

Catalyst 1200和1300交换机中的中间证书和证书链

目标

本文的目的是介绍固件4.1.3.36上Catalyst 1200和1300交换机中的中间证书功能和证书链以及配置步骤。

适用设备 | 软件版本

- Catalyst 1200 交换机 | 4.1.3.36
- Catalyst 1300 交换机 | 4.1.3.36

简介

证书用于网络中，以提供安全访问。证书可由外部证书颁发机构(CA)自签名或数字签名。证书链的组件包括：

- 根CA证书:根CA或CA证书位于证书链层次结构的顶部，并且是自签名证书。它是终极信任锚，用于验证中间证书的真实性。
- 中间证书:中间证书由更高层的CA颁发，该CA是另一个中间CA或根CA。在某些情况下，可以有多个中间证书形成证书链。通常，中间CA负责对服务器证书进行签名。
- 服务器证书:此证书是为特定服务器（例如网站）颁发的。它包含服务器的公钥并由CA签名。CA可以是根或中间CA。

在交换机（HTTPS服务器）和浏览器（HTTPS客户端）之间的SSL/TLS握手期间，交换机显示其签名证书。浏览器将CA证书置于其受信任的存储中，使用CA的公钥验证服务器证书上的签名。此过程建立服务器标识的真实性。经过验证后，服务器和浏览器继续交换加密参数，对它们之间传输的数据进行加密，确保通过HTTPS传输数据的安全且经过身份验证的连接。

虽然服务器证书可由根CA证书直接签名，但使用中间证书会引入增强签名过程的分层结构。中间证书充当服务器证书和根CA之间的中介，提供多种好处，例如通过隔离密钥泄露来提高安全性、证书管理灵活性以及授予签名权限的能力。这种分层方法提高了可扩展性，简化了证书续订流程，并能够对撤销进行更精细的控制。实际上，使用中间证书可以增强安全性、灵活性和简化的证书管理，从而丰富签名过程。

在Catalyst 1200和1300交换机的固件4.1.3.36中，现在您可以导入中间证书并查看已安装服务器证书的证书链。Catalyst交换机支持与中间证书和HTTPS服务器证书链相关的以下功能：

- 安装一个或多个中间证书。
- 在与HTTPS客户端的TLS握手中包含中间证书
- 显示中间证书
- 显示设备的HTTPS服务器证书的证书链

继续阅读以了解更多信息！

目录

- [导入中间证书](#)
- [证书链](#)
- [证书链示例](#)

导入中间证书

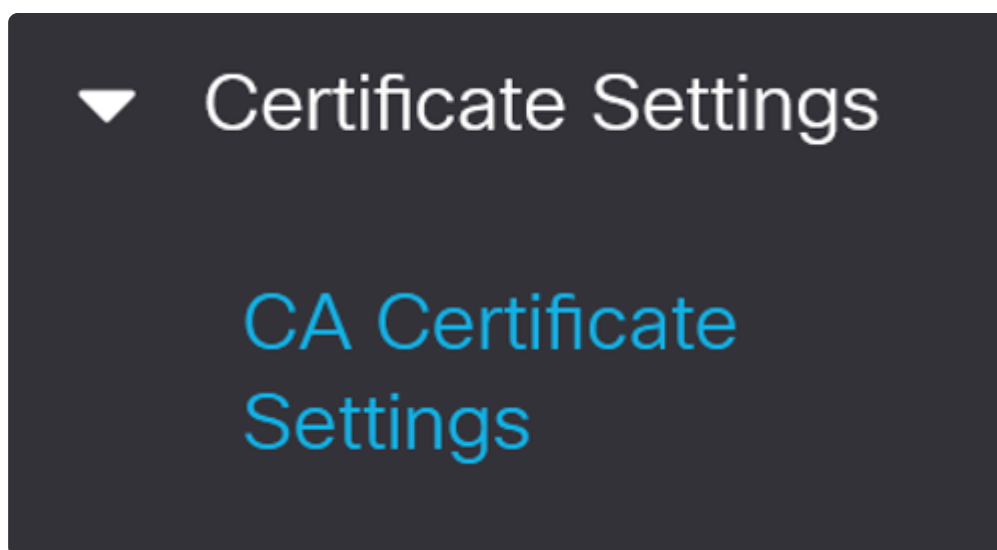
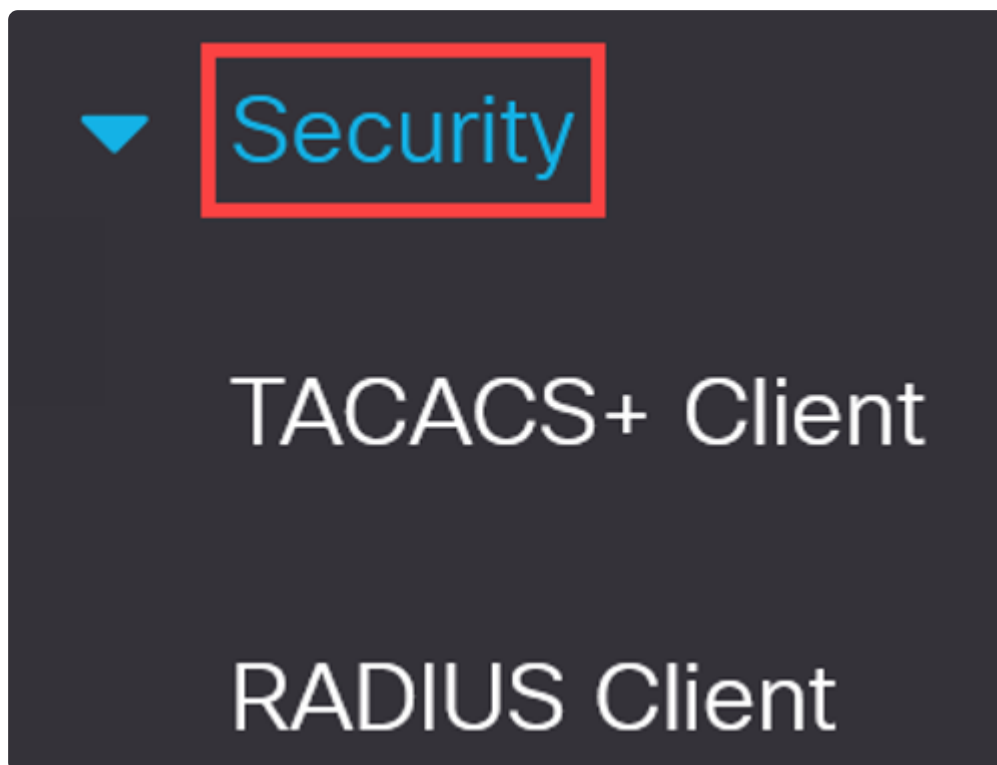
在Catalyst 1200和1300交换机的固件版本4.1.3.36中，您可以选择使用交换机的Web用户界面导入中间证书。

Note:

根据CA，证书供应商将提供根证书和中间证书作为捆绑包以支持服务器证书。

第 1 步

在高级视图下，导航到导航窗格中的安全>证书设置> CA证书设置。



第 2 步

点击加号图标导入证书。

CA Certificate Settings

CA Certificate Table



Details...



第 3 步

输入Certificate Name，选择Intermediate作为证书类型，将证书粘贴到提供的框中，然后单击Apply。

Import CA Certificate x

Success. To permanently save the configuration, go to the [File Operations](#) page or click the Save icon.

When entering the certificate, it must contain the "BEGIN" and "END" markers.

Certificate Name: (20/160 characters used) **1**

Certificate Type: Root Intermediate **2**

Certificate: **3**

4

成功通知将显示在屏幕顶部。

Note:

如果证书类型与要安装的证书不匹配，则会出现错误消息。

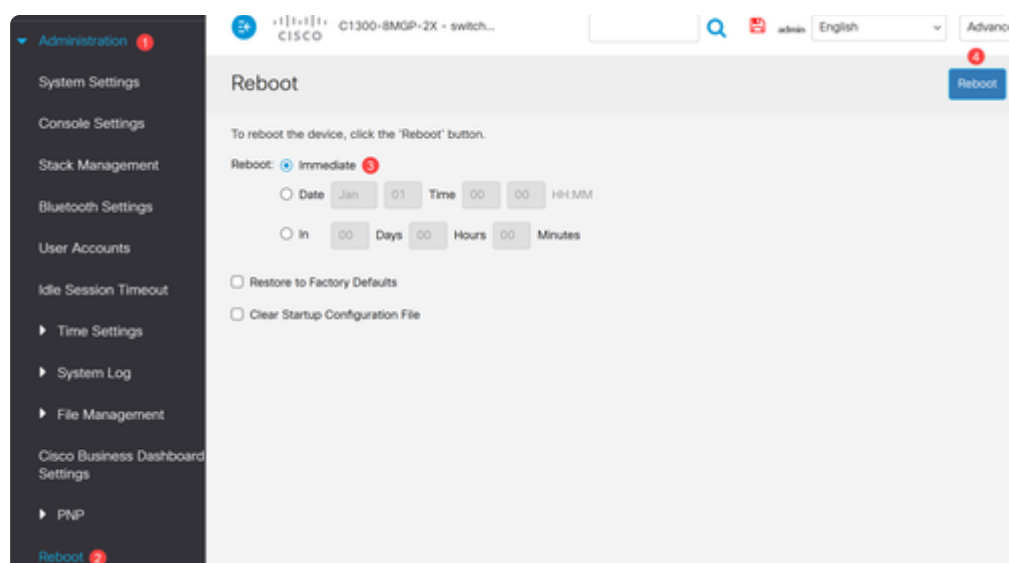
第 4 步

单击屏幕顶部的Save图标。



步骤 5

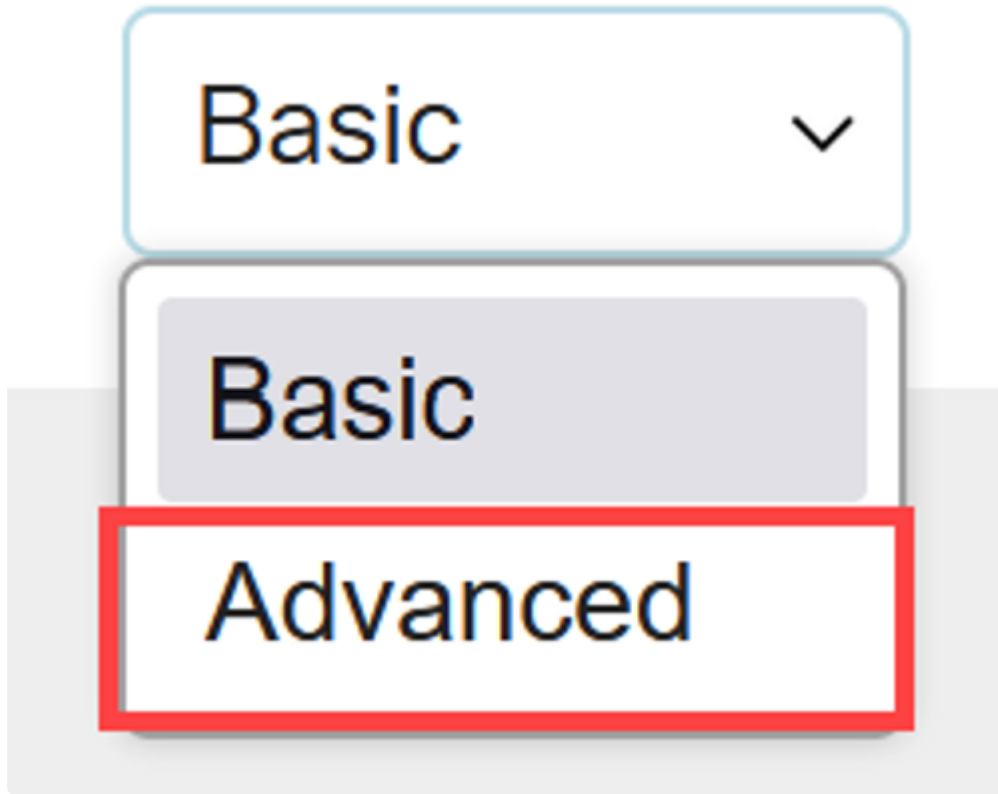
重新启动交换机，使所有更改生效。要重新启动，请导航到Administration > Reboot菜单，并确保选中Immediate reboot选项。单击“Reboot (重新启动)”按钮。



证书链

第 1 步

登录到Catalyst 1300交换机，然后从用户界面右上角的下拉菜单切换到Advanced视图。



第 2 步

导航到导航窗格中的安全 > SSL 服务器 > SSL 服务器身份验证设置。

▼ Security 1

TACACS+ Client

RADIUS Client

▶ RADIUS Server

Dynamic Authorization
Server

Login Settings

Login Protection Status

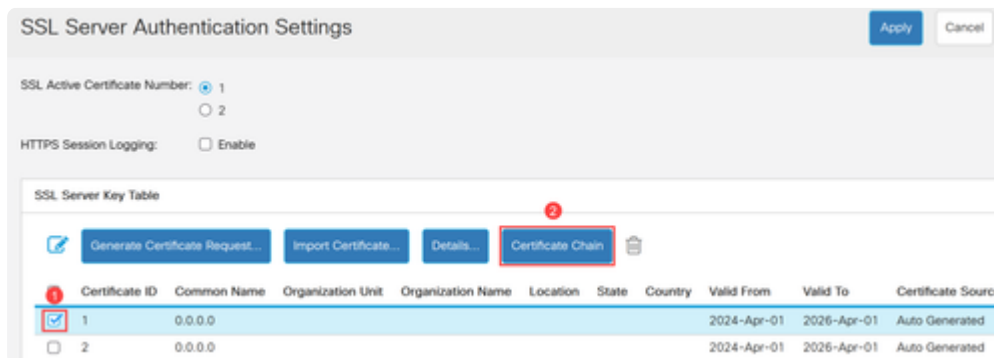
▶ Key Management

▶ Mgmt Access Method

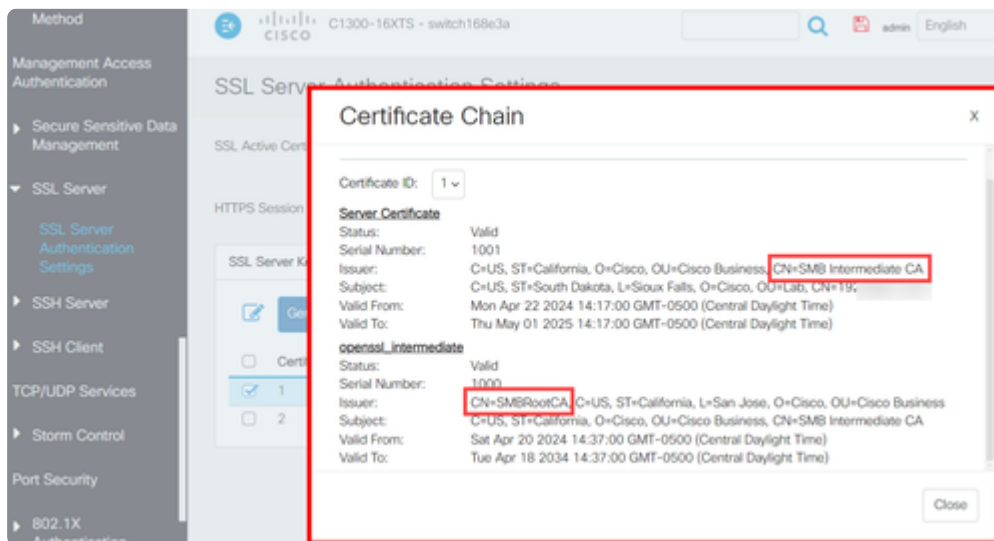
Management Access

第 3 步

从表中选择证书，然后单击证书链按钮。

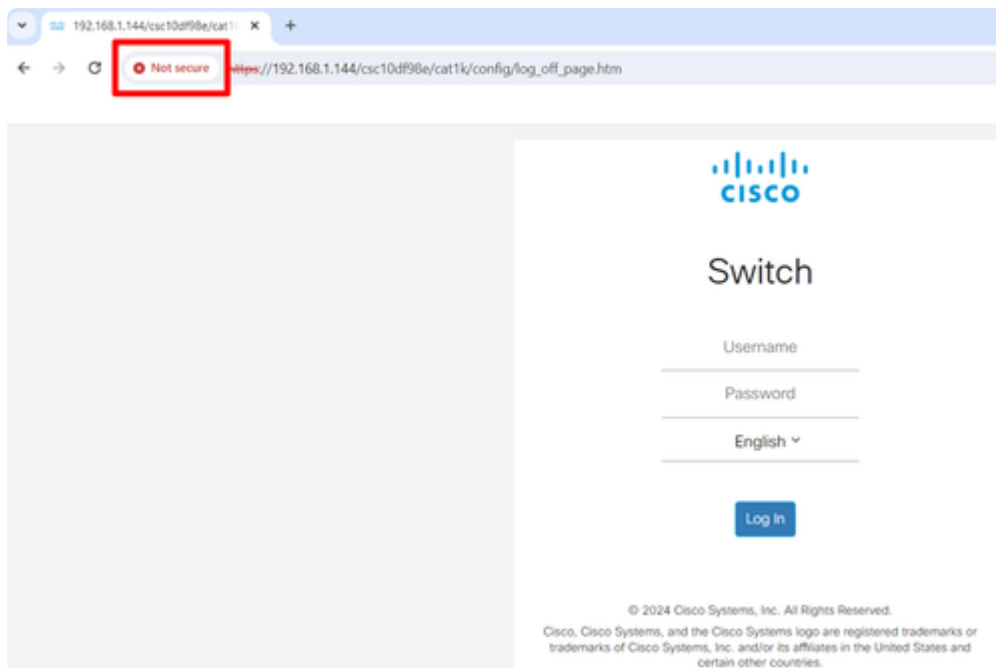


系统将显示一个弹出窗口，显示证书链的详细信息。在本示例中，服务器证书由名为“SMB Intermediate CA”的中间CA签名，如服务器证书中颁发者的公用名(CN)所记录。中间证书的颁发者是SMBRootCA。

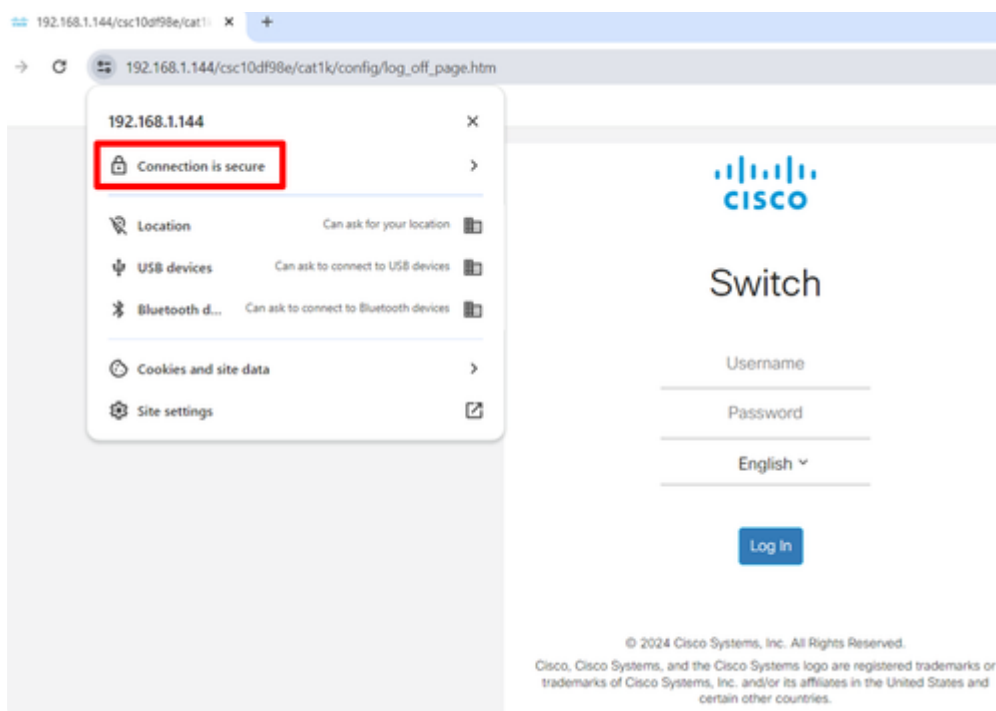


证书链示例

当交换机默认使用自签名证书时，这将导致客户端系统（在本例中为Web浏览器）显示连接不安全的消息。



另一方面，当安装了根证书、中间证书和服务器证书的证书链完成时，浏览器将显示连接是Secure。



结论

好了！现在您已经知道如何在Catalyst 1200和1300交换机中上传中间证书并查看证书链

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。