# TLS-Handshake-Fehler an der VCS-Webschnittstelle

## Inhalt



## Einführung

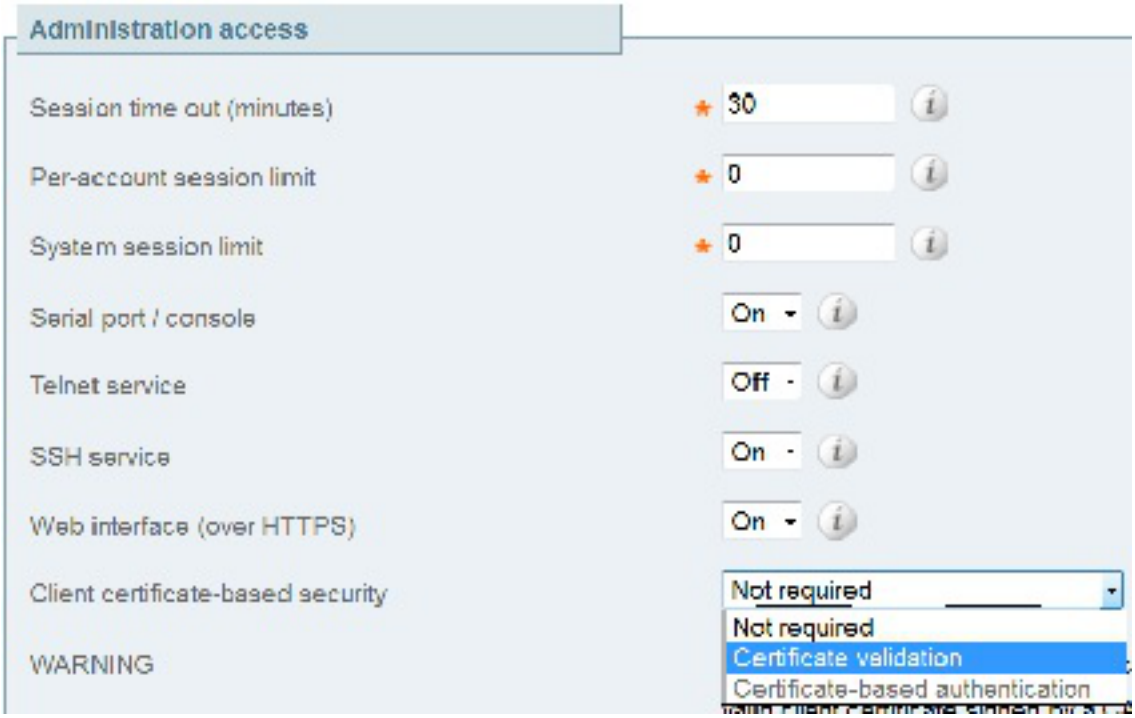
Der Cisco Video Communication Server (VCS) verwendet Client-Zertifikate für den Authentifizierungs- und Autorisierungsprozess. Diese Funktion ist in einigen Umgebungen äußerst nützlich, da sie eine zusätzliche Sicherheitsebene ermöglicht und für die einmalige Anmeldung verwendet werden kann. Bei falsch konfigurierter Konfiguration können Administratoren jedoch die VCS-Webschnittstelle verlassen.

Die Schritte in diesem Dokument werden verwendet, um die auf Client-Zertifikaten basierende Sicherheit auf dem Cisco VCS zu deaktivieren.

## Problem

Wenn auf einem VCS Client-zertifizierte Sicherheit aktiviert und falsch konfiguriert ist, können Benutzer möglicherweise nicht auf die VCS-Webschnittstelle zugreifen. Beim Zugriff auf die Webschnittstelle kommt es zu einem Handshake-Fehler (Transport Layer Security, TLS).

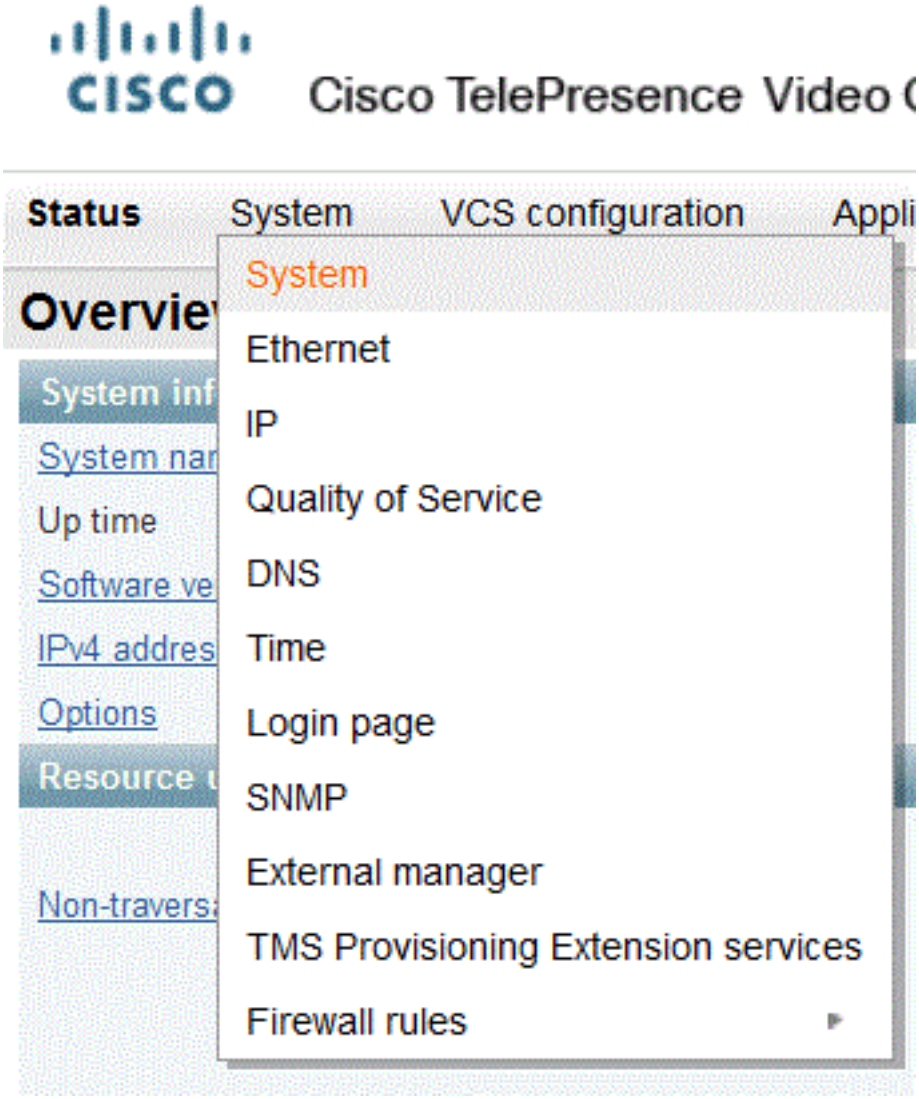
Diese Konfigurationsänderung löst das Problem aus:



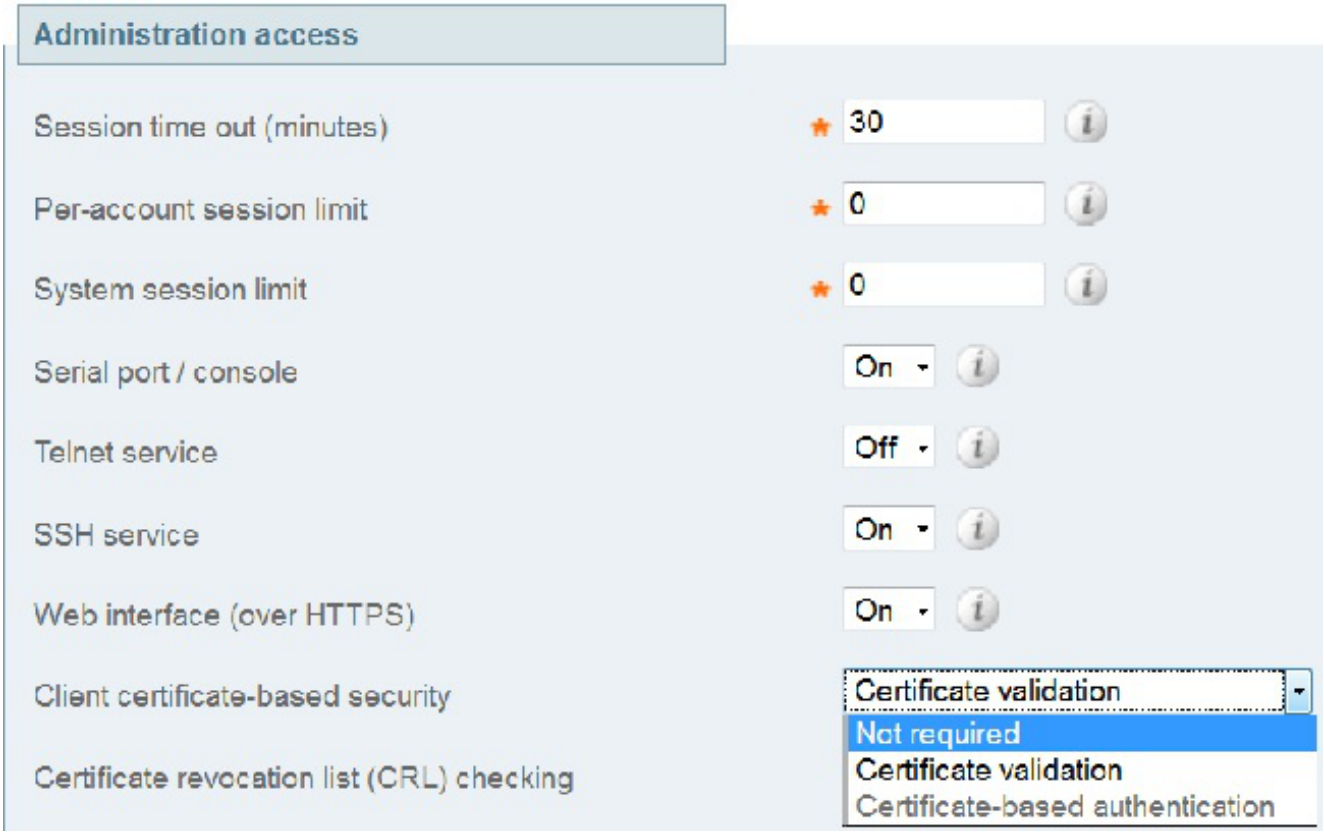

# Lösung

Gehen Sie wie folgt vor, um die Client-zertifizierte Sicherheit zu deaktivieren und das System in einen Zustand zurückzusetzen, in dem Administratoren auf die Webschnittstelle des VCS zugreifen können:

1. Stellen Sie über Secure Shell (SSH) eine Verbindung zum VCS als Root her.
2. Geben Sie diesen Befehl als root ein, um den Apache als Hard-Code zu verwenden, um auf keinen Fall Client-zertifizierte Sicherheit zu verwenden:
   ```
   echo "SSLVerifyClient none" > /tandberg/persistent/etc/opt/apache2/ssl.d/removecba.conf
   ```
   **Hinweis**: Nachdem dieser Befehl eingegeben wurde, kann der VCS für Client-zertifikatbasierte Sicherheit erst neu konfiguriert werden, wenn die Datei **removecba.conf** gelöscht und der VCS neu gestartet wurde.
3. Sie müssen den VCS neu starten, damit diese Konfigurationsänderung wirksam wird. Wenn Sie zum Neustart des VCS bereit sind, geben Sie die folgenden Befehle ein:
   ```
   tshell
   xcommand restart
   ```
   **Hinweis**: Dadurch wird das VCS neu gestartet und alle Anrufe/Registrierungen werden beendet.
4. Nach dem Neuladen des VCS ist die Client-zertifizierte Sicherheit deaktiviert. Sie ist jedoch nicht wünschenswert deaktiviert. Melden Sie sich beim VCS mit einem Lese- und Schreibadministrator-Konto an. Navigieren Sie zu **System > System** im VCS.




Stellen Sie auf der Systemverwaltungsseite des VCS sicher, dass die auf Client-Zertifikaten basierende Sicherheit auf "Not required" (Nicht erforderlich) gesetzt ist:




Speichern Sie die Änderungen, sobald diese vorgenommen wurden.

5. Geben Sie diesen Befehl als root in SSH ein, um den Apache wieder auf den normalen Modus zurückzusetzen:
   `rm /tandberg/persistent/etc/opt/apache2/ssl.d/removecba.conf`
   **Warnung**: Wenn Sie diesen Schritt überspringen, können Sie die auf Clientzertifikaten basierende Sicherheit nie wieder aktivieren.
6. Starten Sie das VCS noch einmal neu, um zu überprüfen, ob das Verfahren funktioniert hat. Nachdem Sie jetzt über Webzugriff verfügen, können Sie das VCS über die Webschnittstelle unter **Wartung > Neustart** neu starten.

Herzlichen Glückwunsch! Der VCS wird jetzt ausgeführt, wenn die Client-Zertifizierung aktiviert ist.