

如何在TC/CE终端升级以后排除故障“在TMS的没有HTTPS答复”错误

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[问题](#)

[解决方案](#)

[启用在TMS Windows服务器的TLS 1.1和1.2 TMS的15.x和更加高](#)

[在TMS工具的安全性变化](#)

[考虑事项为了升级安全设置](#)

[验证](#)

[对于TMS版本比15降低](#)

简介

本文描述如何排除故障“在网真管理套件(TMS)的没有HTTPS答复”消息。

[先决条件](#)

[要求](#)

Cisco 建议您了解以下主题：

- 思科TMS
- Windows 服务器

[使用的组件](#)

本文档中的信息基于以下软件版本：

- TC 7.3.6以上
- CE 8.1.0以上
- TMS 15.2.1
- Windows服务器2012 R2
- SQL server 2008 R2和2012

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

此问题出现，当终端被移植到TC 7.3.6和协作终端(CE)时8.1.0软件以上。

问题

在对TC7.3.6的终端升级以上或8.1.0以上和在终端和TMS之间的通信方法设置作为传输层安全(TLS)后，错误消息“HTTPS答复”在TMS不冒出通过选择终端，在系统>浏览器下。

这发生由于此情况。

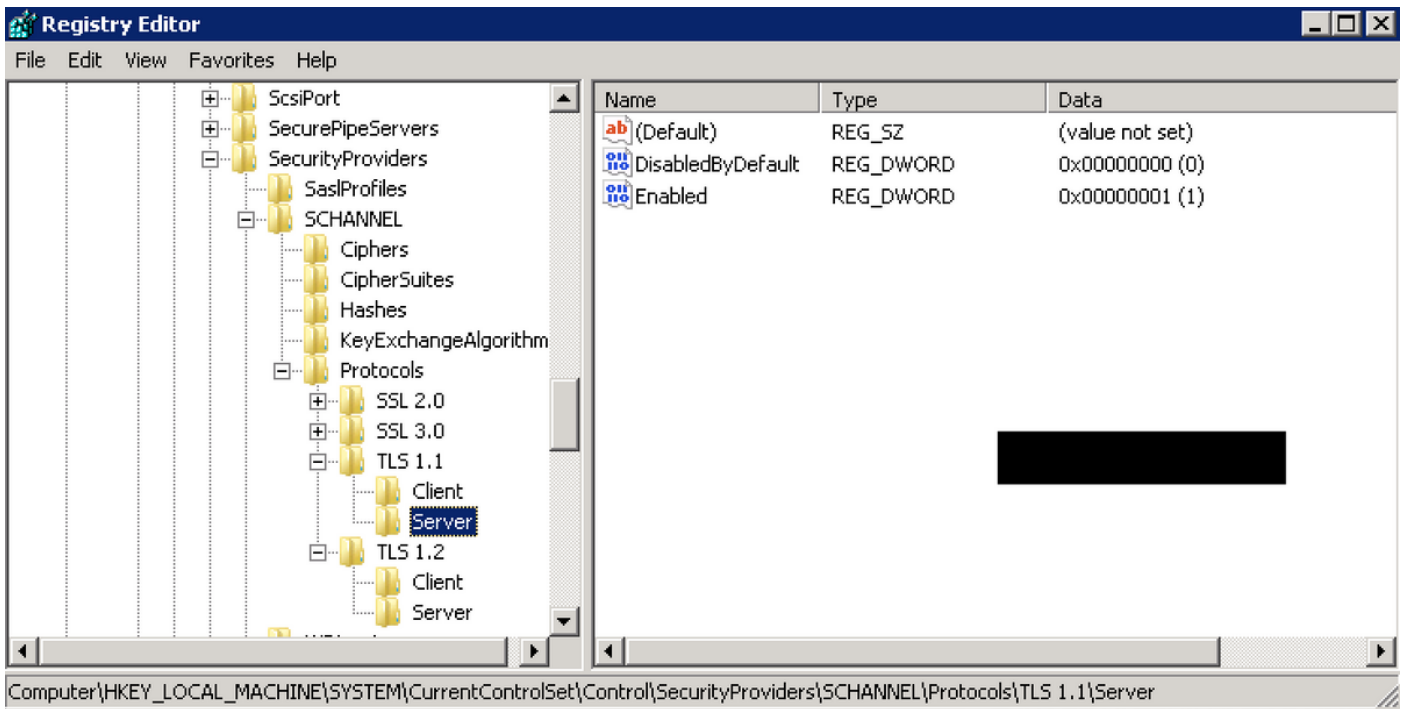
- 在不再上的TC 7.3.6和CE 8.1.0和根据版本注释支持TLS 1.0。
http://www.cisco.com/c/dam/en/us/td/docs/telepresence/endpoint/software/tc7/release_notes/tc-software-release-notes-tc7.pdf
- 默认情况下MS Windows服务器有禁用的TLS版本1.1和1.2。
- 默认情况下TMS工具在其传输层安全选项使用介质通信通信安全性。
- 当TLS版本1.0禁用时，并且两个TLS版本1.1和1.2启用，TMS不发送安全套接字层SSL客户端Hello，在TCP三通的握手成功与终端后。使用TLS版本1.2，能加密数据。
- 仍然，因为TMS只将发送或通告1.0在其客户端hello消息，启用TLS版本1.2使用工具或在Windows注册表不是足够。

解决方案

TMS安装的Windows服务器，需要有启用的TLS版本1.1和1.2，这可以用下个步骤完成。

启用在TMS Windows服务器的TLS 1.1和1.2 TMS的15.x和更加高

- 1.TMSWindows
- 2.(Start->Run->Regedit)
3.
 -
 -
 -
 -
 -
 - Save
4. Enable (event) TLS 1.1TLS 1.2
 -
 - HKEY_LOCAL_MACHINE-->SYSTEM--> Currentcontrolset-->> SecurityProviders--> SCHANNEL-->**
 - TLS 1.1TLS 1.2
 - TLS 1.1TLS 1.2
 - client'



DwordTLS

DisabledByDefault [Value = 0]

Enabled [Value = 1]

5.TLSTMS Windows

aplicable https://technet.microsoft.com/en-us/library/dn786418%28v=ws.11%29.aspx#BKMK_SchannelTR_TLS12

NARACTLS <https://www.nartac.com/Products/IISCrypto/Download>

在TMS工具的安全性变化

当正确版本启用时，请更改在TMS工具的安全设置有此步骤的。

步骤1.打开TMS工具

步骤2.导航对**安全设置>Advanced安全设置**

第三步：在**传输层安全选项下**，设置通信安全性为介质**海伊**

步骤4.点击**“Save”**

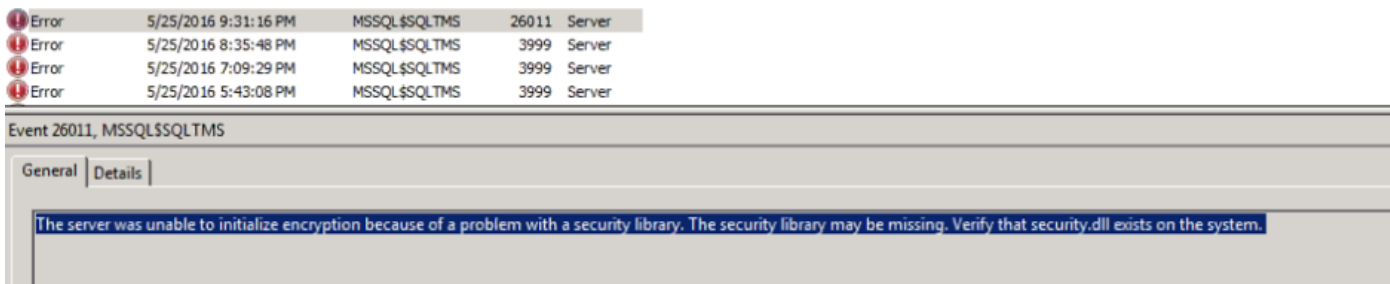
第五步：然后请重新启动**互联网信息服务(IIS)**在服务器和**TMSDatabaseScannerService**并且开始**TMSPLCMDirectoryService** (如果终止了)

警告：:: 当TLS选项更改给从介质的介质**海伊**，telnet和简单网络管理协议(SNMP)将禁用。这将造成**TMS SNMP service**终止，并且警报在TMS Web接口将被上升。

考虑事项为了升级安全设置

当SQL 2008 R2是在使用中和已安装在TMS Windows服务器时，我们需要保证TLS1.0和SSL3.0应该也启用或者SQL服务必须先停止和不会开始。

您必须发现此在事件日志的错误：



当SQL 2012是在使用中的时在TMS Windows服务器(<https://support.microsoft.com/en-us/kb/3052404>)要求更新处理TLS更改，如果安装

使用SNMP管理的终端或Telnet显示“安全侵害：Telnet通信没有允许”。



验证

当您更改从介质的TLS选项给介质海伊时，这保证TLS版本1.2在客户端Hello通告，在TCP三通的握手从TMS后成功：

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

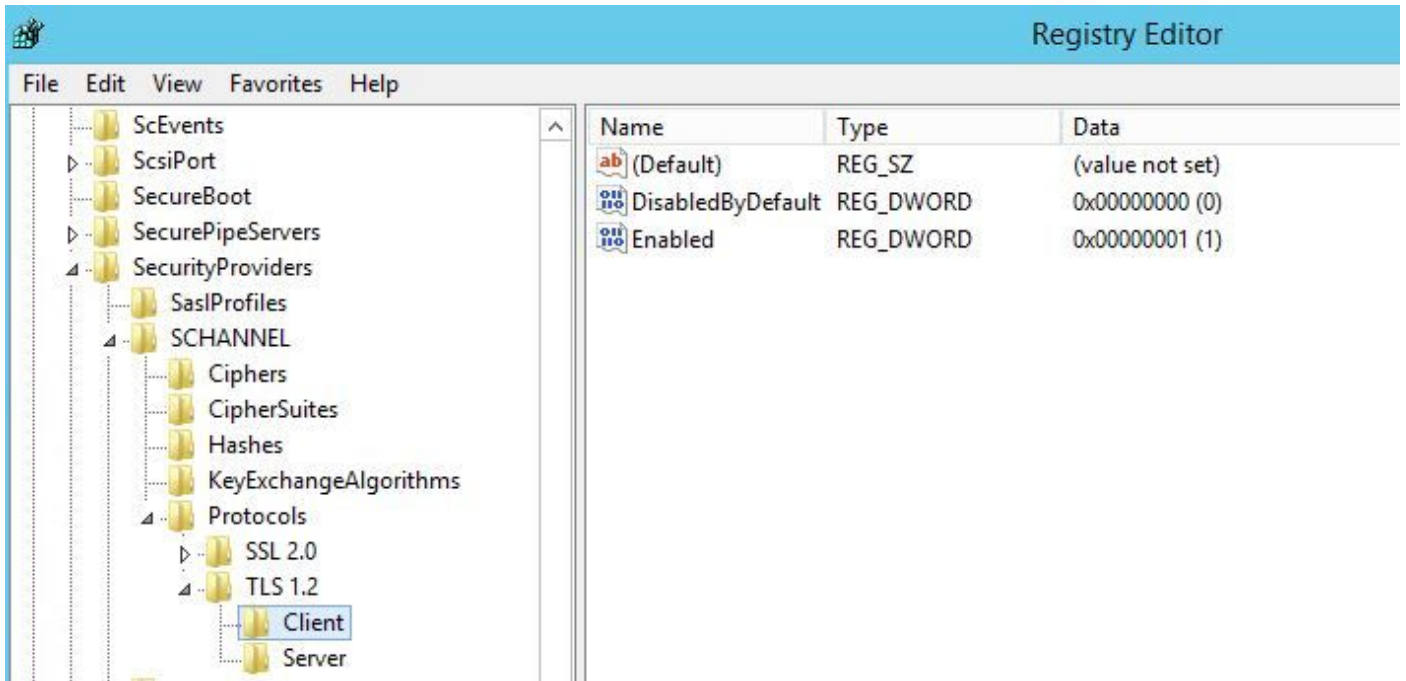
通告的TLS版本1.2：

```
▷ 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
```

如果它离开在中等TMS只将发送在SSL客户端Hello的版本1.0在指定最高的TLS协议版本支持作为客户端，TMS是的协商阶段期间，在这种情况下。

对于TMS版本比15请降低

步骤1.即使TLS版本1.2在注册被添加



第二步：TMS服务器仍然不发送在其SSL客户端Hello的终端支持的版本

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 [FTN, 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

第三步：问题在事实然后在我们不能更改在TMS工具的TLS选项，因为此选项不是可用的

Encryption Key

TLS Client Certificates

Advanced Security Settings

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: Bottom Banner:

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

SAVE

第四步：然后此问题的应急方案是升级TMS到15.x或降级您的TC/CE终端到7.3.3，此问题被跟踪在为版本14.6.X [CSCuz71542](#)创建的软件缺陷。