TMS WebEx SSO Certificate Renewal - Cisco

Contents

Introduction

This document describes the procedure to renew a Webex SSO certificate on TMS when TMS is in Webex Hybrid configuration with SSO.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- TMS (Cisco TelePresence Management Suite)
- Webex SSO (Single Sign-on)
- Cisco Collaboration Meeting Rooms (CMR) Hybrid Configuration

Components Used

The information in this document is based on these software and hardware versions:

- TMS 15.0 and above

The information in this document is based on the Cisco Collaboration Meeting Rooms (CMR) Hybrid Configuration Guide (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. If your network is live, ensure that you understand the potential impact of any command.

Background Information

The article covers a scenario in which a certificate has been already renewed via the CA web portal by clicking on the renew button. The procedure to generate a new CSR (Certificate Signing Request) is not included in this document.

Ensure that you have access to the same Windows server which generated the original CSR. In the case when access to the particular Windows server is not available, a new certificate generation has to be followed, as per the configuration guide.

Procedure to upload the renewed certificate on TMS

Import the certificate

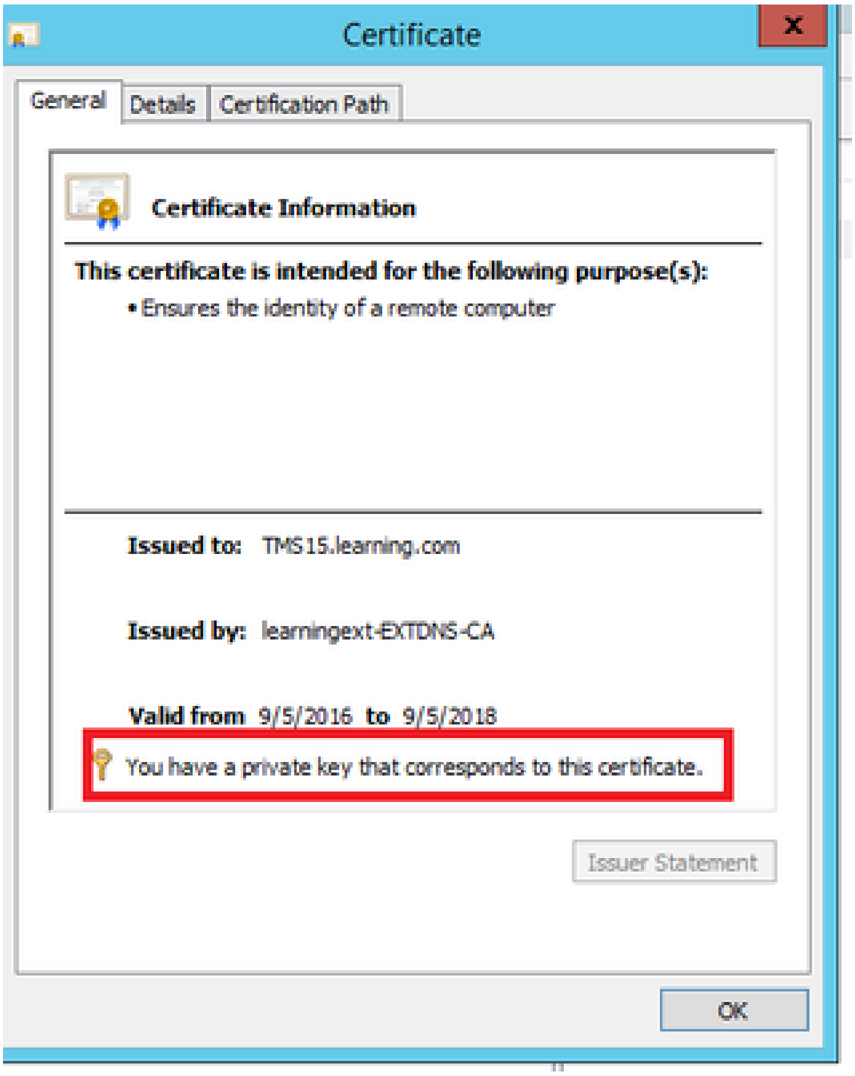
In order to import the renewed certificate on the same Windows server where the original CSR has been generated, perform the following steps.

Step 1. Navigate to **Start > Run > mmc**. Click on **File > Add Snap-in > Local Computer** (the current user can be used).

Step 2. Click on **Action > Import** and select the renewed certificate. Select **Certificate Store: Personal** (chose different if required).

Step 3. Once the certificate is imported, right click on it and open the certificate.

- If the certificate has been renewed based on the private key of the same server, the certificate should display: "You have a private key that corresponds to this certificate" as in the example below:



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

Issued to: TMS15.learning.com

Issued by: learningext-EXTDNS-CA

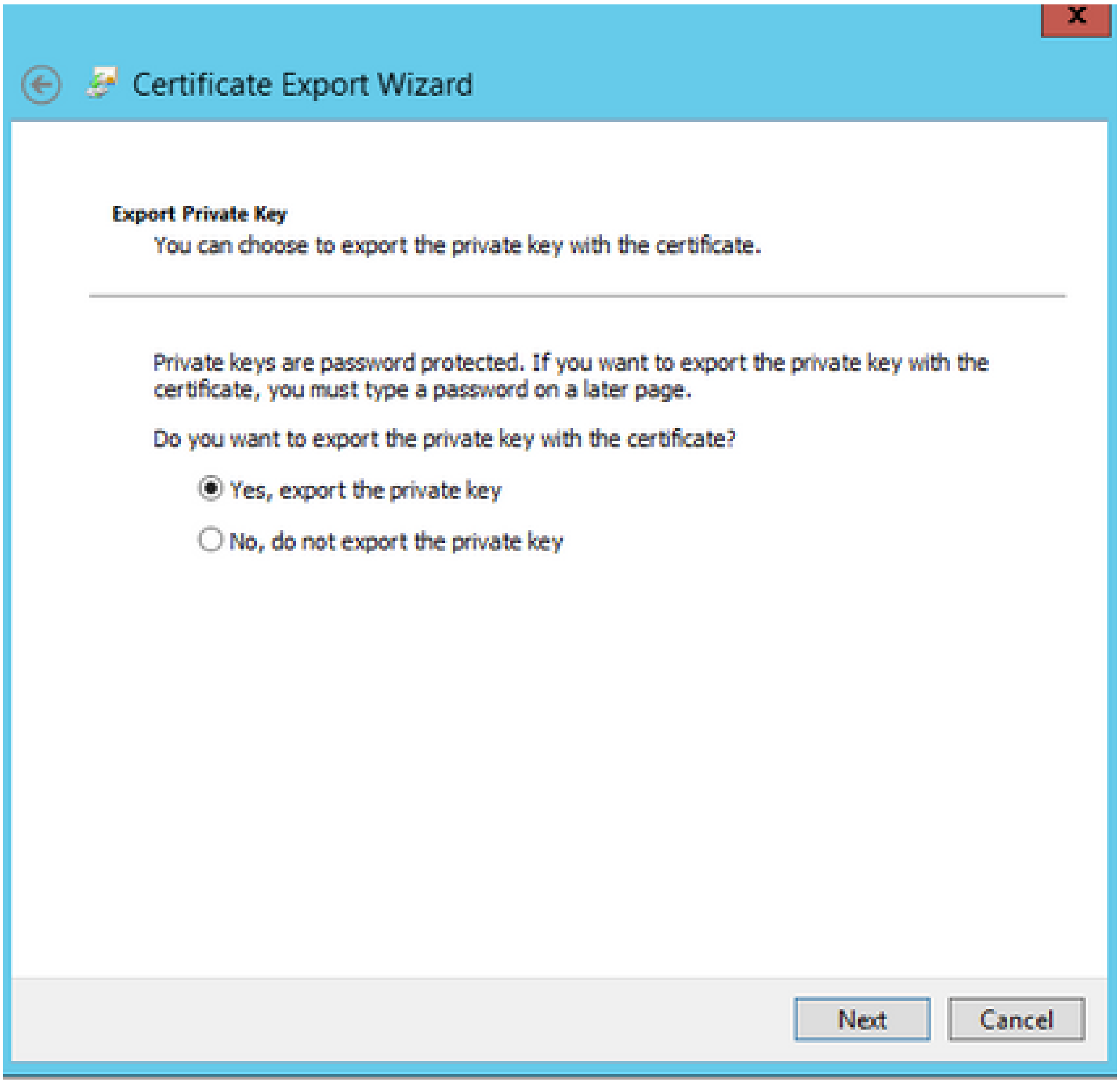
Valid from 9/5/2016 to 9/5/2018

You have a private key that corresponds to this certificate.

Export the certificate and upload it on TMS

In order to export the renewed certificate along with its private key, perform the following steps.

Step 1. Using the **Windows Certificate Manager Snap-in**, export the existing private key (certificate pair) as a **PKCS#12** file:



Export Private Key

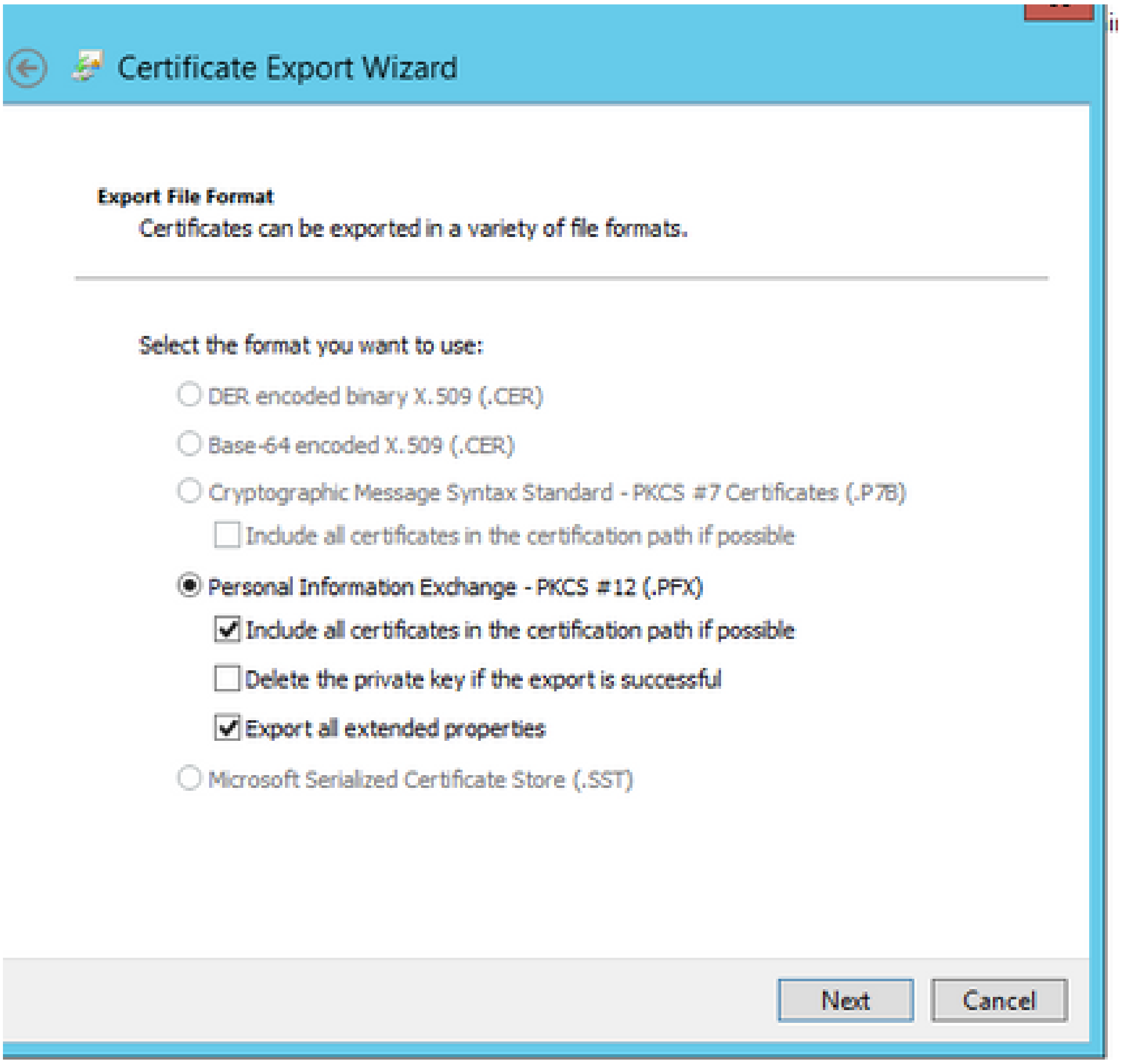
You can choose to export the private key with the certificate.

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



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

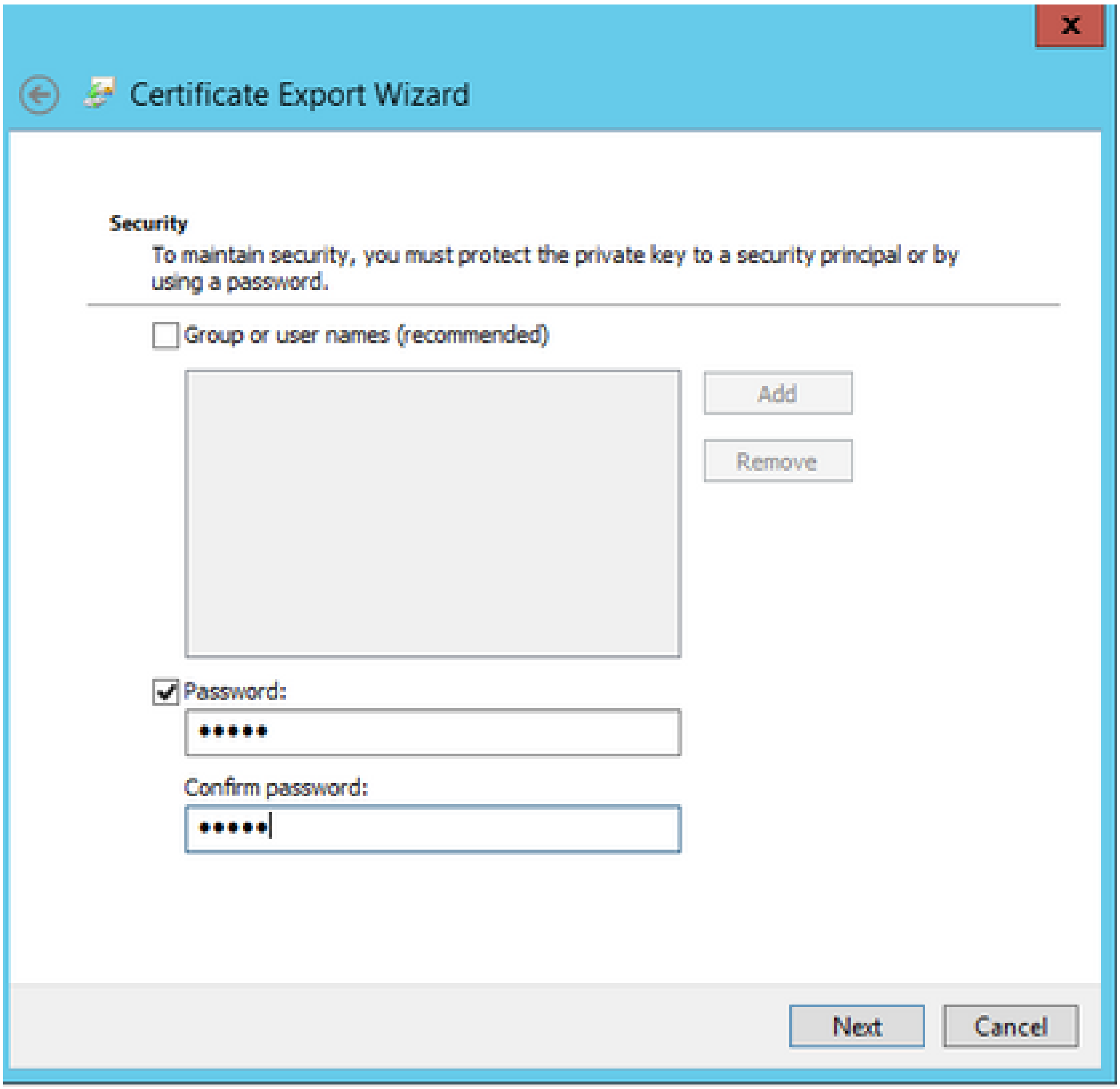
● Personal Information Exchange - PKCS #12 (.PFX)

☑ 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)



Security

To maintain security, you must protect the private key to a security principal or by using a password.

☐ Group or user names (recommended)

☑ Password:

•••••

Confirm password:

•••••

Step 2. Using the **Windows Certificate Manager Snap-in**, export the existing certificate as a **Base64 PEM encoded .CER** file. Ensure that the file extension is either **.cer** or **.crt** and provide this file to the WebEx Cloud Services team.

Step 3. Log into Cisco TMS, and navigate to **Administrative Tools > Configuration > WebEx Settings**. At the WebEx Sites pane, verify all of the settings including SSO.

Step 4. Click on **Browse** and upload the **PKS #12** private key certificate (.pfx) which you generated at **Generating a Certificate for WebEx**. Complete the rest of the SSO configuration fields using the password and other information which you selected when generating the certificate. Click **Save**.

In the case when the private key is available exclusively, you can combine the signed certificate in .pem format with the private key using the following OpenSSL command:

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

You should now have a Cisco TMS certificate which contains the private key for SSO configuration to upload to Cisco TMS.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- Cisco Collaboration Meeting Rooms (CMR) Hybrid Configuration Guide (TMS 15.0 - WebEx Meeting Center WBS30)