Gestión de certificados en el administrador de red FindIT

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. Tras la instalación, FindIT Network Manager genera un certificado autofirmado para proteger la Web y otras comunicaciones con el servidor. Puede elegir reemplazar este certificado por el firmado por una autoridad de certificación (CA) de confianza. Para ello, deberá generar una solicitud de firma de certificado (CSR) para que la CA la firme.

También puede optar por generar un certificado y la clave privada correspondiente completamente independiente del administrador. Si es así, puede combinar el certificado y la clave privada en un archivo de formato de estándares criptográficos de clave pública (PKCS) nº 12 antes de la carga.

FindIT Network Manager sólo admite certificados de formato .pem. Si obtiene otros formatos de certificado, debe volver a convertir el formato o solicitar el certificado de formato .pem de la CA.

En este artículo se proporcionan instrucciones sobre cómo administrar certificados en FindIT Network Manager.

Dispositivos aplicables

- Administrador de redes FindIT

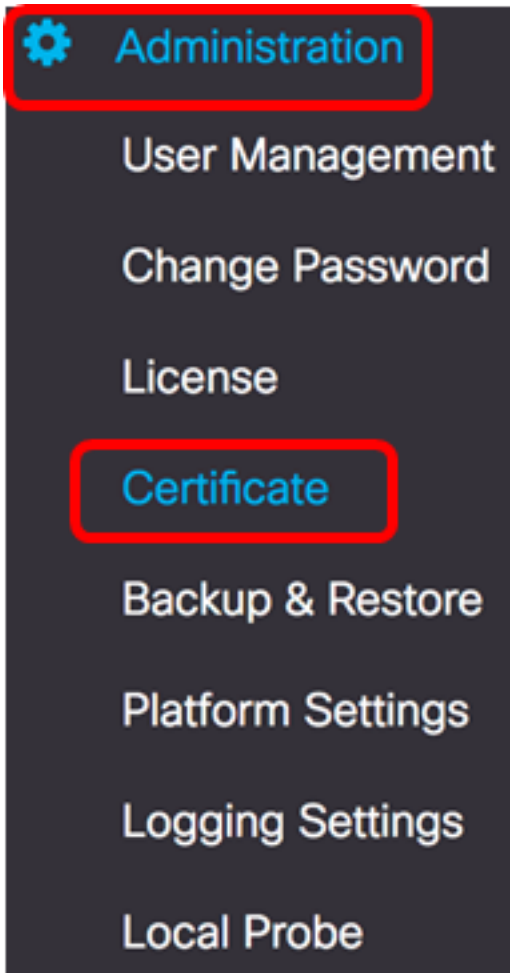
Versión del software

- 1.1

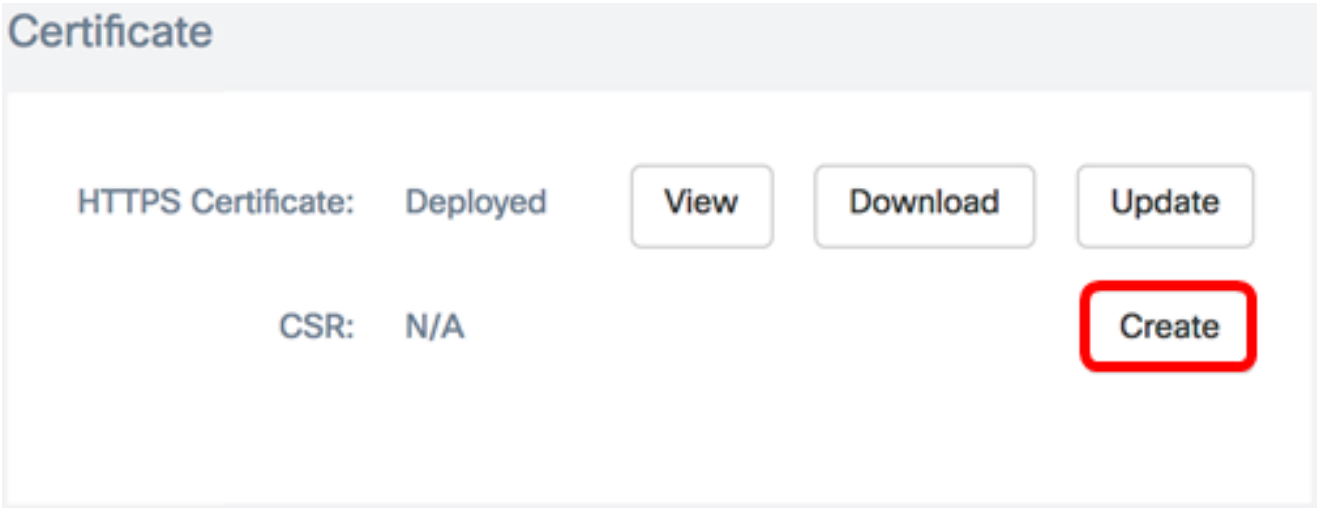
Administrar certificados en FindIT Network Manager

Generar una CSR

Paso 1. Inicie sesión en la GUI de administración de su FindIT Network Manager y luego elija **Administration > Certificate**.

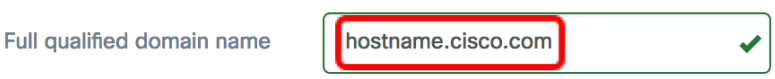


Paso 2. En el área CSR, haga clic en el botón **Crear**.



Los valores introducidos en el formulario de certificado se utilizarán para construir el CSR y se incluirán en el certificado firmado que reciba de la CA.

Paso 3. Ingrese la dirección IP o el nombre de dominio en el campo *Nombre de dominio completo calificado*. En este ejemplo, se utiliza hostname.cisco.com.



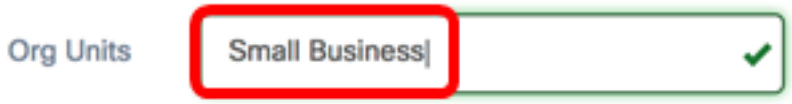
Paso 4. Introduzca el código de país en el campo *Country*. En este ejemplo, se utiliza US.

Paso 5. Introduzca el código de estado en el campo *Estado*. En este ejemplo, se utiliza CA.

Paso 6. Introduzca la ciudad en el campo *Ciudad*. En este ejemplo, se utiliza Irvine.

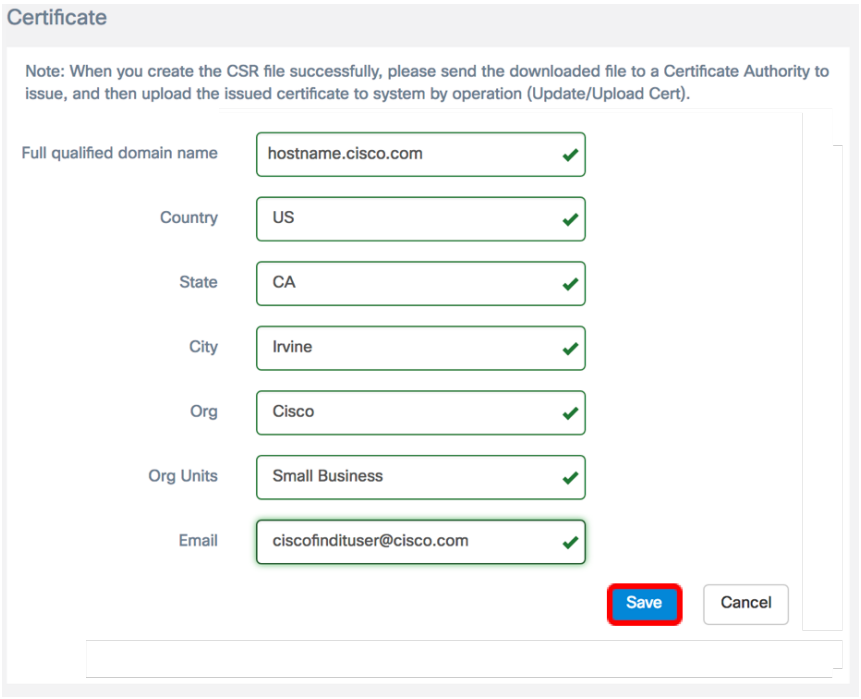
Paso 7. Introduzca el nombre de la organización en el campo *Org*. En este ejemplo, se utiliza Cisco.

Paso 8. Introduzca las unidades de organización en el campo *Unidades de organización*. En este ejemplo, se utiliza Small Business.

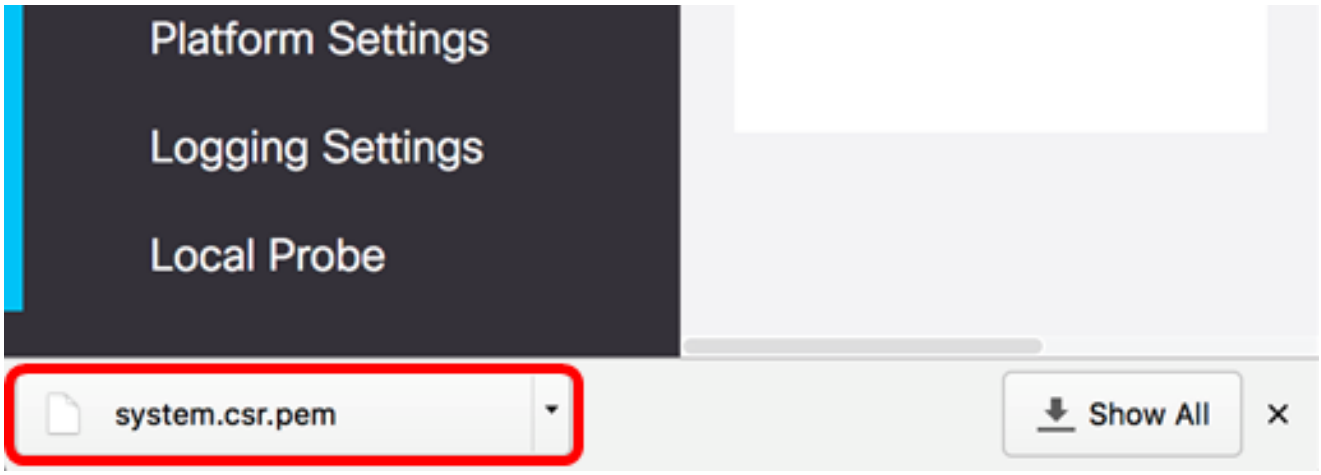


Paso 9. Introduzca su dirección de correo electrónico en el campo *Correo electrónico*. En este ejemplo, se ingresa ciscofindituser@cisco.com.

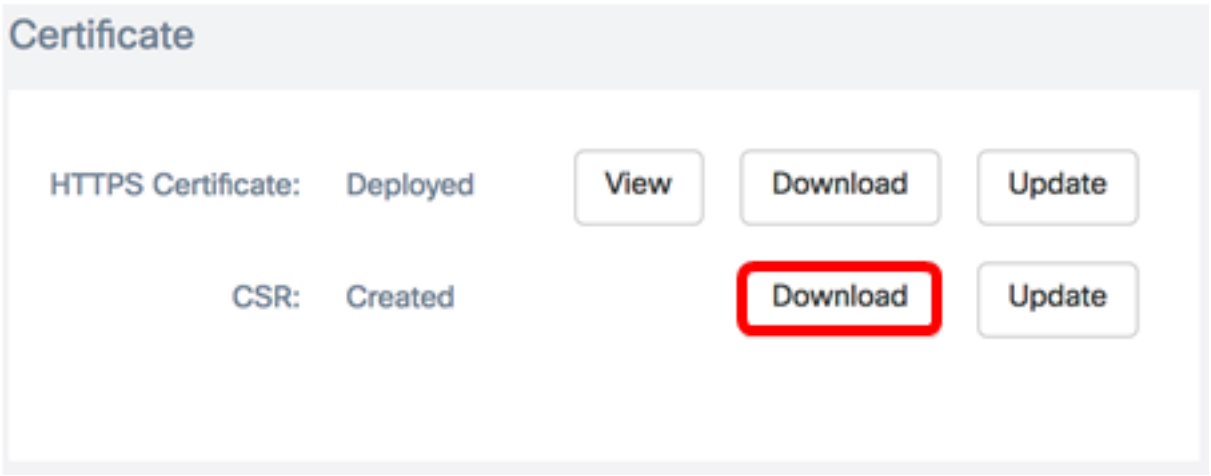
Paso 10. Click **Save**.



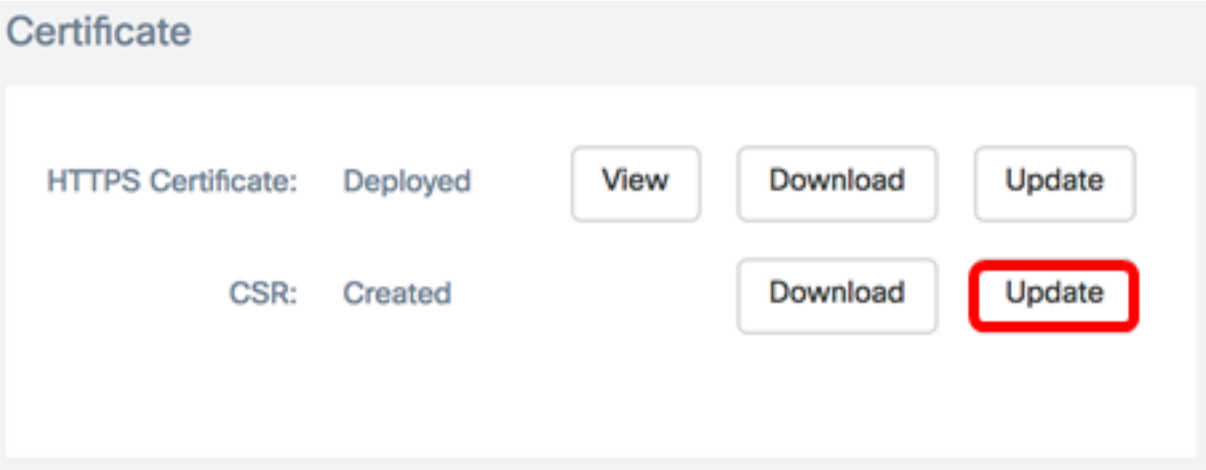
El archivo CSR se descargará automáticamente en el ordenador. En este ejemplo, se genera el archivo system.csr.pem.



Paso 11. (Opcional) En el área CSR, el estado se actualizará de N/A a Creado. Para descargar la CSR creada, haga clic en el botón **Download** .



Paso 12. (Opcional) Para actualizar la CSR creada, haga clic en el botón **Update** y, a continuación, vuelva al paso 3.

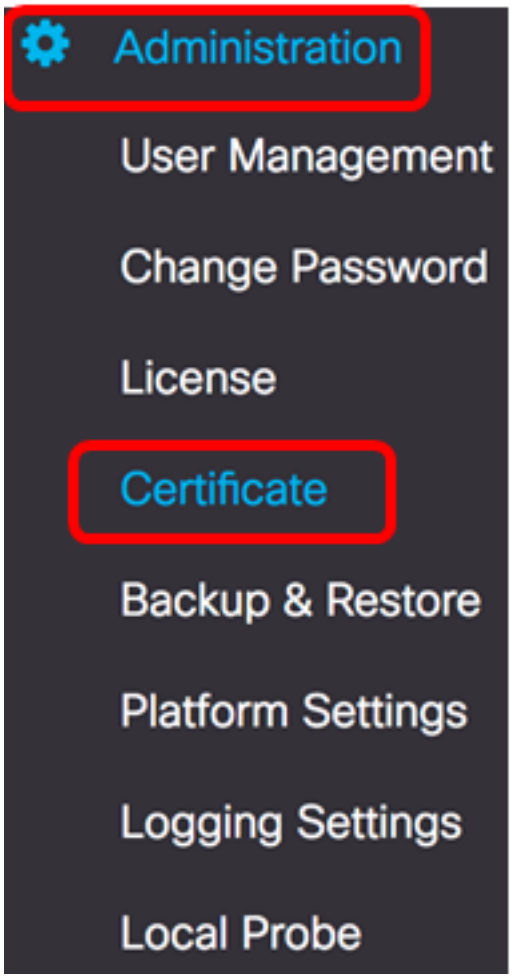


Ahora debería haber generado correctamente una CSR en su administrador de red FindIT. Ahora puede enviar el archivo CSR descargado a la CA.

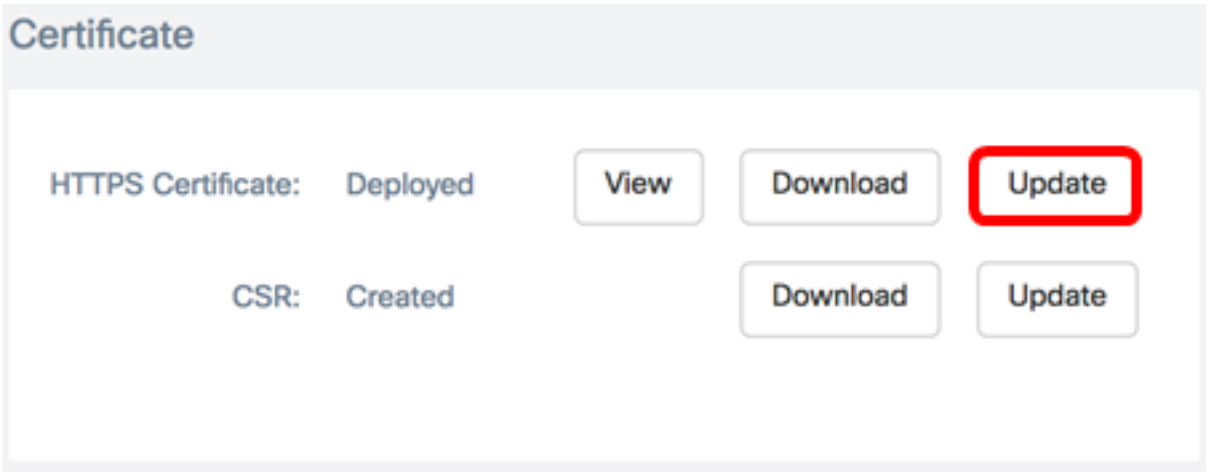
Cargar un certificado firmado desde la CA

Una vez que reciba la CSR firmada de la CA, ahora puede cargarla al administrador.

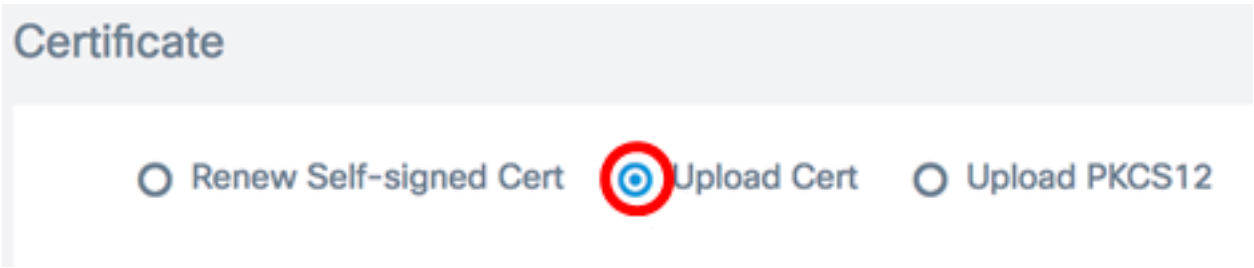
Paso 1. Inicie sesión en la GUI de administración de su FindIT Network Manager y luego elija **Administration > Certificate**.



Paso 2. En el área HTTPS Certificate , haga clic en el botón **Update**.

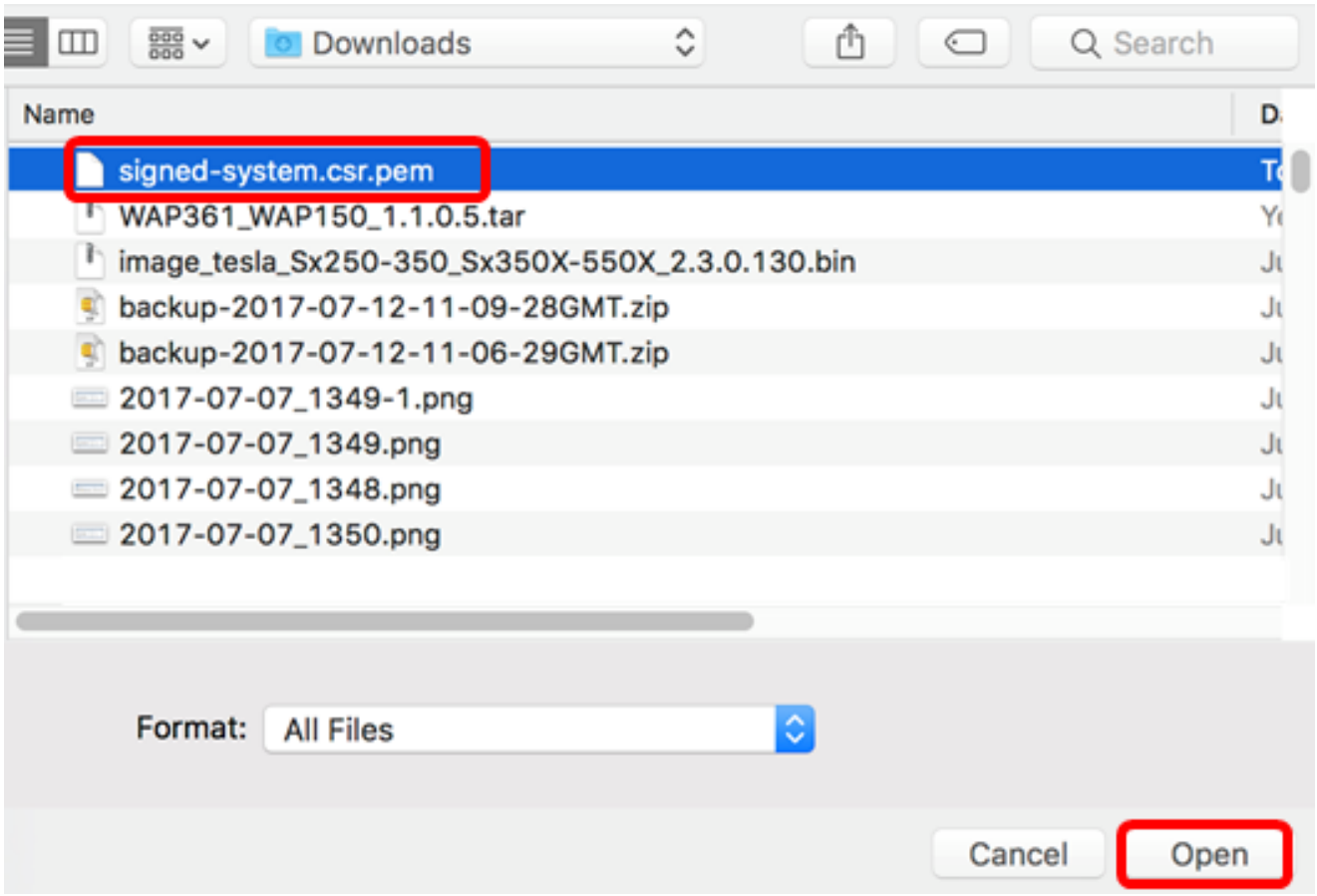


Paso 3. Haga clic en el botón de radio **UploadCert**.



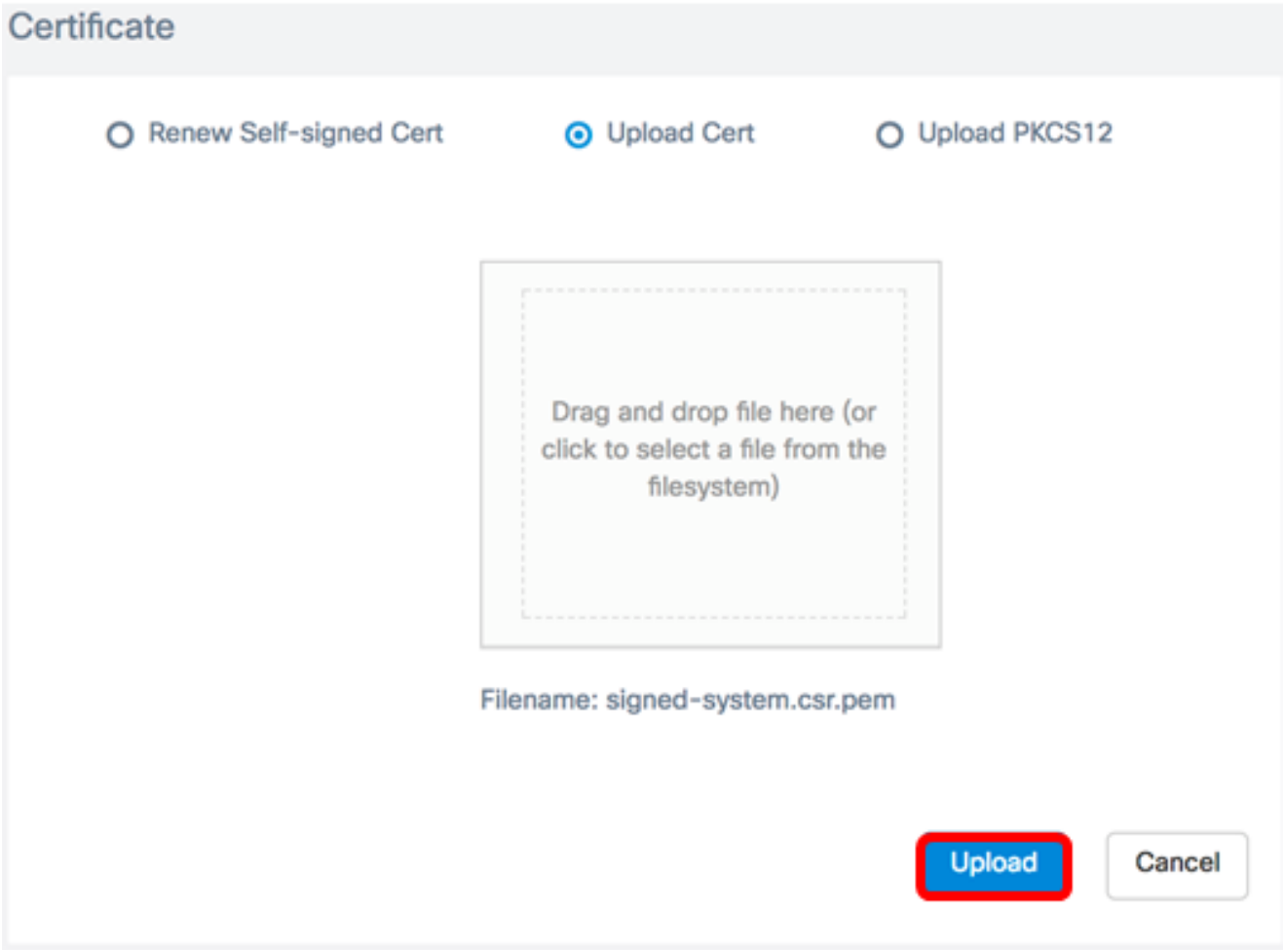
Nota: Alternativamente, puede cargar un certificado con la clave privada asociada en formato PKCS#12 eligiendo el botón de opción **Cargar PKCS12**. La contraseña para desbloquear el archivo debe especificarse en el campo *Password* proporcionado.

Paso 4. Suelte el certificado firmado en el área de destino o haga clic en el área de destino para navegar por el sistema de archivos y luego haga clic en **Abrir**. El archivo debe estar en formato .pem.



Nota: En este ejemplo, se utiliza signed-system.csr.pem.

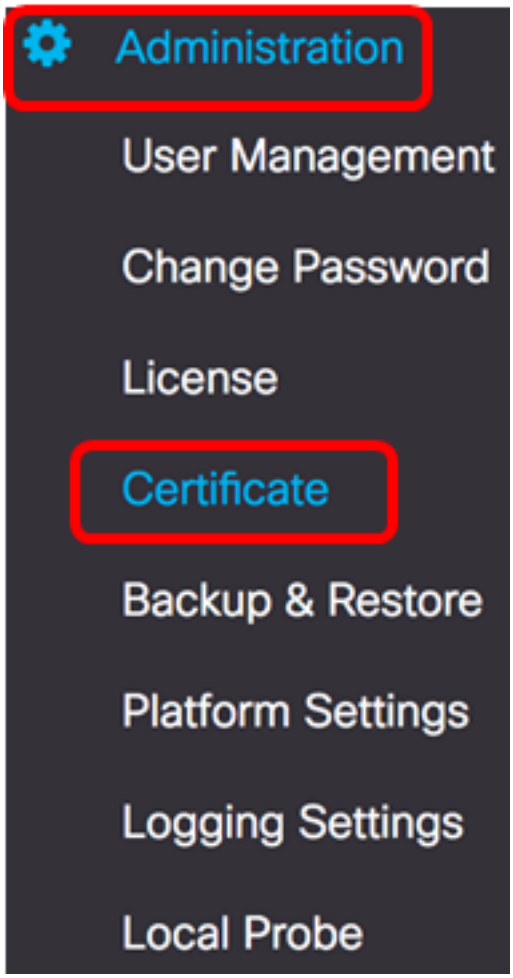
Paso 5. Haga clic en **Cargar**.



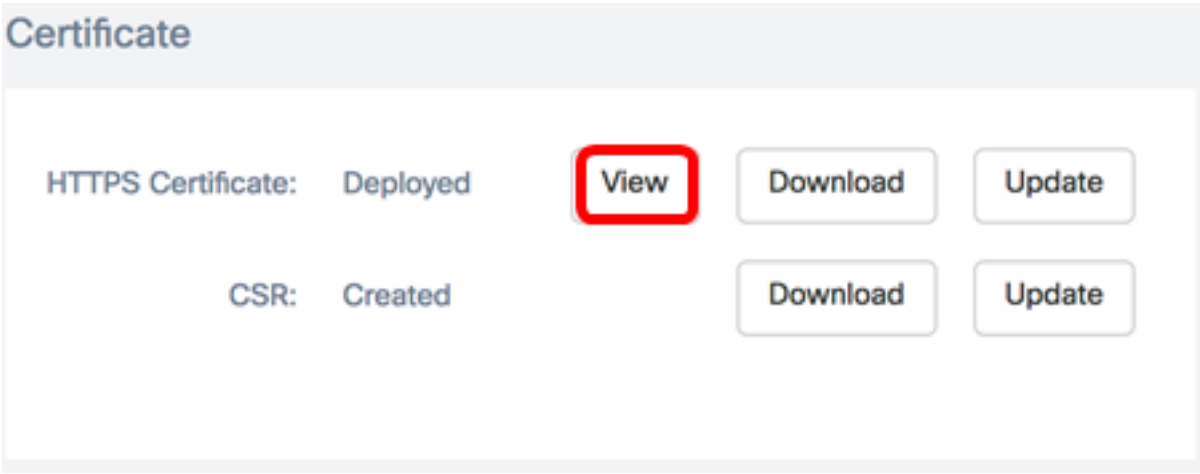
Ahora debería haber cargado correctamente un certificado firmado en FindIT Network Manager.

Administrar certificado actual

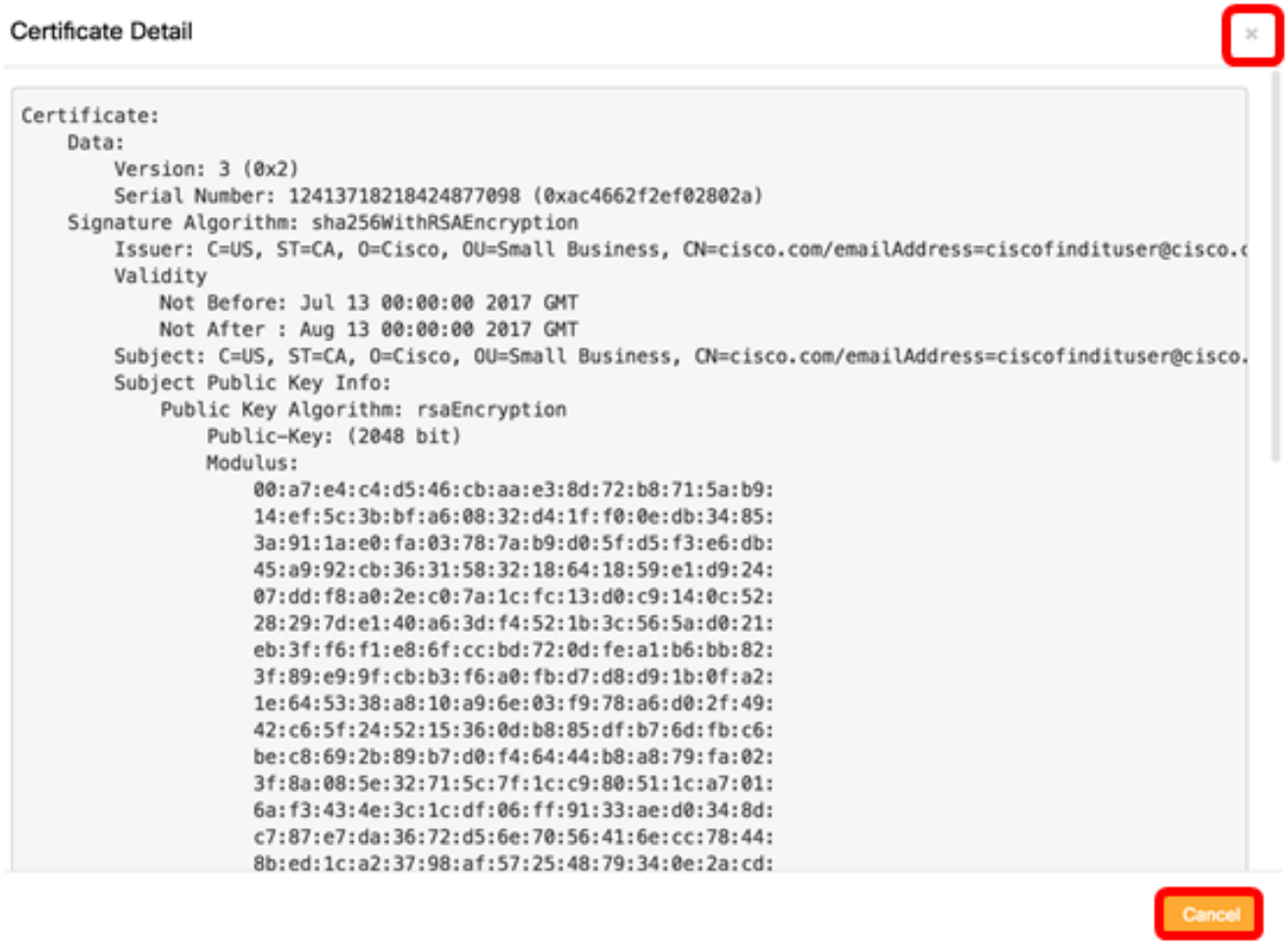
Paso 1. Inicie sesión en la GUI de administración de su FindIT Network Manager y luego elija **Administration > Certificate**.



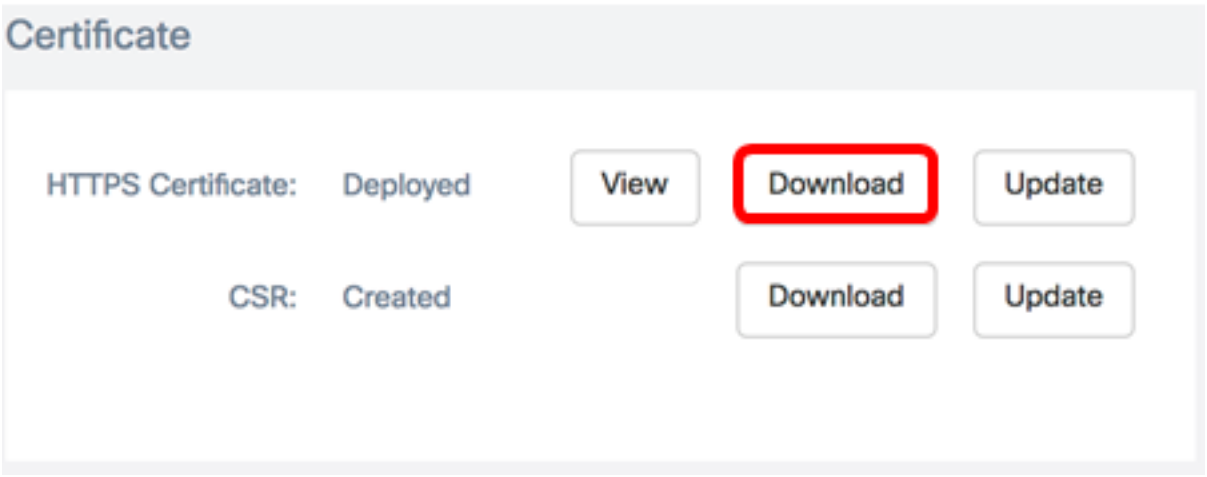
Paso 2. En el área HTTPS Certificate , haga clic en el botón **View**.



Paso 3. El certificado actual se mostrará en formato de texto sin formato en una nueva ventana del navegador. Haga clic en el botón **x** o **Cancel** para cerrar la ventana.



Paso 4. (Opcional) Para descargar una copia del certificado actual, haga clic en el botón **Download** en el área HTTPS Certificate .



Ahora debería haber gestionado correctamente el certificado actual en el administrador de red de FindIT.