# 如何确认对Codian MCU的HTTPS连接？

## 目录



## 简介

此条款与思科网真MCU 4203，思科网真MCU MSE 8420，思科网真MCU 4505，思科网真MCU MSE 8510和思科网真提前的媒体网关3610产品关连。

### Q. 如何确认对Codian MCU的HTTPS连接？

A. 从向前Codian MCU版本2.3，如果安排安全管理(HTTPS)或加密功能密钥安装， MCU支持安全HTTP连接(HTTPS) Web接口的。当这允许将加密时的用户和MCU之间的所有流量，启用此的管理员应该用他们自己替换由供应的证书和专用密钥，允许将验证的MCU的标识。注意您能只有每MCU一证书。

为了创建专用密钥和证书请配对，使用Openssl (例如) ：

1. 如果需要请安装安全管理(HTTPS)或加密功能密钥。
2. 去**网络> Services**并且打开端口。
3. 连接对MCU使用接受temprary证书的HTTPS发出由我们。
4. 在您的计算机安装OpenSSL*。默认情况下这是可用的在许多Unix/Linux系统，并且可以为Windows下载从(在文字时) ：http://www.slproweb.com/products/Win32OpenSSL.html
5. 在命令窗口，去Openssl安装的目录，例如C:\OpenSSL\bin。
6. 生成RSA专用密钥使用下面命令。此命令生成呼叫‘是您的专用密钥的privkey.pem的’文件。TANDBERG推荐此关键是长至少2048个的位。任何地方除在MCU外，如果此专用密钥将存储，应该由密码短语保护：提示您两次输入此密码短语。> openssl genrsa -des3 - privkey.pem 2048
7. 创建根据此专用密钥的证书使用其中一下面命令。为测试和内部使用，此证书可以自己签署的，但是为最大安全性应该由a签字认证机关。创建自签名证书(呼叫cert.pem的文件)使用：> openssl req -新建的-x509 -关键privkey.pem - cert.pem -证书请求的几天1000或能发送到认证机关使用：> openssl req -新密钥privkey.pem - cert.csr一定数量的属性的这两prompt命令。公用名称必须匹配将安装MCU的主机名或IP地址。
8. 如果使用被串连的证书，必须添附被串连的证书，在pem格式，到单元的证书的末端。这可以执行用两种方式：通过复制和插入在文本编辑或者使用某事例如unix命令的cat (即cat cert.pem authority.pem > chained.pem)。然后请上传创建的文件。
9. 在MCU请去**网络> SSL证书**。
10. 对于证书，请单击**浏览**并且查找您创建的证书(这在您以前使用)的目录。如果创建自签名证书，证书呼叫cert.pem。对于签字的一认证机关，请选择他们供应了的签名证书。
11. 对于专用密钥，请选择privkey.pem文件。

12. 对于专用密钥加密密码，请输入使用的密码短语，当生成专用密钥时(若有)。
13. 点击**加载证书并且锁上**。如果加载是成功，本地证书信息更新对那新证书，并且警告出现在Web接口的报头提示您重新启动MCU。
14. 去**设置>关闭**并且重新启动MCU。
15. 在它重新启动后，使用HTTPS，请连接对Web接口。如果使用了一自签名证书，请忽略警告消息。
16. 确认使用正确证书。执行此：-在Firefox ：在页的右键单击，选择**View页信息**。点击**安全选项卡**，并且点击**视图**。-在Internet Explorer ：在页的右键单击，选择**属性**。点击**证书**。

* TANDBERG对第三方网站内容不负责

# 相关信息

- 技术支持和文档 - Cisco Systems