生成第三方证书的CSR并且下载被串连的证书到WLC

Contents

Introduction

本文描述如何生成认证署名请求(CSR)为了获得一个第三方认证和如何下载一个被串连的认证到无线局域网(WLAN)控制器(WLC)。

Prerequisites

Requirements

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
- 公共钥匙结构和数字证书

Components Used

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
- 对微软视窗的Openssl申请

- 是特定的对第三方认证机构(CA)的登记工具

The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.

被串连的证书

证书链是证书顺序，在一系列的每个认证由随后的认证签字。证书链的目的将设立信任一系列从对等体认证的到一个委托的CA证书。当签署它时， CA为在对等体认证的身份担保。如果CA是您委托，由CA证书的复制出现在您的根证明目录里表示的一个，这暗示您能委托签字的对等体认证。

通常，因为他们未创建的是由已知CA，客户端不接受证书。客户端典型地阐明，认证的正确性不可能被验证。这是实际情形，当认证由中间CA时签字，没有为客户端浏览器所知。在这类情况下，使用一个被串连的SSL认证或认证组是必要的。

被串连的认证的技术支持

控制器允许设备认证下载作为Web认证的一个被串连的认证。

认证级别

- 级别0 -使用在WLC的仅一个服务器证明
- 第1级-使用在WLC和CA根证明的一个服务器证明
- 第2级-使用在WLC、一单个CA中间证书和CA根证明的一个服务器证明
- 第3级-使用在WLC、两CA半成品证书和CA根证明的一个服务器证明

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被去除了和以后。

Note:被串连的证书为仅Web认证支持;他们不为管理认证支持。

Note:通配符证书为本地EAP、管理或者webauthentication支持

Web认证证书可以是其中每一个：

- 串连
- 释放
- 主动生成

Note:在WLC版本7.6和以上， Web认证的WLC支持仅被串连的证书。

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。

本文讨论如何适当地安装一个被串连的安全套接字层SSL认证对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普通的名字并且要求附属的替代名称也存在。是此浏览器的一新要求的以下部分将说明如何添加SAN字段到Openssl CSR。

完成这些步骤为了生成与Openssl的CSR ：

1. 安装并且打开Openssl。

   在微软视窗中，默认情况下， openssl.exe位于C:\ **> openssl > bin。**

   Note:Openssl版本0.9.8是老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(请参见Cisco Bug ID CSCti65315 -使用Openssl生成的证书的需要技术支持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"等等应该包含您的证书将有的所有替代名称。您能然后写您使用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2,048位的最大密钥大小。
5. 在您发出命令后，有一提示输入一些信息：国家名，状态，城市，等等。提供必要信息。

   Note:重要的是您提供正确的普通的名字。保证使用创建认证的主机名(普通的名字)匹配虚拟接口IP地址的域名系统(DNS)主机名条目在WLC，并且名字存在于DNS。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：

包括命名**mykey.pem的**一把新的专用密钥包括命名**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。

生成由WLC的CSR将使用2048位密钥大小，并且ecdsa密钥大小将是256位。

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 CSRwebauth是增殖比布鲁塞尔Cisco TAC mywebauthportal.wireless.com tac@cisco.com**
-----开始证书请求-----

MIICqjCCAZICAQAwZTELMAkGA1UECAwCQIIxETAPBgNVBAcMCEJydXNzZWxzMQ4w
DAYDVQQKDAVDaXNjbzEMMAoGA1UECwwDVEFDMSUwIwYDVQQDDBxteXdlYmF1dGhw
b3J0YWwud2lyZWxlc3MuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEAnssc0BxlJ2ULa3xgJH5lAUtbd9CuQVqqf2nflh+V1tu82rzTvz38bjF3g+MX
JiaBbKMA27VJH1J2K2ycDMlhjyYpH9N59T4fXvZr3JNGVfmHIRuYDnCSdiI0ookK
FU4sDwXyOxR6gfB6m+Uv5SCOuzfBsTz5bfQ1NlZqg1hNemnhqVgbXEd90sgJmaF2
0tsL0jUhbLosdwMLUbZ5LUa34mvufoI3VAKA0cmWZh2WzMJiaI2JpbO0afRO3kSg
x3XDkZiR7Z9a8rK6Xd8rwDlx0TcMFWdWVcKMDgh7Tw+Ba1cUjjIMzKT6OOjFGOGu
yNkgYefrrBN+WkDdc6c55bxErwIDAQABoAAwDQYJKoZIhvcNAQELBQADggEBAB0K
ZvEpAafoovphlcXIElL2DSwVzjlbd9u7T5JRGgqri1l9/0wzxFjTymQofga427mj
5dNqlCWxRFmKhAmO0fGQkUoP1YhJRxidu+0T8O46s/stbhj9nuInmoTgPaA0s3YH
tDdWgjmV2ASnroUV9oBNu3wR6RQtKDX/CnTSRG5YufTWOVf9IRnL9LkU6pzA69Xd
YHPLnD2ygR1Q+3Is4+5Jw6ZQAaqlPWyVQccvGyFacscA7L+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是增殖比布鲁塞尔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(键因而重写)。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。

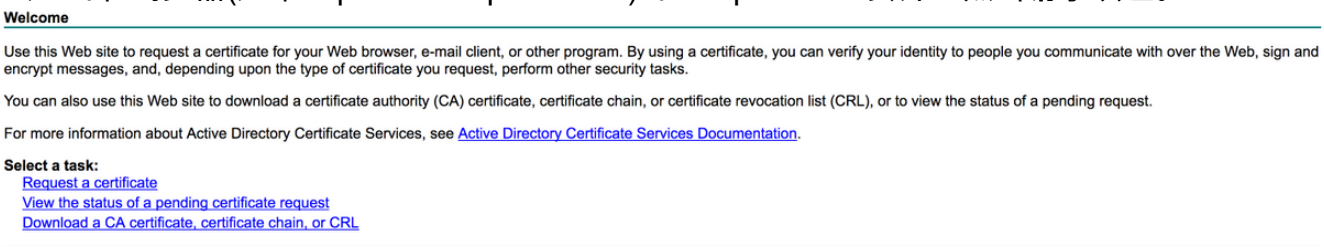
您必须然后移交此CSR给您的第三方签署机关或您的企业公共密钥基础设施(PKI)。

步骤2.获得认证签字

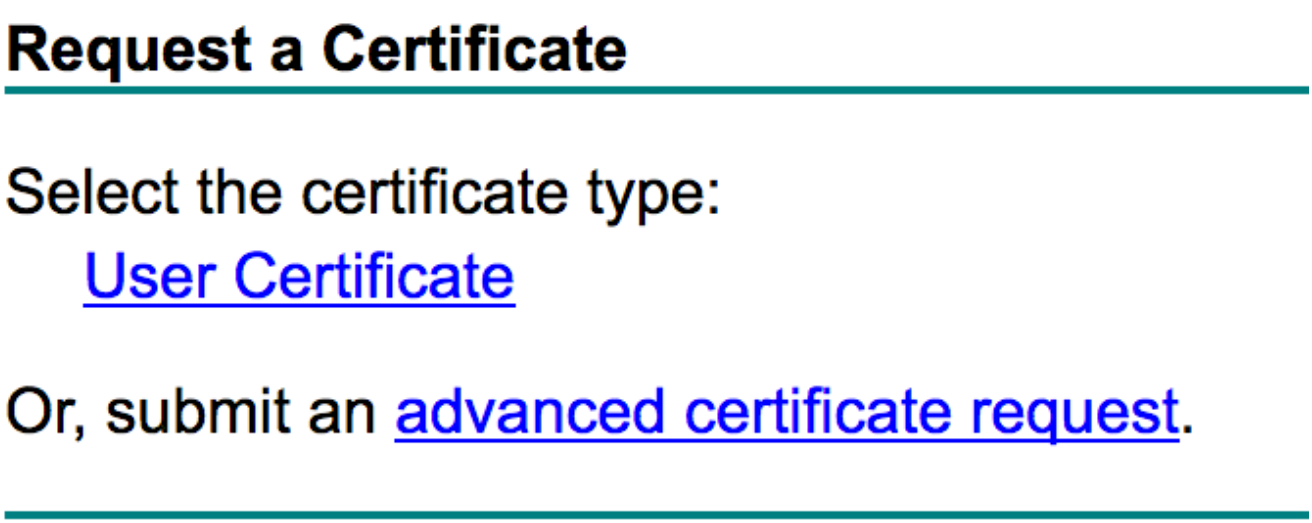
方案A ：获得从您的企业CA的Final.pem文件

此示例只陈列现有的企业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。

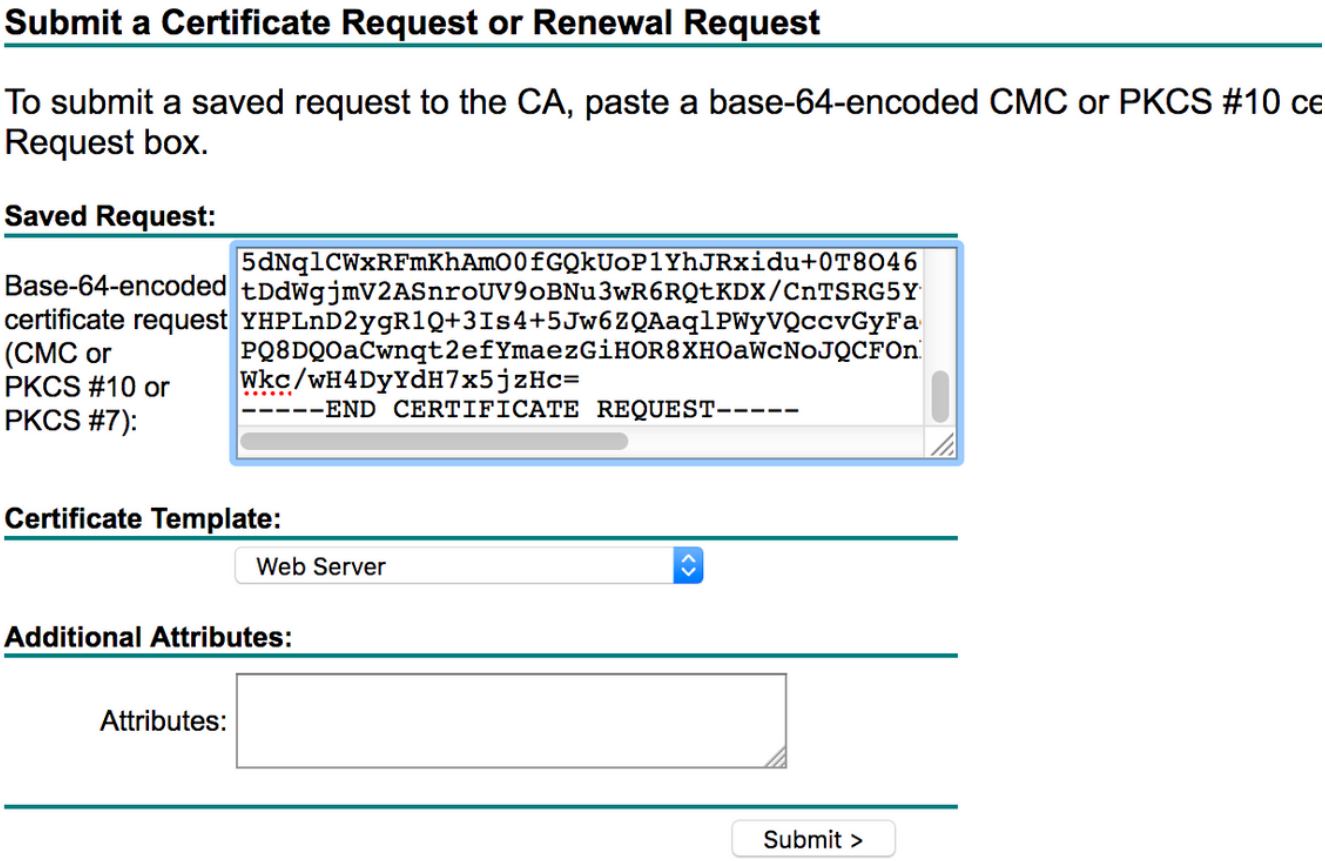
1. 去您的在浏览器(通常https:// <CA-ip>/certsrv)的enteprrise CA页并且点击**请求认证**。



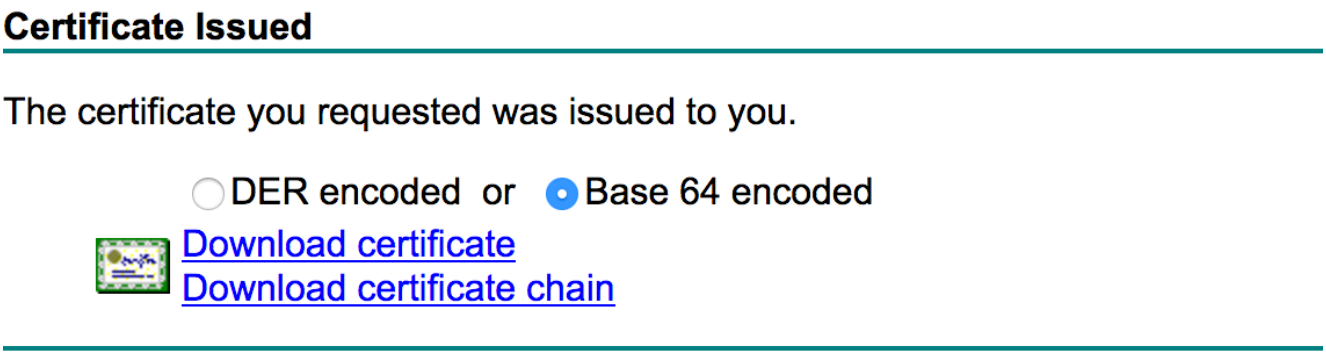
2. 点击**先进的证书请求**。



3. 输入您从WLC或Openssl获得的CSR。在认证模板下拉列表中，请选择**Web服务器**。



4. 点击**Base64编码的**单选按钮。



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”)证书(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。

发出这些in命令Openssl应用程序为了创建全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，您必须输入参数的一个密码**- passin**和**- passout**。为被配置的密码**-passout**参数必须匹配在WLC被配置的**certpassword**参数。在本例中，为被配置**-的**密码**passin**和**- passout**参数是**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。下一步是下载此文件到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。下面请参见第2步方案B (请获得从第三方CA的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中间和根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 ：获得从第三方CA的Final.pem文件

1. 复制和插入CSR信息到所有CA登记工具。

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字的证书链。一旦被串连的证书，您从CA接受证书整个一系列。如果只有一中间证书正如在此示例，您从CA接受这三证书：

根certificate.pem中间certificate.pem设备certificate.pem**Note**:切记认证与安全散列算法1 (SHA1)加密是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：

```
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
```

3. 保存文件如**全certs.pem。**

4. 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。

   发出这些in命令Openssl应用程序为了创建全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，您必须输入参数的一个密码**- passin**和**- passout**。为被配置的密码**- passout**参数必须匹配在WLC被配置的**certpassword**参数。在本例中，为被配置**-的**密码**passin**和**-passout**参数是**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。 下一步是下载此文件到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 ：

1. 移动**final.pem文件**向在您的TFTP server的默认目录。

2. 在CLI中，请发出这些命令为了更改下载设置：

```
    >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文件的密码，以便操作系统能解码SSL键和认证。

```
>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。在本例中， **certpassword**必须是**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**为了查看更新的设置。然后请输入**y**在及时为了确认当前下载设置和开始认证和键下载。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.

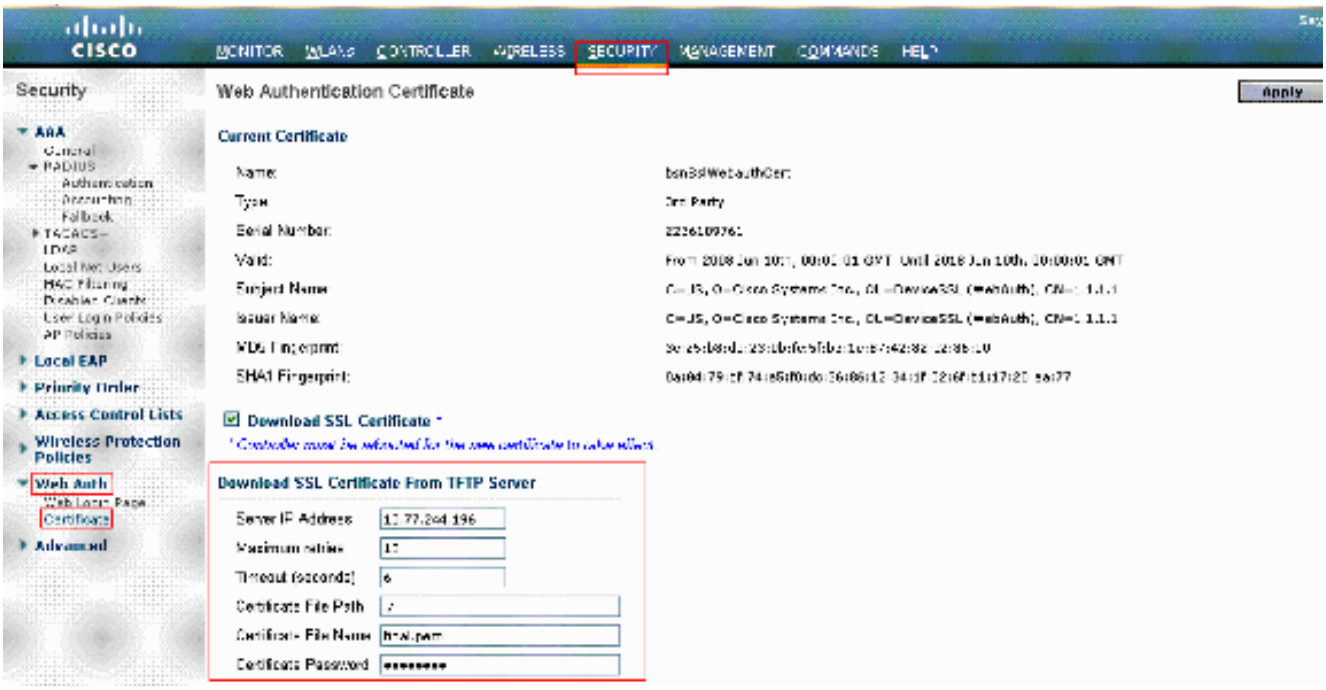
Certificate installed.
Reboot the switch to use new certificate.
```

5. 重新启动WLC为了更改能生效。

步骤3 GUI.下载第三方认证到与GUI的WLC

完成这些步骤为了下载被串连的认证到与GUI的WLC ：

1. 复制设备认证final.pem到在您的TFTP server的默认目录。
2. 选择**安全> Web Auth > Cert**为了打开Web认证认证页。
3. 检查**下载SSL认证**复选框为了查看从TFTP server参数的下载SSL认证。
4. 在IP Address字段，请输入TFTP server的IP地址。



5. 在文件路径领域，请输入认证的目录路径。

6. 在名字段，请输入认证的名字。

7. 在认证密码字段，请输入使用保护认证的密码。

8. 单击 **Apply**。

9. 在下载完成后，请选择**命令>重新启动>重新启动**。

10. 如果提示保存您的更改，请点击**"Save"并且重新启动**。

11. 点击OK键为了确认您的决策重新启动控制器。

Troubleshoot

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**调试转移所有enable (event)**和**pm pki enable (event)**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，当中间CA是不正确的时：

```
(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.
```

Related Information

- 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
- Technical Support & Documentation - Cisco Systems