

AnyConnect により、信頼できるソースとしての自己署名証明書のインストール

目的

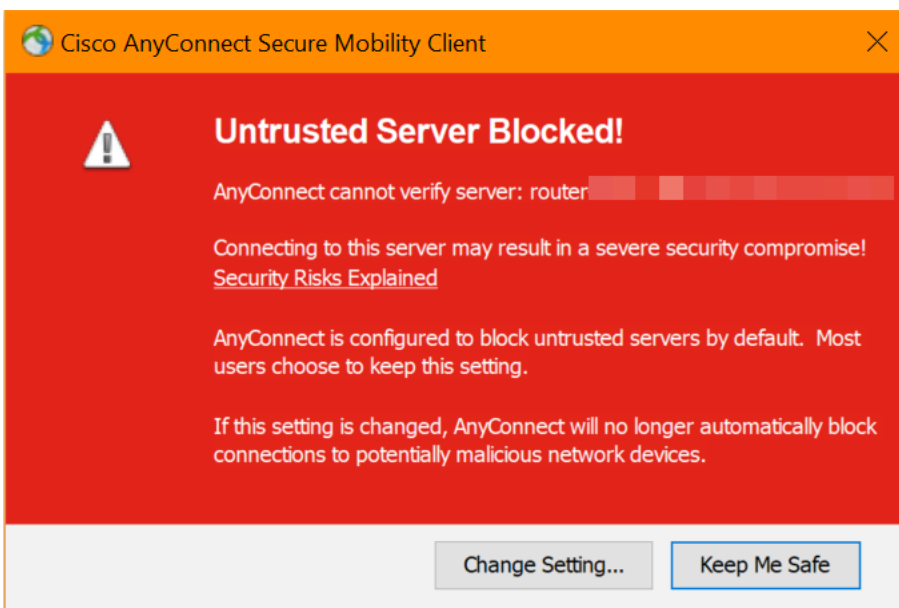
この記事の目的は、Windowsマシンで自己署名証明書を信頼できるソースとして作成し、インストールする手順を説明することです。これにより、AnyConnectで「Untrusted Server」という警告が表示されなくなります。

概要

Cisco AnyConnectバーチャルプライベートネットワーク(VPN)モビリティクライアントは、リモートユーザにセキュアなVPN接続を提供します。Cisco Secure Sockets Layer(SSL)VPNクライアントの利点を提供し、ブラウザベースのSSL VPN接続で使用できないアプリケーションや機能をサポートします。リモートワーカーが一般的に使用するAnyConnect VPNを使用すると、従業員は、たとえオフィスにいなくても、物理的にオフィスにいるかのように企業ネットワークインフラストラクチャに接続できます。これにより、従業員の柔軟性、モビリティ、生産性が向上します。

証明書は通信プロセスで重要であり、個人またはデバイスのIDの確認、サービスの認証、ファイルの暗号化に使用されます。自己署名証明書は、独自の作成者によって署名されたSSL証明書です。

AnyConnect VPN Mobility Clientに初めて接続する場合、次の図に示すように、「Untrusted Server」という警告が表示されることがあります。



この問題を解決するには、この記事の手順に従って、Windowsマシンに信頼できるソースとして自己署名証明書をインストールします。

エクスポートされた証明書を適用する際は、AnyconnectがインストールされているクライアントPCに証明書が置かれていることを確認してください。

AnyConnectソフトウェアバージョン

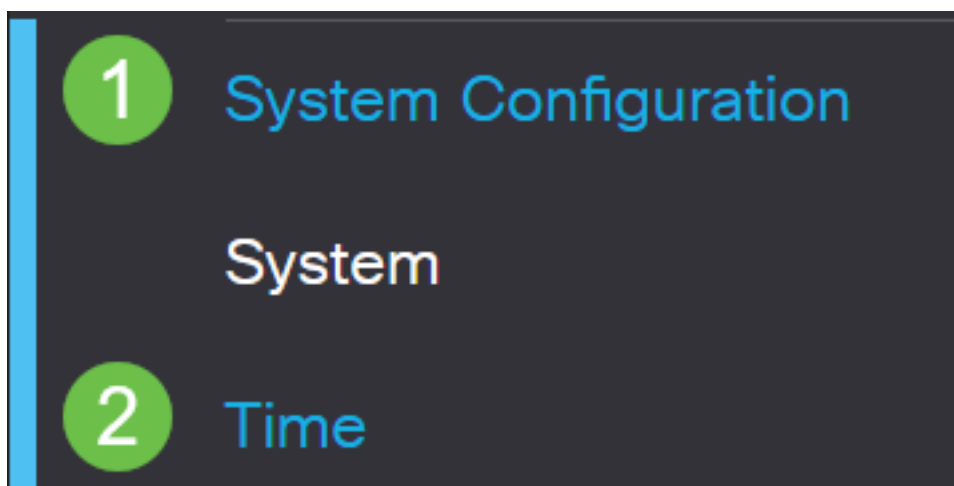
- AnyConnect - v4.9.x(最新のダウンロード)

時間設定の確認

前提条件として、タイムゾーンや夏時間の設定など、ルータに正しい時刻が設定されていることを確認する必要があります。

手順 1

[システム構成] > [時刻]に移動します。



手順 2

すべてが正しく設定されていることを確認します。

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

自己署名証明書の作成

手順 1

RV34xシリーズルータにログインし、[Administration] > [Certificate]に移動します。



Getting Started



Status and Statistics



Administration

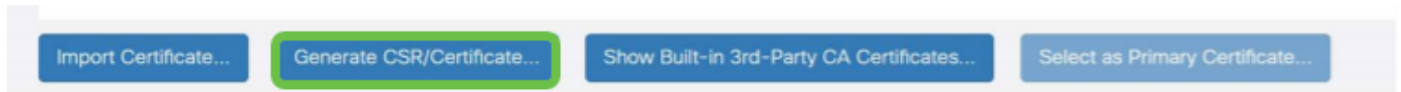
1

File Management

Reboot

手順 2

[Generate CSR/Certificate]をクリックします。

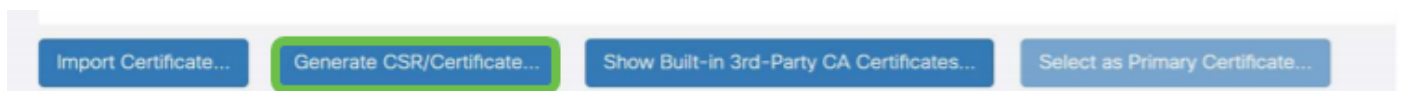


手順 3

次の情報を入力します。

- Type:自己署名証明書
- 証明書名：(任意の名前)
- サブジェクト代替名：WANポートでIPアドレスを使用する場合は、ボックスの下の[IP Address]を選択します。完全修飾ドメイン名を使用する場合は[FQDN]を選択します。ボックスに、WANポートのIPアドレスまたはFQDNを入力します。
- 国名(C):デバイスがある国を選択します
- 都道府県(ST):デバイスが配置されている都道府県を選択します
- ローカリティ名(L): (オプション) デバイスがある場所を選択します。これは、都市、都市などである可能性があります。
- 組織名(O):(オプション)
- 組織単位名(OU):会社名
- 共通名(CN):これは、サブジェクト代替名として設定されたものと一致する必要があります
- 電子メールアドレス(E):(オプション)
- [Key Encryption Length]:2048
- 有効期間：証明書が有効になる時間はどのくらいですか。デフォルトは、360 日です。この値は、10,950日または30年間まで、任意の値に調整できます。

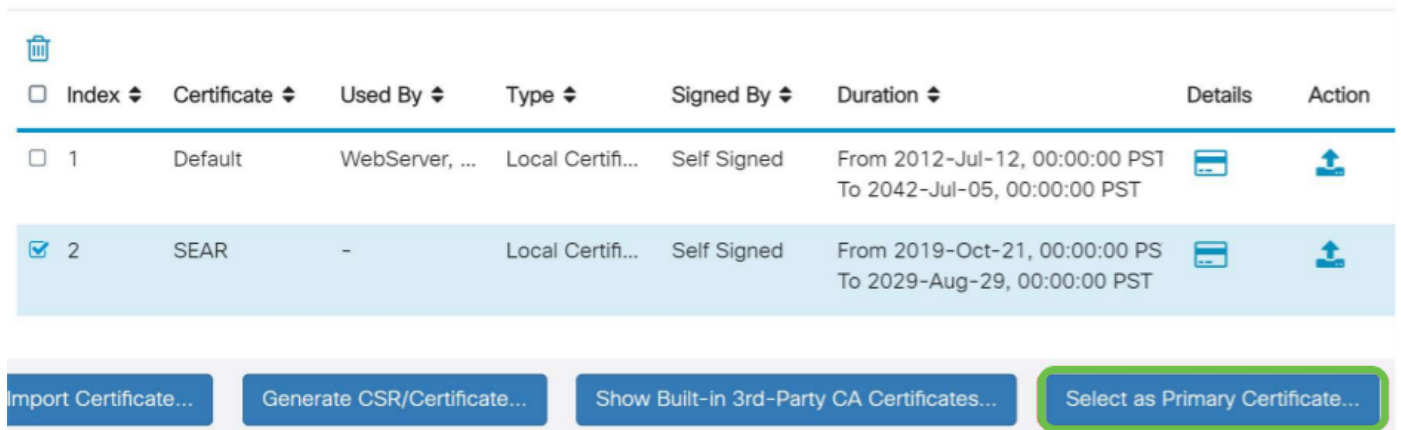




[Generate]をクリックします。



手順 4

作成したばかりの証明書を選択し、「プライマリ証明書として選択」をクリックします。

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...**

手順 5

Webユーザインターフェイス(UI)を更新します。新しい証明書であるため、再度ログインする必要があります。ログインしたら、[VPN] > [SSL VPN]に移動します。

1

VPN

VPN Status

IPSec Profiles

Site-to-Site

Client-to-Site

Teleworker VPN Client

PPTP Server

L2TP Server

GRE Tunnel

2

SSL VPN

手順 6

証明書ファイルを新しく作成した証明書に変更します。

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!"/>	

ステップ7

[Apply] をクリックします。

<input type="button" value="Apply"/>	<input type="button" value="Close"/>
--------------------------------------	--------------------------------------

自己署名証明書のインストール

Windowsマシンに自己署名証明書を信頼できるソースとしてインストールし、AnyConnectで「信頼できないサーバ」という警告が表示されないようにするには、次の手順を実行します。

手順 1

RV34xシリーズルータにログインし、[Administration] > [Certificate]に移動します。



Getting Started



Status and Statistics

手順 2

デフォルトの自己署名証明書を選択し、[Export]ボタンをクリックして証明書をダウンロードします。

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		

手順 3

[証明書のエクスポート]ウィンドウで、証明書のパスワードを入力します。[パスワードの確認]フィールドにパスワードを再入力し、[エクスポート]をクリックします。

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

手順 4

証明書が正常にダウンロードされたことを通知するポップアップウィンドウが表示されます。[OK] をクリックします。

Information

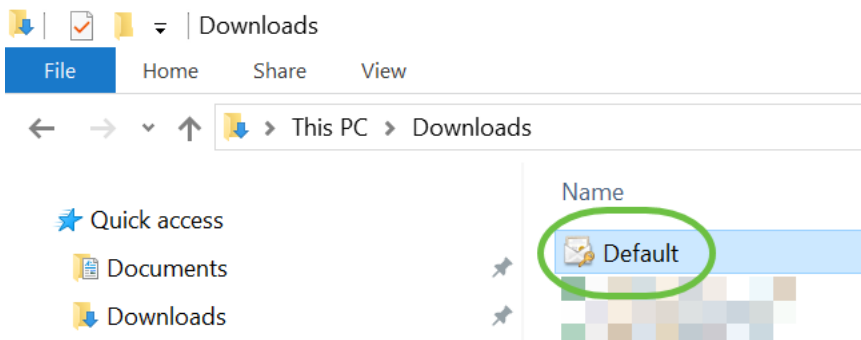


Success

Ok

手順 5

証明書がPCにダウンロードされたら、ファイルを見つけてダブルクリックします。



手順 6

[証明書のインポートウィザード]ウィンドウが表示されます。[ストアの場所]で、[ローカルマシン]を選択します。[next] をクリックします。

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

ステップ7

次の画面に、証明書の場所と情報が表示されます。[next] をクリックします。

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)

手順 8

証明書に選択したパスワードを入力し、[Next]をクリックします。

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

手順 9

次の画面で、[Place all certificates in the following store]を選択し、[Browse]をクリックします。

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

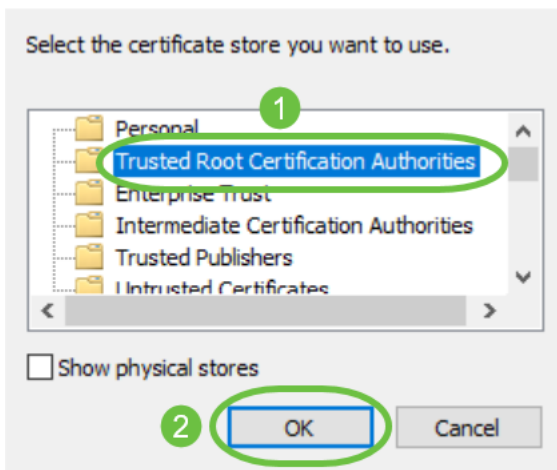
Certificate store:

2

Browse...

手順 10

[Trusted Root Certification Authorities]を選択し、[OK]をクリックします。



手順 11

[next] をクリックします。

← 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

ステップ 12

設定の概要が表示されます。[Finish]をクリックし、証明書をインポートします。

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

手順 13

証明書が正常にインポートされたことを確認するメッセージが表示されます。[OK] をクリックします。

Certificate Import Wizard



The import was successful.

OK

ステップ 14

Cisco AnyConnectを開き、再度接続を試みます。信頼できないサーバの警告が表示されなくなります。

結論

そこだ！これで、自己署名証明書を信頼できるソースとしてWindowsマシンにインストールする手順が正しく学習され、AnyConnectの「信頼できないサーバ」の警告が表示されなくなります。

その他のリソース

基本的なトラブルシューティング AnyConnect管理者ガイドリリース4.9 AnyConnectリリースノート - 4.9 Cisco Business VPNの概要とベストプラクティス