

Como solucionar problemas de erro "Sem resposta HTTPS" no TMS após a atualização de endpoints TC/CE

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Problema](#)

[Solução](#)

[Ative TLS 1.1 e 1.2 no TMS Windows Server para TMS 15.x e posterior](#)

[Alteração de segurança na ferramenta TMS](#)

[Considerações para atualizar as configurações de segurança](#)

[Verificar](#)

[Para versões TMS inferiores a 15](#)

Introduction

Este documento descreve como solucionar problemas de mensagem "sem resposta HTTPS" no Telepresence Management Suite (TMS).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco TMS
- Windows Server

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- TC 7.3.6 e superiores
- CE 8.1.0 e superior
- TMS 15.2.1
- Windows Server 2012 R2
- SQL Server 2008 R2 e 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.

Informações de Apoio

Esse problema ocorre quando os endpoints são migrados para o TC 7.3.6 e para o software Collaboration Endpoint (CE) 8.1.0 ou superior.

Problema

Após uma atualização de endpoint para TC7.3.6 ou superior ou 8.1.0 ou superior e o método de comunicação entre o endpoint e o TMS estiver configurado como Transport Layer Security (TLS), a mensagem de erro "no HTTPS response" aparece no TMS selecionando o Endpoint, em **System > Navigator**.

Isso acontece como resultado dessas situações.

- O TC 7.3.6 e o CE 8.1.0 e posterior não suportam mais TLS 1.0 conforme as notas de versão.
http://www.cisco.com/c/dam/en/us/td/docs/telepresence/endpoint/software/tc7/release_notes/tc-software-release-notes-tc7.pdf
- O servidor Microsoft Windows tem TLS versão 1.1 e 1.2 desabilitadas por padrão.
- Por padrão, as ferramentas do TMS usam o Medium Communication Security em suas opções de segurança da camada de transporte.
- Quando a versão 1.0 do TLS está desativada e as versões 1.1 e 1.2 do TLS estão ativadas, o TMS não envia a saudação do cliente SSL (Secure Socket Layer) depois que o handshake triplo do TCP é bem-sucedido com o Endpoint. No entanto, ainda é possível criptografar dados usando TLS versão 1.2.
- Ativar o TLS versão 1.2 usando uma ferramenta ou no Registro do Windows não é suficiente, pois o TMS ainda enviará ou anunciará apenas 1.0 em suas mensagens de saudação do cliente.

Solução

O servidor Windows onde o TMS está instalado, precisa ter o TLS versão 1.1 e 1.2 habilitado, isso pode ser feito com o próximo procedimento.

Ative TLS 1.1 e 1.2 no TMS Windows Server para TMS 15.x e posterior

Etapa 1. Abra uma Conexão de Área de Trabalho Remota para o Windows Server onde o TMS está instalado.

Etapa 2. Abra o editor do Registro do Windows (**Iniciar->Executar->Regedit**).

Etapa 3. Faça backup do Registro.

Se for solicitada uma senha ou confirmação de administrador, digite a senha ou forneça a confirmação.

Localize e clique na chave ou subchave de backup.

Clique no menu Arquivo e clique em Exportar.

Na caixa Salvar em, selecione o local onde deseja salvar a cópia de backup e digite um nome para o arquivo de backup na caixa Nome do arquivo.

Click Save.

Etapa 4. Ative TLS 1.1 e TLS 1.2.

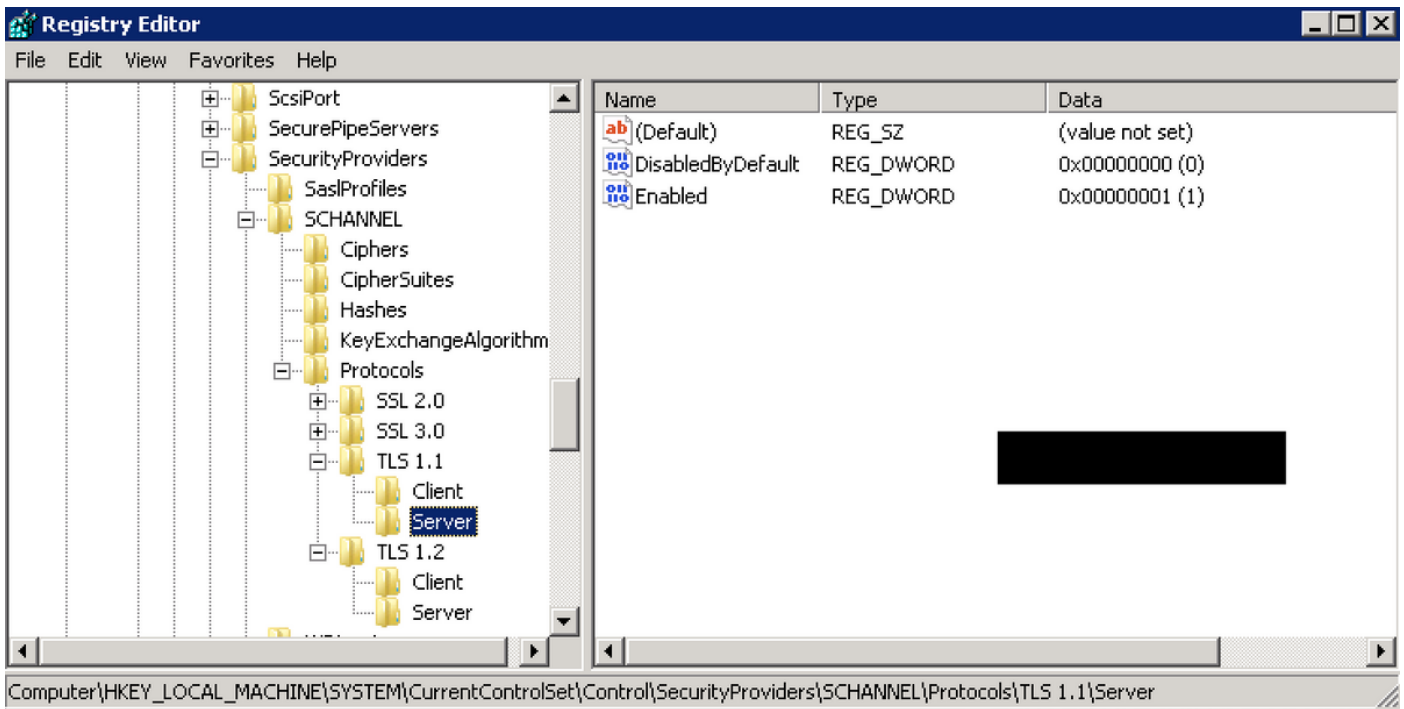
Abrir registro

Navegue até **HKEY_LOCAL_MACHINE** —> **SYSTEM** —> **CurrentControlSet** —> **Control** —> **SecurityProviders**—> **SCHANNEL** —> **Protocolos**

Adicionar suporte TLS 1.1 e TLS 1.2

Criar pastas TLS 1.1 e TLS 1.2

Criar subchaves como cliente e servidor



Crie **DWORDs** para Cliente e Servidor para cada chave TLS criada.

DisabledByDefault [Value = 0]

Enabled [Value = 1]

Etapa 5. Reinicie o servidor do TMS Windows para garantir que o TLS entre em vigor.

Note: Visite este link para obter informações específicas sobre as versões aplicáveis https://technet.microsoft.com/en-us/library/dn786418%28v=ws.11%29.aspx#BKMK_SchanelTR_TLS12

Dica: a ferramenta NARTAC pode ser usada para desativar as versões TLS necessárias depois que você fizer isso, precisará reiniciar o servidor. Você pode fazer o download desse link <https://www.nartac.com/Products/IISCrypto/Download>

Alteração de segurança na ferramenta TMS

Quando as versões corretas estiverem ativadas, altere as configurações de segurança em Ferramentas TMS com este procedimento.

Etapa 1. Abrir ferramentas do TMS

Etapa 2. Navegue até **Configurações de segurança** > **Configurações avançadas de segurança**

Etapa 3. Em **Transport Layer Security Options**, defina a Communication Security como **Medium-High**

Etapa 4. Clique em **Salvar**

Etapa 5. Em seguida, reinicie os Serviços de Informações da Internet (IIS) no servidor e o

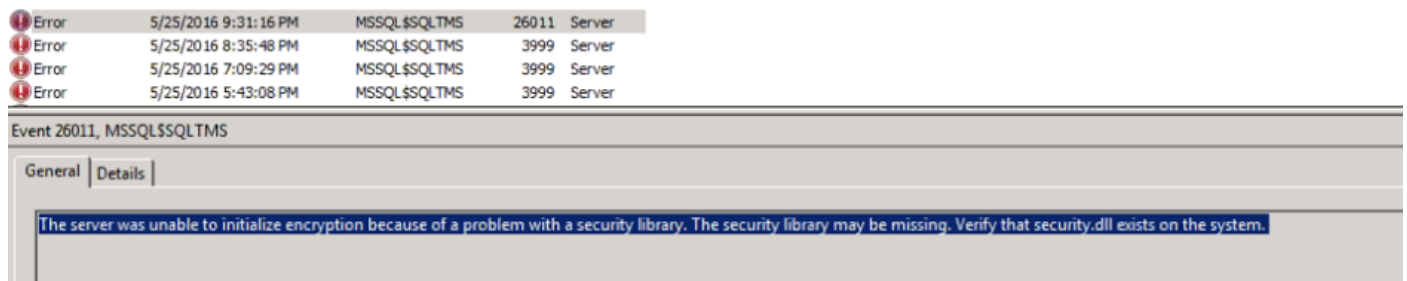
TMSDatabaseScannerService e inicie o TMSPLCMDirectoryService (se ele estiver parado)

aviso: : Quando a opção TLS é alterada para Medium-High de Medium, telnet e Simple Network Management Protocol (SNMP) serão desativados. Isso fará com que o serviço TMS SNMP seja interrompido e um alerta será gerado na interface da Web do TMS.

Considerações para atualizar as configurações de segurança

Quando o **SQL 2008 R2** está em uso e instalado no servidor do TMS windows, precisamos garantir que TLS1.0 e SSL3.0 também estejam ativados ou que o serviço SQL pare e ele não inicie.

Você deve ver esses erros no registro de eventos:



Icon	Time	Source	ID	Category
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

General Details

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.

Quando o **SQL 2012** está em uso, ele precisa ser atualizado para lidar com a alteração de TLS se instalado no servidor do Windows do TMS (<https://support.microsoft.com/en-us/kb/3052404>)

Endpoints gerenciados usando SNMP ou Telnet mostram "Violação de segurança: A comunicação Telnet não é permitida".



MI-AHOC-HDX-Test2

Polycm 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

Edit Settings Ticket Filters Ticket Log

Tickets

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.

Add custom ticket Open system in System Navigator

Verificar

Quando você altera a opção TLS de **Médio** para **Médio a Alto**, isso garante que o TLS versão 1.2 seja anunciado no **Cliente Hello** após o handshake triplo TCP ter êxito do 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 versão 1.2 anunciada:

```

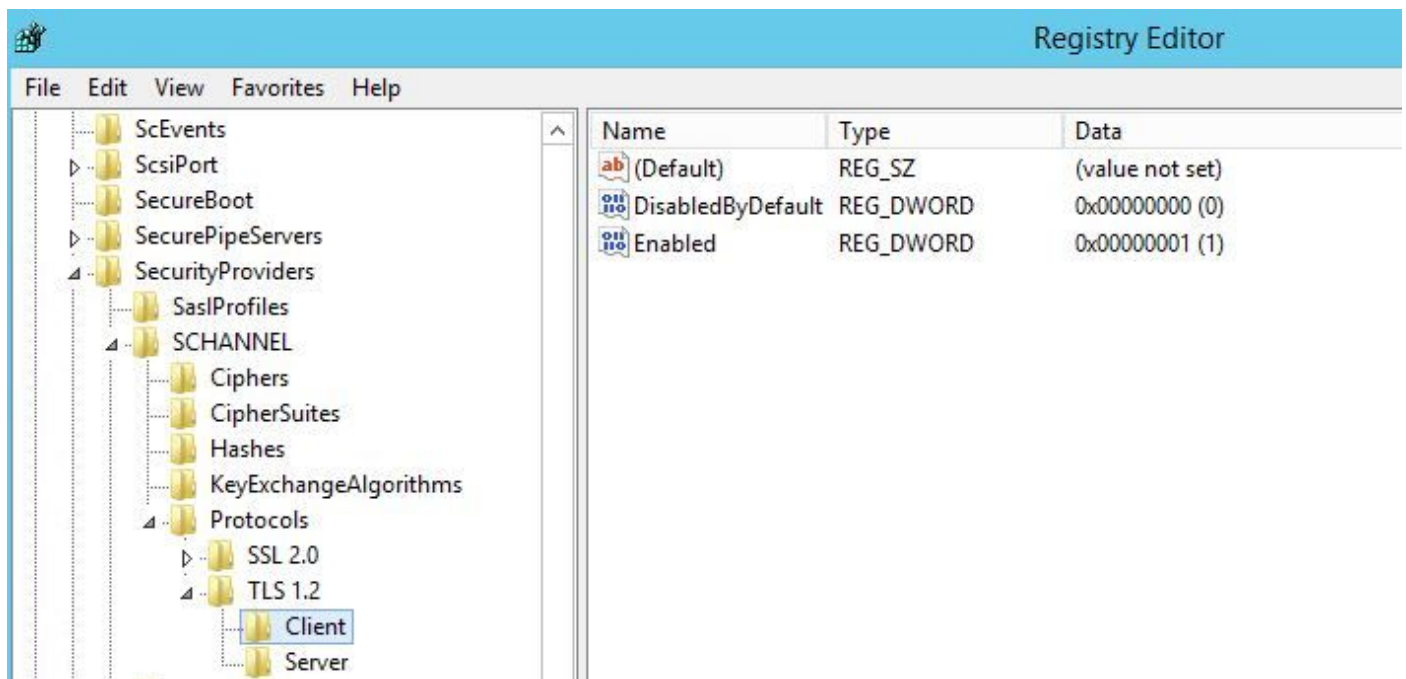
> Frame 787: 351 bytes on wire (2808 bits), 351 bytes captured (2808 bits) on interface 0
> Ethernet II, Src: Vmware_99:59:f1 (00:50:56:99:59:f1), Dst: CiscoInc_29:96:c3 (00:1b:54:29:96:c3)
> Internet Protocol Version 4, Src: 10.48.36.26, Dst: 10.10.245.131
> Transmission Control Protocol, Src Port: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

```

Se for deixado no **meio**, o TMS enviará somente a versão 1.0 na saudação do cliente SSL durante a fase de negociação, que especifica a versão mais alta do protocolo TLS que ele suporta como um cliente, que é o TMS, neste caso.

Para versões TMS inferiores a 15

Etapa 1. Embora a versão 1.2 do TLS seja adicionada no registro



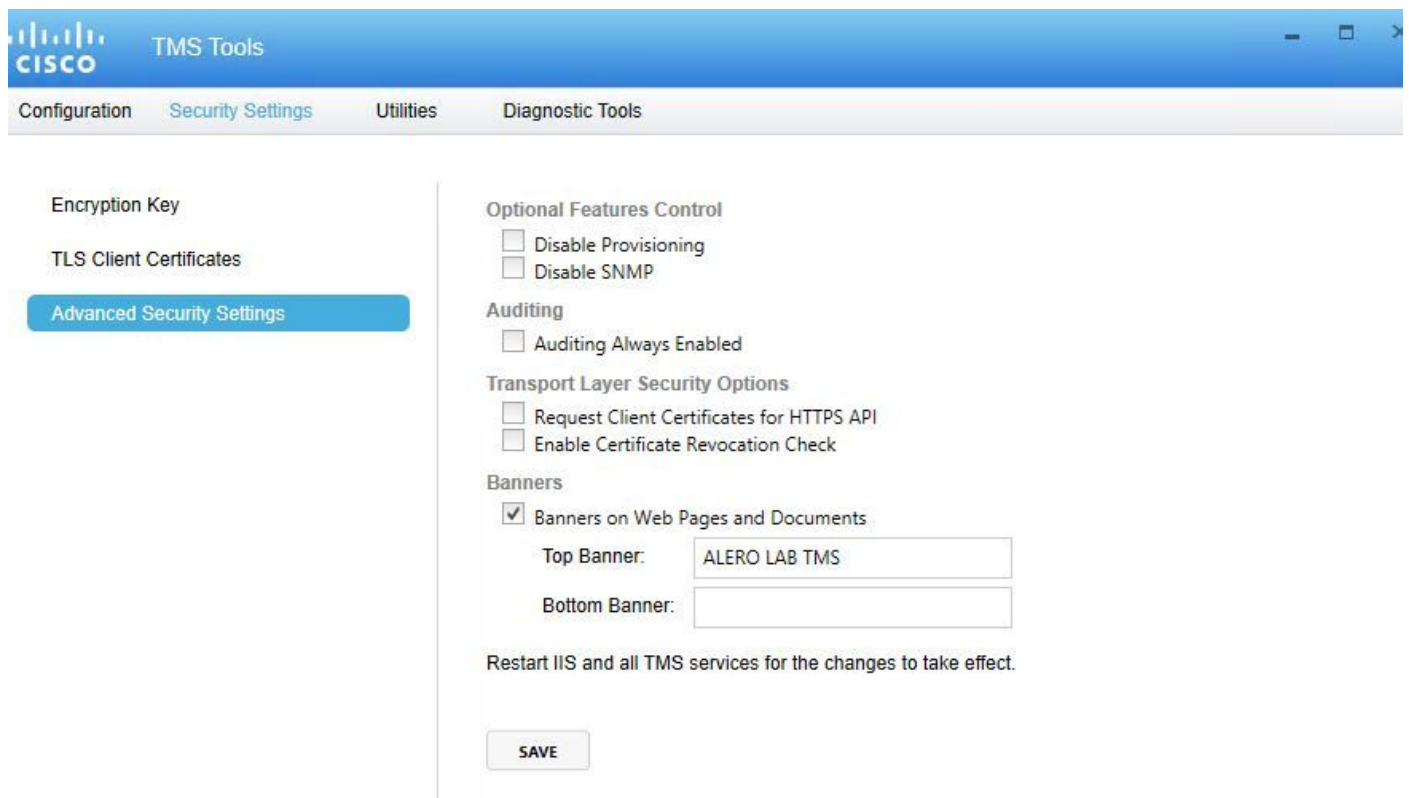
Etapa 2. O servidor TMS ainda não envia a versão suportada pelo Endpoint em sua saudação de cliente SSL

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 [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

Etapa 3. O problema, então, está no fato de que não podemos alterar as opções TLS nas ferramentas TMS porque essa opção não está disponível



Etapa 4. Em seguida, a solução para esse problema é atualizar o TMS para 15.x ou rebaixar seus endpoints TC/CE para 7.3.3, esse problema é rastreado no defeito de software [CSCuz71542](#) criado para a versão 14.6.X.