Renovación de certificados SSO de TMS WebEx - Cisco

Contenido

Introducción

Este documento describe el procedimiento para renovar un certificado SSO de Webex en TMS cuando TMS está en la configuración híbrida de Webex con SSO.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- TMS (Cisco TelePresence Management Suite)
- SSO de Webex (inicio de sesión único)
- Configuración híbrida de Cisco Collaboration Meeting Rooms (CMR)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- TMS 15.0 y superiores

La información de este documento se basa en la Guía de Configuración Híbrida de Cisco Collaboration Meeting Rooms (CMR) (TMS 15.0 - WebEx Meeting Center WBS30).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

El artículo trata de un escenario en el que un certificado ya se ha renovado a través del portal web de la CA haciendo clic en el botón de renovación. El procedimiento para generar una nueva CSR (solicitud de firma de certificado) no se incluye en este documento.

Asegúrese de tener acceso al mismo servidor de Windows que generó el CSR original. En el caso de que no esté disponible el acceso al servidor Windows concreto, debe seguirse una nueva generación de certificados, según la guía de configuración.

Procedimiento para cargar el certificado renovado en TMS

Importar el certificado

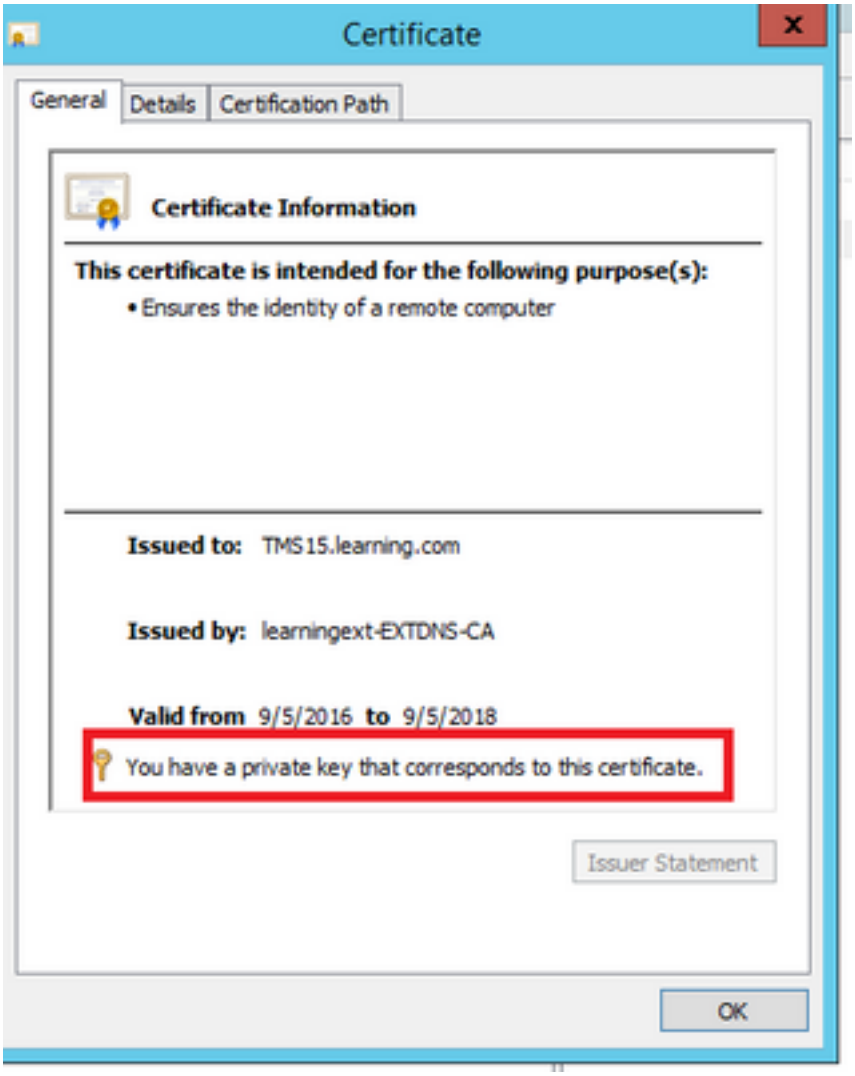
Para importar el certificado renovado en el mismo servidor de Windows donde se ha generado el CSR original, realice los pasos siguientes.

Paso 1. Vaya a **Inicio > Ejecutar > mmc**. Haga clic en **Archivo > Agregar complemento > Equipo local** (se puede utilizar el usuario actual).

Paso 2. Haga clic en **Acción > Importar** y seleccione el certificado renovado. Seleccionar **almacén de certificados: Personal** (elige diferente si es necesario).

Paso 3. Una vez que se haya importado el certificado, haga clic con el botón derecho del ratón en él y abra el certificado.

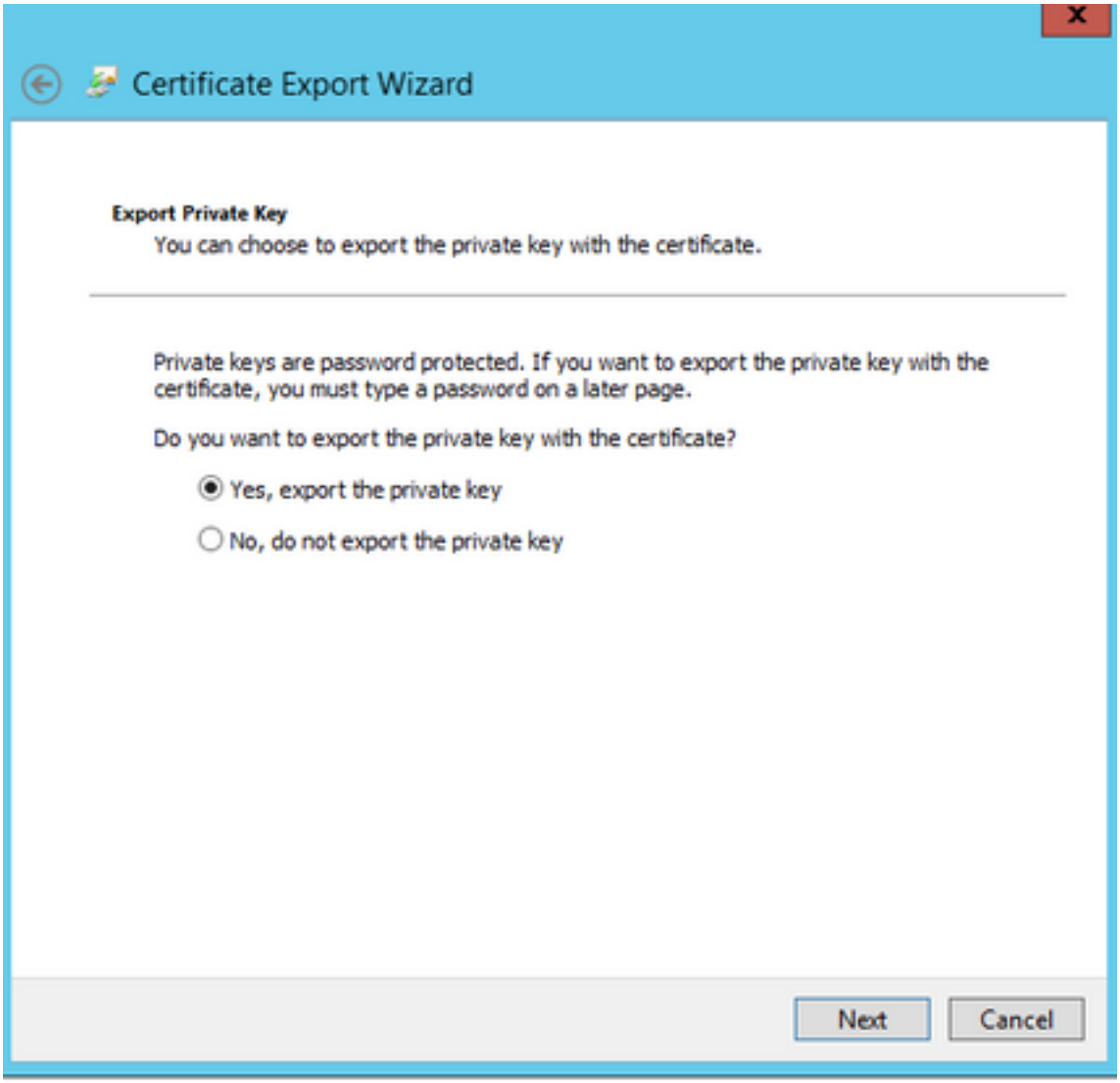
- Si el certificado se ha renovado en función de la clave privada del mismo servidor, el certificado debe mostrar: "Tiene una clave privada que corresponde a este certificado", como en el ejemplo siguiente:

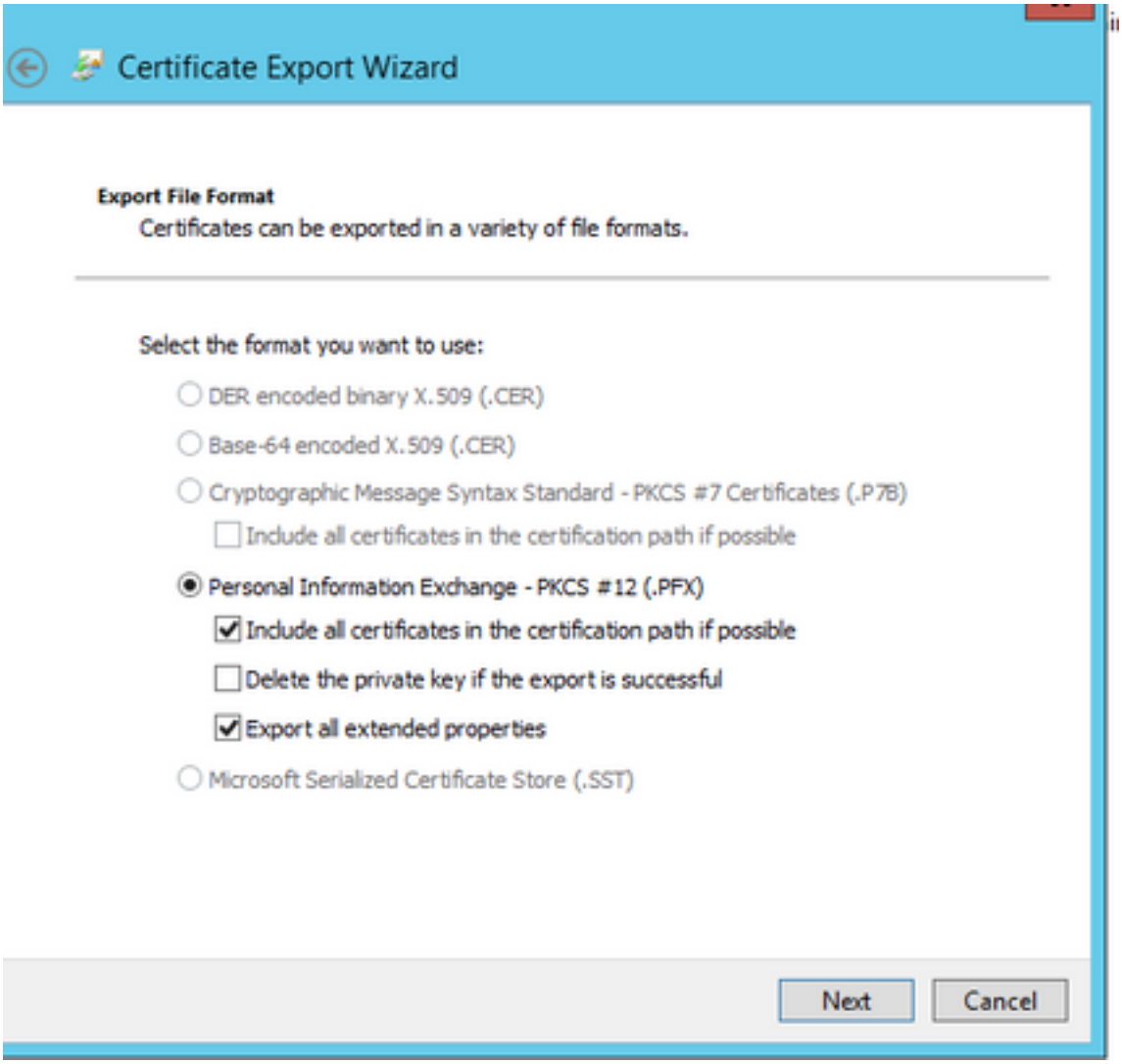


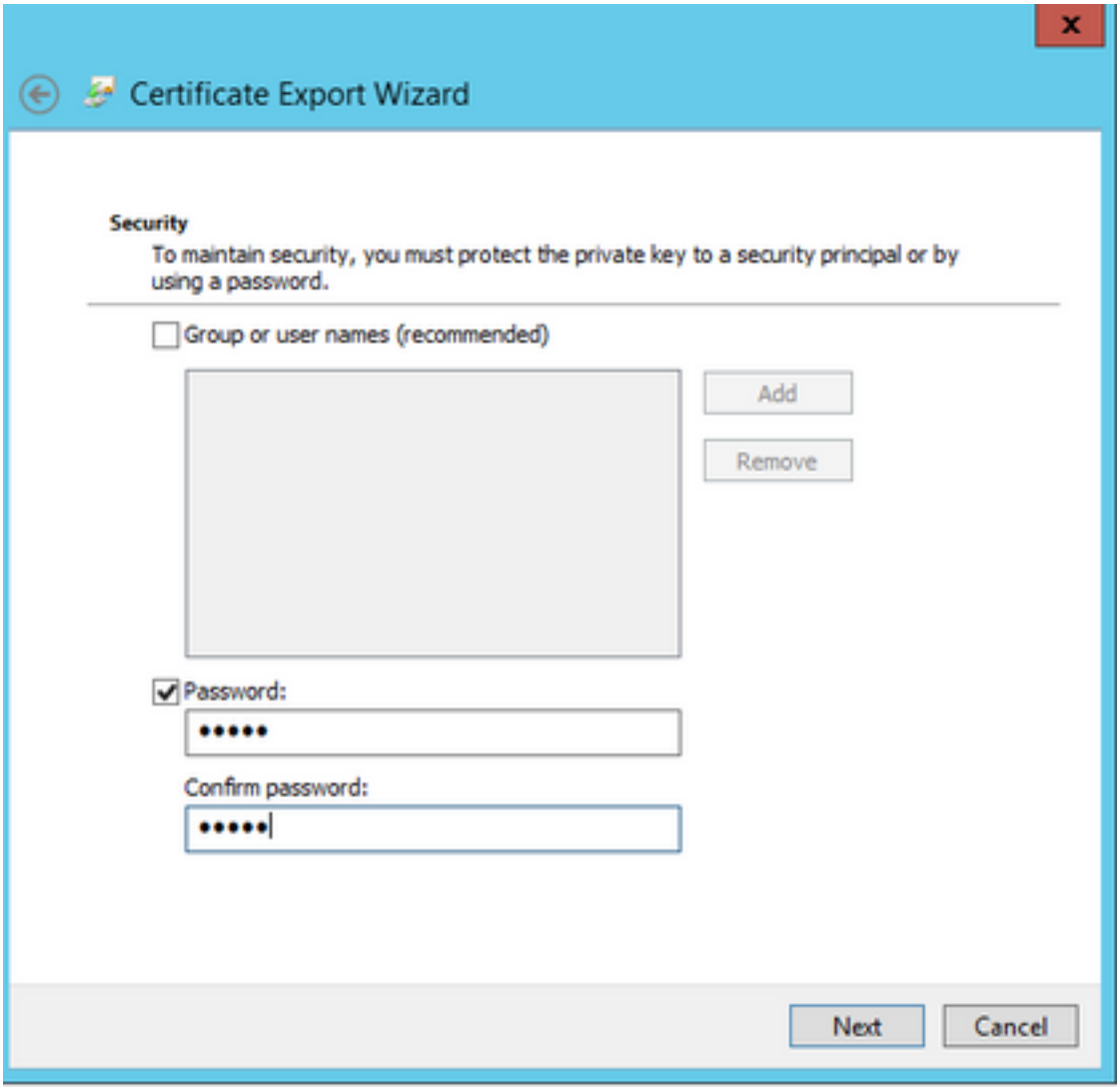
Exportar el certificado y cargarlo en TMS

Para exportar el certificado renovado junto con su clave privada, realice los pasos siguientes.

Paso 1. Mediante el **complemento Administrador de certificados de Windows**, exporte la clave privada existente (par de certificados) como un archivo **PKCS#12**:


Certificate Export Wizard
Export Private Key
You can choose to export the private key with the certificate.
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.
Do you want to export the private key with the certificate?
Yes, export the private key
No, do not export the private key
Next
Cancel


Certificate Export Wizard
Export File Format
Certificates can be exported in a variety of file formats.
Select the format you want to use:
DER encoded binary X.509 (.CER)
Base-64 encoded X.509 (.CER)
Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
Include all certificates in the certification path if possible
Personal Information Exchange - PKCS #12 (.PFX)
Include all certificates in the certification path if possible
Delete the private key if the export is successful
Export all extended properties
Microsoft Serialized Certificate Store (.SST)
Next
Cancel



Paso 2. Mediante el **complemento Administrador de certificados de Windows**, exporte el certificado existente como un **archivo .CER codificado por PEM Base64**. Asegúrese de que la extensión del archivo sea **.cer** o **.crt** y proporcione este archivo al equipo de servicios en la nube de WebEx.

Paso 3. Inicie sesión en Cisco TMS y navegue hasta **Administrative Tools > Configuration > WebEx Settings**. En el panel Sitios de WebEx, verifique todos los parámetros, incluido SSO.

Paso 4. Haga clic en **Examinar** y cargue el **certificado de clave privada (.pfx) PKS #12** que generó al **generar un certificado para WebEx**. Complete el resto de los campos de configuración SSO utilizando la contraseña y otra información que seleccionó al generar el certificado. Click **Save**.

En el caso de que la clave privada esté disponible exclusivamente, puede combinar el certificado firmado en formato .pem con la clave privada mediante el siguiente comando OpenSSL:

openssl pkcs12 -export -inkey tms-privatekey.pem -in tms-cert.pem -out tms-cert-key.p12 -name tms-cert-key

Ahora debe tener un certificado Cisco TMS que contenga la clave privada para que la configuración SSO se cargue en Cisco TMS.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Guía de configuración híbrida de Cisco Collaboration Meeting Rooms (CMR) (TMS 15.0 - WebEx Meeting Center WBS30)