TMS Webex SSO-certificaatvernieuwing - Cisco

Inhoud

Inleiding

In dit document wordt de procedure beschreven om een Webex SSO-certificaat op TMS te vernieuwen wanneer TMS zich in de Webex Hybrid-configuratie met SSO bevindt.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- TMS (Cisco TelePresence Management Suite)
- Webex SSO (één aanmelding)
- Hybride configuratie van Cisco Collaboration Meeting Rooms (CMR)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- TMS 15.0 en hoger

De informatie in dit document is gebaseerd op de Cisco Collaboration Meeting Rooms (CMR) Hybrid Configuration Guide (TMS 15.0 - Webex Meeting Center WBS30).

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

Het artikel betreft een scenario waarin een certificaat al is vernieuwd via het CA-webportaal door op de vernieuwingsknop te klikken. De procedure voor het genereren van een nieuw CSR (certificaatsignaalaanvraag) is niet in dit document opgenomen.

Zorg ervoor dat u toegang hebt tot dezelfde Windows-server die de oorspronkelijke CSR gegenereerd heeft. In het geval dat de toegang tot de specifieke Windows-server niet beschikbaar is, moet een nieuwe certificatengeneratie worden gevolgd, zoals in de configuratiegids wordt beschreven.

Procedure voor het uploaden van het vernieuwde certificaat op TMS

Importeer het certificaat

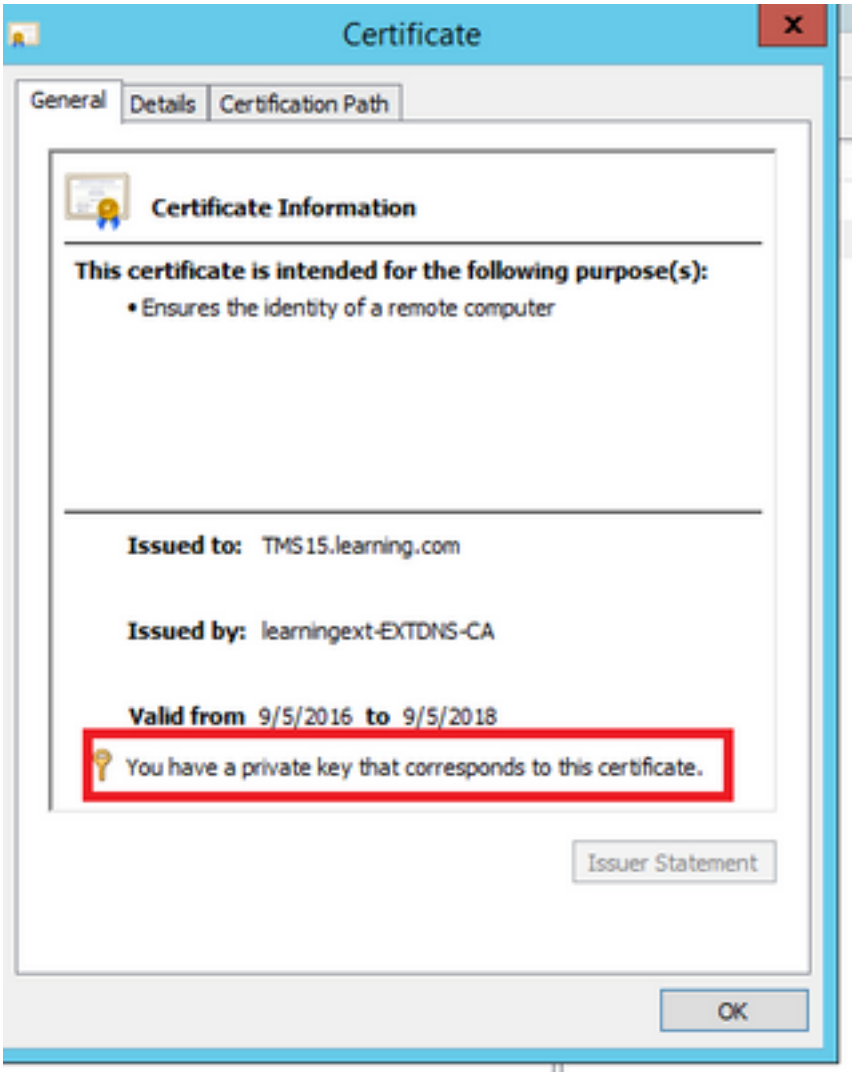
Voer de volgende stappen uit om het hernieuwde certificaat te importeren op dezelfde Windows-server waar de oorspronkelijke CSR is gegenereerd.

Stap 1. Navigeer naar **Start > Run > mmc**. Klik op **Bestand > Magnetisch toevoegen > Lokale computer** (de huidige gebruiker kan worden gebruikt).

Stap 2. Klik op **Actie > Importeren** en selecteer het hernieuwde certificaat. Selecteer **certificaatopslaan: Persoonlijk** (kies indien nodig anders).

Stap 3. Klik met de rechtermuisknop op het certificaat en open het certificaat.

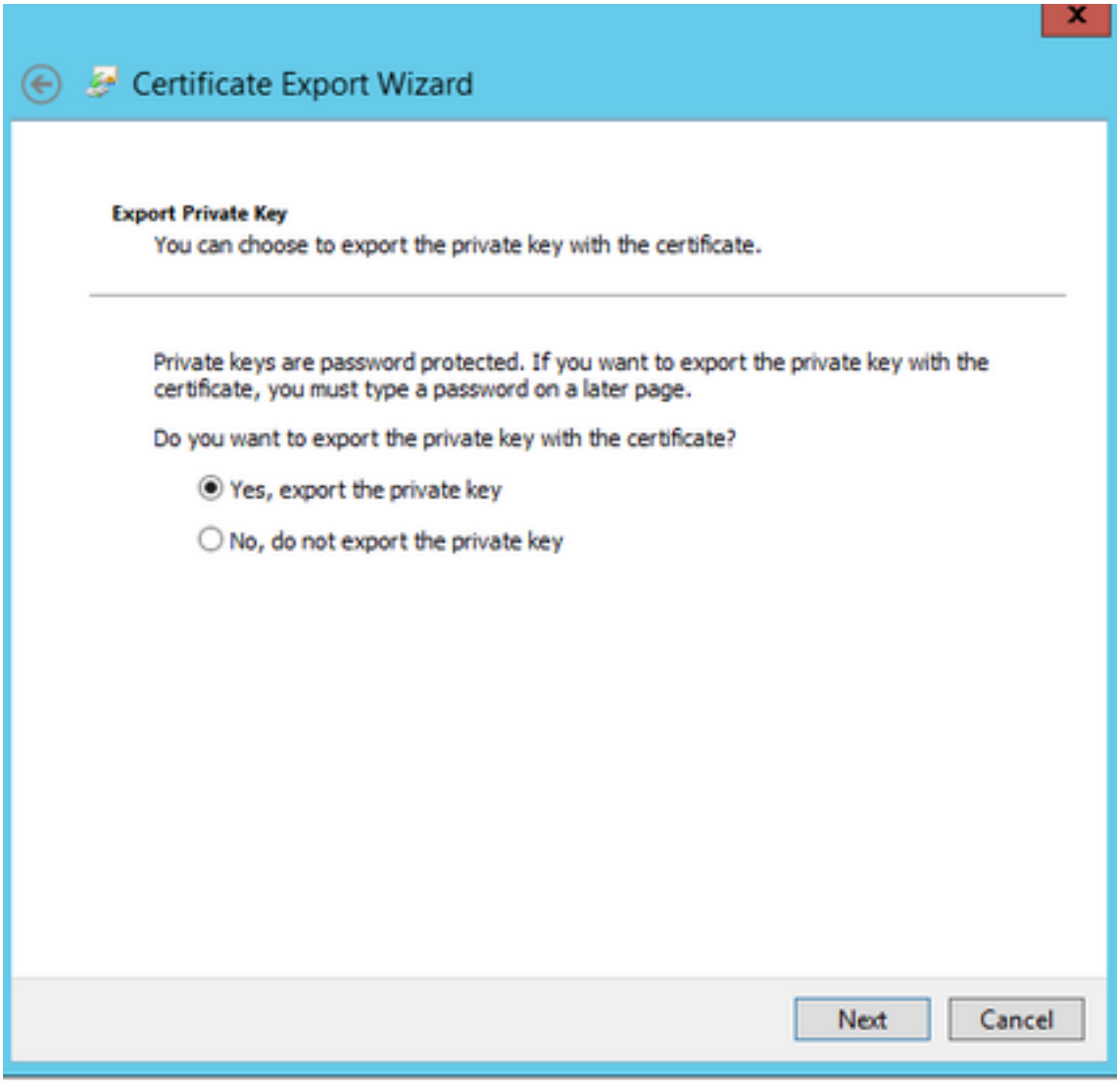
- Als het certificaat is vernieuwd op basis van de privésleutel van dezelfde server, dient het certificaat het volgende te bevatten: "U hebt een privé-sleutel die met dit certificaat overeenkomt" zoals in het onderstaande voorbeeld:

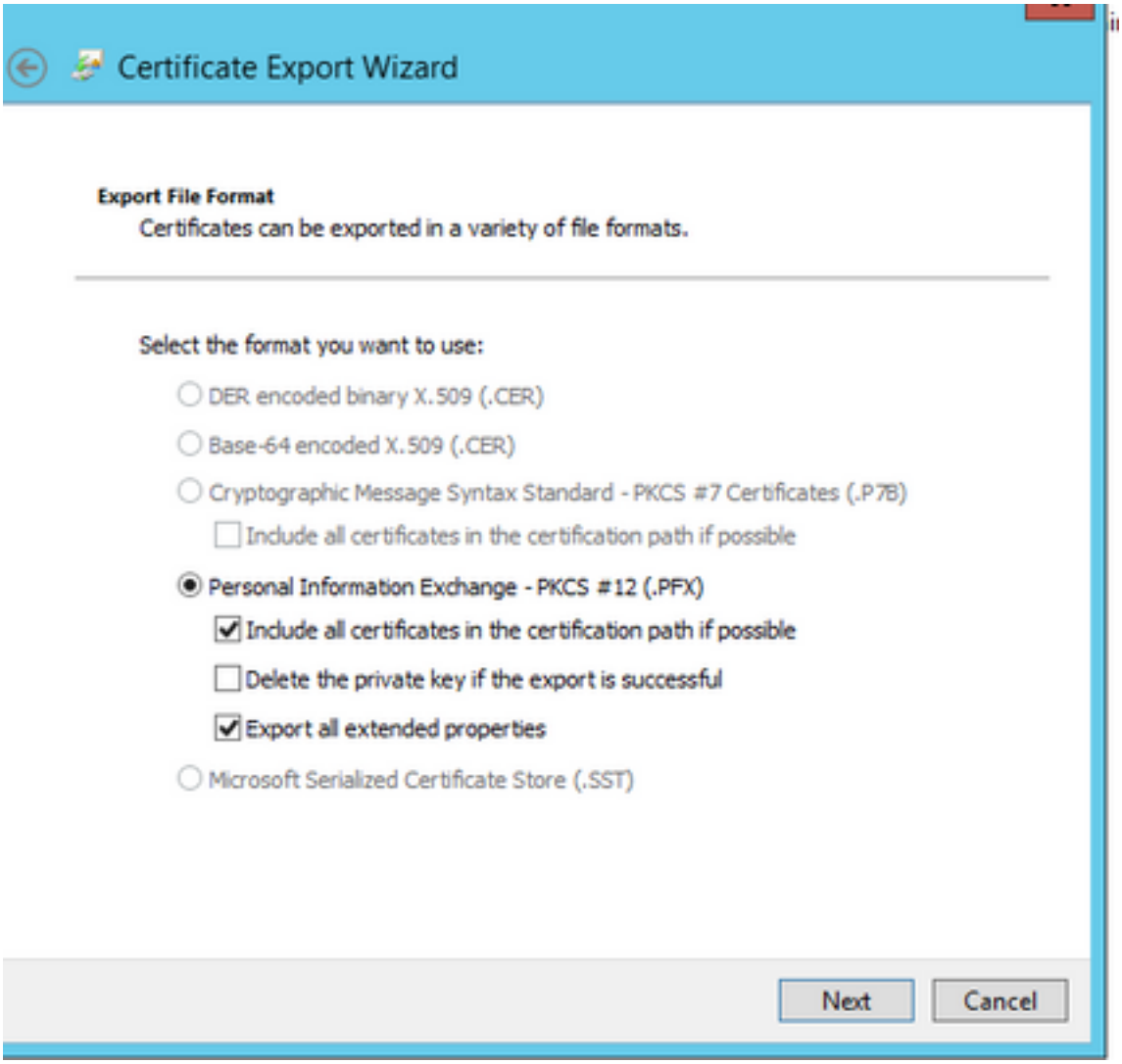


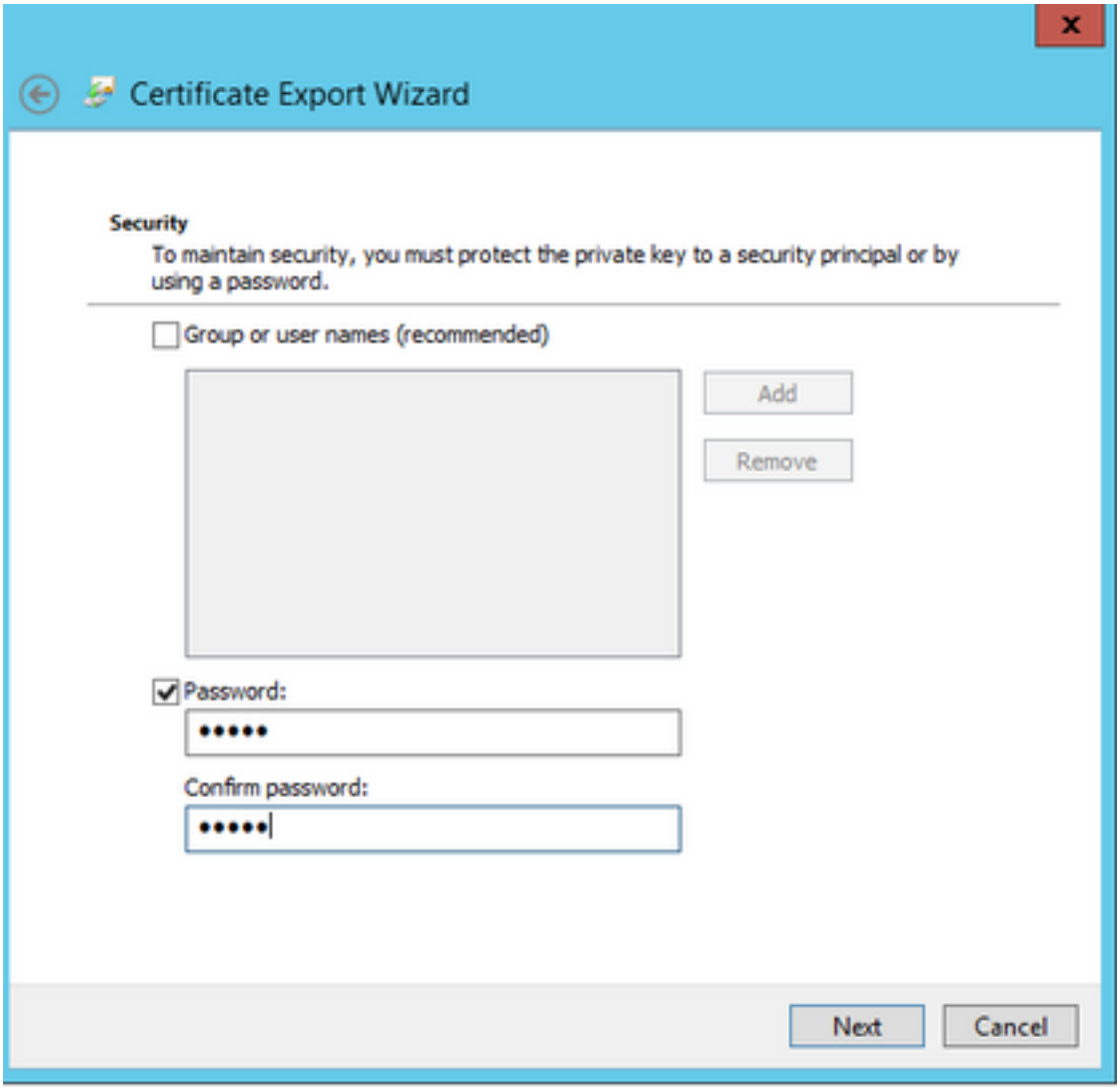
Exporteren op het certificaat en uploaden het op TMS

Voer de volgende stappen uit om het hernieuwde certificaat samen met de bijbehorende particuliere sleutel uit te voeren.

Stap 1. Gebruik de **Windows certificaatManager Magnetisch-in**, voer de bestaande privé-toets (certificaatpaar) uit als **PKCS#12-**bestand:


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



Stap 2. Wanneer u de **Windows certificaatManager Magnetisch-in** gebruikt, exporteert u het bestaande certificaat als een **Base64 PEM-gecodeerd .CER-**bestand. Zorg ervoor dat de bestandsextensie **.cer** of **.crt** is en specificeer dit bestand aan het Webex Cloud Services-team.

Stap 3. Meld u aan bij Cisco TMS en navigeer naar **beheertools > Configuration > Webex Settings**. Controleer in het venster Webex Sites alle instellingen, inclusief de SSO.

Stap 4. Klik op **Bladeren** en uploaden de **PKS #12** privé-sleutelcertificaat (.pfx) dat u gegenereerd hebt **door een certificaat voor Webex te genereren**. Vul de rest van de SSO-configuratievelden in met behulp van het wachtwoord en andere informatie die u hebt geselecteerd bij het genereren van het certificaat. Klik op **Opslaan**.

Wanneer de privé-toets uitsluitend beschikbaar is, kunt u het ondertekende certificaat in .pem-indeling combineren met de privé-toets door de volgende OpenSSL-opdracht te gebruiken:

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

U dient nu een Cisco TMS-certificaat te hebben dat de privésleutel voor de SSO-configuratie bevat om te uploaden naar Cisco TMS.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- Cisco CMR-ruimtes (samenwerkingsruimtes voor vergaderingen) voor hybride configuratie (TMS 15.0 - Webex Meeting Center WBS30)