

TMS-Zertifikate mit TMS-Tools für TLS-Kommunikationskonfigurationsbeispiel

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponente](#)

[Konfigurieren](#)

[Überprüfung](#)

[Fehlerbehebung](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie das Tool TelePresence Management Suite (TMS) verwenden, um das von der TMS-Anwendung verwendete Zertifikat zu konfigurieren, wenn diese ausgehende Verbindungen initiiert. Wenn der TMS-Server Teil einer Domäne ist, wird die Option zum Erstellen von Zertifikaten möglicherweise nicht im TMS-Tool angezeigt.

Voraussetzungen

Anforderungen

Cisco empfiehlt Folgendes:

- Installation und Zugriff von TMS über HTTP und HTTPS
- Zugriff auf den Neustart des IIS-Servers (Internetinformationsdienste)
- Administratorrechte für den Benutzer
- Zugriff auf das zu installierende Transport Layer Security (TLS)-Zertifikat

Verwendete Komponente

Die Informationen in diesem Dokument basieren auf den TMS-Versionen 14.3.2, 14.2.2 und 14.5.

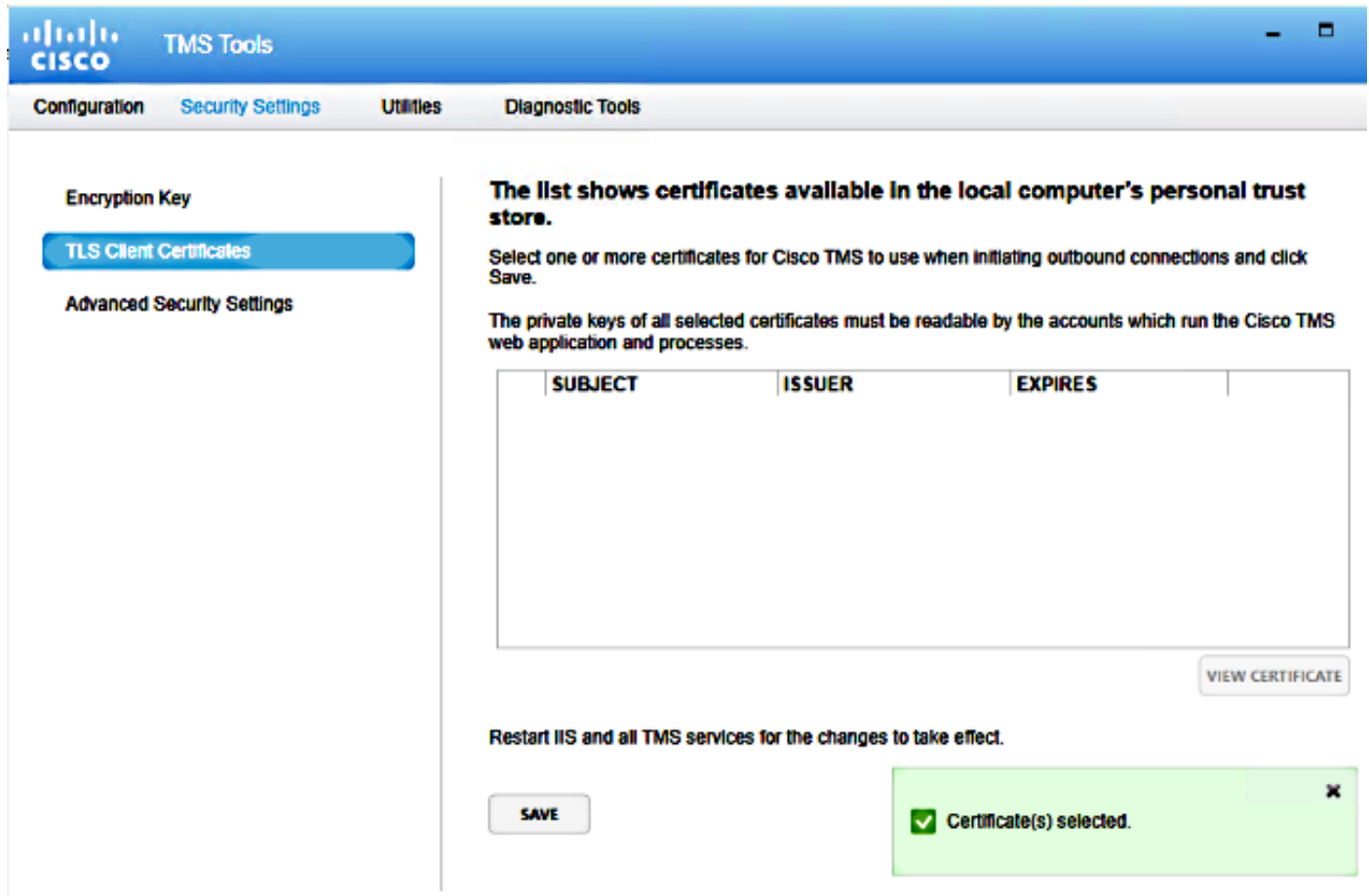
Alle Screenshots in diesem Dokument stammen von der Schnittstelle TMS Version 14.5. Zertifikate für andere Versionen können auch mit derselben Prozedur generiert werden.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die

mögliche Auswirkung jedes möglichen Befehls verstehen.

Konfigurieren

Wenn Sie eine vollständige TLS-Kommunikation vom TMS-Server wünschen und TMS ein TLS-Zertifikat verwenden soll, müssen Sie es mit den TMS-Tools konfigurieren.



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' selected. Under 'Encryption Key', 'TLS Client Certificates' is highlighted. Below it, 'Advanced Security Settings' is visible. 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.' 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.' Below this is a table with columns 'SUBJECT', 'ISSUER', and 'EXPIRES'. A 'VIEW CERTIFICATE' button is located at the bottom right of the table. Below the table, a note says 'Restart IIS and all TMS services for the changes to take effect.' A 'SAVE' button is at the bottom left. A green notification box at the bottom right shows a checkmark and the text 'Certificate(s) selected.'

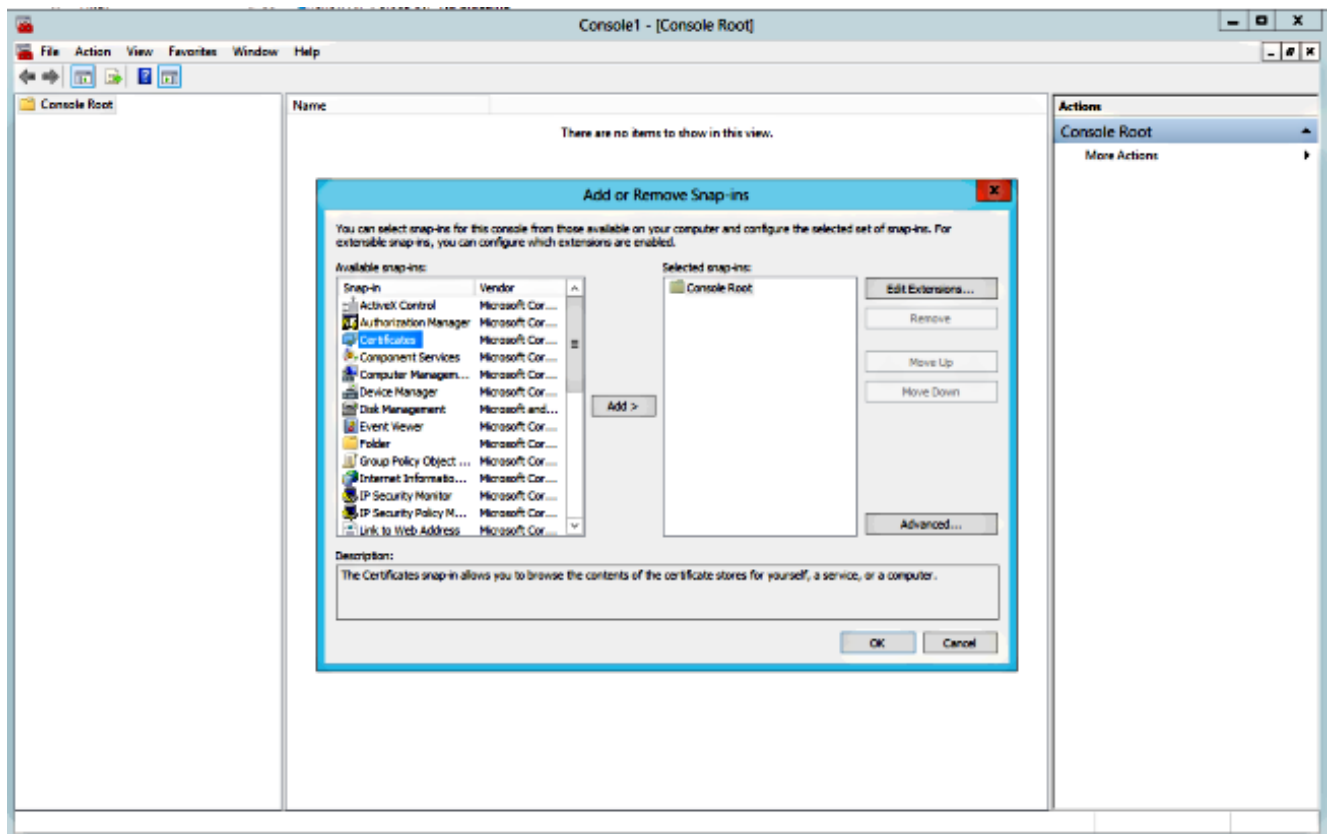
Sie sollten das Zertifikat hier im persönlichen Zertifikatsspeicher des Systems sehen. In diesem Bildschirm werden die Zertifikate aufgelistet, die derzeit im persönlichen Vertrauensspeicher des Servers verfügbar sind und wie zuvor beschrieben zur Verwendung ausgewählt werden können.

Im Administratorleitfaden sind zwei Anforderungen für die Auflistung des Zertifikats aufgeführt:

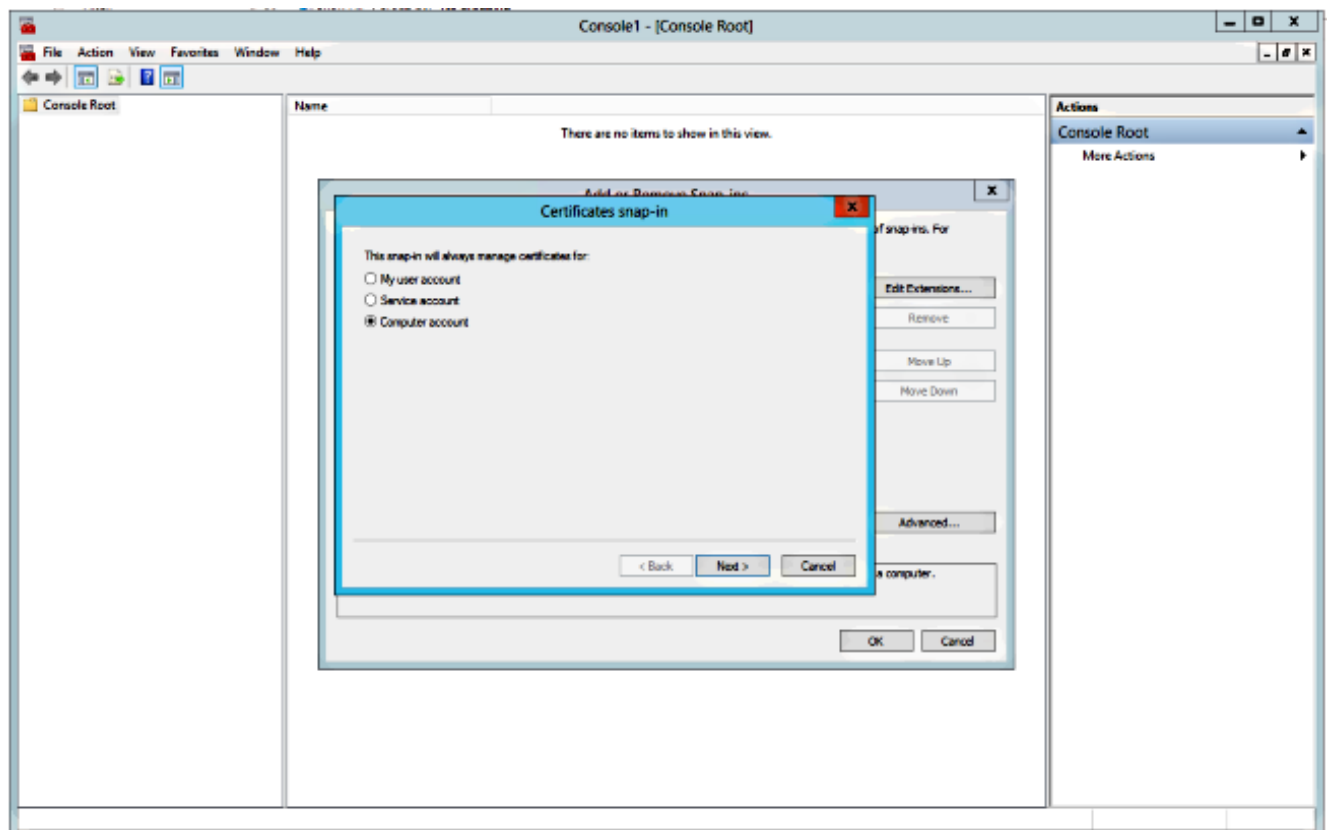
- Wenn hier keine Zertifikate aufgeführt sind, überprüfen Sie, ob das Konto, das Sie zur Ausführung der Cisco TMS-Tools verwenden, über Lesezugriff auf die privaten Schlüssel der Zertifikate verfügt.
- Stellen Sie sicher, dass alle Konten, bei denen die TMS-Dienste angemeldet sind, über Lesezugriff auf die privaten Schlüssel der Zertifikate verfügen.

Um ein Zertifikat in einem persönlichen Vertrauensspeicher zu installieren, müssen Sie Microsoft Management Console (MMC) öffnen und Snap-In für Zertifikat hinzufügen:

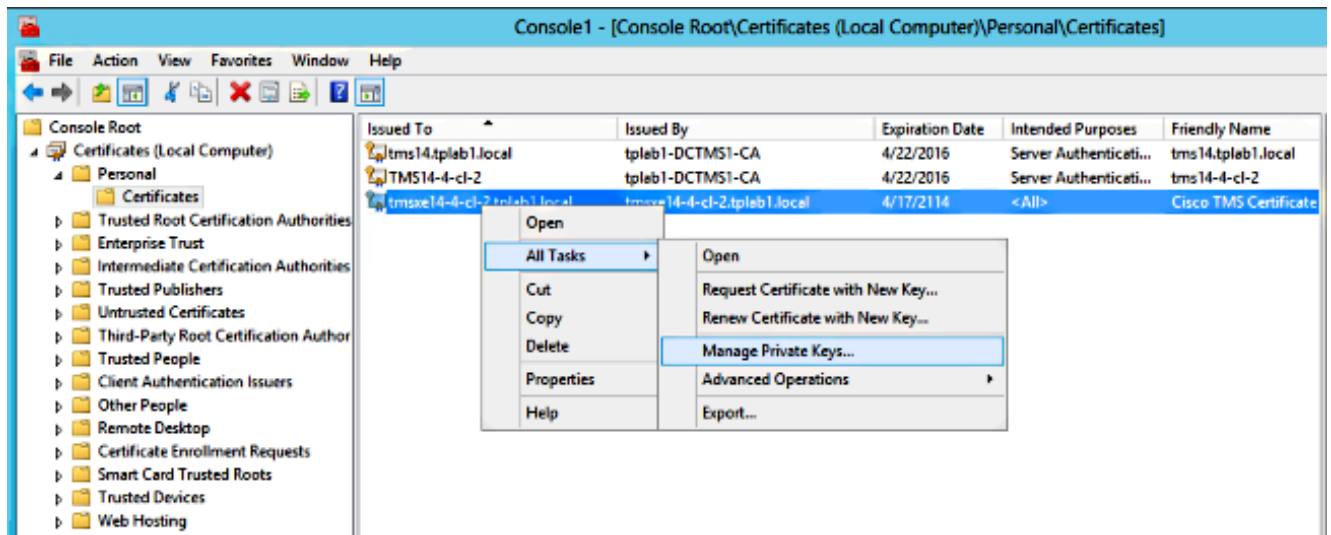
1. Öffnen Sie MMC mit Ausführung auf dem Microsoft Windows-Server.
2. Fügen Sie das Zertifikat Snap-In für MMC hinzu:



3. Stellen Sie sicher, dass Sie das Zertifikat in das **Computerkonto** einfügen:

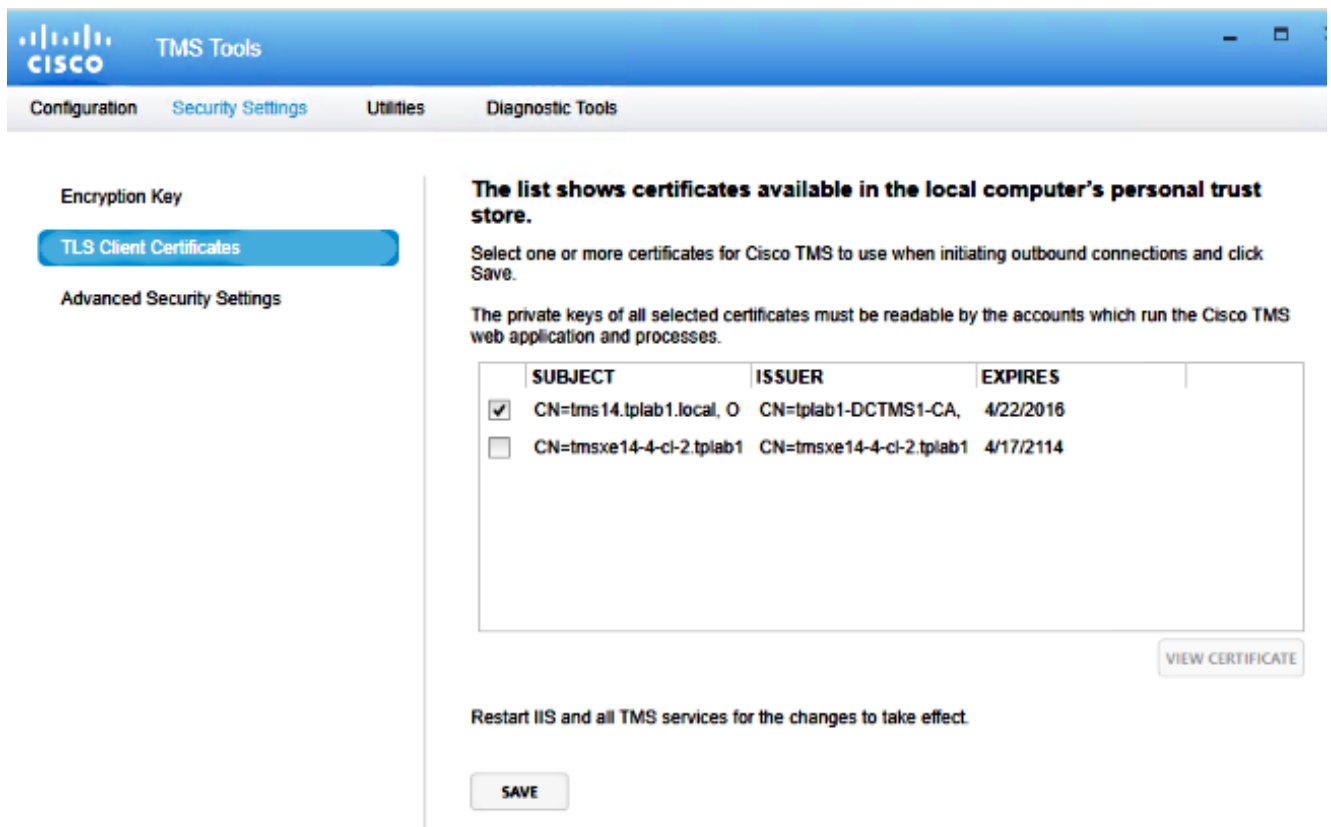


4. Importieren Sie das Zertifikat unter **Persönlich > Zertifikate**, und klicken Sie auf **Private Schlüssel verwalten**:



5. Fügen Sie allen Benutzern, über die auf das TMS-Tool zugegriffen werden kann, Zugriff zum Lesen hinzu.

6. Öffnen Sie **TMS-Tools**, und navigieren Sie zu **TLS-Client-Zertifikaten**:



7. Klicken Sie auf **Speichern** und IIS neu starten.

Überprüfung

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.