Renovação de certificado SSO do TMS WebEx - Cisco

Contents

Introduction

Este documento descreve o procedimento para renovar um certificado SSO do Webex no TMS quando o TMS está na configuração do Webex Hybrid com SSO.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- TMS (Cisco TelePresence Management Suite)
- SSO do Webex (logon único)
- Configuração híbrida do Cisco Collaboration Meeting Rooms (CMR)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- TMS 15.0 e superior

As informações neste documento são baseadas no Guia de Configuração Híbrida do 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O artigo aborda um cenário em que um certificado já foi renovado via portal da CA clicando no botão de renovação. O procedimento para gerar um novo CSR (Certificate Signing Request) não está incluído neste documento.

Verifique se você tem acesso ao mesmo servidor Windows que gerou o CSR original. Se o acesso ao servidor Windows específico não estiver disponível, uma nova geração de certificado deve ser seguida, de acordo com o guia de configuração.

Procedimento para carregar o certificado renovado no TMS

Importar o certificado

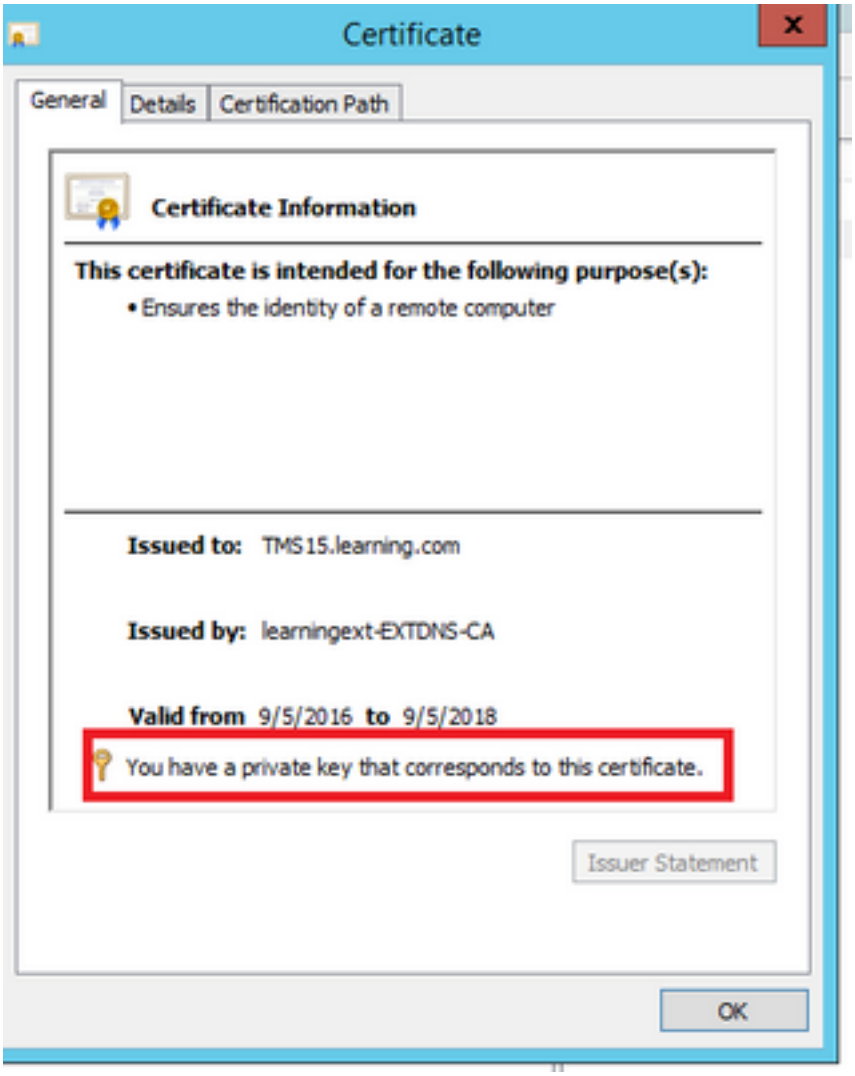
Para importar o certificado renovado no mesmo servidor Windows onde o CSR original foi gerado, execute as seguintes etapas.

Etapa 1. Navegue até **Iniciar > Executar > mmc**. Clique em **Arquivo > Adicionar Snap-in > Computador local** (o usuário atual pode ser usado).

Etapa 2. Clique em **Ação > Importar** e selecione o certificado renovado. Selecionar **Repositório de Certificados: Pessoal** (escolha diferente se necessário).

Etapa 3. Quando o certificado for importado, clique nele com o botão direito do mouse e abra o certificado.

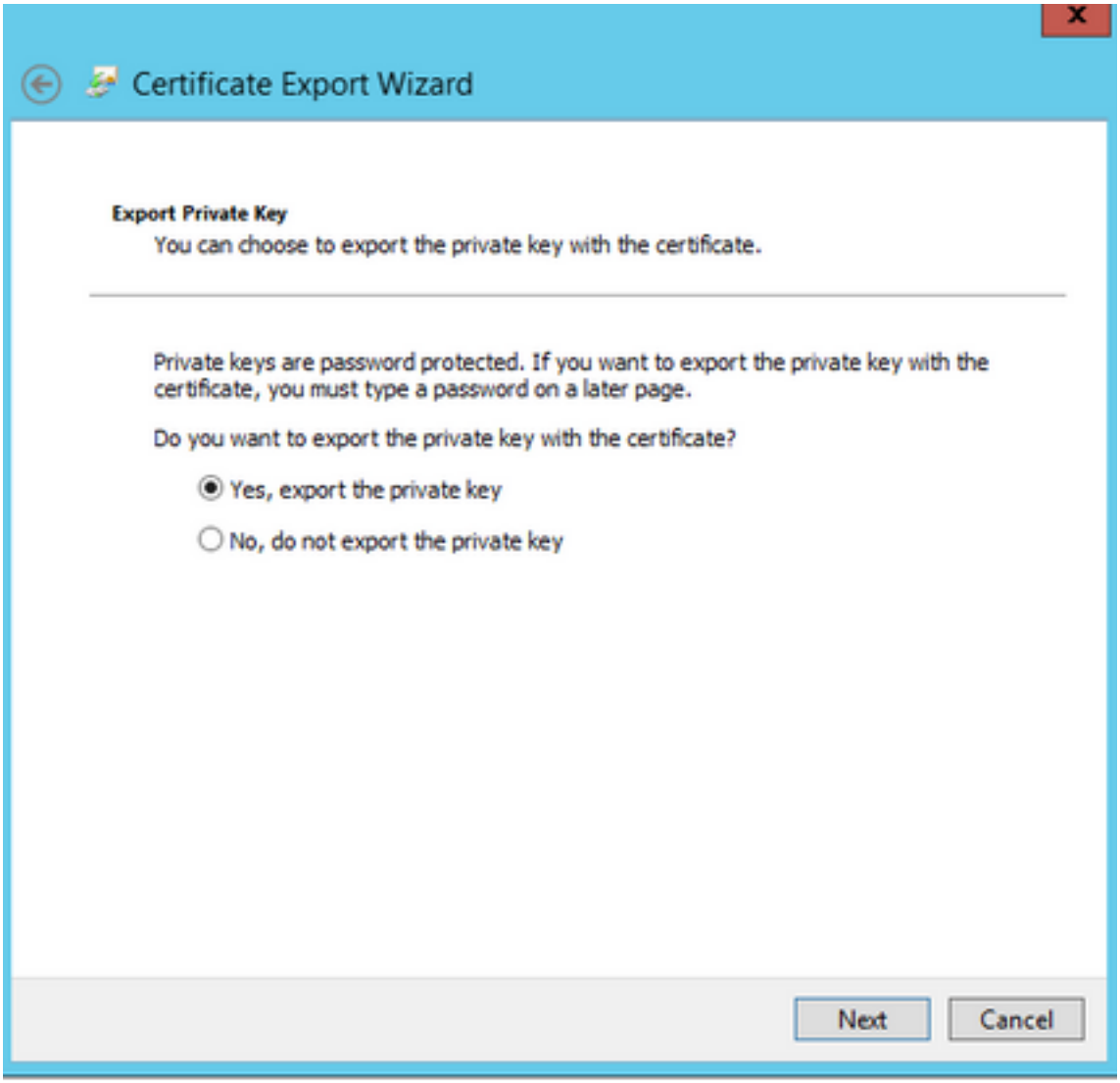
- Se o certificado tiver sido renovado com base na chave privada do mesmo servidor, o certificado deverá exibir: "Você tem uma chave privada que corresponde a este certificado", como no exemplo abaixo:

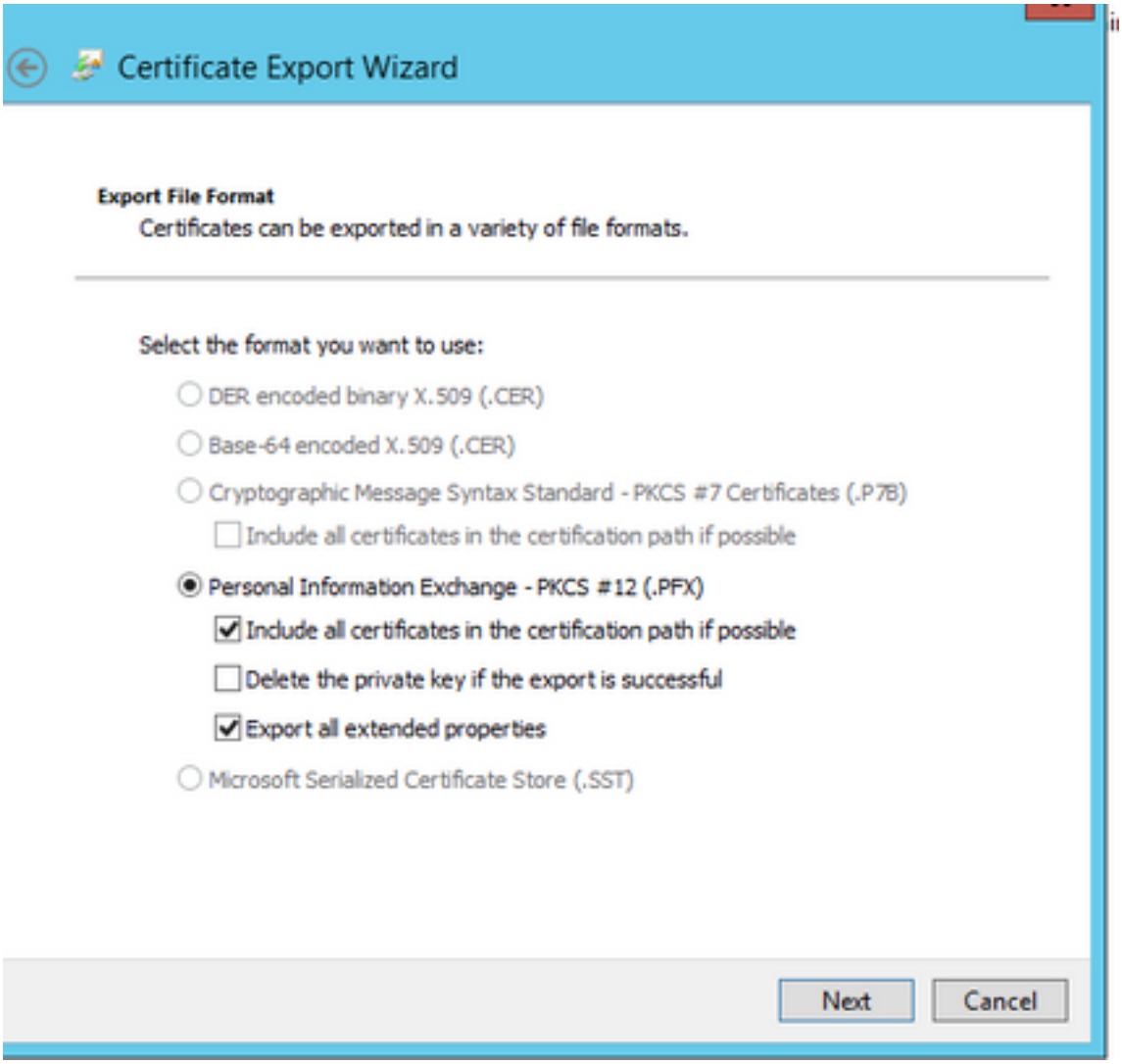


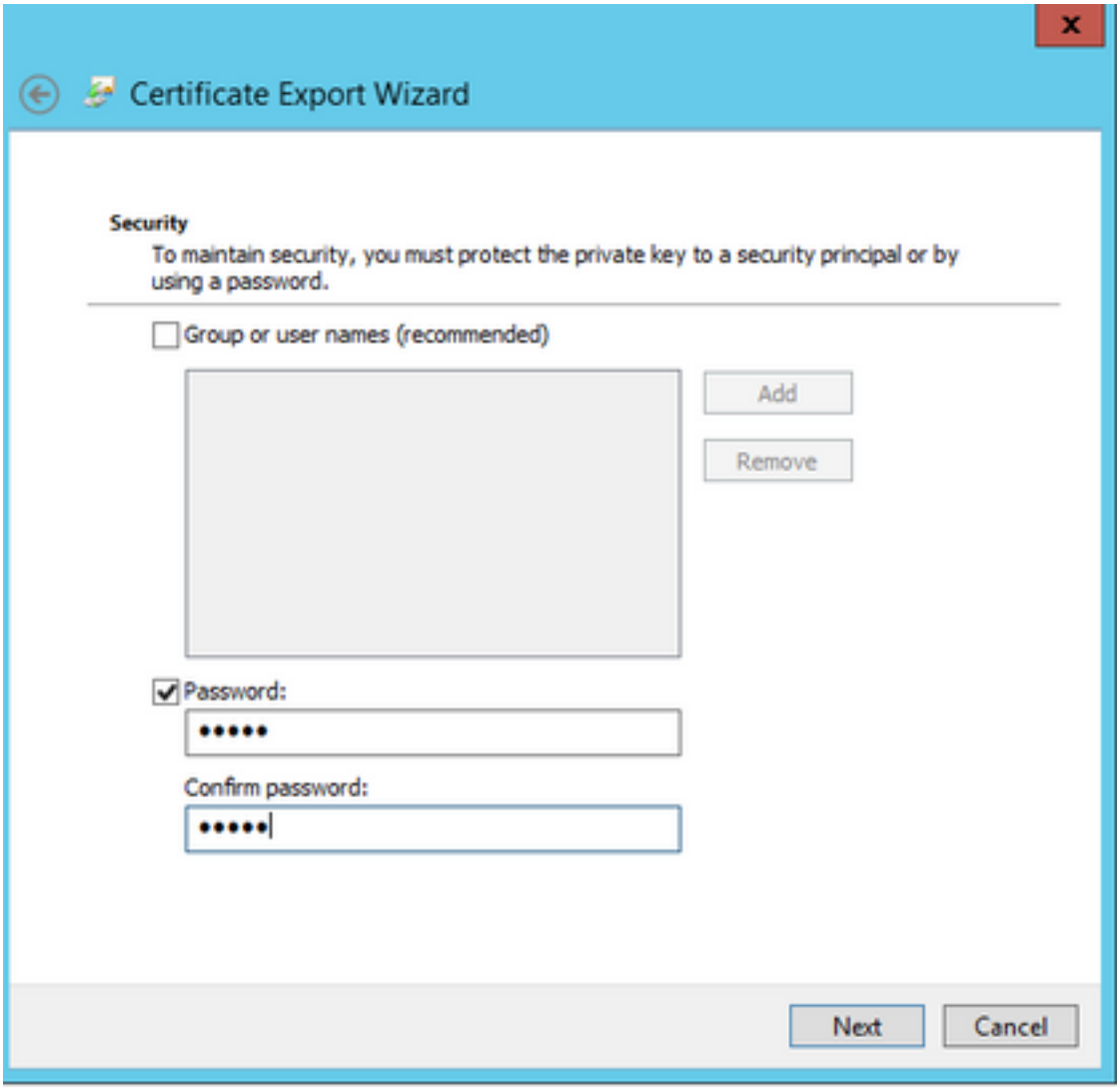
Exportar o certificado e carregá-lo no TMS

Para exportar o certificado renovado junto com sua chave privada, execute as seguintes etapas.

Etapa 1. Usando o **Snap-in do Windows Certificate Manager**, exporte a chave privada existente (par de certificados) como um arquivo **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



Etapa 2. Usando o **Snap-in do Windows Certificate Manager**, exporte o certificado existente como um arquivo **.CER codificado PEM Base64**. Certifique-se de que a extensão do arquivo seja **.cer** ou **.crt** e forneça esse arquivo à equipe de serviços em nuvem do WebEx.

Etapa 3. Faça login no Cisco TMS e navegue para **Administrative Tools > Configuration > WebEx Settings**. No painel WebEx Sites, verifique todas as configurações, incluindo SSO.

Etapa 4. Clique em **Procurar** e carregue o **PKS #12** certificado de chave privada (.pfx) gerado em **Geração de um certificado para WebEx**. Preencha o restante dos campos de configuração SSO usando a senha e outras informações selecionadas ao gerar o certificado. Click **Save**.

Se a chave privada estiver disponível exclusivamente, você poderá combinar o certificado assinado no formato .pem com a chave privada usando o seguinte comando OpenSSL:

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

Agora você deve ter um certificado Cisco TMS que contenha a chave privada para a configuração SSO a ser carregada para o Cisco TMS.

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta

configuração.

Informações Relacionadas

- Guia de configuração híbrida do Cisco Collaboration Meeting Rooms (CMR) (TMS 15.0 - WebEx Meeting Center WBS30)