VCS 웹 인터페이스의 TLS 핸드셰이크 실패

목차

소개

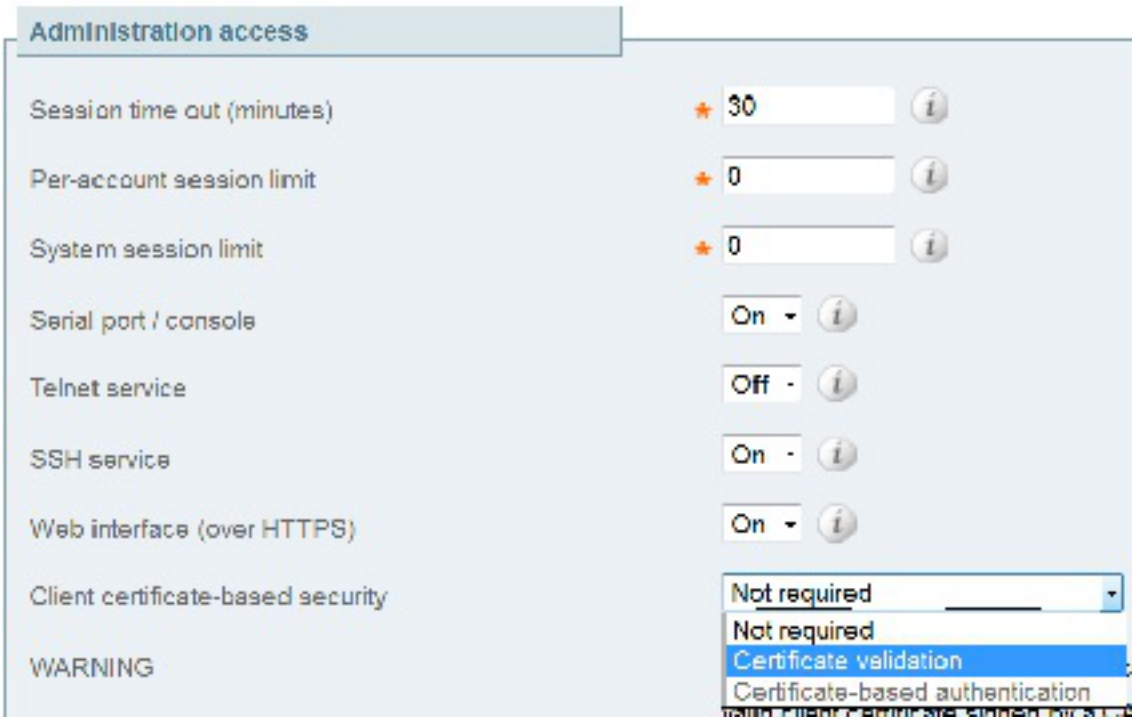
Cisco VCS(Video Communication Server)는 인증 및 권한 부여 프로세스에 클라이언트 인증서를 사용합니다.이 기능은 추가 보안 계층을 허용하며 Single Sign-On 용도로 사용할 수 있으므로 일부 환경에 매우 유용합니다.그러나 잘못 구성된 경우 VCS 웹 인터페이스에서 관리자를 잠글 수 있습니다.

이 문서의 단계는 Cisco VCS에서 클라이언트 인증서 기반 보안을 비활성화하는 데 사용됩니다.

문제

VCS에서 클라이언트 인증서 기반 보안이 활성화되고 잘못 구성된 경우 사용자가 VCS 웹 인터페이스에 액세스하지 못할 수 있습니다.웹 인터페이스에 액세스하려는 시도가 TLS(Transport Layer Security) 핸드셰이크 실패와 함께 충족됩니다.

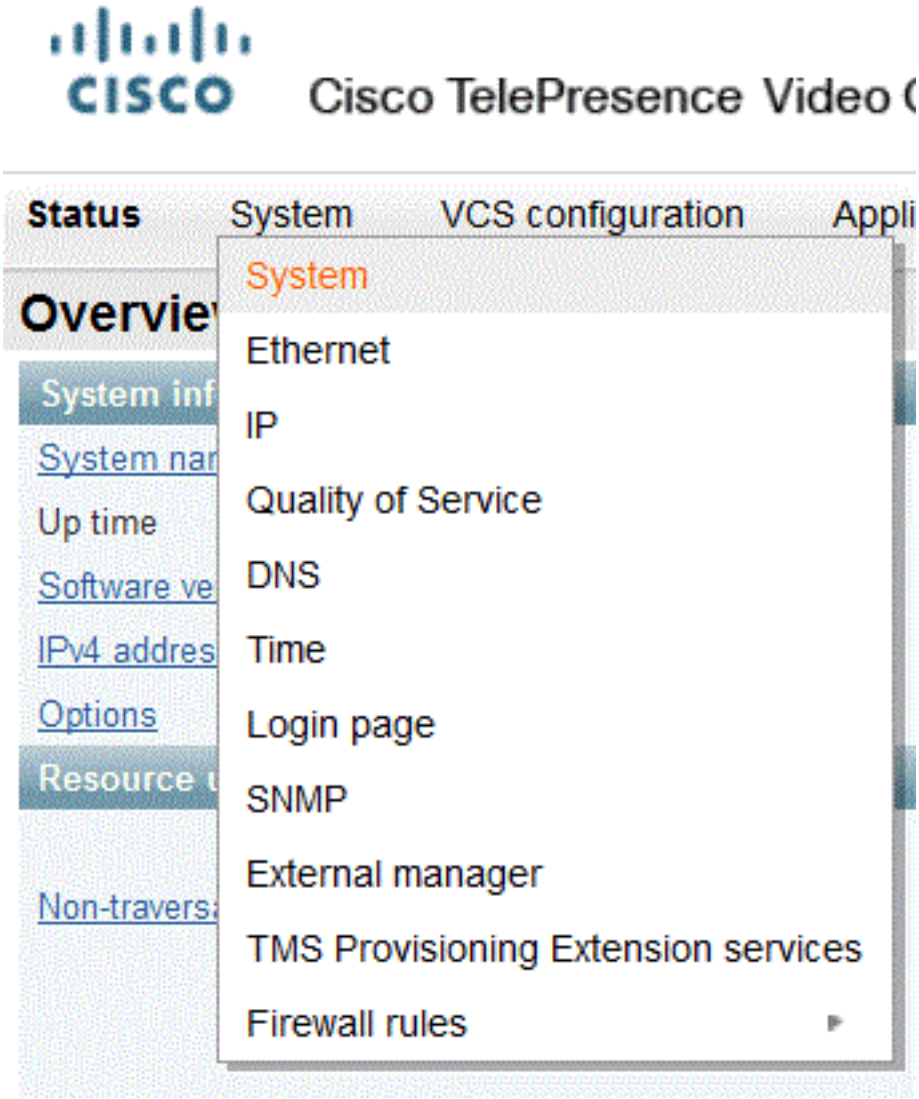
문제를 트리거하는 컨피그레이션 변경입니다.



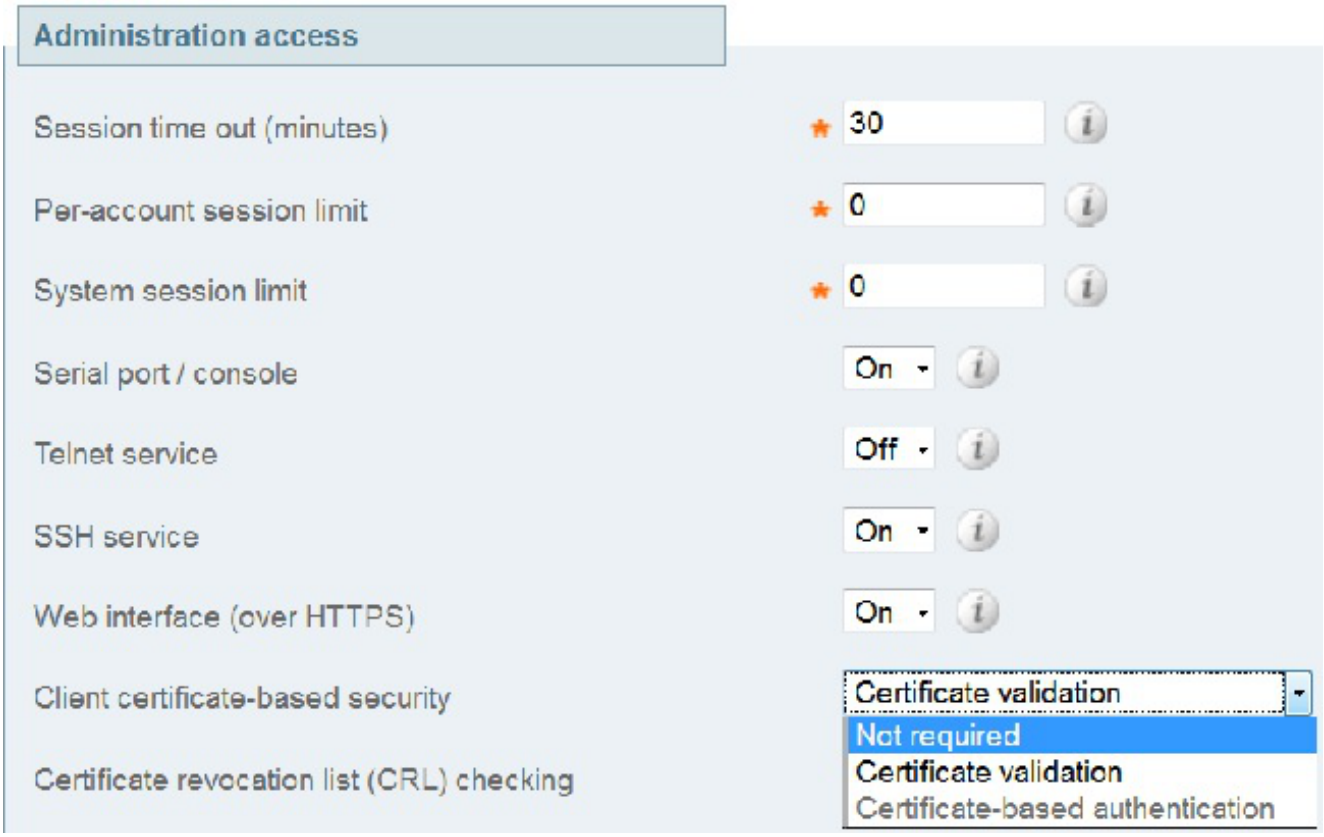
솔루션

클라이언트 인증서 기반 보안을 비활성화하고 관리자가 VCS의 웹 인터페이스에 액세스할 수 있는 상태로 시스템을 되돌리려면 다음 단계를 완료합니다.

1. SSH(Secure Shell)를 통해 루트로 VCS에 연결합니다.
2. Apache가 클라이언트 인증서 기반 보안을 사용하지 않도록 하드 코드하려면 이 명령을 루트로 입력합니다.
   ```
   echo "SSLVerifyClient none" > /tandberg/persistent/etc/opt/apache2/ssl.d/removecba.conf
   ```
   참고:이 명령을 입력한 후에는 removecba.conf 파일이 삭제되고 VCS가 다시 시작될 때까지 클라이언트 인증서 기반 보안**을 위해** VCS를 다시 구성할 수 없습니다.
3. 이 구성 변경 사항을 적용하려면 VCS를 다시 시작해야 합니다.VCS를 다시 시작할 준비가 되면 다음 명령을 입력합니다.
   ```
   tshell
   xcommand restart
   ```
   참고:이렇게 하면 VCS가 다시 시작되고 모든 통화/등록이 삭제됩니다.
4. VCS가 다시 로드되면 클라이언트 인증서 기반 보안이 비활성화됩니다.그러나, 그것은 바람직한 방식으로 비활성화되지 않는다.읽기-쓰기 관리자 계정으로 VCS에 로그인합니다.VCS에서 **System > System 페이지**로 이동합니다.



VCS의 시스템 관리 페이지에서 클라이언트 인증서 기반 보안이 "Not required"로 설정되어 있는지 확인합니다.



이 변경 사항이 적용되면 변경 사항을 저장합니다.

5. 완료되면 이 명령을 SSH에 루트로 입력하여 Apache를 다시 정상으로 재설정합니다.
   `rm /tandberg/persistent/etc/opt/apache2/ssl.d/removecba.conf`
   경고:이 단계를 건너뛰면 클라이언트 인증서 기반 보안을 다시 활성화할 수 없습니다.
6. VCS를 한 번 더 다시 시작하여 프로시저가 작동하는지 확인합니다.이제 웹 액세스가 가능하므로 Maintenance(**유지 관리**) > Restart(재시작) 아래의 웹 인터페이스에서 VCS를 다시 시작할 수 **있습니다**.

축하합니다!이제 VCS가 클라이언트 인증서 기반 보안이 비활성화된 상태에서 실행됩니다.