Обновление сертификата SSO WebEx TMS - Cisco

Содержание

Введение

Когда TMS находится в Гибридной конфигурации Webex с SSO, этот документ описывает процедуру для возобновления сертификата SSO Webex на TMS.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- TMS (система управления Cisco TelePresence)
- SSO Webex (единая точка входа)
- Комнаты для совещаний Cisco Collaboration (CMR) гибридная конфигурация

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- TMS 15.0 и выше

Сведения в этом документе основываются [на Комнатах для совещаний Cisco Collaboration (CMR) Руководство Гибридной конфигурации (TMS 15.0 - Центр Совещания WebEx WBS30)](#).

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. Если ваша сеть является оперативной, гарантируйте понимание потенциального воздействия любой команды.

Общие сведения

Статья касается сценария , в котором сертификат был уже возобновлен через веб-портал CA путем щелчка по возобновить кнопке. Процедура для генерации нового CSR (Запрос подписи сертификата) не включена в этот документ.

Гарантируйте, что у вас есть доступ к тому же Windows Server, который генерировал исходный CSR. В случае, когда доступ к определенному Windows Server не доступен, новая генерация сертификата должна придерживаться согласно руководству по конфигурации.

Процедура для загрузки возобновленного сертификата на TMS

Импортируйте сертификат

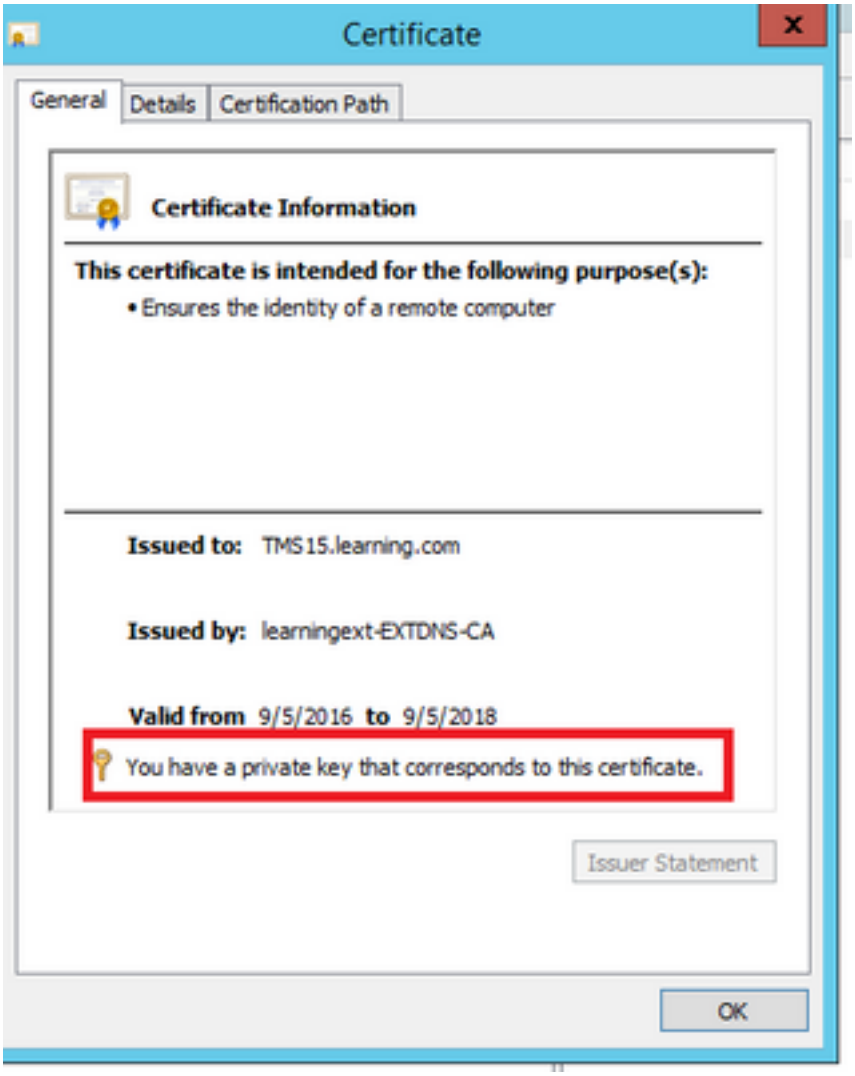
Для импорта возобновленного сертификата на том же Windows Server , где исходный CSR генерировался, выполните следующие шаги.

Шаг 1. Перейдите к **Пуску> Выполнить> mmc**. Щелкните **по File> Add Snap - в> Локальный компьютер** (текущий пользователь может использоваться).

Шаг 2. Щелкните **по Action> Import** и выберите возобновленный сертификат. Выберите **Certificate Store: Персональный** (выбрал другой при необходимости).

Шаг 3. Как только сертификат импортирован, щелкните правой кнопкой по нему и откройте сертификат.

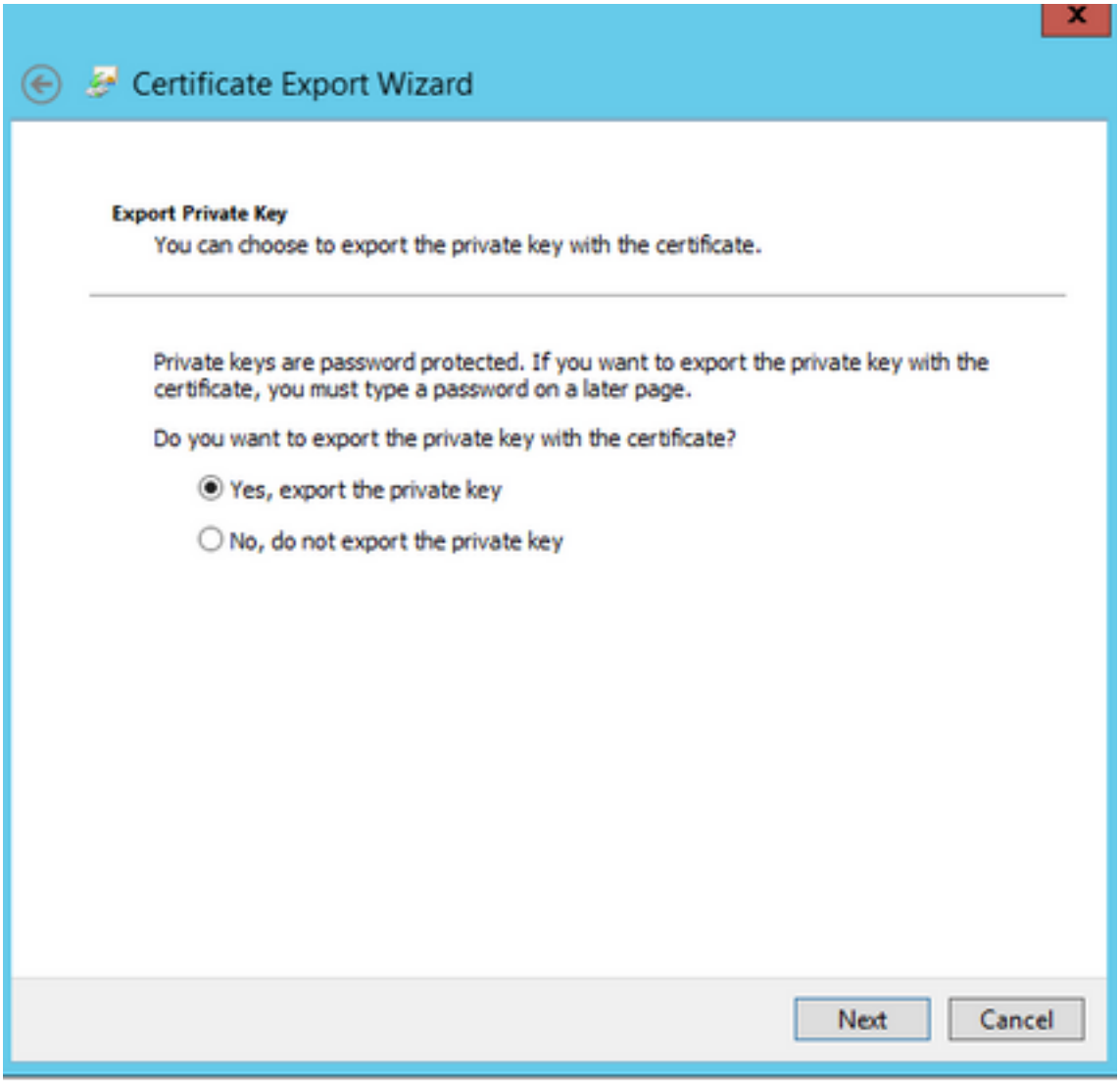
- Если сертификат был возобновлен на основе секретного ключа того же сервера, сертификат должен отобразиться: "У вас есть секретный ключ, который соответствует этому сертификату" как в примере ниже:

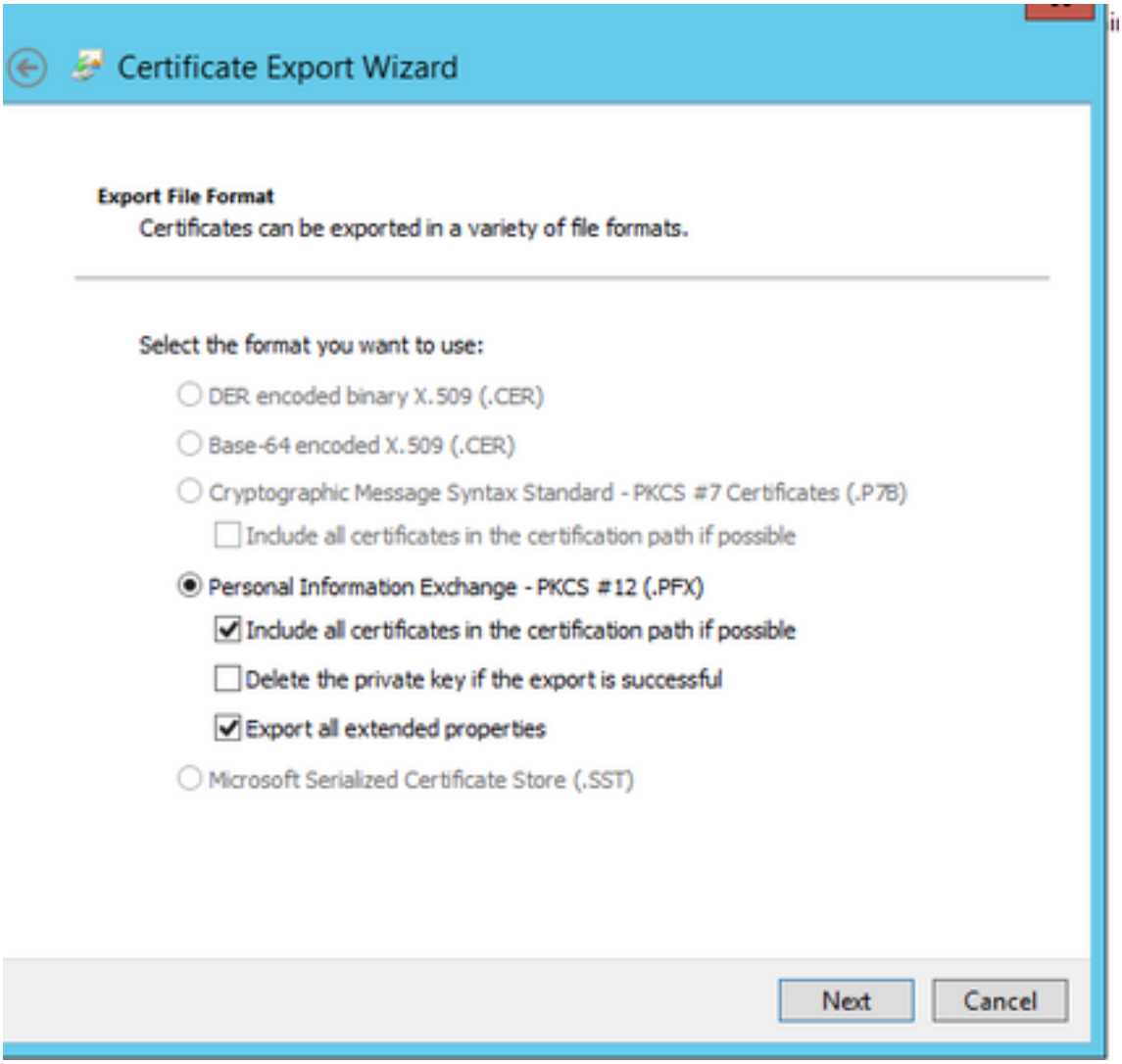


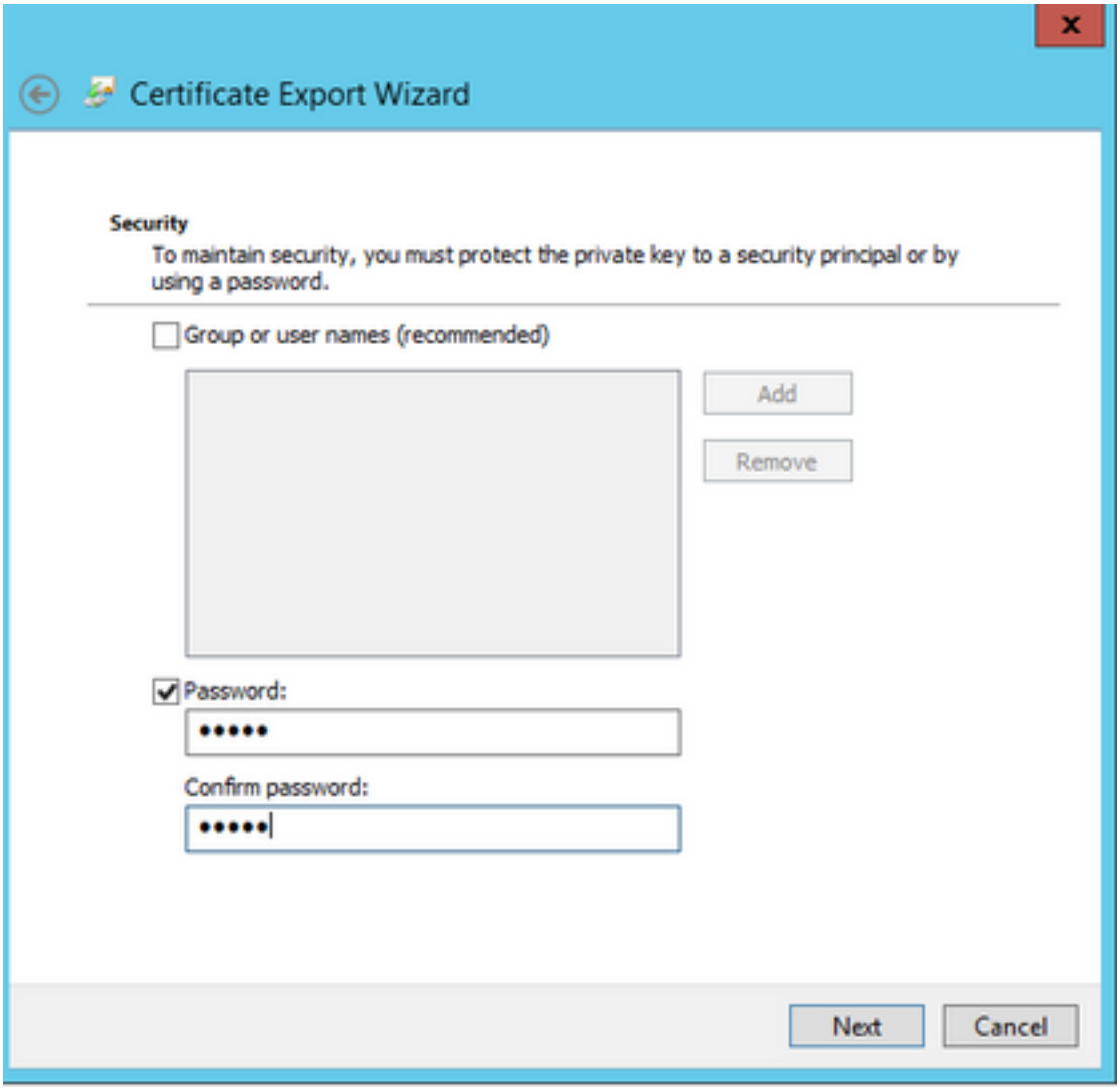
Экспортируйте сертификат и загрузите его на TMS

Для экспортирования возобновленного сертификата наряду с его секретным ключом выполните следующие шаги.

Шаг 1. Использование **менеджера сертификатов Windows Снэпа - в**, экспортируйте существующий секретный ключ (пара сертификата) как файл **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



Шаг 2. Использование **менеджера сертификатов Windows Снэпа - в**, экспортируйте существующий сертификат, поскольку **PEM Base64 закодировал.CER** файл. Гарантируйте, что расширение файла является или **.cer** или **.crt**, и предоставьте этот файл команде Облачных сервисов WebEx.

Шаг 3. Войдите в TMS Cisco и перейдите к **Средствам администрирования> Конфигурация> Параметры настройки WebEx**. В области WebEx Sites проверьте все параметры настройки включая SSO.

Шаг 4. . Щелкните **по Browse** и загрузите **PK #12** сертификат с закрытым ключом (.pfx), который вы генерировали при **Генерации Сертификата для WebEx**. Завершенный остаток полей конфигурации SSO с помощью пароля и другой информации , которую вы выбрали при генерации сертификата. **Нажмите Save.**

В случае, когда секретный ключ доступен исключительно, можно объединить подписанный сертификат в формате .pem с секретным ключом с помощью следующей команды OpenSSL:

pkcs12 openssl - экспортирует-inkey TM-privatekey.pem - в TM-cert.pem - tms-cert-key.p12 - называют tms-cert-key

У вас должен теперь быть сертификат TMS Cisco , который содержит секретный ключ для конфигурации SSO для загрузки к TMS Cisco.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- Комнаты для совещаний Cisco Collaboration (CMR) руководство гибридной конфигурации (TMS 15.0 - центр совещания WebEx WBS30)