

Cómo solucionar el error "Sin respuesta HTTPS" en TMS después de la actualización de terminales TC/CE

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Problema](#)

[Solución](#)

[Habilitar TLS 1.1 y 1.2 en TMS Windows Server para TMS 15.x y versiones posteriores](#)

[Cambio de seguridad en la herramienta TMS](#)

[Consideraciones para actualizar la configuración de seguridad](#)

[Verificación](#)

[Para versiones TMS inferiores a 15](#)

Introducción

Este documento describe cómo resolver problemas del mensaje "sin respuesta HTTPS" en Telepresence Management Suite (TMS).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco TMS
- Windows Server

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

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

Antecedentes

Este problema se produce cuando los terminales se migran a TC 7.3.6 y al software Collaboration Endpoint (CE) 8.1.0 o posterior.

Problema

Después de una actualización del terminal a TC7.3.6 o posterior o a 8.1.0 o posterior y de configurar el método de comunicación entre el terminal y TMS como Transport Layer Security (TLS), aparece el mensaje de error "no HTTPS response" en TMS seleccionando el terminal, en **System > Navigator**.

Esto ocurre como resultado de estas situaciones.

- TC 7.3.6 y CE 8.1.0 y superiores ya no admiten TLS 1.0 según las notas de la versión.
http://www.cisco.com/c/dam/en/us/td/docs/telepresence/endpoint/software/tc7/release_notes/tc-software-release-notes-tc7.pdf
- El servidor de Microsoft Windows tiene las versiones 1.1 y 1.2 de TLS desactivadas de forma predeterminada.
- Las herramientas de TMS utilizan la seguridad de comunicación media en sus opciones de seguridad de la capa de transporte de forma predeterminada.
- Cuando TLS versión 1.0 está inhabilitada y las versiones 1.1 y 1.2 de TLS están habilitadas, TMS no envía saludo al cliente de Secure Socket Layer (SSL) después de que el intercambio de señales TCP de 3 vías tenga éxito con el terminal. Sin embargo, aún puede cifrar los datos mediante la versión 1.2 de TLS.
- La habilitación de la versión 1.2 de TLS con una Herramienta o en el Registro de Windows no es suficiente, ya que TMS sólo enviará o anunciará 1.0 en sus mensajes hello de cliente.

Solución

El servidor de Windows donde está instalado TMS necesita tener TLS versión 1.1 y 1.2 habilitado, esto se puede lograr con el siguiente procedimiento.

Habilitar TLS 1.1 y 1.2 en TMS Windows Server para TMS 15.x y versiones posteriores

Paso 1. Abra una conexión de Escritorio remoto a Windows Server donde TMS está instalado.

Paso 2. Abra el editor del Registro de Windows (**Inicio ->Ejecutar ->Regedit**).

Paso 3. Realice la copia de seguridad del Registro.

Si se le solicita una contraseña o confirmación del administrador, escriba la contraseña o proporcione confirmación.

Busque y haga clic en la clave o subclave de la que desea realizar una copia de seguridad.

Haga clic en el menú Archivo y, a continuación, haga clic en Exportar.

En el cuadro Guardar en, seleccione la ubicación en la que desea guardar la copia de seguridad y, a continuación, escriba un nombre para el archivo de copia de seguridad en el cuadro Nombre de archivo.

Click Save.

Paso 4. Habilite TLS 1.1 y TLS 1.2.

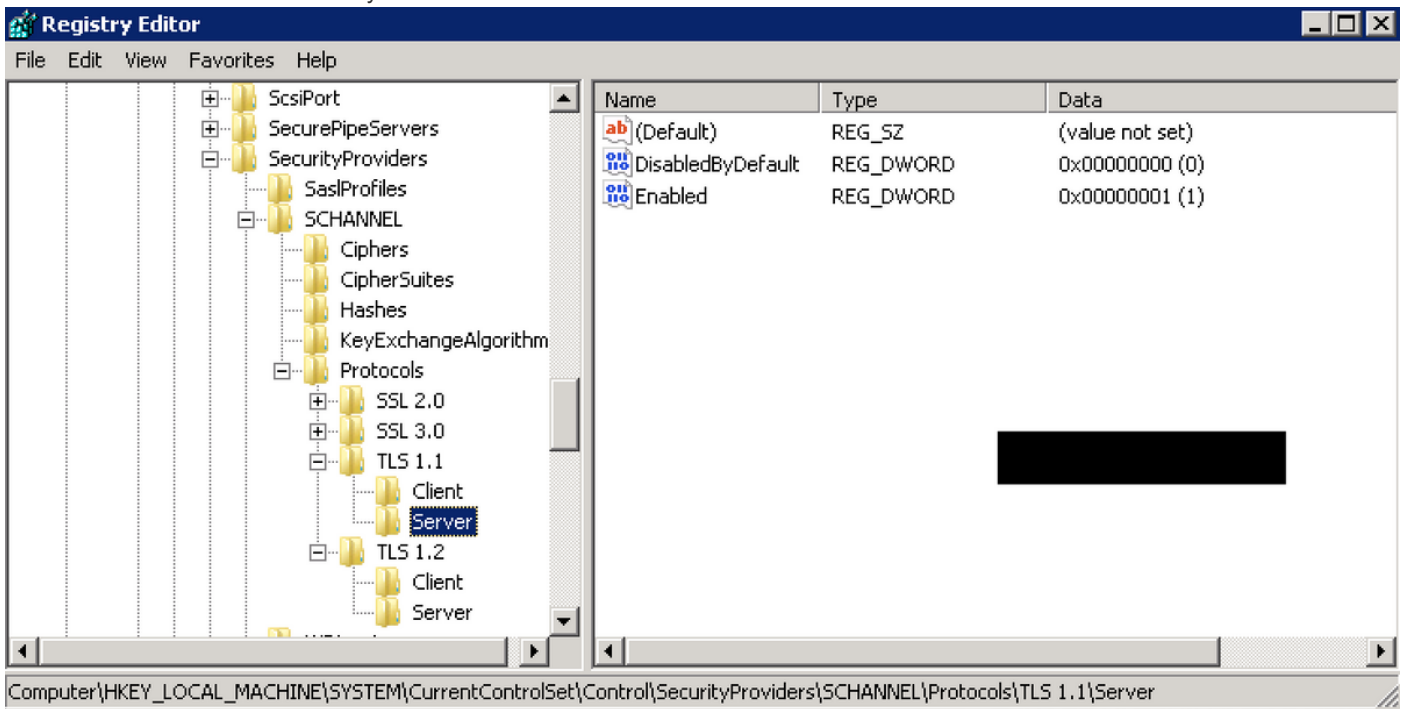
Registro abierto

Vaya a **HKEY_LOCAL_MACHINE** → **SYSTEM** → **CurrentControlSet** → **Control** → **SecurityProviders** → **SCHANNEL** → **Protocolos**

Agregar compatibilidad con TLS 1.1 y TLS 1.2

Crear carpetas TLS 1.1 y TLS 1.2

Crear subclaves como cliente y servidor



Cree **DWORD** tanto para el Cliente como para el Servidor para cada clave TLS creada.

DisabledByDefault [Value = 0]

Enabled [Value = 1]

Paso 5. Reinicie el servidor TMS de Windows para asegurarse de que TLS surta efecto.

Nota: Visite este enlace para obtener información específica sobre las versiones aplicables

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

Sugerencia: la herramienta NARTAC se puede utilizar para inhabilitar las versiones TLS necesarias después de hacerlo, es necesario reiniciar el servidor. Puede descargarlo de este enlace <https://www.nartac.com/Products/IISCrypto/Download>

Cambio de seguridad en la herramienta TMS

Cuando se habiliten las versiones correctas, cambie la configuración de seguridad en TMS Tools con este procedimiento.

Paso 1. Herramientas TMS abiertas

Paso 2. Vaya a **Security Settings > Advanced Security Settings**

Paso 3. En **Opciones de seguridad de la capa de transporte**, establezca la seguridad de comunicación en **Mediana-Alta**

Paso 4. Haga clic en **Save (Guardar)**.

Paso 5. A continuación, reinicie los Servicios de Internet Information Server (IIS) en el servidor y

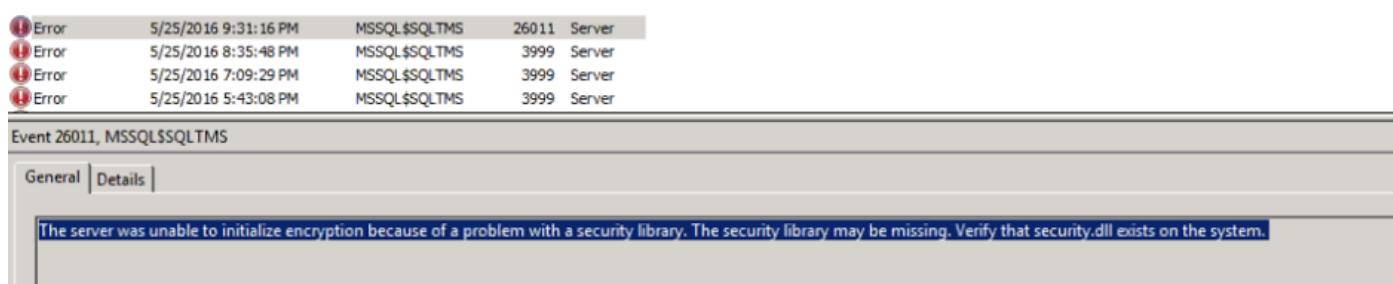
TMSDatabaseScannerService e inicie TMSPLCMDirectoryService (si se ha detenido)

Advertencia: : cuando la opción TLS se cambia a Media-Alta desde Media, Telnet y el protocolo simple de administración de red (SNMP) se desactivarán. Esto hará que TMS SNMPservice se detenga y se producirá una alerta en la interfaz web de TMS.

Consideraciones para actualizar la configuración de seguridad

Cuando **SQL 2008 R2** está en uso e instalado en TMS windows server, necesitamos asegurar que TLS1.0 y SSL3.0 también deberían estar habilitados o que el servicio SQL se detenga y no se inicie.

Debe ver estos errores en el 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.

Cuando **SQL 2012** está en uso, debe actualizarse para hacer frente al cambio de TLS si se instala en el servidor TMS windows (<https://support.microsoft.com/en-us/kb/3052404>)

Los terminales administrados mediante SNMP o Telnet muestran "Violación de seguridad: No se permite la comunicación Telnet".



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

Verificación

Cuando cambia la opción TLS de **Media** a **Media-Alta**, esto asegura que la versión 1.2 de TLS se anuncie en el **Cliente Hello** después de que el intercambio de señales TCP de 3 direcciones tenga éxito desde 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 versión 1.2 anunciada:

```

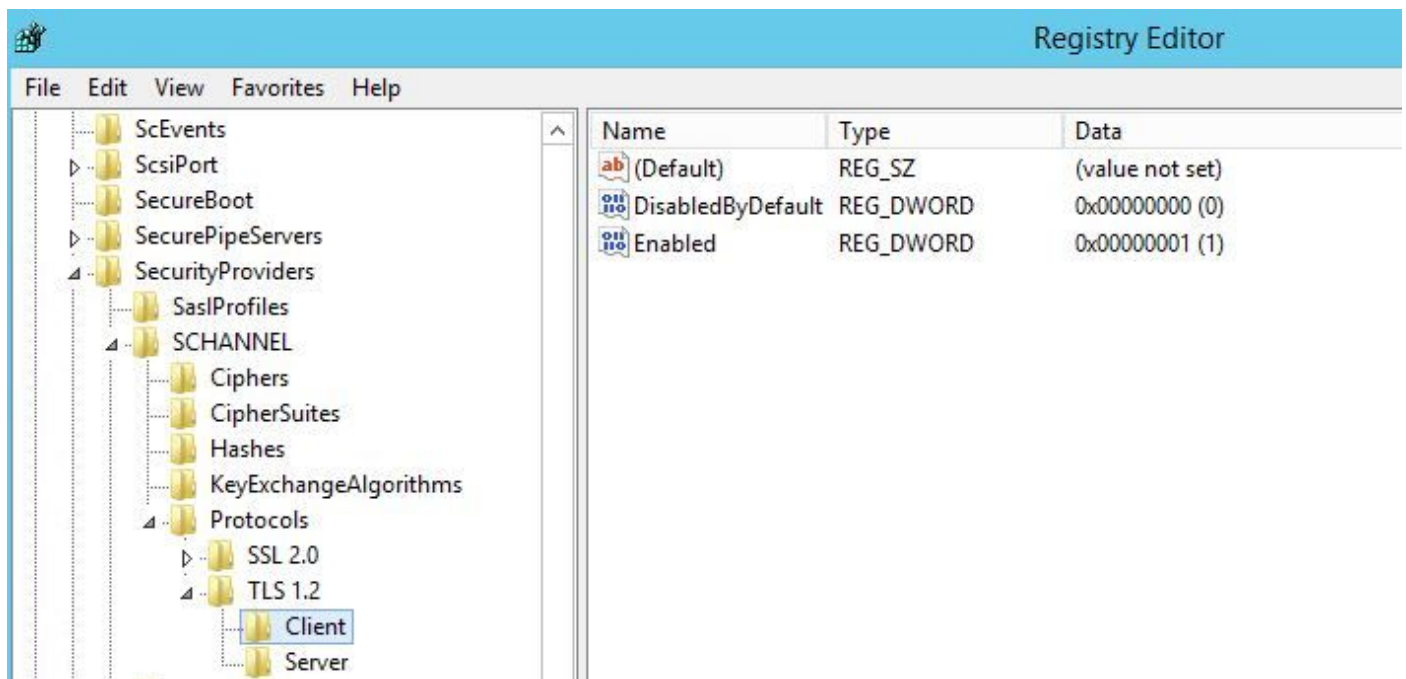
> Frame 787: 351 bytes on wire (2808 bits), 351 bytes captured (2808 bits) on interface 0
> Ethernet II, Src: Vmware_99:59:f1 (00:50:56:99:59:f1), Dst: CiscoInc_29:96:c3 (00:1b:54:29:96:c3)
> Internet Protocol Version 4, Src: 10.48.36.26, Dst: 10.10.245.131
> Transmission Control Protocol, Src Port: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

```

Si se deja en el **medio** TMS sólo enviará la versión 1.0 en el saludo de SSL Client durante la fase de negociación que especifica la versión de protocolo TLS más alta que soporta como cliente, que TMS es, en este caso.

Para versiones TMS inferiores a 15

Paso 1. Aunque la versión 1.2 de TLS se agrega en el registro



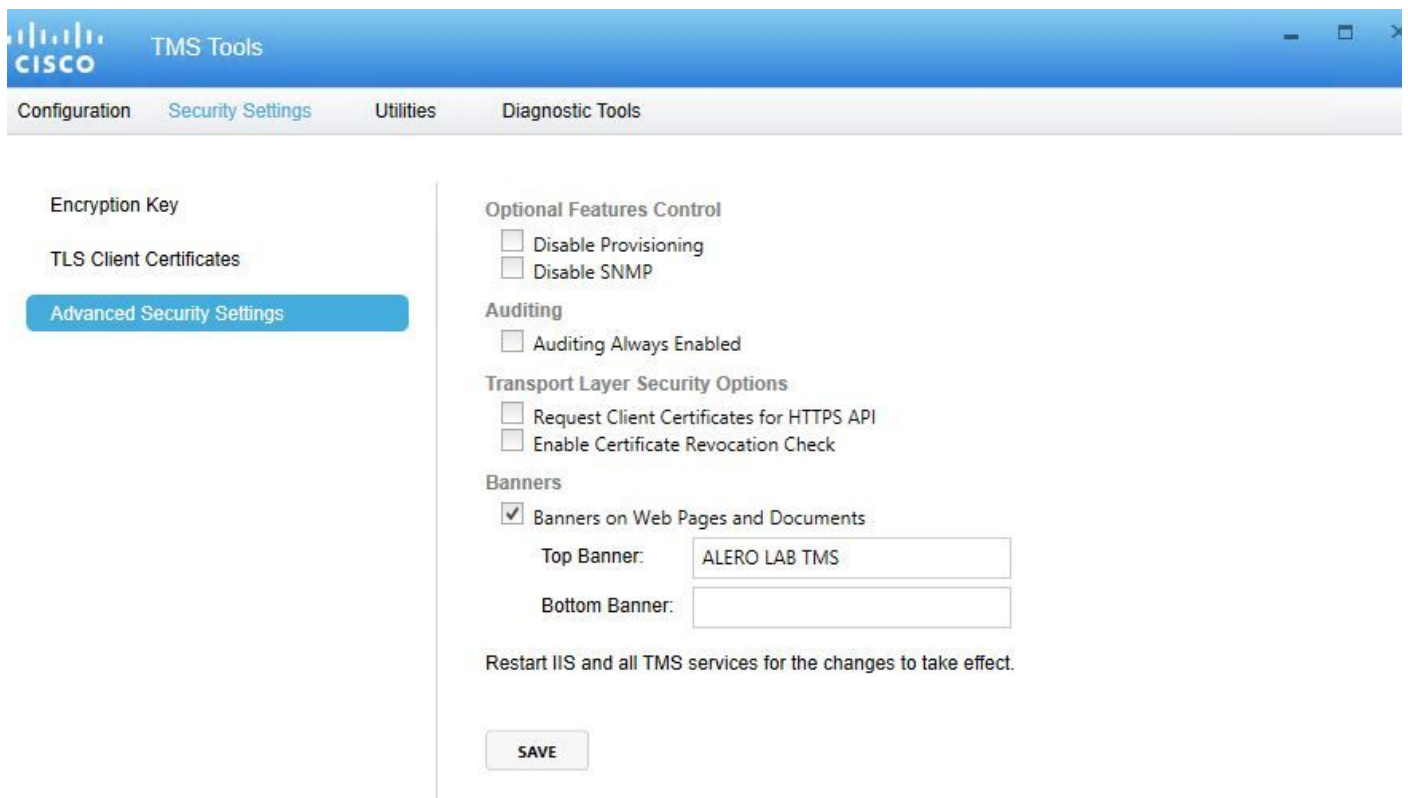
Paso 2. El servidor TMS todavía no envía la versión admitida por el terminal en su cliente SSL hello

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 [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

Paso 3. El problema radica entonces en el hecho de que no podemos cambiar las opciones de TLS en las herramientas de TMS ya que esta opción no está disponible



Paso 4. A continuación, la solución temporal para este problema es actualizar TMS a 15.x o rebajar los terminales TC/CE a 7.3.3. Este problema se rastrea en el defecto de software [CSCuz71542](#) creado para la versión 14.6.X.