Как не Устранить неполадки "Никакой Ошибки" ответа HTTPS на TMS После Обновления Оконечных точек TC/CE

Содержание

Введение

Этот документ описывает, как не устранить неполадки "никакого сообщения" ответа HTTPS на Комплекте системы управления telepresence (TMS).

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- TMS Cisco
- Сервер Windows

Используемые компоненты

Сведения, содержащиеся в этом документе, касаются следующих версий программного обеспечения:

- TC 7.3.6 и выше
- CE 8.1.0 и выше
- TMS 15.2.1
- Windows Server 2012 R2
- Сервер SQL 2008 R2 и 2012

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.

Общие сведения

Когда оконечные точки перемещены на программное обеспечение TC 7.3.6 и Collaboration Endpoint (CE) 8.1.0 или выше, эта проблема происходит.

Проблема

После того, как обновление оконечной точки к TC7.3.6 или выше или 8.1.0 или выше и метод подключения между оконечной точкой и TMS установлено как Transport Layer Security (TLS), сообщение об ошибках "никакой ответ HTTPS" появляется на TMS путем выбора Endpoint под **Системой> Навигатор**.

Это происходит в результате этого ситуации.

- TC 7.3.6 и CE 8.1.0 и выше больше не поддерживают TLS 1.0 согласно Комментариям к выпуску.
  http://www. cisco .
  com/c/dam/en/us/td/docs/telepresence/endpoint/software/tc7/release_notes/tc-software-release-notes-tc7.pdf

- Microsoft Windows server отключили версию TLS 1.1 и 1.2 по умолчанию.
- Программные средства TMS используют Среднюю Безопасность Связи в ее Опциях Transport Layer Security по умолчанию.
- Когда версия TLS 1.0 отключена, и обе версии TLS 1.1 и 1.2 включены, TMS не передает Сообщение приветствия клиента Протокола SSL после того, как трехстороннее квитирование TCP успешно выполняется с Оконечной точкой. Однако, все еще способный зашифровать данные с помощью версии TLS 1.2.
- Включение версии TLS 1.2 с помощью Программного средства или в Реестре Windows недостаточно, поскольку TMS все еще только передаст или даст объявление 1.0 в его сообщениях Сообщения приветствия клиента.

Решение

Windows Server, где TMS установлен, нужно было включить версию TLS 1.1 и 1.2, это может быть достигнуто со следующей процедурой.

Включите TLS 1.1 и 1.2 на Windows Server TMS для TMS 15.x и выше

Шаг 1. Откройте Соединение Удаленного рабочего стола с Windows Server, где установлен TMS.

Шаг 2. Редактор реестра Открытых окон (**Запускаются**-> **Выполнение**-> **Regedit**).

Шаг 3. Возьмите резервную копию Реестра.

Если вам предлагают для пароля администратора или подтверждения, введите пароль или предоставьте подтверждение.

Найдите и нажмите ключ или подключ, что вы хотите выполнить резервное копирование.

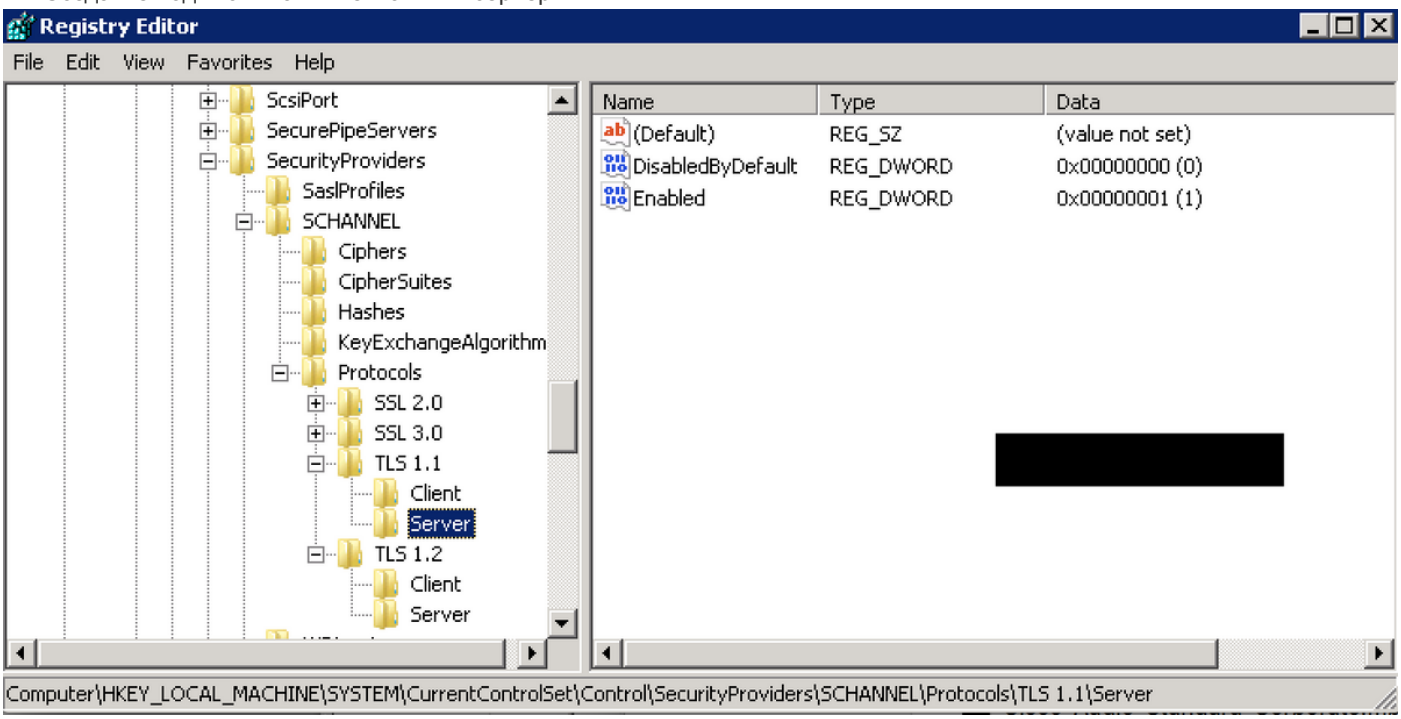
Нажмите Меню Файл, и затем нажмите Export.

В Сохранении в коробке выберите местоположение, где вы хотите сохранить резервную копию к, и затем ввести имя

для резервного файла в коробке Имени файла.
Нажмите Save.

Шаг 4. . Включите TLS 1.1 и TLS 1.2.

Открытый реестр
Перейдите к **HKEY_LOCAL_MACHINE**-> **СИСТЕМА**-> **CurrentControlSet**-> **Контроль**-> **SecurityProviders**-> **SCHANNEL**-> **Протоколы**
Добавьте поддержка TLS 1.2 и TLS 1.1
Папки Create TLS 1.1 и TLS 1.2
Создайте подключи как клиентский' и 'сервер



Создайте **DWORD** для обоих Клиентов и серверов для каждого созданного ключа TLS.

```
DisabledByDefault [Value = 0]
Enabled [Value = 1]
```

Шаг 5. . Windows Server TMS перезапуска для обеспечения TLS вступает в силу.

> **Примечание:** Посетите эту ссылку для определенной информации о применимых версиях https://technet.microsoft.com/en-us/library/dn786418%28v=ws.11%29.aspx#BKMK_SchannelTR_TLS12

> **Совет:** Программное средство NARTAC может использоваться для отключения необходимых версий TLS после того, как вы делаете это, необходимо перезапустить сервер. Можно загрузить его от этой ссылки https://www.nartac.com/Products/IISCrypto/Download

Изменение безопасности на Программном средстве TMS

Когда правильные версии включены, изменяют Параметры безопасности на Программных средствах TMS с этой процедурой.

Шаг 1. Открытые программные средства TMS

Шаг 2. Перейдите к **Параметрам безопасности> Параметры настройки Дополнительной безопасности**

Шаг 3. Под **Опциями Transport Layer Security**, набор Безопасность Связи к **Среднему Высокому**

Шаг 4. . **Нажмите Save**

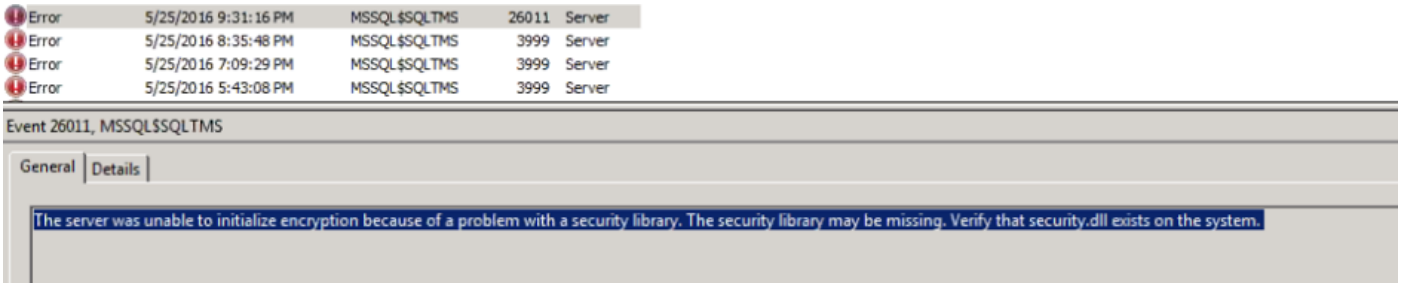
Шаг 5. . Затем перезапустите и информационные сервисы интернета (IIS) на сервере и **TMSDatabaseScannerService** и запустите **TMSPLCMDirectoryService** (если это остановлено),

> **% Warning:**: Когда опция TLS будет изменена на Средний Высокий от Среды, telnet и Протокол SNMP будут отключены. Это вызовет к TMSSNMPservice для остановки, и предупреждение будет выдано на веб-интерфейсе TMS.

Факторы для обновления параметров безопасности

Когда **SQL 2008 R2** используется и установленный на Windows Server TMS, мы должны гарантировать TLS1.0, и SSL3.0 должен также быть включен или иначе SQL сервисная остановка, и это не запустится.

Необходимо видеть это ошибки на журнале событий:

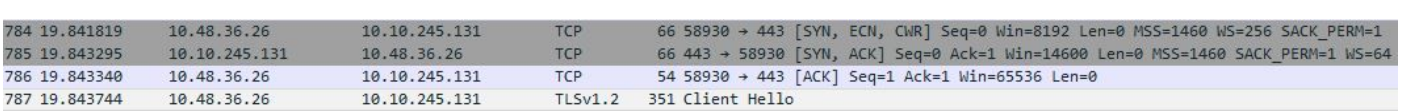


Когда **SQL, 2012** используется, он требует, чтобы быть обновленным для занятия изменением TLS, если установлено на Windows Server TMS (https://support.microsoft.com/en-us/kb/3052404)

Оконечные точки управляемое использование SNMP или Telnet показывают "Нарушение безопасности: Связь Telnet не позволена".

Проверка

При изменении опции TLS от **Среды** до **Среднего Высокого** это гарантирует, что версия TLS 1.2 объявлена в **Сообщении приветствия клиента** после того, как трехстороннее квитирование TCP успешно выполняется от TMS:



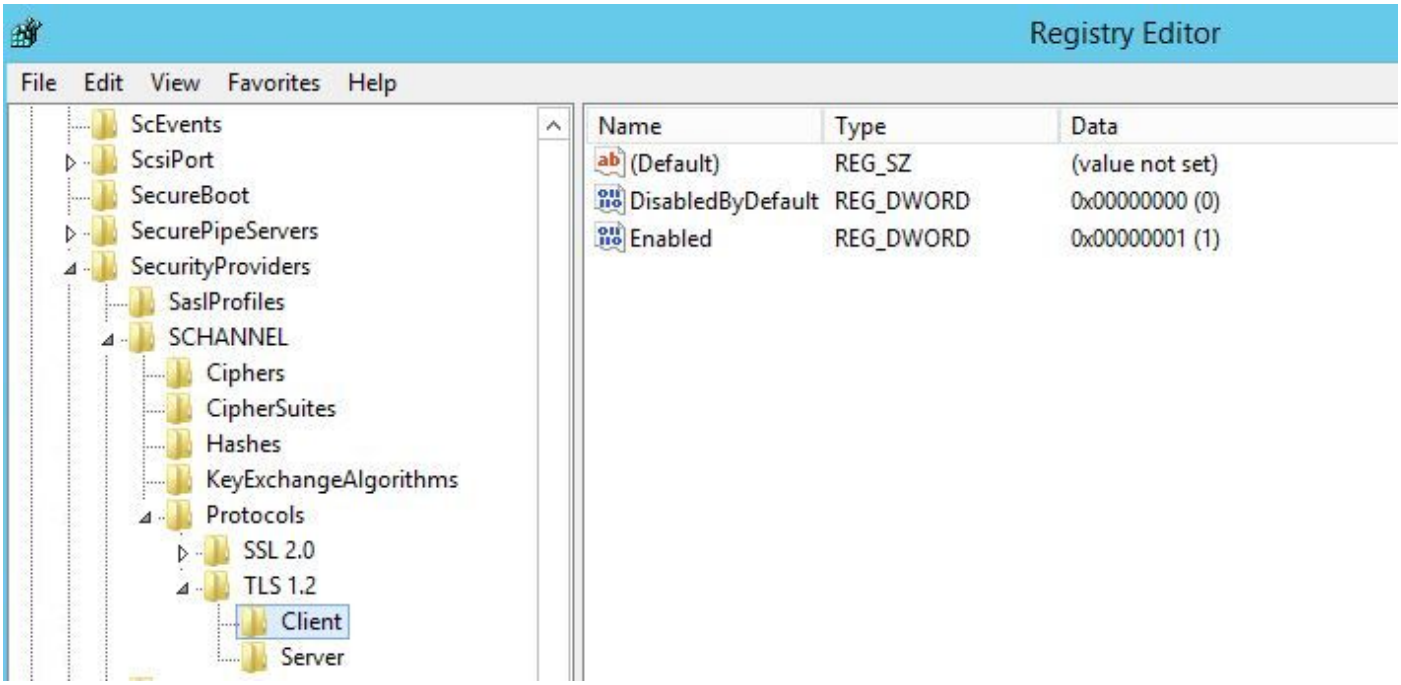
Версия TLS 1.2 дала объявление:

```
▷ Frame 787: 351 bytes on wire (2808 bits), 351 bytes captured (2808 bits) on interface 0
▷ Ethernet II, Src: Vmware_99:59:f1 (00:50:56:99:59:f1), Dst: CiscoInc_29:96:c3 (00:1b:54:29:96:c3)
▷ Internet Protocol Version 4, Src: 10.48.36.26, Dst: 10.10.245.131
▷ Transmission Control Protocol, Src Port: 58930 (58930), Dst Port: 443 (443), Seq: 1, Ack: 1, Len: 297
◢ Secure Sockets Layer
  ◢ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 292
    ▷ Handshake Protocol: Client Hello
```

Если это оставят в **среднем** TMS, то будет только send version 1.0 в Сообщение приветствия клиента SSL во время этапа согласования, который задает самую высокую версию протокола TLS, которую это поддерживает как клиент, который TMS в этом случае.

Для версий TMS ниже, чем 15

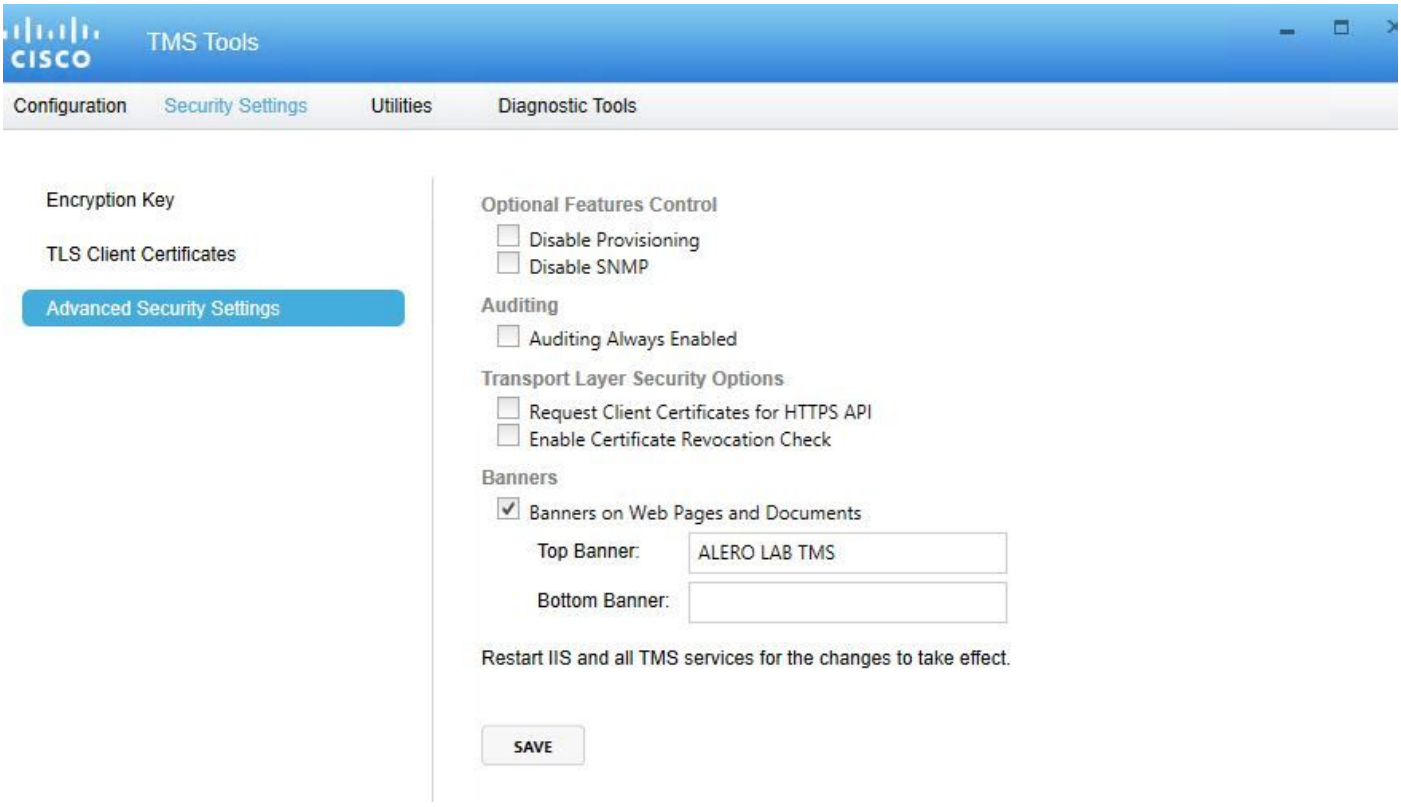
Шаг 1. Даже при том, что версия TLS 1.2 добавлена в реестре



Шаг 2. Сервер TMS все еще не передает версию, поддерживаемую Оконечной точкой в сообщение приветствия клиента SSL

```
1287 11.9999090 10.48.79.117  10.10.0.53      TCP      66 57380→443 [SYN, ECN, CWR] Seq=0 W
1288 12.0011950 10.10.0.53    10.48.79.117    TCP      66 443→57380 [SYN, ACK] Seq=0 Ack=1
1289 12.0012090 10.48.79.117  10.10.0.53      TCP      54 57380→443 [ACK] Seq=1 Ack=1 Win=6
1290 12.0013900 10.48.79.117  10.10.0.53      SSL     157 Client Hello
1291 12.0027650 10.10.0.53    10.48.79.117    TCP      60 443→57380 [ACK] Seq=1 Ack=104 Win
1292 12.0035480 10.10.0.53    10.48.79.117    TCP      60 443→57380 [RST, ACK] Seq=1 Ack=10
1294 12.0068970 10.48.79.117  10.10.0.53      TCP      66 57381→80 [SYN, ECN, CWR] Seq=0 Wi
1295 12.0084020 10.10.0.53    10.48.79.117    TCP      66 80→57381 [SYN, ACK] Seq=0 Ack=1 W
1296 12.0084170 10.48.79.117  10.10.0.53      TCP      54 57381→80 [ACK] Seq=1 Ack=1 Win=65
1297 12.0084980 10.48.79.117  10.10.0.53      HTTP    217 GET /tcs/systemunit.xml HTTP/1.1
1298 12.0099360 10.10.0.53    10.48.79.117    TCP      60 80→57381 [ACK] Seq=1 Ack=164 Win=
1299 12.0104210 10.10.0.53    10.48.79.117    HTTP    444 HTTP/1.1 301 Moved Permanently
1300 12.0105360 10.10.0.53    10.48.79.117    TCP      60 80→57381 [FIN, ACK] Seq=391 Ack=1
Frame 1290: 157 bytes on wire (1256 bits), 157 bytes captured (1256 bits) on interface 0
Ethernet II, Src: Vmware_99:42:e9 (00:50:56:99:42:e9), Dst: Cisco_29:96:c7 (00:1b:54:29:96:c7)
Internet Protocol Version 4, Src: 10.48.79.117 (10.48.79.117), Dst: 10.10.0.53 (10.10.0.53)
Transmission Control Protocol, Src Port: 57380 (57380), Dst Port: 443 (443), Seq: 1, Ack: 1, Len: 10
Secure Sockets Layer
⊟ SSL Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 98
  ⊞ Handshake Protocol: Client Hello
```

Шаг 3. Проблема тогда заключается в том, что мы не можем изменить Опции TLS в программных средствах TMS, поскольку эта опция не доступна



Шаг 4. . Затем обходной путь для этой проблемы является или TMS обновления к 15.x, или понизьте свои оконечные точки TC/CE до 7.3.3, эта проблема отслежена в ошибках ПО CSCuz71542, созданный для версии 14.6. X.