TMS Certificates with TMS Tools for TLS Communication Configuration 예

목차

소개

이 문서에서는 아웃바운드 연결을 시작할 때 TMS 애플리케이션에서 사용하는 인증서를 구성하기 위해 TMS(TelePresence Management Suite) 도구를 사용하는 방법에 대해 설명합니다. TMS 서버가 도메인의 일부인 경우 TMS 툴에 인증서 생성 옵션이 표시되지 않을 수 있습니다.

사전 요구 사항

요구 사항

Cisco는 다음과 같은 기능을 권장합니다.

- HTTP 및 HTTPS를 통해 설치 및 액세스 가능한 TMS
- IIS(인터넷 정보 서비스) 서버를 다시 시작하는 액세스
- 사용자에 대한 관리자 권한
- 설치해야 하는 TLS(Transport Layer Security) 인증서에 대한 액세스

사용된 구성 요소

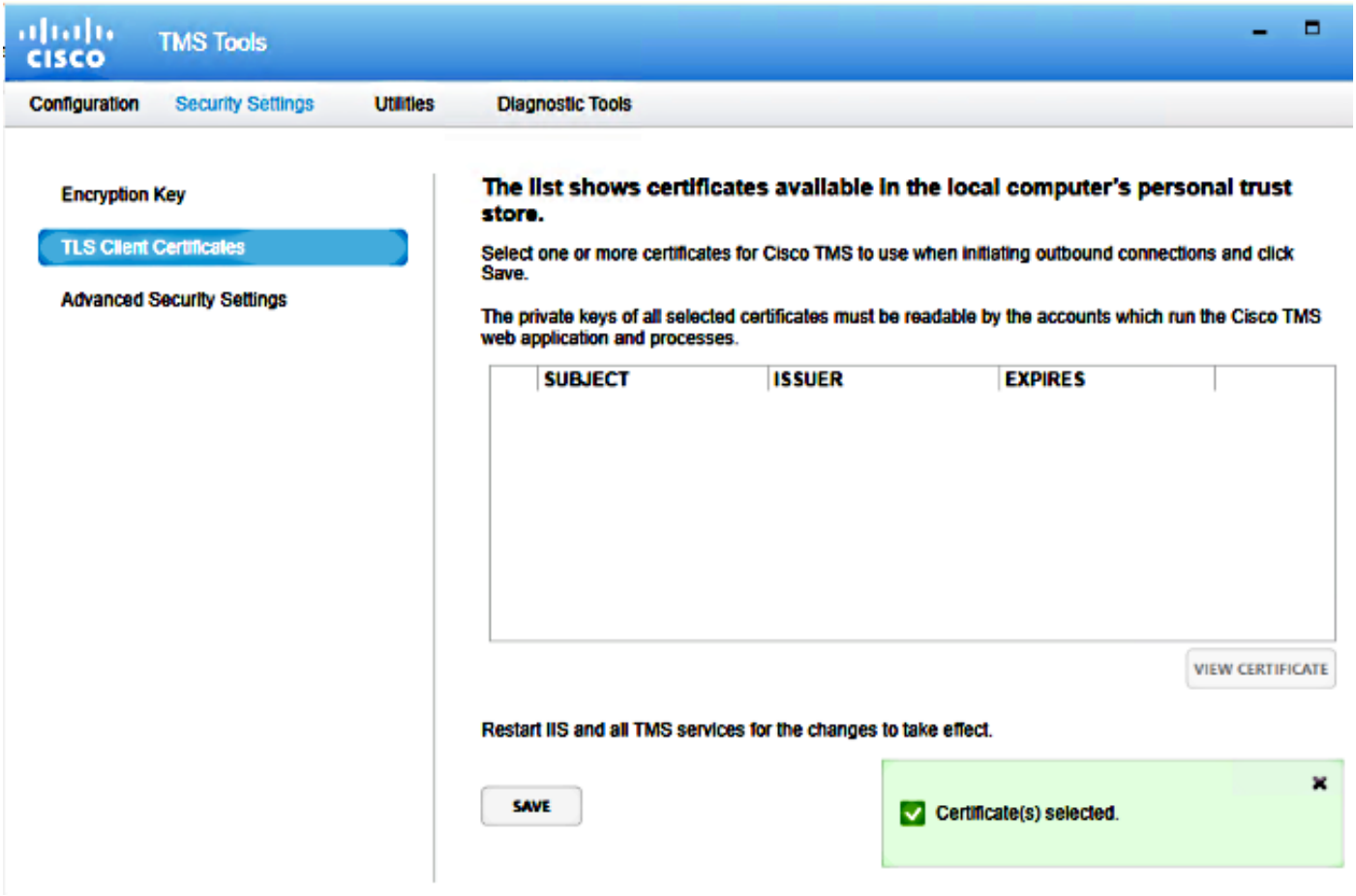
이 문서의 정보는 TMS 버전14.3.2, 14.2.2 및 14.5를 기반으로 합니다.

이 문서의 모든 스크린샷은 TMS 버전 14.5 인터페이스에서 가져온 것입니다. 다른 버전에 대한 인증서는 동일한 절차에 따라 생성할 수도 있습니다.

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

구성

TMS 서버에서 TLS 통신을 완료하고 TMS에서 TLS 인증서를 사용하도록 하려면 TMS 도구를 사용하여 구성해야 합니다.



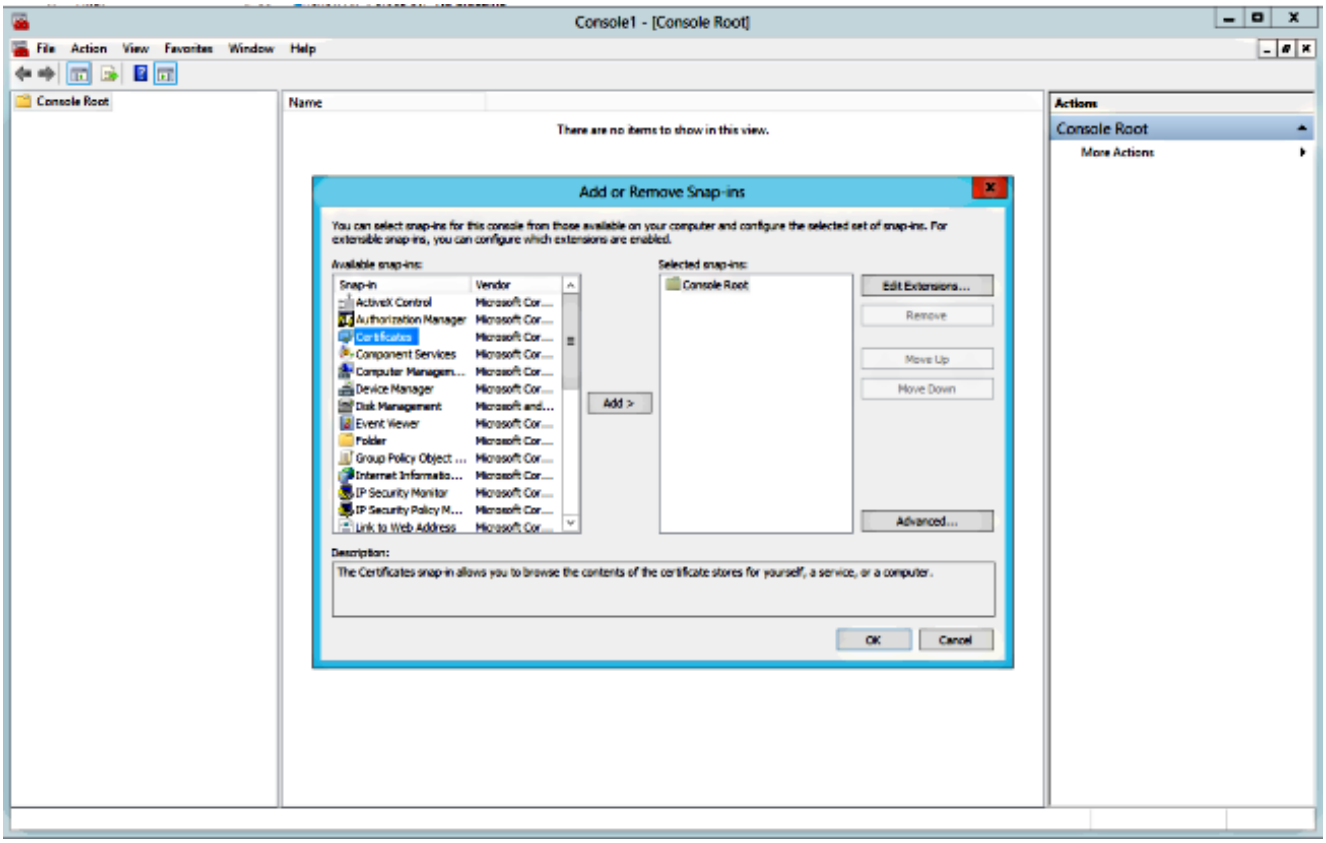
시스템의 개인 인증서 저장소에서 인증서를 볼 수 있습니다. 이 화면에는 서버의 개인 트러스트 저장소에서 현재 사용 가능한 인증서가 이전에 설명한 대로 사용하도록 선택할 수 있습니다.

관리자 가이드에서는 다음과 같은 두 가지 요구 사항이 있습니다.

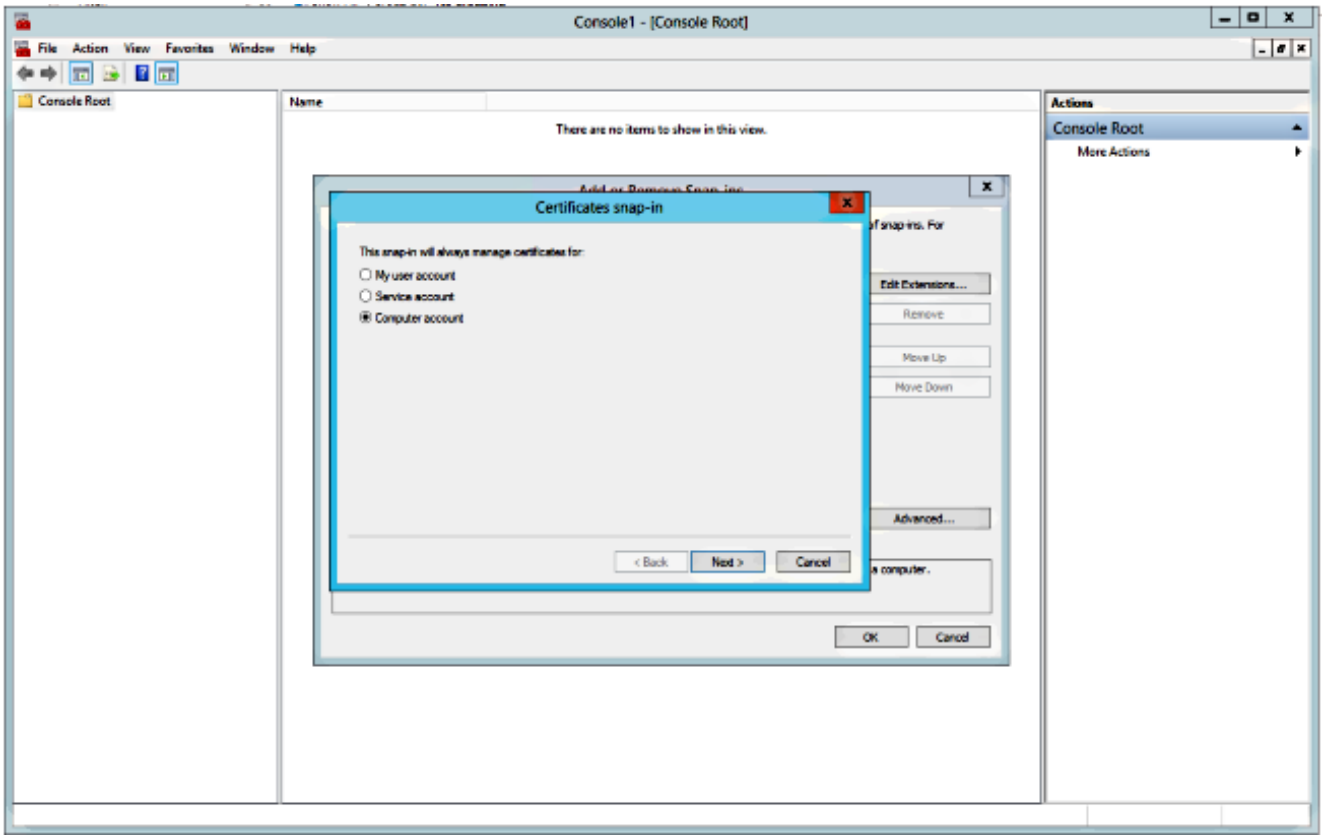
- 여기에 나열된 인증서가 없는 경우 Cisco TMS 툴을 실행하기 위해 사용하는 계정에 인증서의 개인 키에 대한 읽기 권한이 있는지 확인하십시오.
- TMS 서비스가 로그온된 모든 계정에 인증서의 개인 키에 대한 읽기 권한이 있는지 확인합니다 .

개인 트러스트 저장소에 인증서를 설치하려면 MMC(Microsoft Management Console)를 열고 인증서에 대한 스냅인을 추가해야 합니다.

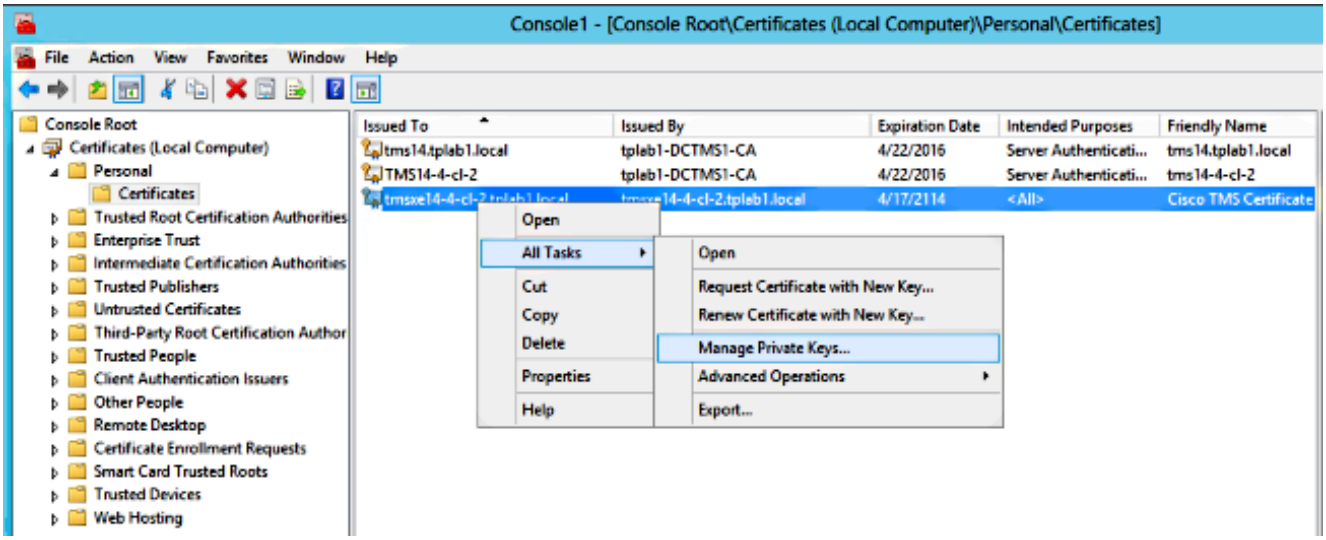
1. Microsoft Windows 서버에서 실행되는 MMC를 엽니다.
2. MMC에서 인증서 스냅인을 추가합니다.



3. **컴퓨터 계정**에 인증서를 추가해야 합니다.

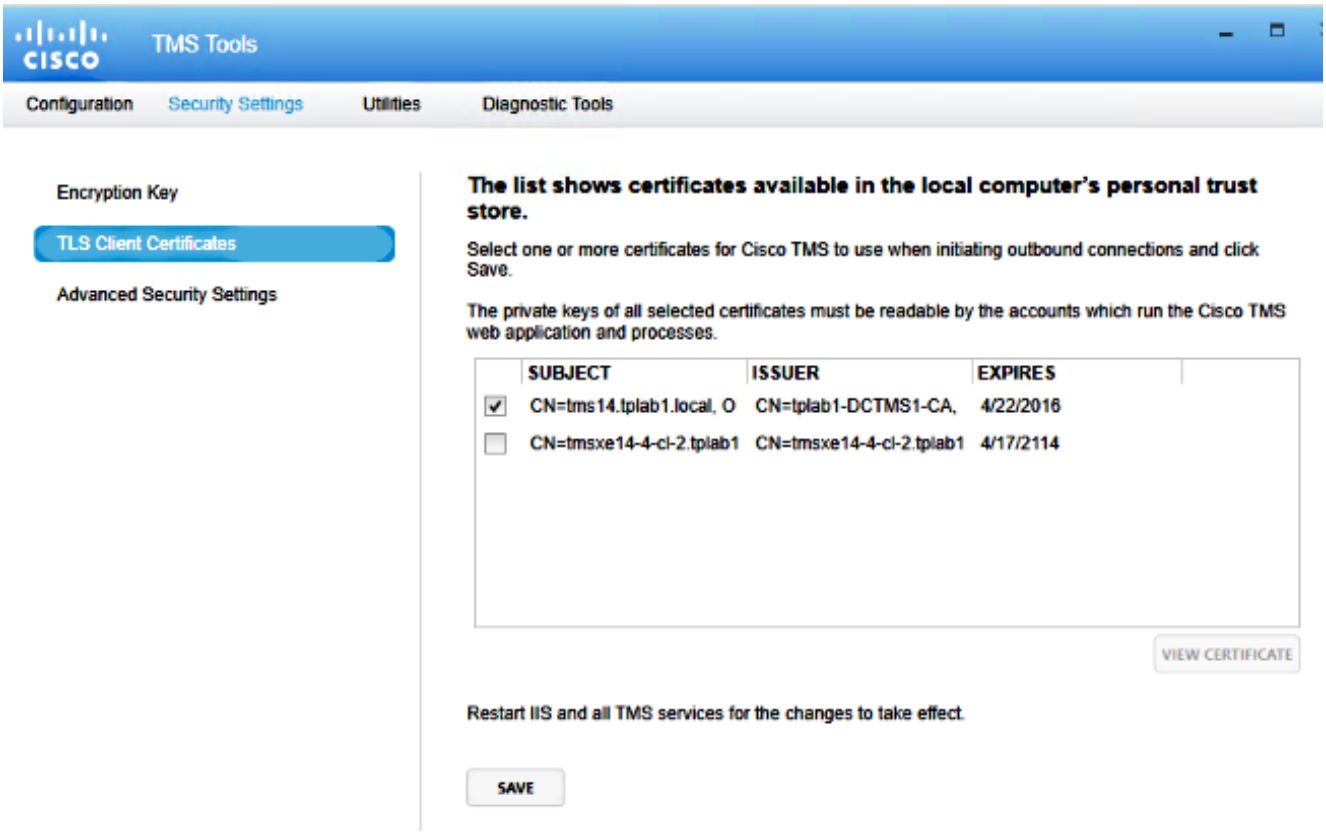


4. Personal(**개인**) **> Certificates(인증서)**에서 인증서를 가져오고 Manage **Private Keys(개인 키 관리)를** 클릭합니다.



5. TMS 툴에 액세스할 수 있는 모든 사용자에게 액세스를 추가하고 읽기 액세스를 제공합니다.

6. TMS **Tools(TMS 툴)**를 열고 **TLS Client Certificates(TLS 클라이언트 인증서)로 이동합니다**.



7. Save(**저장**)를 클릭하고 IIS를 다시 시작합니다.

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.