TMS WebEx SSO証明書の更新：シスコ

内容

概要

このドキュメントでは、TMSがSSOを使用したWebexハイブリッド設定のときにTMSでWebex SSO証明書を更新する手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- TMS(Cisco TelePresence Management Suite)
- Webex SSO（シングルサインオン）
- Cisco Collaboration Meeting Rooms(CMR)ハイブリッド設定

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- TMS 15.0以降

このドキュメントの情報は、『Cisco Collaboration Meeting Rooms(CMR)Hybrid Configuration Guide(TMS 15.0 - WebEx Meeting Center WBS30)』に基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

この記事では、[Renew]ボタンをクリックして、CA Webポータル経由で証明書がすでに更新されているシナリオについて説明します。新しいCSR（証明書署名要求）を生成する手順は、このドキュメントには含まれていません。

元のCSRを生成した同じWindowsサーバにアクセスできることを確認します。特定のWindowsサーバにアクセスできない場合は、構成ガイドに従って新しい証明書を生成する必要があります。

更新された証明書をTMSにアップロードする手順

証明書のインポート

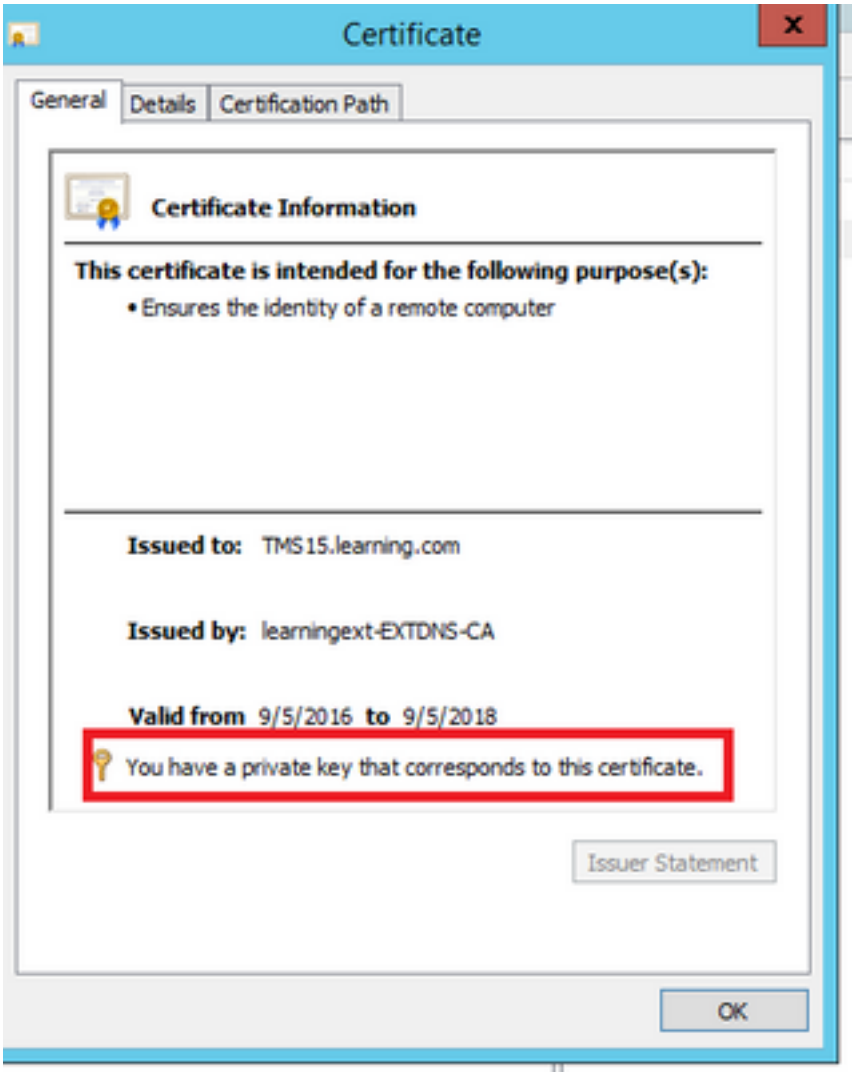
元のCSRが生成された同じWindowsサーバで更新された証明書をインポートするには、次の手順を実行します。

ステップ1:[Start] > [Run] > [mmc]**の順に移動します**。[File] > [Add Snap-in] > [Local Computer]**をクリックします(現在のユーザー**を使用できます)。

ステップ2:[Action] > [Import]をクリ**ックし、更新さ**れた証明書を選択します。証明書スト**アの選択：個人**（必要に応じて異なる項目を選択）。

ステップ3：証明書がインポートされたら、右クリックして証明書を開きます。

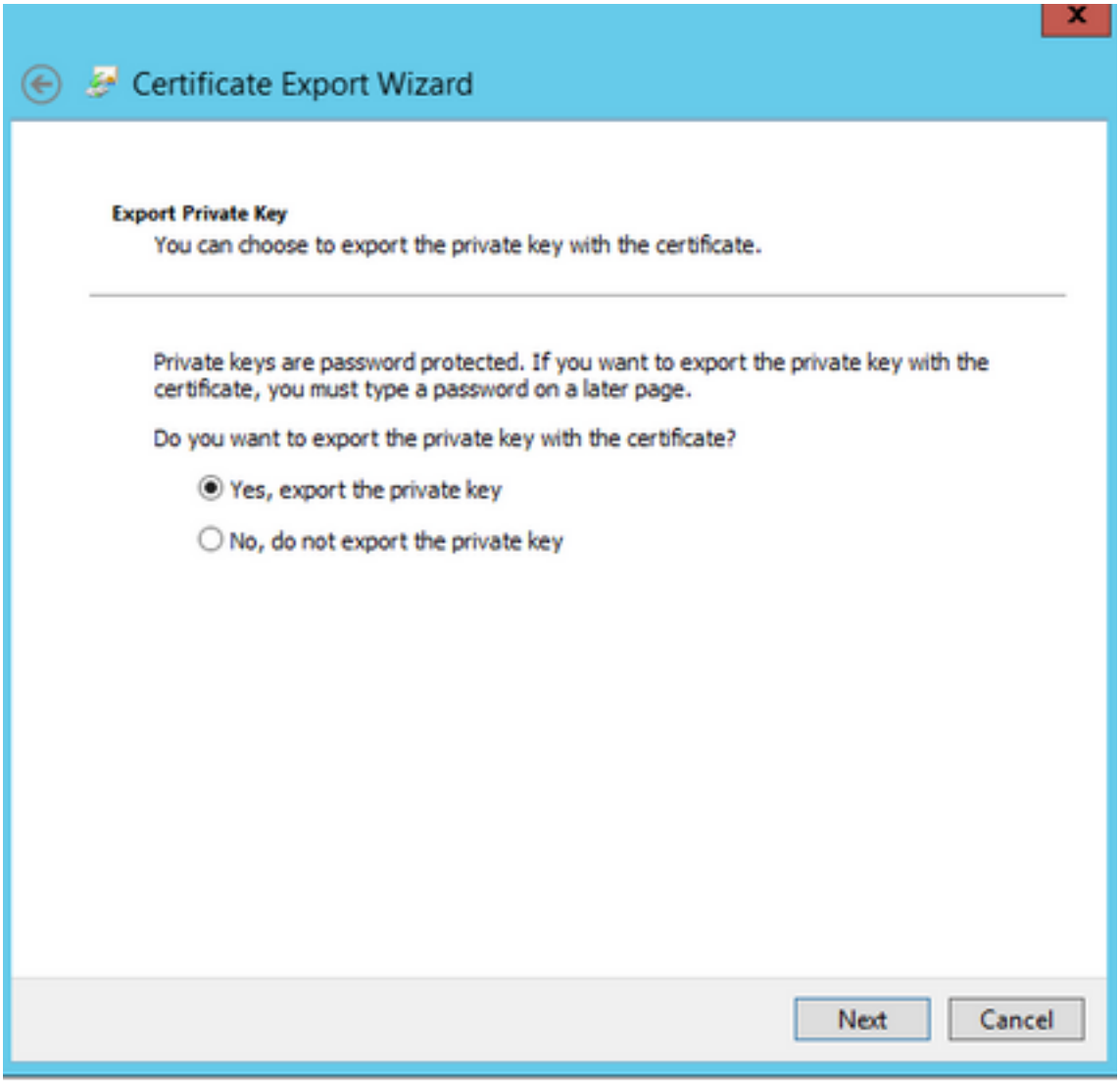
- 同じサーバの秘密キーに基づいて証明書が更新された場合、証明書には次のように表示されます。次の例のように、「この証明書に対応する秘密キーがあります。」

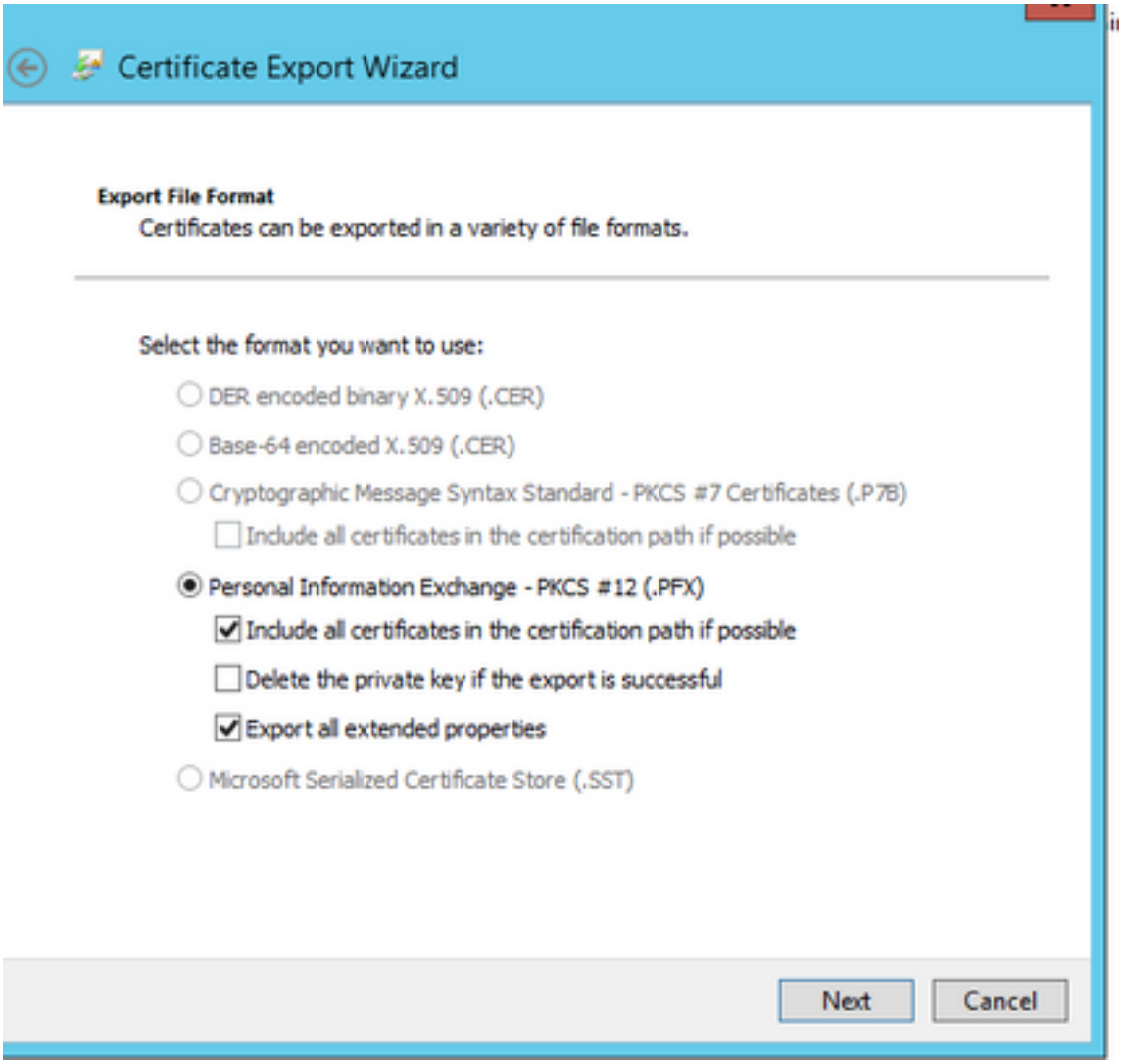


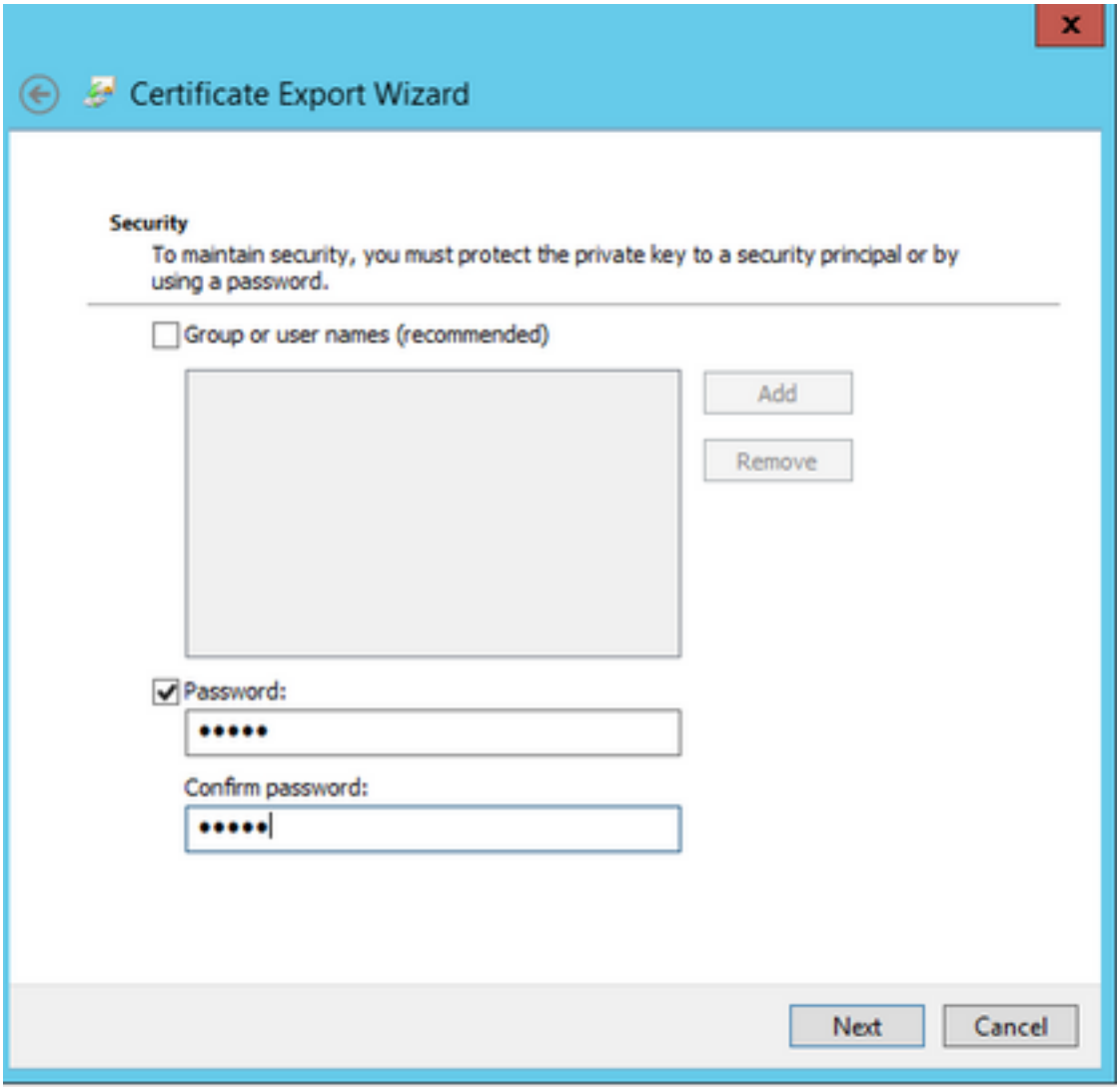
証明書をエクスポートし、TMSにアップロードします

更新された証明書を秘密キーとともにエクスポートするには、次の手順を実行します。

ステップ1:**Windows証明書マネージャースナップインを使用して**、既存の秘密キー（証明書ペア）を**PKCS#12ファイルとしてエクスポート**します。


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



ステップ2:**Windows証明書マネージャースナップインを使用して**、既存の証明書を**Base64 PEMエンコードされた.CERファイルとしてエクスポート**します。ファイル拡張子が.cerまたは.crtであることを確認し、このファイルをWebEx Cloud Servicesチームに提供してください。

ステップ3:Cisco TMSにログインし、[管理ツール(**Administrative Tools)] > [設定(Configuration)] > [WebEx設定(WebEx Settings)]に移動します。WebExサイトペインで、SSOを含むすべての設定を確認します。**

ステップ4:[Browse]をクリックし、[**Generating a Certificate for WebEx**]で生成した**PKS 12秘密キー証明書(.pfx)をアップロードします**。証明書の生成時に選択したパスワードとその他の情報を使用して、SSO設定の残りのフィールドに入力します。[Save] をクリックします。

秘密キーが排他的に使用できる場合は、次のOpenSSLコマンドを使用して、.pem形式の署名付き証明書と秘密キーを組み合わせることができます。

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

これで、Cisco TMSにアップロードするSSO構成の秘密キーを含むCisco TMS証明書が作成されます。

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- Cisco Collaboration Meeting Rooms(CMR)ハイブリッド設定ガイド(TMS 15.0 - WebEx Meeting Center WBS30)