

AnyConnect: Instalação de um certificado autoassinado como fonte confiável

Objetivo

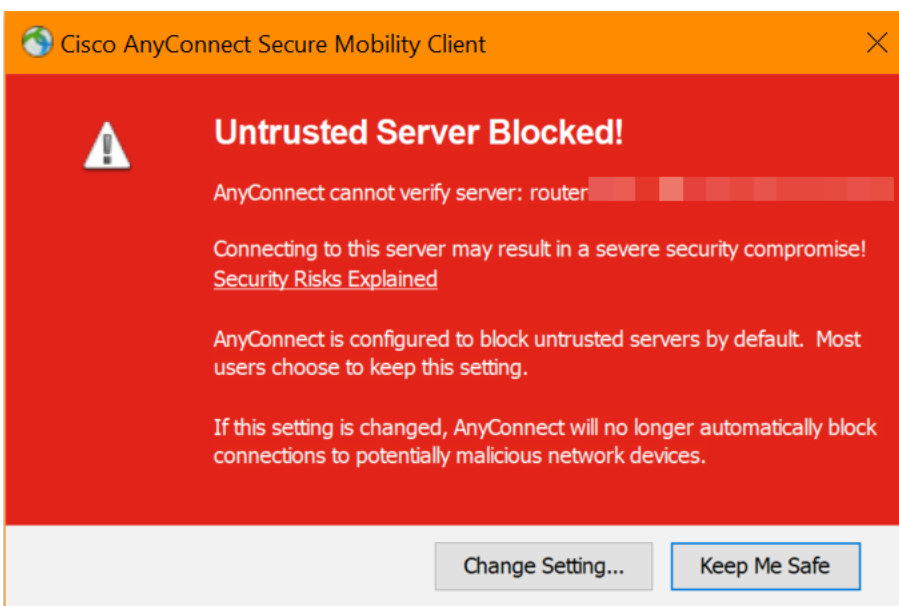
O objetivo deste artigo é guiá-lo pela criação e instalação de um certificado autoassinado como uma fonte confiável em uma máquina Windows. Isso eliminará o aviso "Servidor não confiável" no AnyConnect.

Introduction

O Cisco AnyConnect Virtual Private Network (VPN) Mobility Client fornece aos usuários remotos uma conexão VPN segura. Ele oferece os benefícios de um cliente VPN Cisco Secure Sockets Layer (SSL) e suporta aplicativos e funções indisponíveis para uma conexão VPN SSL baseada em navegador. Geralmente usado por funcionários remotos, o AnyConnect VPN permite que os funcionários se conectem à infraestrutura de rede corporativa como se estivessem fisicamente no escritório, mesmo quando não estão. Isso aumenta a flexibilidade, a mobilidade e a produtividade de seus funcionários.

Os certificados são importantes no processo de comunicação e são usados para verificar a identidade de uma pessoa ou dispositivo, autenticar um serviço ou criptografar arquivos. Certificado autoassinado é um certificado SSL assinado por seu próprio criador.

Ao se conectarem ao AnyConnect VPN Mobility Client pela primeira vez, os usuários podem encontrar um aviso de "Servidor não confiável", como mostrado na imagem abaixo.



Siga as etapas neste artigo para instalar um certificado autoassinado como uma fonte confiável em uma máquina Windows, para eliminar esse problema.

Ao aplicar o certificado exportado, certifique-se de colocá-lo no PC cliente com o Anyconnect instalado.

Versão de software do AnyConnect

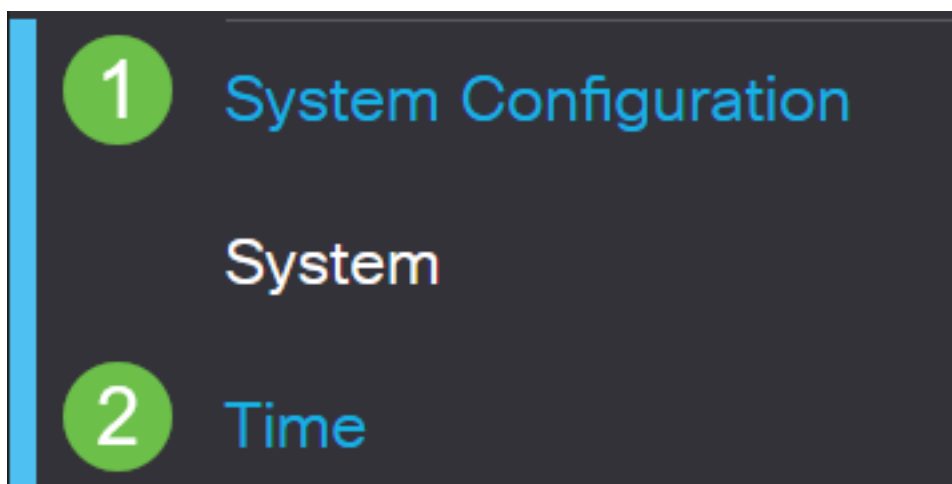
- AnyConnect - v4.9.x ([Download mais recente](#))

Verificar configurações de hora

Como pré-requisito, você precisa garantir que o roteador tenha o horário correto, incluindo as configurações de fuso horário e horário de verão.

Passo 1

Navegue até **Configuração do sistema > Hora**.



Passo 2

Verifique se tudo está definido corretamente.

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

Criar um certificado autoassinado

Passo 1

Efetue login no roteador RV34x series e navegue até **Administration > Certificate**.



Getting Started



Status and Statistics



Administration

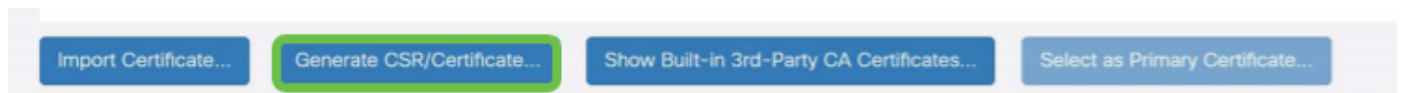
1

File Management

Reboot

Passo 2

Clique em **Gerar CSR/Certificado**.

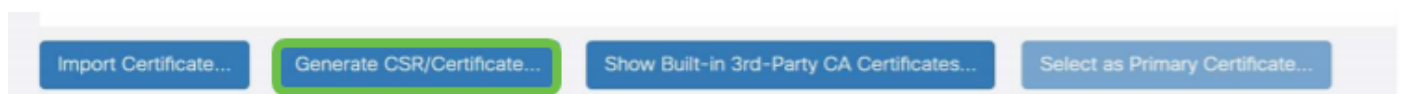


Etapa 3

Preencha as seguintes informações:

- Digite: Certificado autoassinado
- Nome do certificado: (Qualquer nome que você escolher)
- Nome alternativo do assunto: Se um endereço IP for usado na porta WAN, selecione **IP Address (Endereço IP)** abaixo da caixa ou **FQDN** se estiver usando o Fully Qualified Domain Name (Nome de domínio totalmente qualificado). Na caixa, insira o endereço IP ou FQDN da porta WAN.
- Nome do país (C): Selecione o país onde o dispositivo está localizado
- Nome do Estado ou Província (ST): Selecione o Estado ou Província onde o dispositivo está localizado
- Nome da localidade (L): (Opcional) Selecione o local onde o dispositivo está localizado. Isto pode ser uma cidade, uma cidade, etc.
- Nome da organização (O): (Opcional)
- Nome da unidade da organização (OU): Nome da empresa
- Nome comum (CN): Deve corresponder ao que foi definido como o nome alternativo do assunto
- Endereço de e-mail (E): (Opcional)
- Comprimento da criptografia de chave: 2048
- Duração válida: Este é o período de validade do certificado. O padrão é 360 dias. Você pode ajustá-lo a qualquer valor desejado, até 10.950 dias ou 30 anos.

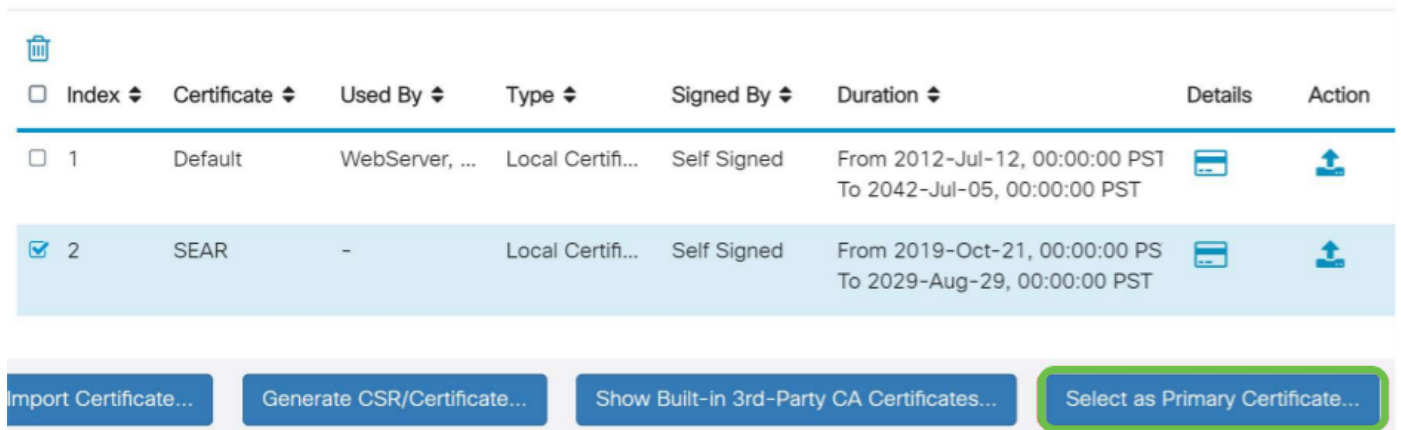
Clique em **Gerar**.







Passo 4

Selecione o certificado que acabou de ser criado e clique em **Selecionar como certificado primário**.

Certificate Table



The image shows a web interface for managing certificates. At the top, there is a 'Certificate Table' header. 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 index 1, 'Default', used by 'WebServer, ...', type 'Local Certifi...', signed by 'Self Signed', and duration 'From 2012-Jul-12, 00:00:00 PST To 2042-Jul-05, 00:00:00 PST'. The second row is index 2, 'SEAR', used by '-', type 'Local Certifi...', signed by 'Self Signed', and duration 'From 2019-Oct-21, 00:00:00 PS To 2029-Aug-29, 00:00:00 PST'. 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.

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...**

Etapa 5

Atualize a Interface de Usuário da Web (IU). Como é um novo certificado, você precisará fazer login novamente. Depois de fazer login, vá para **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

Etapa 6

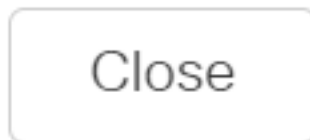
Alterar **Arquivo de Certificado** para Certificado recém-criado.

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!"/>	

Etapa 7

Clique em Apply.

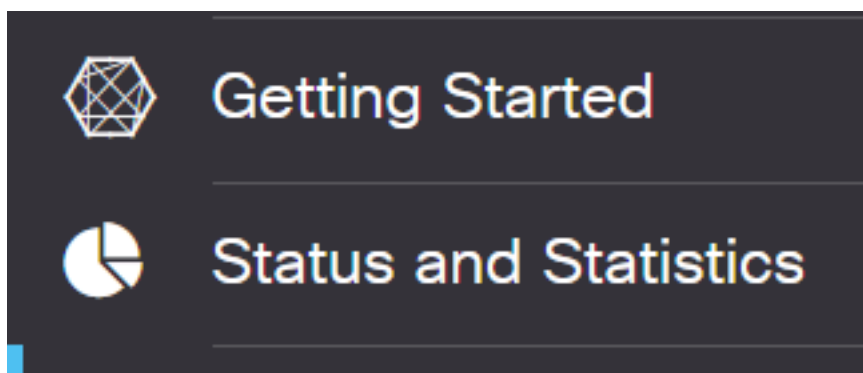


Instalação de um certificado autoassinado

Para instalar um certificado autoassinado como fonte confiável em uma máquina Windows, para eliminar o aviso "Servidor não confiável" no AnyConnect, siga estas etapas:

Passo 1

Efetue login no roteador RV34x series e navegue até **Administration > Certificate**.



Passo 2

Selecione o certificado autoassinado padrão e clique no botão **Exportar** para baixar o certificado.

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		

Etapa 3

Na janela *Exportar certificado*, digite uma senha para o certificado. Digite novamente a senha no campo *Confirmar senha* e clique em **Exportar**.

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

Passo 4

Você verá uma janela pop-up para notificar que o Certificado foi baixado com êxito. Click **OK**.

Information

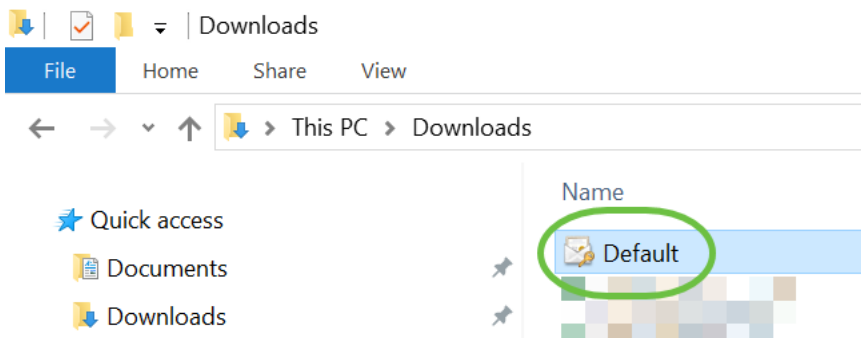


Success

Ok

Etapa 5

Depois de baixar o certificado em seu PC, localize o arquivo e clique duas vezes nele.



Etapa 6

A janela *Assistente de importação de certificado* será exibida. Para o *local da loja*, selecione **Máquina local**. Clique em Next.

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

Etapa 7

Na tela a seguir, o local do certificado e as informações serão exibidos. Clique em Next.

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)

Passo 8

Insira a *Senha* selecionada para o Certificado e clique em **Avançar**.

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

Passo 9

Na próxima tela, selecione **Place all certificate in the seguinte store** e, em seguida, clique em **Browse**.

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

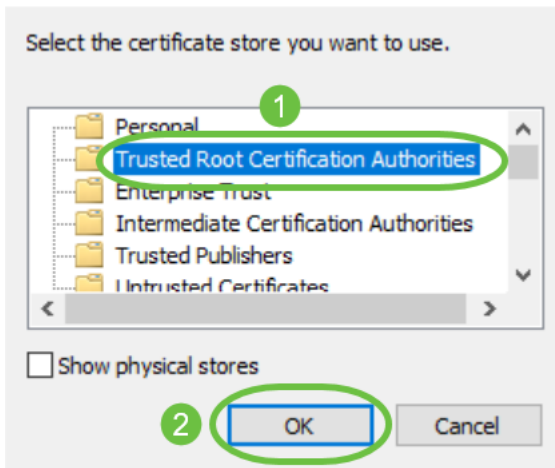
Certificate store:

2

Browse...


Passo 10

Selecione **Autoridades de Certificação de Raiz Confiáveis** e clique em **OK**.



Passo 11

Clique em Next.

←  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

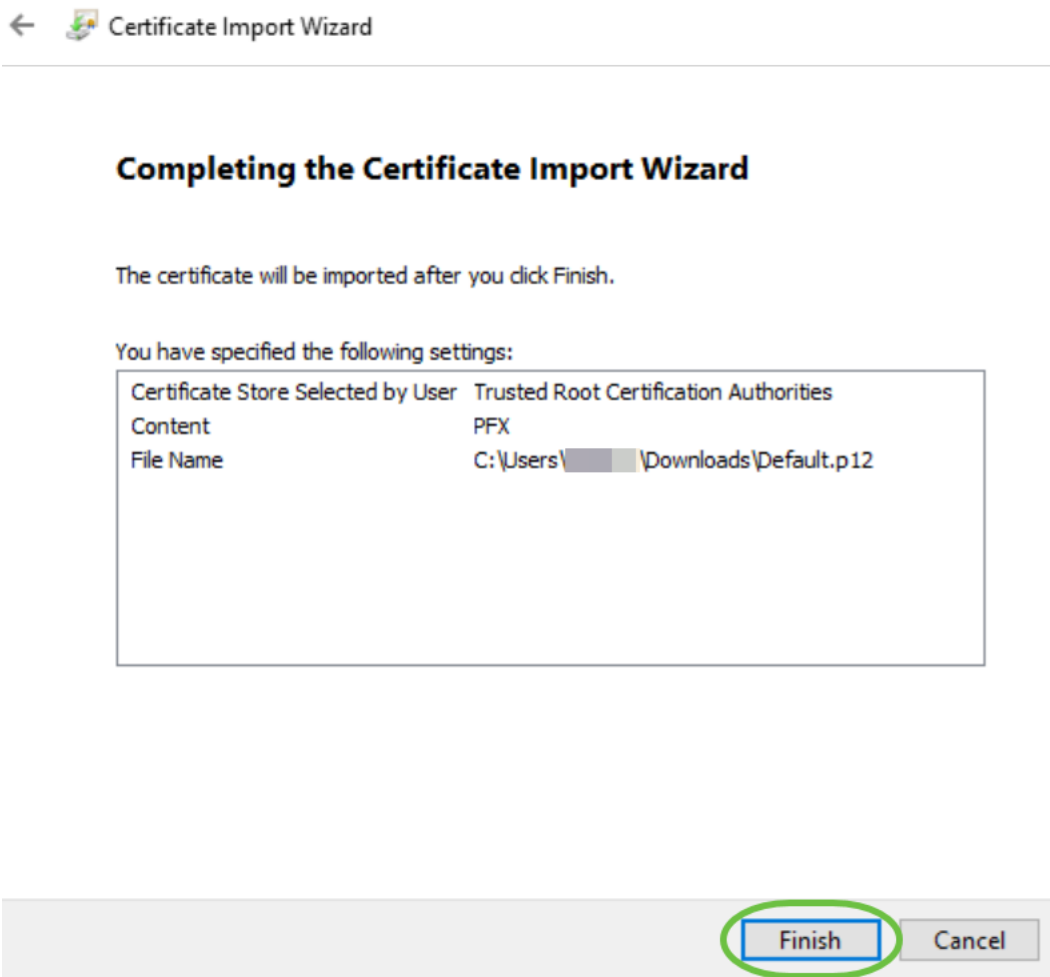
Browse...

Next

Cancel

Etapa 12

Um resumo das configurações será exibido. Clique em **Concluir** para importar o certificado.



Passo 13

Você verá uma confirmação de que o certificado foi importado com êxito. Click **OK**.

Certificate Import Wizard ×

i The import was successful.



Passo 14

Abra o Cisco AnyConnect e tente se conectar novamente. Você não deve mais ver o aviso do servidor não confiável.

Conclusão

Pronto. Agora você aprendeu com êxito as etapas para instalar um certificado autoassinado como uma fonte confiável em uma máquina Windows, para eliminar o aviso "Servidor não confiável" no AnyConnect.

Outros recursos

[Troubleshooting Básico Guia do administrador do AnyConnect versão 4.9 Notas da versão do AnyConnect - 4.9 Visão geral e práticas recomendadas do Cisco Business VPN](#)