

AnyConnect Installieren eines selbstsignierten Zertifikats als vertrauenswürdige Quelle

Ziel

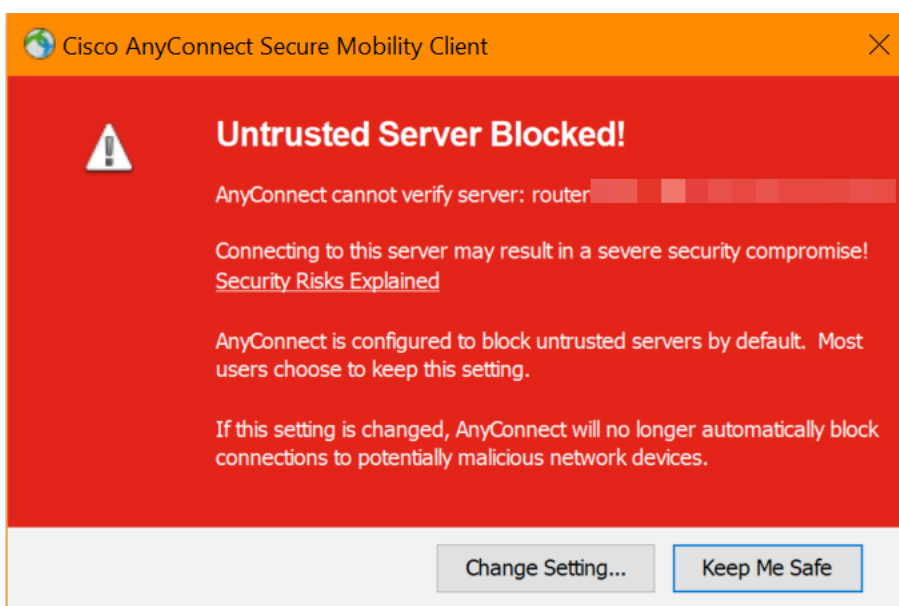
In diesem Artikel erfahren Sie, wie Sie ein selbstsigniertes Zertifikat als vertrauenswürdige Quelle auf einem Windows-Computer erstellen und installieren. Dadurch wird die Warnung "Nicht vertrauenswürdiger Server" in AnyConnect entfernt.

Einführung

Der Cisco AnyConnect Virtual Private Network (VPN) Mobility Client stellt Remote-Benutzern eine sichere VPN-Verbindung zur Verfügung. Sie bietet die Vorteile eines Cisco Secure Sockets Layer (SSL)-VPN-Clients und unterstützt Anwendungen und Funktionen, die für eine browserbasierte SSL VPN-Verbindung nicht verfügbar sind. AnyConnect VPN wird häufig von Remote-Mitarbeitern verwendet und ermöglicht es Mitarbeitern, eine Verbindung zur Netzwerkinfrastruktur des Unternehmens herzustellen, so als ob sie sich direkt im Büro aufhielten, selbst wenn dies nicht der Fall ist. Dies erhöht die Flexibilität, Mobilität und Produktivität Ihrer Mitarbeiter.

Zertifikate sind für den Kommunikationsprozess wichtig und dienen dazu, die Identität einer Person oder eines Geräts zu überprüfen, einen Dienst zu authentifizieren oder Dateien zu verschlüsseln. Ein selbst signiertes Zertifikat ist ein SSL-Zertifikat, das von einem eigenen Ersteller signiert wird.

Wenn Benutzer zum ersten Mal eine Verbindung zum AnyConnect VPN Mobility Client herstellen, wird möglicherweise die Warnung "Untrusted Server" angezeigt, wie in der Abbildung unten gezeigt.



Befolgen Sie die Schritte in diesem Artikel, um ein selbstsigniertes Zertifikat als vertrauenswürdige Quelle auf einem Windows-Computer zu installieren, um dieses

Problem zu beheben.

Stellen Sie beim Anwenden des exportierten Zertifikats sicher, dass es auf dem Client-PC mit installiertem AnyConnect abgelegt wird.

Version der AnyConnect-Software

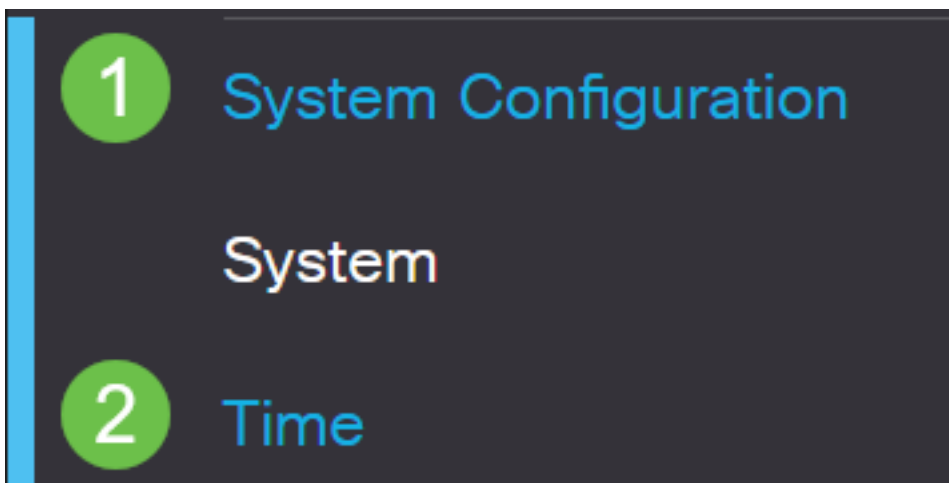
- AnyConnect - v4.9.x ([neueste Version herunterladen](#))

Zeiteinstellungen überprüfen

Voraussetzung ist, dass der Router die richtige Zeiteinstellung hat, einschließlich der Zeitzone und der Sommerzeiteinstellungen.

Schritt 1

Navigieren Sie zu **Systemkonfiguration > Zeit**.



Schritt 2

Stellen Sie sicher, dass alle Einstellungen korrekt sind.

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

Erstellen eines selbstsignierten Zertifikats

Schritt 1

Melden Sie sich beim Router der Serie RV34x an, und navigieren Sie zu **Administration > Certificate**.



Getting Started



Status and Statistics



Administration

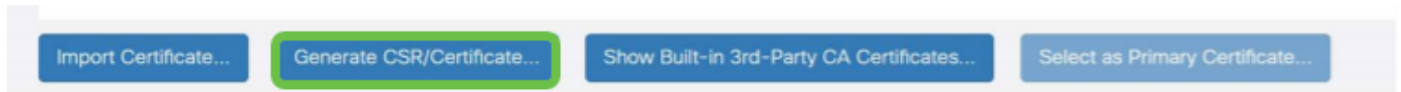
1

File Management

Reboot

Schritt 2

Klicken Sie auf **CSR/Zertifikat generieren**.

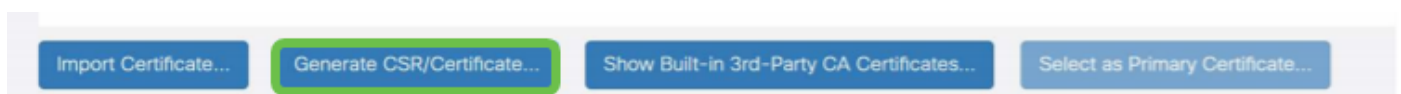


Schritt 3

Geben Sie die folgenden Informationen an:

- Typ: Selbstsigniertes Zertifikat
- Zertifikatsname: (Beliebiger Name, den Sie auswählen)
- Alternativer Betreff-Name: Wenn eine IP-Adresse auf dem WAN-Port verwendet wird, wählen Sie unterhalb des Felds die **IP-Adresse** oder **FQDN aus**, wenn Sie den vollqualifizierten Domännennamen verwenden. Geben Sie in das Feld die IP-Adresse oder den FQDN des WAN-Ports ein.
- Ländername (C): Wählen Sie das Land aus, in dem sich das Gerät befindet.
- Bundesland (ST): Wählen Sie das Bundesland oder die Provinz aus, in dem das Gerät installiert ist.
- Ortsname (L): (Optional) Wählen Sie den Ort aus, an dem sich das Gerät befindet. Dies könnte eine Stadt, eine Stadt usw. sein.
- Name der Organisation (O): (Optional)
- Name der Organisationseinheit (OB): Firmenname
- Common Name (CN): Dieser MUSS mit dem als Subject Alternative Name (Alternativer Name) festgelegten Namen übereinstimmen.
- E-Mail-Adresse: (Optional)
- Schlüssellänge für Verschlüsselung: 2048
- Gültige Dauer: So lange ist das Zertifikat gültig. Der Standardwert ist 360 Tage. Sie können dies an jeden beliebigen Wert anpassen, bis zu 10.950 Tage oder 30 Jahre.

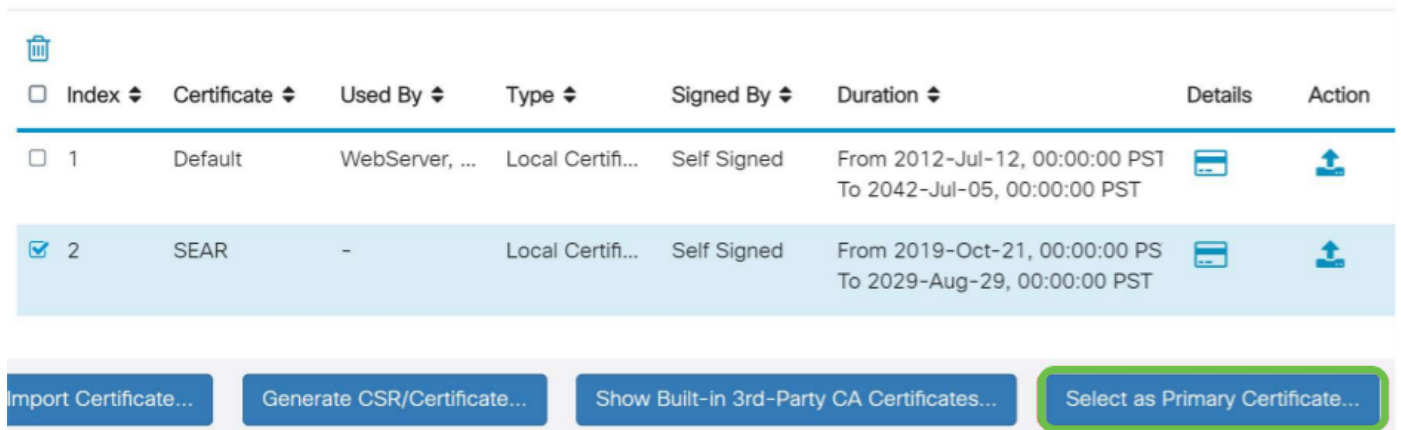
Klicken Sie auf **Generieren**.



Schritt 4

Wählen Sie das gerade erstellte Zertifikat aus, und klicken Sie auf **Als primäres Zertifikat auswählen**.

Certificate Table



The image shows a 'Certificate Table' with a trash icon at the top left. The table has columns: Index, Certificate, Used By, Type, Signed By, Duration, Details, and Action. There are two rows of certificates. The second row is highlighted in light blue. Below the table is a row of four buttons: 'Import Certificate...', 'Generate CSR/Certificate...', 'Show Built-in 3rd-Party CA Certificates...', and 'Select as Primary Certificate...' (which is highlighted with a green border).

<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...**

Schritt 5

Aktualisieren der Webbenutzeroberfläche (UI) Da es sich um ein neues Zertifikat handelt, müssen Sie sich erneut anmelden. Wenn Sie sich angemeldet haben, gehen Sie zu **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

Schritt 6

Ändern Sie die **Zertifikatsdatei** in das neu erstellte Zertifikat.

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!"/>	

Schritt 7

Klicken Sie auf **Apply** (Anwenden).

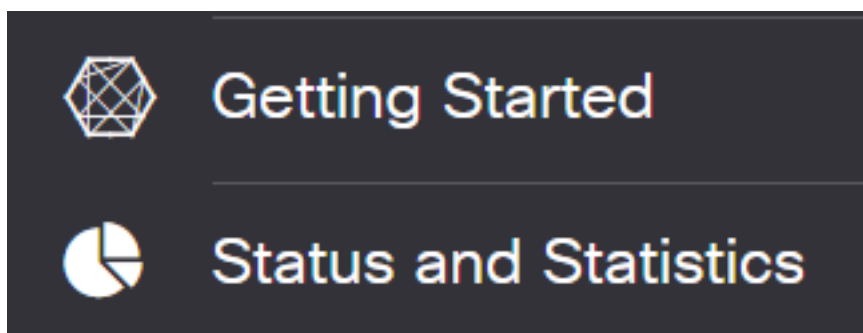


Installieren eines selbstsignierten Zertifikats

So installieren Sie ein selbstsigniertes Zertifikat als vertrauenswürdige Quelle auf einem Windows-Computer, um die Warnung "Nicht vertrauenswürdiger Server" in AnyConnect zu entfernen:

Schritt 1

Melden Sie sich beim Router der Serie RV34x an, und navigieren Sie zu **Administration > Certificate**.



Schritt 2

Wählen Sie das selbst signierte Standardzertifikat aus, und klicken Sie auf die Schaltfläche **Exportieren**, um das Zertifikat herunterzuladen.

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		

Schritt 3

Geben Sie im Fenster *Zertifikat exportieren* ein Kennwort für Ihr Zertifikat ein. Geben Sie das Kennwort erneut in das Feld *Kennwort bestätigen* ein, und klicken Sie dann auf **Exportieren**.

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

Schritt 4

Sie sehen ein Popup-Fenster, in dem Sie benachrichtigt werden, dass das Zertifikat erfolgreich heruntergeladen wurde. Klicken Sie auf **OK**.

Information

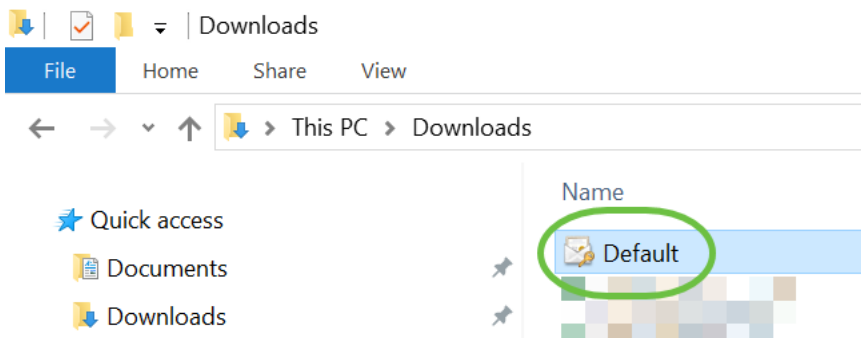


Success



Schritt 5

Sobald das Zertifikat auf den Computer heruntergeladen wurde, suchen Sie die Datei, und doppelklicken Sie darauf.



Schritt 6

Das Fenster *Certificate Import Wizard* (Assistent zum Importieren von Zertifikaten) wird angezeigt. Wählen Sie als *Speicherstandort* die Option **Lokaler Computer aus**. Klicken Sie auf **Weiter**.

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

Schritt 7

Auf dem folgenden Bildschirm werden Zertifikatsspeicherort und -informationen angezeigt. Klicken Sie auf **Weiter**.

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)

Schritt 8

Geben Sie das *Kennwort* ein, das Sie für das Zertifikat ausgewählt haben, und klicken Sie auf **Weiter**.

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

Schritt 9

Wählen Sie im nächsten Bildschirm die Option **Alle Zertifikate im folgenden Speicher platzieren aus**, und klicken Sie dann auf **Durchsuchen**.

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

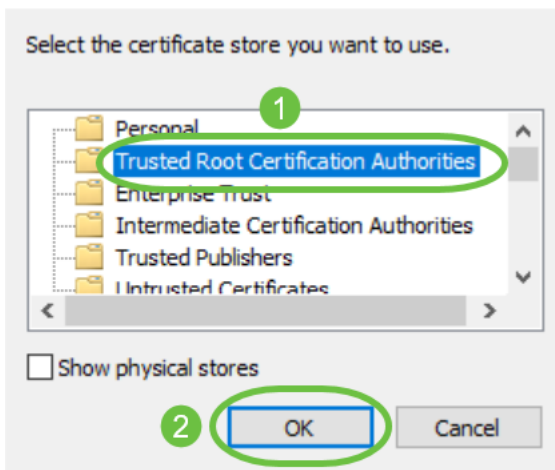
Certificate store:

2

Browse...


Schritt 10

Wählen Sie **Vertrauenswürdige Stammzertifizierungsstellen** und klicken Sie auf **OK**.



Schritt 11

Klicken Sie auf **Weiter**.

←  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

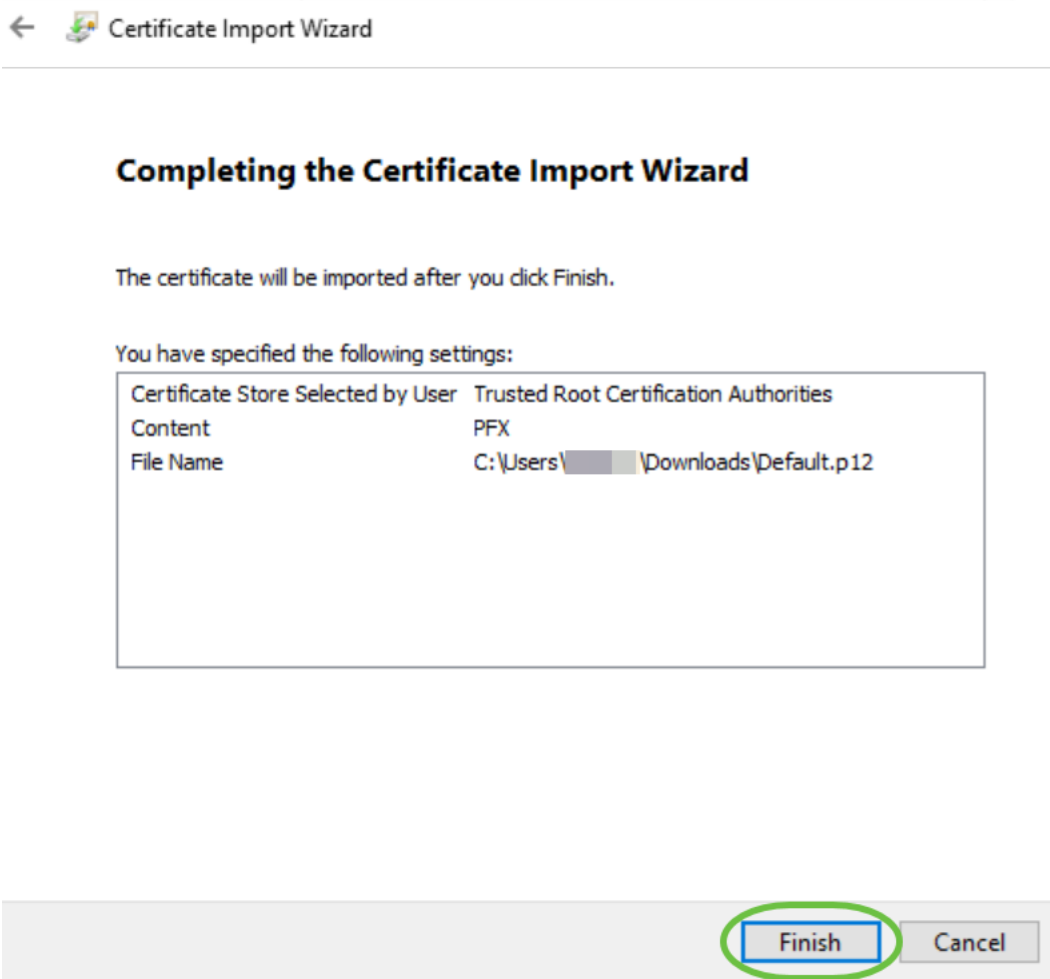
Browse...

Next

Cancel

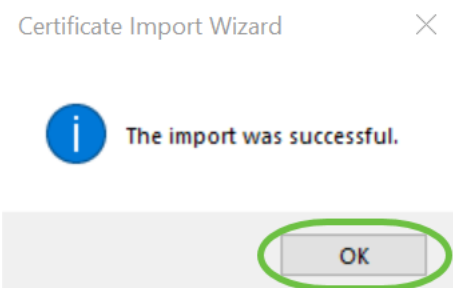
Schritt 12

Eine Zusammenfassung der Einstellungen wird angezeigt. Klicken Sie auf **Fertig stellen**, um das Zertifikat zu importieren.



Schritt 13

Sie sehen eine Bestätigung, dass das Zertifikat erfolgreich importiert wurde. Klicken Sie auf **OK**.



Schritt 14

Öffnen Sie Cisco AnyConnect, und versuchen Sie erneut, eine Verbindung herzustellen. Sie sollten die Warnung Nicht vertrauenswürdiger Server nicht mehr sehen.

Fazit

Da hast du es! Sie haben nun die Schritte zur Installation eines selbstsignierten Zertifikats als vertrauenswürdige Quelle auf einem Windows-Computer erfolgreich gelernt, um die Warnung "Nicht vertrauenswürdiger Server" in AnyConnect zu beseitigen.

Zusätzliche Ressourcen

[Grundlegende Fehlerbehebung AnyConnect Administratorhandbuch Version 4.9 Versionshinweise zu AnyConnect - 4.9 Cisco Business VPN - Überblick und Best Practices](#)