Renovación del certificado del WebEx SSO TMS - Cisco

Contenido

Introducción

Este documento describe el procedimiento para renovar un certificado del WebEx SSO en TMS cuando TMS está en Configuración de Híbrido del WebEx con el SSO.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- TMS (conjunto de administración del Cisco TelePresence)
- WebEx SSO (escoja Muestra-en)
- Configuración de Híbrido de las Salas de reuniones de la colaboración de Cisco (CMR)

Componentes Utilizados

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

- TMS 15.0 y arriba

La información en este documento se basa en la guía de Configuración de Híbrido de las Salas de reuniones de la colaboración de Cisco (CMR) (TMS 15.0 - el centro WBS30 de la reunión del WebEx).

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si su red está viva, asegúrese de que usted entienda el impacto potencial del comando any.

Antecedentes

El artículo cubre un escenario en el cual un certificado ha sido renovado ya vía el portal de red CA haciendo clic en el botón Renew Button. El procedimiento para generar un nuevo CSR (pedido de firma de certificado) no se incluye en este documento.

Asegúrese de que usted tenga acceso al mismo Servidor Windows que generó el CSR original. En el caso cuando el acceso al Servidor Windows determinado no está disponible, una nueva generación del certificado tiene que ser seguida, según la guía de configuración.

Procedimiento para cargar el certificado renovado en TMS

Importe el certificado

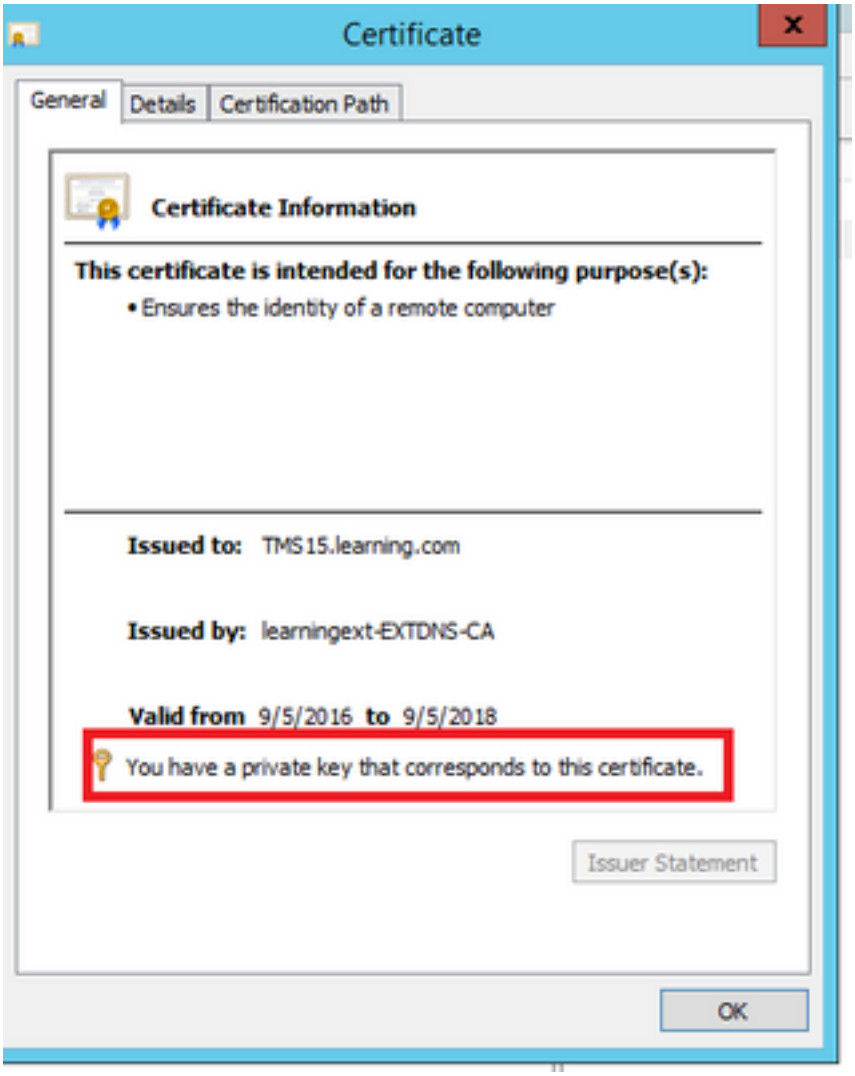
Para importar el certificado renovado en el mismo Servidor Windows donde se ha generado el CSR original, realice los pasos siguientes.

Paso 1. Navegue al **Start (Inicio) > Run (Ejecutar) > al mmc**. Haga clic en el **archivo > Add Broche-en > computadora local** (el Usuario usuario actual puede ser utilizado).

Paso 2. Haga clic en la **acción > la importación** y seleccione el certificado renovado. Seleccione el **almacén de certificados: Personal** (eligió diferente si procede).

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

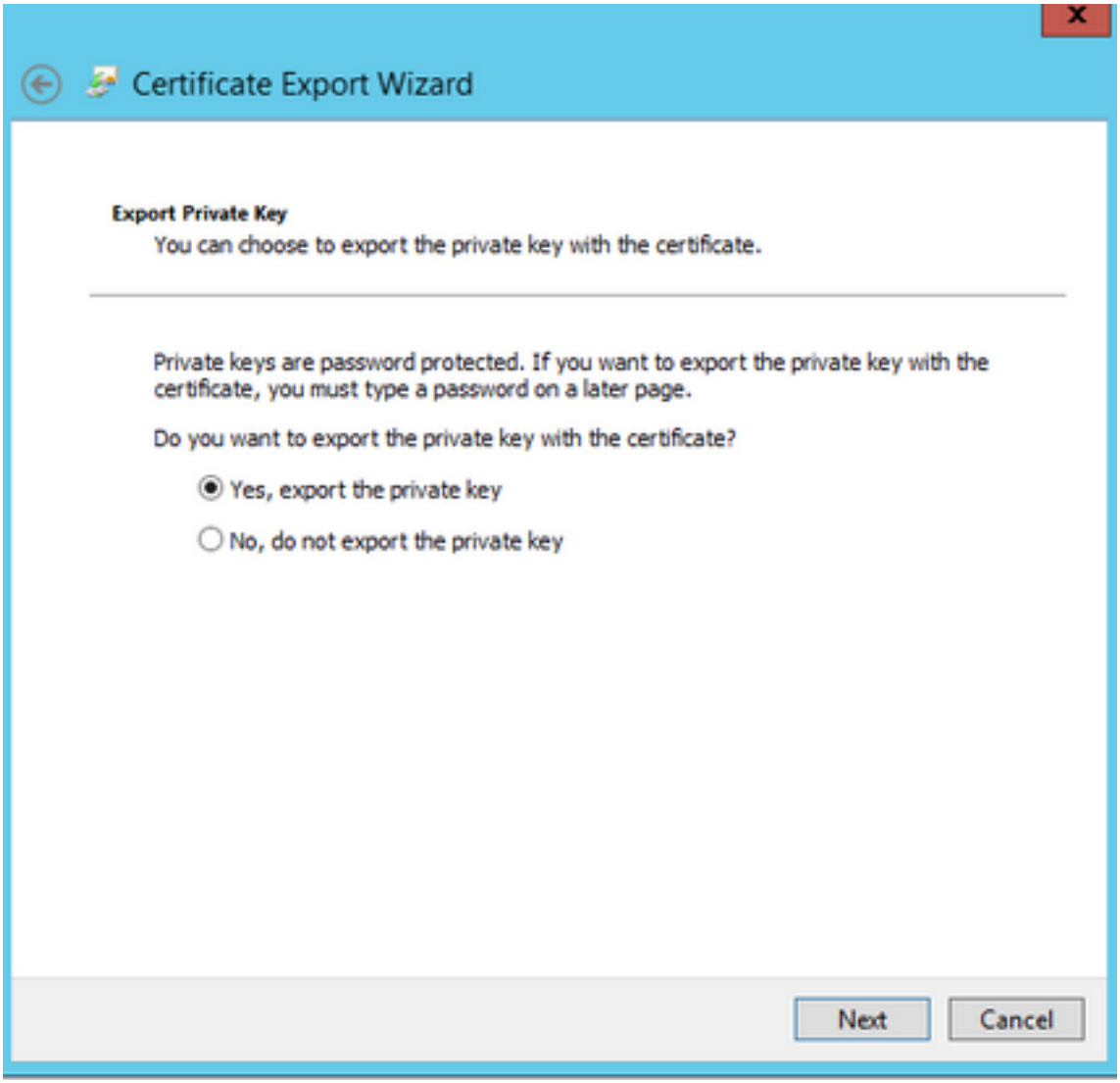
- Si se renueva el certificado basó en la clave privada del mismo servidor, el certificado visualiza: “Usted tiene una clave privada que corresponda a este certificado” como en el ejemplo abajo:

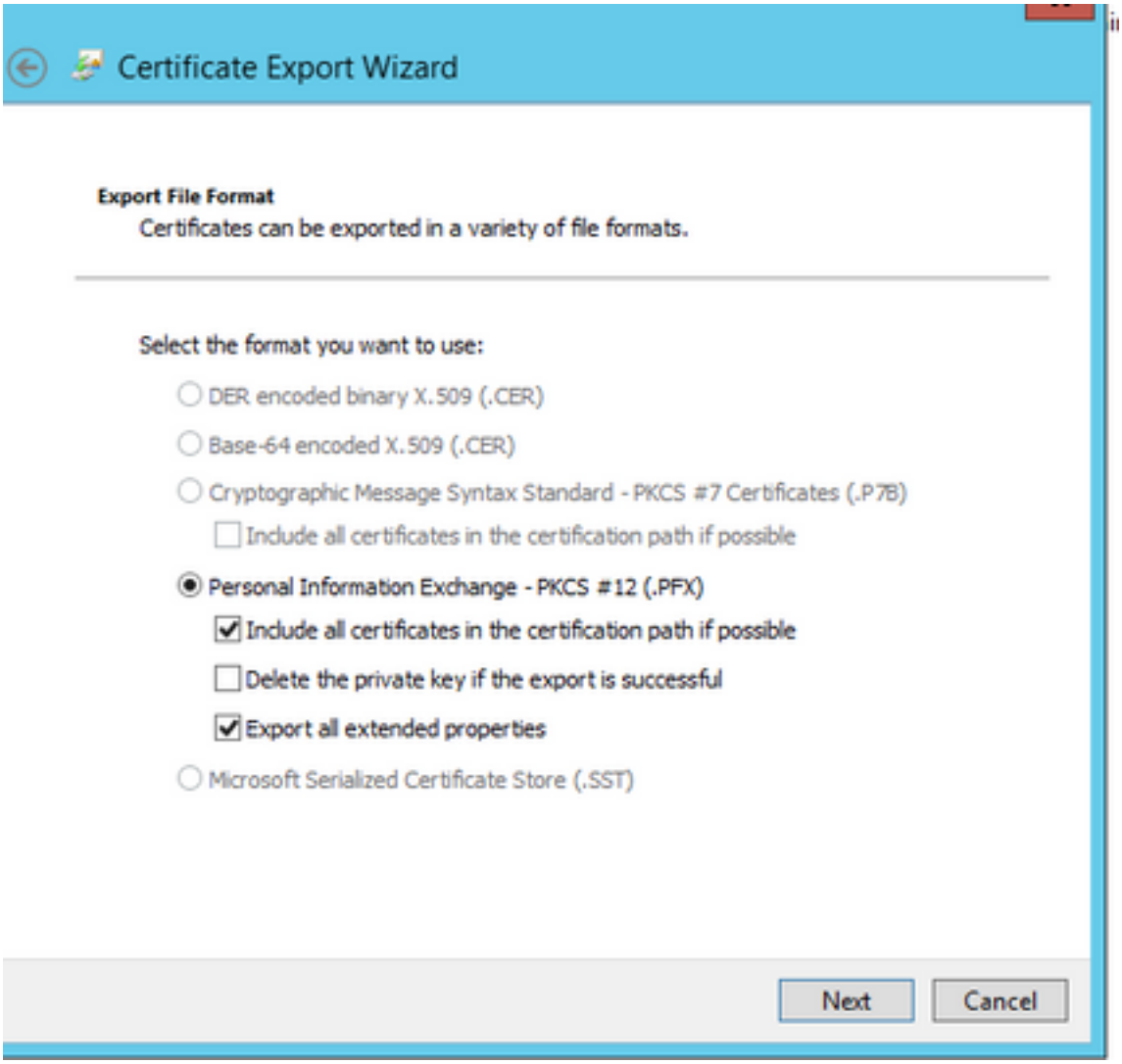


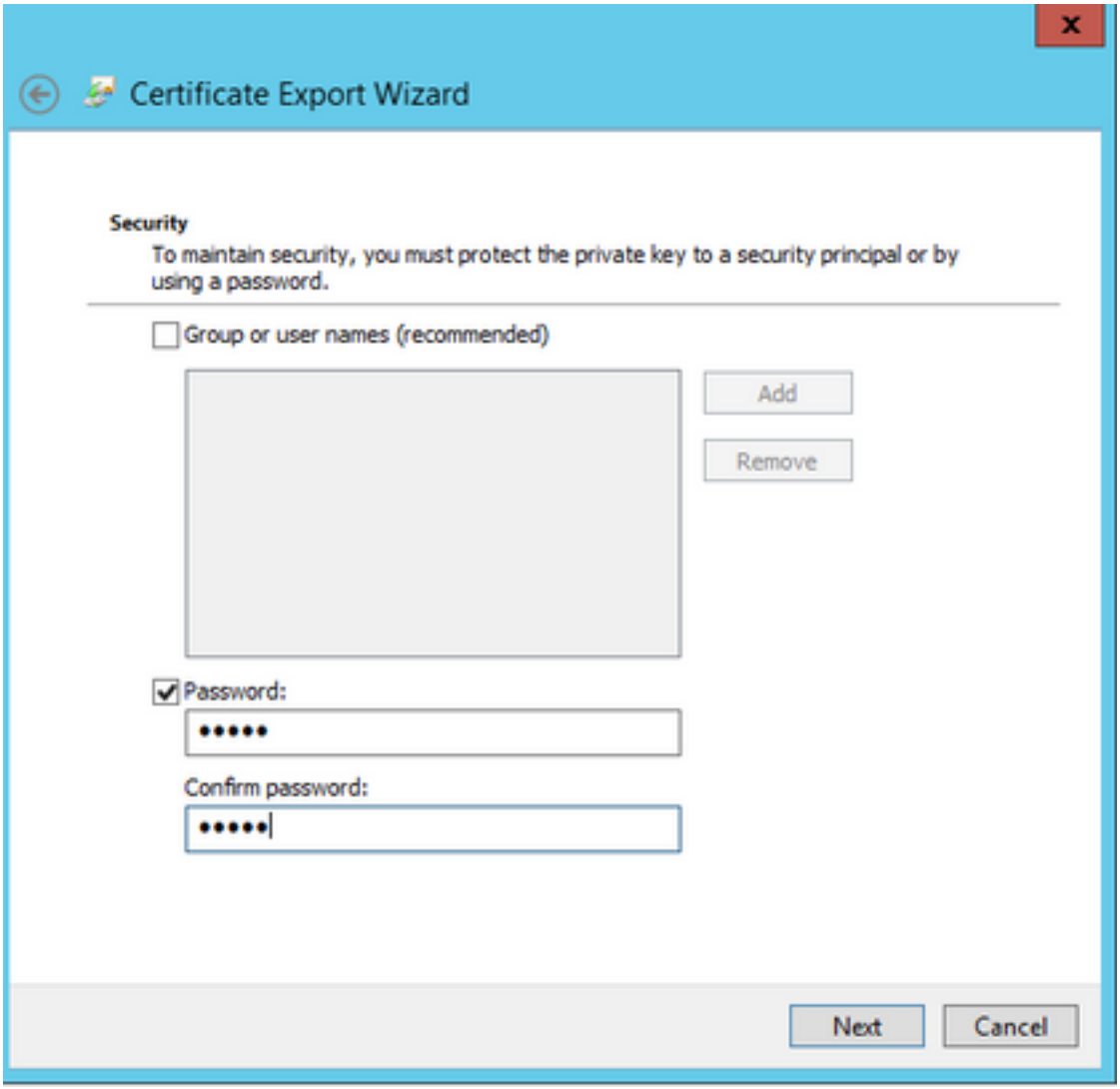
Exporte el certificado y carguelo en TMS

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

Paso 1. Usando el **Certificate Manager de Windows Broche-en**, exporte la clave privada existente (par del certificado) como archivo del **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. Usando el **Certificate Manager de Windows Broche-en**, exporte el certificado existente como un **base64 PEM codificó el** archivo **.CER**. Asegúrese de que la extensión de archivo sea **.cer** o **.crt** y proporcione este archivo al equipo de los servicios de la nube del WebEx.

Paso 3. Registre en Cisco TMS, y navegue a las **herramientas administrativas > a las configuraciones de la configuración > del WebEx**. En el cristal de los sitios del WebEx, verifique todas las configuraciones incluyendo el SSO.

Paso 4. Haga clic en **hojean** y cargan el certificado de la clave privada **PKS #12** (.pfx) que usted generó en la **generación de un certificado para el WebEx**. Complete el resto de los campos configuraciones SSO usando la contraseña y la otra información que usted seleccionó al generar el certificado. Haga clic en Save (Guardar).

En el caso cuando la clave privada está disponible exclusivamente, usted puede combinar el certificado firmado en el formato del .pem con la clave privada usando el comando siguiente del OpenSSL:

pkcs12 del openssl - exportación - el inkey tms-privatekey.pem - en tms-cert.pem - hacia fuera tms-cert-key.p12 - nombre la tms-CERT-clave

Usted debe ahora tener un certificado de Cisco TMS que contenga la clave privada para que la configuración SSO cargue a Cisco TMS.

Troubleshooting

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

Información Relacionada

- Guía de Configuración de Híbrido de las Salas de reuniones de la colaboración de Cisco (CMR) (TMS 15.0 - centro WBS30 de la reunión del WebEx)