# TMS证书与TLS通信工具的TMS配置示例

### 目录

<u>简介</u> <u>先决条件</u> <u>要求</u> 使用的组件 配置 验证 故障排除

### 简介

本文档介绍如何使用网真管理套件(TMS)工具来配置TMS应用在启动出站连接时使用的证书。如果 TMS服务器是域的一部分,则证书创建选项可能在TMS工具上不可见。

### 先决条件

#### 要求

Cisco 建议您:

- •TMS已安装并可通过HTTP和HTTPS访问
- •访问以重新启动Internet信息服务(IIS)服务器
- 用户的管理员权限
- •访问必须安装的传输层安全(TLS)证书

#### 使用的组件

本文档中的信息基于TMS版本14.3.2、14.2.2和14.5。

本文档中的所有屏幕截图都来自TMS 14.5版界面。其他版本的证书也可以使用相同的步骤生成。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。

### 配置

如果希望从TMS服务器完成TLS通信,并且希望TMS使用TLS证书,则必须使用TMS工具对其进行

#### 配置。



您应从系统上的个人证书存储中看到证书。此屏幕列出服务器个人信任存储中当前可用的证书,这 些证书可以选择为按前面所述使用。

管理员指南中提到了以下两个要求,以便列出证书:

如果此处未列出证书,请检查用于运行思科TMS工具的帐户是否具有对证书私钥的读取访问权限。

•确保TMS服务登录的所有帐户都具有对证书私钥的读取访问权限。

要在个人信任存储上安装证书,您需要打开Microsoft管理控制台(MMC)并添加证书管理单元:

1. 打开在Microsoft Windows服务器上运行的MMC。

2. 在MMC上添加证书管理单元:

<b>a</b>	Console1 - [Console Root]	_ 0 X
🖀 File Action View Favorites Window	Help	_ # ×
🗢 🔶 📷 🔂 🖬 📷		
🚞 Console Root	Name	Action
	There are no items to show in this view.	Console Root 🔺
		More Actions +
	Add or Remove Snap-ins	
	You can select map-ins for this consist from those available on your computer and configure the selected set of imap-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	
	T Active? Control Microsoft Cor Authorization Nanager Microsoft Cor Remove	
	Contificator Microsoft Cor 1	
	Component Services Microsoft Cor      Move Up	
	Device Manager Hicrosoft Cor	
	Disk Management Microsoft and Add >	
	Polar Microsoft Cor	
	Group Policy Object Microsoft Cor	
	Platernet Informatio Microsoft Cor	
	D Security Policy N Microsoft Cor	
	Chik to Web Address Microsoft Cor	
	Description:	
	The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.	
	OK Cancel	

3. 确保在计算机帐户中添**加证书**:

<b>a</b>		Console1 - [Console Root]			_ 0 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	<u> </u>
		Add or Domese Coop inc	×		
		Certificates snap-in	f shap ins. For		
		This anap-in will always manage certificates for:			
		O My user account	Edit Extensions		
		Serves account     Econputer account	Renove		
			Move Up		
			Move Down		
	Ţ	< Back Next > Carcel	Advanced a computer. XX Cancel		
the second se					

4. 在"个人">"证**书"上导入证**书,然**后单击"管理私钥**:

<b>*</b>		Console1 - [	Conso	ole R	oot\Certificates (Loc	al Computer)\P	ersonal\Certificates	]
🖀 File Action View Favorites Window	Help							
🗢 🏓 🖄 📷 🔏 🖦 🗶 📾 📓	<b>•••</b>							
Console Root	Issued To		Issued	By		Expiration Date	Intended Purposes	Friendly Name
a 🗇 Certificates (Local Computer)	🕼 tms14.tplab1.loca	1	tplab1	-DCT	MS1-CA	4/22/2016	Server Authenticati	tms14.tplab1.local
a 🧮 Personal	🕼 TM514-4-cl-2		tplab1	-DCT	IMS1-CA	4/22/2016	Server Authenticati	tms14-4-cl-2
Certificates	tmsxe14-4-cl-2 to	lab1.local	tensore	14-4-	cl-2.tplab1.local	4/17/2114	<all></all>	<b>Cisco TMS Certificate</b>
Trusted Root Certification Authorities		Open						
Enterprise Trust		All Tasks	•		Open			
Intermediate Certification Authorities			-	ŀ	-		-	
Trusted Publishers		Cut			Request Certificate with	New Key		
Untrusted Certificates		Сору			Renew Certificate with N	ew Key		
Third-Party Root Certification Author Trusted Basels		Delete	1		Manage Private Keys			
p Instea People b Client Authentication Issuers		Properties	L		Advanced Operations	,	-	
b Cherr People			_	ŀ			-	
b Bemate Deskton		Help			Export			
Certificate Enrollment Requests								
b Smart Card Trusted Roots								
Trusted Devices								
Web Hosting								

- 5. 向所有用户添加访问权限,TMS工具可通过这些权限进行访问并提供读取权限。
- 6. 打开TMS工具并导航至TLS客户端证书:

alialia cisco	TMS Tools								
Configuration	Security Settings	Utilities	Diagnostic Tools						
Encryption TLS Client Advanced S	Coniguration Security Settings Online: 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 TMS 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.		VIEW CERTIFICATE			

7. 单击Save并重新启动IIS。

### 验证

当前没有可用于此配置的验证过程。

## 故障排除

目前没有针对此配置的故障排除信息。