目录

简介

本文档说明了如何生成证书签名请求 (CSR) 以获取第三方证书，以及如何将链接证书下载到无线局域网 (WLAN) 控制器 (WLC)。

先决条件

要求

在您尝试此配置前，您应该有这些主题知识：

- 如何配置WLC、轻量级接入点(LAP)和基本操作的无线客户端卡
- 如何使用Openssl应用程序
- 公共钥匙结构和数字证书

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行固件版本 5.1.151.0 的 Cisco 4400 WLC
- 适用于 Microsoft Windows 的 OpenSSL 应用程序
- 特定于第三方证书颁发机构 (CA) 的注册工具

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。

链接证书

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。证书链的目的将设立信任一系列从对等项证书的到委托CA证书。当签署它时， CA为在对等项证书的标识担保。如果您信任该 CA，即您的根证书目录中具有该 CA 证书的副本，则意味着您也可以信任签署的对等体证书。

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。

对链接证书的支持

在控制器版本中早于版本5.1.151.0， Web验证证书是仅设备证书，并且不应该包含CA根被串连对设备证书(没有被串连的证书)。使用控制器版本 5.1.151.0 及更高版本时，控制器允许用户以链接证书的形式下载设备证书，以便进行 Web 身份验证。

证书级别

- 级别0 -使用在WLC的仅一服务器证书
- 1级-使用在WLC和CA根证明的一服务器证书
- 2级-使用在WLC、一单个CA中间证书和CA根证明的一服务器证书
- 3级-使用在WLC、两CA半成品证书和CA根证明的一服务器证书

WLC在大小上更比10KB不支持被串连的证书在WLC。然而，此限制在WLC版本7.0.230.0删除和以后。

> **注意**：链接证书只能用于 Web 身份验证；不支持将它们用于管理证书。

Web 身份验证证书可以是以下任何一种证书：

- 串连
- 释放
- 自动生成的

对于与软件版本的WLCs早于版本5.1.151.0，应急方案是使用这些选项之一：

- 从 CA 获取非链接证书，这意味着签名根是受信任的。
- 将所有有效的中间 CA 根证书（受信任或不受信任）都安装到客户端上。

有关如何使用 WLC 上的链接证书的信息，请参阅生成第三方证书的 CSR 并将非链接证书下载到 WLC。

本文档讨论如何将安全套接字层 (SSL) 链接证书正确安装到 WLC。

生成 CSR

请完成下列步骤以生成 CSR：

1. 安装并且打开Openssl。

在Microsoft Windows中，默认情况下， openssl.exe查找在C:\ **> openssl > bin。**

注意：Openssl版本0.9.8是推荐的版本;然而，自版本7.5， Openssl版本1.0的支持也被添加了(参考的Cisco Bug ID CSCti65315 -使用Openssl生成的证书的需要支持v1.0)。

2. 发出此命令为了生成新的CSR ：

```
OpenSSL>req -new -newkey rsa:1024 -nodes -keyout mykey.pem -out myreq.pem
```

注意：WLCs支持最大密钥大小2,048个位。

3. 有时，当您设法生成新的CSR时，您也许收到**无法的**错误**装载从/usr/local/ssl/openssl.cnf错误的设置信息在req。**这能发生，如果openssl.cfg (或openssl.cnf)文件的位置不在默认Openssl文件夹。为了调整此问题，您必须指定整个路径名到在命令的openssl.cfg文件生成CSR。示例如下：

```
OpenSSL> req -config "C:\Open SSL1\OpenSSL\bin\openssl.cfg" -new -newkey rsa:
1024 -nodes -keyout mykey.pem -out myreq.pem
```

此路径， **<** C:\Open SSL1\OpenSSL\bin\openssl.cfg **>**， Openssl配置文件也许有所不同基于文件位置。

4. 在您发出此命令后，系统将提示您输入一些信息：国家/地区名称、州、城市，等等。 提供必填信息。

注意：重要的是，您应该提供正确的公用名称。保证使用创建证书的主机名(公用名称)匹配虚拟接口IP地址的域名系统(DNS)主机名名称条目在，并且名称在DNS存在的WLC。并且，在您做对Virtual IP (VIP)接口后的变动，您必须重新启动系统为了此更改能生效。

示例如下：

```
OpenSSL>req -new -newkey rsa:1024 -nodes -keyout mykey.pem -out myreq.pem
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....................................................................++++++
.....................................................++++++
writing new private key to 'mykey.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:CA
Locality Name (eg, city) []:San Jose
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ABC
Organizational Unit Name (eg, section) []:CDE
Common Name (eg, YOUR name) []:XYZ.ABC
Email Address []:Test@abc.com

Please enter the following 'extra' attributes
```

```
to be sent with your certificate request
A challenge password []:Test123
An optional company name []:OpenSSL>
```

5. 在您提供所有需要的细节后，两个文件生成：

   包含名称 *mykey.pem* 的新私钥包含名称 *myreq.pem* 的 CSR

得到Final.pem文件

1. 复制 CSR 信息并将其粘贴到任意 CA 注册工具中。

   在您提交CSR对第三方CA后，第三方CA数字式地签署证书并且退还签名证书一系列通过电子邮件。一旦被串连的证书，您接收证书整个一系列从CA的。如果在本例中只有一中间证书类似，您接收从CA:的这三证书

   根 certificate.pem中间 certificate.pem设备 certificate.pem

   注意：确保证书是有安全散列算法1 (SHA1)加密的Apache兼容。
2. 一旦有全部三证书，请复制和插入每个.pem文件的内容到另一个文件按此顺序：

```
------BEGIN CERTIFICATE------
*Device cert*
------END CERTIFICATE------
------BEGIN CERTIFICATE------
*Intermediate CA cert *
------END CERTIFICATE--------
------BEGIN CERTIFICATE------
*Root CA cert *
------END CERTIFICATE------
```

3. 将文件另存为 *All-certs.pem*。

4. 将 All-certs.pem 证书以及与 CSR 一起生成的私钥（设备证书的私钥，在本示例中为 mykey.pem）结合，并将此文件另存为 *final.pem*。

   在 OpenSSL 应用程序中发出以下命令，以创建 All-certs.pem 和 final.pem 文件：

```
openssl>pkcs12 -export -in All-certs.pem -inkey mykey.pem
-out All-certs.p12 -clcerts -passin pass:check123
-passout pass:check123

openssl>pkcs12 -in All-certs.p12 -out final.pem
-passin pass:check123 -passout pass:check123
```

   注意：在此命令中，您必须为参数 **- passin** 和 **- passout** 输入口令。为 **- passout** 参数配置的口令必须与在 WLC 上配置的 **certpassword** 参数匹配。在本示例中，为 **-passin** 和 **-passout** 参数配置的口令为 **check123**。

   final.pem是您必须下载到WLC的文件。下一步是将此文件下载到 WLC。

下载第三方证书到与CLI的WLC

完成这些步骤为了下载被串连的证书到与CLI的WLC ：

1. 将 final.pem 文件移到 TFTP 服务器上的默认目录。

2. 在 CLI 中，发出以下命令以更改下载设置：

```
    >transfer download mode tftp
>transfer download datatype webauthcert
>transfer download serverip <TFTP server IP address>
>transfer download path <absolute TFTP server path to the update file>
>transfer download filename final.pem
```

3. 输入 .pem 文件的口令，以使操作系统可以解密 SSL 密钥和证书。

```
>transfer download certpassword password
```

注意：请确保 **certpassword** 的值与生成 CSR 部分步骤 4 中设置的 **-passout** 参数口令相同。在本示例中，**certpassword** 必须为 **check123**。

4. 发出 **transfer download start** 命令以查看更新的设置。然后在提示符处输入 **y** 以确认当前下载设置并开始证书和密钥下载。示例如下：

```
(Cisco Controller) >transfer download start

Mode..................................................... TFTP
Data Type................................................ Site Cert
TFTP Server IP........................................... 10.77.244.196
TFTP Packet Timeout...................................... 6
TFTP Max Retries......................................... 10
TFTP Path....................................../
TFTP Filename............................................ final.pem

This may take some time.
Are you sure you want to start? (y/N) y

TFTP EAP Dev cert transfer starting.

Certificate installed.
Reboot the switch to use new certificate.
```

5. 重新启动 WLC，以使更改生效。

下载第三方证书到与GUI的WLC

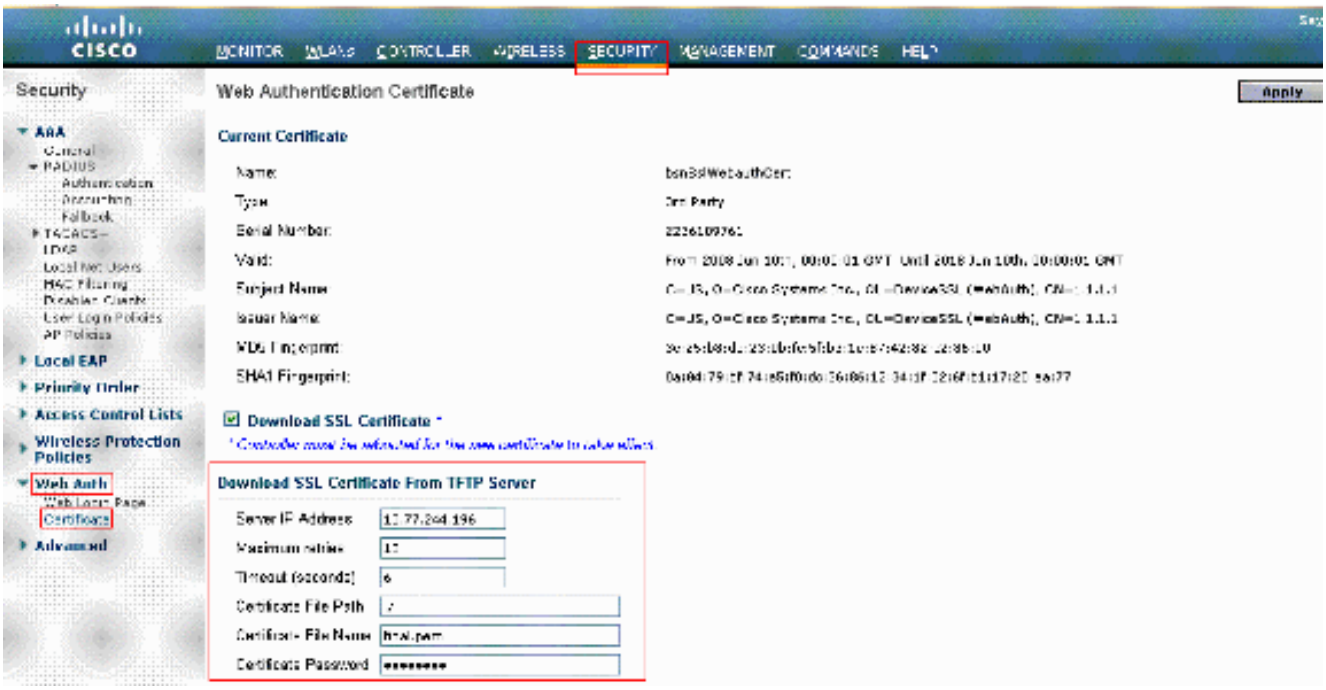
完成这些步骤为了下载被串连的证书到与GUI的WLC ：

1. 将设备证书 final.pem 复制到 TFTP 服务器上的默认目录。

2. 选择 **Security > Web Auth > Cert** 以打开 Web Authentication Certificate 页。

3. 选中 **Download SSL Certificate** 复选框以查看 Download SSL Certificate From TFTP Server 参数。

4. 在 IP Address 字段中输入 TFTP 服务器的 IP 地址。



5. 在 File Path 字段中输入证书的目录路径。

6. 在 File Name 字段中输入证书的名称。

7. 在 Certificate Password 字段中输入用于保护证书的口令。

8. 单击 **Apply**。

9. 下载完成后，选择 **Commands > Reboot > Reboot**。

10. 如果系统提示您保存所做的更改，请单击 **Save and Reboot**。

11. 单击 **OK** 以确认您需要重新启动控制器。

相关信息

- [生成第三方证书的CSR并且下载被释放的证书到WLC]
- [在一个无线控制系统(WCS)上为第三方证书生成的证书签名请求(CSR)]
- [在Linux服务器上安装的无线控制系统(WCS)证书签名请求(CSR)配置示例]
- [技术支持和文档 - Cisco Systems]