Renouvellement de certificat du WebEx SSO TMS - Cisco

Contenu

Introduction

Ce document décrit la procédure pour renouveler un certificat du WebEx SSO sur TMS quand TMS est en configuration hybride de WebEx avec SSO.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- TMS (suite logicielle de gestion Cisco TelePresence)
- WebEx SSO (ouverture de session simple)
- Configuration hybride des salles de téléconférence de Cisco Collaboration (CMR)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- TMS 15.0 et en haut

Les informations dans ce document sont basées sur le guide de configuration hybride des salles de téléconférence de Cisco Collaboration (CMR) (TMS 15.0 - WebEx Meeting Center WBS30).

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est vivant, assurez-vous que vous comprenez l'impact potentiel de n'importe quelle commande.

Informations générales

L'article couvre un scénario dans lequel un certificat a été déjà renouvelé par l'intermédiaire du portail web CA en cliquant sur sur le bouton de renouveler. La procédure pour générer un nouveau CSR (demande de signature de certificat) n'est pas incluse dans ce document.

Assurez-vous que vous avez accès aux mêmes Windows Server qui ont généré le CSR d'original. Dans le cas quand l'accès aux Windows Server particuliers n'est pas disponible, une nouvelle génération de certificat doit être suivie, selon le guide de configuration.

Procédure pour télécharger le certificat renouvelé sur TMS

Importez le certificat

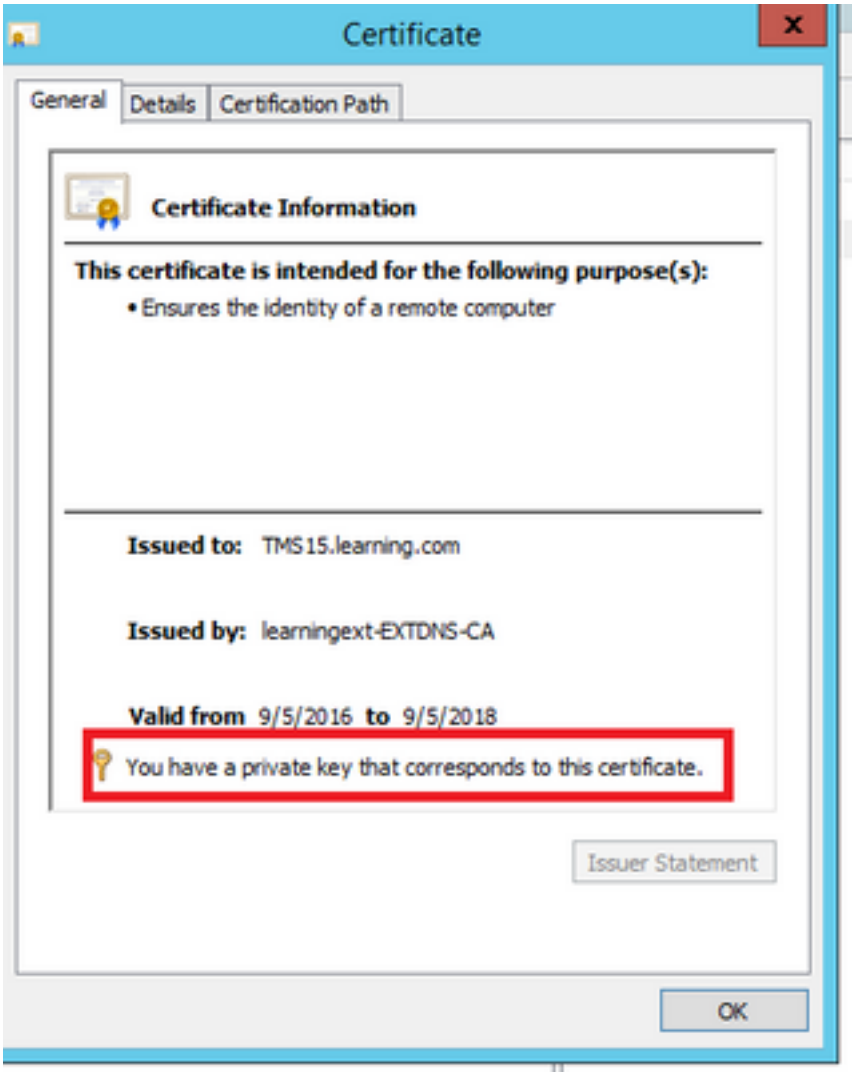
Afin d'importer le certificat renouvelé sur les mêmes Windows Server où le CSR d'original a été généré, exécutez les étapes suivantes.

Étape 1. Naviguez vers le **Start > Run > le MMC**. Cliquez sur en fonction le **fichier > ajoutent SNAP-dans > ordinateur local** (l'utilisateur courant peut être utilisé).

Étape 2. Cliquez sur en fonction l'**action > l'importation** et sélectionnez le certificat renouvelé. **Mémoire** choisie de **certificat : Personnel** (a choisi s'il y a lieu différent).

Étape 3. Une fois le certificat est importé, clic droit là-dessus et ouvre le certificat.

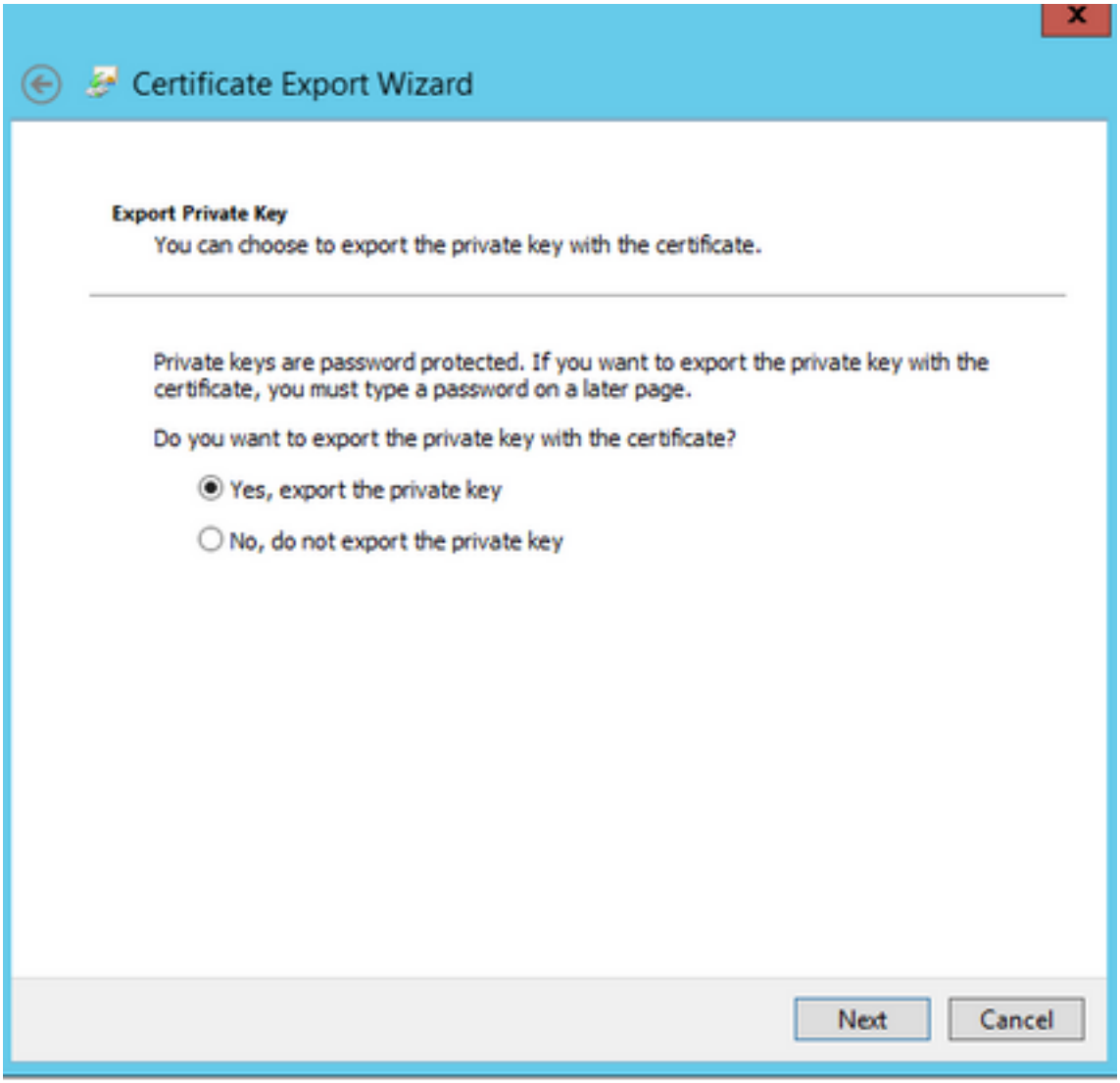
- Si le certificat a été renouvelé basait sur la clé privée du même serveur, le certificat affiche : « Vous avez une clé privée qui correspond à ce certificat » comme dans l'exemple ci-dessous :

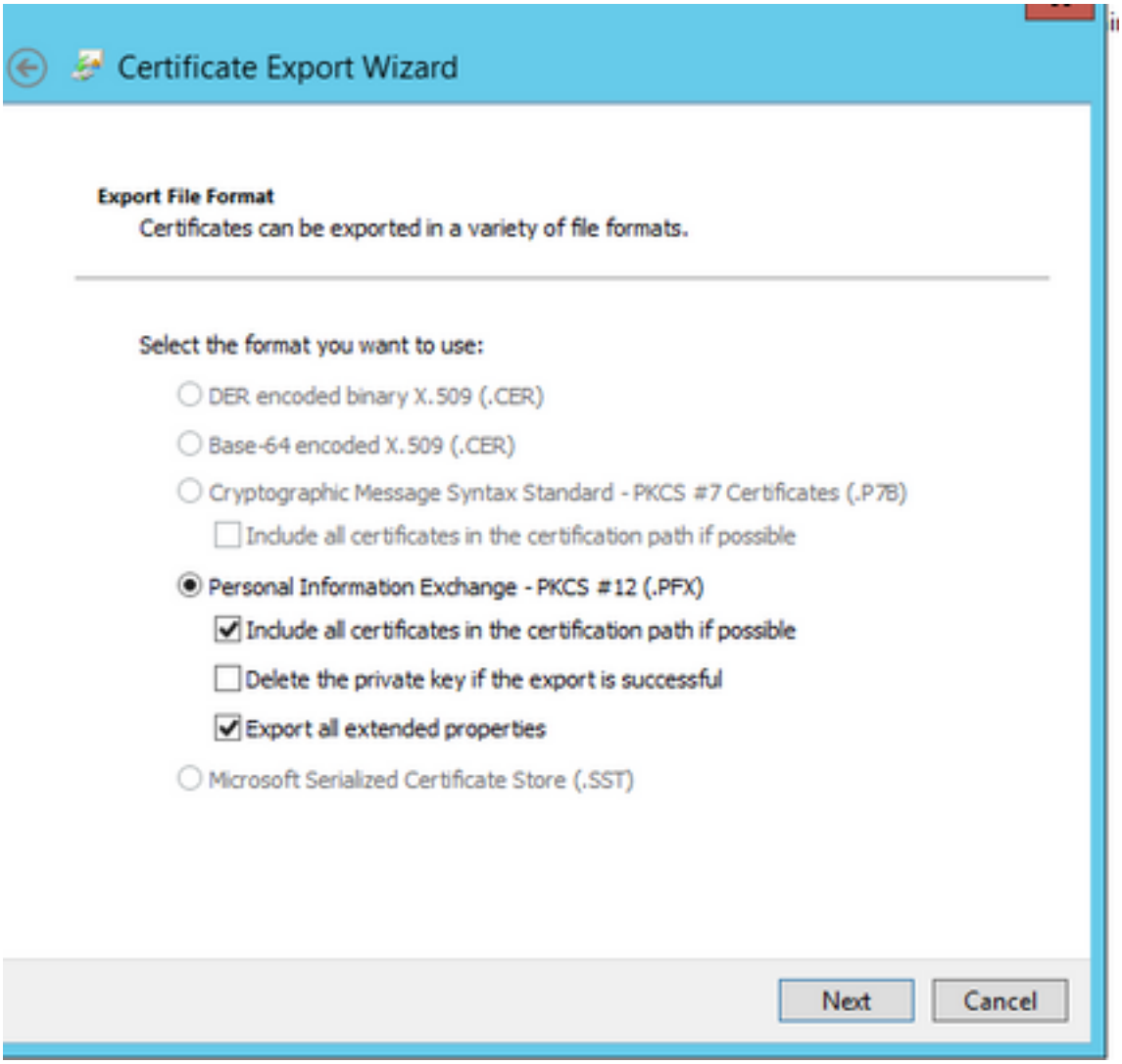


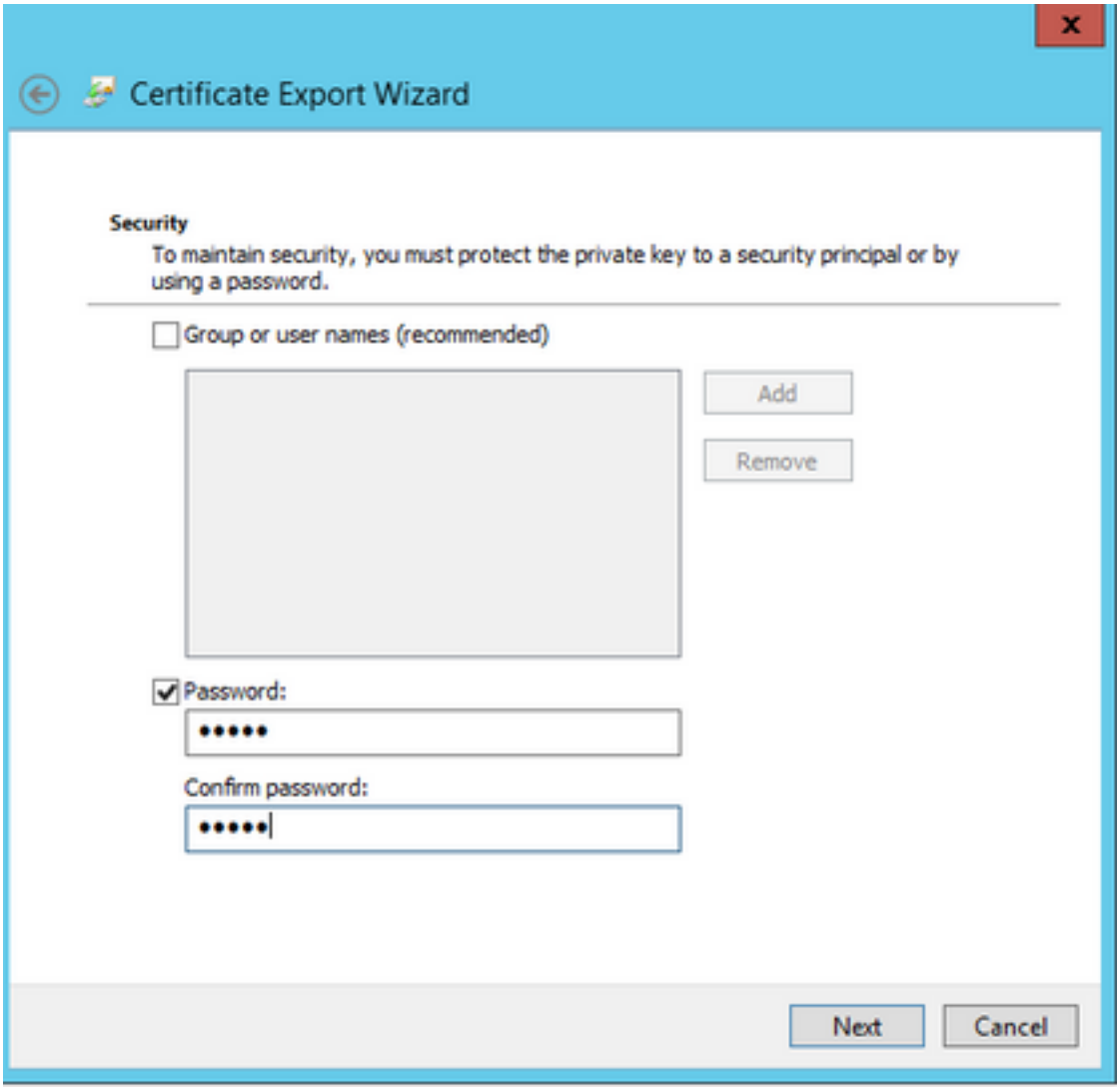
Exportez le certificat et téléchargez-le sur TMS

Afin d'exporter le certificat renouvelé avec sa clé privée, exécutez les étapes suivantes.

Étape 1. Utilisant le **gestionnaire de certificat de Windows SNAP-dans**, exportez la clé privée existante (paire de certificat) comme un fichier **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



Étape 2. Utilisant le **gestionnaire de certificat de Windows SNAP-dans**, exportez le certificat existant comme un **PEM Base64 a encodé le** fichier **.CER**. Assurez-vous que l'extension de fichier est **.cer** ou **.crt** et fournissez ce fichier à l'équipe de services en nuage de WebEx.

Étape 3. Connectez-vous dans Cisco TMS, et naviguez vers des **outils d'administration > des configurations de configuration > de WebEx**. Au volet de sites de WebEx, vérifiez toutes les configurations comprenant SSO.

Étape 4. Cliquez sur en fonction **Browse** et téléchargez le certificat de clé privée **PKS #12** (.pfx) que vous avez généré à **générer un certificat pour le WebEx**. Terminez-vous le reste des champs de configuration SSO utilisant le mot de passe et d'autres informations que vous avez sélectionnés en générant le certificat. Cliquez sur **Save**.

Dans le cas quand la clé privée est disponible exclusivement, vous pouvez combiner le certificat signé dans le format .pem avec la clé privée utilisant la commande suivante d'OpenSSL :

l'openssl pkcs12 - exportation - l'inkey tms-privatekey.pem - dans tms-cert.pem - tms-cert-key.p12 - nommez la tms-CERT-clé

Vous devriez maintenant avoir un certificat de Cisco TMS qui contient la clé privée pour que la configuration SSO la télécharge à Cisco TMS.

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Guide de configuration hybride des salles de téléconférence de Cisco Collaboration (CMR) (TMS 15.0 - WebEx Meeting Center WBS30)