TMS WebEx SSO证书续订-思科

目录

简介

当TMS在与SSO时的WebEx混合配置方面本文描述步骤更新在TMS的一WebEx SSO证书。

先决条件

要求

Cisco 建议您了解以下主题：

- TMS (思科网真管理套件)
- WebEx SSO (单一登录)
- 思科协作会议室(CMR)混合配置

使用的组件

本文档中的信息基于以下软件和硬件版本：

- TMS 15.0以上

本文档中的信息根据思科协作会议室(CMR)混合配置指南(TMS 15.0 - WebEx会议中心WBS30)。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络实际，请保证您了解所有命令潜在影响。

背景信息

条款包括证书通过CA Web门户已经被更新了通过单击在Renew按钮的方案。 生成新的CSR的步骤(证书签名请求)在本文没有包括。

保证您访问生成原始CSR的同一Windows服务器。 在案件中，当对特定的Windows服务器的访问不

是可用的时，新证书生成必须根据配置指南被跟随。

上传在TMS的更新的证书的步骤

导入证书

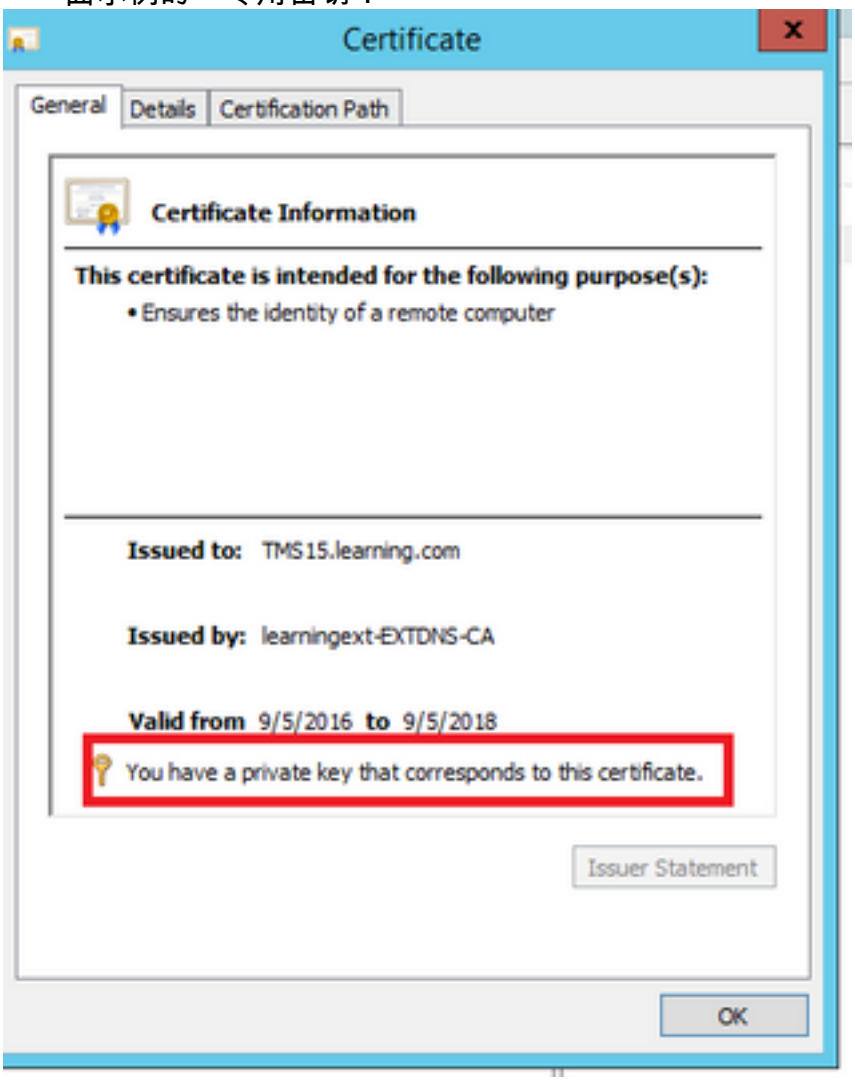
为了导入在原始CSR生成的同一Windows服务器的更新的证书，请执行以下步骤。

步骤1.导航对**Start > Run > mmc**。点击**File>添加管理单元>本地计算机**(可以使用当前用户)。

步骤2.点击**操作>导入**并且选择更新的证书。选择**证书存储：个人**(如果必须选择不同的)。

第三步：一旦证书导入，请用鼠标右键单击对此并且打开证书。

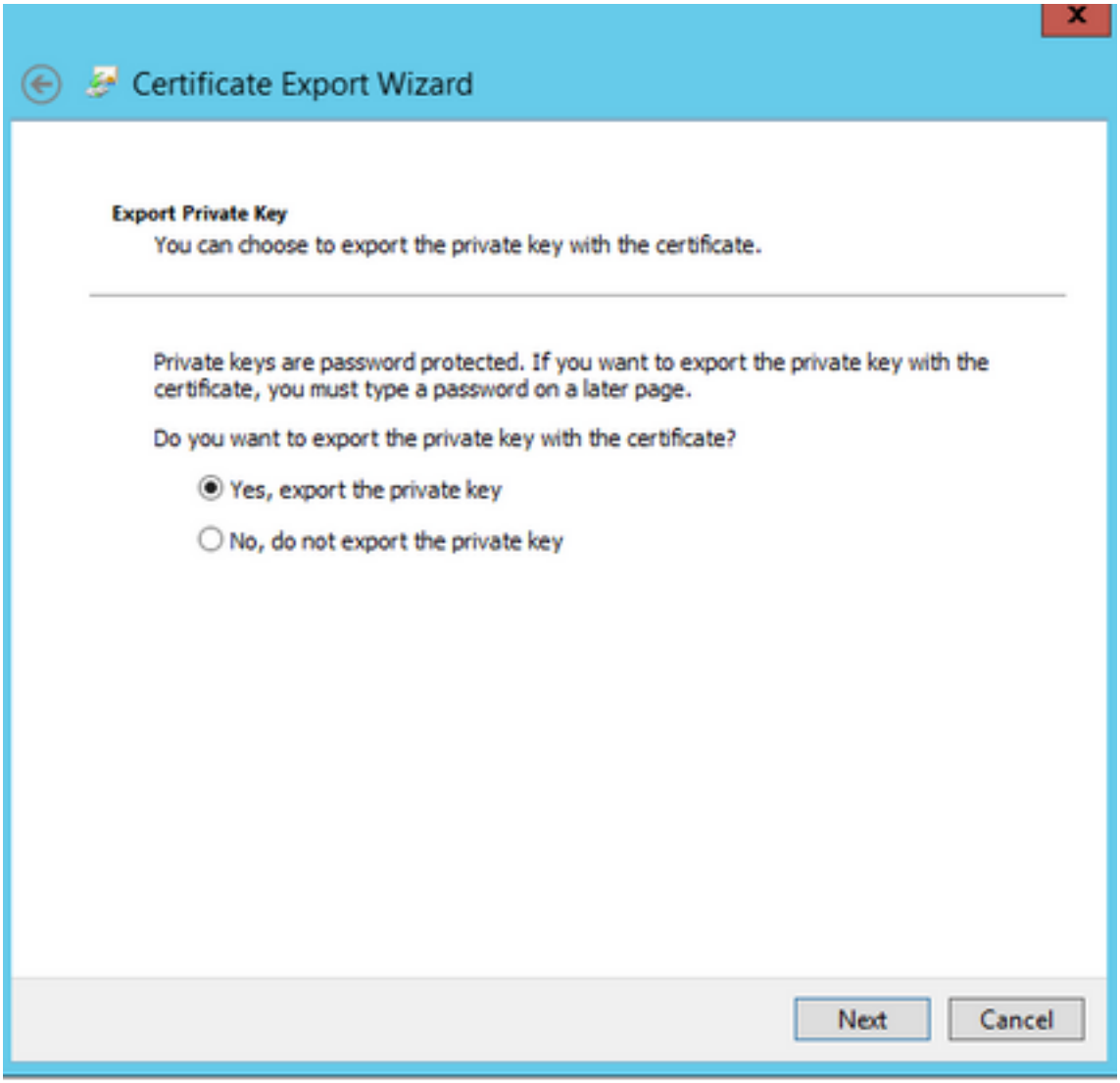
- 如果证书被更新了根据同一个服务器的专用密钥，证书应该显示："您有对应于此证书"正如在下面示例的一专用密钥：

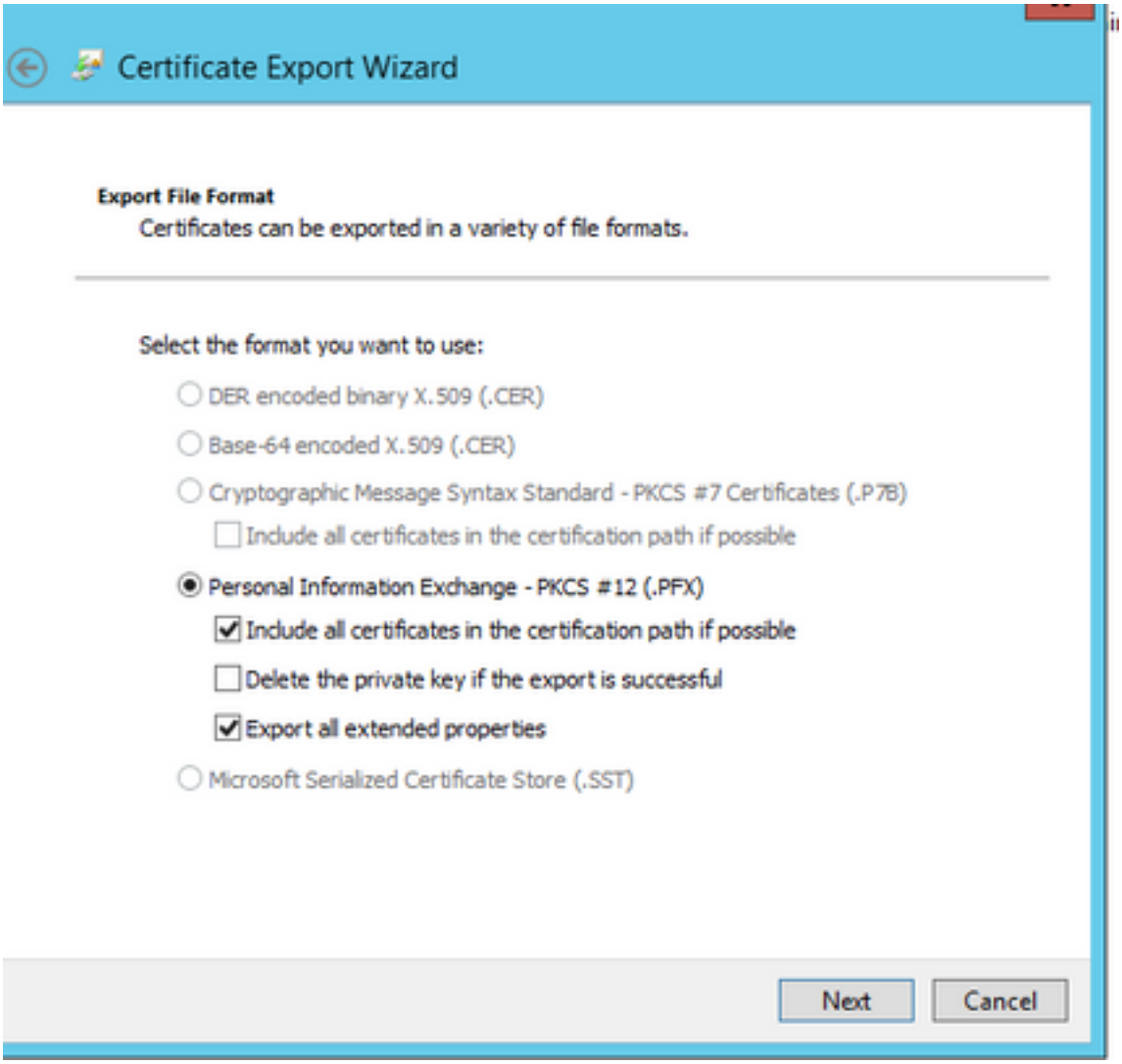


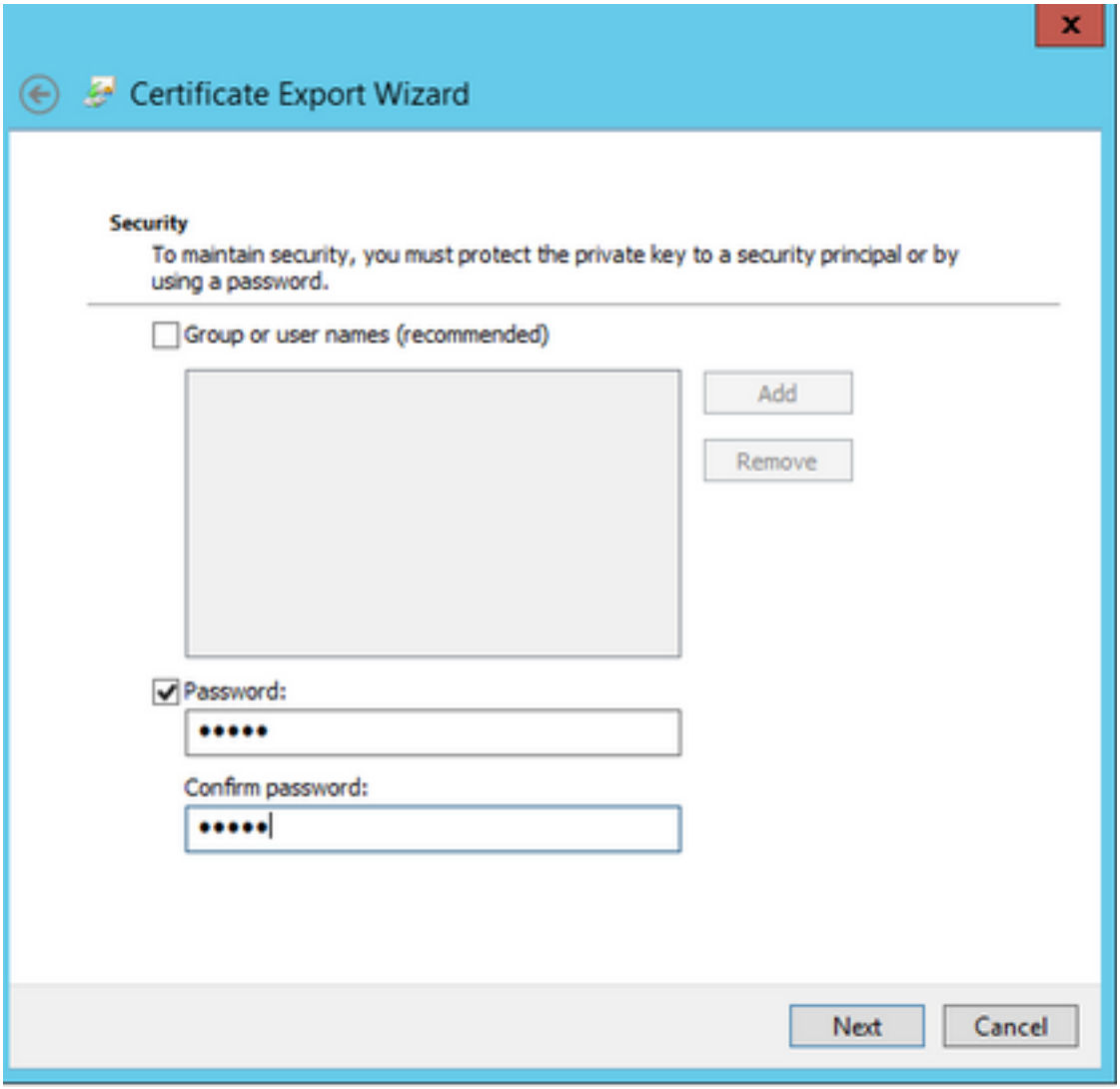
导出证书并且上传它在TMS

为了与其专用密钥一起导出更新的证书，请执行以下步骤。

步骤1:使用**Windows认证管理器管理单元**，请导出现有专用密钥(证书对)作为**PKCS-12**文件：


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



第二步： 使用**Windows认证管理器管理单元**，请导出现有的证书作为**Base64 PEM编码的.CER**文件。保证文件扩展是**.cer**或**.crt**并且提供此文件给WebEx Cloud服务团队。

步骤3.登录思科TMS，并且导航对**管理工具> Configuration> WebEx设置**。 在WebEx站点窗格，请验证所有设置包括SSO。

步骤4.点击**Browse**并且上传您生成在**生成WebEx的一证书的PKS #12**专用密钥证书(.pfx)。填入SSO配置字段的其余使用您选择，当生成证书时的密码和其他信息。单击 **Save**。

在案件中，当专用密钥完全时是可用的使用以下Openssl命令，您能与专用密钥结合在.pem格式的签名证书：

openssl pkcs12 -出口- inkey TMSprivatekey.pem -在TMScert.pem - tms-cert-key.p12 -命名TMS CERT KEY

您应该当前有包含SSO配置的专用密钥能上传到思科TMS的思科TMS证书。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- 思科协作会议室(CMR)混合配置指南(TMS 15.0 - WebEx会议中心WBS30)