Certificado autofirmado para impresoras electrónicas del PdV

Es probable que algunos modelos de impresora que se pueden usar sin un **sistema IoT** necesiten un **protocolo HTTPS** para establecer una conexión segura entre el navegador y la impresora. Sin embargo, la mayoría de los navegadores le mostrarán una página de advertencia si intenta conectarse a la dirección IP de la impresora a través de HTTPS. En ese caso, puede **forzar la conexión** de forma temporal, así podrá conectarse a la página HTTPS y usar una impresora ePOS con Odoo siempre y cuando no cierre la ventana del navegador.

> **Advertencia**
> Si cierra la ventana del navegador se perderá la conexión. Por lo tanto, este método solo se debe usar como una **solución temporal** o como un requisito previo para las **siguientes instrucciones**.

Genere, exporte e importe certificados autofirmados.

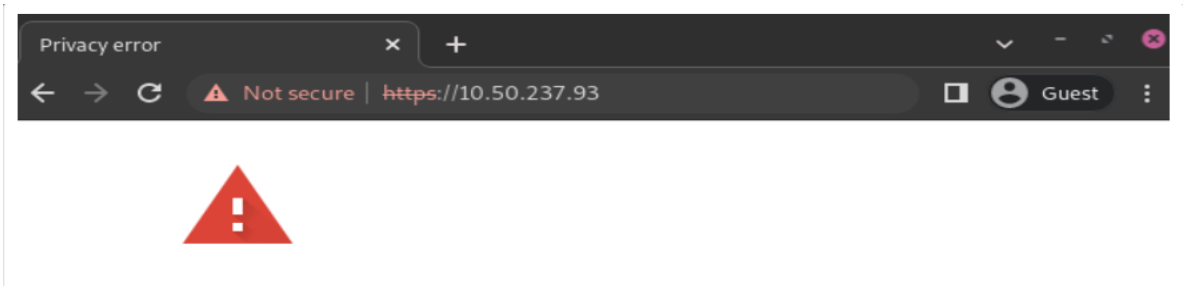
Para obtener una solución a largo plazo debe generar un **certificado autofirmado**. Después, expórtelo e impórtelo a su navegador.

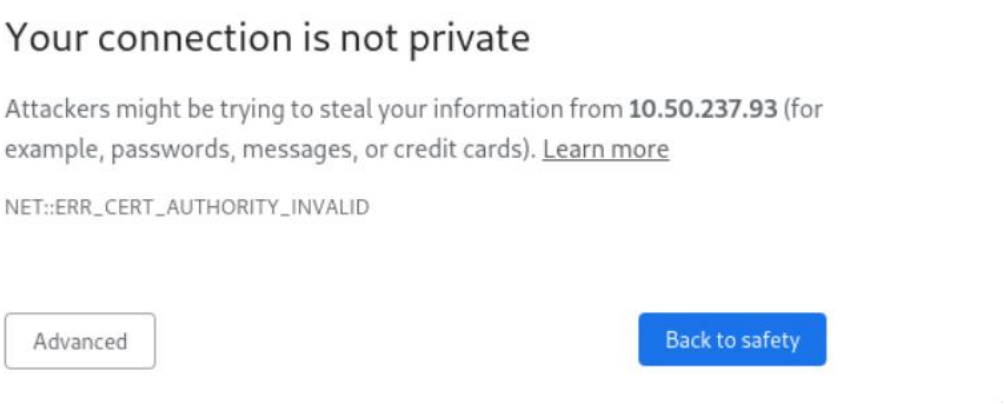
> **Importante**
> Un certificado SSL solo se debería **generar una vez**. Si crea otro certificado, los dispositivos que usen el certificado previo perderán el acceso al HTTPS.

Windows 10 & Linux OS

Generar un certificado autofirmado

Navegue a la dirección IP de la impresora ePOS (p. ej. `https://192.168.1.25`) y haga clic en **Avanzado** y después en **Proceeder a [dirección IP] (no es seguro)** para forzar la conexión.





Página de advertencia de Google Chrome en Windows 10

Después, use las credenciales de su impresora para ingresar a los ajustes de la impresora ePOS. Para iniciar sesión, ingrese epson en el campo **ID** y en el campo **Contraseña** ingrese el número de serie de la impresora.

Para generar un **certificado autofirmado** haga clic en **Certificate list** (lista de certificados) que se encuentra en la sección de **Autenticación**. El **Common Name** (nombre común) se debería de llenar de manera automática, pero si no es así ahí puede poner la dirección IP de la impresora. En el campo **Validity Period** (periodo de validez) ponga los años por los que el certificado será válido, haga clic en **Create** (crear) y **restablezca** o reinicie la impresora manualmente.

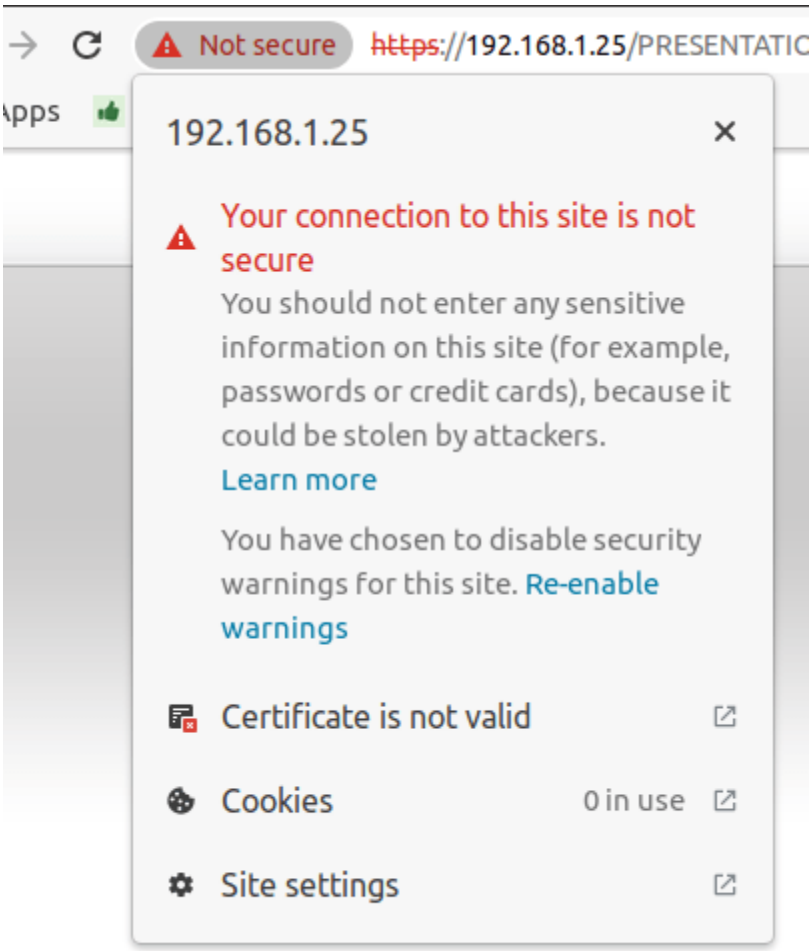
Ya se generó el el certificado autofirmado. Vuelva a cargar la página, vaya a la sección **Security** (seguridad) y haga clic en **SSL/TLS** para asegurarse de que el **certificado autofirmado** se seleccionó correctamente en la sección **Server certificate** (certificado del servidor).

Exportar un certificado autofirmado

El proceso de exportación depende mucho del **Sistema operativo** y del navegador. Primero vaya a la dirección IP (p. ej., https://192.168.1.25) e ingrese a los ajustes de su impresora ePOS en su navegador web Después, fuerce la conexión como se explica en **Generar un certificado autofirmado**.

Si está usando **Google chrome**,

1. haga clic en **No es seguro** a un lado de la barra de búsqueda, **Certificado inválido**;



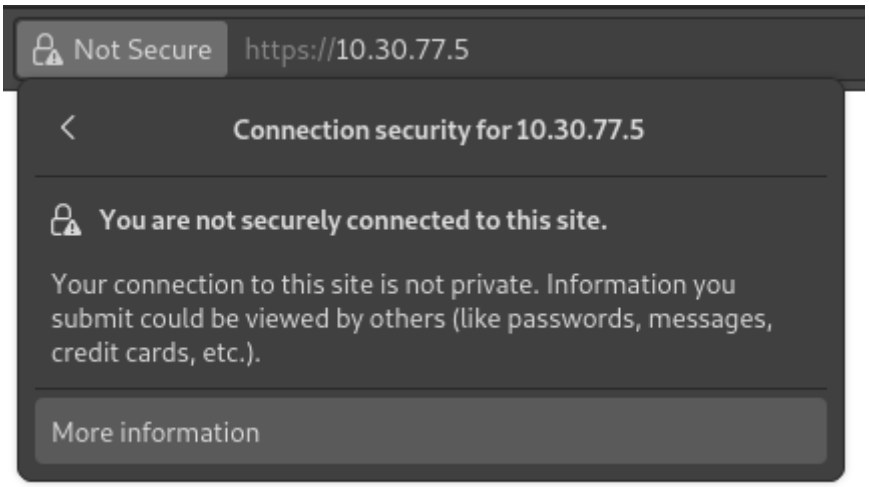
2. vaya a la pestaña **Detalles** y haga clic en **Exportar**;
3. agregue `.crt` al final del nombre del archivo para asegurarse de que sea la extensión correcta;
4. seleccione **Base64-encoded ASCII, single certificate** (Base64-codificado ASCII, certificado único), que se encuentra en la parte inferior de la ventana emergente;
5. guárdelo y habrá exportado el certificado.

> **Advertencia**
>
> Asegúrese de que el certificado termina con la extensión `.crt`. Si no es así, es probable que algunos navegadores no puedan ver el archivo durante el proceso de importación.

Si está usando **Mozilla Firefox**,

1. haga clic en el icono **en forma de cerradura** que se encuentra a la izquierda de la barra;

2. vaya a **Conexión no segura ► Más información ► Pestaña de seguridad ► Ver certificado**;



1. baje a la sección **Misceláneo**;
2. haga clic en **PEM (cert)** que se encuentra en la sección **Descargar**;
3. guárdelo y habrá exportado el certificado.

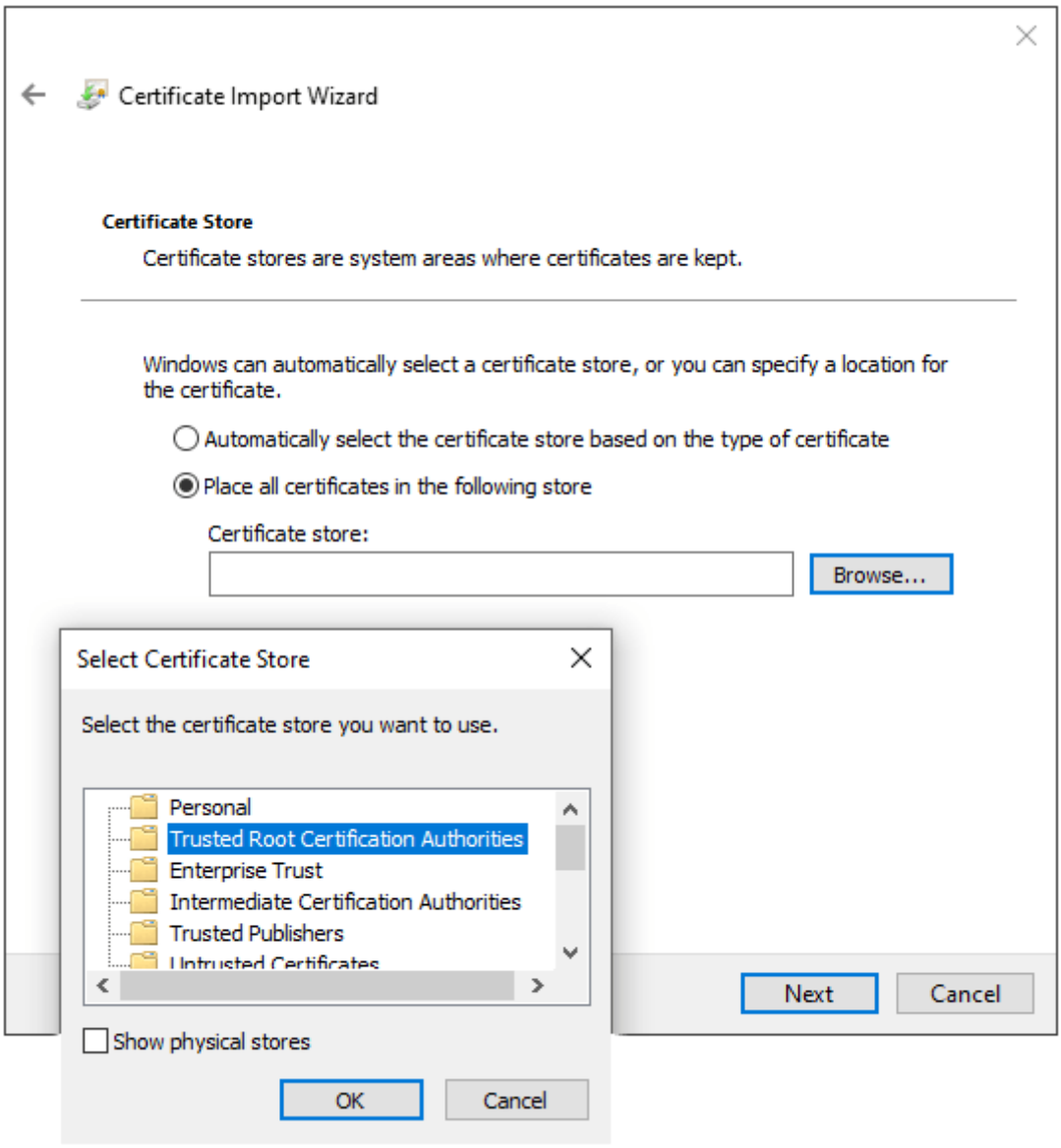
Importar un certificado autofirmado

El proceso de importación depende mucho del **Sistema operativo** y del navegador.

Windows 10

Windows 10 gestiona certificados, lo que significa que los certificados autofirmados se tienen que importar desde el archivo de certificación y no del navegador. Para hacerlo,

1. abra el explorador de archivos de Windows y encuentre el archivo de certificación que descargó;
2. haga clic derecho en el archivo de certificación y presione **Instalar certificado**;
3. seleccione dónde instalar el certificado y si para el **Usuario actual** o para todos los usuarios (**equipo local**) y después haga clic en **Siguiente**;
4. en la pantalla de Almacén de certificados marque **Place all certificates in the following store** (Colocar todos los certificados en el siguiente almacenamiento), haga clic en **Buscar…** y seleccione **Entidades de certificación raíz de confianza**;



5. haga clic en **Terminar** y acepte la ventada emergente;
6. reinicie la computadora para asegurarse de que se aplicaron los cambios.

Linux

Si está usando **Google chrome**,

1. abra Chrome;
2. vaya a **Ajustes** ▸ **Privacidad y seguridad** ▸ **Seguridad** ▸ **Gestionar certificados**;
3. vaya a la pestaña **Entidades**, haga clic en **Importar** y seleccione el archivo de certificación que exportó;

4. acepte todas las advertencias;
5. haga clic en **ok**;
6. reinicie su navegador.

Si está usando **Mozilla Firefox**,

1. abra Firefox;
2. go to **Ajustes** ▸ **Privacidad y seguridad** ▸ **Seguridad** ▸ **Ver certificados…** ▸ **Importar**;
3. seleccione el archivo de certificado que exportó;
4. marque las casillas y valide;
5. reinicie su navegador.

Mac OS

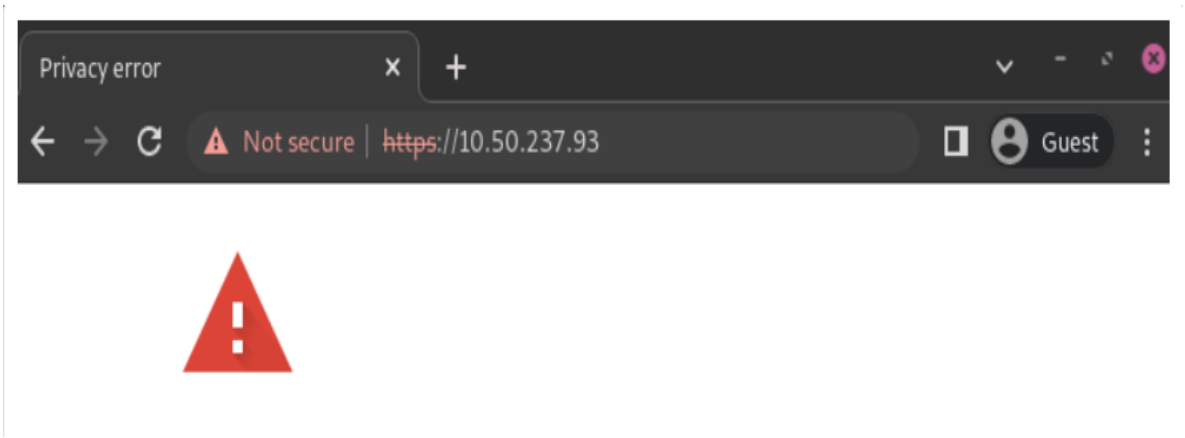
Para asegurar la conexión en Mac OS en todos los navegadores, tiene que seguir los siguientes pasos:

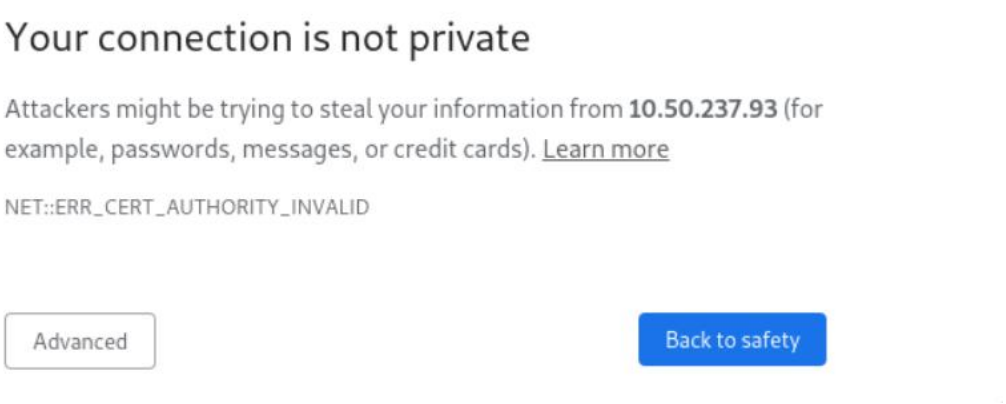
1. Abra Safari y vaya a la dirección IP de su impresora. Esta acción le redirigirá a una página de advertencia.
2. En la página de advertencia vaya a **Mostrar detalles** ▸ **Visitar este sitio web** ▸ **Visitar sitio web** y valídelo.
3. reinicie la impresora para que la puede usar con cualquier navegador.

Para generar y exportar un certificado SSL y enviarlo a dispospositivo IOS, abra **Google Chrome** o **Mozilla Firefox**. Después,

Generar un certificado autofirmado

Navegue a la dirección IP de la impresora ePOS (p. ej. https://192.168.1.25) y haga clic en **Avanzado** y después en **Proceder a [dirección IP] (no es seguro)** para forzar la conexión.





Página de advertencia de Google Chrome en Windows 10

Después, use las credenciales de su impresora para ingresar a los ajustes de la impresora ePOS. Para iniciar sesión, ingrese epson en el campo **ID** y en el campo **Contraseña** ingrese el número de serie de la impresora.

Para generar un **certificado autofirmado** haga clic en **Certificate list** (lista de certificados) que se encuentra en la sección de **Autenticación**. El **Common Name** (nombre común) se debería de llenar de manera automática, pero si no es así ahí puede poner la dirección IP de la impresora. En el campo **Validity Period** (periodo de validez) ponga los años por los que el certificado será válido, haga clic en **Create** (crear) y **restablezca** o reinicie la impresora manualmente.

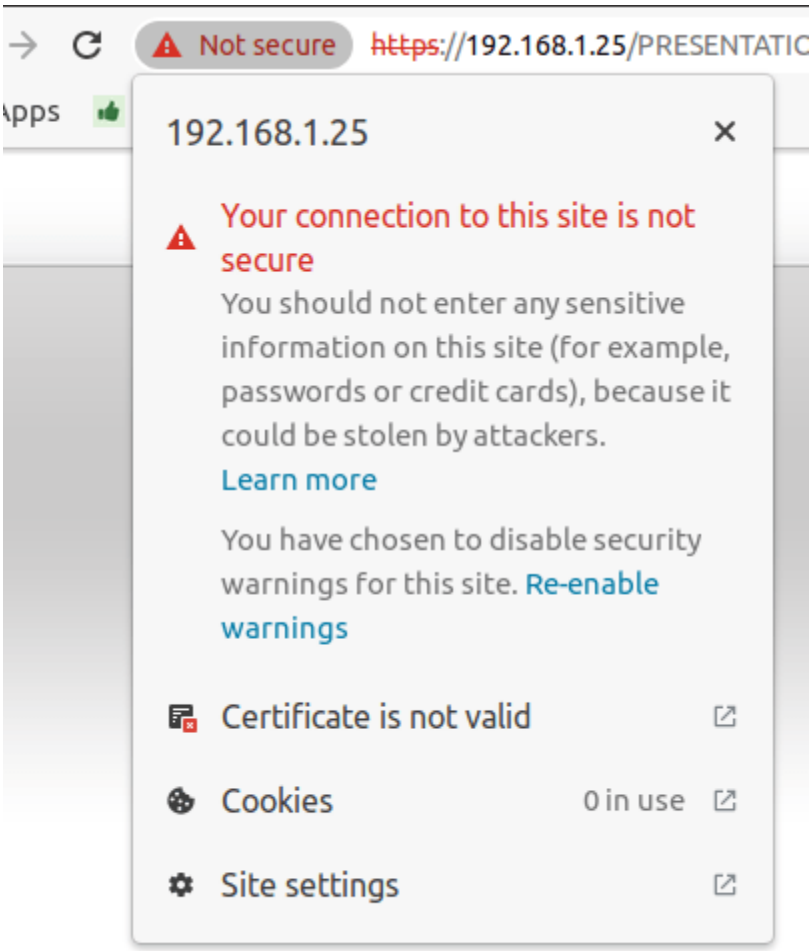
Ya se generó el el certificado autofirmado. Vuelva a cargar la página, vaya a la sección **Security** (seguridad) y haga clic en **SSL/TLS** para asegurarse de que el **certificado autofirmado** se seleccionó correctamente en la sección **Server certificate** (certificado del servidor).

Exportar un certificado autofirmado

El proceso de exportación depende mucho del **Sistema operativo** y del navegador. Primero vaya a la dirección IP (p. ej., https://192.168.1.25) e ingrese a los ajustes de su impresora ePOS en su navegador web Después, fuerce la conexión como se explica en **Generar un certificado autofirmado**.

Si está usando **Google chrome**,

6. haga clic en **No es seguro** a un lado de la barra de búsqueda, **Certificado inválido**;



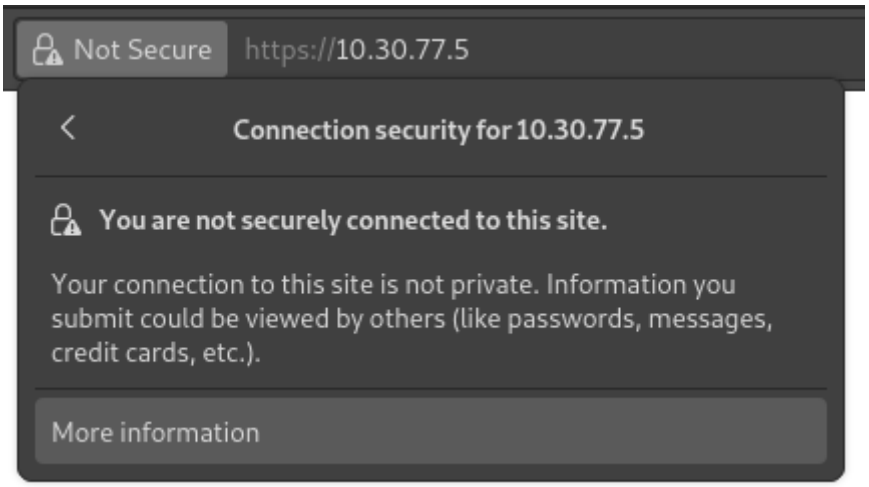
7. vaya a la pestaña **Detalles** y haga clic en **Exportar**;
8. agregue `.crt` al final del nombre del archivo para asegurarse de que sea la extensión correcta;
9. seleccione **Base64-encoded ASCII, single certificate** (Base64-codificado ASCII, certificado único), que se encuentra en la parte inferior de la ventana emergente;
10. guárdelo y habrá exportado el certificado.

> **Advertencia**
>
> Asegúrese de que el certificado termina con la extensión `.crt`. Si no es así, es probable que algunos navegadores no puedan ver el archivo durante el proceso de importación.

Si está usando **Mozilla Firefox**,

3. haga clic en el icono **en forma de cerradura** que se encuentra a la izquierda de la barra;

4. vaya a **Conexión no segura ► Más información ► Pestaña de seguridad ► Ver certificado**;



4. baje a la sección **Misceláneo**;
5. haga clic en **PEM (cert)** que se encuentra en la sección **Descargar**;
6. guárdelo y habrá exportado el certificado.

Android OS

Para importar el certificado SSL a un dispositivo Android primero debe crearlo y exportarlo desde una computadora. Después, transfiera el archivo `.crt` al dispositivo a través de un correo, Bluetooth o USB. Una vez que el archivo esté en el dispositivo,

1. abra los ajustes y busque el `certificado`;
2. haga clic en **Certificado CA** (Instalar desde el almacenamiento del dispositivo);
3. seleccione el archivo de certificado para instalarlo en el dispositivo.

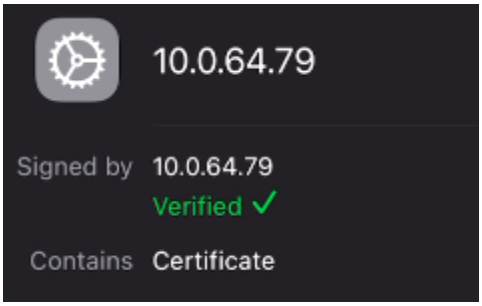
> **Nota**
> Los pasos a seguir para instalar un certificado pueden variar según la versión de Android y el fabricante del dispositivo.

iOS

Para importar el certificado SSL a un dispositivo iOS primero debe crearlo y exportarlo desde una computadora. Después, transfiera el archivo `.crt` al dispositivo a través de un correo, Bluetooth, o cualquier servicio para compartir archivos.

Al descargar este archivo se activa una ventana emergente de advertencia. Haga clic en **Permitir** para descargar el perfil de configuración y cerrar la segunda ventana emergente. Después,

1. vaya a la **aplicación Configuraciones** en el dispositivo iOS;
2. haga clic en **perfil descargado** en la caja de detalles del usuario;
3. buque el archivo .crt descargado y selecciónelo;
4. haga clic en **Instalar** en la parte superior derecha de la pantalla;
5. si el dispositivo tiene contraseña, ingrese la contraseña;
6. haga clic en **Instalar** en la parte superior derecha de la ventana de advertencia del certificado y en la ventana emergente;
7. haga clic en **Listo**.



El certificado se instaló, pero todavía se tiene que autenticar. Para hacerlo,

1. vaya a **Ajustes ► General ► Acerca de > Ajustes de confianza del certificado**;
2. active el certificado instalado con el **botón deslizable**;
3. haga clic en **Continuar** en la ventana emergente.

> **Importante**
>
> - Si necesita exportar certificados SSL desde un sistema operativo o un navegador que no hemos mencionado, busque `exportar certificado SSL` + `el nombre de su navegador o sistema operativo` en su motor de búsqueda preferido
> - Es lo mismo si necesita importar certificados SSL desde un sistema operativo o navegador que no mencionamos, busque `exportar certificado SSL` + `el nombre de su navegador o sistema operativo` en su motor de búsqueda preferido.

Revise si el certificado se importó correctamente

Para confirmar que la conexión de su impresora es segura, conéctese a su dirección IP mediante HTTPS. Por ejemplo, vaya a https://192.168.1.25 en su navegador. Si el certificado SSL se aplicó de forma correcta, entonces ya no debería aparecer la página de advertencia y en la barra de direcciones debería aparecer un icono de candado que indica que la conexión es segura.