Rinnovo certificato WebEx SSO TMS - Cisco

Sommario

Introduzione

Questo documento descrive la procedura per rinnovare un certificato Webex SSO su TMS quando TMS è in configurazione Webex Hybrid con SSO.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- TMS (Cisco TelePresence Management Suite)
- Webex SSO (Single Sign-On)
- Configurazione ibrida Cisco Collaboration Meeting Rooms (CMR)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- TMS 15.0 e versioni successive

Le informazioni fornite in questo documento si basano sulla guida alla configurazione ibrida delle Cisco Collaboration Meeting Rooms (CMR) (TMS 15.0 - WebEx Meeting Center WBS30).

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Nell'articolo viene descritto uno scenario in cui un certificato è già stato rinnovato tramite il portale Web della CA facendo clic sul pulsante di rinnovo. La procedura per generare una nuova richiesta di firma del certificato (CSR) non è inclusa in questo documento.

Assicurarsi di disporre dell'accesso allo stesso server Windows che ha generato il CSR originale. Nel caso in cui l'accesso a un determinato server Windows non sia disponibile, è necessario eseguire una nuova generazione di certificati, come indicato nella guida alla configurazione.

Procedura per caricare il certificato rinnovato su TMS

Importa il certificato

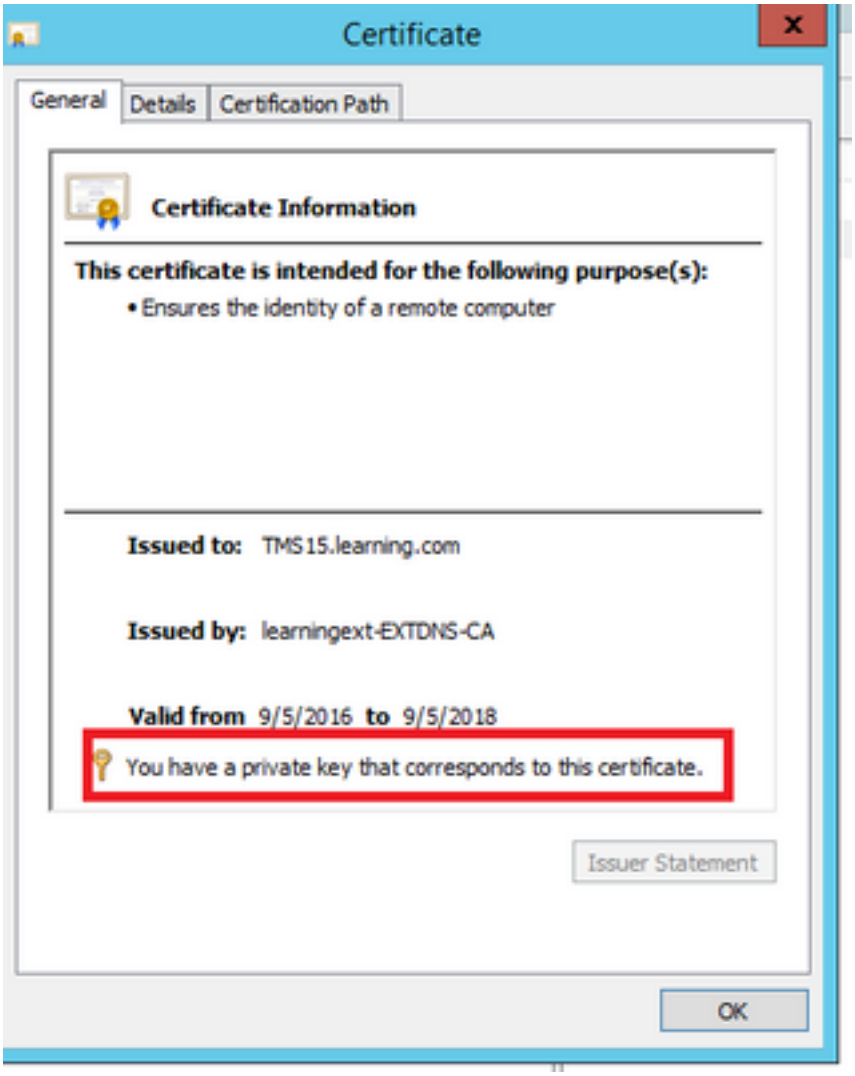
Per importare il certificato rinnovato nello stesso server Windows in cui è stato generato il CSR originale, eseguire la procedura seguente.

Passaggio 1. Passare a **Start > Esegui > mmc**. Fare clic su **File > Aggiungi snap-in > Computer locale** (è possibile utilizzare l'utente corrente).

Passaggio 2. Fare clic su **Azione > Importa** e selezionare il certificato rinnovato. Seleziona **archivio certificati: Personale** (scegliere diverso se necessario).

Passaggio 3. Una volta importato il certificato, fare clic con il pulsante destro del mouse su di esso e aprire il certificato.

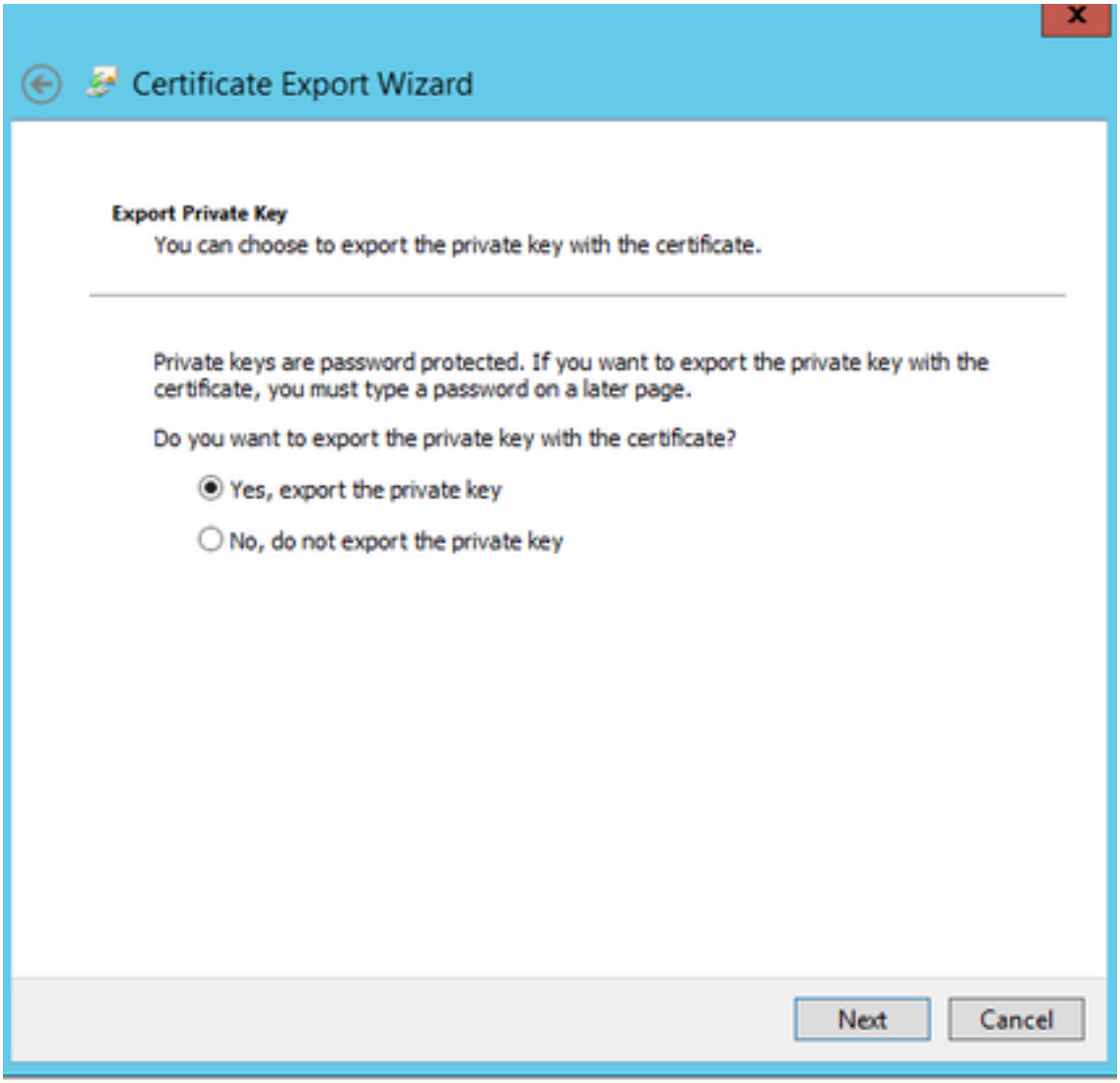
- Se il certificato è stato rinnovato in base alla chiave privata dello stesso server, nel certificato dovrebbe essere visualizzato quanto segue: "Si dispone di una chiave privata che corrisponde a questo certificato", come nell'esempio seguente:

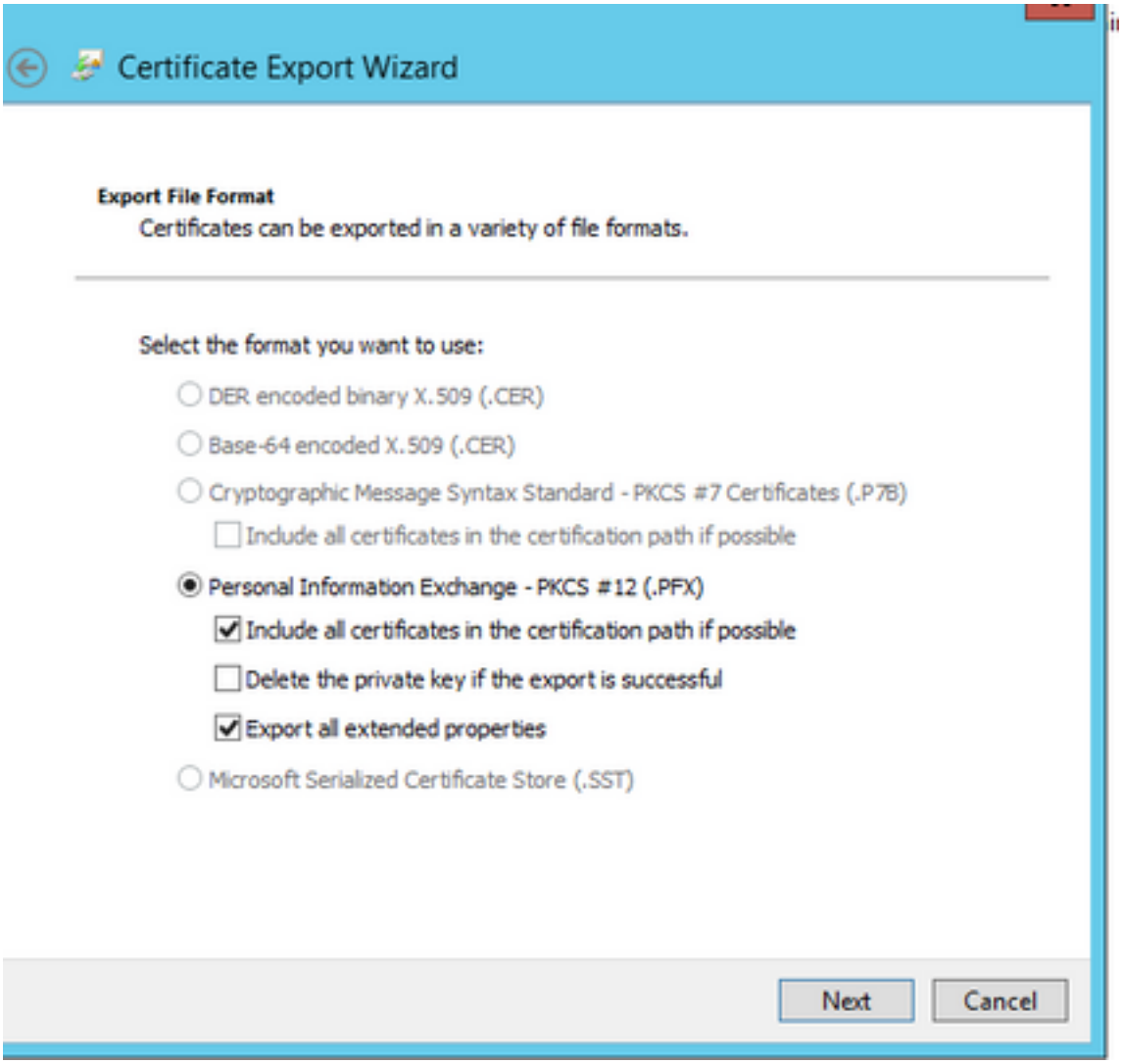


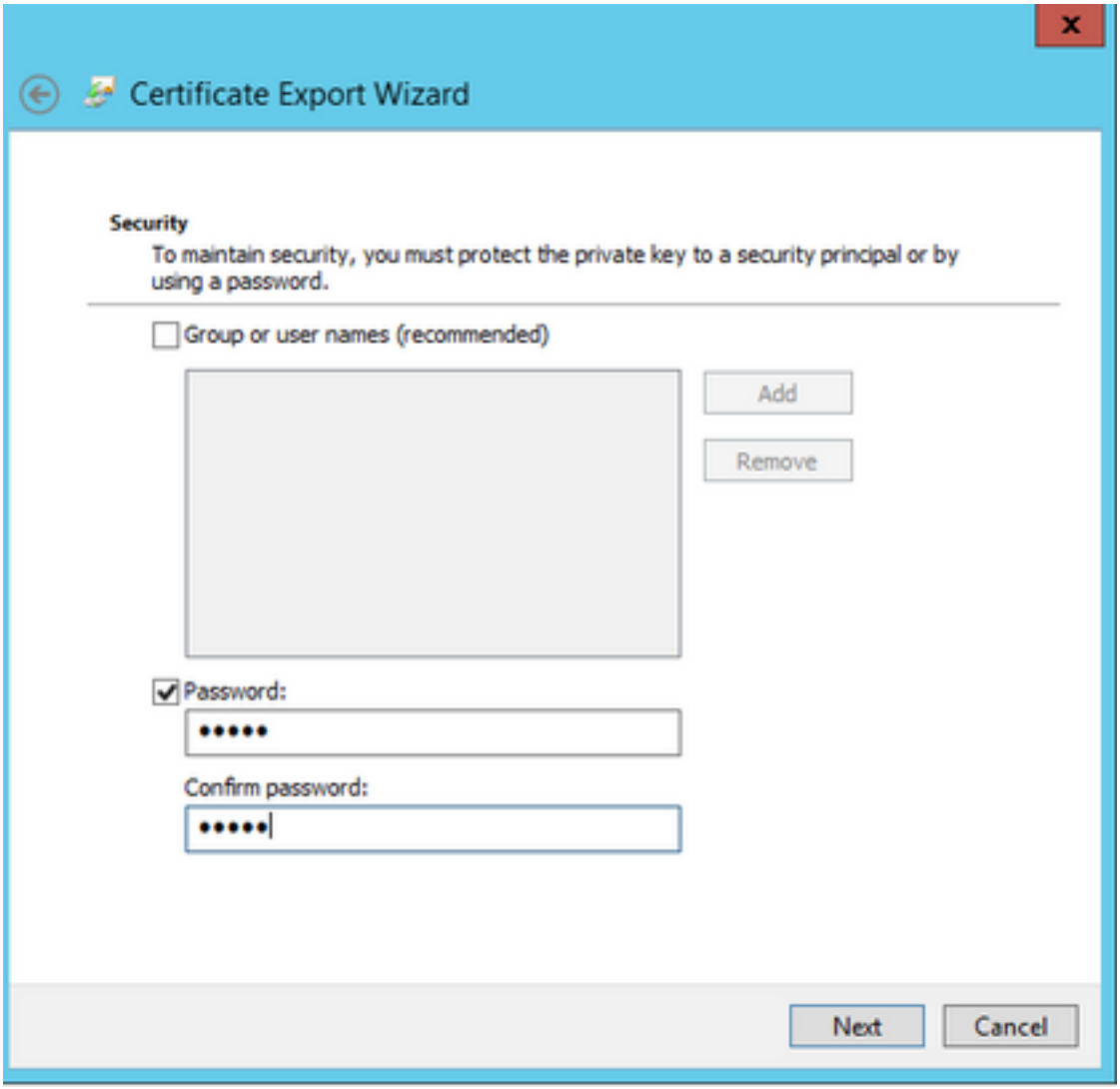
Esporta il certificato e caricalo in TMS

Per esportare il certificato rinnovato insieme alla relativa chiave privata, eseguire la procedura seguente.

Passaggio 1. Utilizzando lo **snap-in Gestione certificati di Windows**, esportare la chiave privata esistente (coppia di certificati) come file **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



Passaggio 2. Utilizzando lo **snap-in Gestione certificati di Windows**, esportare il certificato esistente come file **CER con codifica Base64 PEM**. Verificare che l'estensione del file sia **.cer** o **.crt** e fornire il file al team dei servizi cloud WebEx.

Passaggio 3. Accedere a Cisco TMS e selezionare **Strumenti di amministrazione > Configurazione > Impostazioni WebEx**. Nel riquadro Siti WebEx verificare tutte le impostazioni, incluso l'SSO.

Passaggio 4. Fare clic su **Sfoglia** e caricare il certificato con chiave privata (pfx) **PKS #12** generato durante la **generazione di un certificato per WebEx**. Completare gli altri campi di configurazione SSO utilizzando la password e altre informazioni selezionate durante la generazione del certificato. Fare clic su **Salva**.

Se la chiave privata è disponibile in modalità esclusiva, è possibile combinare il certificato firmato in formato .pem con la chiave privata utilizzando il comando OpenSSL seguente:

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

A questo punto, è necessario disporre di un certificato Cisco TMS contenente la chiave privata per la configurazione SSO da caricare in Cisco TMS.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Guida alla configurazione ibrida di Cisco Collaboration Meeting Rooms (CMR) (TMS 15.0 - WebEx Meeting Center WBS30)