

# AnyConnect: Installazione di un certificato autofirmato come fonte attendibile

## Obiettivo

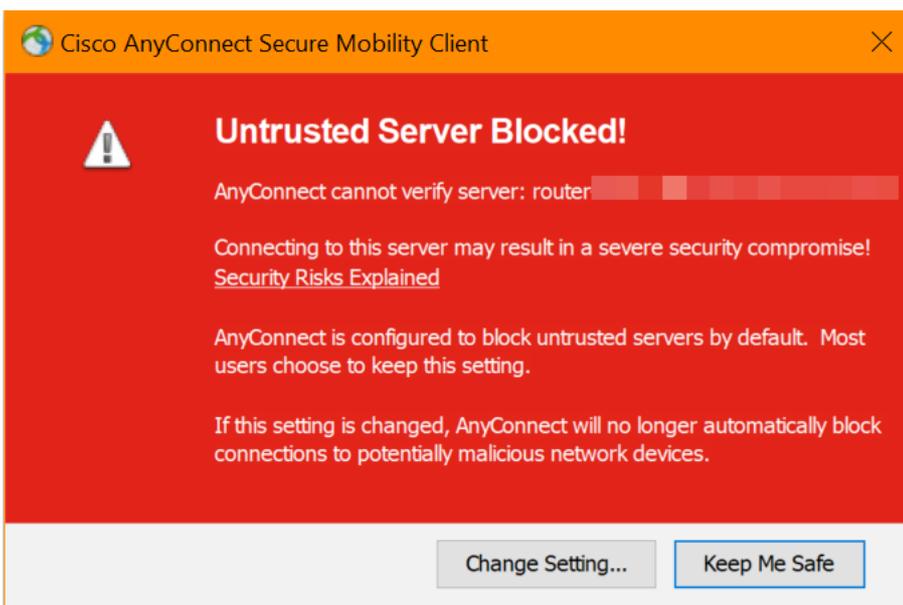
L'obiettivo di questo articolo consiste nel fornire assistenza durante la creazione e l'installazione di un certificato autofirmato come fonte attendibile in un computer Windows. In questo modo si elimina l'avviso "Server non attendibile" in AnyConnect.

## Introduzione

Il client di mobilità Cisco AnyConnect Virtual Private Network (VPN) offre agli utenti remoti una connessione VPN sicura. Offre i vantaggi di un client VPN Cisco Secure Sockets Layer (SSL) e supporta applicazioni e funzioni non disponibili per una connessione VPN SSL basata su browser. Comunemente utilizzata da utenti remoti, AnyConnect VPN consente ai dipendenti di connettersi all'infrastruttura di rete aziendale come se fossero fisicamente in ufficio, anche quando non lo sono. Ciò aumenta la flessibilità, la mobilità e la produttività dei dipendenti.

I certificati sono importanti nel processo di comunicazione e vengono utilizzati per verificare l'identità di una persona o di un dispositivo, autenticare un servizio o crittografare i file. Il certificato autofirmato è un certificato SSL firmato dal proprio creatore.

Quando ci si connette a AnyConnect VPN Mobility Client per la prima volta, è possibile che venga visualizzato un avviso di server non attendibile, come mostrato nell'immagine seguente.



Per eliminare il problema, eseguire la procedura descritta in questo articolo per installare un certificato autofirmato come fonte attendibile in un computer Windows.

Quando si applica il certificato esportato, accertarsi che venga inserito sul PC client con

Anyconnect installato.

## Versione del software AnyConnect

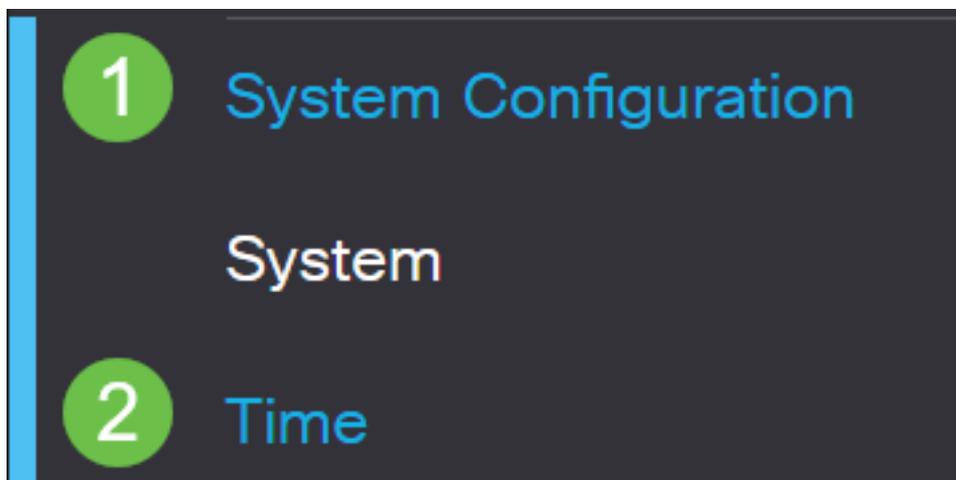
- AnyConnect v4.9.x ([scarica la versione più recente](#))

## Verifica impostazioni ora

Come prerequisito, è necessario verificare che sul router sia impostata l'ora corretta, incluse le impostazioni di fuso orario e ora legale.

### Passaggio 1

Selezionare **Configurazione di sistema > Tempo**.



### Passaggio 2

Assicurarsi che tutto sia impostato correttamente.

# 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

## Creazione di un certificato autofirmato

### Passaggio 1

Accedere al router della serie RV34x e selezionare **Amministrazione > Certificato**.



Getting Started



Status and Statistics



Administration

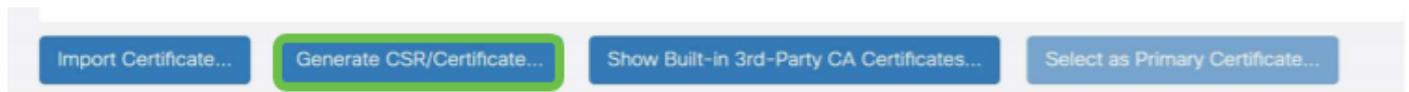
1

File Management

Reboot

## Passaggio 2

Fare clic su **Generate CSR/Certificate**.



## Passaggio 3

Immettere le informazioni seguenti:

- Tipo: Certificato autofirmato
- Nome certificato: (Qualsiasi nome scelto)
- Nome alternativo soggetto: Se sulla porta WAN verrà utilizzato un indirizzo IP, selezionare **Indirizzo IP** sotto la casella o **FQDN** se si intende utilizzare il nome di dominio completo. Nella casella, immettere l'indirizzo IP o il nome di dominio completo della porta WAN.
- Nome paese (C): Selezionare il paese in cui si trova il dispositivo
- Nome provincia (ST): Selezionare la provincia in cui si trova il dispositivo
- Nome località (L): (Facoltativo) Selezionare la Località in cui si trova il dispositivo. Potrebbe essere una città, una città, ecc.
- Nome organizzazione (O): (Facoltativo)
- Nome unità organizzativa: Nome società
- Nome comune (CN): DEVE corrispondere a quello impostato come Nome alternativo soggetto
- Indirizzo e-mail (E): (Facoltativo)
- Lunghezza crittografia chiave: 2048
- Durata validità: Indica per quanto tempo il certificato sarà valido. L'impostazione predefinita è 360 giorni. Potete regolare questo valore in base alle vostre esigenze, fino a 10.950 giorni o 30 anni.

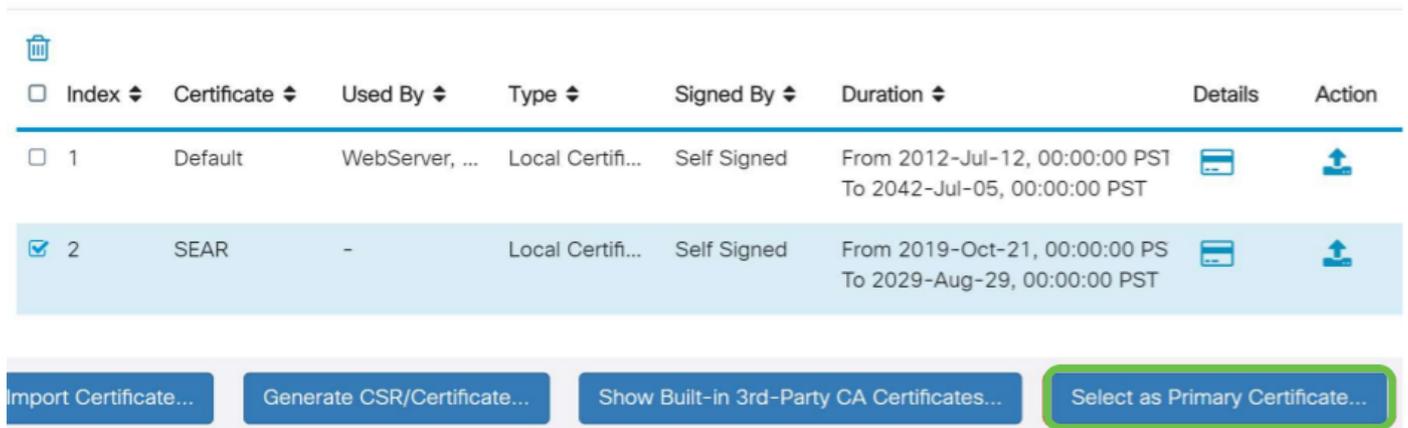
Fare clic su **Genera**.



## Passaggio 4

Selezionare il certificato appena creato e fare clic su **Seleziona come certificato principale**.

## Certificate Table



The image shows a 'Certificate Table' interface. At the top left is a trash icon. Below it is a table with columns: Index, Certificate, Used By, Type, Signed By, Duration, Details, and Action. There are two rows of certificates. The first row is unselected, and the second row is selected. 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...'. The 'Select as Primary Certificate...' button 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...**

## Passaggio 5

Aggiornare l'interfaccia utente Web. Poiché si tratta di un nuovo certificato, sarà necessario eseguire nuovamente l'accesso. Una volta eseguito l'accesso, passare a **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

### Passaggio 6

Sostituire **File certificato** con il nuovo certificato creato.

# 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!"/>	

## Passaggio 7

Fare clic su **Apply** (Applica).

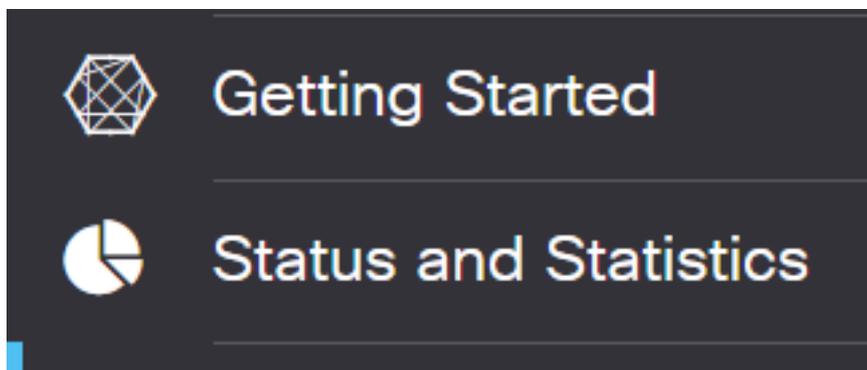


## Installazione di un certificato autofirmato

Per installare un certificato autofirmato come origine attendibile su un computer Windows, eliminare l'avviso "Server non attendibile" in AnyConnect e attenersi alla seguente procedura:

## Passaggio 1

Accedere al router della serie RV34x e selezionare **Amministrazione > Certificato**.



## Passaggio 2

Selezionare il certificato autofirmato predefinito e fare clic sul pulsante **Esporta** per scaricare il certificato.

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		

## Passaggio 3

Nella finestra *Esporta certificato* immettere una password per il certificato. Immettere nuovamente la password nel campo *Conferma password* e fare clic su **Esporta**.

### 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

## Passaggio 4

Verrà visualizzata una finestra popup per indicare che il download del certificato è stato completato correttamente. Fare clic su **OK**.

# Information

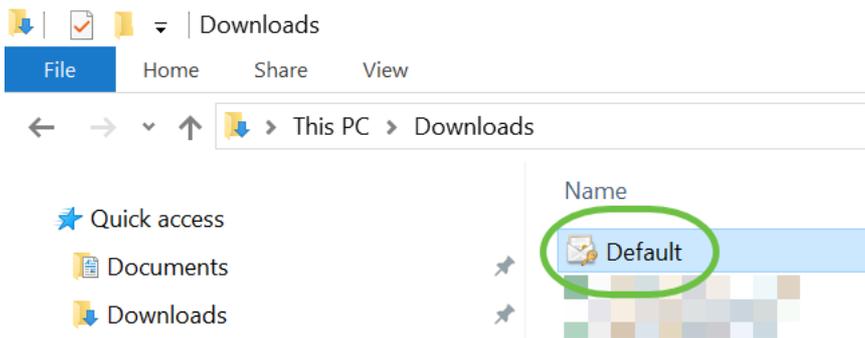


Success

Ok

## Passaggio 5

Dopo aver scaricato il certificato nel PC, individuare il file e fare doppio clic su di esso.



## Passaggio 6

Verrà visualizzata la finestra *Importazione guidata certificati*. Per il *Percorso archivio*, selezionare **Computer locale**. Fare clic su **Next** (Avanti).

## 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**

### Passaggio 7

Nella schermata seguente verranno visualizzati il percorso e le informazioni del certificato. Fare clic su **Next** (Avanti).

**File to Import**

Specify the file you want to import.

File name:

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

Browse...

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)

Next

Cancel

**Passaggio 8**

Immettere la *password* selezionata per il certificato e fare clic su **Avanti**.

### 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

## Passaggio 9

Nella schermata successiva selezionare **Mettere tutti i certificati nel seguente archivio** e quindi fare clic su **Sfoggia**.

### 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

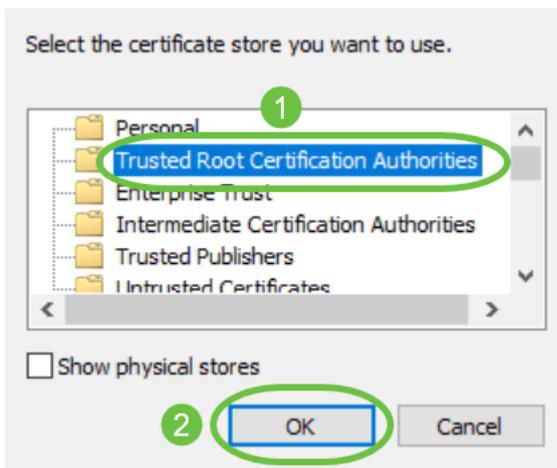
Certificate store:

2

Browse...

## Passaggio 10

Selezionare **Autorità di certificazione principali attendibili** e fare clic su **OK**.



## Passaggio 11

Fare clic su **Next** (Avanti).

←  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

## Passaggio 12

Verrà visualizzato un riepilogo delle impostazioni. Fare clic su **Fine** per importare il certificato.

## 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

### Passaggio 13

Verrà visualizzata una conferma dell'avvenuta importazione del certificato. Fare clic su OK.

Certificate Import Wizard



The import was successful.

OK

### Passaggio 14

Aprire Cisco AnyConnect e riprovare a connettersi. L'avviso Server non attendibile non verrà più visualizzato.

## Conclusioni

Ecco qua! A questo punto, sono stati completati i passaggi per installare un certificato autofirmato come origine attendibile su un computer Windows, in modo da eliminare l'avviso "Server non attendibile" in AnyConnect.

### Ulteriori risorse

[Risoluzione dei problemi di base Guida per l'amministratore di AnyConnect release 4.9 Note sulla release di AnyConnect - 4.9 Panoramica e best practice di Cisco Business VPN](#)