TMS Certificates with TMS Tools for TLS Communication Configuration Example

Document ID: 118723

Contributed by Vivek Kumar Singh, Cisco TAC Engineer
Jan 27, 2015

Contents

Introduction

This document describes how to use the TelePresence Management Suite (TMS) tool in order to configure the certificate used by the TMS application when it initiates outbound connections. If the TMS server is a part of a domain, then the certificate creation option might not be visible on the TMS tool.

Prerequisites

Requirements

Cisco recommends that you have:

- TMS installed and accessible through HTTP and HTTPS
- Access to restart the Internet Information Services (IIS) server
- Admin rights for the user
- Access to the Transport Layer Security (TLS) certificate that must be installed

Component Used

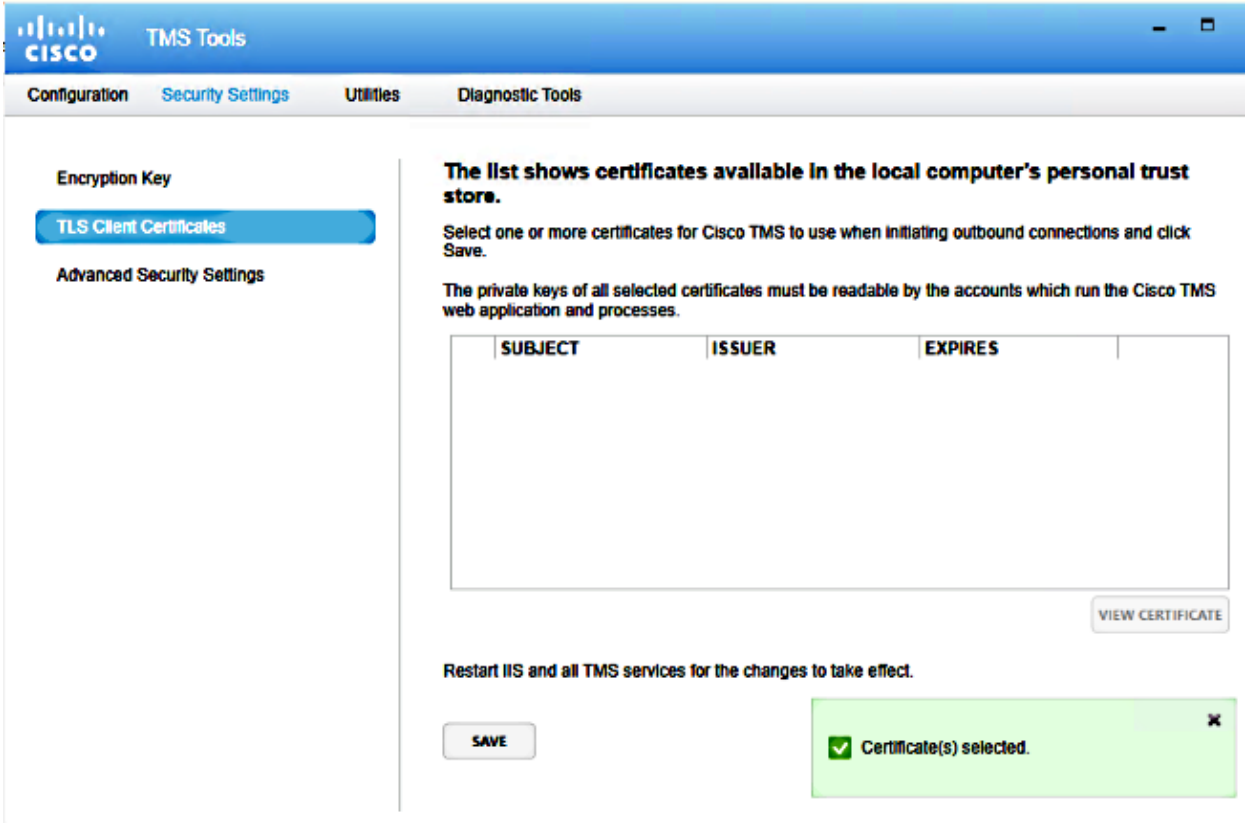
The information in this document is based on TMS Versions14.3.2, 14.2.2, and 14.5.

All screenshots in this document are from the TMS Version 14.5 interface. Certificates for other versions can also be generated with the same procedure.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configure

When you want to have complete TLS communication from the TMS server and you want TMS to use a TLS certificate, you must configure it with the TMS tools.



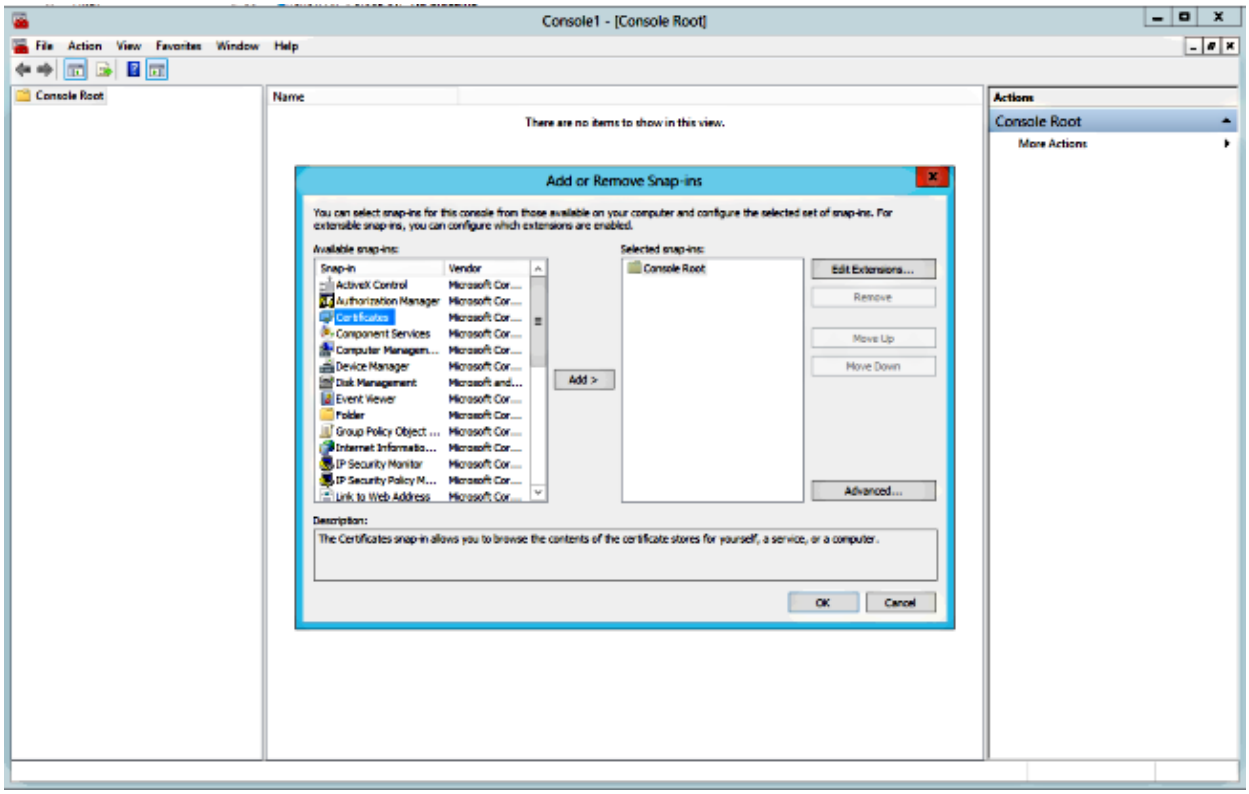
You should see the certificate here from the personal certificate store on the system. This screen lists the certificates currently available in the server's personal trust store that can be selected to be used as described previously.

There are two requirement mentioned in the admin guide for the certificate to be listed here:

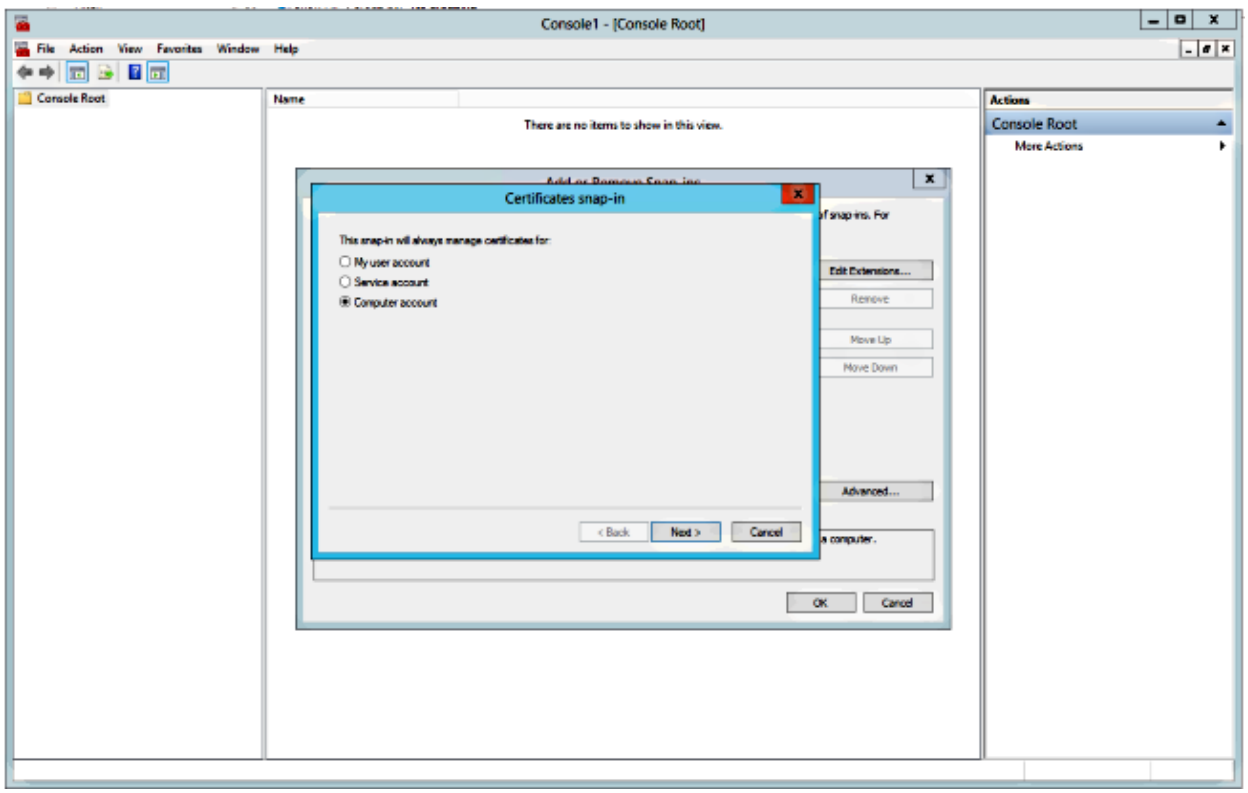
- If there are no certificates listed here, check that the account you use in order to run Cisco TMS Tools has read access to the private keys of the certificates.
- Ensure that all accounts the TMS services are logged on have read access to the private keys of the certificates.

In order to install a certificate on a personal trust store, you need to open Microsoft Management Console (MMC) and add Snap−in for certificate:

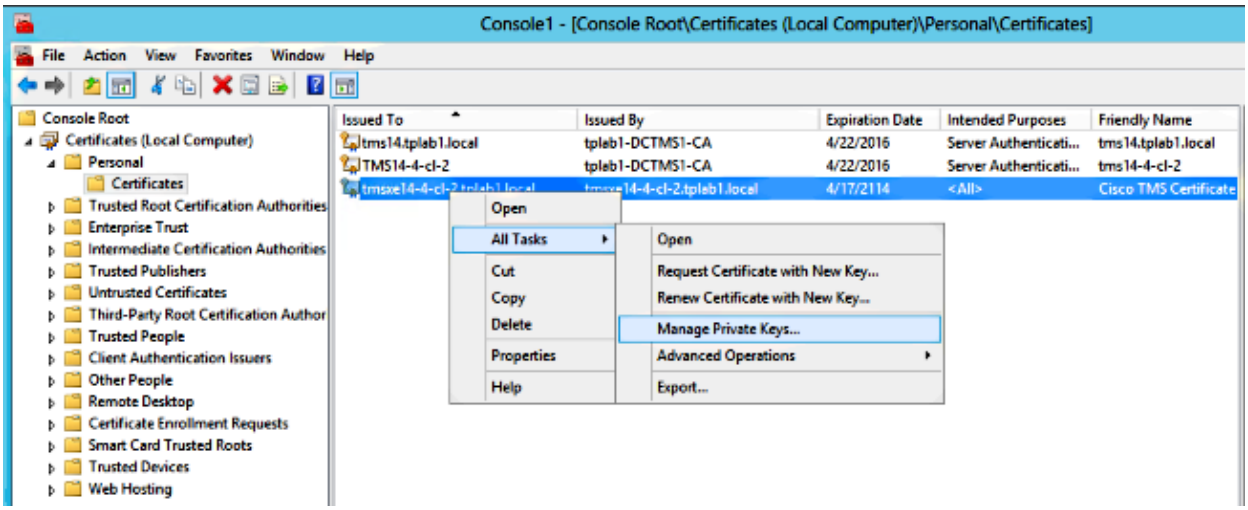
1. Open MMC with run on the Microsoft Windows server.
2. Add the certificate Snap−in on MMC:



3. Ensure that you add the certificate in the ***Computer account***:

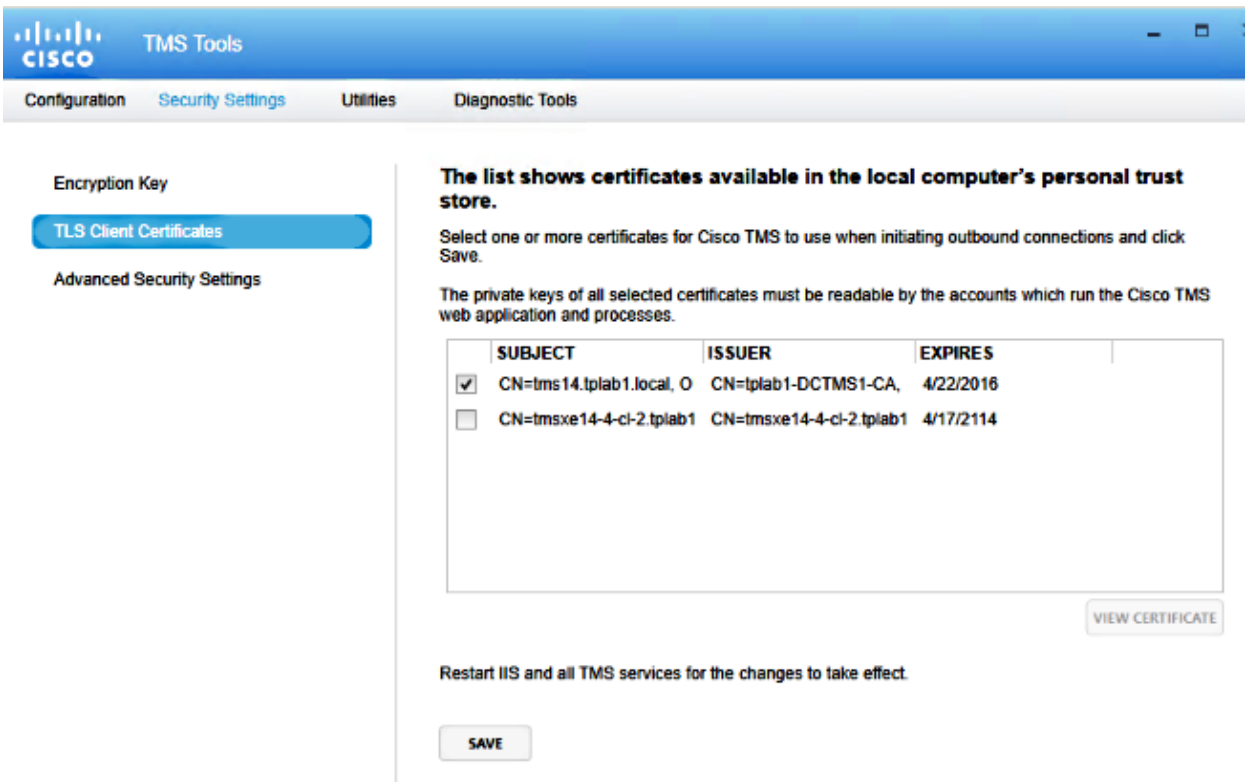


4. Import the certificate on ***Personal > Certificates*** and click ***Manage Private Keys***:



5. Add access to all users through which the TMS tool can be accessed and provide Read access.

6. Open ***TMS Tools*** and navigate to ***TLS Client Certificates***:



7. Click ***Save*** and restart IIS.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Updated: Jan 27, 2015 Document ID: 118723