Renouvellement de certificat TMS WebEx SSO - Cisco

Contenu

Introduction

Ce document décrit la procédure de renouvellement d'un certificat Webex SSO sur TMS lorsque TMS est en configuration Webex Hybrid avec SSO.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- TMS (Cisco TelePresence Management Suite)
- Webex SSO (authentification unique)
- Configuration hybride des salles de réunion Cisco Collaboration (CMR)

Components Used

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

- TMS 15.0 et versions ultérieures

Les informations de ce document sont basées sur le Guide de configuration hybride des salles de réunion de collaboration Cisco (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 votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

L'article couvre un scénario dans lequel un certificat a déjà été renouvelé via le portail Web de l'Autorité de certification en cliquant sur le bouton Renouveler. La procédure de génération d'une nouvelle demande de signature de certificat n'est pas incluse dans ce document.

Vérifiez que vous avez accès au même serveur Windows qui a généré le CSR d'origine. Dans le cas où l'accès au serveur Windows n'est pas disponible, une nouvelle génération de certificat doit être suivie, conformément au guide de configuration.

Procédure de téléchargement du certificat renouvelé sur TMS

Importer le certificat

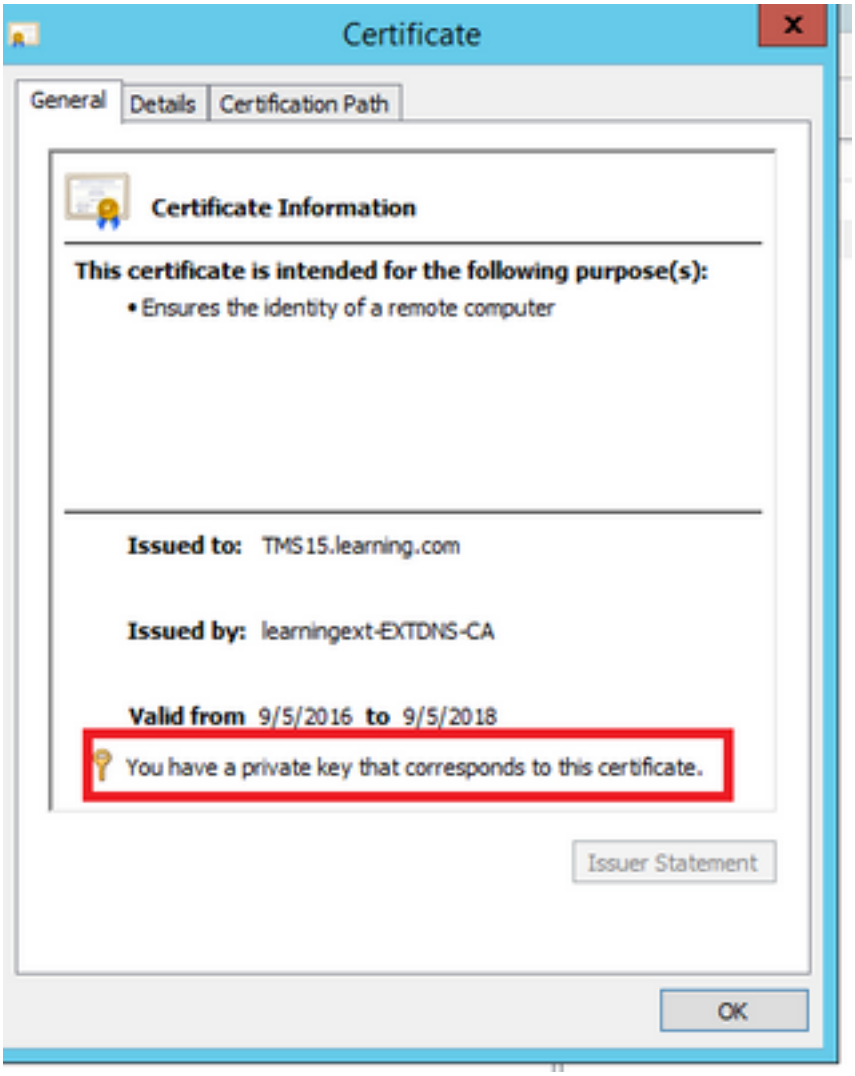
Afin d'importer le certificat renouvelé sur le même serveur Windows sur lequel le CSR d'origine a été généré, procédez comme suit.

Étape 1. Accédez à **Démarrer > Exécuter > mmc**. Cliquez sur **Fichier > Ajouter un composant logiciel enfichable > Ordinateur local** (l'utilisateur actuel peut être utilisé).

Étape 2. Cliquez sur **Action > Importer** et sélectionnez le certificat renouvelé. Sélectionnez **Magasin de certificats : Personnel** (choix différent si nécessaire).

Étape 3. Une fois le certificat importé, cliquez dessus avec le bouton droit de la souris et ouvrez-le.

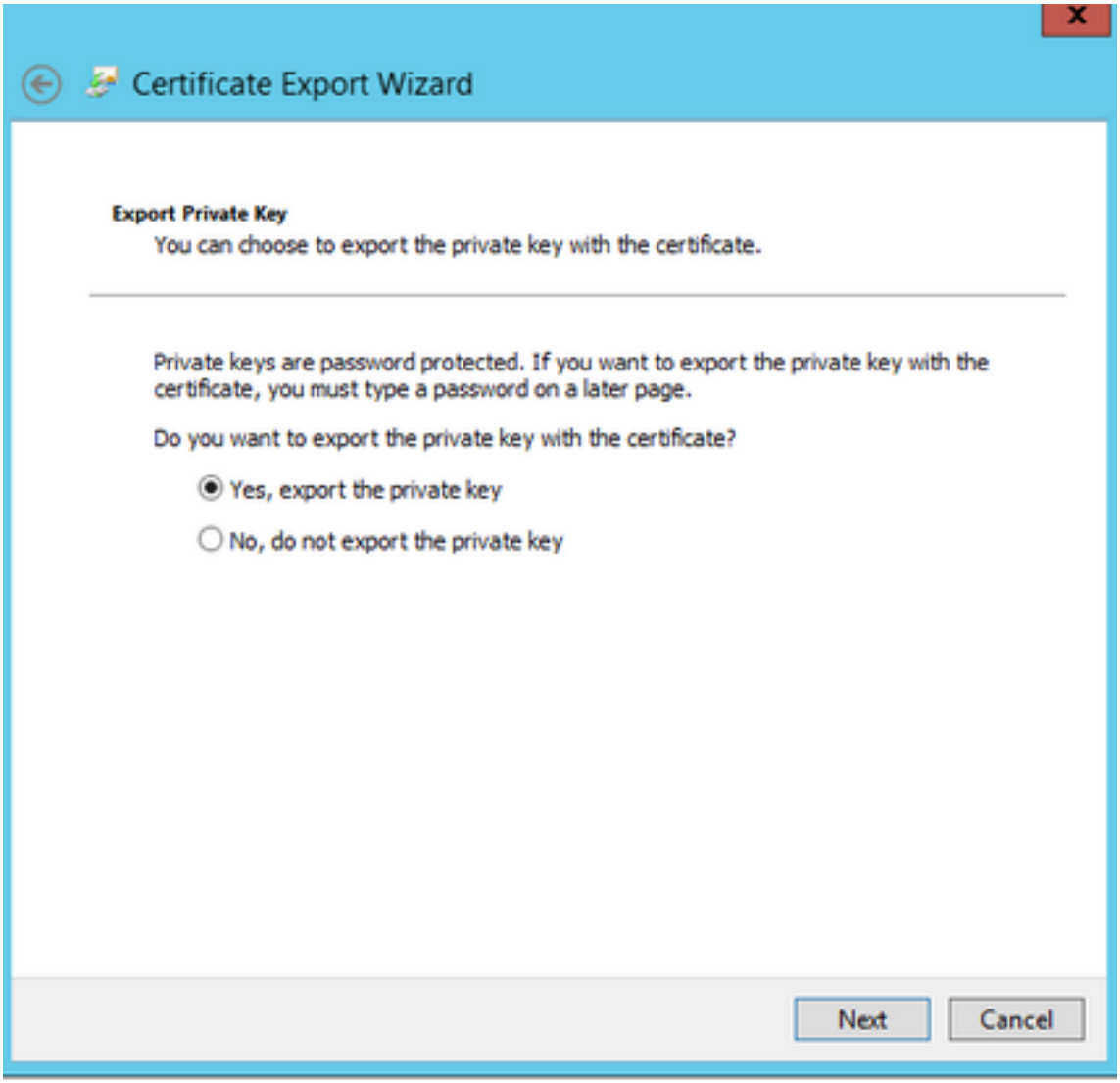
- Si le certificat a été renouvelé en fonction de la clé privée du même serveur, le certificat doit afficher : « Vous avez une clé privée qui correspond à ce certificat » comme dans l'exemple ci-dessous :

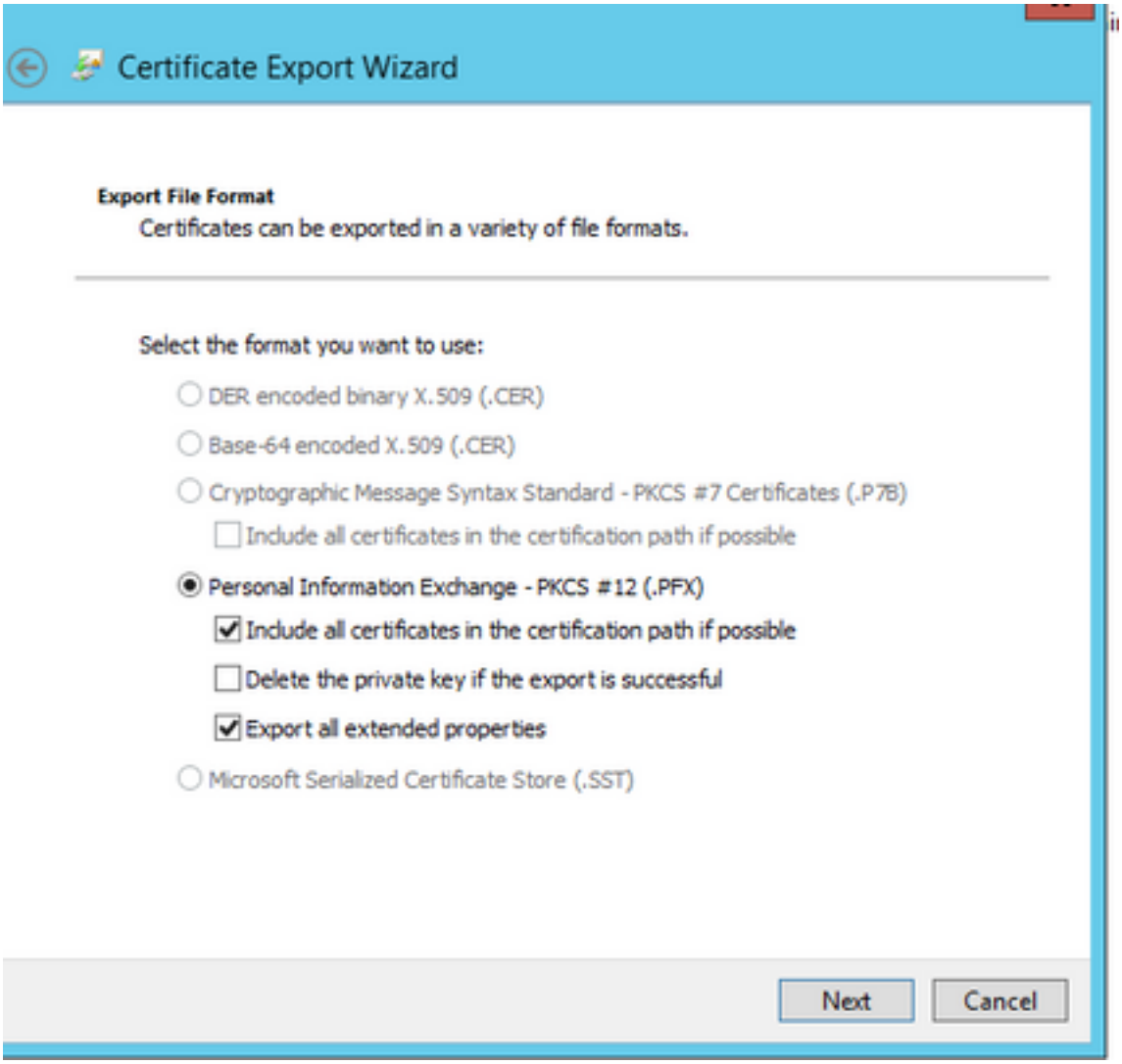


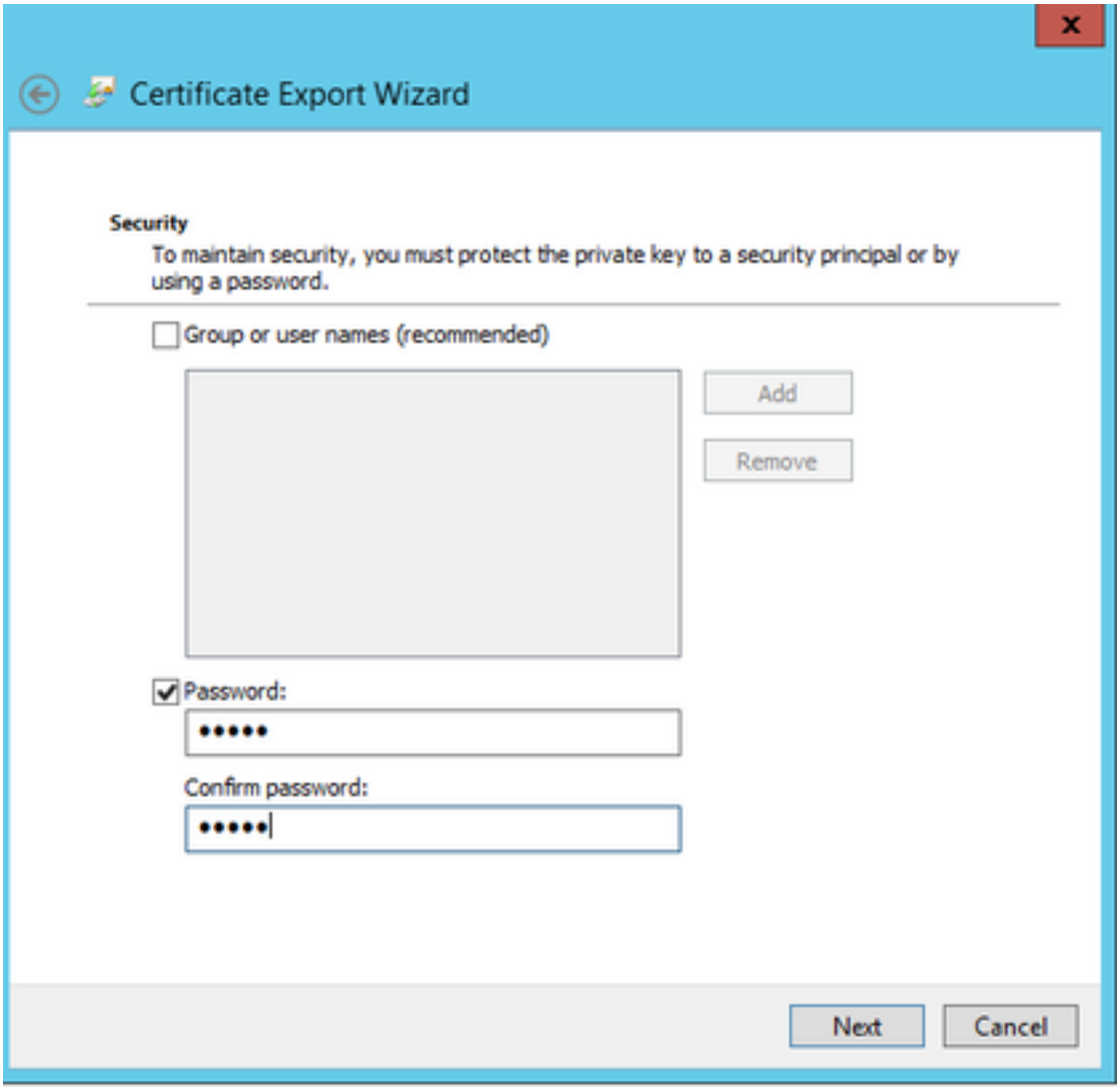
Exporter le certificat et le télécharger sur TMS

Pour exporter le certificat renouvelé avec sa clé privée, procédez comme suit.

Étape 1. À l'aide du composant logiciel enfichable **Gestionnaire de certificats Windows**, exportez la clé privée existante (paire de certificats) en tant que 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. À l'aide du **composant logiciel enfichable Gestionnaire de certificats Windows**, exportez le certificat existant sous la forme d'un fichier **.CER codé par PEM Base64**. Assurez-vous que l'extension de fichier est **.cer** ou **.crt** et fournissez ce fichier à l'équipe WebEx Cloud Services.

Étape 3. Connectez-vous à Cisco TMS et accédez à **Outils d'administration > Configuration > Paramètres WebEx**. Dans le volet Sites WebEx, vérifiez tous les paramètres, y compris SSO.

Étape 4. Cliquez sur **Parcourir** et téléchargez le certificat de clé privée **PKS #12** (.pfx) que vous avez généré lors de **Génération d'un certificat pour WebEx**. Complétez les autres champs de configuration SSO en utilisant le mot de passe et les autres informations que vous avez sélectionnées lors de la génération du certificat. Click **Save**.

Dans le cas où la clé privée est disponible exclusivement, vous pouvez combiner le certificat signé au format .pem avec la clé privée à l'aide de la commande OpenSSL suivante :

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

Vous devez maintenant avoir un certificat Cisco TMS qui contient la clé privée pour la configuration SSO à télécharger sur Cisco TMS.

Dépannage

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

Informations connexes

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