

# Certificats TMS avec des outils TMS pour l'exemple de configuration de transmission de TLS

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composant utilisé](#)

[Configurez](#)

[Vérifiez](#)

[Dépannez](#)

## Introduction

Ce document décrit comment utiliser l'outil de la suite de gestion TelePresence (TMS) afin de configurer le certificat utilisé par l'application TMS quand il initie les connexions sortantes. Si le serveur TMS est une partie d'un domaine, alors l'option de création de certificat ne pourrait pas être visible sur l'outil TMS.

## Conditions préalables

### Conditions requises

Cisco recommande que vous ayez :

- HTTP TMS et HTTPS par installés et accessibles
- Access pour redémarrer le serveur de l'Internet Information Services (IIS)
- Juste d'admin pour l'utilisateur
- Access au certificat de Transport Layer Security (TLS) qui doit être installé

### Composant utilisé

Les informations dans ce document sont basées sur TMS Versions 14.3.2, 14.2.2, et 14.5.

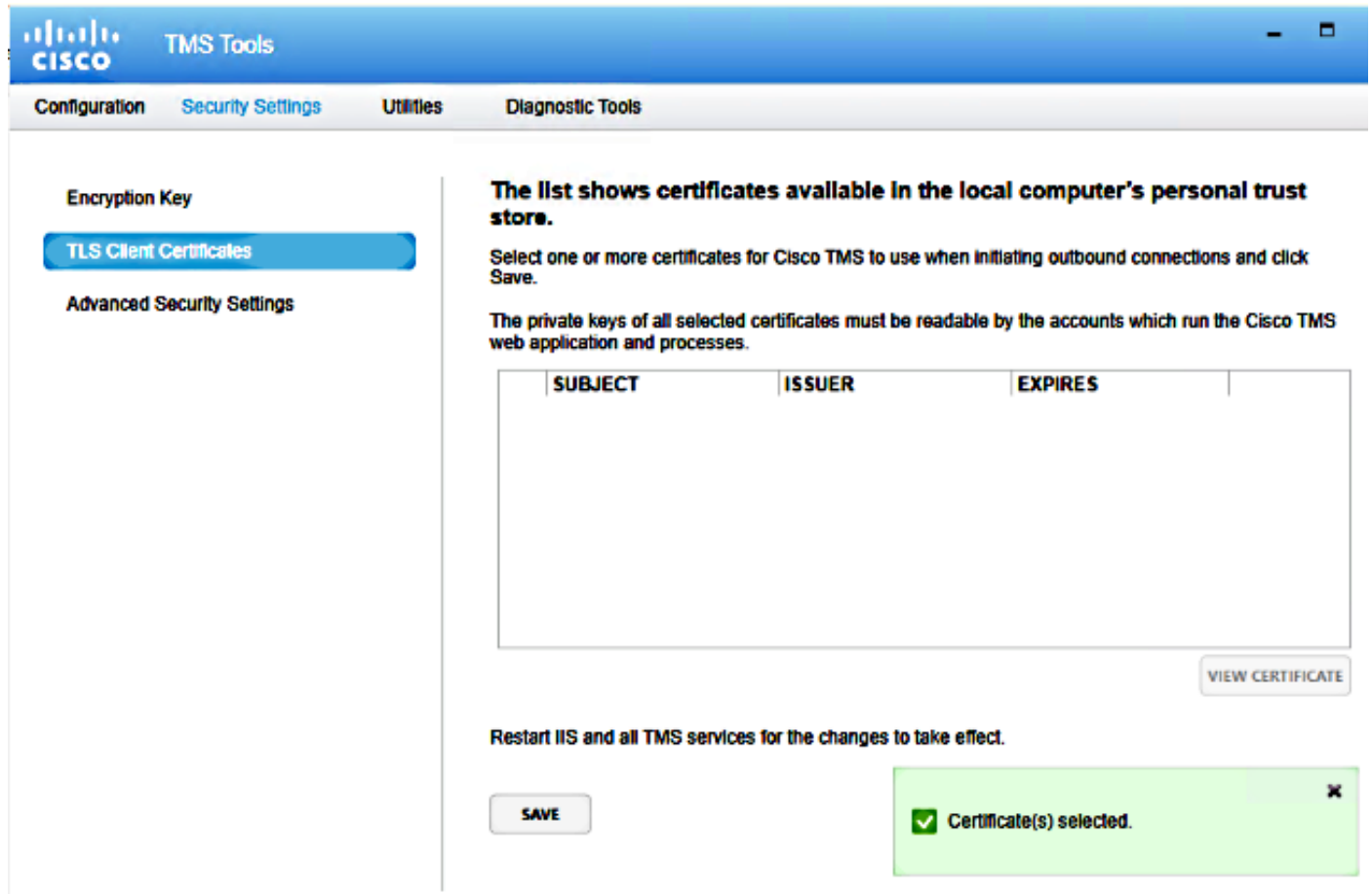
Toutes les captures d'écran dans ce document sont de l'interface de version 14.5 TMS. Des Certificats pour d'autres versions peuvent également être générés avec la même procédure.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un

environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

## Configurez

Quand vous voulez faire vouloir la transmission complète de TLS du serveur et de vous TMS que TMS utilise un certificat de TLS, vous devez le configurer avec les outils TMS.



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, showing 'Encryption Key' with sub-options 'TLS Client Certificates' (selected) and 'Advanced Security Settings'. The main content area displays instructions: 'The list shows certificates available in the local computer's personal trust store.' and 'Select one or more certificates for Cisco TMS to use when initiating outbound connections and click Save.' Below this is a table with columns 'SUBJECT', 'ISSUER', and 'EXPIRES', which is currently empty. A 'VIEW CERTIFICATE' button is located at the bottom right of the table. A note states: 'The private keys of all selected certificates must be readable by the accounts which run the Cisco TMS web application and processes.' At the bottom, there is a 'SAVE' button and a green notification box that says 'Certificate(s) selected.' with a close button (X).

Vous devriez voir le certificat ici de la mémoire personnelle de certificat sur le système. Cet écran répertorie les Certificats actuellement disponibles dans la mémoire personnelle de la confiance du serveur qui peut être sélectionnée pour être utilisée comme décrit précédemment.

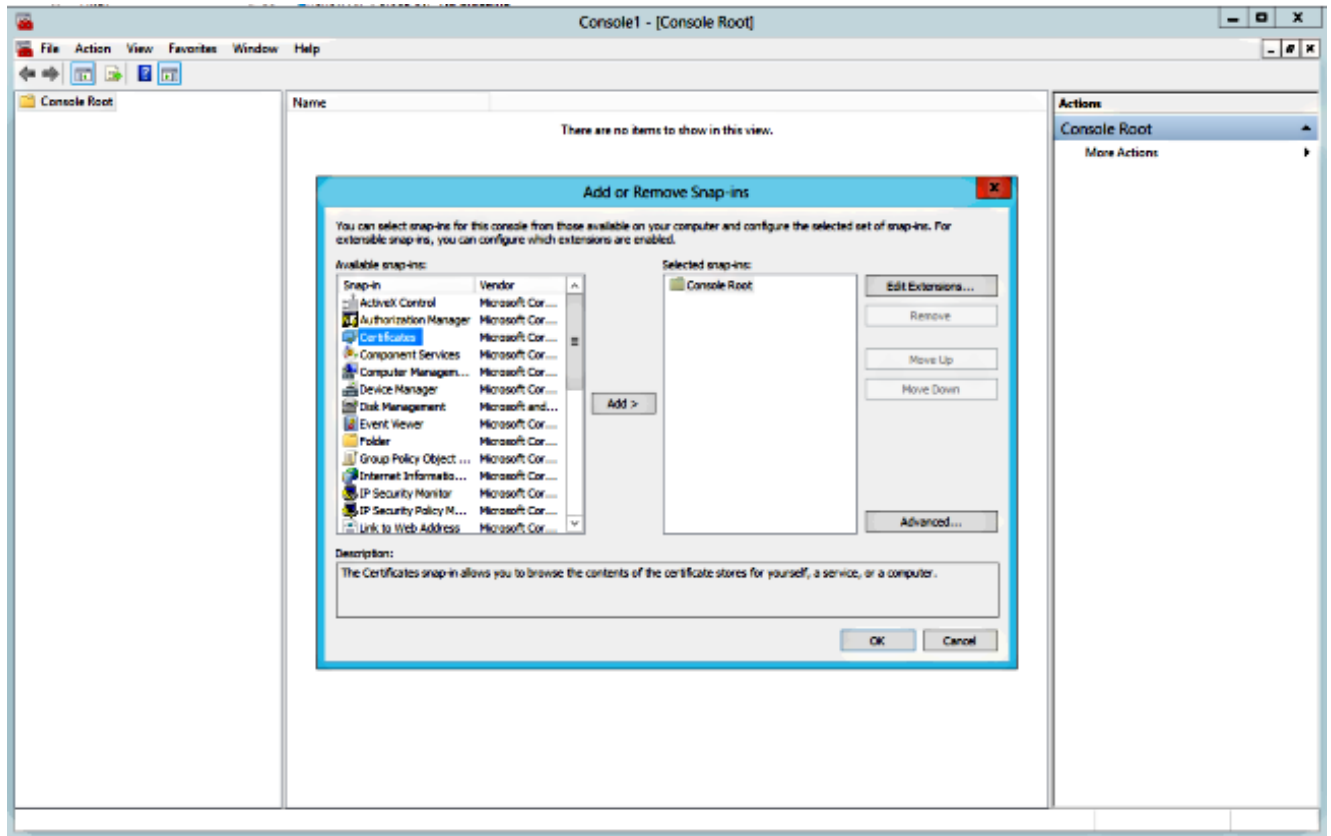
Il y a la condition requise deux mentionnée du guide d'admin pour que le certificat soit répertorié ici :

- S'il n'y a aucun Certificats répertorié ici, vérifiez que le compte que vous utilisez afin d'exécuter des outils de Cisco TMS a l'accès en lecture aux clés privées des Certificats.
- Assurez-vous que tout rend compte les services TMS est ouvert une session a l'accès en lecture aux clés privées des Certificats.

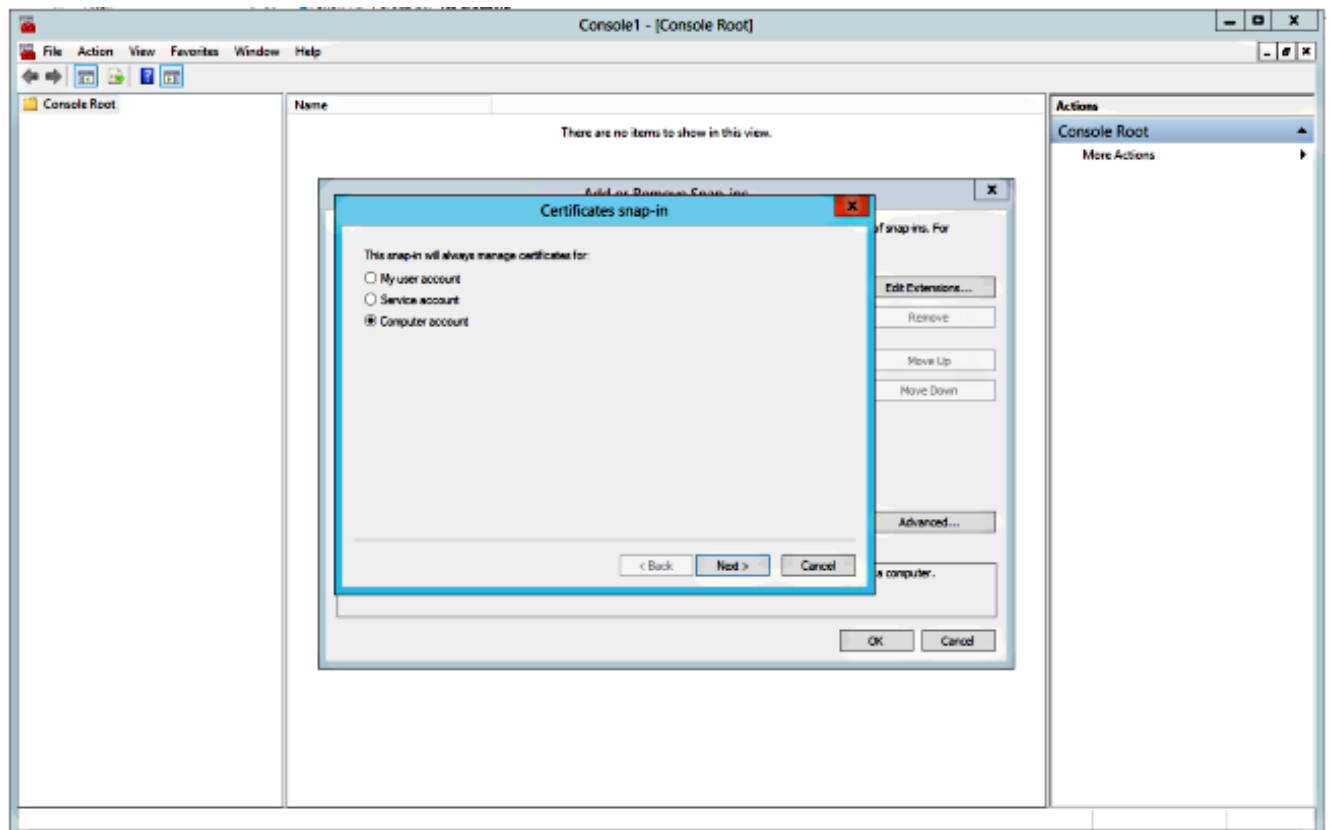
Afin d'installer un certificat sur une mémoire personnelle de confiance, vous devez ouvrir Microsoft Management Console (MMC) et ajouter SNAP-dans pour le certificat :

1. Ouvrez le MMC avec le passage sur le serveur de Microsoft Windows.

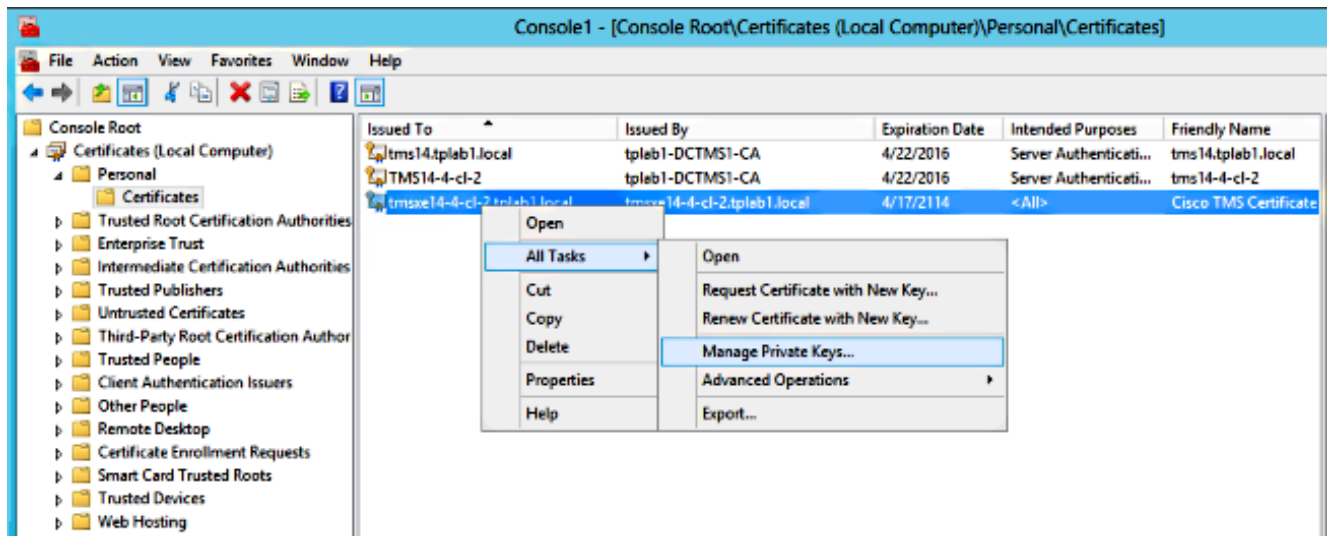
2. Ajoutez le certificat SNAP-dans sur le MMC :



3. Assurez-vous que vous ajoutez le certificat dans le compte d'ordinateur :

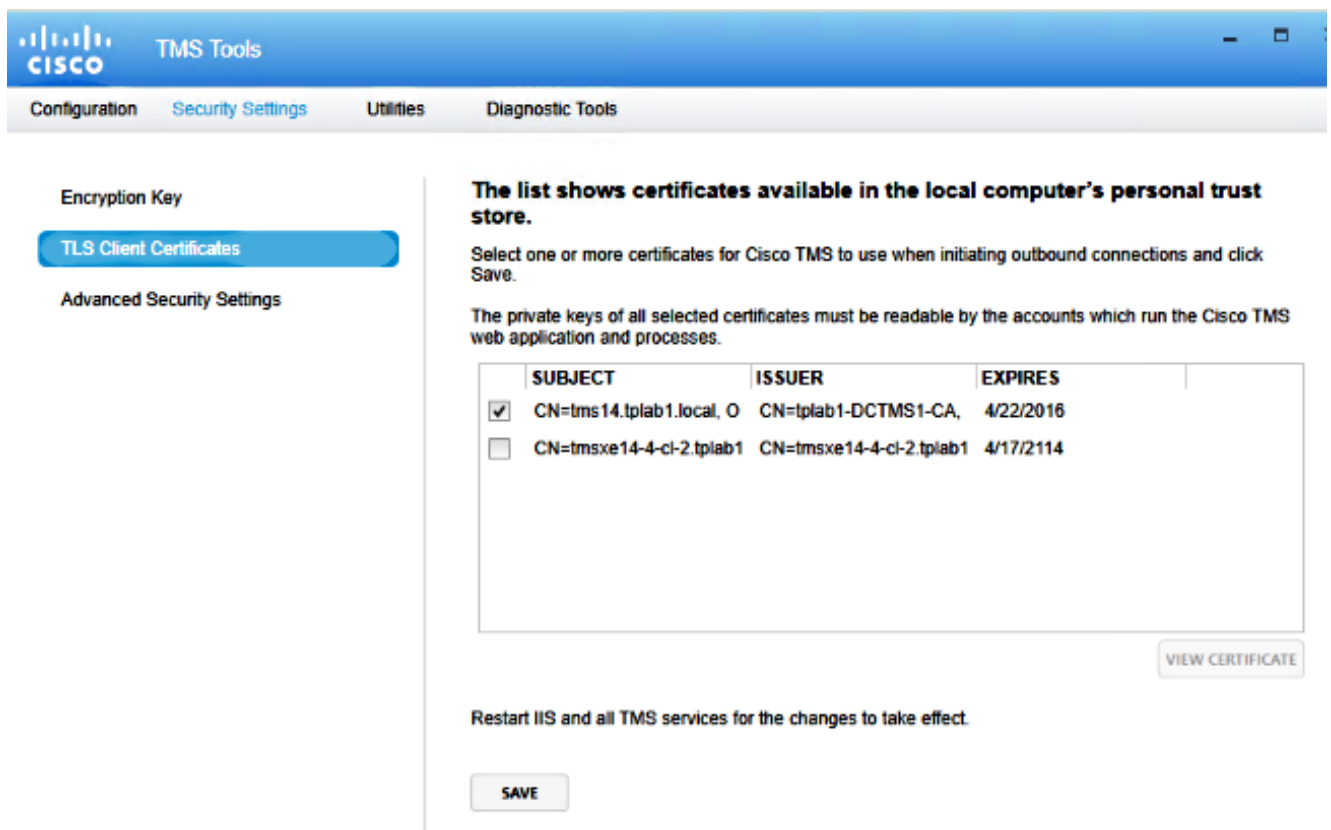


4. Importez le certificat sur **personnel > des Certificats** et le clic **gèrent des clés privées** :



5. Ajoutez l'accès à tous les utilisateurs par lesquels l'outil TMS peut être accédé à et fournir l'accès en lecture.

6. Ouvrez les outils TMS et naviguez vers des certificats client de TLS :



7. Sauvegarde et reprise IIS de clic.

## Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

## Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.