TLS Handshake Failure on the VCS Web Interface

Document ID: 116416

Contributed by Vernon Depee, Cisco TAC Engineer.
Aug 09, 2013

Contents

Introduction

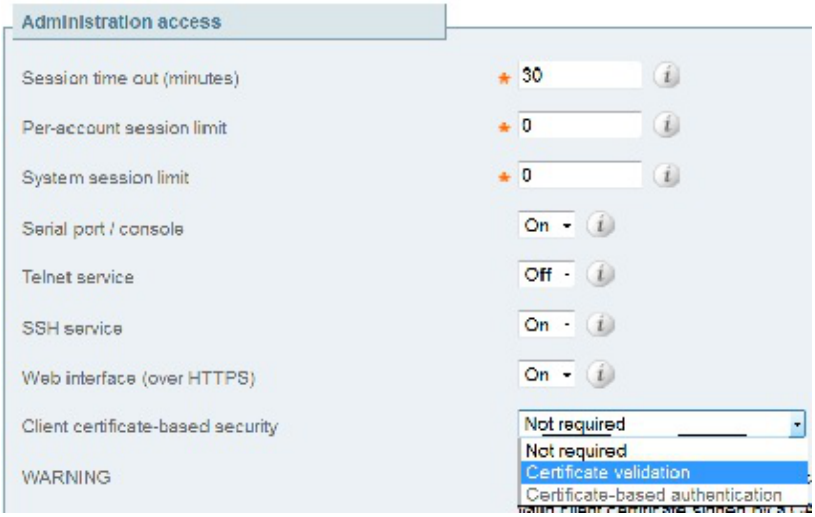
The Cisco Video Communication Server (VCS) uses client certificates for the authentication and authorization process. This feature is extremely useful for some environments, because it allows an added layer of security and can be used for single sign on purposes. However, if incorrectly configured, it can lock administrators out of the VCS web interface.

The steps in this document are used to disable Client certificate−based security on the Cisco VCS.

Problem

If Client certificate−based security is enabled on a VCS, and is incorrectly configured, users might not be able to access the VCS web interface. Attempts to access the web interface are met with a Transport Layer Security (TLS) handshake failure.

This is the configuration change that triggers the issue:



Administration access

Session time out (minutes) * 30
Per-account session limit * 0
System session limit * 0
Serial port / console On
Telnet service Off
SSH service On
Web interface (over HTTPS) On
Client certificate-based security Not required
WARNING

Solution

Complete these steps in order to disable Client certificate−based security and return the system to a state where administrators are able to access the web interface of the VCS:

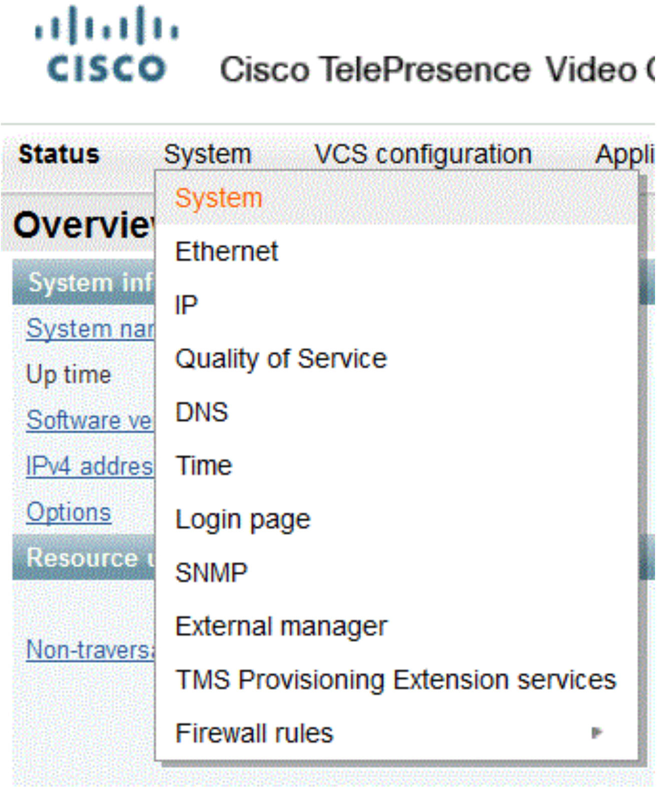
1. Connect to the VCS as root via Secure Shell (SSH).
2. Enter this command as root in order to hard−code Apache to never use Client certificate−based security:

   ```
   echo "SSLVerifyClient none" > /tandberg/persistent/etc/opt/apache2/ssl.d/removecba.conf
   ```

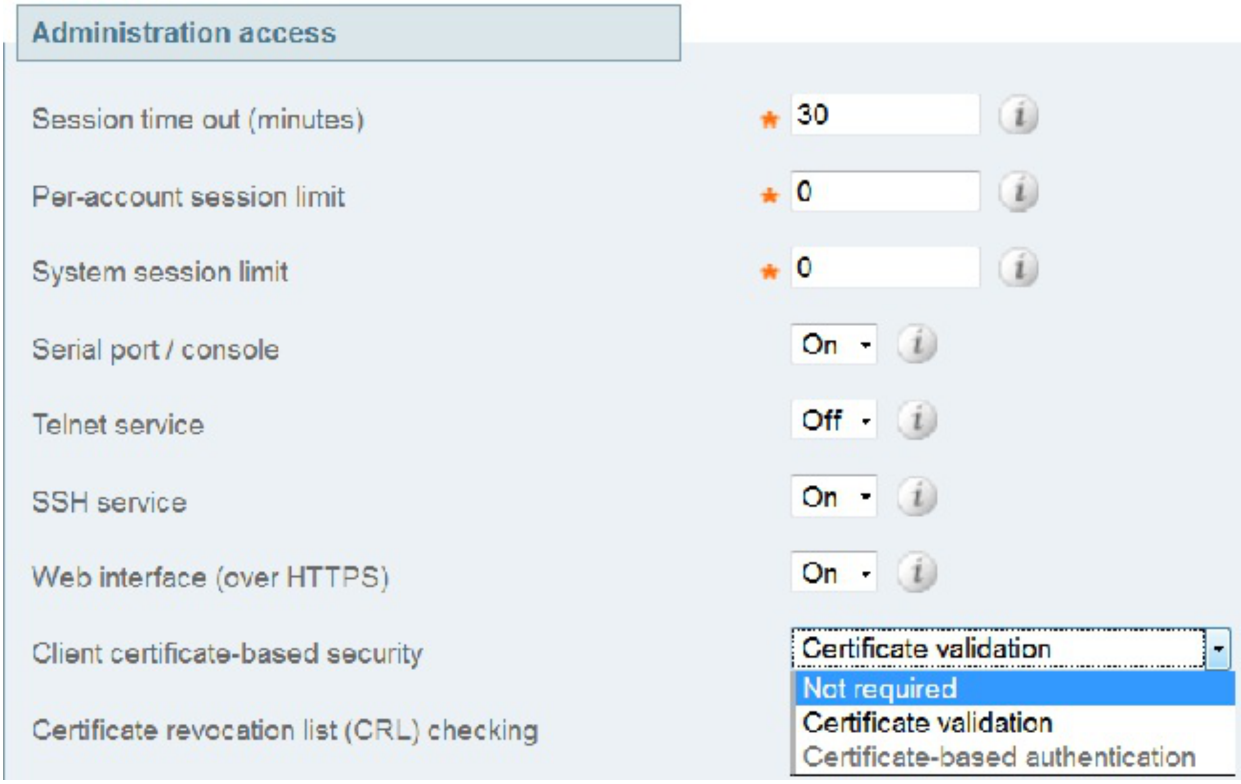
   Note: After this command is entered, the VCS cannot be reconfigured for Client certificate−based security until the ***removecba.conf*** file is deleted and the VCS is restarted.
3. You must restart the VCS in order for this configuration change to take effect. When you are ready to restart the VCS, enter these commands:

   ```
   tshell
   xcommand restart
   ```

   Note: This restarts the VCS and drops all calls/registrations.
4. Once the VCS reloads, Client certificate−based security is disabled. However, it is not disabled in a desirable way. Log in to the VCS with a read−write admin account. Navigate to ***System*** > ***System page*** on the VCS.

   On the system administration page of the VCS, ensure that Client certificate−based security is set to "Not required":



Administration access

Session time out (minutes) * 30

Per-account session limit * 0

System session limit * 0

Serial port / console: On

Telnet service: Off

SSH service: On

Web interface (over HTTPS): On

Client certificate-based security: Certificate validation

Certificate revocation list (CRL) checking

Once this change is made, save the changes.

5. Once complete, enter this command as root in SSH in order to reset Apache back to normal:

   ```
   rm /tandberg/persistent/etc/opt/apache2/ssl.d/removecba.conf
   ```

   Warning: If you skip this step, you can never re−enable Client certificate−based security.
6. Restart the VCS one more time in order to verify that the procedure worked. Now that you have web access, you can restart the VCS from the web interface under ***Maintenance*** > ***Restart***.

Congratulations! Your VCS now runs with Client cerificate−based security disabled.

Updated: Aug 09, 2013 Document ID: 116416