Beheben des Fehlers "Keine HTTPS-Antwort" bei TMS nach Aktualisierung von TC-/CE-Endgeräten

Inhalt

[Einführung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Hintergrundinformationen](#)
[Problem](#)
[Lösung](#)
[Aktivieren Sie TLS 1.1 und 1.2 auf TMS Windows Server für TMS 15.x und höher.](#)
[Sicherheitsänderung beim TMS-Tool](#)
[Überlegungen zum Aktualisieren der Sicherheitseinstellungen](#)
[Überprüfen](#)
[Für TMS-Versionen unter 15](#)

Einführung

In diesem Dokument wird beschrieben, wie die Meldung "Keine HTTPS-Antwort" in der Telepresence Management Suite (TMS) behoben wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco TMS
- Windows-Server

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Softwareversionen:

- TC 7.3.6 und höher
- CE 8.1.0 und höher
- TMS 15.2.1
- Windows Server 2012 R2
- SQL Server 2008 R2 und 2012

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren

(Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Dieses Problem tritt auf, wenn die Endpunkte zur Software TC 7.3.6 und Collaboration Endpoint (CE) 8.1.0 oder höher migriert werden.

Problem

Nach einem Endpunkt-Upgrade auf TC7.3.6 oder höher oder 8.1.0 oder höher und die Kommunikationsmethode zwischen Endgerät und TMS als Transport Layer Security (TLS) eingerichtet, wird die Fehlermeldung "no HTTPS response" (Keine HTTPS-Antwort) in TMS angezeigt, indem Sie unter **System > Navigator** den Endpunkt auswählen.

Dies geschieht aufgrund dieser Situationen.

- TC 7.3.6 und CE 8.1.0 und höher unterstützen TLS 1.0 nicht mehr, wie in den Versionshinweisen beschrieben. http://www.cisco.com/c/dam/en/us/td/docs/telepresence/endpoint/software/tc7/release_notes/tc-software-release-notes-tc7.pdf

- Auf dem Microsoft Windows-Server sind die TLS-Versionen 1.1 und 1.2 standardmäßig deaktiviert.
- TMS-Tools verwenden standardmäßig Medium Communication Security in ihren Transport Layer Security-Optionen.
- Wenn die TLS-Version 1.0 deaktiviert und beide TLS-Versionen 1.1 und 1.2 aktiviert sind, sendet die TMS nach dem erfolgreichen TCP-Handshake mit dem Endpunkt keinen SSL-Client (Secure Socket Layer). Die Daten können jedoch weiterhin mit TLS-Version 1.2 verschlüsselt werden.
- Die Aktivierung von TLS Version 1.2 mithilfe eines Tools oder in der Windows-Registrierung ist nicht ausreichend, da die TMS immer noch nur 1.0 in ihren Client-Hello-Nachrichten sendet oder ankündigt.

Lösung

Auf dem Windows-Server, auf dem das TMS installiert ist, müssen die TLS-Versionen 1.1 und 1.2 aktiviert sein. Dies kann mit der nächsten Prozedur erreicht werden.

Aktivieren Sie TLS 1.1 und 1.2 auf TMS Windows Server für TMS 15.x und höher.

Schritt 1: Öffnen Sie eine Remotedesktopverbindung zu Windows Server, auf dem TMS installiert ist.

Schritt 2: Öffnen Sie den Windows-Registrierungseditor (**Start**->**Ausführen**->**Regedit**).

Schritt 3: Sicherung der Registrierung

Wenn Sie zur Eingabe eines Administrator-Kennworts oder einer Bestätigung aufgefordert werden, geben Sie das Kennwort ein, oder bestätigen Sie es.
Suchen Sie den Schlüssel oder den Unterschlüssel, den Sie sichern möchten, und klicken Sie darauf.
Klicken Sie auf das Menü Datei und anschließend auf Exportieren.
Wählen Sie im Feld Speichern in den Speicherort aus, an dem die Sicherungskopie gespeichert werden soll, und geben Sie dann einen Namen für die Sicherungsdatei in das Feld Dateiname ein.

Klicken Sie auf Speichern.

Schritt 4: Aktivieren Sie TLS 1.1 und TLS 1.2.

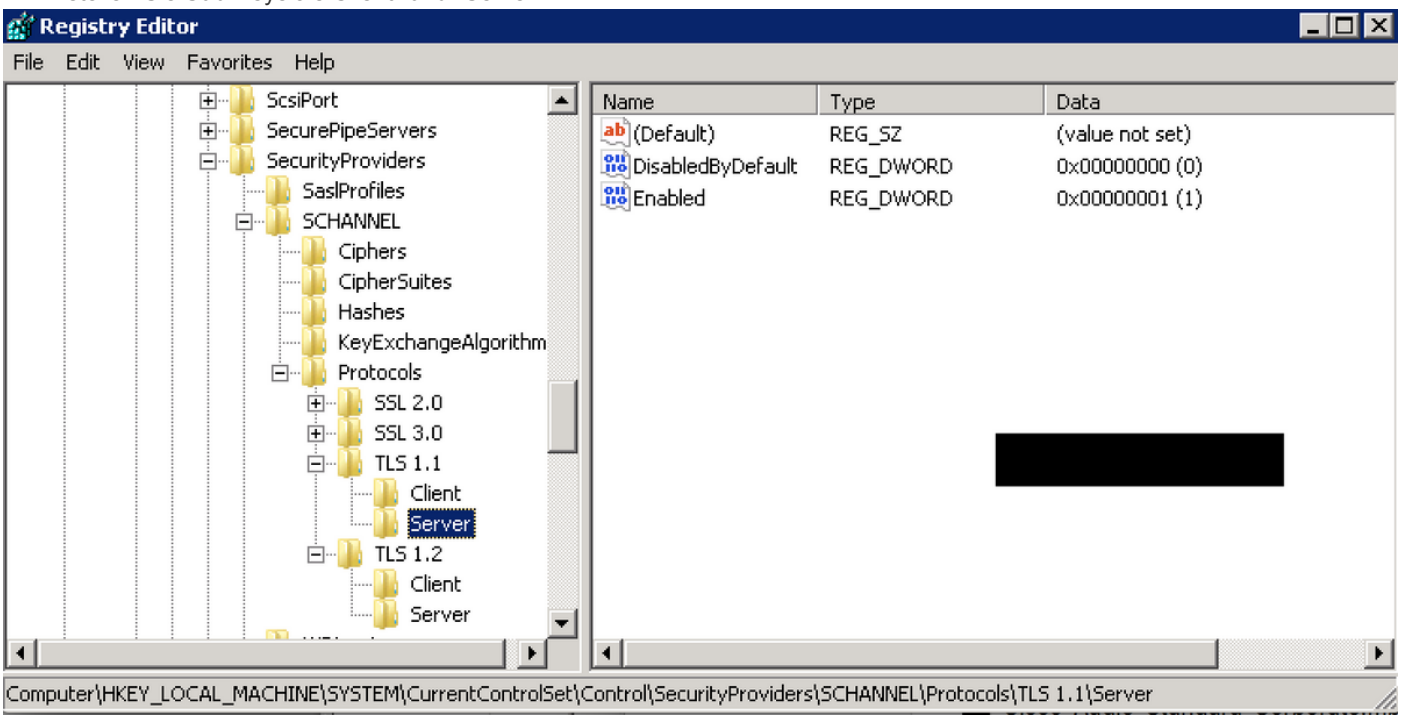
Registrierung öffnen

Navigieren Sie zu **HKEY_LOCAL_MACHINE —> SYSTEM —> CurrentControlSet —> Control —> SEKurityProvider—> SCHANNEL —> Protokolle**

Unterstützung für TLS 1.1 und TLS 1.2

Erstellen von Ordnern für TLS 1.1 und TLS 1.2

Erstellen Sie Sub-Keys als Client" und "Server".



Erstellen Sie **DWORDs** für Client und Server für jeden erstellten TLS-Schlüssel.

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

Schritt 5: Starten Sie den TMS Windows-Server neu, um sicherzustellen, dass TLS wirksam wird.

> **Hinweis**: Unter diesem Link finden Sie weitere Informationen zu den entsprechenden Versionen https://technet.microsoft.com/en-us/library/dn786418%28v=ws.11%29.aspx#BKMK_SchannelTR_TLS12

> **Tipp**: Mit dem NARTAC-Tool können Sie nach dem Neustart des Servers die benötigten TLS-Versionen deaktivieren. Sie können es über diesen Link herunterladen https://www.nartac.com/Products/IISCrypto/Download

Sicherheitsänderung beim TMS-Tool

Wenn die richtigen Versionen aktiviert sind, ändern Sie mit diesem Verfahren die Sicherheitseinstellungen unter TMS-Tools.

Schritt 1: TMS-Tools öffnen

Schritt 2: Navigieren Sie zu **Sicherheitseinstellungen > Erweiterte Sicherheitseinstellungen.**

Schritt 3: Legen Sie unter **Transportschichtsicherheitsoptionen** die Kommunikationssicherheit auf **Mittel-Hoch fest.**

Schritt 4: Klicken Sie auf **Speichern**

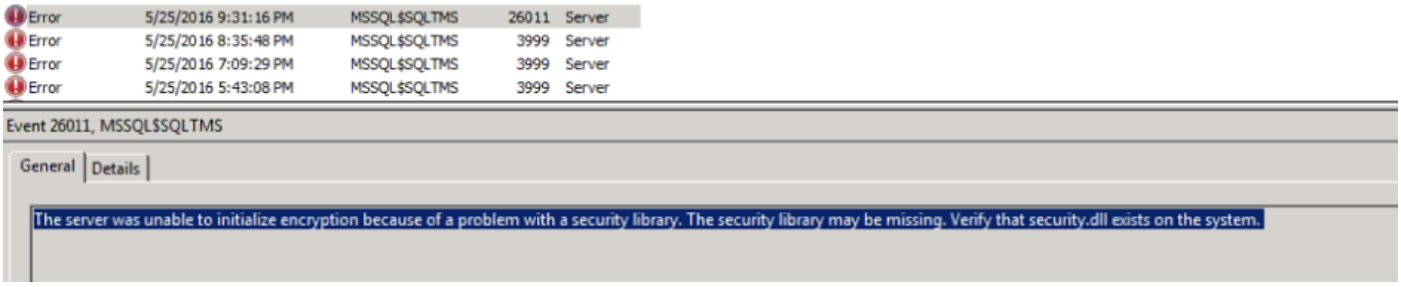
Schritt 5: Starten Sie dann sowohl die Internetinformationsdienste (IIS) auf dem Server als auch den **TMSDatabaseScannerService** neu, und starten Sie **TMSPLCMDirectoryService** (wenn dieser angehalten wird).

> **Warnung**: : Wenn die TLS-Option von "Mittel-Hoch" zu "Mittel-Hoch" geändert wird, werden telnet und Simple Network Management Protocol (SNMP) deaktiviert. Dies führt dazu, dass der TMSSNMPservice beendet wird, und es wird eine Warnung auf der TMS-Webschnittstelle ausgegeben.

Überlegungen zum Aktualisieren der Sicherheitseinstellungen

Wenn **SQL 2008 R2** verwendet und auf dem TMS-Windows-Server installiert wird, müssen wir sicherstellen, dass auch TLS1.0 und SSL3.0 aktiviert ist, andernfalls wird der SQL-Dienst beendet und es wird nicht gestartet.

Diese Fehler müssen im Ereignisprotokoll angezeigt werden:

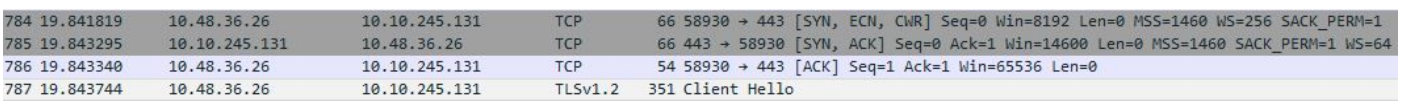


Wenn **SQL 2012** verwendet wird, muss es aktualisiert werden, um die TLS-Änderung zu beheben, wenn es auf dem TMS-Windows-Server installiert wird (https://support.microsoft.com/en-us/kb/3052404).

Mit SNMP oder Telnet verwaltete Endgeräte zeigen "Sicherheitsverletzung: Telnet-Kommunikation ist nicht zulässig."

Überprüfen

Wenn Sie die TLS-Option von **Mittel** zu **Mittel-Hoch** ändern, wird dadurch sichergestellt, dass TLS Version 1.2 im **Client Hello** nach dem TCP-Dreiwegehandshake von TMS angekündigt wird:



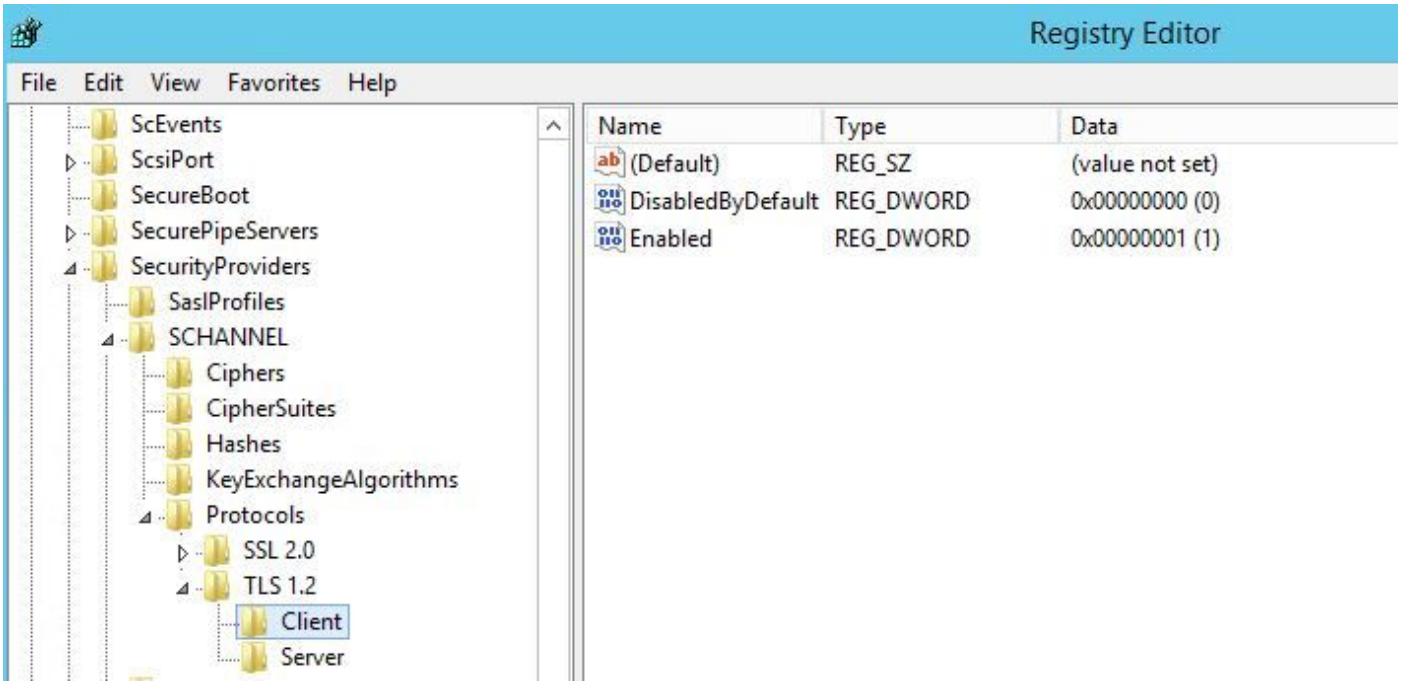
TLS-Version 1.2 angekündigt:

```
▷ 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
```

Wenn es bei **mittlerem** TMS verbleibt, sendet das TMS während der Aushandlungsphase nur Version 1.0 im SSL-Client hello, die die höchste unterstützte TLS-Protokollversion angibt, in diesem Fall TMS.

Für TMS-Versionen unter 15

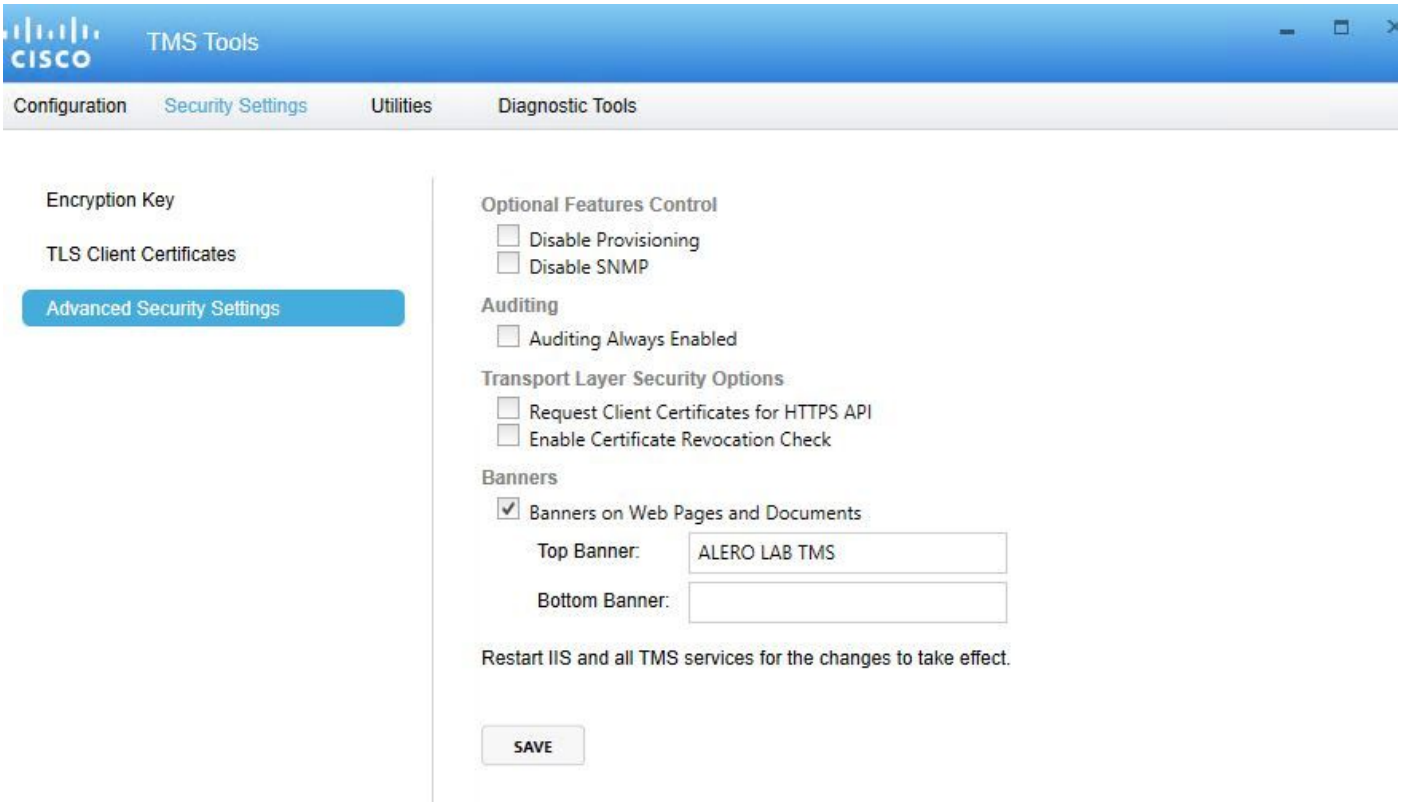
Schritt 1: Auch wenn die TLS-Version 1.2 in die Registrierung aufgenommen wurde



Schritt 2: Der TMS-Server sendet immer noch nicht die vom Endpunkt in seinem SSL-Client unterstützte Version 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
```

Schritt 3: Das Problem besteht dann darin, dass wir die TLS-Optionen in den TMS-Tools nicht ändern können, da diese Option nicht verfügbar ist.



Schritt 4: Die Lösung für dieses Problem ist dann entweder ein TMS-Upgrade auf 15.x oder ein Downgrade der TC/CE-Endgeräte auf 7.3.3. Dieses Problem wird im Softwarefehler CSCuz71542 verfolgt, der für Version 14.6.x erstellt wurde.