How to Troubleshoot "No HTTPS response" Error on TMS After TC/CE Endpoints Upgrade

Contents

Introduction

This document describes how to troubleshoot "no HTTPS response" message on Telepresence Management Suite (TMS).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco TMS
- Windows Server

Components Used

The information in this document is based on these software versions:

- TC 7.3.6 and above
- CE 8.1.0 and above
- TMS 15.2.1
- Windows Server 2012 R2
- SQL Server 2008 R2 and 2012

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.

Background Information

This issue occurs when the endpoints are migrated to TC 7.3.6 and Collaboration Endpoint (CE) 8.1.0 software or above.

Problem

After an endpoint upgrade to TC7.3.6 or above or 8.1.0 or above and the communication method between the endpoint and the TMS is set up as Transport Layer Security (TLS), the error message "no HTTPS response" pops up on TMS by selecting the Endpoint, under **System** > **Navigator**.

This happens as a result of this situations.

- TC 7.3.6 and CE 8.1.0 and above no longer support TLS 1.0 as per the release notes. 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 has TLS version 1.1 and 1.2 disabled by default.
- TMS tools uses Medium Communication Security in its Transport Layer Security Options by default.
- When TLS version 1.0 is disabled and both TLS version 1.1 and 1.2 are enabled, TMS doesn’t send Secure Socket Layer (SSL) Client hello after TCP 3-Way handshake succeeds with the Endpoint. However still able to encrypt data using TLS version 1.2.
- Enabling TLS version 1.2 using a Tool or in the Windows Registry is not enough, as the TMS will still only send or advertise 1.0 in its Client hello messages.

Solution

The Windows server where the TMS is installed, needs to have TLS version 1.1 and 1.2 enabled, this can be achieved with the next procedure.

Enable TLS 1.1 and 1.2 on TMS Windows Server for TMS 15.x and higher

Step 1. Open a Remote Desktop Connection to Windows Server where TMS is installed.

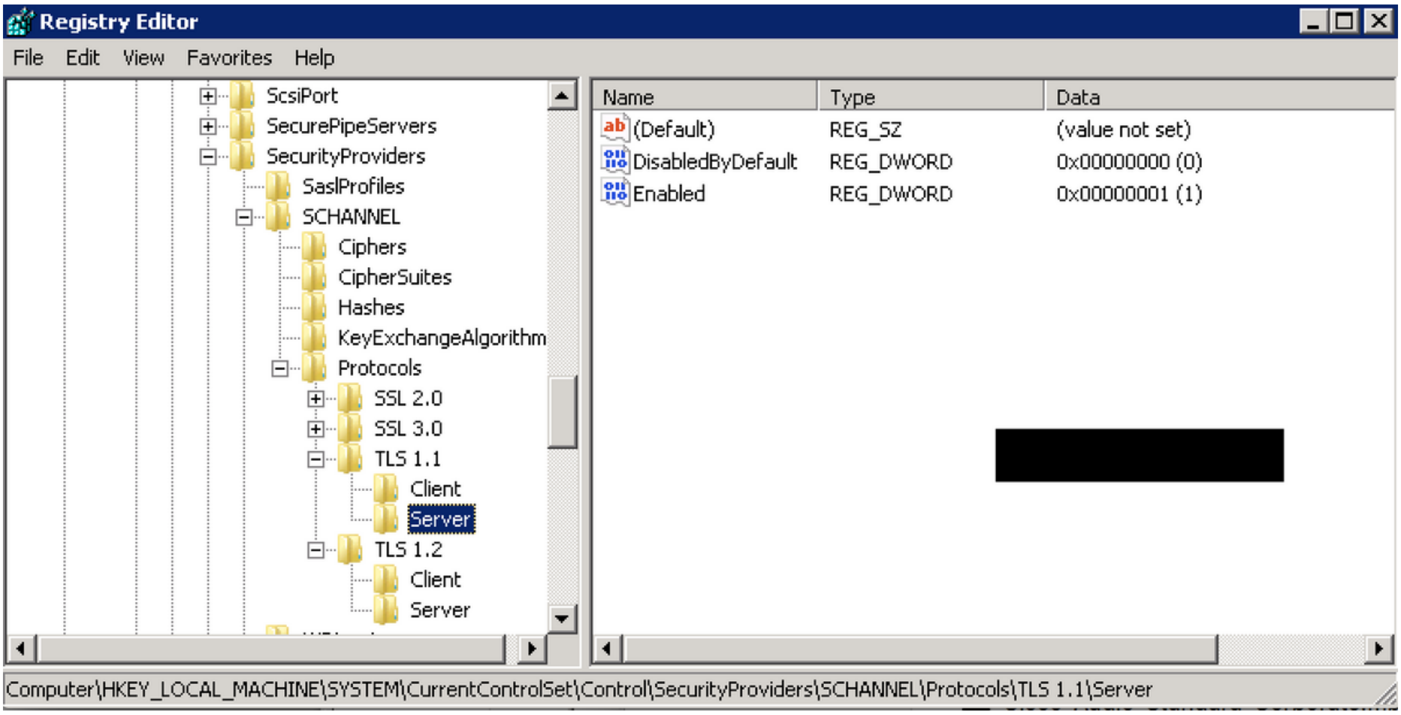
Step 2. Open Windows Registry editor (**Start**->**Run**->**Regedit**).

Step 3. Take backup of Registry.

- If you're prompted for an administrator password or confirmation, type the password or provide confirmation.
- Locate and click the key or subkey that you want to back up.
- Click the File menu, and then click Export.
- In the Save in box, select the location where you want to save the backup copy to, and then type a name for the backup file in the File name box.
- Click Save.

Step 4. Enable TLS 1.1 and TLS 1.2.

- Open Registry
- Navigate to **HKEY_LOCAL_MACHINE** --> **SYSTEM** --> **CurrentControlSet** --> **Control** --> **SecurityProviders**--> **SCHANNEL** --> **Protocols**
- Add TLS 1.1 and TLS 1.2 support
- Create TLS 1.1 and TLS 1.2 folders
- Create sub-keys as client' and 'server



```
ScsiPort
SecurePipeServers
SecurityProviders
  SaslProfiles
  SCHANNEL
    Ciphers
    CipherSuites
    Hashes
    KeyExchangeAlgorithm
    Protocols
      SSL 2.0
      SSL 3.0
      TLS 1.1
        Client
        Server
      TLS 1.2
        Client
        Server
```

Name	Type	Data
(Default)	REG_SZ	(value not set)
DisabledByDefault	REG_DWORD	0x00000000 (0)
Enabled	REG_DWORD	0x00000001 (1)

[redacted]

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server

Create **DWORDs** for both Client and Server for each TLS key created.

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

Step 5. Restart TMS Windows server to ensure TLS take effect.

Note: Visit this link for specific information on aplicable versions https://technet.microsoft.com/en-us/library/dn786418%28v=ws.11%29.aspx#BKMK_SchannelTR_TLS12

Tip: NARTAC tool can be used to disable the TLS needed versions after you do that you need to restart the server. You can download it from this link https://www.nartac.com/Products/IISCrypto/Download

Security change on TMS Tool

When the correct versions are enabled, change the Security settings on TMS Tools with this procedure.

Step 1. Open TMS tools

Step 2. Navigate to **Security Settings** > **Advanced Security Settings**

Step 3. Under **Transport Layer Security Options**, set the Communication Security to **Medium-High**

Step 4. Click **Save**

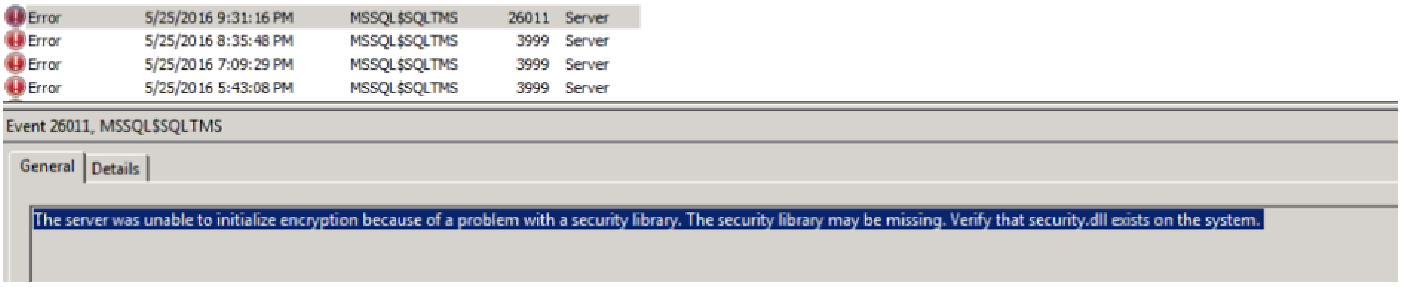
Step 5. Then restart both the Internet Information Services (IIS) on the server and **TMSDatabaseScannerService** and start **TMSPLCMDirectoryService** (if it’s stopped)

Warning: : When TLS option is changed to Medium-High from Medium, telnet and Simple Network Management Protocol (SNMP) will be disabled. This will cause to TMSSNMPservice to stop and an alert will be raised on TMS web interface.

Considerations in order to upgrade security settings

When **SQL 2008 R2** is in use and installed on TMS windows server, we need to ensure TLS1.0 and SSL3.0 should also be enabled or else SQL service stop and it won't start.

You must see this errors on the event log:



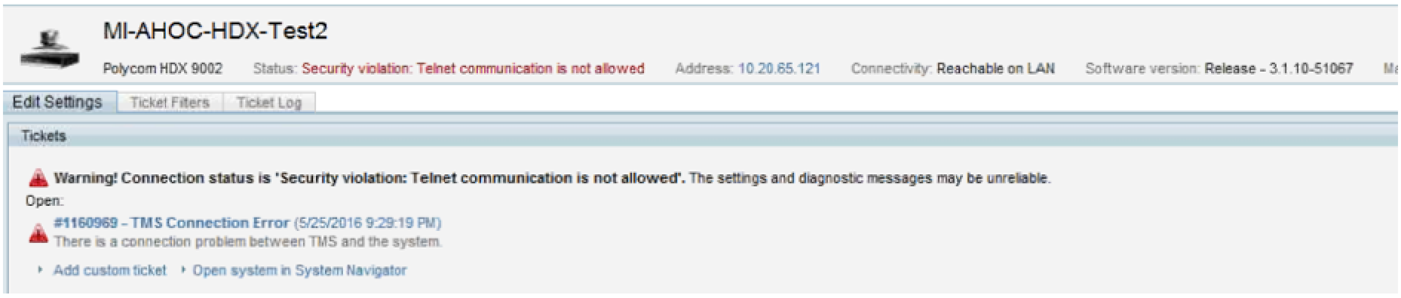
```
Error    5/25/2016 9:31:16 PM    MSSQL$SQLTMS    26011   Server
Error    5/25/2016 8:35:48 PM    MSSQL$SQLTMS     3999   Server
Error    5/25/2016 7:09:29 PM    MSSQL$SQLTMS     3999   Server
Error    5/25/2016 5:43:08 PM    MSSQL$SQLTMS     3999   Server
```

Event 26011, MSSQL$SQLTMS

The server was unable to initialize encryption because of a problem with a security library. The security library may be missing. Verify that security.dll exists on the system.

When **SQL 2012** is in use it requires to be updated to tackle TLS change if installed on TMS windows server (https://support.microsoft.com/en-us/kb/3052404)

Endpoints managed using SNMP or Telnet show "Security violation: Telnet communication is not allowed".



MI-AHOC-HDX-Test2

Polycom HDX 9002   Status: Security violation: Telnet communication is not allowed   Address: 10.20.65.121   Connectivity: Reachable on LAN   Software version: Release - 3.1.10-51067

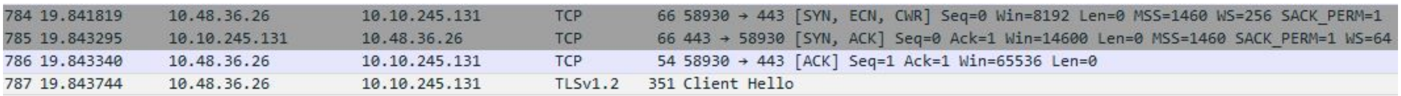
Warning! Connection status is 'Security violation: Telnet communication is not allowed'. The settings and diagnostic messages may be unreliable.

Open:

#1160969 - TMS Connection Error (5/25/2016 9:29:19 PM)
There is a connection problem between TMS and the system.

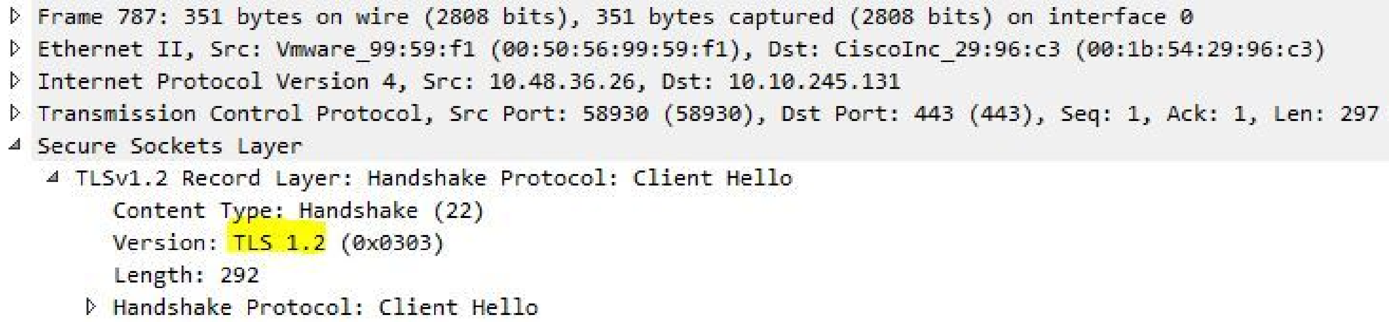
Verify

When you change the TLS option from **Medium** to **Medium-High,** this ensures that TLS version 1.2 is advertised in the **Client Hello** after the TCP 3-Way handshake suceeds from TMS:



```
784 19.841819    10.48.36.26      10.10.245.131    TCP       66 58930 → 443 [SYN, ECN, CWR] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
785 19.843295    10.10.245.131    10.48.36.26      TCP       66 443 → 58930 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=64
786 19.843340    10.48.36.26      10.10.245.131    TCP       54 58930 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
787 19.843744    10.48.36.26      10.10.245.131    TLSv1.2  351 Client Hello
```

TLS version 1.2 advertised:

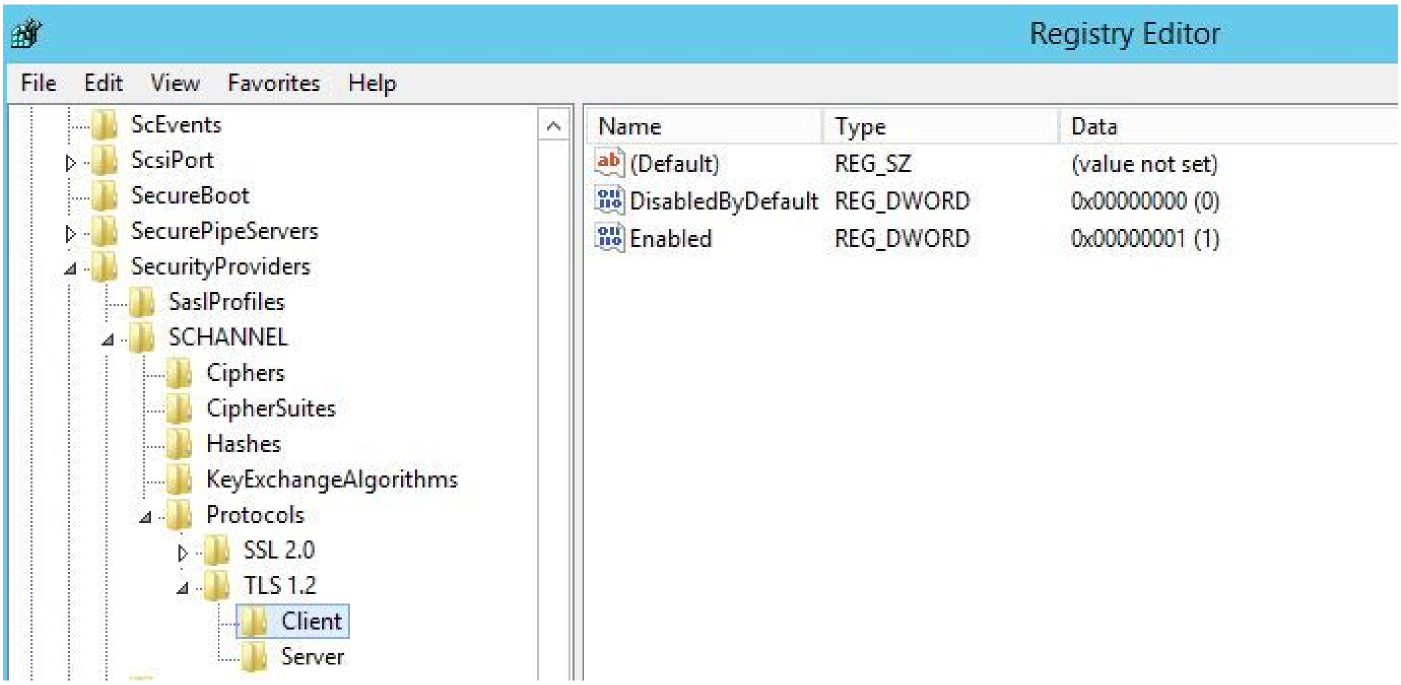


```
▷ Frame 787: 351 bytes on wire (2808 bits), 351 bytes captured (2808 bits) on interface 0
▷ Ethernet II, Src: Vmware_99:59:f1 (00:50:56:99:59:f1), Dst: CiscoInc_29:96:c3 (00:1b:54:29:96:c3)
▷ Internet Protocol Version 4, Src: 10.48.36.26, Dst: 10.10.245.131
▷ Transmission Control Protocol, Src Port: 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
```

If it's left at **medium** TMS will only send version 1.0 in the SSL Client hello during the negotiation phase which specifies the highest TLS protocol version it supports as a client, which TMS is, in this case.

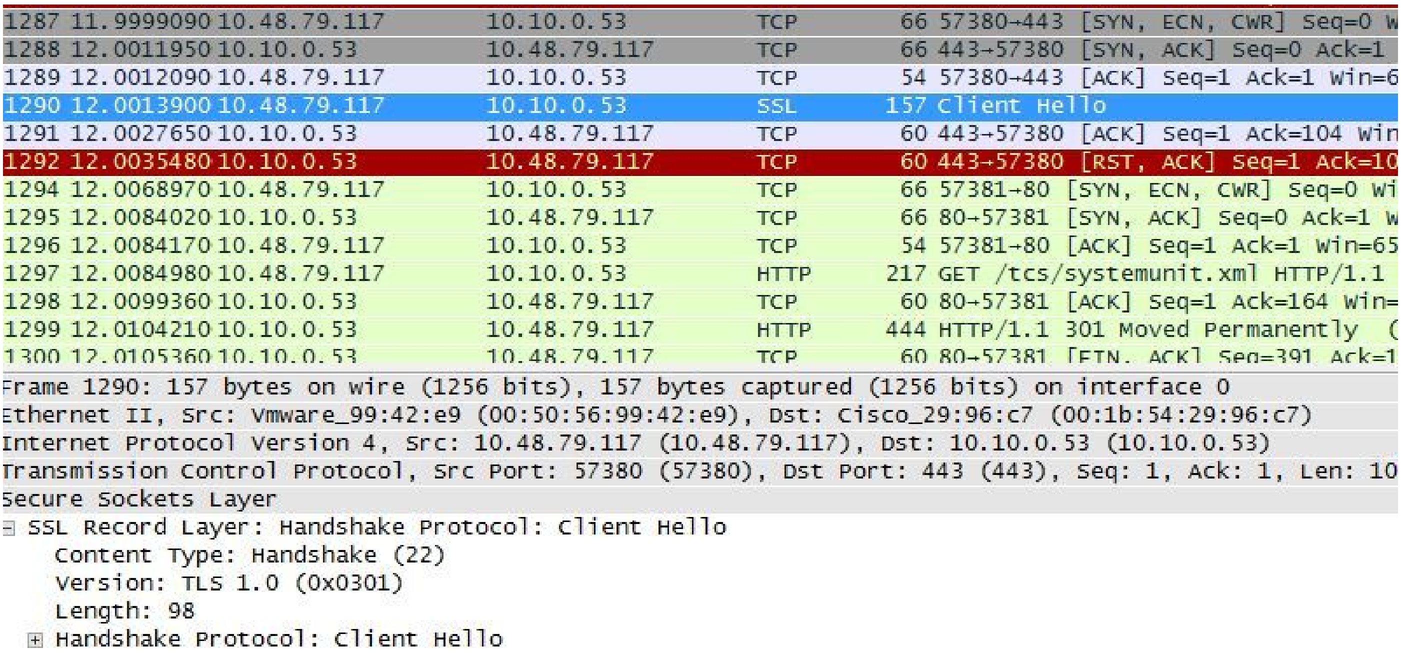
For TMS versions lower than 15

Step 1. Even though the TLS version 1.2 is added in the registry



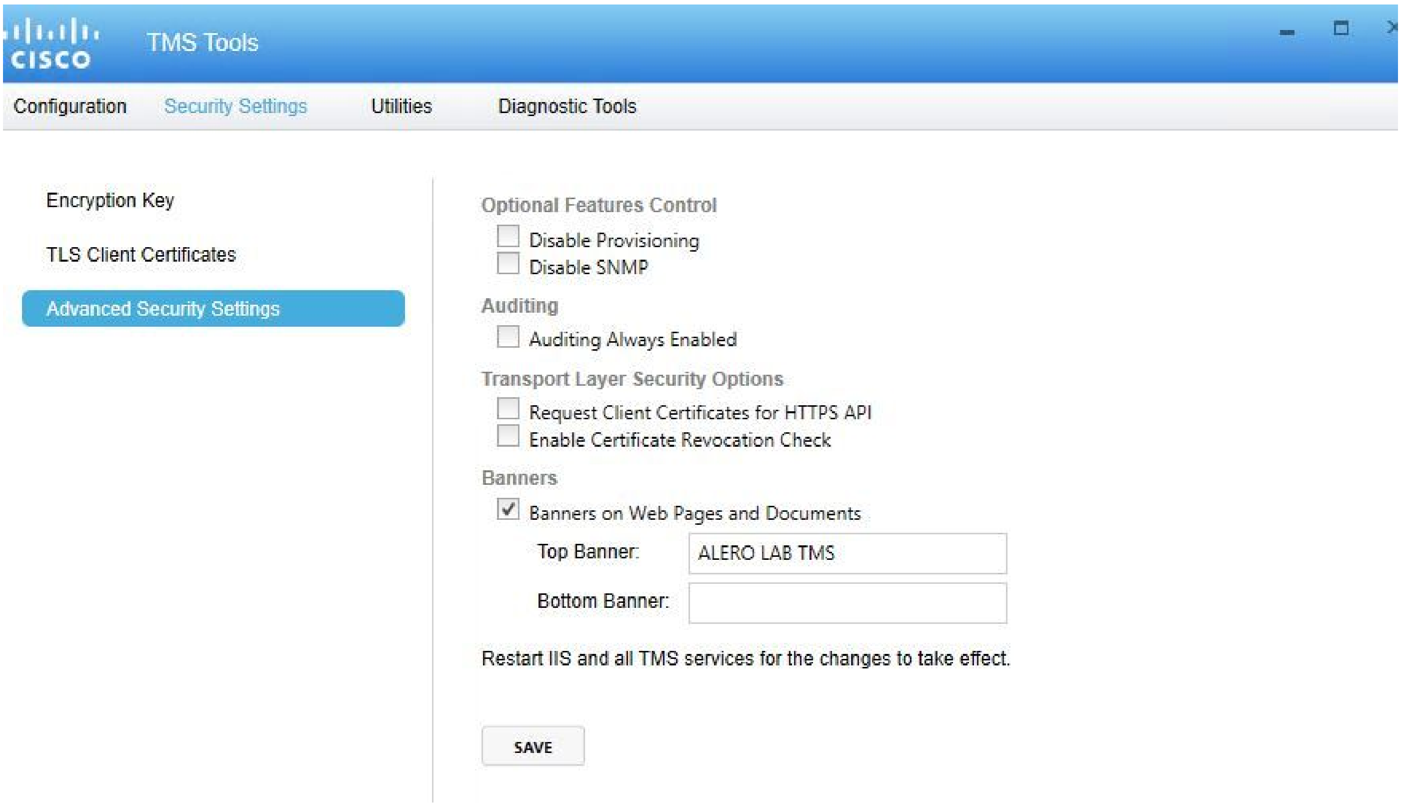
Name	Type	Data
(Default)	REG_SZ	(value not set)
DisabledByDefault	REG_DWORD	0x00000000 (0)
Enabled	REG_DWORD	0x00000001 (1)

Step 2. The TMS server still doesn't send the version supported by the Endpoint in its SSL client hello



```
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
```

Step 3. The problem then lies in the fact that we cannot change the TLS Options in TMS tools as this option is not available



Optional Features Control

□ Disable Provisioning
□ Disable SNMP

Auditing

□ Auditing Always Enabled

Transport Layer Security Options

□ Request Client Certificates for HTTPS API
□ Enable Certificate Revocation Check

Banners

☑ Banners on Web Pages and Documents

Top Banner: ALERO LAB TMS

Bottom Banner:

Restart IIS and all TMS services for the changes to take effect.

Step 4. Then the workaround for this issue is either upgrade TMS to 15.x or downgrade your TC/CE endpoints to 7.3.3, this issue is tracked in software defect CSCuz71542 created for version 14.6.X.