Сертификаты TMS с программными средствами TMS для примера конфигурации связи TLS

Содержание

Введение

Этот документ описывает , как использовать программное средство Комплекта системы управления telepresence (TMS) для настройки сертификата, используемого приложением TMS, когда это инициирует исходящие соединения. Если сервер TMS является частью домена, то опция создания сертификата не могла бы быть видима на программном средстве TMS.

Предварительные условия

Требования

Cisco рекомендует иметь:

- TMS, установленный и доступный через HTTP и HTTPS
- Доступ для перезапуска сервера информационных сервисов интернета (IIS)
- Права администратора для пользователя
- Доступ к сертификату Transport Layer Security (TLS), который должен быть установлен

Используемый компонент

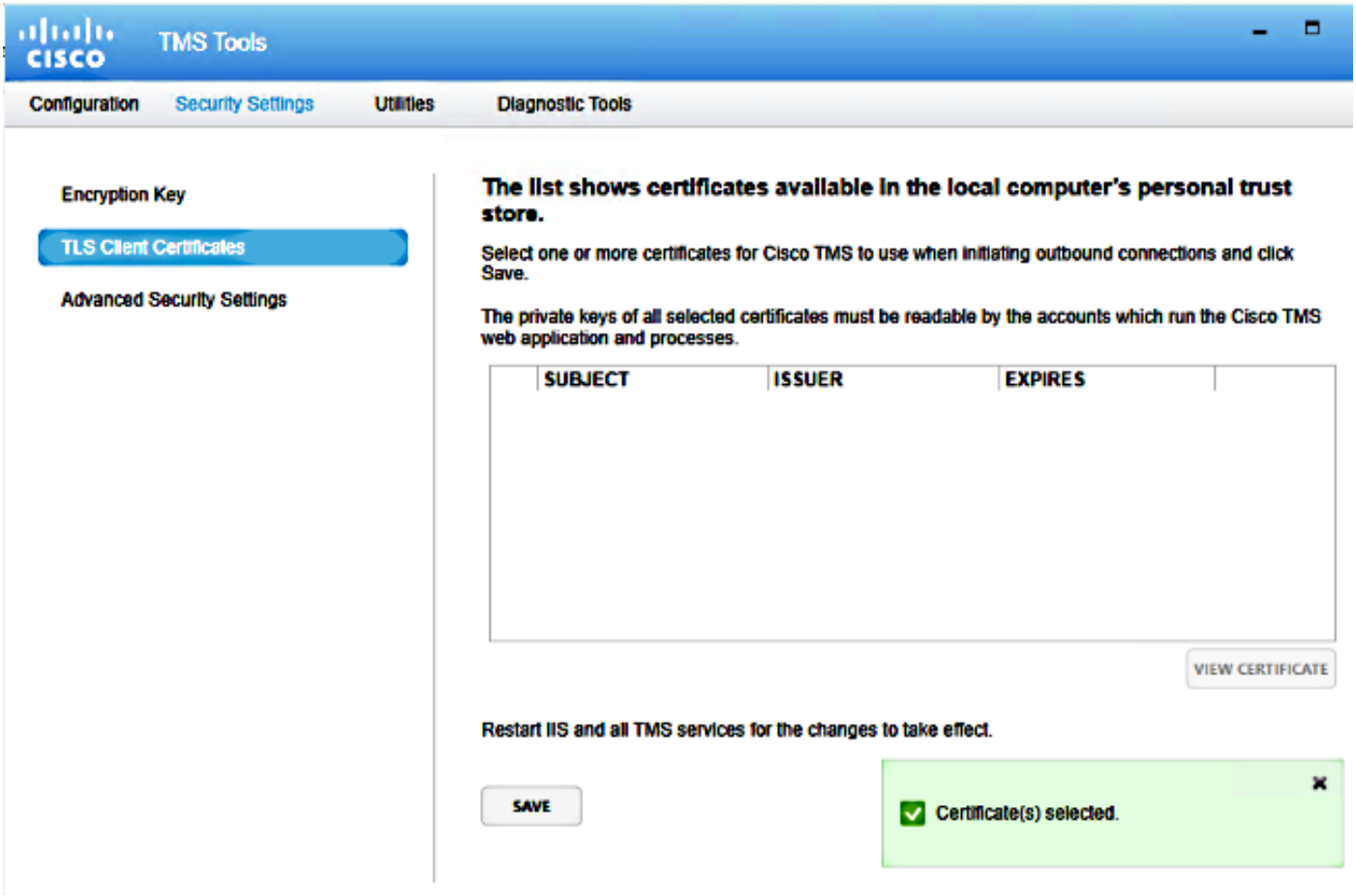
Сведения в этом документе основываются на TMS Versions14.3.2, 14.2.2, и 14.5.

Все снимки экрана в этом документе от интерфейса Версии 14.5 TMS. Сертификаты для других версий могут также генерироваться с той же процедурой.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Настройка

Когда вы хотите иметь завершенную связь TLS от сервера TMS, и вы хотите, чтобы TMS использовал сертификат TLS, необходимо настроить его с программными средствами TMS.



Необходимо видеть сертификат здесь от хранилища персонального сертификата в системе. Этот экран перечисляет сертификаты, в настоящее время доступные в персональной базе доверенных сертификатов сервера, которая может быть выбрана, чтобы использоваться, как описано ранее.

Существует два требования, упомянутые в руководстве admin для сертификата, который будет перечислен здесь:

- Если нет никаких сертификатов, перечисленных здесь, проверьте, что учетная запись, которую вы используете для выполнения Программных средств TMS Cisco имеет доступ для чтения к секретным ключам сертификатов.

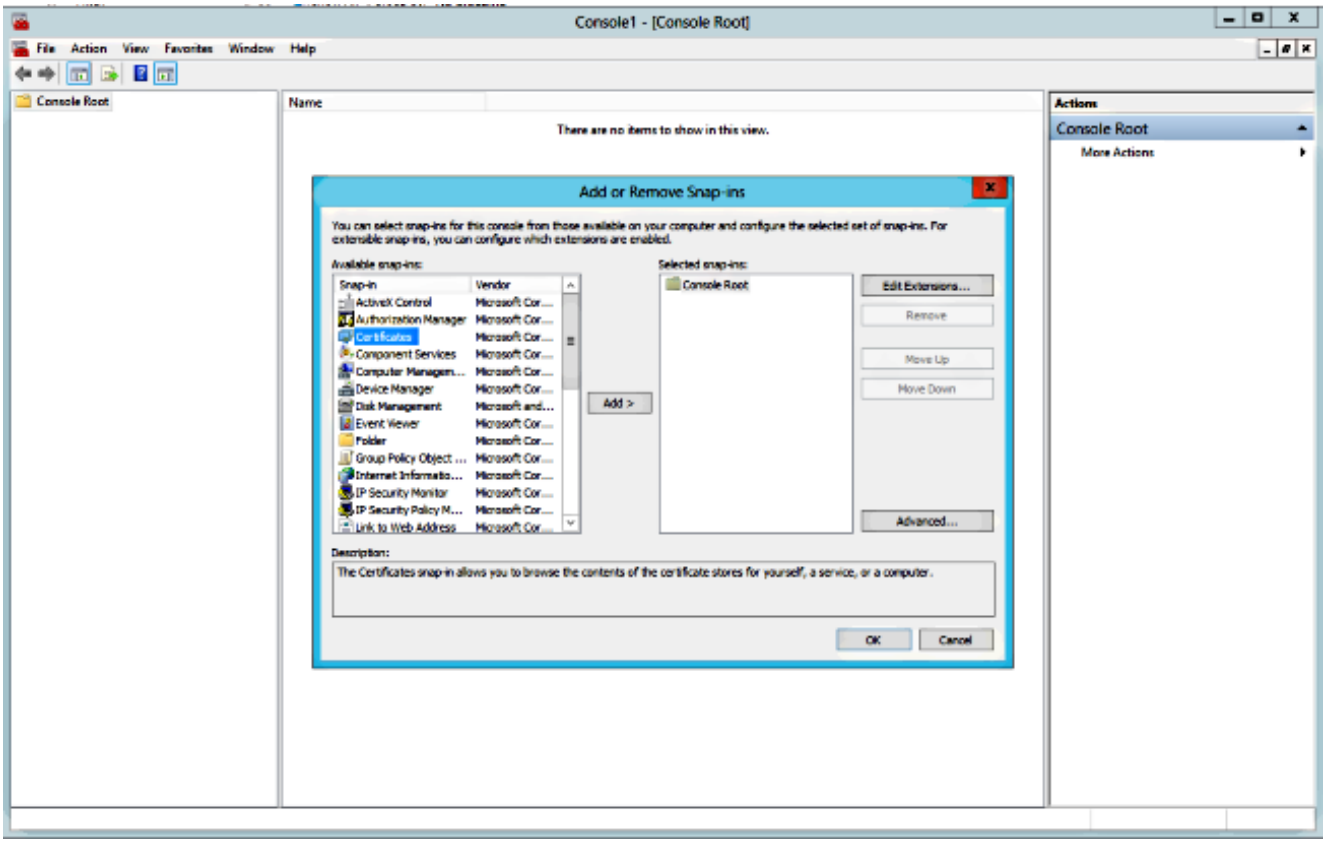
- Гарантируйте, что все учетные записи, сервисы TMS входятся в систему, имеют доступ для чтения к секретным ключам сертификатов.

Для установки сертификата на персональной базе доверенных сертификатов необходимо

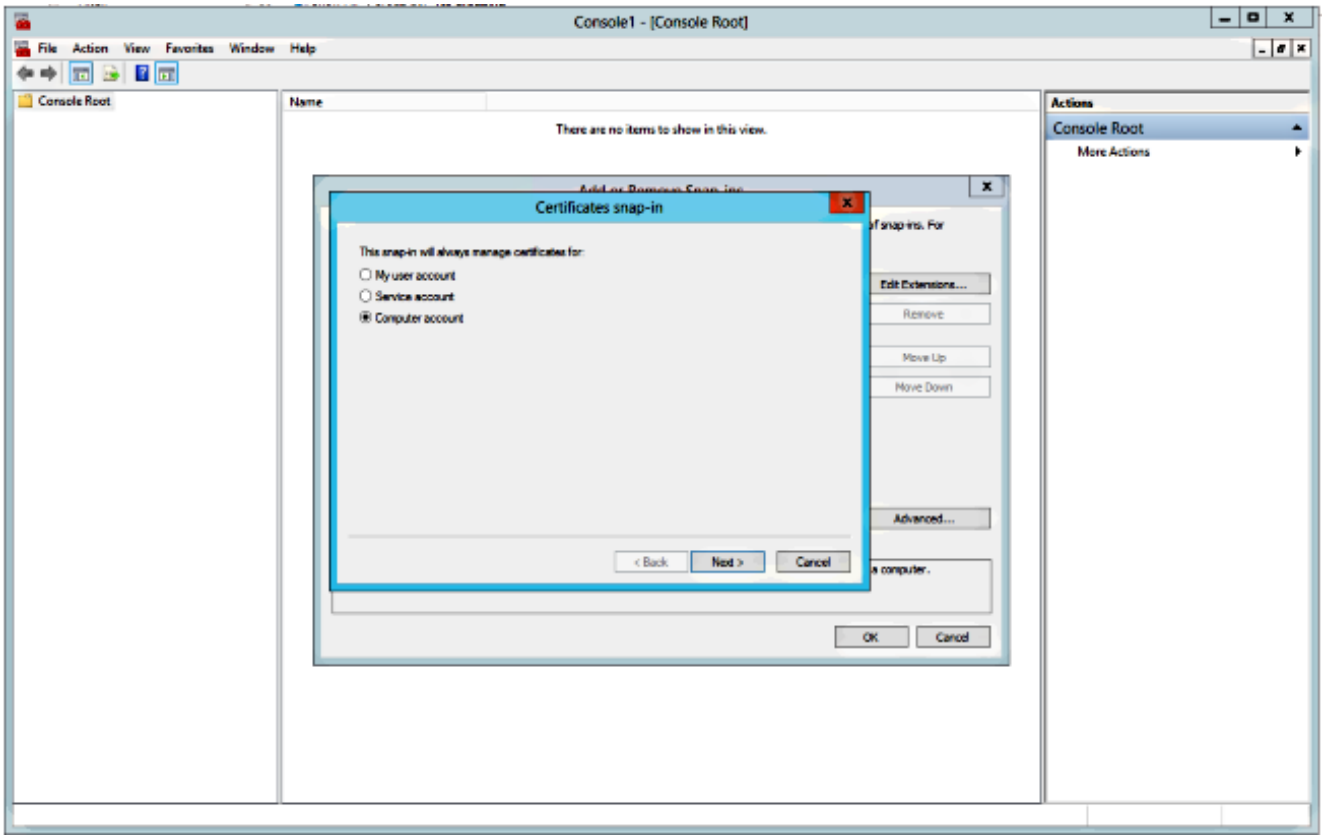
открыть Консоль управления Microsoft (MMC) и добавить Моментальный снимок - в для сертификата:

1. Открытый MMC с работавшим Microsoft Windows server.

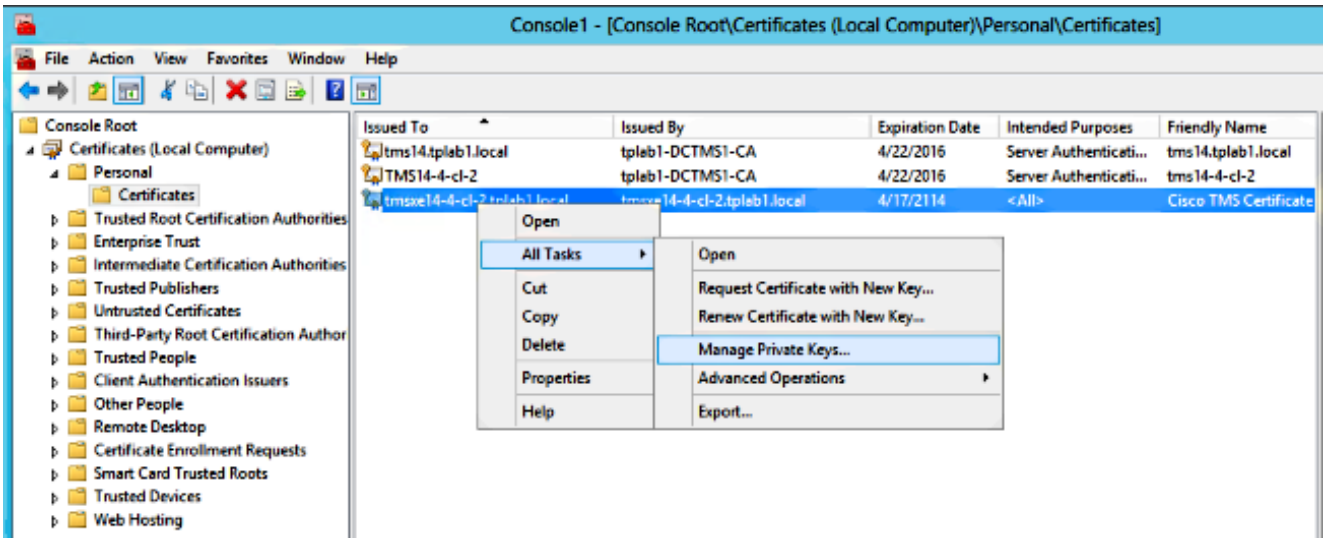
2. Добавьте Моментальный снимок сертификата - в на MMC:



3. Гарантируйте добавление сертификата в **Учетной записи компьютера**:

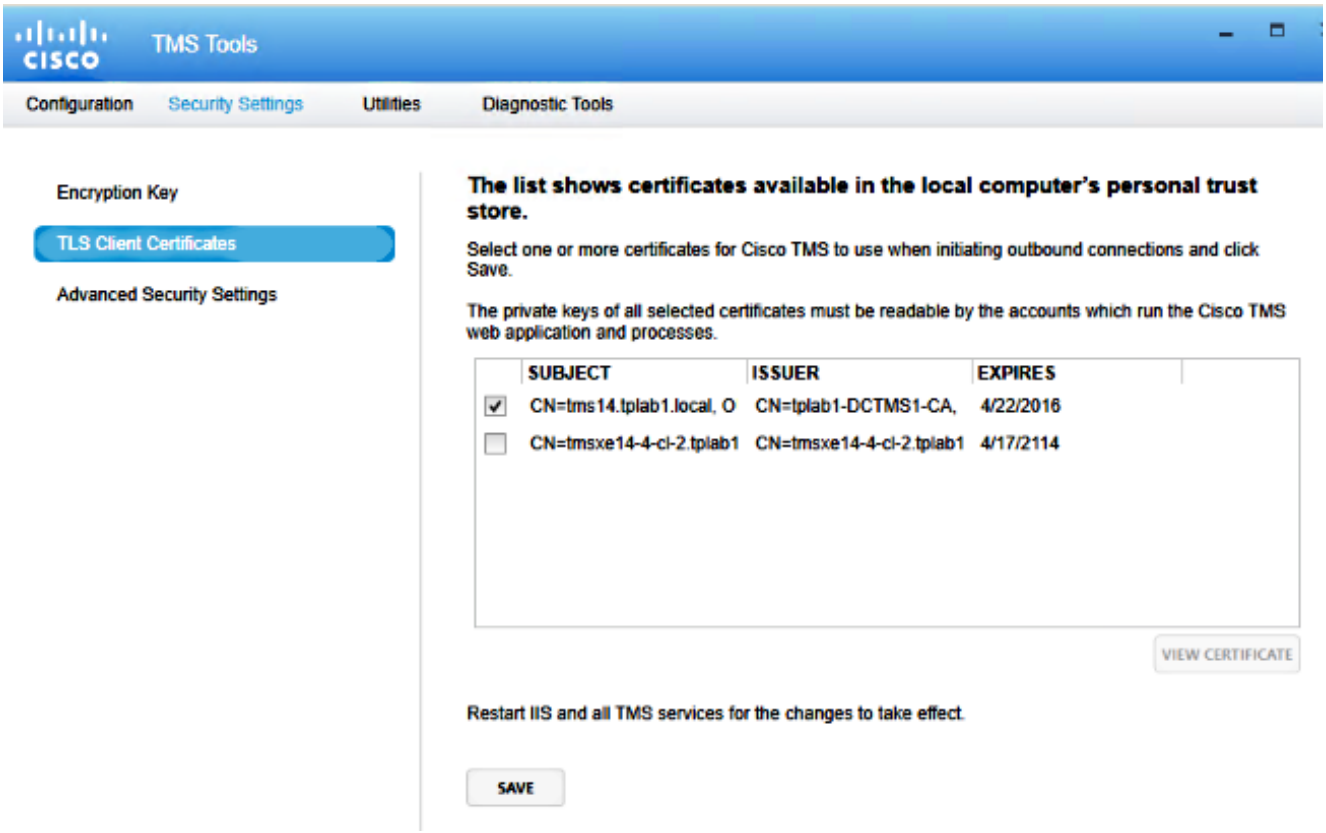


4. Импортируйте сертификат на **Персональном> Сертификаты** и нажмите **Manage Private Keys**:



5. Добавьте доступ ко всем пользователям, через которых к программному средству TMS можно обратиться и предоставить Доступ для чтения.

6. Открытые **Программные средства TMS** и перешли к **Сертификатам клиента TLS**:



7. Нажмите **Save** и перезапустите IIS.

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.