TMS Certificates with TMS Tools for TLS Communication Configuration 예

목차

<u>소개</u> <u>사전 요구 사항</u> <u>요구 사항</u> <u>사용된 구성 요소</u> <u>구성</u> <u>다음을 확인합니다.</u> <u>문제 해결</u>

소개

이 문서에서는 아웃바운드 연결을 시작할 때 TMS 애플리케이션에서 사용하는 인증서를 구성하기 위해 TMS(TelePresence Management Suite) 도구를 사용하는 방법에 대해 설명합니다. TMS 서버 가 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 인 증서는 동일한 절차에 따라 생성할 수도 있습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다. TMS 서버에서 TLS 통신을 완료하고 TMS에서 TLS 인증서를 사용하도록 하려면 TMS 도구를 사용 하여 구성해야 합니다.



시스템의 개인 인증서 저장소에서 인증서를 볼 수 있습니다. 이 화면에는 서버의 개인 트러스트 저 장소에서 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 인증 서에 대한 스냅인을 추가해야 합니다.

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

·	Console1 - [Console Root]	-	. o x
🖀 File Action View Favorites Window	Help		- 0 ×
(+ +) 🖬 🕞 🖬 🖬			
🚞 Console Root	Name	Actions	
	There are no items to show in this view.	Console Root	
		More Actions	•
	Add or Remove Span-ins X		
	You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.		
	Available snap-ins: Selected snap-ins:		
	Snap-in Vendor A Console Root Edit Extensions		
	Remove Remove		
	Contification Microsoft Cor =		
	Component Services Microsoft Cor Move Up		
	Device Manager Hisrasoft Cor		
	Disk Management Microsoft and 400 >		
	Poller Microsoft Cor		
	Group Policy Object Microsoft Cor		
	B P Security Monitor Microsoft Cor		
	B IP Security Policy M Microsoft Cor		
	Thurk to Web Address Microsoft Cor		
	Description: The /lotificates even is allown use to because the contents of the continue strong for unusual is earlier, or a response		
	The Celonates step in allows you to brank the cancers of the celonates sortes to yoursely a server, or a computer.		
	OK Canol		

3. 컴퓨터 계정에 인증서를 추가해야 합니다.

a	Console1 - [Console Root]	_ 0 X
File Action View Favorites Window	r Help	_ / ×
Console Root	Name	Actions
	There are no items to show in this view.	Console Root
		More Actions
	Add or Domorn Coon inc	
	This anapin will always manage certificates for	
	O My user account O Service account	
	Computer account	
	Move Up	
	Nove Down	
	Advanced < Buck Next > Cancel x computer. OK Cancel	
	1	
L		

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

 File Action View Favorites Window Help File Action View Favorites Window Help Console Root Console Root Certificates (Local Computer) Personal Certificates Trusted Root Certification Authorities Firendly Name Intermediate Certification Authorities Trusted Publishers Trusted Publishers Trusted Publishers Trusted Publishers Trusted Publishers Thrid-Party Root Certification Authorities Third-Party Root Certification Authorities Third-Party Root Certification Authorities 										
	File Action View Favorites Windo									
Issued To Issued By Expiration Date Intended Purposes Friendly Name Intended Purposes Friendly Name Intended Purposes Friendly Name Intermediate Certification Authorities Intermediate Certification Authorities Intermediate Certificates Open Intermediate Certificates Cut Request Certificate with New Key Request Certificate with New Key Introde Purpose Third-Party Root Certification Authorities Delete Manage Private Keys										
▲ ② Certificates (Local Computer) ▲ ③ Personal tplab1-DCTMS1-CA 4/22/2016 Server Authenticati tms14.tplab1.local ▲ ③ Personal ③ Certificates ↓ ③ Trusted Root Certification Authorities ↓ ③ Trusted Root Certification Authorities ↓ ④ Open ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓	Console Root									
▲ Personal Certificates Server Authenticati tmstel 4-4-cl-2 ▶ Trusted Root Certification Authorities Open Cisco TMS Certificate ▶ Intermediate Certification Authorities Open Cisco TMS Certificate ▶ Intermediate Certificates Open Cut Request Certificate with New Key ▶ Untrusted Certificates Cut Request Certificate with New Key Delete ▶ Third-Party Root Certification Authorities Delete Manage Private Keys Delete	Certificates (Local Computer)									
Certificates Intermediate Certification Authorities Intermediate Certification Authorities Open Intermediate Certificates Cut Intrusted Certificates Cut Intrusted Certificates Copy Third-Party Root Certification Authority Delete	a 🧮 Personal									
▷ Trusted Root Certification Authorities ▷ Enterprise Trust ▷ Intermediate Certification Authorities ▷ Trusted Publishers ▷ Untrusted Certificates ▷ Third-Party Root Certification Author ▷ Third-Party Root Certification Author	Certificates									
▷ Enterprise Trust Open ▷ Intermediate Certification Authorities Cut Request Certificate with New Key ▷ Untrusted Certificates Copy Renew Certificate with New Key ▷ Third-Party Root Certification Author Delete Manage Private Keys	Trusted Root Certification Authorities									
p Intermediate Certificate Authorities p Trusted Publishers p Untrusted Certificates p Third-Party Root Certification Author p Third-Party Root Certification Author Delete Manage Private Keys	 Enterprise Trust Intermediate Certification Authorities Trusted Publishers 									
b Untrusted Certificates Copy Renew Certificate with New Key b Third-Party Root Certification Author Delete Manage Private Keys										
Third-Party Root Certification Author Delete Manage Private Keys	Untrusted Certificates									
Delete Manage Private Keys	Third-Party Root Certification Author									
p inusted reopie	Trusted People									
▷ Client Authentication Issuers Properties Advanced Operations ►	Client Authentication Issuers									
Description of the people o	Differ People									
Remote Desktop	Remote Desktop									
Certificate Enrollment Requests	Certificate Enrollment Requests									
Smart Card Trusted Roots	Smart Card Trusted Roots									
Trusted Devices	Trusted Devices									
Web Hosting	Web Hosting									

- 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.

ISCO TMS Tools onfiguration Security Settings	ties Diagnostic Tools
Encryption Key TLS Client Certificates Advanced Security Settings	The list shows certificates available in the local computer's personal trust store. Select one or more certificates for Cisco TMS to use when initiating outbound connections and click save. The private keys of all selected certificates must be readable by the accounts which run the Cisco TM web application and processes. SUBJECT ISSUER EXPIRES CN=tms14.tplab1.local, O CN=tplab1-DCTMS1-CA, 4/22/2016 CN=tmsxe14-4-cl-2.tplab1 CN=tmsxe14-4-cl-2.tplab1
	Restart IIS and all TMS services for the changes to take effect.

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.