TMS WebEx SSO 認証 更新- Cisco

目次

概要

この資料は TMS が SSO の WebEx ハイブリッド設定にあるとき TMS の WebEx SSO 認証を更新するためにプロシージャを記述したものです。

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（TMS））
- WebEx SSO（単一 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くものです。

- TMS 15.0 以上に

この文書に記載されている情報は Cisco Collaboration Meeting Rooms（CMR）ハイブリッド設定 ガイド（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たものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 対象のネットワークが実稼働中である場合には、どのような作業についても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

記事は認証が CA ウェブ ポータルによって Renew ボタンのクリックによって既に更新されてしまったシナリオをカバーします。 新しい CSR （証明書署名要求）を生成するプロシージャはこの資料に含まれていません。

オリジナル 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て下さい。 ケースでは特定のウィンドウ サーバへのアクセスが利用できないとき、新しい認証 生成はコンフィギュレーション ガイドによって、続かれなければなりません。

TMS の更新された認証をアップロードするプロシージャ

認証をインポートして下さい

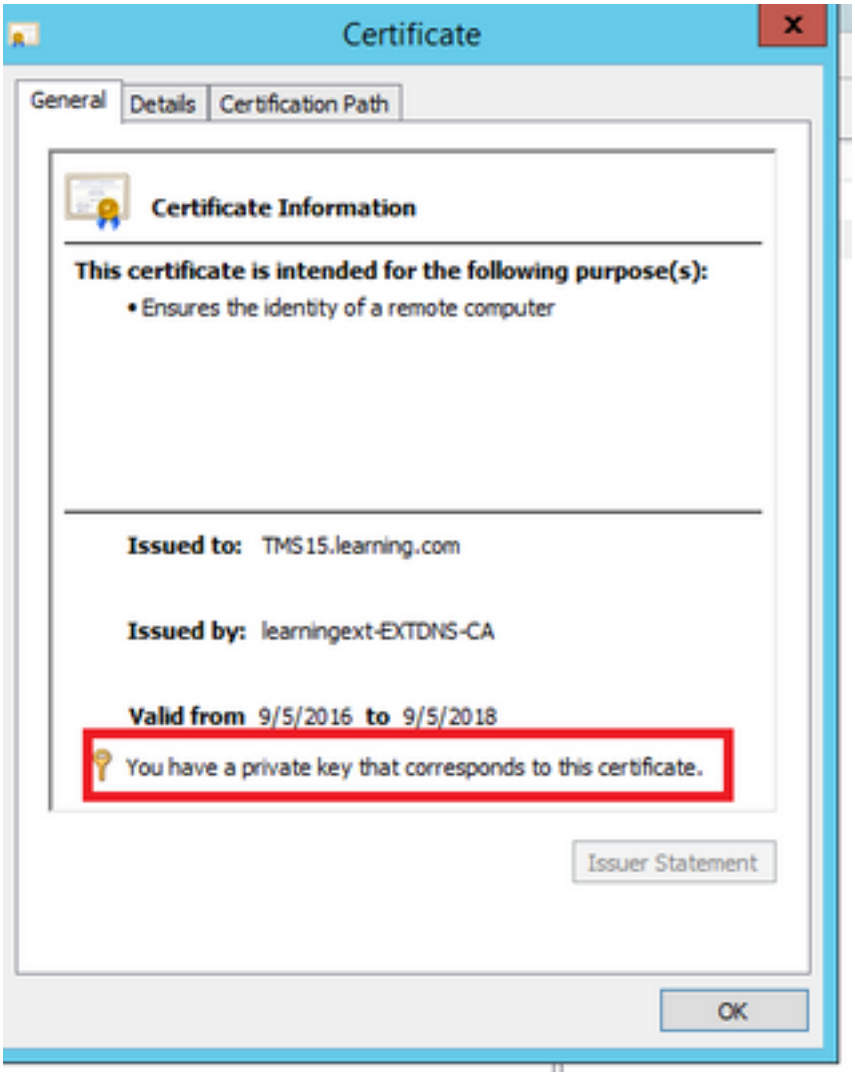
オリジナル CSR が生成された同じ Windows サーバの更新された認証をインポートするために、次のステップを実行して下さい。

ステップ 1. **Start > Run > mmc** へのナビゲート。 **スナップ式 > Add を > ローカル コンピュータ**『File』 をクリック して下さい（現在のユーザは使用することができます）。

ステップ 2. **> インポート**『Action』 をクリック し、更新された認証を選択して下さい。 **ストアを**『Certificate』 を選択 して下さい: **個人的**（別を必要であれば選択しました）。

ステップ 3 認証がインポートされたら、それを右クリックし、認証を開いて下さい。

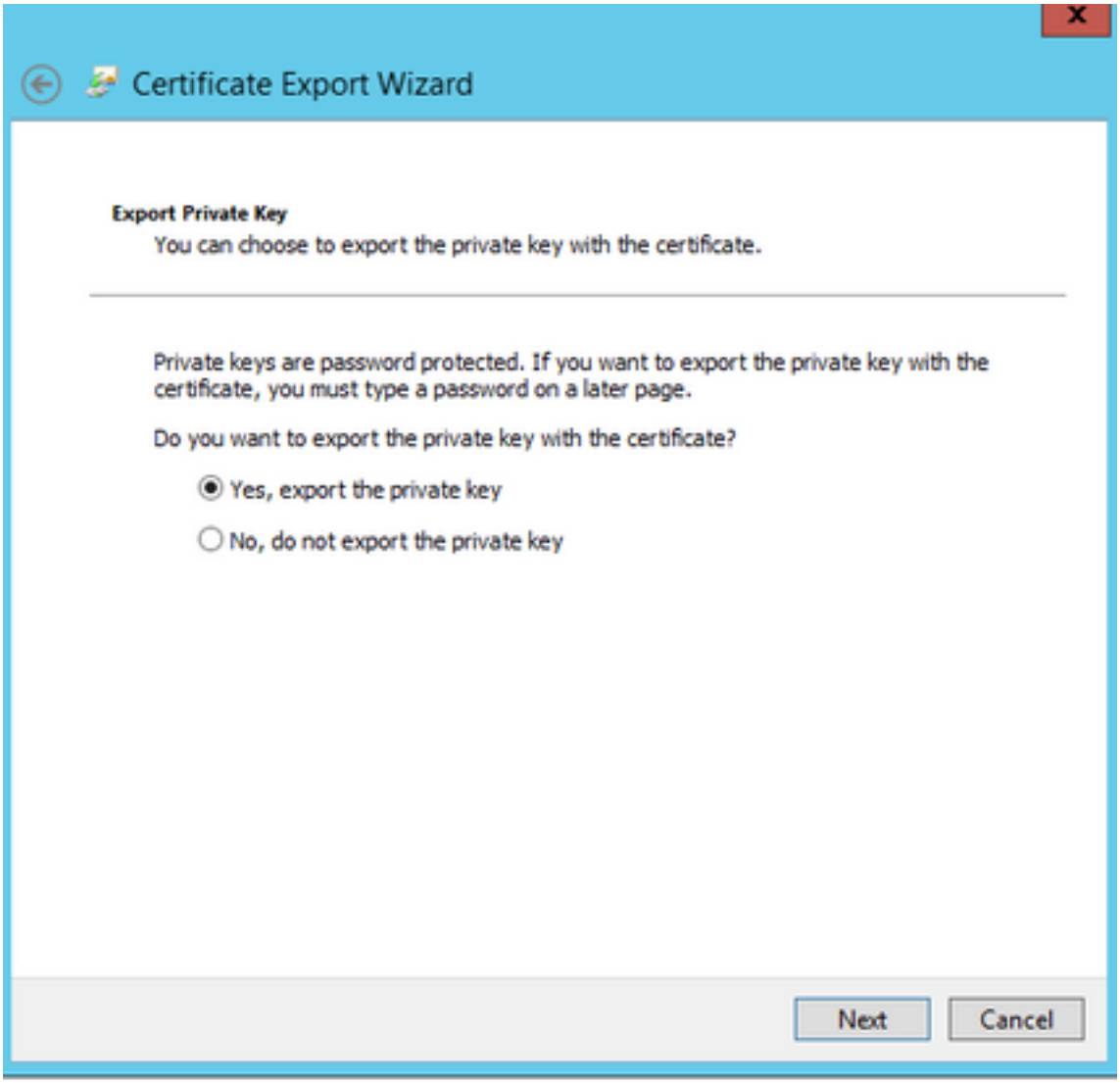
- 認証が同じサーバのプライベートキーに基づいていたら、認証下記のものを表示すれば更新されたら:「この認証に」次 下記の例対応するプライベートキーがあります:

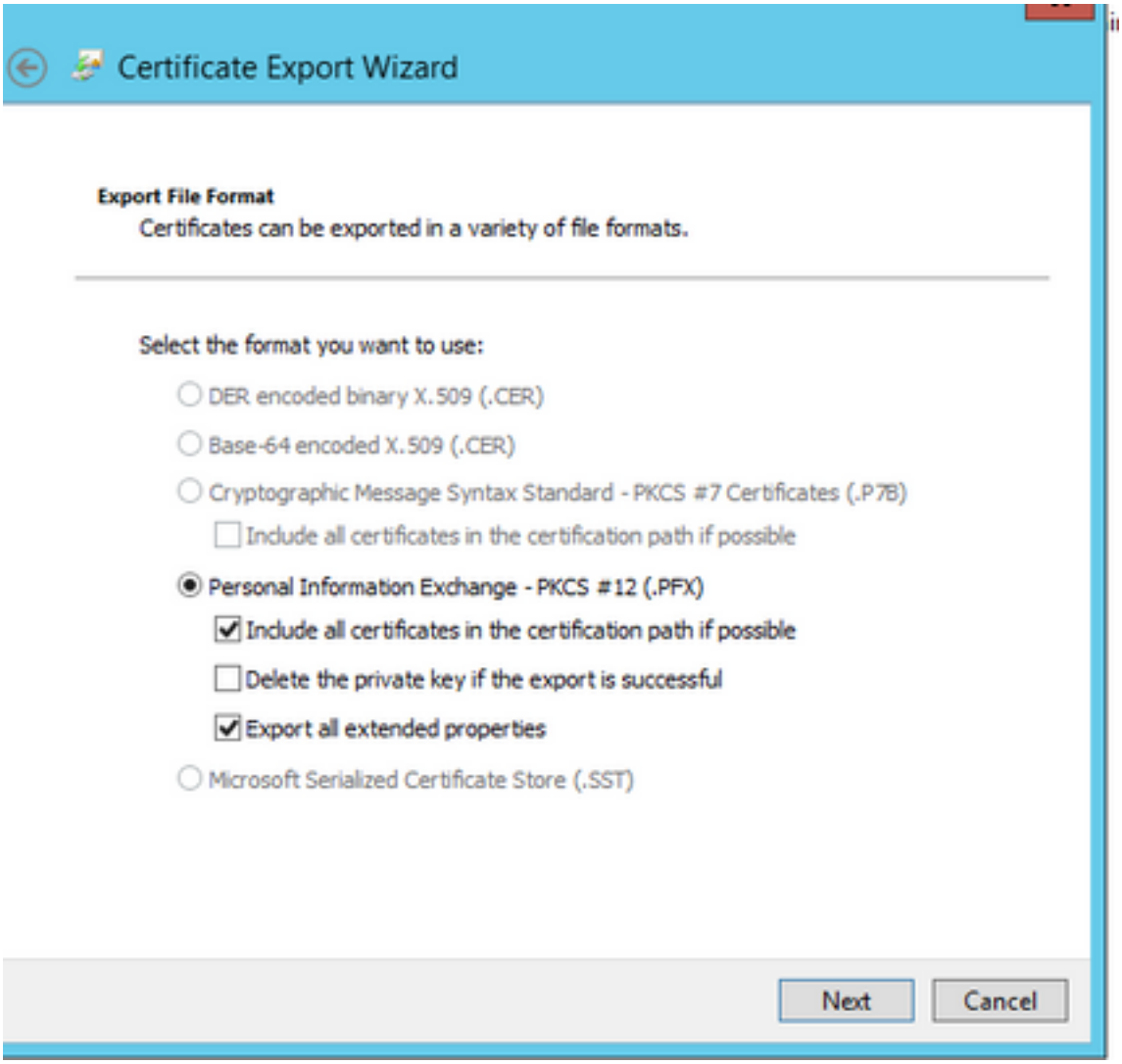


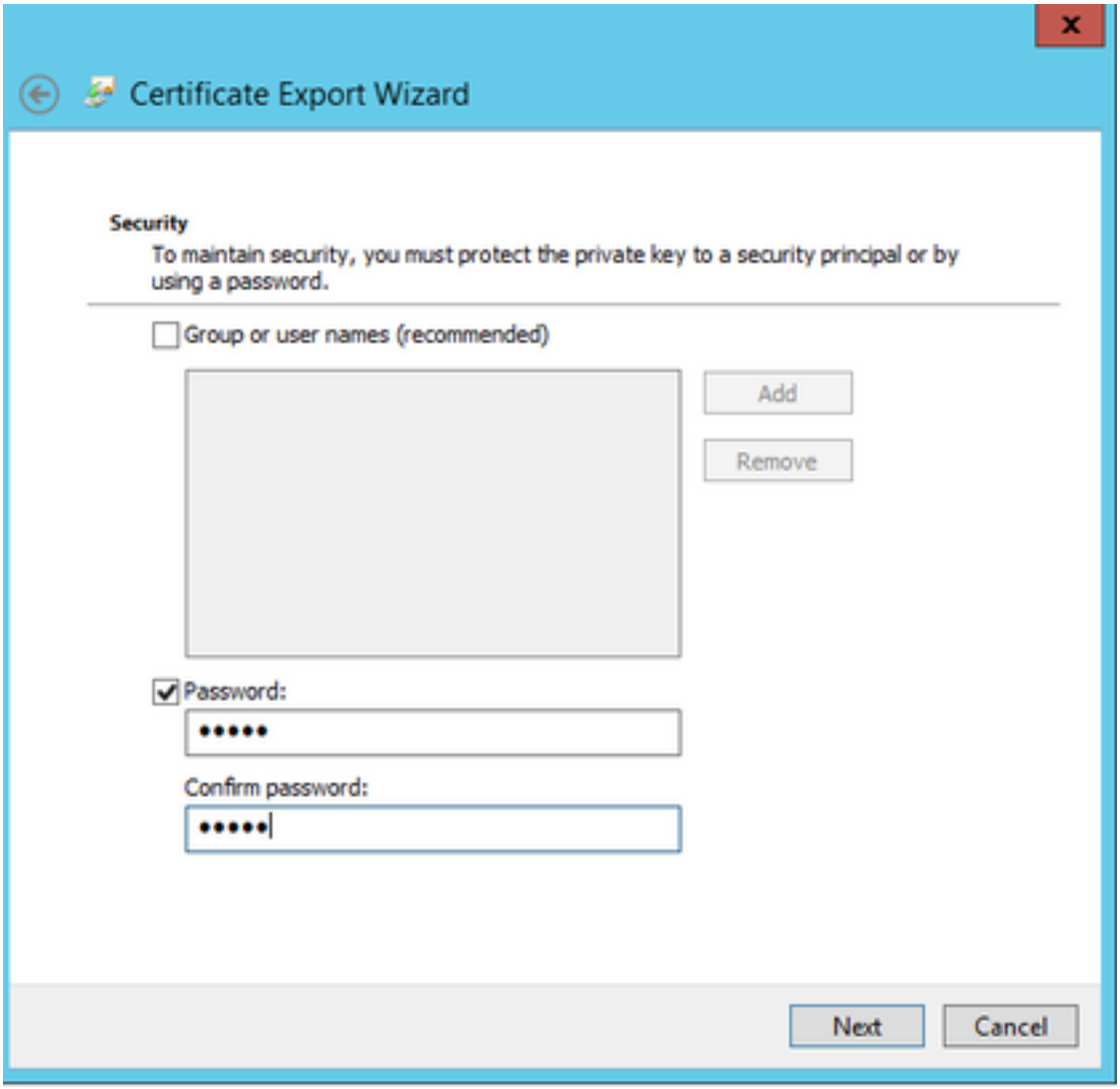
認証をエクスポートし、TMS でアップロードして下さい

更新された認証をプライベートキーと共にエクスポートするために、次のステップを実行して下さい。

ステップ 1： **Windows 認証マネージャ スナップイン**を使用する、既存のプライベートキー（認証ペア）をように **PKCS#12** ファイル エクスポートして下さい:


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



呼び出します。 **Windows 認証マネージャ スナップイン**を使用する、**Base64 PEM によって符号化される .CER** ファイルとして既存 の 認証をエクスポートして下さい。 ファイル拡張子が **.cer** または **.crt** である確認し、WebEx クラウド サービス チームにこのファイルをことを提供して下さい。

ステップ 3. Cisco TMS にログイン し、**管理ツール > 設定 > WebEx 設定**にナビゲート して下さい。 WebEx サイト ペインで、SSO を含む設定すべてを確認して下さい。

ステップ 4. **WebEx のための認証の生成**で生成した **PKS #12** プライベートキー 認証 (.pfx) を『Browse』 をクリック し、アップ ロードして下さい。 選択した他の情報およびパスワードを使用して SSO 設定フィールドの残りに入力して下さい認証を生成した場合。 [Save] をクリックします。

ケースではプライベートキーが専ら利用できるとき、OpenSSL 次のコマンドを使用してプライベートキーと .pem 形式の署名入り認証を結合できます:

openssl pkcs12 -エクスポート- inkey tms-privatekey.pem - tms-cert.pem で- tms-cert-key.p12 -ネーム tms 証明書キー

今 Cisco TMS にアップロードするために SSO 設定のためのプライベートキーが含まれている Cisco TMS 認証があるはずです。

トラブルシューティング

現在のところ、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）