Gestión de certificados en el router serie RV34x

Objetivo

Un certificado digital certifica la propiedad de una clave pública por el sujeto designado del certificado. Esto permite que las partes que confían en ellas dependan de las firmas o afirmaciones hechas por la clave privada que corresponde a la clave pública certificada. Un router puede generar un certificado autofirmado, un certificado creado por un administrador de red. También puede enviar solicitudes a las autoridades de certificación (CA) para solicitar un certificado de identidad digital. Es importante disponer de certificados legítimos de aplicaciones de terceros.

Hablemos de obtener un certificado de una autoridad certificadora (CA). Se utiliza una CA para la autenticación. Los certificados se compran en cualquier número de sitios de terceros. Es una manera oficial de probar que su sitio es seguro. Básicamente, la CA es una fuente de confianza que verifica que usted es una empresa legítima y de confianza. Según sus necesidades, un certificado a un coste mínimo. La CA le desprotege y, una vez que verifiquen su información, le emitirán el certificado. Este certificado se puede descargar como un archivo en su equipo. A continuación, puede ir al router (o al servidor VPN) y cargarlo allí.

El objetivo de este artículo es mostrarle cómo generar, exportar e importar certificados en el RV34x Series Router.

Dispositivos aplicables | Versión de software

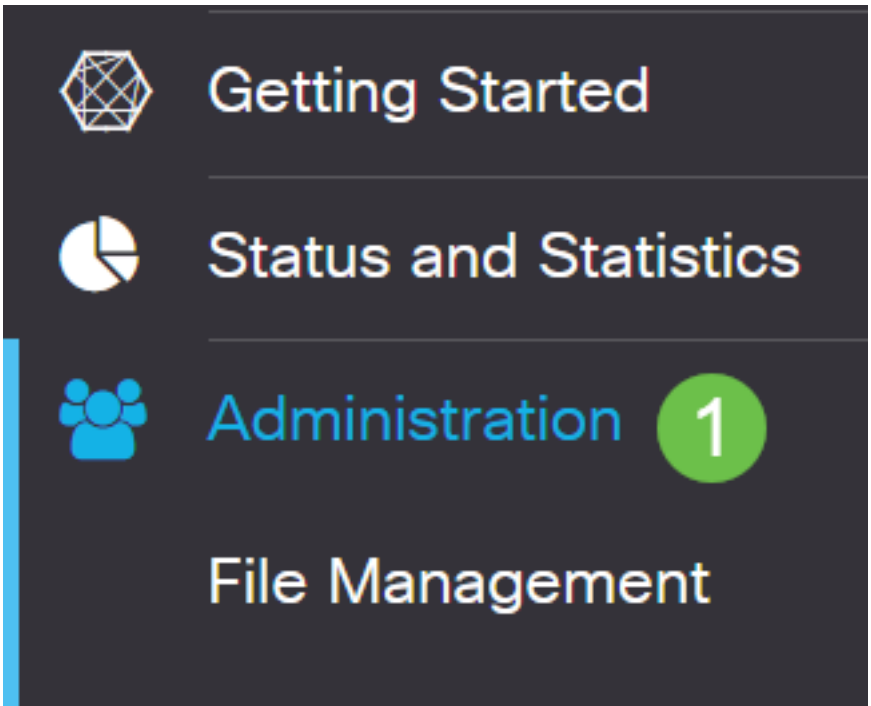
- Serie RV34x |1.0.03.20

Administración de certificados en el router

Generar CSR/Certificado

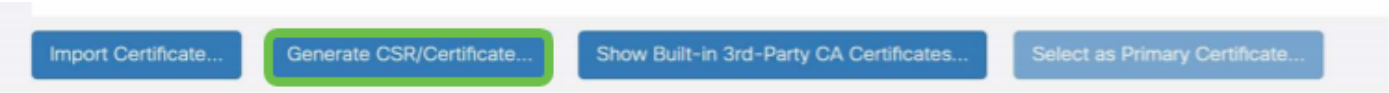
Paso 1

Inicie sesión en la utilidad basada en web del router y elija **Administration > Certificate**.



Paso 2

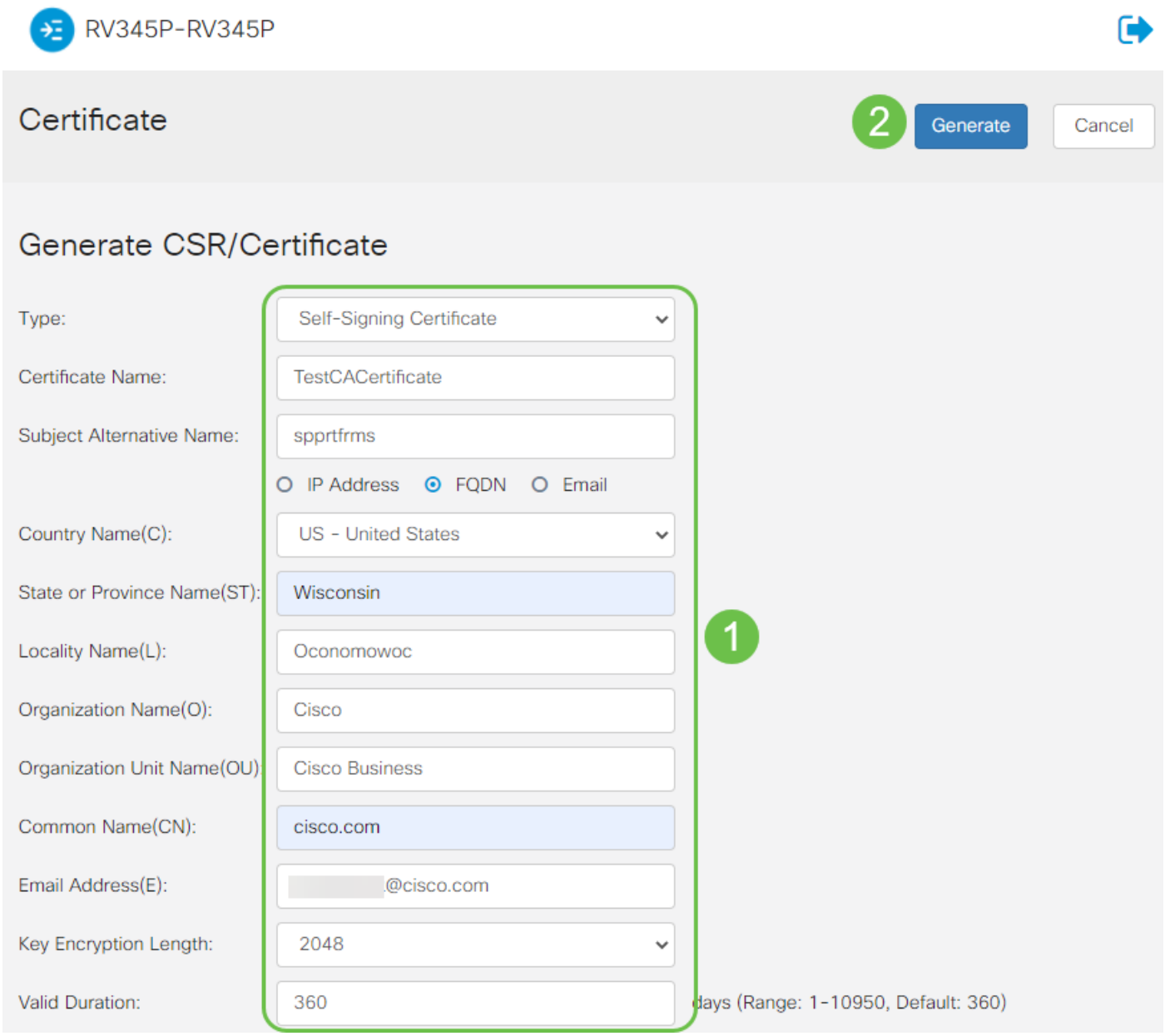
Haga clic en **Generar CSR/Certificado**. Accederá a la página Generar CSR/Certificado.



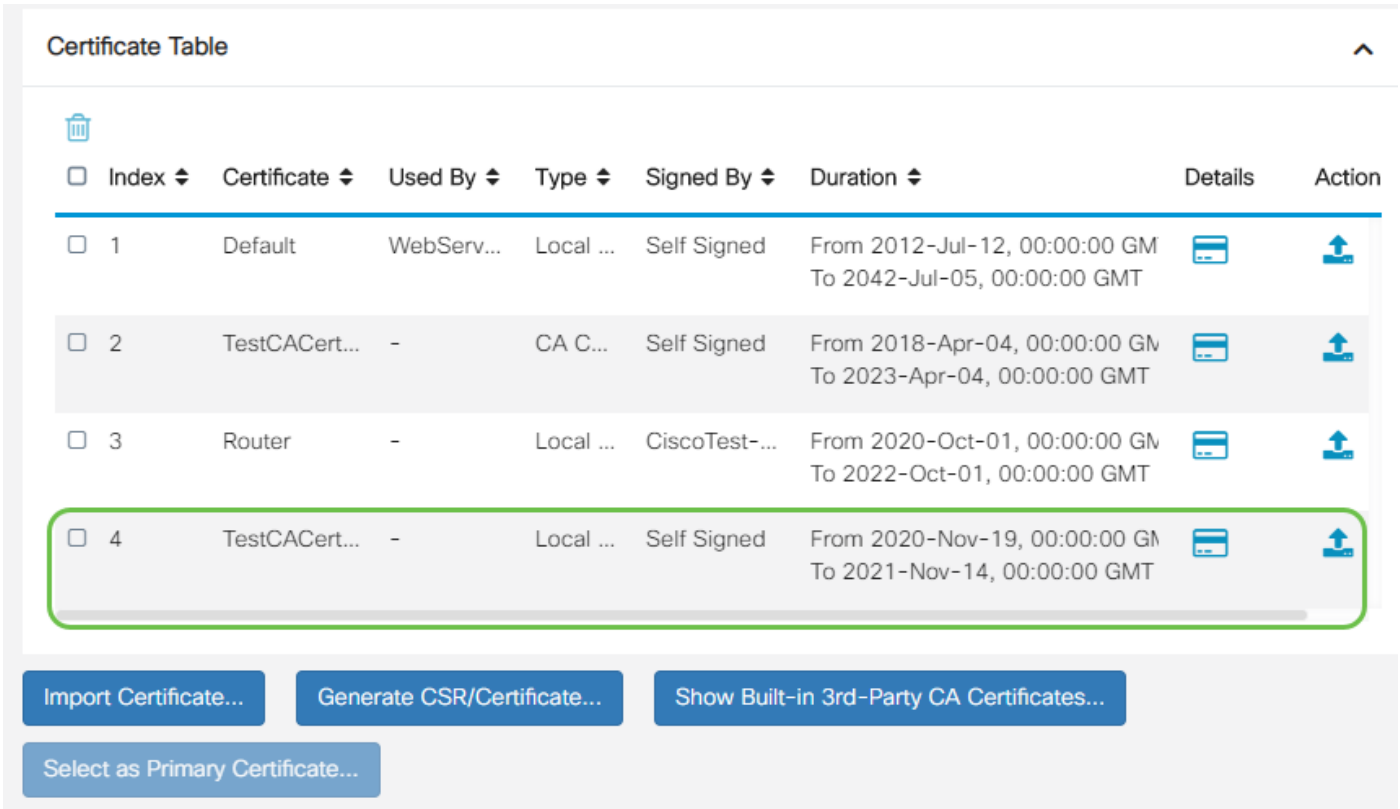
Paso 3

Rellene los cuadros con lo siguiente:

- Elija el tipo de certificado adecuado
  - Certificado de firma automática: este es un certificado de capa de socket seguro (SSL) firmado por su propio creador. Este certificado es menos confiable, ya que no se puede cancelar si la clave privada está comprometida de alguna manera por un atacante.
  - Solicitud de firma certificada: se trata de una infraestructura de clave pública (PKI) que se envía a la autoridad certificadora para solicitar un certificado de identidad digital. Es más seguro que autofirmado, ya que la clave privada se mantiene en secreto.
- Introduzca un nombre para el certificado en el campo *Nombre del certificado* para identificar la solicitud. Este campo no puede estar en blanco ni contener espacios ni caracteres especiales.
- (Opcional) En el área Nombre alternativo del sujeto, haga clic en un botón de opción. Las opciones son:
  - Dirección IP: introduzca una dirección de protocolo de Internet (IP)
  - FQDN: introduzca un nombre de dominio completo (FQDN)
  - Correo electrónico: introduzca una dirección de correo electrónico
- En el campo *Subject Alternative Name*, ingrese el FQDN.
- Elija un nombre de país en el que su organización esté registrada legalmente en la lista desplegable Nombre de país.
- Introduzca un nombre o abreviatura del estado, provincia, región o territorio en el que se encuentra su organización en el campo *Nombre de estado o provincia(ST)*.
- Introduzca un nombre de la localidad o ciudad en la que está registrada su organización o ubicada en el campo *Nombre de localidad*.
- Introduzca un nombre con el que se registre legalmente su empresa. Si se está inscribiendo como pequeña empresa o propietario exclusivo, introduzca el nombre del solicitante del certificado en el campo *Organization Name*. No se pueden utilizar caracteres especiales.
- Introduzca un nombre en el campo *Organization Unit Name* para diferenciar las divisiones de una organización.
- Introduzca un nombre en el campo *Nombre común*. Este nombre debe ser el nombre de dominio completo del sitio web para el que utiliza el certificado.
- Introduzca la dirección de correo electrónico de la persona que desea generar el certificado.
- En la lista desplegable Key Encryption Length (Longitud de cifrado de la clave), elija una longitud de clave. Las opciones son 512, 1024 y 2048. Cuanto mayor sea la longitud de la clave, más seguro será el certificado.
- En el campo *Duración válida*, introduzca el número de días que el certificado será válido. El valor predeterminado es 360.
- Haga clic en **Generar**.



Nota: El certificado generado debe aparecer ahora en la tabla de certificados.

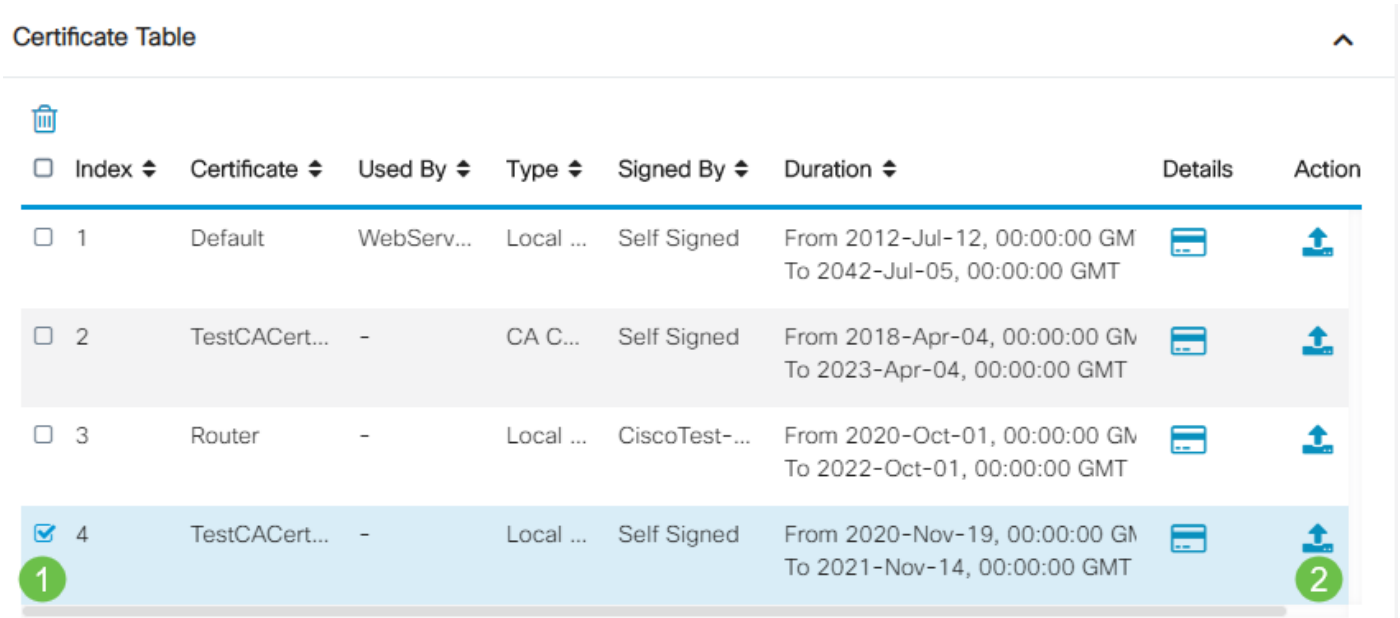


Ahora debería haber creado correctamente un certificado en el router RV345P.

Exportar un certificado

Paso 1

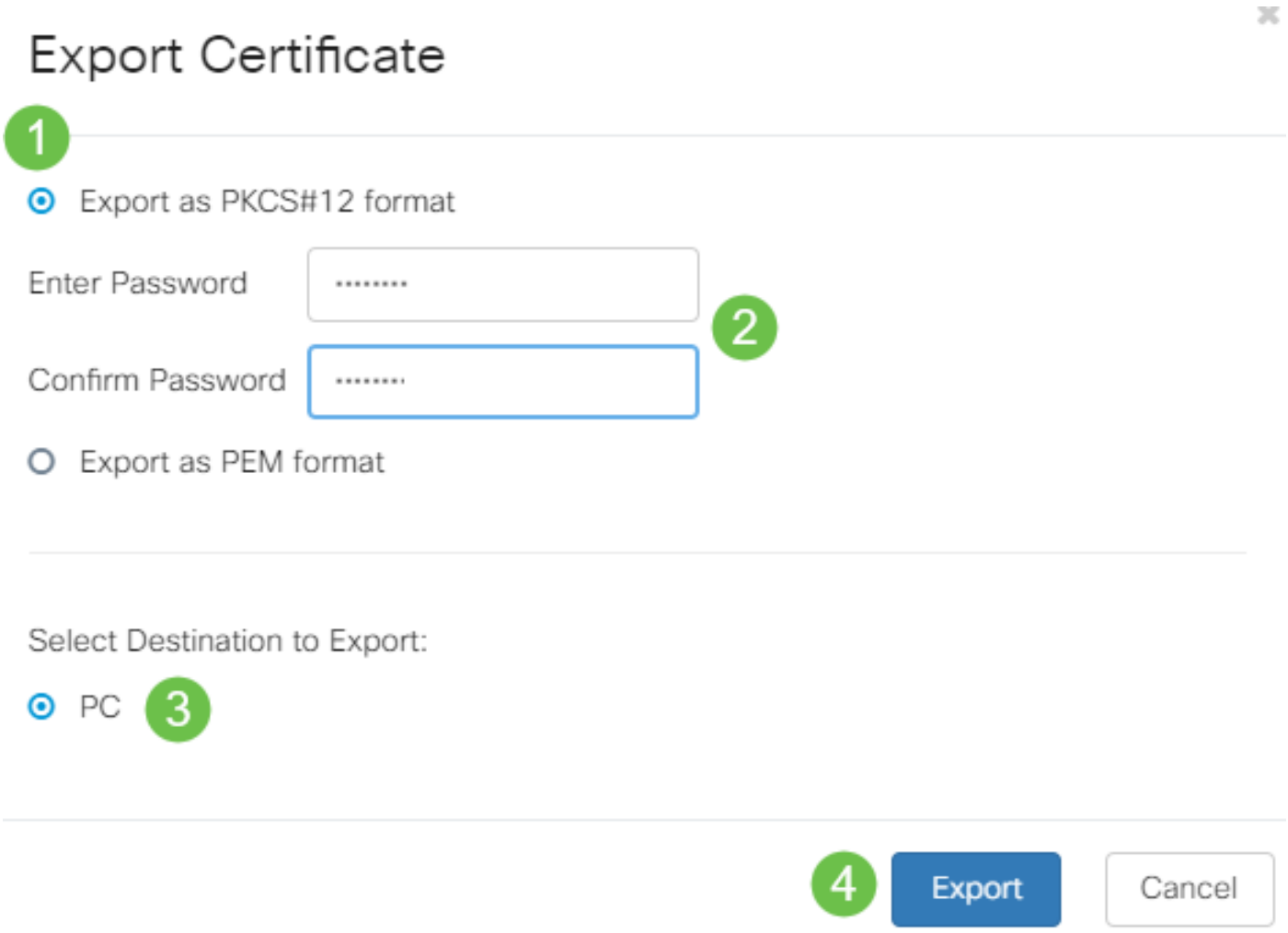
En la tabla de certificados, active la casilla de verificación del certificado que desea exportar y haga clic en el **icono de exportación**.



Paso 2

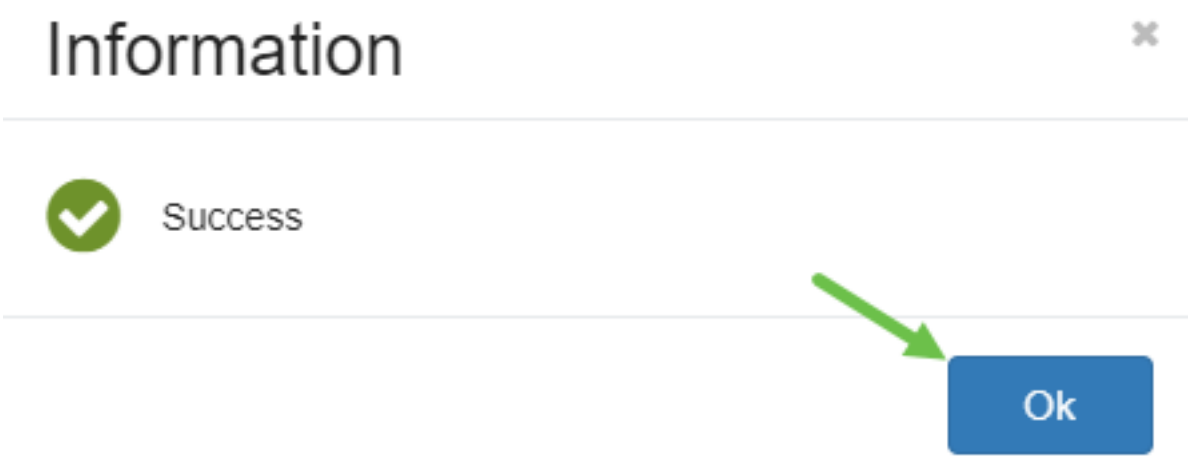
- Haga clic en un formato para exportar el certificado. Las opciones son:
  - PKCS #12 — Public Key Cryptography Standards (PKCS) #12 es un certificado exportado que viene en una extensión .p12. Se requerirá una contraseña para cifrar el archivo para protegerlo a medida que se exporta, importa y elimina.

    - PEM: el correo mejorado de privacidad (PEM) se utiliza con frecuencia en los servidores web para que puedan traducirse fácilmente a datos legibles mediante un editor de texto simple, como el bloc de notas.
- Si selecciona PEM, haga clic en **Exportar**.
- Introduzca una contraseña para proteger el archivo que se exportará en el campo *Introducir contraseña*.
- Vuelva a introducir la contraseña en el campo *Confirmar contraseña*.
- En el área Seleccionar destino, se ha seleccionado PC y es la única opción disponible actualmente.
- Haga clic en **Exportar**.



Paso 3

Debajo del botón Download (Descargar) aparecerá un mensaje que indica el éxito de la descarga. Un archivo comenzará a descargarse en el explorador. Click OK.

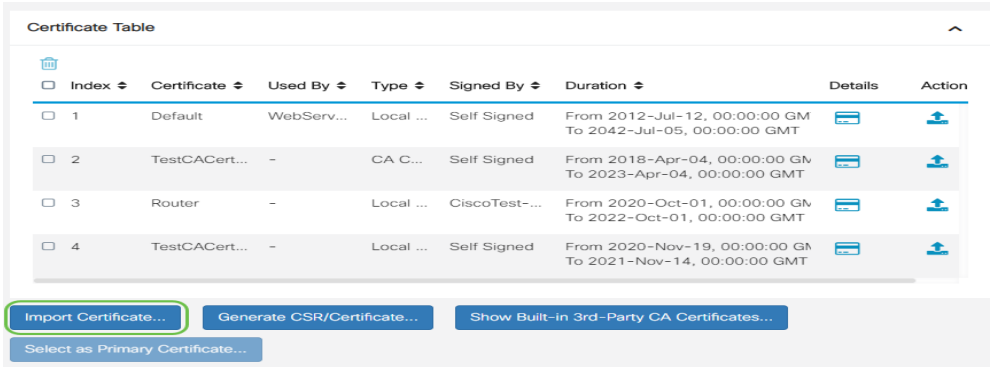


Ahora debería haber exportado correctamente un certificado en el router serie Rv34x.

Importar un certificado

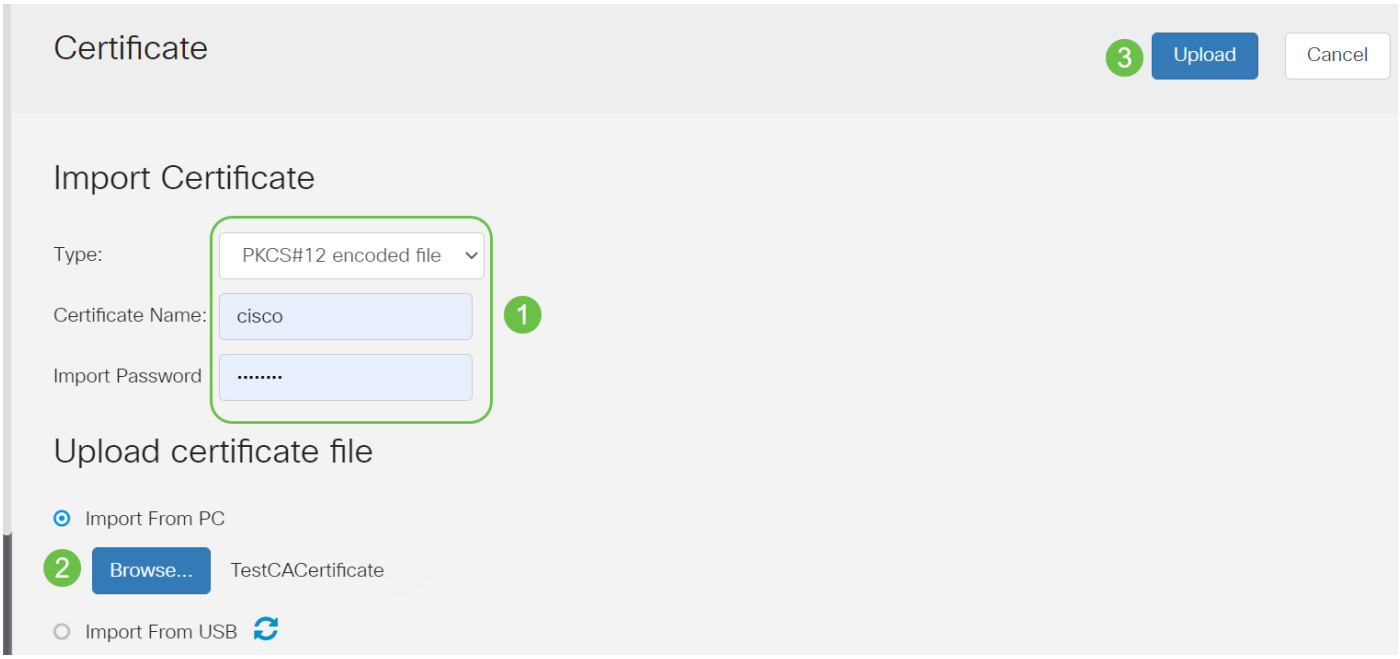
Paso 1

Haga clic en **Importar certificado...**.

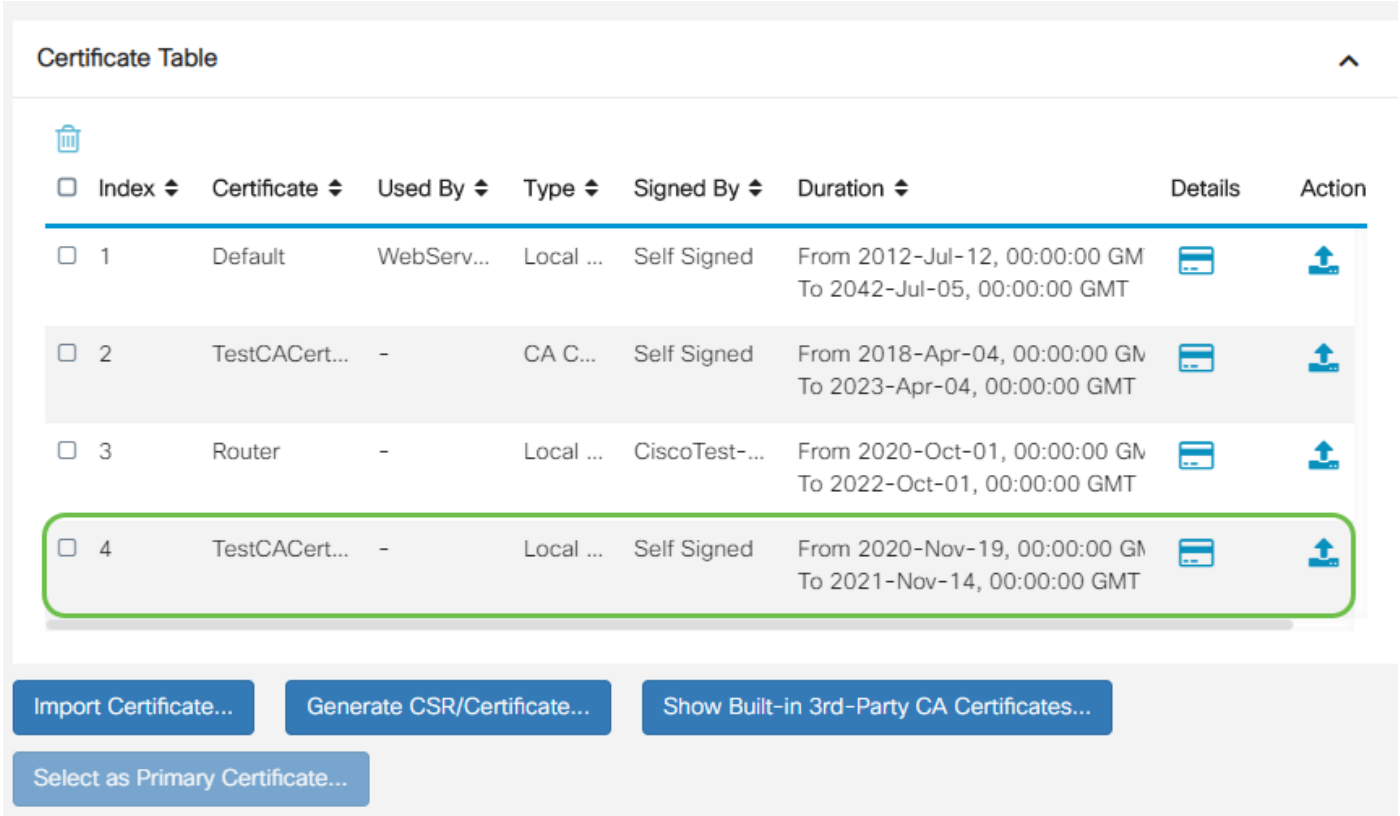


Paso 2

- Elija el tipo de certificado que desea importar en la lista desplegable. Las opciones son:
  - Certificado local: certificado generado en el router.
  - Certificado CA: certificado certificado certificado por una autoridad de terceros de confianza que ha confirmado que la información contenida en el certificado es exacta.
  - Archivo PKCS #12 codificado — Public Key Cryptography Standards (PKCS) #12 es un formato para almacenar un certificado de servidor.
- Introduzca un nombre para el certificado en el campo *Nombre del certificado*.
- Si se eligió PKCS #12, introduzca una contraseña para el archivo en el campo *Importar contraseña*. Caso contrario, siga con el paso 3.
- Haga clic en un origen para importar el certificado. Las opciones son:
  - Importar desde PC
  - Importar desde USB
- Si el router no detecta una unidad USB, la opción Importar desde USB se atenuará.
- Si ha seleccionado Importar desde USB y el router no reconoce el USB, haga clic en Actualizar.
- Haga clic en el botón Choose File (Elegir archivo) y elija el archivo adecuado.
- Haga clic en **Cargar**.



Una vez realizado correctamente, se le llevará automáticamente a la página principal de certificados. La tabla de certificados se rellenará con el certificado recientemente importado.



Ahora debería haber importado correctamente un certificado en el router serie RV34x.