# Falha do handshake de TLS na interface da WEB VC

## Índice



## Introdução

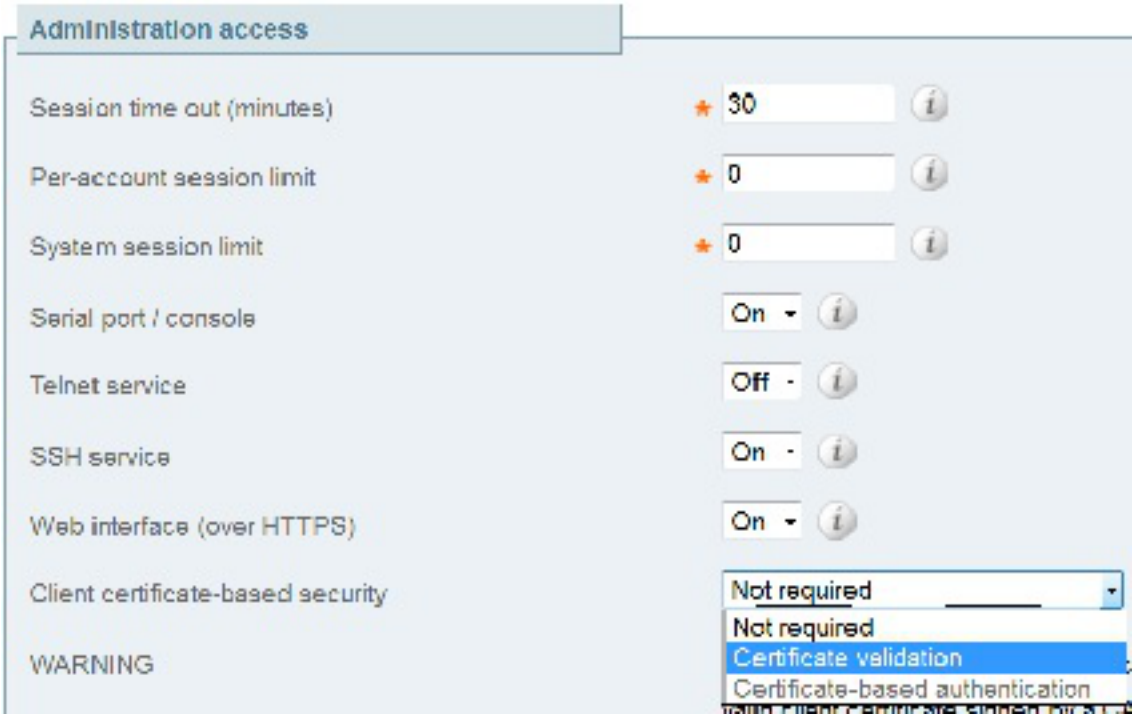
O servidor de comunicação da vídeo Cisco (VC) usa certificados de cliente para o processo de authentication e autorização. Esta característica é extremamente útil para alguns ambientes, porque reserva uma camada adicionada de Segurança e pode ser usada para o único sinal em finalidades. Contudo, se configurada incorretamente, pode travar administradores fora da interface da WEB VC.

As etapas neste documento são usadas para desabilitar a Segurança certificado-baseada cliente em Cisco VC.

## Problema

Se a Segurança certificado-baseada cliente é permitida no VC, e configurada incorretamente, os usuários não puderam poder alcançar a interface da WEB VC. As tentativas de alcançar a interface da WEB são encontradas com uma falha do aperto de mão do Transport Layer Security (TLS).

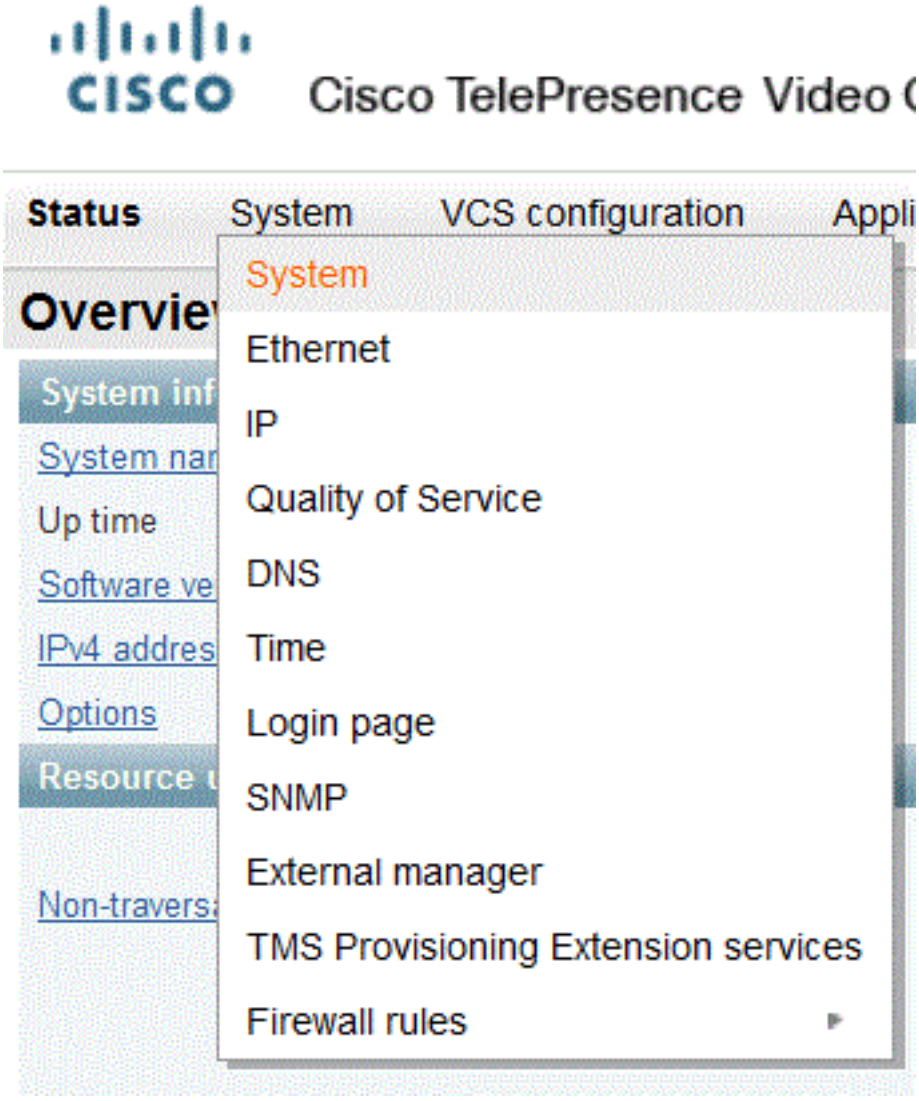
Esta é a alteração de configuração que provoca a edição:



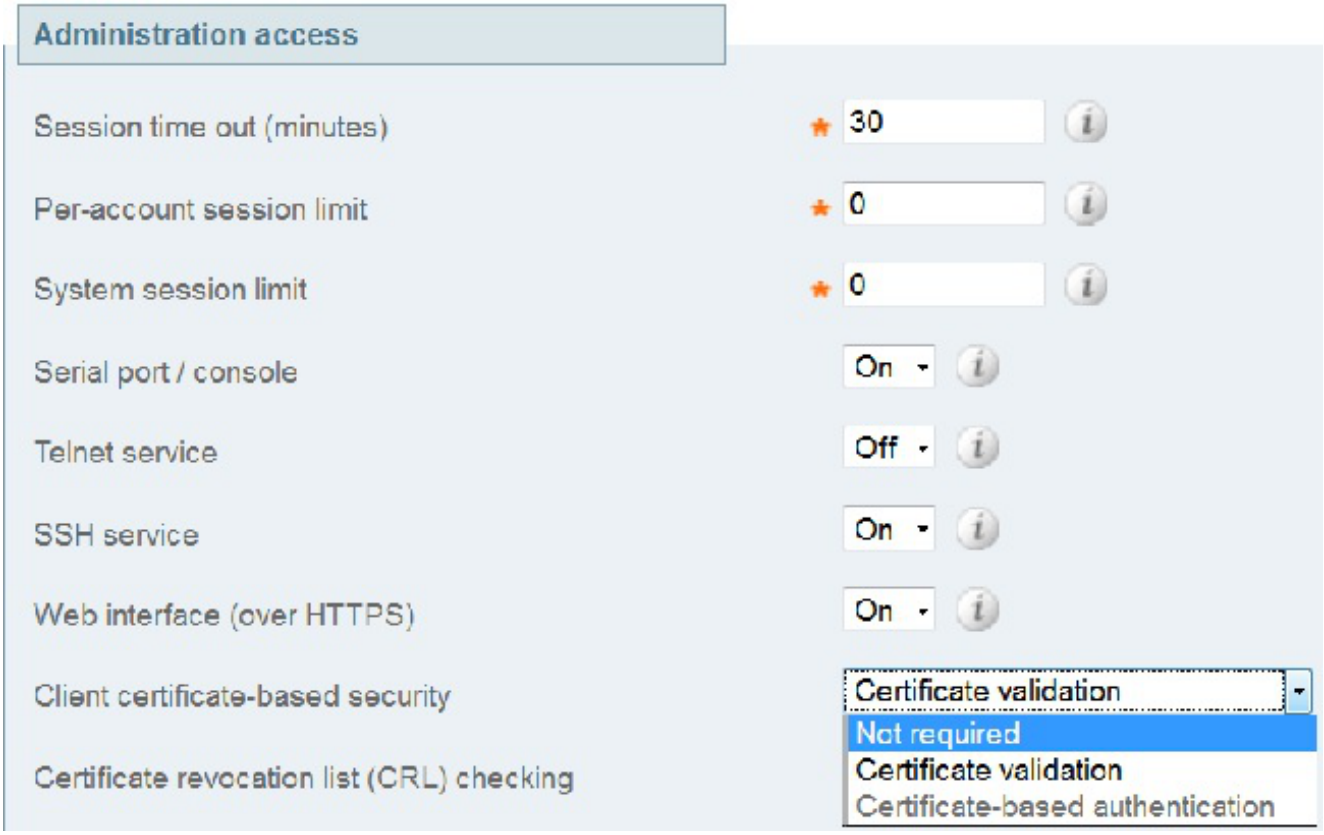

# Solução

Termine estas etapas a fim desabilitar a Segurança certificado-baseada cliente e retornar o sistema a um estado onde os administradores possam alcançar a interface da WEB dos VC:

1. Conecte aos VC como a raiz através do Shell Seguro (ssh).
2. Incorpore este comando como o duro-código Apache da raiz para usar nunca a Segurança certificado-baseada cliente:`echo "SSLVerifyClient none" > /tandberg/persistent/etc/opt/apache2/ssl.d/removecba.conf`Nota: Depois que este comando é incorporado, os VC não podem ser reconfigurados para a Segurança certificado-baseada cliente até que o **arquivo removecba.conf** esteja suprimido e os VC estiverem reiniciados.
3. Você deve reiniciar os VC para que esta alteração de configuração tome o efeito. Quando você está pronto para reiniciar os VC, incorpore estes comandos:`tshell xcommand restart`Nota: Isto reinicia os VC e deixa cair todos os atendimentos/registros.
4. Uma vez que os reloads VC, Segurança certificado-baseada cliente são desabilitados. Contudo, não é desabilitada em uma maneira desejável. Entre aos VC com uma conta admin de leitura/gravação. Navegue à **página do sistema** > do **sistema nos** VC.




Na página da administração do sistema dos VC, assegure-se de que a Segurança certificado-baseada cliente esteja ajustada “ao não exigido”:




Uma vez que esta mudança é feita, salvar as mudanças.

5. Uma vez que completo, incorpore este comando como a raiz no SSH a fim restaurar Apache de volta ao normal:`rm /tandberg/persistent/etc/opt/apache2/ssl.d/removecba.conf`**aviso:** Se você salta esta etapa, você pode nunca re-permitir a Segurança certificado-baseada cliente.
6. Reinicie os VC mais uma vez a fim verificar que o procedimento trabalhou. Agora que você tem o acesso à Web, você pode reiniciar os VC da interface da WEB sob a **manutenção** > o **reinício**.

Felicitações! Seus VC são executado agora com a Segurança cerificate-baseada cliente desabilitada.