Contenido

Introducción

Este artículo se relaciona con el Cisco TelePresence MCU 4203, el Cisco TelePresence MCU MSE 8420, el Cisco TelePresence MCU 4505, el Cisco TelePresence MCU MSE 8510 y los Productos avanzados Cisco TelePresence del gateway de medios 3610.

Q. ¿Cómo certifico las conexiones HTTPS a mi Codian MCU?

A. De la versión 2.3 de Codian MCU hacia adelante, si usted hace la Administración segura (HTTPS) o la clave de la función de encripción instalar, los soportes MCU aseguran las conexiones HTTP (HTTPS) para la interfaz Web. Mientras que esto permite todo el tráfico entre el usuario y el MCU que se cifrará, los administradores que habilitan esto deben substituir el certificado y la clave privada suministrados por sus la propio, para permitir que la identidad del MCU sea autenticada. Observe que usted puede solamente tener un certificado por el MCU.

Para crear una clave privada y un certificado empareje, usando el OpenSSL (por ejemplo):

1. En caso necesario instale la Administración segura (HTTPS) o la clave de la función de encripción.
2. Vaya al **> Services (Servicios) de la red** y abra los puertos.
3. Conecte con el MCU usando el HTTPS que valida el certificado temprary publicado por nosotros.
4. En su ordenador instale OpenSSL*. Esto está disponible por abandono en mucho Unix/sistemas Linux, y se puede descargar para Windows de (a la hora de la escritura): http://www.slproweb.com/products/Win32OpenSSL.html
5. En una ventana de comando, va al directorio en el cual el OpenSSL fue instalado, por ejemplo C:\OpenSSL\bin.
6. Genere una clave privada RSA usando el comando abajo. Este comando genera un archivo llamado “privkey.pem” que sea su clave privada. TANDBERG recomienda este dominante sea por lo menos 2048 bits de largo. Si esta clave privada es salvada dondequiera aparte de en el MCU, debe ser protegida por un passphrase: a le indican que ingrese este passphrase dos veces. > genrsa -des3 del openssl - hacia fuera privkey.pem 2048
7. Cree un certificado basado en esta clave privada usando uno de los comandos abajo. Para probar y el uso interno, este certificado puede uno mismo-ser firmado, pero para la seguridad máxima debe ser firmado por un Certificate Authority. Para crear un uso del certificado autofirmado (un archivo llamado cert.pem): > req del openssl - nuevo -x509 - clave privkey.pem - hacia fuera cert.pem - días 1000 o para que un pedido de certificado sea enviado a un uso del Certificate Authority: > req del openssl - nuevo - clave privkey.pem - hacia fuera cert.csr ambos comandos prompt para varios atributos. El Common Name debe hacer juego el nombre del host o la dirección IP del MCU en el cual será instalada.

8. Si usted está utilizando los Certificados encadenados, los Certificados encadenados, en el formato PEM, se deben añadir al final del fichero al final del certificado de unidad. Esto se puede hacer de dos maneras: copiando y pegando en un editor de textos, o usando algo tal como el comando unix del gato (e.g gato cert.pem authority.pem > chained.pem). Entonces cargue el archivo creado.
9. En el MCU vaya a la **red > a los Certificados SSL**.
10. Para los Certificados, el tecleo **hojea** y encuentra el certificado que usted creó (éste está en el directorio usted utilizó previamente). Si usted creó un certificado autofirmado, el certificado se llama cert.pem. Para uno firmado por un Certificate Authority, elija el certificado firmado que han suministrado.
11. Para la clave privada, seleccione el archivo privkey.pem.
12. Para la contraseña de la encripción de claves privadas, ingrese el passphrase usado al generar la clave privada (eventualmente).
13. Haga clic el **certificado y la clave de la carga**. Si la carga es un éxito, la información local del certificado se pone al día a la del nuevo certificado, y una advertencia aparece en la encabezado de la interfaz Web indicarle a que recomience el MCU.
14. Vaya a las **configuraciones > apagan** y recomienzan el MCU.
15. Después de que haya recomenzado, conecte con la interfaz Web usando el HTTPS. Si usted utilizó un certificado autofirmado, ignore los mensajes de advertencia.
16. Confirme que se está utilizando el certificado correcto. Para llevar esto a cabo: - En Firefox: el click derecho en la página, elige la **información de la página de la visión**. Haga clic en la **ficha de seguridad**, y haga clic la **visión**. - En el Internet Explorer: el click derecho en la página, elige las **propiedades**. Haga clic en los **Certificados**.

* TANDBERG no es responsable por el contenido de los sitios web del otro vendedor

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems