

生成第三方证书的CSR并且下载被串连的证书到WLC

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[链接证书](#)

[对链接证书的支持](#)

[证书级别](#)

[步骤1.生成CSR](#)

[与Openssl的选项A. CSR](#)

[选项B.由WLC的CSR Generated](#)

[步骤2.获得认证签字](#)

[方案 A : 从您的企业CA获取Final.pem文件](#)

[方案 B : 从第三方CA获取Final.pem文件](#)

[步骤3 CLI.下载第三方认证到与CLI的WLC](#)

[步骤3 GUI.下载第三方认证到WLC用GUI](#)

[故障排除](#)

[相关信息](#)

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，您应该有这些题目知识：

- 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
- 公共密钥结构和数字证书

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8.3.102的Cisco 5508 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一个委托的CA证书。当签署它时，CA为在对等项证书的身份担保。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](#)

控制器允许作为Web认证的一个被串连的认证将下载的设备认证。

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、两个CA半成品认证和CA根证明的一服务器证书

WLC在大小上更比10KB不支持被串连的认证在WLC。然而，此限制在WLC版本7.0.230.0被去除了和以后。

Note: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。

Note:通配符认证为本地EAP、管理或者webauthentication支持

Web 身份验证证书可以是以下任何一种证书：

- 串连
- 释放
- 主动生成

Note:在WLC版本7.6和以上，Web认证的WLC支持仅被串连的认证。

如果查找生成管理目的一个被释放的认证，您能跟随本文和忽略认证与CA证书一起的零件。

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。

步骤1.生成CSR

有两种方式生成CSR。手工与Openssl (唯一方法可能在pre-8.3 WLC软件)或使用WLC生成CSR (可用在8.3.102以后)。

与Openssl的选项A. CSR

Note:镀铬物版本58和以上不委托单独认证的共同名称并且要求附属的替代名称也存在。以下部分如何将说明添加SAN字段对是此浏览器的一新要求的Openssl CSR。

完成这些步骤为了生成与Openssl的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。

Note:Openssl版本0.9.8是旧有WLC版本的推荐的版本;然而，自版本7.5，Openssl版本1.0的技术支持也被添加了(请是指Cisco Bug ID [CSCti65315](#) -使用Openssl生成的认证的需要技术支持v1.0)并且是使用的推荐的版本。Openssl 1.1工作也测试了并且运作极大在8.x及以后WLC版本。

2. 寻找您的Openssl配置文件并且做复制它为了为此CSR编辑它。编辑复制添加以下部分 :
- 3.

```
[req]
req_extensions = v3_req

[ v3_req ]

# Extensions to add to a certificate request

basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
subjectAltName = @alt_names

[alt_names]
DNS.1 = server1.example.com
DNS.2 = mail.example.com
DNS.3 = www.example.com
DNS.4 = www.sub.example.com
DNS.5 = mx.example.com
DNS.6 = support.example.com
```

开始从"DNS.1"的线路，"DNS.2"等等应该包含您的认证将有的所有替代名称。您能然后写入您使用WLC的所有可能的URL。在粗体上述的线路不存在也未被评论在我们的实验室openssl版本，可能根据操作系统和openssl版本非常地变化。我们保存设置的此修正的版本作为**opensslsan.cnf**此示例。

4. 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 -config openssl-
san.cnf
```

Note:WLCs技术支持最大密钥大小2,048位。

5. 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。

Note:重要的是，您应该提供正确的公用名称。保证使用创建认证的主机名(共同名称)匹配虚拟接口IP地址的域名系统(DNS)主机名名称条目在，并且名字在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 -config openssl-
san.cnf
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>
```

6. 您能验证CSR (特别是对于SAN归因于存在)与openssl req -文本- noout -在csrfilename

7. 在您提供所有必需的细节后，两个文件生成：

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

选项B.由WLC的CSR Generated

如果您的WLC运行软件版本8.3.102或以上，更多安全选项(和最容易太)是使用WLC生成CSR。优点是键在WLC生成和从未离开WLC;因而在外界从未显示。

到现在，此方法不准许配置在也许导致某些浏览器的问题要求SAN属性的出现的CSR的SAN。某个CA准许插入SAN字段在签署的时间，因此它是一个好想法检查与您的CA。

Note:如果运行csr生成命令，并且不安装发生的认证，您的WLC将是完全不能得到的在HTTPS在下辆重新启动，因为WLC将使用最近生成的CSR键，在重新启动，但是没有连同它的认证后。

为了生成Web认证的CSR，请输入此命令：

```
(WLC) >config certificate generate csr webauth是BR布鲁塞尔Cisco TAC
mywebauthportal.wireless.com tac@cisco.com
```

-----开始证书请求-----

```
MIICqjCCAZICAQAwZTELMakGA1UECAwCQlIxETAPBgNVBAcMCEJydXNzZWxzMQ4w
DAYDVQQKDAVDaXNjbzEMMAoGA1UECwwDVEFDMSUwIwYDVQQDDDBxteXdIYmF1dGhw
b3J0YWwud2lyZWxlc3MuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
```

```
AQEAnssc0BxIJ2ULa3xgJH5IAUtbd9CuQVqqf2nflh+V1tu82rzTvz38bjF3g+MX
JiaBbKMA27VJH1J2K2ycDMLhJyYpH9N59T4fXvZr3JNGVfmHIRuYDnCSdil0ookK
FU4sDwXyOxR6gfB6m+Uv5SCOuzfBsTz5bfQ1NIZqg1hNemnhqVgbXEd90sgJmaF2
0tsL0jUhbLosdwMLUbZ5LUa34mvufol3VAKA0cmWZh2WzMJial2JpbO0afRO3kSg
x3XDkZiR7Z9a8rK6Xd8rwDIx0TcMFWdWVcKMDgh7Tw+Ba1cUjIMzKT6OOjFGOGu
yNkgYefrBN+WkDdc6c55bxErwIDAQABoAAwDQYJKoZIhvcNAQELBQADggEBAB0K
ZvEpAafoovphlcXIEIL2DSwVzjlb9u7T5JRGgqri1l9/0wzxFjTymQofga427mj
5dNqlCWxRFmKhAmO0fGQkUoP1YhJRxidU+0T8O46s/stbhj9nulnmoTgPaA0s3YH
tDdWgjmV2ASnroUV9oBNu3wR6RQtKDX/CnTSRG5YufTWOVf9IRnL9LkU6pzA69Xd
YHPLnD2ygR1Q+3ls4+5Jw6ZQAaqIPWyVQccvGyFacscA7L+nZK3SSITzGt9B2HAa
PQ8DQOaCwnqt2efYmaezGiHOR8XHOaWcNoJQCFOnb4KK6/1aF/7eOS4LMA+jSzt4
Wkc/wH4DyYdH7x5jzHc=
-----END证书请求-----
```

为了生成webadmin的CSR，命令几乎不能更改：

```
(WLC) >config certificate generate csr WebAdmin是BR布鲁塞尔Cisco TAC
mywebauthportal.wireless.com tac@cisco.com
```

Note:在您输入命令后，CSR在终端被打印。没有其他方式检索它;从WLC加载它是不可能的亦不是它可能保存它。在您输入命令后，您必须复制/粘贴它到在您的计算机的一个文件。生成的键在WLC坚持，直到下个CSR生成(键因而覆盖)。如果必须稍后更换WLC硬件(RMA)，您不能重新安装和一样新密钥和CSR在新的WLC将必须生成的认证。

您必须然后移交此CSR给您的第三方签署机关或您的企业公共密钥基础设施(PKI)。

步骤2.获得认证签字

方案 A：从您的企业CA获取Final.pem文件

此示例只陈列现有企业CA (在本例中的Windows服务器2012)和不包括步骤从头设置Windows服务器CA。

1. 去您的在浏览器(通常https:// <CA-ip>/certsrv)的enterprise CA页并且点击请求认证。

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

[Request a certificate](#)

[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

2. 点击先进的证书请求。

Request a Certificate

Select the certificate type:

[User Certificate](#)

Or, submit an [advanced certificate request](#).

3. 输入您从WLC或Openssl得到的CSR。在认证模板下拉列表中，请选择**网络服务器**。

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request into the Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
5dNq1CWxRFmKhAm00fGQkUoPlYhJRxidU+0T8046
tDdWgjmV2ASnroUV9oBNu3wR6RQtKDX/CnTSRG5Y
YHPLnD2ygR1Q+3Is4+5Jw6ZQAaqlPWYVQccvGyFa
PQ8DQ0aCwnqt2efYmaezGiHOR8XHOaWcNoJQCFOn
Wkc/wH4DyYdH7x5jzHc=
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Web Server

Additional Attributes:

Attributes:

Submit >

4. 点击Base64编码的单选按钮。

Certificate Issued

The certificate you requested was issued to you.

DER encoded or Base 64 encoded



[Download certificate](#)

[Download certificate chain](#)

5. 如果下载的认证是类型PKCS7 (.p7b)，则您需要转换它成PEM (在下面的示例我们下载了证书链作为文件名"All-certs.p7b")：

在全certs.pem的All-certs.p7b的openssl pkcs7 - print_certs - -

6. 与您与CSR的专用密钥结合证书链(在本例中，被命名“全certs.pem”)认证(设备认证的专用密钥一起生成，是在本例中的mykey.pem)，如果去与方案A (即您使用Openssl生成CSR)，并且保存文件作为final.pem。如果生成了CSR直接地从WLC (选项B)您能跳到此步骤。

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
```

Note: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，如果跟随“选项A. CSR以Openssl”。如果跟随了“WLC生成的选项B. CSR”，则全certs.pem是您必须下载到WLC的文件。下一步是将此文件下载到 WLC。

Note:如果认证的加载对WLC的发生故障，可能是您没有在pem文件的全部的一系列。下面是指第2步方案B (请从第三方CA获取final.pem)发现如何应该看起来象。如果只看到在文件的一个认证，则您需要手工下载所有半成品和根CA证书文件和添附他们(由简单复制粘贴)到文件创建一系列。

方案 B：从第三方CA获取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给第三方CA后，第三方CA数字式地签署认证并且通过电子邮件退还签名证书一系列。一旦被串连的认证，您接收认证整个一系列从CA的。如果只有一中间证书正如在此示例，您接收从CA:的这三个认证

根 certificate.pem中间 certificate.pem设备 certificate.pemNote:确保认证与安全散列算法1 (SHA1)加密是Apache兼容。

- 一旦有全部三个认证，请复制和插入每个.pem文件的内容到另一个文件按此顺序：

```
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
```

- 将文件另存为 *All-certs.pem*。
- 与您与CSR的专用密钥结合全certs.pem认证(设备认证的专用密钥一起生成，是在本例中的mykey.pem)，如果去与方案A (即您使用Openssl生成CSR)，并且保存文件作为final.pem。如果生成了CSR直接地从WLC (选项B)您能跳到此步骤。

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
```

Note: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，如果跟随“选项A. CSR以Openssl”。如果跟随了“WLC生成的选项B. CSR”，则全certs.pem是您必须下载到WLC的文件。下一步是将此文件下载到 WLC。

Note:也支持SHA2。Cisco Bug ID [CSCuf20725](#)是一个要求SHA512技术支持。

步骤3 CLI.下载第三方认证到与CLI的WLC

完成这些步骤为了下载被串连的认证到与CLI的WLC：

- 将 final.pem 文件移到 TFTP 服务器上的默认目录。
- 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
```

Note:在第4步设置的请务必certpassword的值是相同的象- passout参数密码(或5)生成CSR部分。在本示例中，certpassword 必须为 check123。如果选择了方案B (即请使用WLC生成CSR)您能留下certpassword字段空白。

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 might 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。

步骤3 GUI. 下载第三方认证到WLC用GUI

完成这些步骤为了下载被串连的认证到WLC用GUI：

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。

故障排除

什么很可能将摆在问题是认证的安装在WLC的。为了排除故障，打开在WLC的一line命令和参与调试转移全部请启用并且pki然后完成下载认证程序。

```
(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 might 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.

您需要验证证书格式和然后串连。切记WLCs晚于版本7.6要求全部的一系列存在，因此您能不仅加载单独您的WLC认证。至根CA的一系列一定是存在文件。

这是调试示例，当半成品CA不正确时：

```
(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 might 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.

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](#)