TMS WebEx SSO 인증서 갱신 - Cisco

목차

소개

이 문서에서는 TMS가 SSO를 사용하는 Webex Hybrid 컨피그레이션에 있을 때 TMS에서 Webex SSO 인증서를 갱신하는 절차에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- TMS(Cisco TelePresence Management Suite)
- Webex SSO(단일 로그인)
- Cisco CMR(Collaboration Meeting Rooms) 하이브리드 컨피그레이션

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- TMS 15.0 이상

이 문서의 정보는 Cisco CMR(Collaboration Meeting Rooms) 하이브리드 컨피그레이션 가이드 (TMS 15.0 - WebEx Meeting Center WBS30)를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

이 문서에서는 CA 웹 포털을 통해 갱신 버튼을 클릭하여 인증서가 이미 갱신된 시나리오를 다룹니다. 새 CSR(Certificate Signing Request)을 생성하는 절차는 이 문서에 포함되어 있지 않습니다.

원래 CSR을 생성한 동일한 Windows 서버에 액세스할 수 있는지 확인하십시오. 특정 Windows 서버에 액세스할 수 없는 경우 구성 설명서에 따라 새 인증서를 생성해야 합니다.

TMS에 갱신된 인증서를 업로드하는 절차

인증서 가져오기

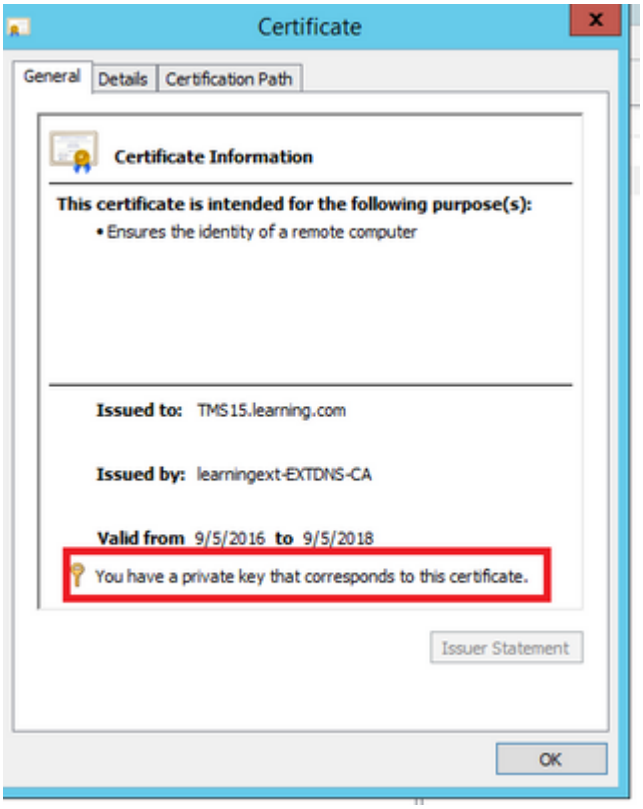
원래 CSR이 생성된 동일한 Windows 서버에서 갱신된 인증서를 가져오려면 다음 단계를 수행합니다.

1단계. 시작 > 실행 > mmc로 이동합니다. 파일 > 스냅인 추가 > 로컬 컴퓨터(현재 사용자 사용 가능)를 클릭합니다.

2단계. Action(작업) > Import(가져오기)를 클릭하고 갱신된 인증서를 선택합니다. 인증서 저장소 선택: 개인(필요한 경우 다른 선택)

3단계. 인증서를 가져오면 마우스 오른쪽 버튼으로 클릭하고 인증서를 엽니다.

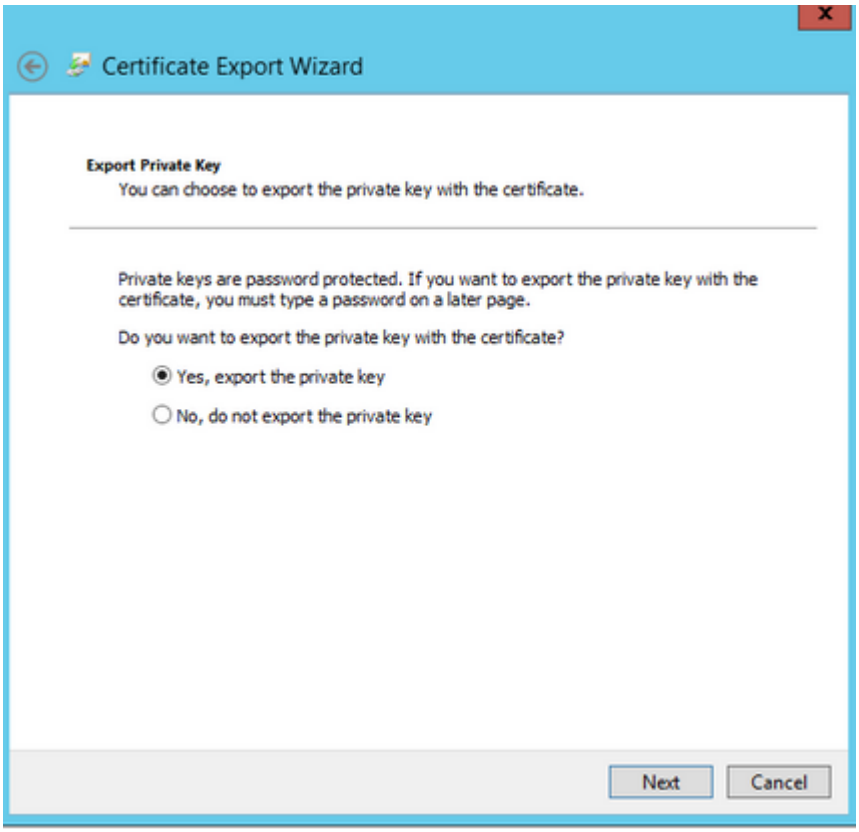
- 인증서가 동일한 서버의 개인 키를 기반으로 갱신된 경우 인증서는 다음과 같이 표시되어야 합니다. 아래 예와 같이 "이 인증서에 해당하는 개인 키가 있습니다."

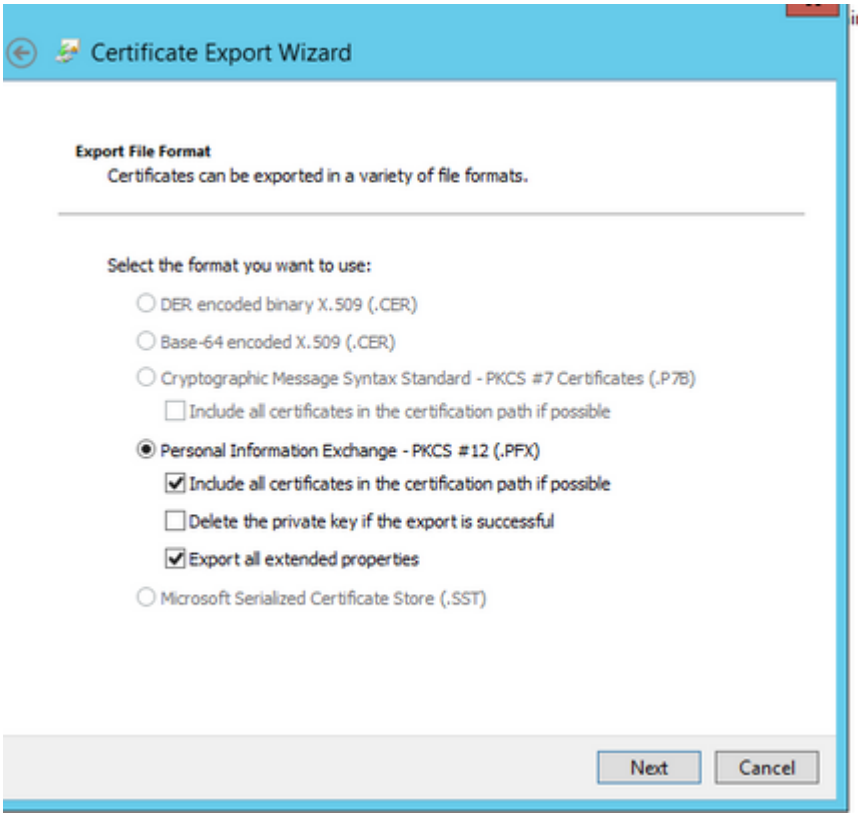


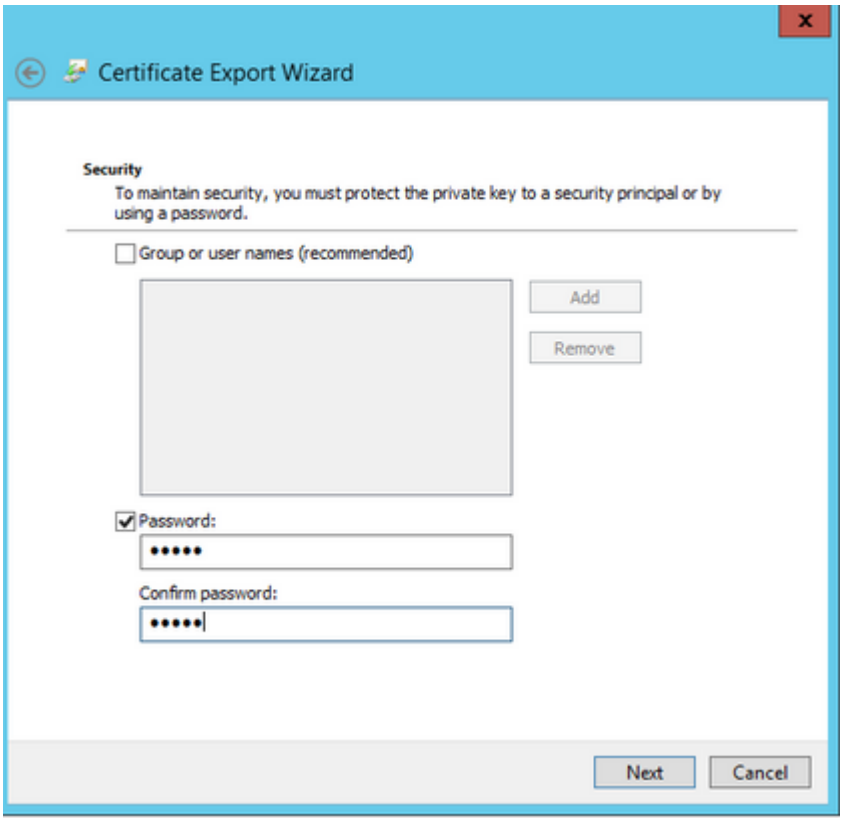
인증서를 내보내고 TMS에 업로드

갱신된 인증서를 개인 키와 함께 내보내려면 다음 단계를 수행합니다.

1단계. Windows Certificate Manager 스냅인을 사용하여 기존 개인 키(인증서 쌍)를 PKCS #12 파일로 내보냅니다.







2단계. Windows Certificate Manager 스냅인을 사용하여 기존 인증서를 Base64 PEM 인코딩 .CER 파일로 내보냅니다. 파일 확장명이 .cer 또는 .crt인지 확인하고 이 파일을 WebEx 클라우드 서비스 팀에 제공합니다.

3단계. Cisco TMS에 로그인하고 관리 도구 > 구성 > WebEx 설정으로 이동합니다. WebEx 사이트 창에서 SSO를 비롯한 모든 설정을 확인합니다.

4단계. Browse(찾아보기)를 클릭하고 WebEx용 인증서 생성에서 생성한 PKS #12 개인 키 인증서(.pfx)를 업로드합니다. 인증서를 생성할 때 선택한 비밀번호 및 기타 정보를 사용하여 SSO 컨피그레이션 필드의 나머지 부분을 완료합니다. 저장을 클릭합니다.

개인 키를 단독으로 사용할 수 있는 경우 다음 OpenSSL 명령을 사용하여 .pem 형식의 서명된 인증서를 개인 키와 결합할 수 있습니다.

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

이제 Cisco TMS에 업로드할 SSO 컨피그레이션의 개인 키가 포함된 Cisco TMS 인증서가 있어야 합니다.

문제 해결

현재 이 설정에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- Cisco CMR(Collaboration Meeting Rooms) 하이브리드 컨피그레이션 가이드(TMS 15.0 -

WebEx Meeting Center WBS30)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.