Comment est-ce que je certifie des connexions HTTPS à mon Codian MCU ?

Contenu

Introduction

Cet article associe aux Produits de la TelePresence Cisco MCU 4203, de la TelePresence Cisco MCU MSE 8420, de la TelePresence Cisco MCU 4505, de la TelePresence Cisco MCU MSE 8510 et du Cisco TelePresence Advanced Media Gateway 3610.

Q. Comment est-ce que je certifie des connexions HTTPS à mon Codian MCU ?

A. De la version 2.3 de Codian MCU en avant, si vous faites installer la Gestion sécurisée (HTTPS) ou la clé de fonctionnalité de chiffrement, les supports MCU sécurisent les connexions HTTP (HTTPS) pour l'interface de Web. Tandis que ceci permet tout le trafic entre l'utilisateur et le MCU à chiffrer, les administrateurs activant ceci devraient remplacer le certificat fourni et la clé privée par leurs propres moyens, pour permettre l'identité du MCU à authentifier. Notez que vous pouvez seulement avoir un certificat par MCU.

Afin de créer une clé privée et délivrer un certificat des paires, utilisant OpenSSL (par exemple) :

1. Installez s'il y a lieu la Gestion sécurisée (HTTPS) ou la clé de fonctionnalité de chiffrement.
2. Allez au **réseau > aux services** et ouvrez les ports.
3. Connectez au MCU utilisant HTTPS recevant le certificat temprary délivré par nous.
4. Sur votre ordinateur installez OpenSSL*. C'est disponible par défaut sur beaucoup d'Unix/de systèmes Linux, et peut être téléchargé pour Windows de (au moment de l'écriture) : http://www.slproweb.com/products/Win32OpenSSL.html
5. Dans une fenêtre de commandes, allez au répertoire dans lequel OpenSSL a été installé, par exemple C:\OpenSSL\bin.
6. Générez une clé privée RSA utilisant la commande ci-dessous. Cette commande génère un fichier appelé le « privkey.pem » qui est votre clé privée. TANDBERG recommande ce principal soit au moins 2048 bits longs. Si cette clé privée sera enregistrée n'importe où indépendamment de sur le MCU, elle devrait être protégée par un mot de passe : vous êtes incité à entrer dans ce mot de passe deux fois. > genrsa -des3 d'openssl - privkey.pem 2048
7. Créez un certificat basé sur cette clé privée utilisant une des commandes ci-dessous. Pour le test et l'usage interne, ce certificat peut auto-être signé, mais pour la sécurité maximale il devrait être signé par une autorité de certification. Pour créer une utilisation auto-signée de certificat (un fichier appelé le cert.pem) : > req d'openssl - nouveau -x509 - clé privkey.pem -

cert.pem - jours 1000 ou pour qu'une demande de certificat soit envoyée à une utilisation d'autorité de certification : > req d'openssl - nouveau - clé privkey.pem - cert.csr demande de chacun des deux commandes pour un certain nombre d'attributs. Le nom commun doit apparier le nom d'hôte ou l'adresse IP du MCU sur lequel elle sera installée.

8. Si vous utilisez les Certificats enchaînés, les Certificats enchaînés, dans le format PEM, doivent être ajoutés à l'extrémité du certificat d'unité. Ceci peut être fait de deux manières : en copiant et en collant dans un éditeur de texte, ou en utilisant quelque chose telle que la commande d'unix de cat (par exemple cat cert.pem authority.pem > chained.pem). Téléchargez alors le fichier créé.
9. Sur le MCU allez au **réseau > aux Certificats SSL**.
10. Pour des Certificats, le clic **parcourent** et trouvent le certificat que vous avez créé (c'est dans le répertoire vous avez utilisé précédemment). Si vous créiez un certificat auto-signé, le certificat s'appelle le cert.pem. Pour un signé par une autorité de certification, choisissez le certificat signé qu'elles ont fourni.
11. Pour la clé privée, sélectionnez le fichier privkey.pem.
12. Pour le mot de passe de chiffrement à clé privé, entrez dans le mot de passe utilisé en générant la clé privée (le cas échéant).
13. Cliquez sur Upload le **certificat et la clé**. Si le téléchargement est un succès, les informations locales de certificat sont mises à jour à celle du nouveau certificat, et un avertissement semble sur l'en-tête de l'interface web vous inciter à redémarrer le MCU.
14. Allez aux **configurations > à l'arrêt** et redémarrez le MCU.
15. Après qu'il ait redémarré, connectez à l'interface web utilisant HTTPS. Si vous utilisiez un certificat auto-signé, ignorez les messages d'avertissement.
16. Confirmez que le certificat correct est utilisé. Pour faire ceci : - Dans Firefox : cliquez avec le bouton droit à la page, choisissez les **informations de page de vue**. Cliquez sur en fonction l'**onglet Sécurité**, et cliquez sur la **vue**. - En Internet Explorer : le clic droit à la page, choisissent Properties. Cliquez sur en fonction les **Certificats**.

* TANDBERG n'est pas responsable du contenu des sites Web de tiers

Informations connexes

- Support et documentation techniques - Cisco Systems