Renovação do certificado do WebEx SSO TMS - Cisco

Índice

Introdução

Este documento descreve o procedimento para renovar um certificado do WebEx SSO em TMS quando TMS está na configuração híbrida do WebEx com SSO.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- TMS (suite de gerenciamento do Cisco TelePresence)
- WebEx SSO (escolha Sinal-em)
- Configuração híbrida das salas de reuniões da colaboração do Cisco (CMR)

Componentes Utilizados

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

- TMS 15.0 e acima

A informação neste documento é baseada no guia de configuração híbrida das salas de reuniões da colaboração do Cisco (CMR) (TMS 15.0 - centro WBS30 da reunião do WebEx).

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se sua rede está viva, assegure-se de que você compreenda o impacto potencial do comando any.

Informações de Apoio

O artigo cobre uma encenação em que um certificado tem sido renovado já através do portal da web de CA clicando no botão Renew Button. O procedimento para gerar um CSR novo (solicitação de assinatura de certificado) não é incluído neste documento.

Assegure-se de que você tenha o acesso ao mesmo Windows Server que gerou o CSR original. No caso quando o acesso ao Windows Server particular não está disponível, uma geração nova do certificado tem que ser seguida, conforme o manual de configuração.

Procedimento para transferir arquivos pela rede o certificado renovado em TMS

Importe o certificado

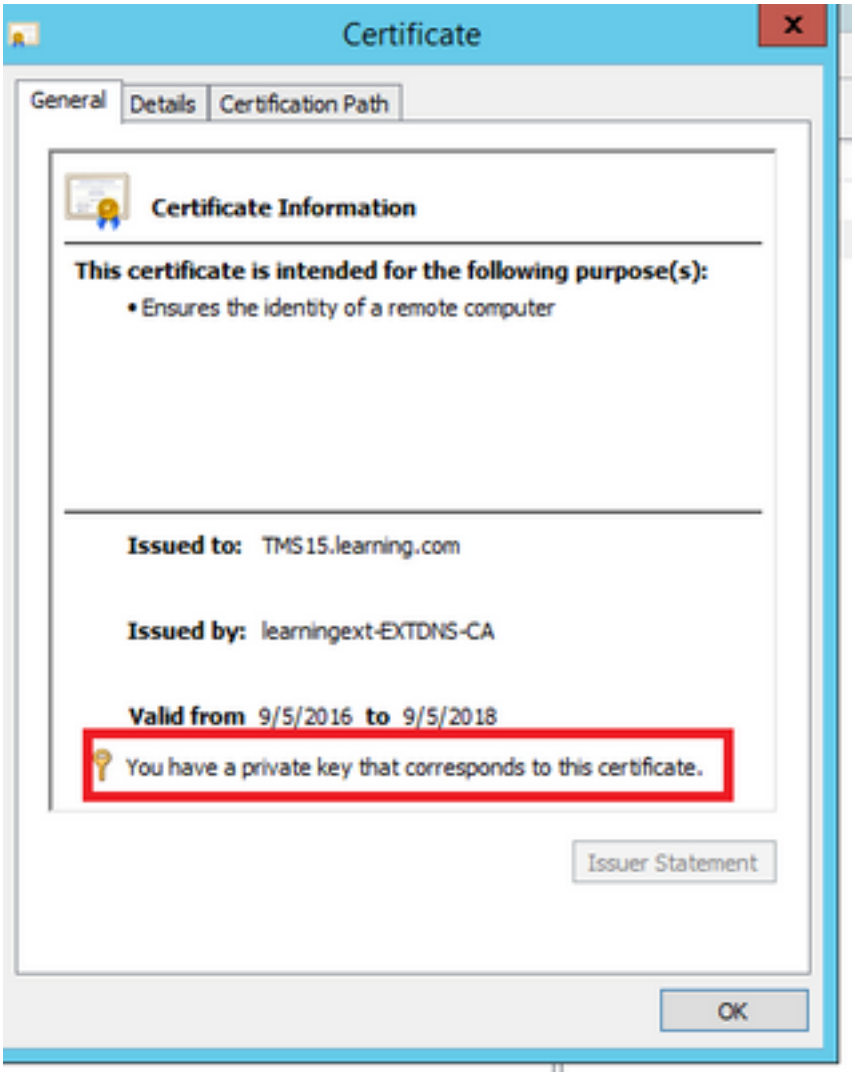
A fim importar o certificado renovado no mesmo Windows Server onde o CSR original foi gerado, execute as seguintes etapas.

Etapa 1. Navegue ao **Iniciar > Executar > ao mmc**. Clique sobre o **> Add do arquivo Pressão-em > computador local** (o usuário atual pode ser usado).

Etapa 2. Clique sobre a **ação > a importação** e selecione o certificado renovado. Selecione a **loja do certificado: Pessoal** (escolheu diferente se for necessário).

Etapa 3. Uma vez que o certificado é importado, clicar com o botão direito nele e abra o certificado.

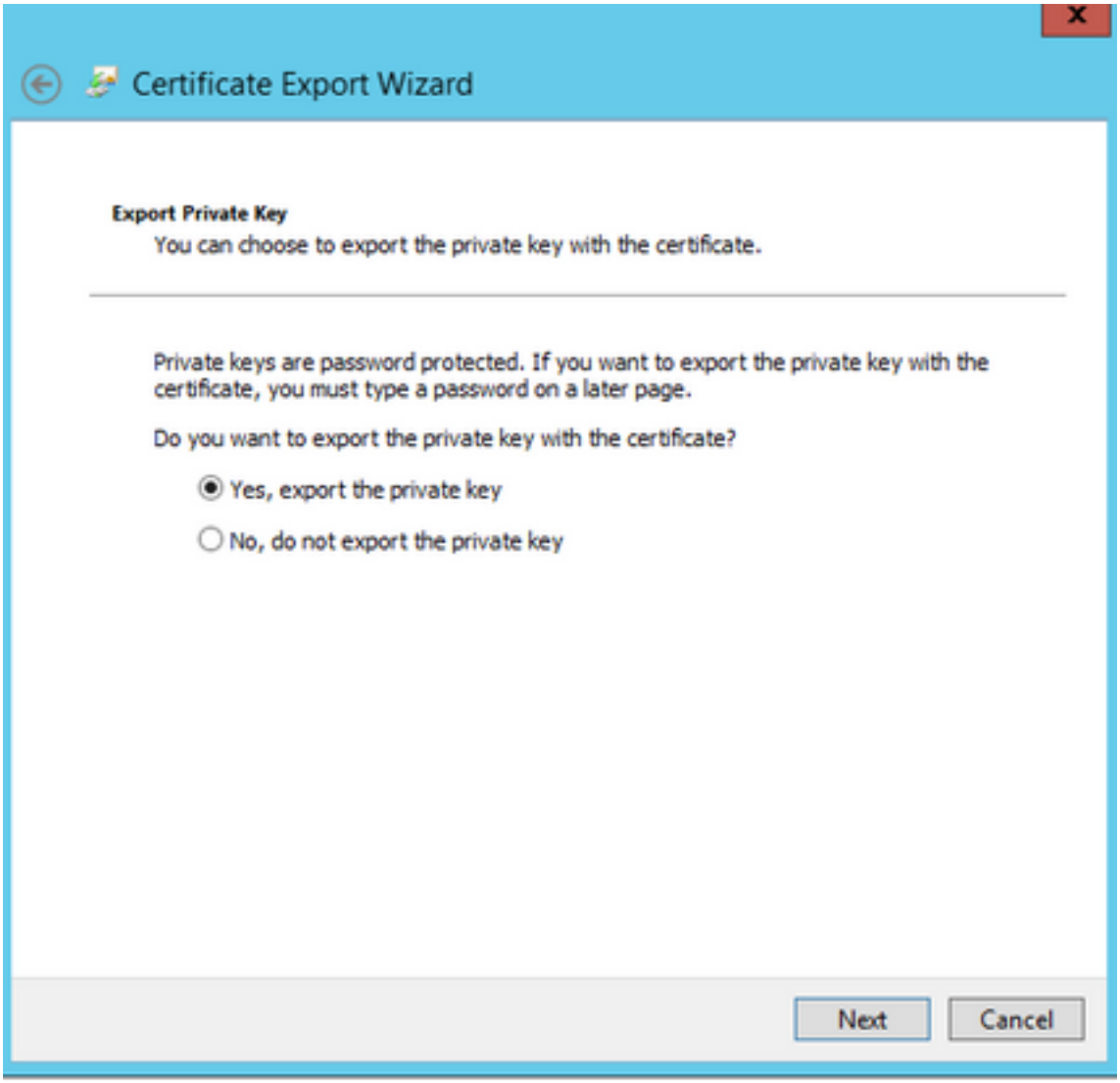
- Se o certificado for renovado baseou na chave privada do mesmo server, o certificado indica: “Você tem uma chave privada que corresponda a este certificado” como no exemplo abaixo:

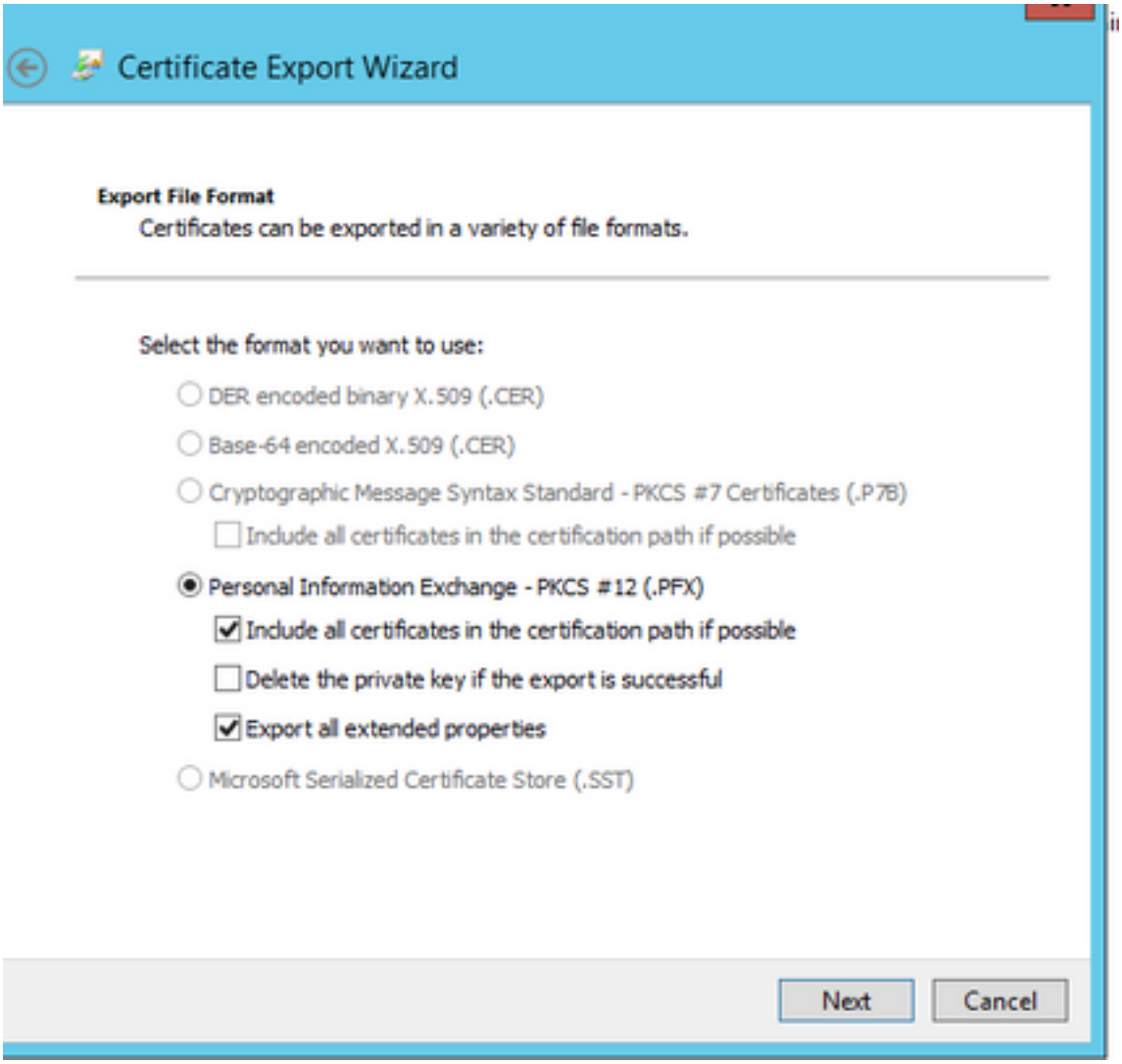


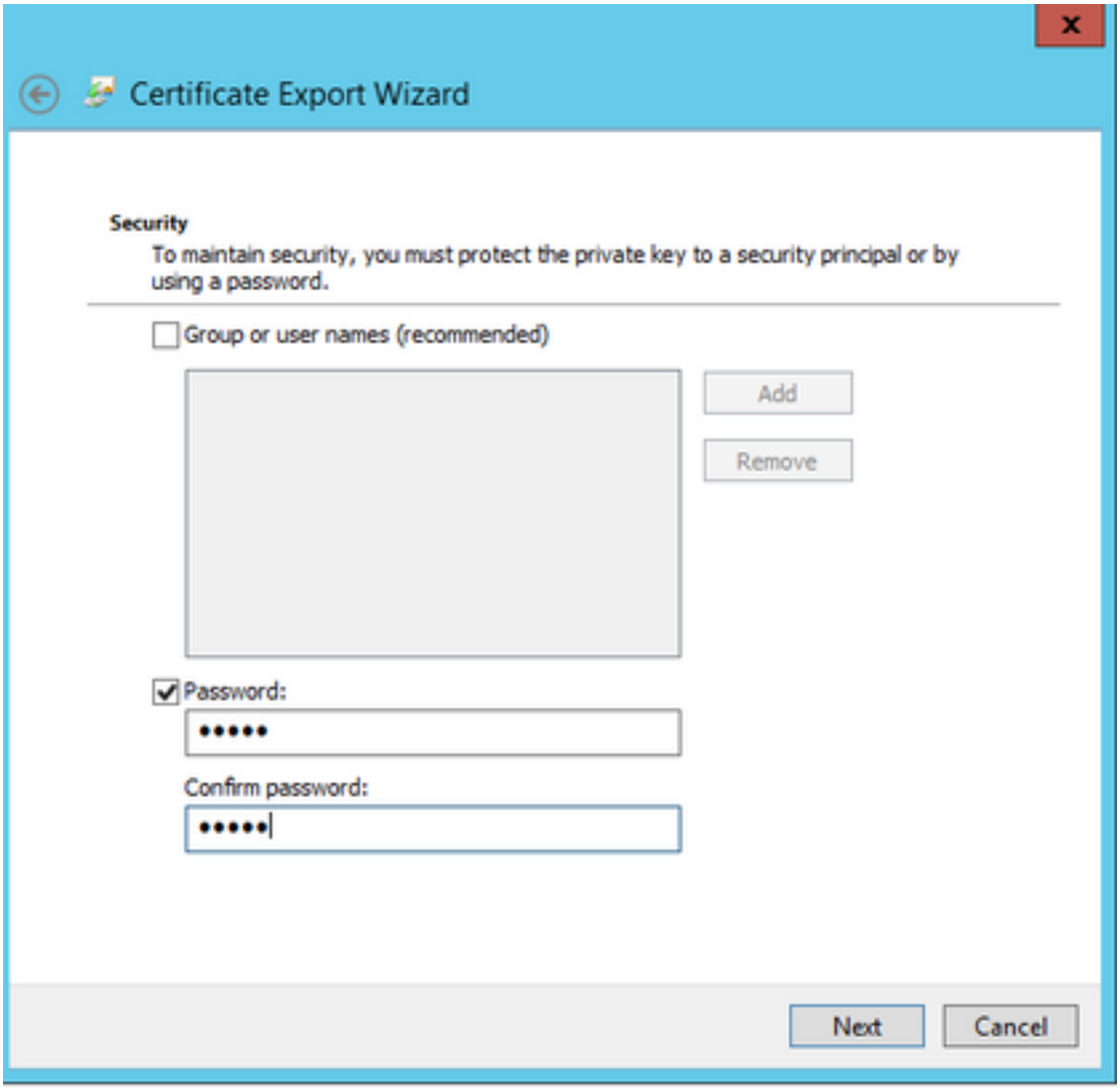
Exporte o certificado e transfira-o arquivos pela rede em TMS

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

Etapa 1. Usando o **gerenciador certificado de Windows Pressão-em**, exporte a chave privada existente (par do certificado) como um arquivo do **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 **gerenciador certificado de Windows Pressão-em**, exporte o certificado existente como **Base64 PEM codificou o** arquivo **.CER**. Assegure-se de que a extensão de arquivo seja **.cer** ou **.crt** e forneça-se este arquivo à equipe dos serviços da nuvem do WebEx.

Etapa 3. Registre em Cisco TMS, e navegue às **ferramentas administrativas > aos ajustes da configuração > do WebEx**. Na placa dos locais do WebEx, verifique todos os ajustes que incluem o SSO.

Etapa 4. Clique sobre **Browse** e transfira arquivos pela rede o certificado da chave privada **PKS #12** (.pfx) que você gerou em **gerar um certificado para o WebEx**. Termine o resto dos campos de configuração SSO usando a senha e a outra informação que você selecionou ao gerar o certificado. Clique em Salvar.

No caso quando a chave privada está disponível exclusivamente, você pode combinar o certificado assinado no formato do .pem com a chave privada usando o seguinte comando do OpenSSL:

pkcs12 do OpenSSL - exportação - o inkey tms-privatekey.pem - em tms-cert.pem - para fora tms-cert-key.p12 - nomeie a tms-CERT-chave

Você deve agora ter um certificado de Cisco TMS que contenha a chave privada para que a configuração SSO transfira arquivos pela rede a Cisco TMS.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Guia de configuração híbrida das salas de reuniões da colaboração do Cisco (CMR) (TMS 15.0 - centro WBS30 da reunião do WebEx)