使用TMS工具的TMS證書的TLS通訊配置示例

目錄

簡介

本文說明如何使用TelePresence Management Suite(TMS)工具來配置TMS應用程式在啟動出站連線時使用的證書。如果TMS伺服器是域的一部分，則證書建立選項在TMS工具上可能不可見。

必要條件

需求

思科建議您：

- 安裝並可通過HTTP和HTTPS訪問TMS
- 訪問以重新啟動Internet資訊服務(IIS)伺服器
- 使用者的管理員許可權
- 訪問必須安裝的傳輸層安全(TLS)證書

採用元件

本文檔中的資訊基於TMS版本14.3.2、14.2.2和14.5。

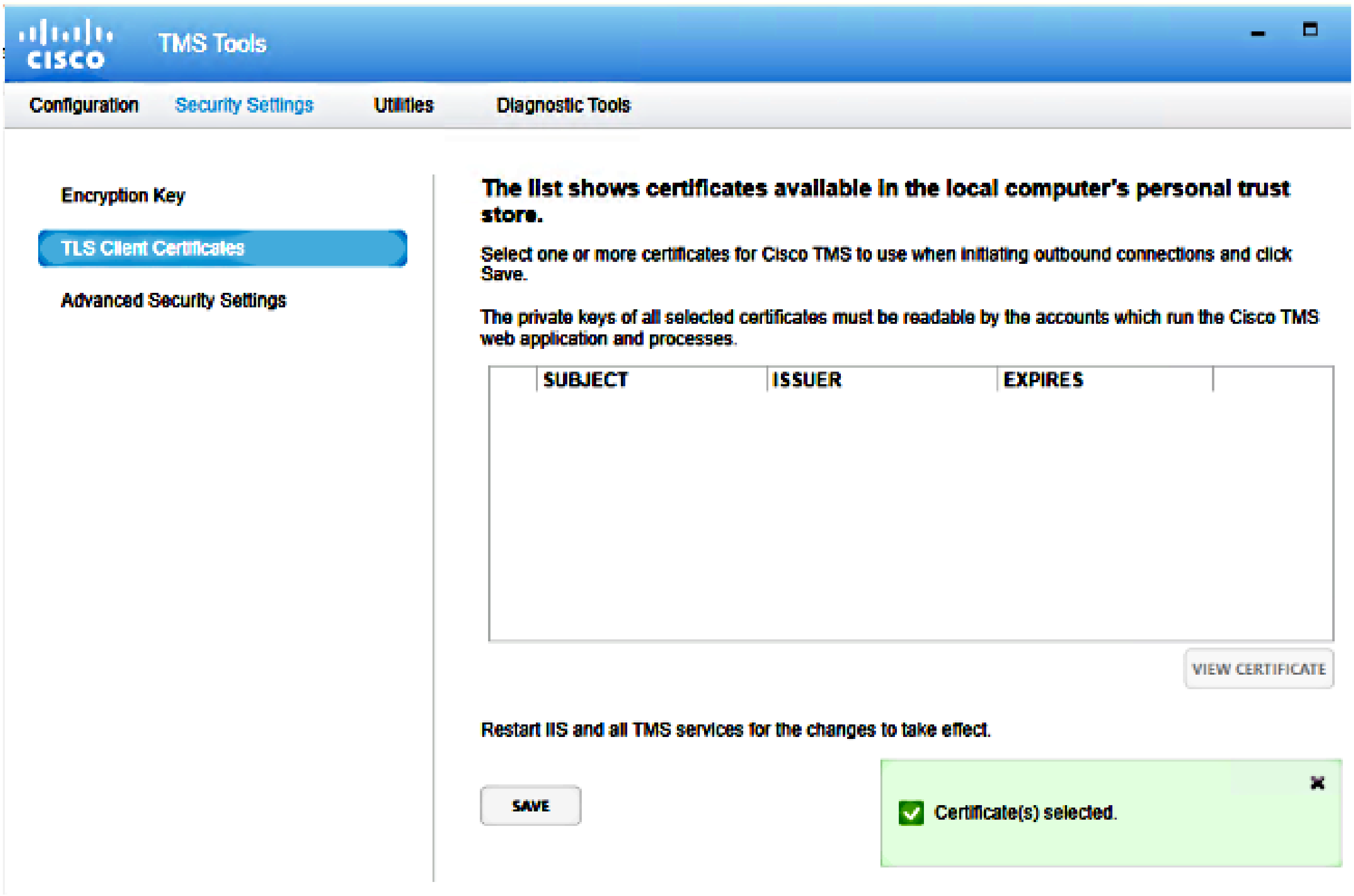
本文檔中的所有螢幕截圖均來自TMS版本14.5介面。也可以使用相同的過程生成其他版本的證書。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

如果您希望從TMS伺服器獲得完整的TLS通訊，並且希望TMS使用TLS證書，則必須使用TMS工具

進行配置。



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

Restart IIS and all TMS services for the changes to take effect.

✓ Certificate(s) selected.

您應該從系統上的個人證書儲存看到此處的證書。此螢幕列出了伺服器的個人信任儲存中當前可用的證書，這些證書可以按照前面所述選擇使用。

管理指南中提及的兩個要求用於此處列出的證書：

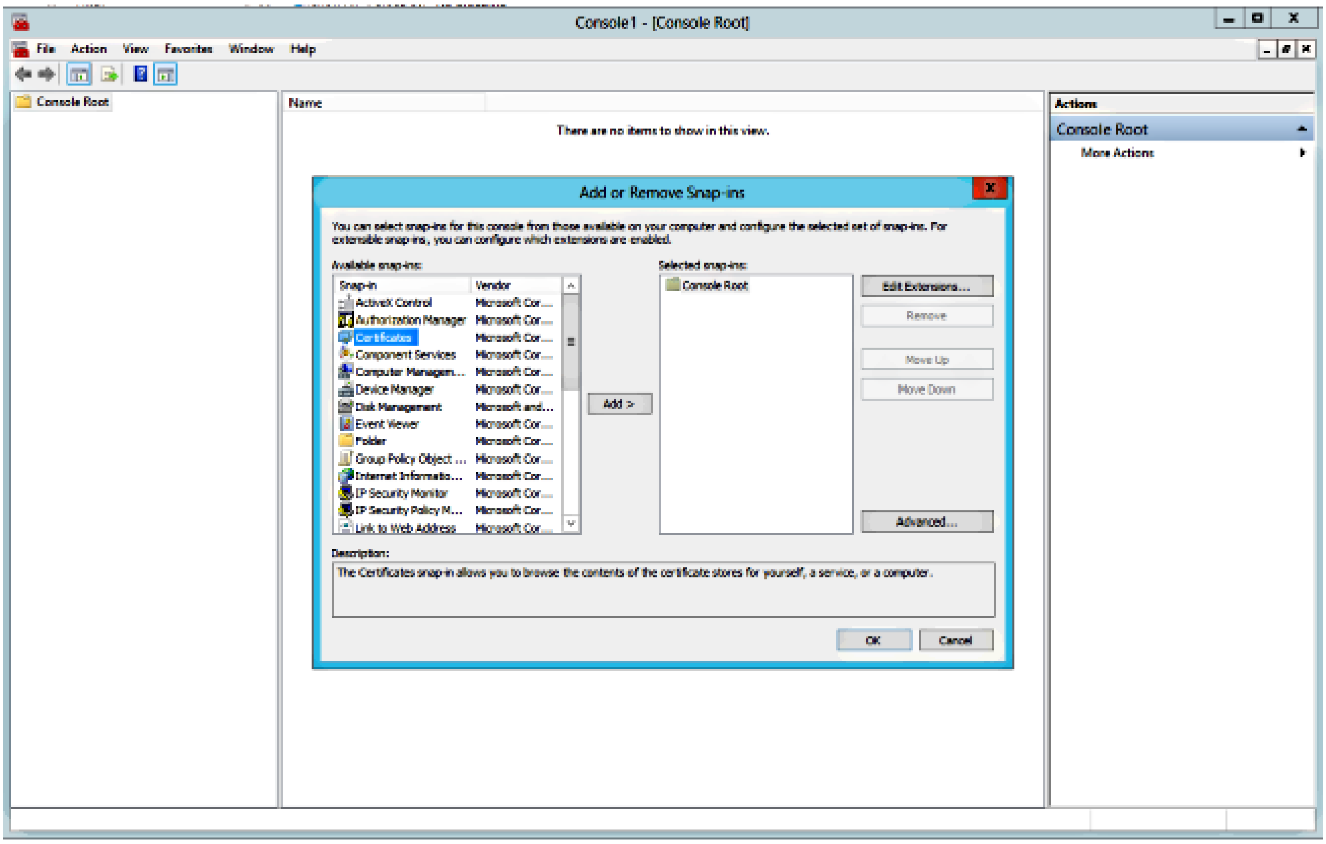
- 如果此處未列出任何證書，請檢查您用於運行Cisco TMS工具的帳戶是否具有對這些證書私鑰的讀取訪問許可權。

- 確保TMS服務登入的所有帳戶都具有對證書私鑰的讀取訪問許可權。

若要在個人信任儲存上安裝證書，需要開啟Microsoft管理控制檯(MMC)並為證書新增管理單元：

1. 在Microsoft Windows伺服器上運行開啟MMC。

2. 在MMC上新增證書管理單元：



Add or Remove Snap-ins

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:

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
Internet Informatio...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...
Link to Web Address	Microsoft Cor...

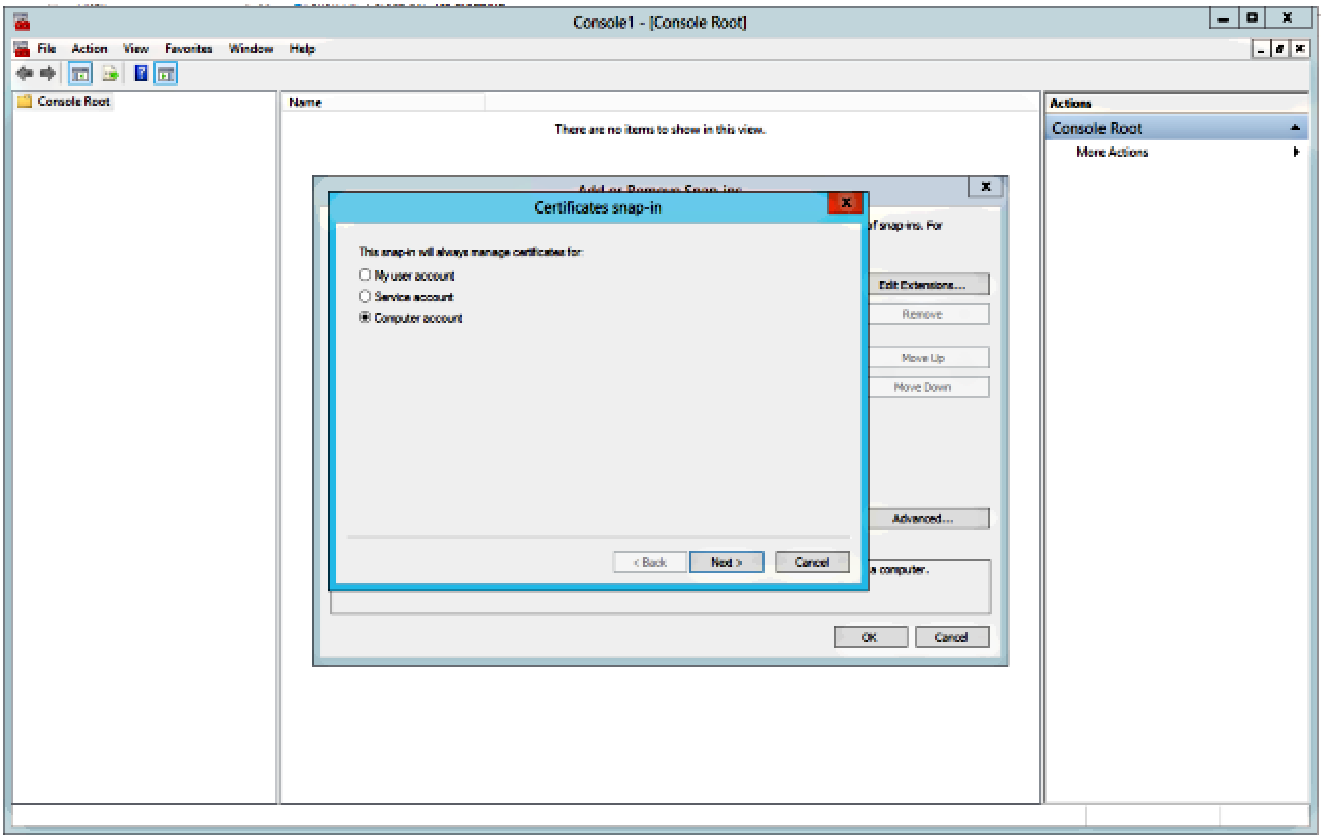
Selected snap-ins:

Console Root

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

3. 確保在**Computer account**：（電腦帳戶：）中添**加證書。**



Certificates snap-in

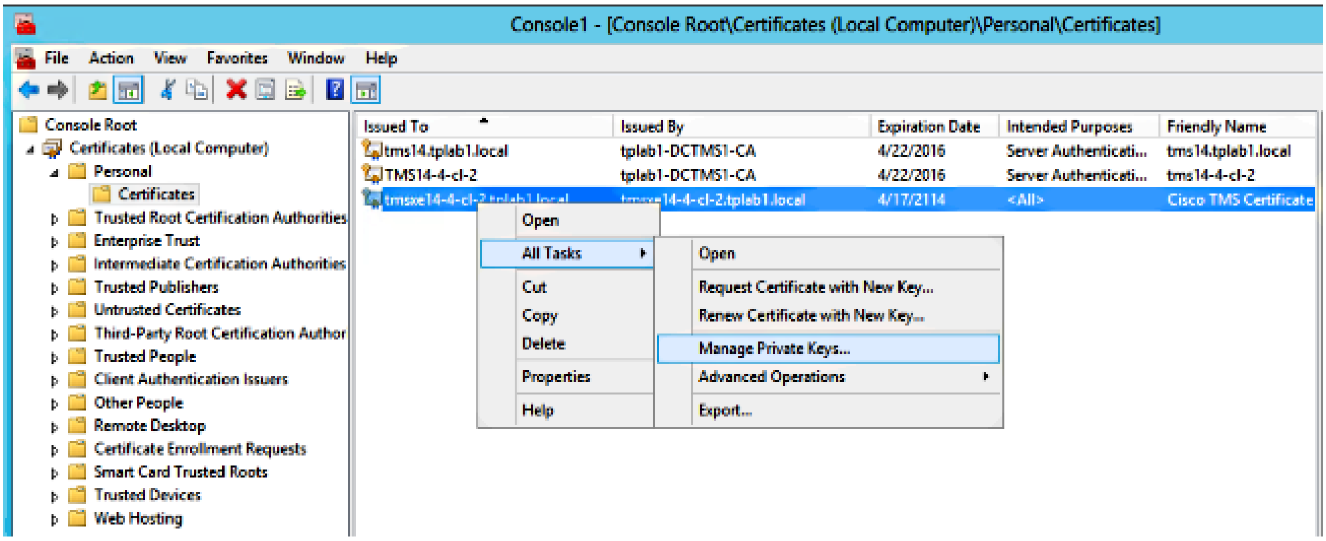
This snap-in will always manage certificates for:

○ My user account

○ Service account

● Computer account

4. 在**Personal > Certificates**上匯入證書，然後按一下**Manage Private Keys**:

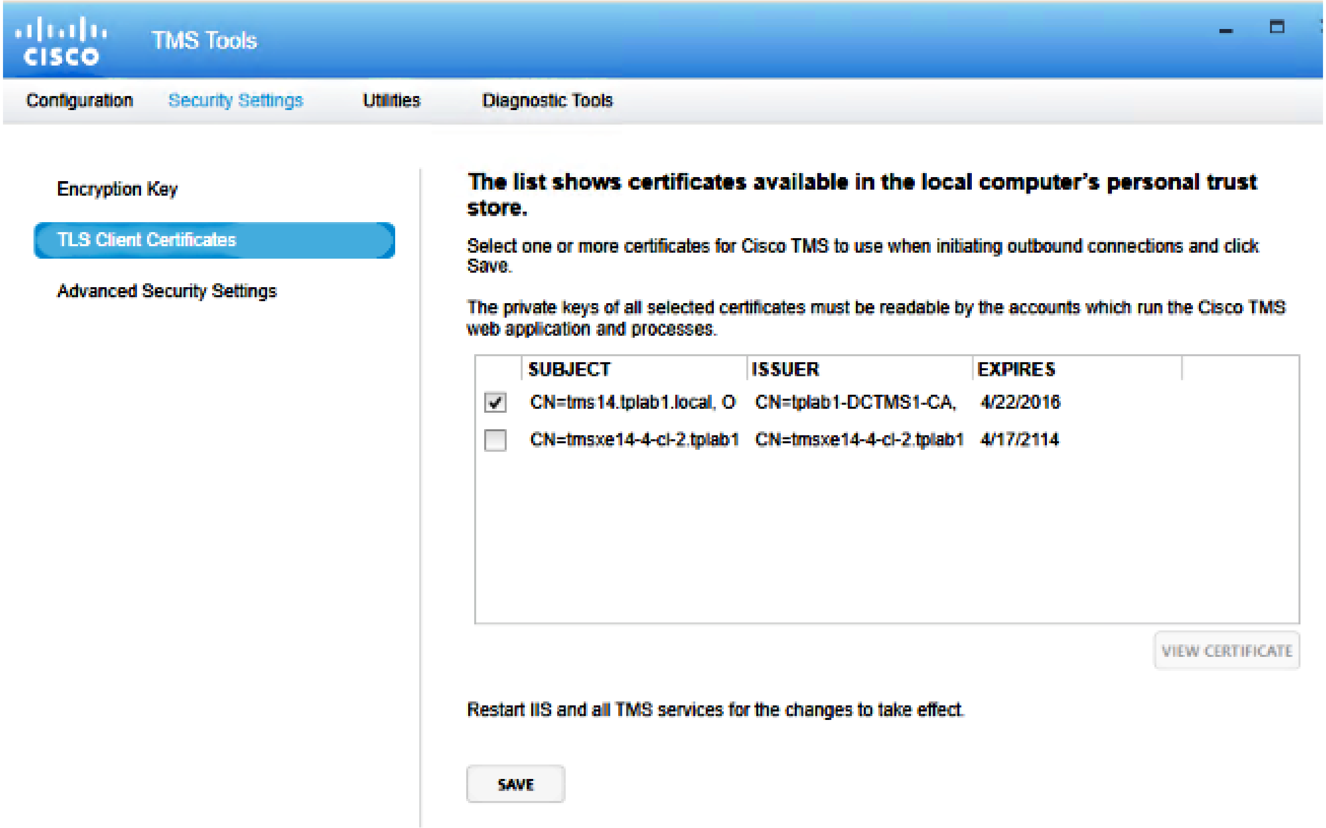


Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Author
Trusted People
Client Authentication Issuers
Other People
Remote Desktop
Certificate Enrollment Requests
Smart Card Trusted Roots
Trusted Devices
Web Hosting
Open
All Tasks
Cut
Copy
Delete
Properties
Help
Open
Request Certificate with New Key...
Renew Certificate with New Key...
Manage Private Keys...
Advanced Operations
Export...

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
tms14.tplab1.local	tplab1-DCTMS1-CA	4/22/2016	Server Authenticati...	tms14.tplab1.local
TMS14-4-cl-2	tplab1-DCTMS1-CA	4/22/2016	Server Authenticati...	tms14-4-cl-2
tmsxe14-4-cl-2.tplab1.local	tmsxe14-4-cl-2.tplab1.local	4/17/2114	<All>	Cisco TMS Certificate

5. 新增對TMS工具可通過其訪問的所有使用者的訪問許可權，並提供讀取訪問許可權。

6. 開啟**TMS工具**並導航到**TLS客戶端證書**:



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	4/17/2114

Restart IIS and all TMS services for the changes to take effect.

7. 按一下**Save**並重新啟動IIS。

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。