Renouvellement du certificat SSO TMS WebEx - Cisco

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Procédure de téléchargement du certificat renouvelé sur TMS

- Importer le certificat
- Exporter le certificat et le télécharger sur TMS

Dépannage

Informations connexes

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

Exigences

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)

Composants utilisés

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 contenues dans ce document sont basées sur le Guide de configuration hybride des salles de réunion 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 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 que celui qui a généré le CSR d'origine. Dans le cas où l'accès au serveur Windows particulier 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

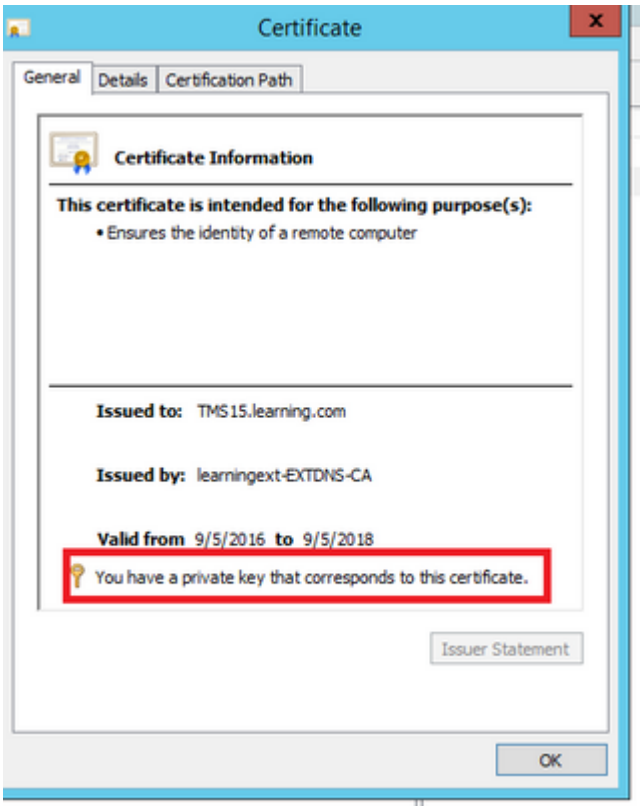
Afin d'importer le certificat renouvelé sur le même serveur Windows où le CSR d'origine a été généré, effectuez les étapes suivantes.

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 > Import et sélectionnez le certificat renouvelé. Sélectionner le magasin de certificats : Personnel (choisissez différent si nécessaire).

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

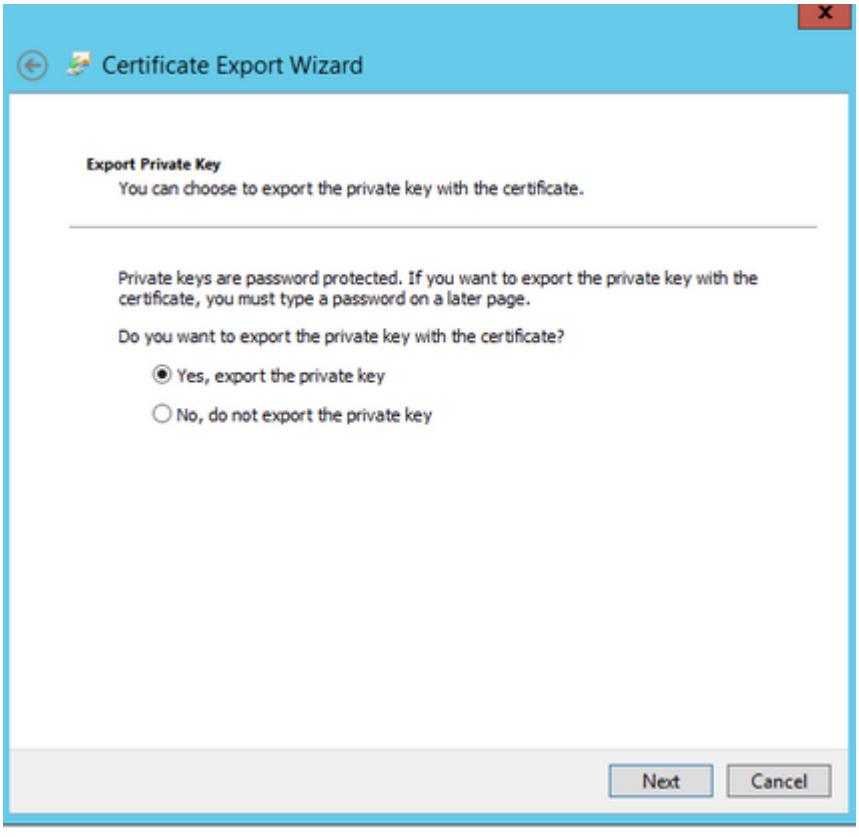
- Si le certificat a été renouvelé sur la base de la clé privée du même serveur, le certificat doit afficher : "Vous avez une clé privée qui correspond à ce certificat" comme dans l'exemple ci-dessous :

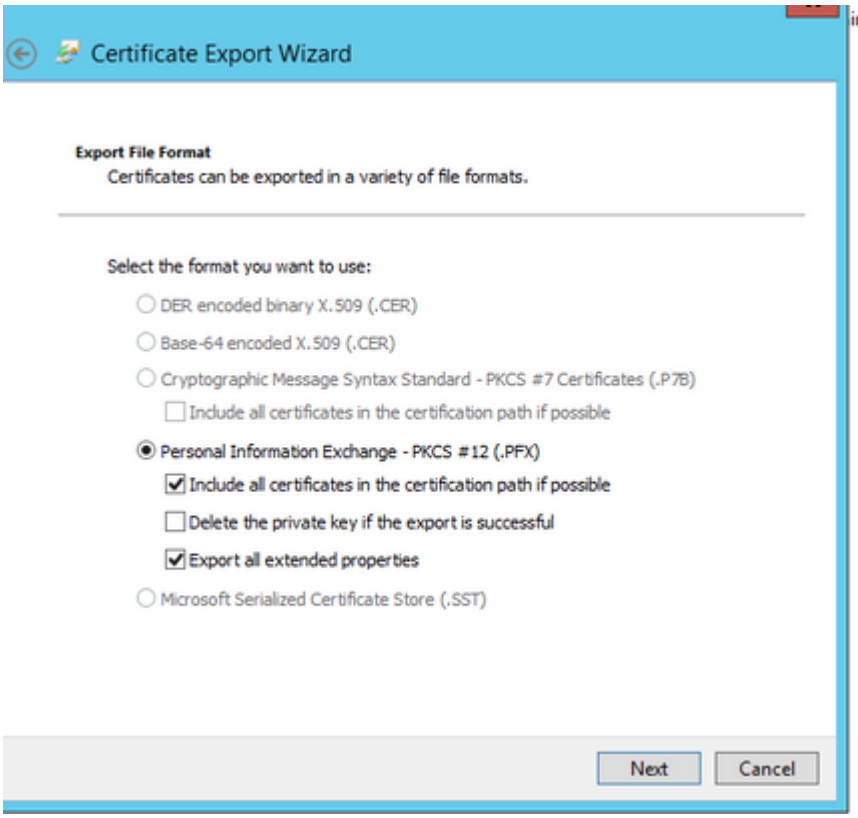


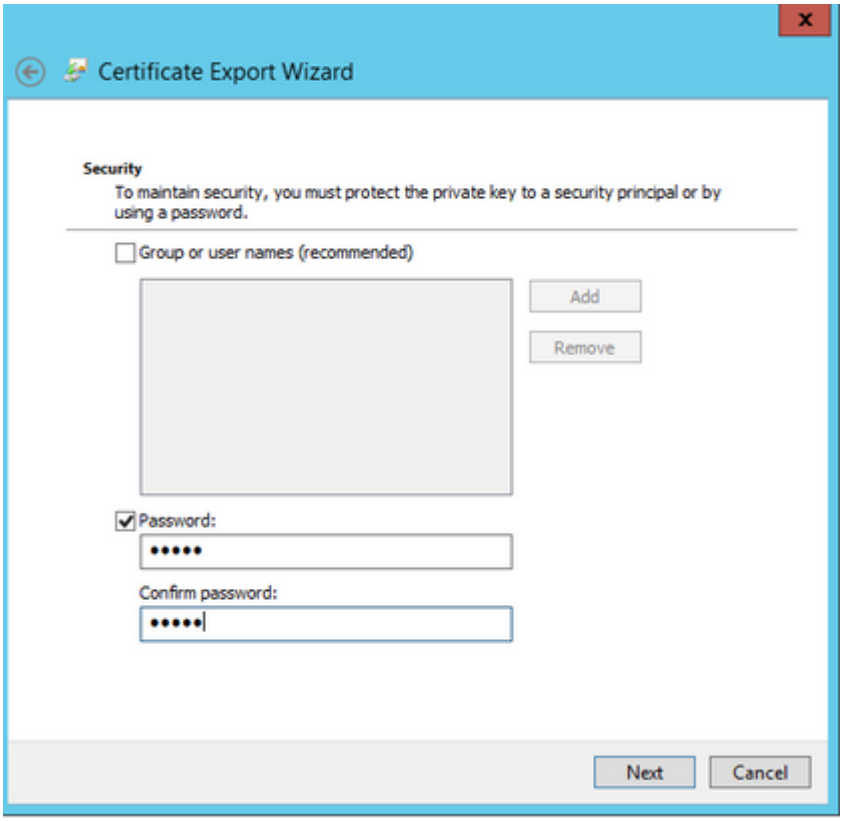
Exporter le certificat et le télécharger sur TMS

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

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 :







Étape 2. À l’aide du composant logiciel enfichable Gestionnaire de certificats Windows, exportez le certificat existant en tant que fichier .CER codé 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 Browse et téléchargez le certificat de clé privée (.pfx) PKS n° 12 que vous avez généré lors de la génération d'un certificat pour WebEx. Renseignez 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. Cliquez sur 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 vers Cisco TMS.

Dépannage

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

Informations connexes

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

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.