

TLS 通信用の TMS ツールを使用した TMS 証明書の設定例

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

概要

このドキュメントでは、TelePresence Management Suite(TMS)ツールを使用して、発信接続を開始するときにTMSアプリケーションによって使用される証明書を設定する方法について説明します。TMSサーバがドメインの一部である場合、TMSツールに証明書作成オプションが表示されない可能性があります。

前提条件

要件

Cisco では次の前提を満たす推奨しています。

- TMSがインストールされ、HTTPおよびHTTPSからアクセス可能
- インターネットインフォメーションサービス(IIS)サーバを再起動するためのアクセス
- ユーザーの管理者権限
- インストールする必要があるTransport Layer Security(TLS)証明書へのアクセス

使用するコンポーネント

このドキュメントの情報は、TMSバージョン14.3.2、14.2.2、および14.5に基づくものです。

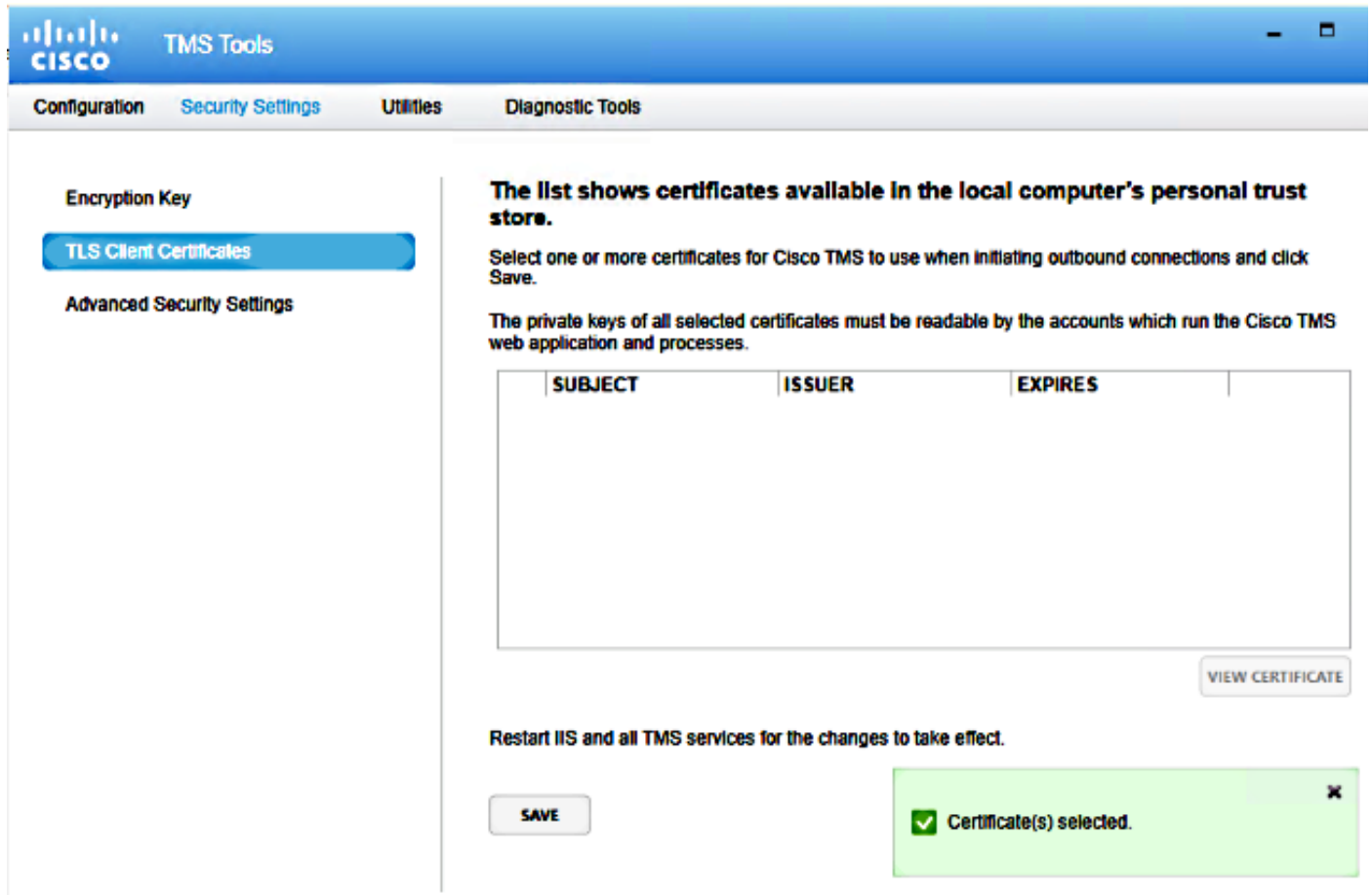
このドキュメントのすべてのスクリーンショットは、TMSバージョン14.5インターフェイスのもので、他のバージョンの証明書も、同じ手順で生成できます。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが稼働中である場合には、どのようなコマンドについても、その潜在的

な影響について確実に理解しておく必要があります。

設定

TMSサーバから完全なTLS通信を行い、TMSでTLS証明書を使用する場合は、TMSツールで設定する必要があります。



The screenshot shows the Cisco TMS Tools interface. The top navigation bar includes 'Configuration', 'Security Settings', 'Utilities', and 'Diagnostic Tools'. The 'Security Settings' section is active, with 'Encryption Key' and 'Advanced Security Settings' as sub-sections. The 'TLS Client Certificates' section is highlighted. The main content area displays the following text:

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
---------	--------	---------

VIEW CERTIFICATE

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

SAVE

Certificate(s) selected.

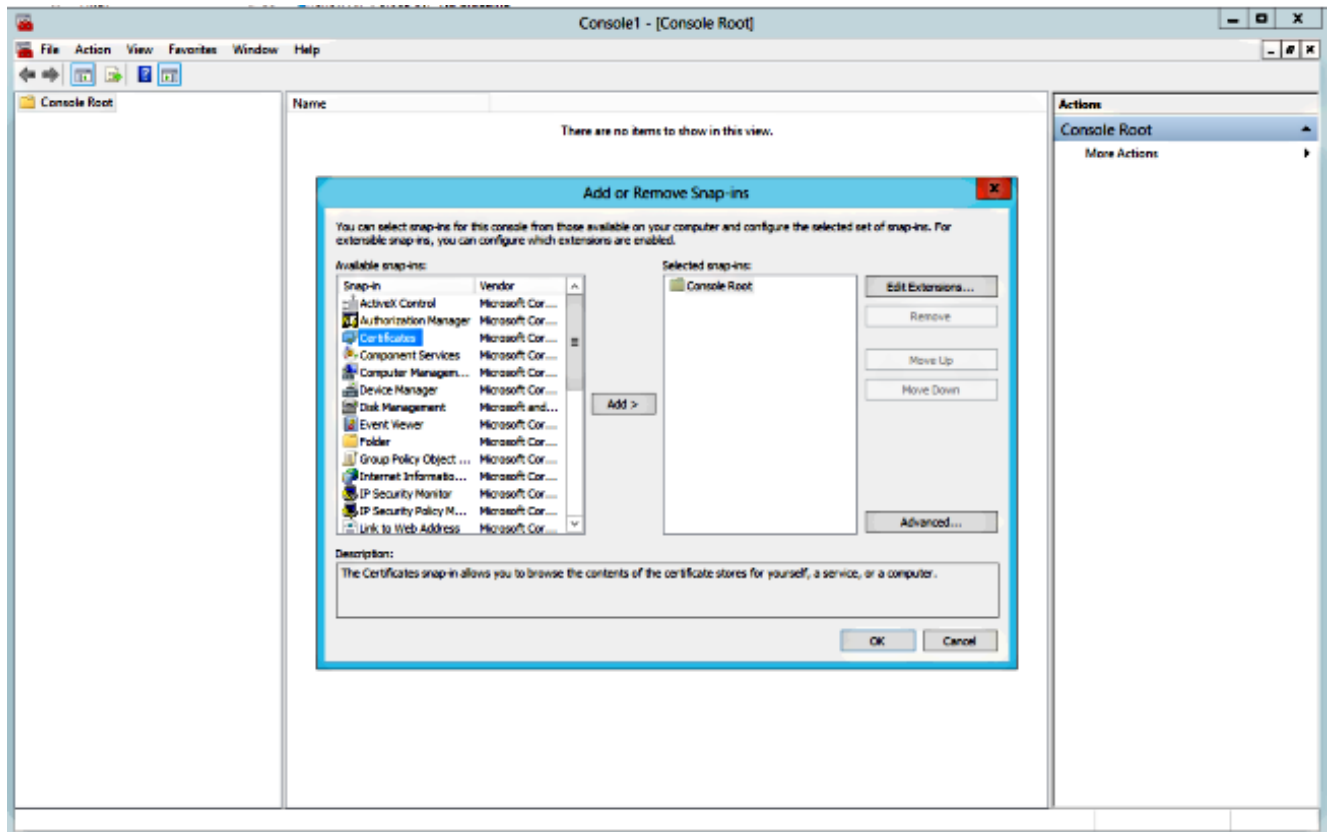
システムの個人証明書ストアから証明書が表示されます。この画面には、サーバの個人信頼ストアで現在使用可能な証明書が一覧表示されます。この証明書は、前述のように選択して使用できます。

次に示す証明書の管理者ガイドには、2つの要件が記載されています。

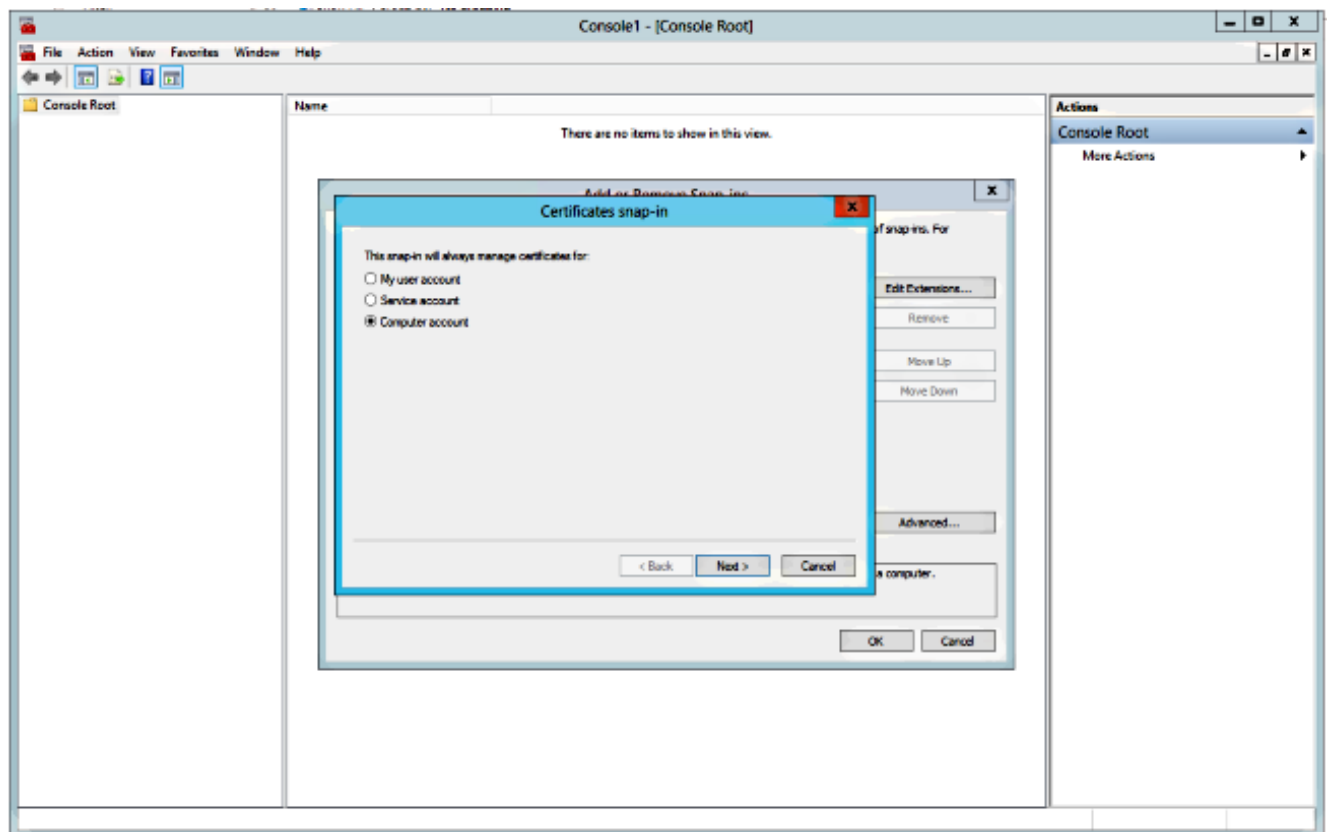
- ここに証明書がリストされていない場合は、Cisco TMSツールを実行するために使用するアカウントに、証明書の秘密キーへの読み取りアクセス権があることを確認します。
- TMSサービスがログオンしているすべてのアカウントが、証明書の秘密キーに読み取りアクセスできることを確認します。

個人信頼ストアに証明書をインストールするには、Microsoft管理コンソール(MMC)を開き、証明書のスナップインを追加する必要があります。

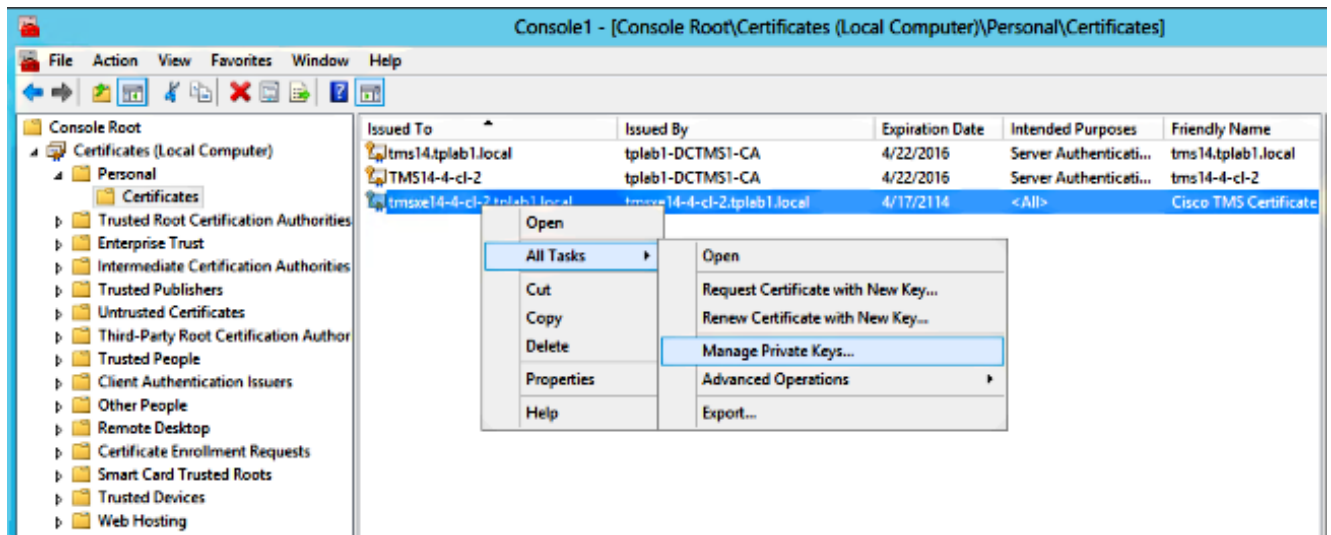
- Microsoft Windowsサーバで実行するMMCを開きます。
- MMCで証明書スナップインを追加します。



3. 証明書がコンピュータアカウントに追加されていることを確認してください。

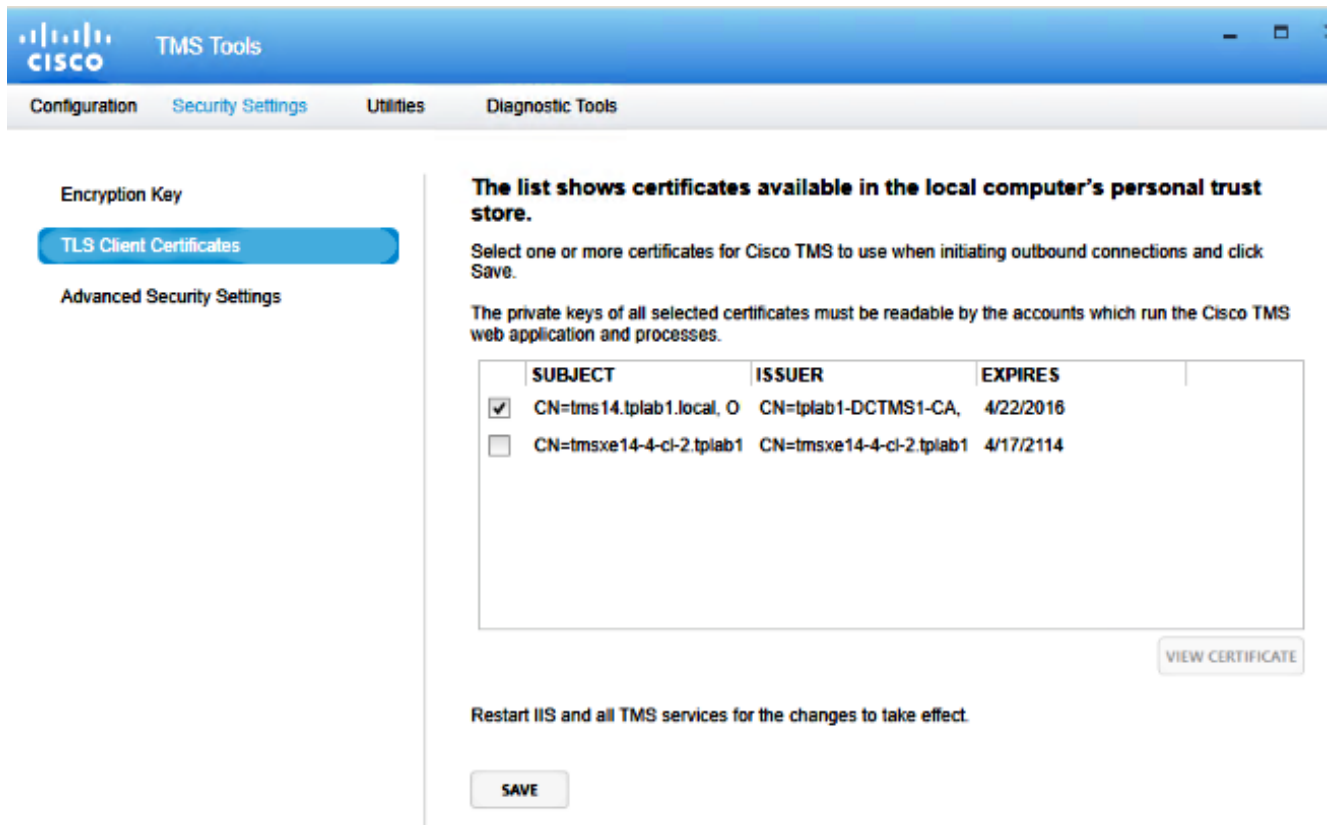


4. [Personal] > [Certificates]で証明書をインポートし、[Manage Private Keys]をクリックします。



5. TMSツールにアクセスできるすべてのユーザにアクセス権を追加し、読み取りアクセス権を付与します。

6. TMSツールを開き、[TLS Client Certificates]に移動します。



7. [Save]をクリックし、IISを再起動します。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。