

AnyConnect: Instalación de un certificado firmado automáticamente como origen de confianza

Objetivo

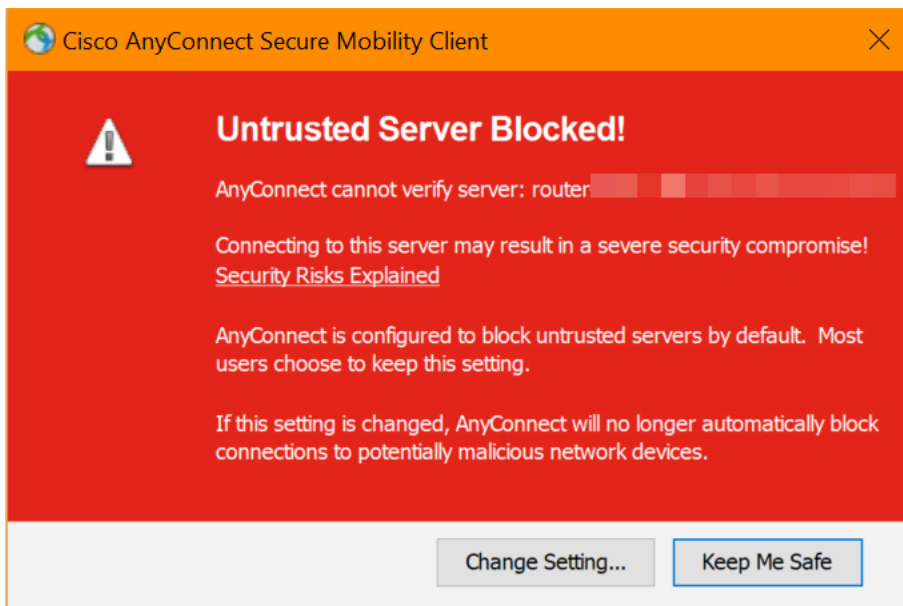
El objetivo de este artículo es guiarle a través de la creación e instalación de un certificado autofirmado como fuente de confianza en un equipo con Windows. Esto eliminará la advertencia "Servidor no fiable" de AnyConnect.

Introducción

Cisco AnyConnect Virtual Private Network (VPN) Mobility Client proporciona a los usuarios remotos una conexión VPN segura. Proporciona las ventajas de un cliente VPN de Cisco Secure Sockets Layer (SSL) y admite aplicaciones y funciones que no están disponibles para una conexión VPN SSL basada en navegador. AnyConnect VPN, que suelen utilizar los trabajadores remotos, permite a los empleados conectarse a la infraestructura de red corporativa como si estuvieran físicamente en la oficina, incluso cuando no lo están. Esto aumenta la flexibilidad, la movilidad y la productividad de sus trabajadores.

Los certificados son importantes en el proceso de comunicación y se utilizan para verificar la identidad de una persona o dispositivo, autenticar un servicio o cifrar archivos. El certificado autofirmado es un certificado SSL firmado por su propio creador.

Cuando se conecta a AnyConnect VPN Mobility Client por primera vez, los usuarios pueden encontrar una advertencia de "Servidor no fiable", como se muestra en la siguiente imagen.



Siga los pasos descritos en este artículo para instalar un certificado autofirmado como origen de confianza en un equipo con Windows, para eliminar este problema.

Al aplicar el certificado exportado, asegúrese de que se coloca en el equipo cliente con Anyconnect instalado.

Versión de software de AnyConnect

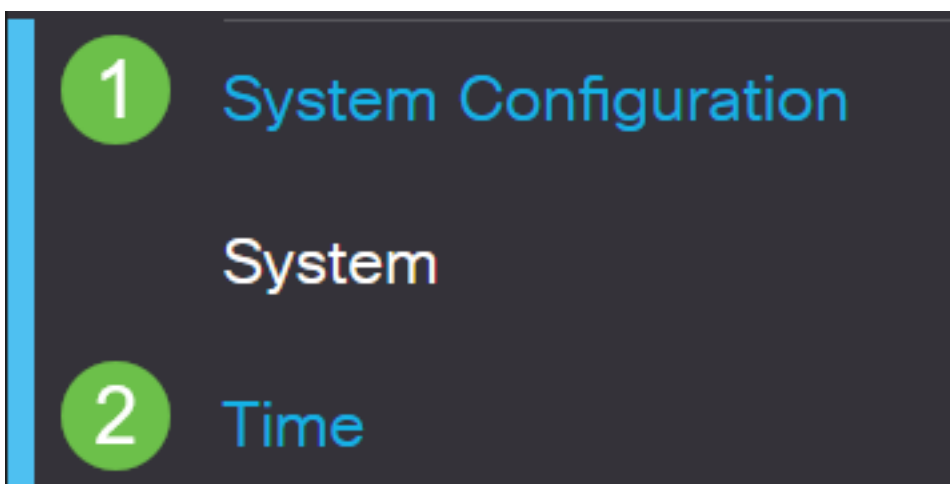
- AnyConnect - v4.9.x ([última descarga](#))

Comprobar configuración de hora

Como requisito previo, debe asegurarse de que el router tiene la hora correcta, incluidos los parámetros de horario de ahorro de la zona horaria y la luz diurna.

Paso 1

Vaya a **Configuración del sistema > Hora**.



Paso 2


Asegúrese de que todo está configurado correctamente.

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)

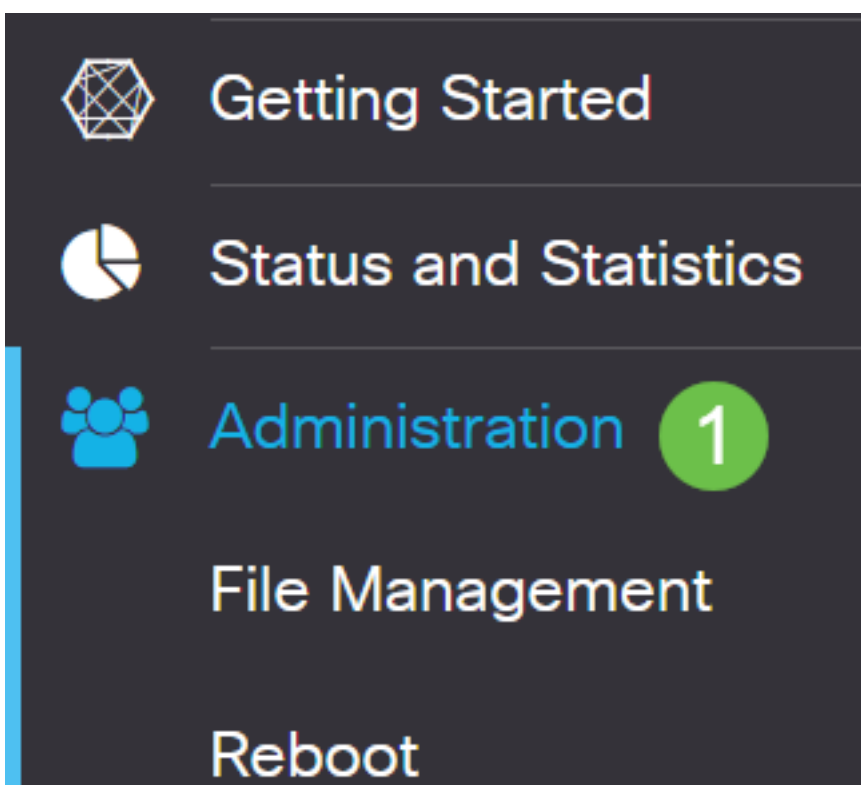
To: Month 11 ▼ Day 03 ▼ Time 02 ▼ : 00 ▼ (24hh:mm)

Daylight Saving Offset: +60 ▼ Minutes

Crear un certificado firmado automáticamente

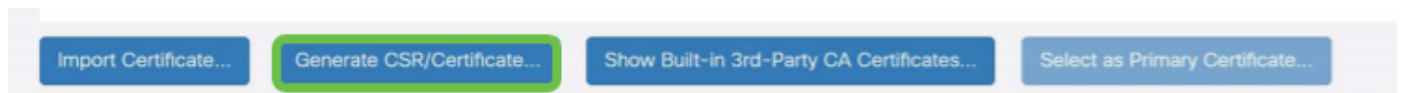
Paso 1

Inicie sesión en el RV34x Series Router y navegue hasta **Administration > Certificate**.



Paso 2

Haga clic en **Generar CSR/Certificado**.

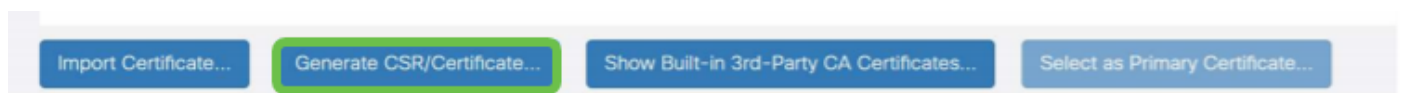


Paso 3

Complete la siguiente información:

- Tipo: Certificado firmado automáticamente
- Nombre del certificado: (Cualquier nombre que elija)
- Nombre alternativo del asunto: Si se utilizará una dirección IP en el puerto WAN, seleccione **Dirección IP** debajo del cuadro o **FQDN** si va a utilizar el nombre de dominio completamente calificado. En el cuadro, introduzca la dirección IP o FQDN del puerto WAN.
- Nombre del país (C): Seleccione el país en el que se encuentra el dispositivo
- Nombre de estado o provincia (ST): Seleccione el estado o provincia donde se encuentra el dispositivo
- Nombre de localidad (L): (Opcional) Seleccione la localidad en la que se encuentra el dispositivo. Esto podría ser una ciudad, una ciudad, etc.
- Nombre de la organización (O): (Opcional)
- Nombre de unidad de organización (OU): Nombre de la empresa
- Nombre común (CN): Esto DEBE coincidir con lo establecido como nombre alternativo del sujeto
- Dirección de correo electrónico (E): (Opcional)
- Longitud de cifrado de la clave: 2048
- Duración válida: Este es el tiempo que el certificado será válido. El valor predeterminado es 360 días. Puede ajustar esto a cualquier valor que desee, hasta 10 950 días o 30 años.

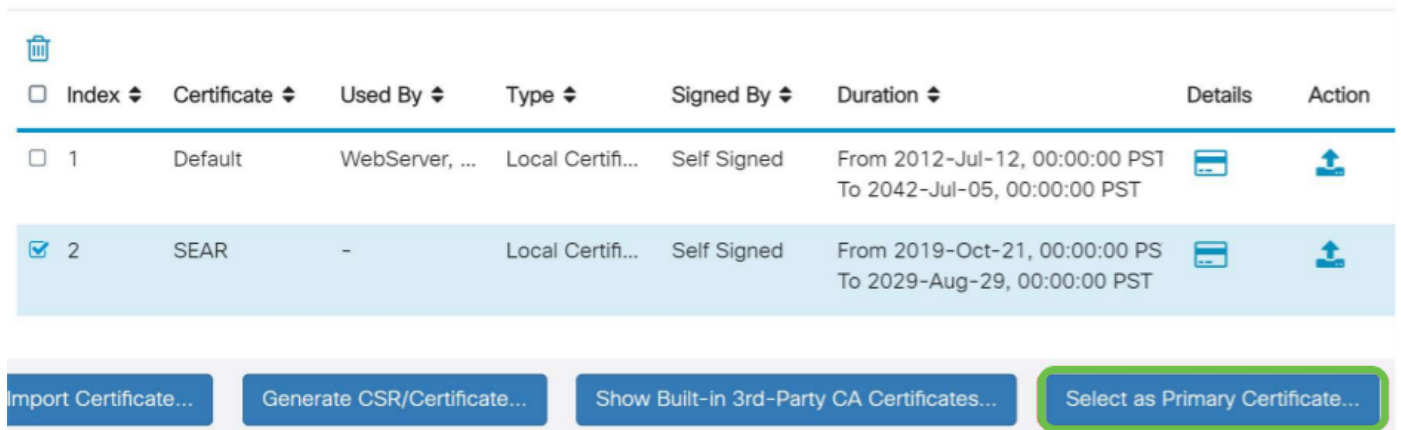




Haga clic en **Generar**.



Paso 4

Seleccione el certificado que se acaba de crear y haga clic en **Seleccionar como certificado 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...**

Paso 5

Actualice la interfaz de usuario web. Dado que se trata de un certificado nuevo, tendrá que volver a iniciar sesión. Una vez que haya iniciado sesión, vaya 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

Paso 6

Cambie el **archivo de certificado** al certificado recién creado.

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!"/> | |

Paso 7

Haga clic en Apply (Aplicar).

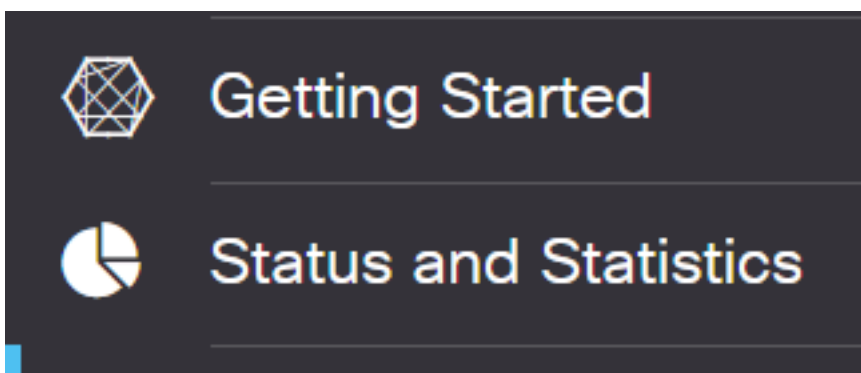


Instalación de un certificado autofirmado

Para instalar un certificado autofirmado como origen de confianza en un equipo con Windows, para eliminar la advertencia "Servidor no fiable" en AnyConnect, siga estos pasos:

Paso 1

Inicie sesión en el RV34x Series Router y navegue hasta **Administration > Certificate**.



Paso 2

Seleccione el certificado autofirmado predeterminado y haga clic en el botón **Exportar** para descargar el certificado.

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 | | |

Paso 3

En la ventana *Exportar certificado*, introduzca una contraseña para el certificado. Vuelva a introducir la contraseña en el campo *Confirmar contraseña* y, a continuación, haga clic en **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

Paso 4

Aparecerá una ventana emergente para notificar que el certificado se ha descargado correctamente. Click OK.

Information

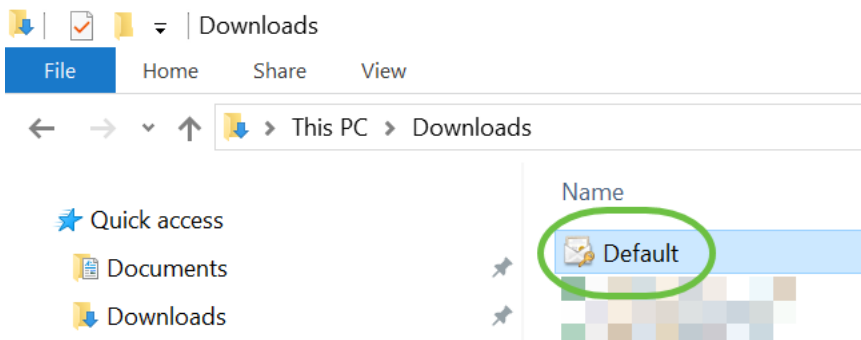


Success



Paso 5

Una vez descargado el certificado en el PC, localice el archivo y haga doble clic en él.



Paso 6

Aparecerá la ventana *Asistente para importación de certificados*. Para la *Ubicación de la tienda*, seleccione **Máquina local**. Haga clic en Next (Siguiete).

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

Paso 7

En la siguiente pantalla, se mostrará la ubicación y la información del certificado. Haga clic en Next (Siguiete).

File to Import

Specify the file you want to import.

File name:

C:\Users\... \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)

Paso 8

Introduzca la *contraseña* seleccionada para el certificado y haga clic en **Siguiente**.

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

Paso 9

En la siguiente pantalla, seleccione **Colocar todos los certificados en la siguiente tienda** y, a continuación, haga clic en **Examinar**.

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

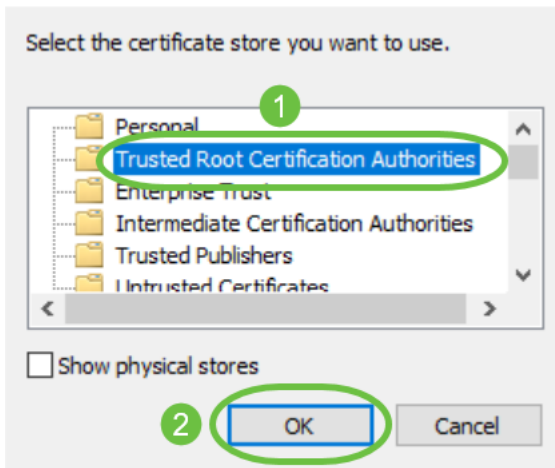
Certificate store:

2

Browse...


Paso 10

Seleccione **Autoridades de certificación raíz de confianza** y haga clic en **Aceptar**.



Paso 11

Haga clic en Next (Siguiente).

←  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

Paso 12

Se mostrará un resumen de los parámetros. Haga clic en **Finalizar** para importar el certificado.

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

Paso 13

Verá una confirmación de que el certificado se importó correctamente. Click OK.

Certificate Import Wizard



The import was successful.

OK

Paso 14

Abra Cisco AnyConnect e intente conectarse de nuevo. Ya no debería ver la advertencia del servidor no fiable.

Conclusión

¡Ahí lo tienes! Ya ha aprendido correctamente los pasos para instalar un certificado autofirmado como origen de confianza en un equipo con Windows, para eliminar la advertencia "Servidor no fiable" en AnyConnect.

Recursos adicionales

[Resolución de problemas básicos](#) [Guía del administrador de AnyConnect versión 4.9](#) [Notas de la versión de AnyConnect - 4.9](#) [Descripción general y prácticas recomendadas de Cisco Business VPN](#)