Verlängerung des TMS WebEx SSO-Zertifikats - Cisco

Inhalt

Einführung

Dieses Dokument beschreibt das Verfahren zur Verlängerung eines Webex SSO-Zertifikats auf TMS, wenn sich das TMS in der WebEx Hybrid-Konfiguration mit SSO befindet.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- TMS (Cisco TelePresence Management Suite)
- WebEx SSO (einmalige Anmeldung)
- Cisco Collaboration Meeting Rooms (CMR) - Hybrid-Konfiguration

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- TMS 15.0 und höher

Die Informationen in diesem Dokument basieren auf dem Cisco Collaboration Meeting Rooms (CMR) Hybrid Configuration Guide (TMS 15.0 - WebEx Meeting Center WBS30).

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Der Artikel behandelt ein Szenario, in dem ein Zertifikat bereits über das CA-Webportal durch Klicken auf die Schaltfläche "Erneuern" verlängert wurde. Das Verfahren zum Generieren eines neuen CSR (Certificate Signing Request) ist in diesem Dokument nicht enthalten.

Stellen Sie sicher, dass Sie Zugriff auf denselben Windows-Server haben, der den ursprünglichen CSR generiert hat. Wenn kein Zugriff auf den jeweiligen Windows-Server möglich ist, muss entsprechend dem Konfigurationsleitfaden eine neue Zertifikatgenerierung durchgeführt werden.

Verfahren zum Hochladen des erneuerten Zertifikats auf TMS

Zertifikat importieren

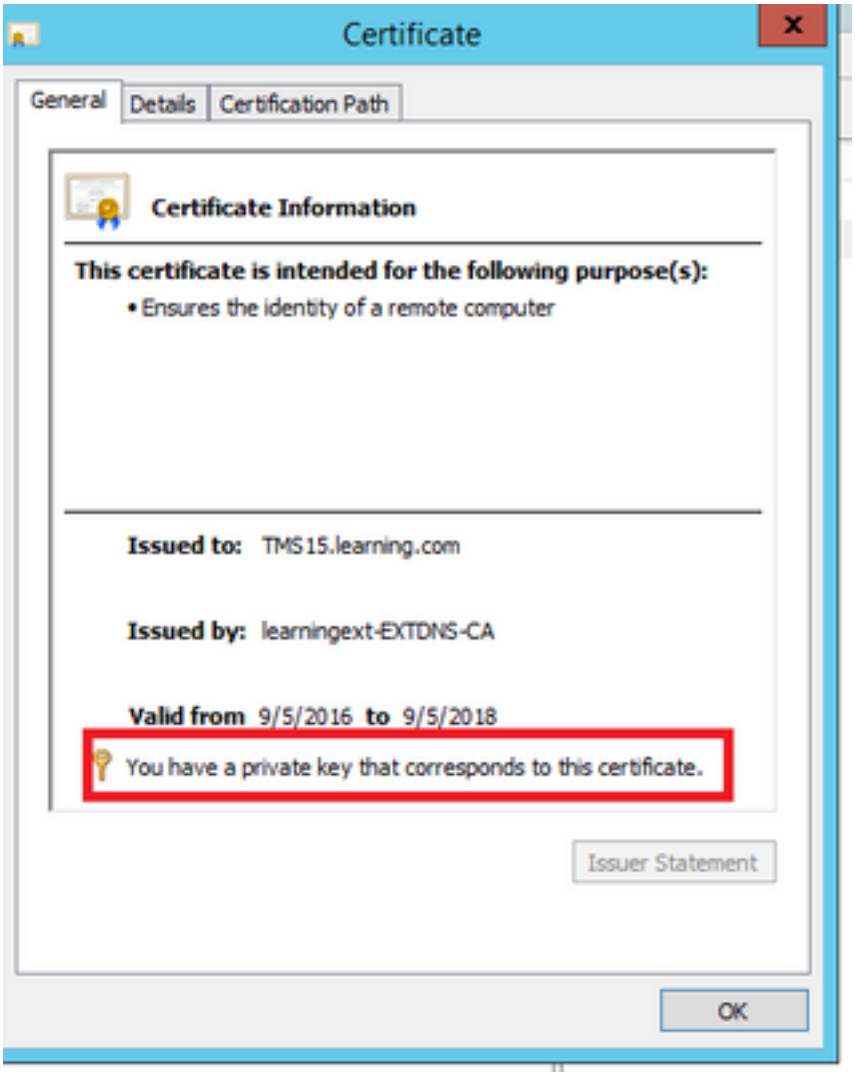
So importieren Sie das erneuerte Zertifikat auf demselben Windows-Server, auf dem der ursprüngliche CSR generiert wurde.

Schritt 1: Navigieren Sie zu **Start > Ausführen > MMC**. Klicken Sie auf **Datei > Snap-In hinzufügen > Lokaler Computer** (der aktuelle Benutzer kann verwendet werden).

Schritt 2: Klicken Sie auf **Aktion > Importieren,** und wählen Sie das erneuerte Zertifikat aus. Wählen Sie **Zertifikatsspeicher aus: Persönlich** (Wählen Sie bei Bedarf etwas Anderes aus).

Schritt 3: Wenn das Zertifikat importiert wurde, klicken Sie mit der rechten Maustaste darauf, und öffnen Sie das Zertifikat.

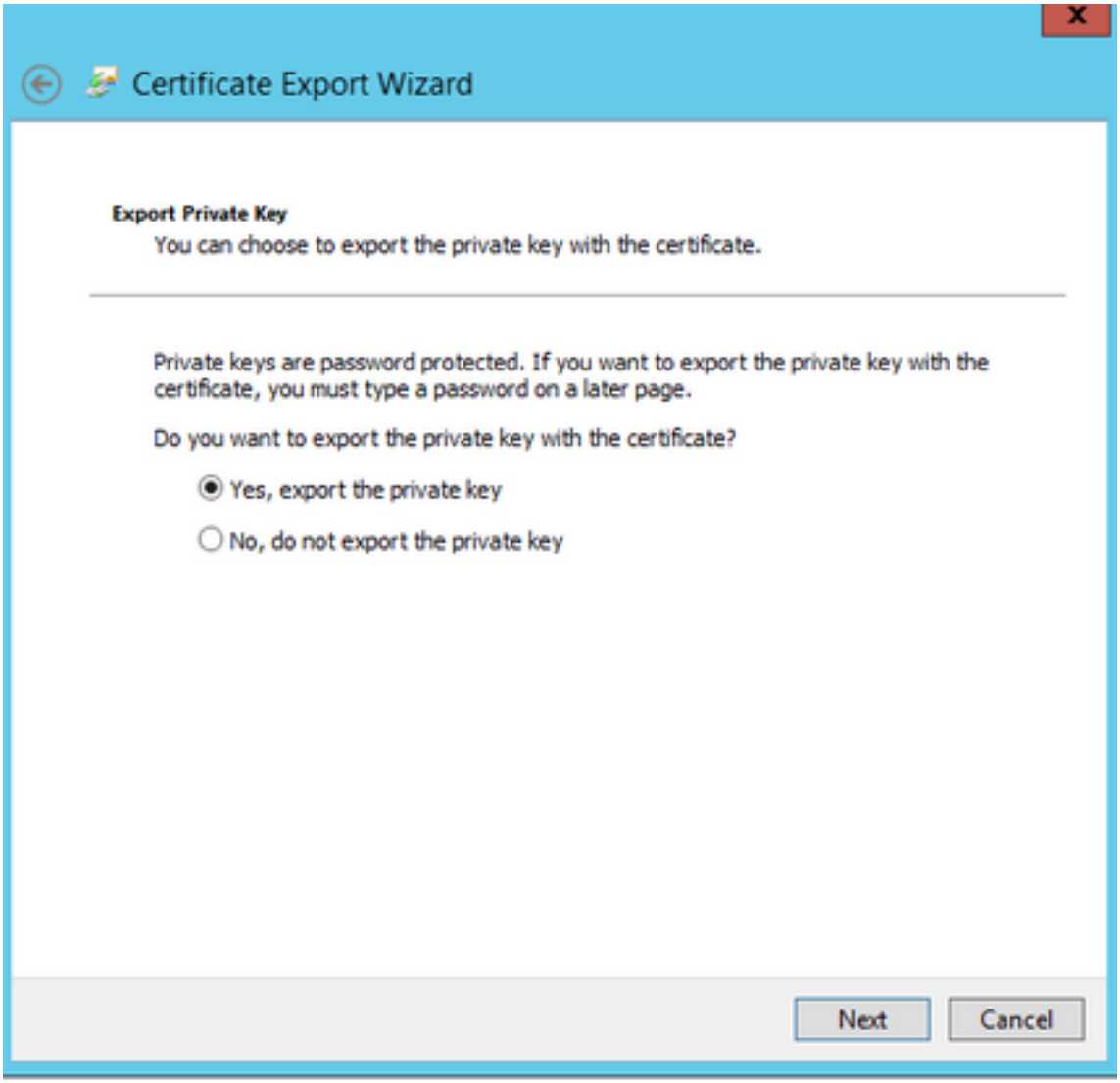
- Wenn das Zertifikat auf der Grundlage des privaten Schlüssels desselben Servers erneuert wurde, muss das Zertifikat Folgendes anzeigen: "Sie haben einen privaten Schlüssel, der diesem Zertifikat entspricht", wie im Beispiel unten gezeigt:

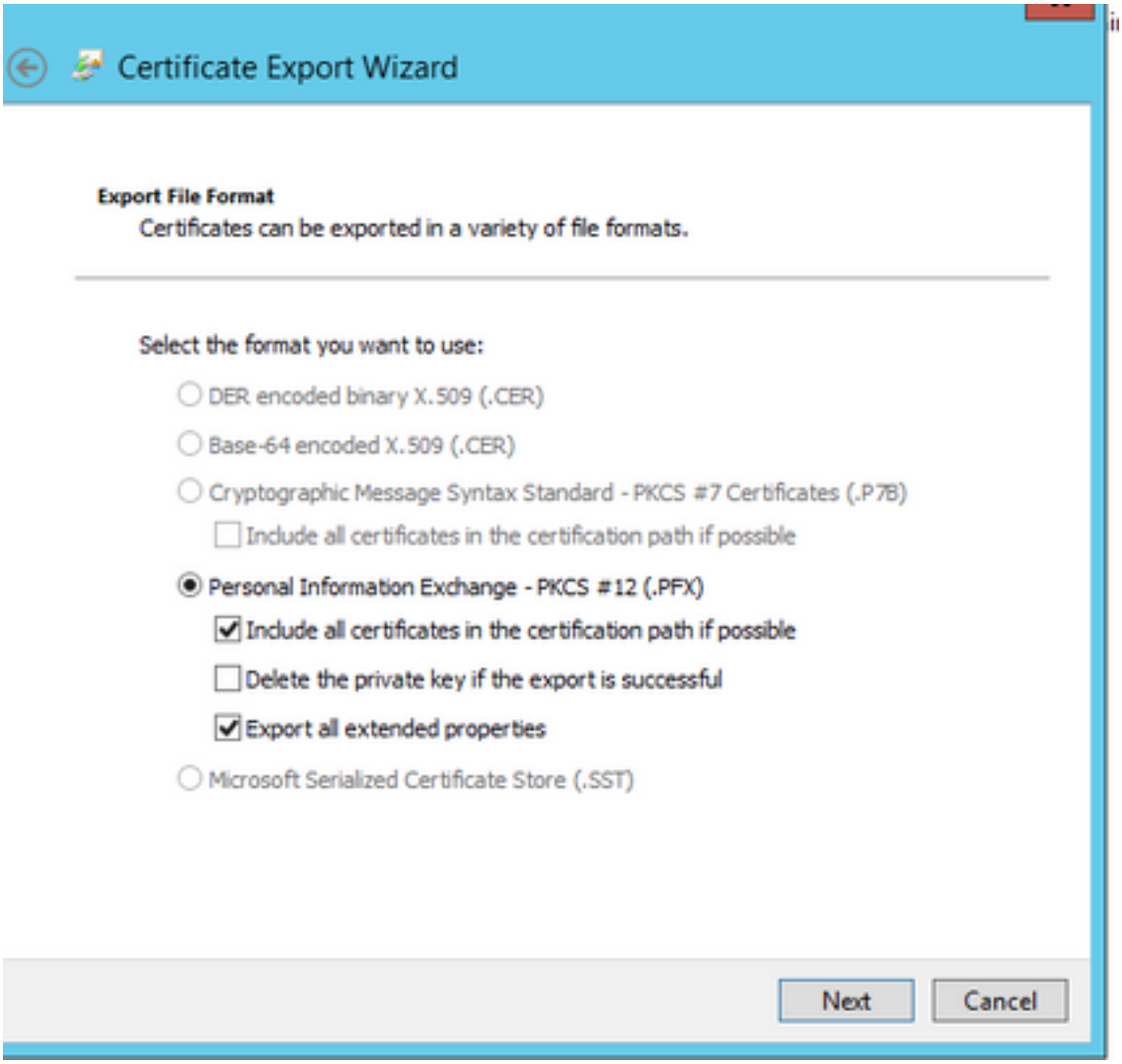


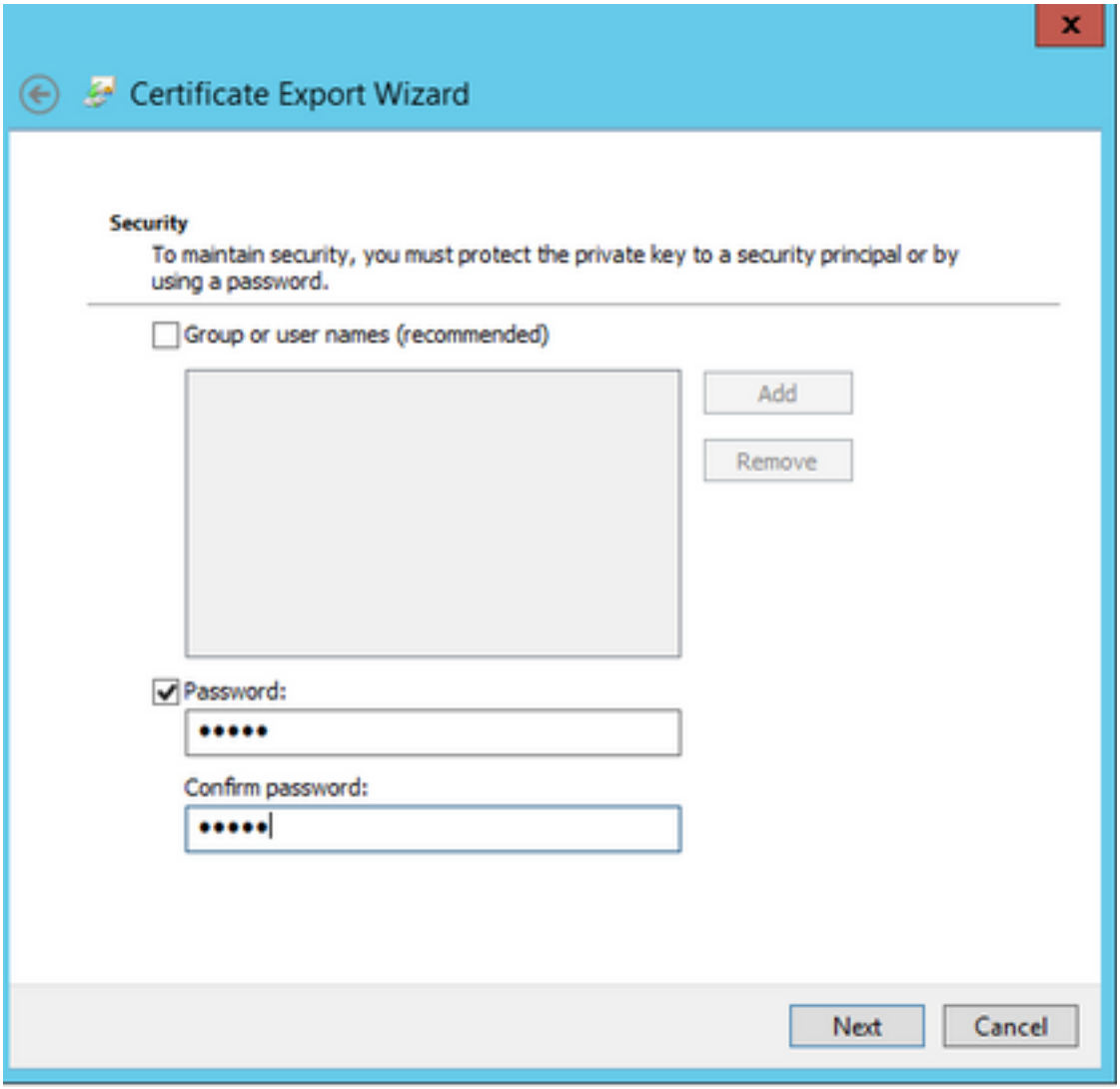
Zertifikat exportieren und auf TMS hochladen

So exportieren Sie das erneuerte Zertifikat zusammen mit dem privaten Schlüssel.

Schritt 1: Exportieren Sie den vorhandenen privaten Schlüssel (Zertifikatpaar) mithilfe des **Snap-Ins für den Windows Certificate Manager** als **PKCS#12-**Datei:


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



Schritt 2: Exportieren Sie das vorhandene Zertifikat mithilfe des **Snap-Ins für den Windows Certificate Manager** als **PEM-kodierte CER-**Datei **Base64**. Stellen Sie sicher, dass die Dateierweiterung **.cer** oder **.crt** lautet, und stellen Sie diese Datei dem WebEx Cloud Services-Team zur Verfügung.

Schritt 3: Melden Sie sich bei Cisco TMS an, und navigieren Sie zu **Verwaltung > Konfiguration > WebEx Einstellungen**. Überprüfen Sie im Bereich "WebEx Sites" alle Einstellungen einschließlich SSO.

Schritt 4: Klicken Sie auf **Durchsuchen** und laden Sie das **PKS #12** Private Key Certificate (PFX) hoch, das Sie bei der **Generating a Certificate for WebEx** generiert haben. Füllen Sie die übrigen Felder für die SSO-Konfiguration mit dem Kennwort und anderen Informationen aus, die Sie bei der Erstellung des Zertifikats ausgewählt haben. Klicken Sie auf **Speichern**.

Wenn der private Schlüssel exklusiv verfügbar ist, können Sie das signierte Zertifikat im .pem-Format mit dem privaten Schlüssel mithilfe des folgenden OpenSSL-Befehls kombinieren:

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

Sie sollten jetzt über ein Cisco TMS-Zertifikat verfügen, das den privaten Schlüssel für die SSO-Konfiguration zum Hochladen auf Cisco TMS enthält.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

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