

# 如何安装一被串连的SSL证书到CSS SSL模块

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[逐步指导](#)

[相关信息](#)

## 简介

证书链是一个证书序列，链中的每个证书由随后的证书签署。证书链的目的是在对等体证书与可信的证书颁发机构 (CA) 证书之间建立一个信任链。CA 通过签署证书为对等体证书中的身份进行担保。如果CA是您委托的一个(指示由CA证书的复制的出现在您的根证明目录的)，这暗示您能委托签字的对等项证书。

通常，客户端不接受这些证书，因为它们并非由已知的 CA 创建。客户端通常会指出证书有效性无法进行验证。如果证书由不为客户端浏览器所知的中间 CA 签署，即会出现这种情况。在这类情况下，需要使用链接 SSL 证书或证书组。本文讨论如何适当地安装一被串连的安全套接字层SSL证书对CSS SSL模块。

## 先决条件

### 要求

本文档没有任何特定的要求。

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- CSS11506 SSL模块(强加密) - CSS 506-SSL-K9
- CSS11501 SSL模块(强加密) - CSS 501-SSL-K9
- 仅CSS11506交换机模块- CSS 506-SM
- WebNS 7.10和7.20

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始(默认)配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

### 规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

## [逐步指导](#)

此部分显示如何安装在CSS SSL模块的一被串连的证书有CSS11500的。

如果被串连的证书在多个文件，请使用下面略述的步骤。

1. 转换所有证书对同一个格式。如果证书分开和不在增强加密邮件(PEM)格式，您需要转换他们到PEM格式然后连接。
2. 连接所有证书到一个文件;保证他们被连接，当他们在一系列出现。服务器证书应该是第一个在一系列，跟随由半成品(服务器证书和半成品CA证书)。
3. 导入被统合的证书文件到CSS。
4. 关联证书对ssl服务器。
5. 应用ssl服务器的CA在ssl代理列表内的。

如果所有这些证书被串连到一个PKCS-12文件(许多PKCS-12证书请是)，您应该导入被串连的证书作为PKCS-12，并且关联/应用它作为正常。PKCS-12不能够被连接。

**注意：** Distinguished Encoding Rule (DER)格式不支持一系列，因此这不应该是问题。

要验证，需要使用的密钥是生成证书签名请求的密钥(CSR)文件创建服务器证书。只有证书的一密钥，假如是串连或正常。在他们导入后，请确保验证证书和密钥。您能发出下面显示的命令。

```
(config)# ssl verify myrsacert1 myrsakey1 Certificate and key match
```

## [相关信息](#)

- [CSS高级配置指南](#)
- [巩固/商务站点赞成服务器ID安装-英特尔NetStructure 7110电子商务加速器](#)
- [网络应用服务产品支持](#)
- [技术支持和文档 - Cisco Systems](#)