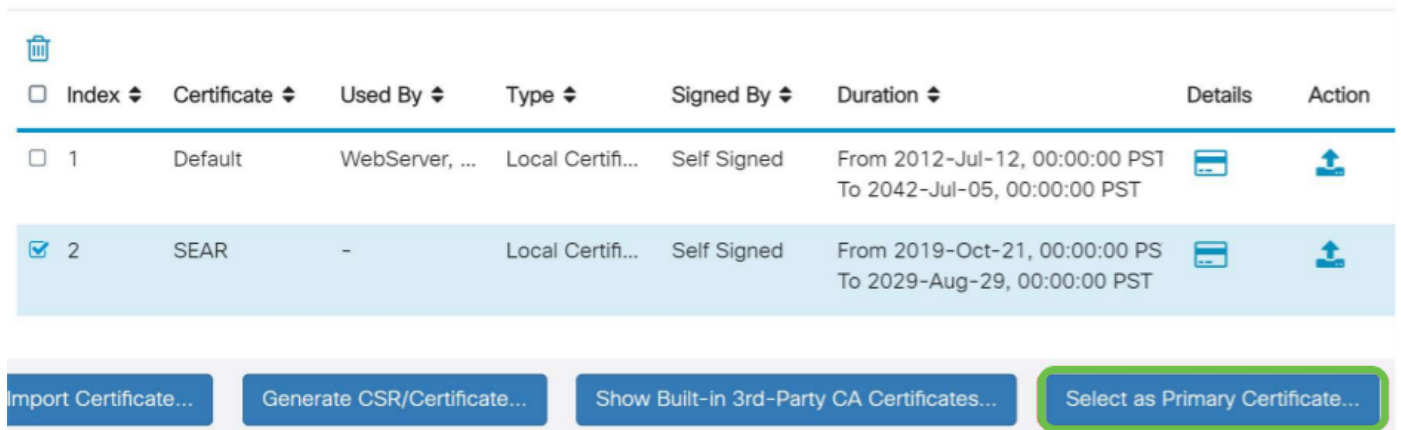
Cliquez sur **Generate**.



Étape 4

Sélectionnez le certificat qui vient d'être créé et cliquez sur **Sélectionner comme certificat principal**.

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...**

Étape 5

Actualiser l'interface utilisateur Web. Comme il s'agit d'un nouveau certificat, vous devrez vous reconnecter. Une fois connecté, accédez à **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

Étape 6

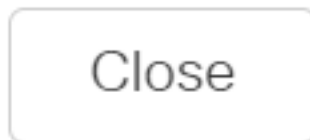
Remplacez le **fichier de certificat** par le nouveau certificat créé.

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!"/>	

Étape 7

Cliquez sur Apply.



Installation d'un certificat auto-signé

Pour installer un certificat auto-signé en tant que source fiable sur un ordinateur Windows, pour supprimer l'avertissement " Untrust Server " dans AnyConnect, procédez comme suit :

Étape 1

Connectez-vous au routeur de la gamme RV34x et accédez à **Administration > Certificate**.



Getting Started



Status and Statistics

Étape 2

Sélectionnez le certificat auto-signé par défaut et cliquez sur le bouton **Exporter** pour télécharger votre certificat.

Certificate

Certificate Table

Index	Certificate	Used By	Type	Signed By	Duration	Details	Action
1	Default	WebServer, ...	Local Certifi...	Self Signed	From 2019-Feb-22, 00:00:00 GM To 2049-Feb-14, 00:00:00 GMT		

Étape 3

Dans la fenêtre *Exporter le certificat*, saisissez un mot de passe pour votre certificat. Saisissez à nouveau le mot de passe dans le champ *Confirmer le mot de passe*, puis cliquez sur **Exporter**.

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

Étape 4

Une fenêtre contextuelle s'affiche pour vous informer que le certificat a été téléchargé avec succès. Cliquez sur **OK**.

Information

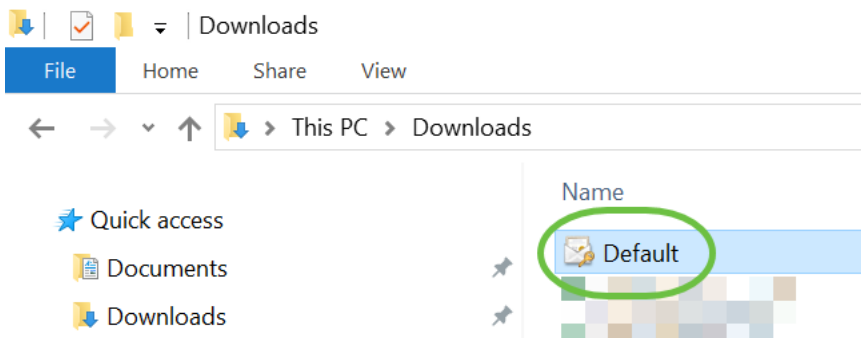


Success



Étape 5

Une fois le certificat téléchargé sur votre ordinateur, localisez le fichier et double-cliquez dessus.



Étape 6

La fenêtre *Assistant Importation de certificat* s'affiche. Pour l'emplacement du magasin, sélectionnez **Ordinateur local**. Cliquez sur **Next** (Suivant).

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

Étape 7

Dans l'écran suivant, l'emplacement et les informations du certificat s'affichent. Cliquez sur **Next** (Suivant).

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)

Étape 8

Entrez le *mot de passe* sélectionné pour le certificat et cliquez sur **Suivant**.

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

Étape 9

Dans l'écran suivant, sélectionnez **Placer tous les certificats dans le magasin suivant**, puis cliquez sur **Parcourir**.

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

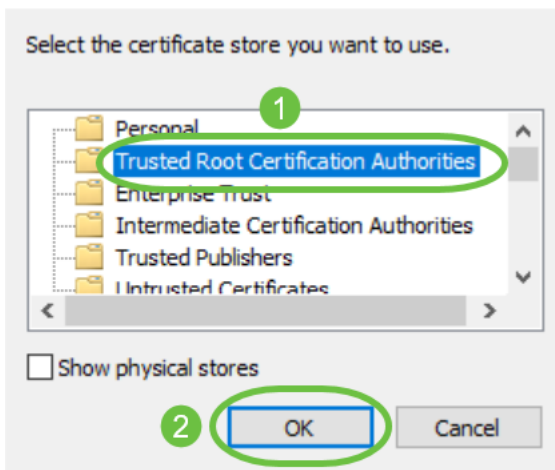
Certificate store:

2

Browse...


Étape 10

Sélectionnez **Autorités de certification racines de confiance** et cliquez sur **OK**.



Étape 11

Cliquez sur **Next** (Suivant).

←  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

Étape 12

Un résumé des paramètres s'affiche. Cliquez sur **Terminer** pour importer le certificat.

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

Étape 13

Une confirmation de l'importation du certificat s'affiche. Click OK.

Certificate Import Wizard



The import was successful.

OK

Étape 14

Ouvrez Cisco AnyConnect et essayez de vous reconnecter. Vous ne devriez plus voir l'avertissement Serveur non approuvé.

Conclusion

Voilà ! Vous avez maintenant correctement appris les étapes d'installation d'un certificat auto-signé en tant que source fiable sur un ordinateur Windows, afin d'éliminer l'avertissement " Untrust Server " dans AnyConnect.

Ressources supplémentaires

[Dépannage de base Guide de l'administrateur AnyConnect version 4.9 Notes de version d'AnyConnect - 4.9 Présentation et meilleures pratiques de Cisco Business VPN](#)