生成和导入第三方证书的CSR

目录

简介

本文档介绍如何在AireOS WLC上生成和导入证书。

先决条件

要求

Cisco 建议您了解以下主题：

- 如何配置 WLC、轻量级无线接入点 (LAP) 和无线客户端卡以执行基本操作.
- 如何使用OpenSSL应用.
- 公钥基础设施和数字证书

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

- 特定于第三方认证机构(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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

链接证书

证书链是证书序列，链中的每个证书由后续证书签名。

证书链的目的是建立从对等证书到受信任CA证书的信任链。签名时，CA将对等证书中的身份进行担保。

如果CA是您信任的CA（通过根证书目录中存在的CA证书副本指示），则意味着您也可以信任签名对等证书。

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

控制器允许将设备证书下载为用于 Web 身份验证的链接证书。

证书级别

- 0级 — 仅在WLC上使用服务器证书
- 1级 — 在WLC上使用服务器证书和CA根证书
- 第2级 — 在WLC上使用服务器证书、一个CA中间证书和一个CA根证书
- 第3级 — 在WLC上使用服务器证书、两个CA中间证书和一个CA根证书

WLC 不支持在 WLC 上使用大小超过 10KB 的链接证书。但是，WLC 7.0.230.0 及更高版本中已去除这一限制。

注意：链接证书受支持，并且实际上是Web身份验证和Web管理所必需的。

注意：本地EAP、管理或Web身份验证完全支持通配符证书。

Web 身份验证证书可以是以下任何一种证书：

- 链式
- 未链接
- 自动生成

注意：在WLC版本7.6及更高版本中，仅支持链接证书（因此是必需的）。

要生成用于管理的非链接证书，本文档将忽略证书与CA证书结合使用的部分。

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

生成CSR有两种方法。使用OpenSSL（8.3之前的WLC软件中唯一可能的方式）手动生成CSR，或者进入WLC自身生成CSR（8.3.102之后提供）。

选项 A：使用 OpenSSL 生成 CSR

> 注意：Chrome版本58及更高版本不信任证书的公用名，并且要求同时提供使用者备用名。下一节将介绍如何将SAN字段添加到OpenSSL CSR，这是此浏览器的一项新要求。

完成以下步骤，以使用 OpenSSL 生成 CSR：

1. 安装并打开OpenSSL。

   在 Microsoft Windows 中，默认情况下，openssl.exe 位于以下位置：C:\ > openssl > bin。

   > 注意：OpenSSL 0.9.8版是适用于旧WLC版本的推荐版本；但是，自7.5版起，也添加了对OpenSSL 1.0版的支持(请参阅Cisco Bug ID CSCti65315 -需要支持使用OpenSSL v1.0生成的证书)，这是推荐使用的版本。OpenSSL 1.1 works也经过测试，可在8.x及更高版本的WLC上运行。

2. 找到 OpenSSL 配置文件并复制该配置文件，以便为生成此 CSR 编辑该副本。编辑副本以添加以下部分：
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
```

   以“DNS.1”、“DNS.2”（依此类推）开头的行必须包含证书的所有备用名称。然后写下所有可

用于WLC的URL。上一个示例中以粗体显示的行不存在，或者在我们的实验openSSL版本中进行了注释。它可能因操作系统和openssl版本而异。在本例中，我们将修改后的配置文件保存为 openssl-san.cnf。

4. 输入以下命令以生成新的CSR：

```
OpenSSL>req -new -newkey rsa:3072 -nodes -keyout mykey.pem -out myreq.pem -config openssl-san.cnf
```

注意：自8.5软件版本起，WLC支持的最大密钥大小为4096位。

5. 系统会提示输入某些信息：国家/地区名称、州/省、城市等。提供必填信息。

注意：提供正确的公用名非常重要。确保用于创建证书的主机名（通用名称）与 WLC 上虚拟接口 IP 地址对应的域名系统 (DNS) 主机名条目匹配，并且该名称也存在于 DNS 中。此外，在对虚拟 IP (VIP) 接口进行更改后，必须重新启动系统才能使更改生效。

例如：

```
OpenSSL>req -new -newkey rsa:3072 -nodes -keyout mykey.pem -out myreq.pem -config openssl-san.cnf
Loading 'screen' into random state - done
Generate a 1024 bit RSA private key
.....................................................................++++++
.....................................................++++++
writing new private key to 'mykey.pem'
-----
You are about to be asked to enter information that is 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 is a default value,
If you enter '.', the field is 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 []:(email address)

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:Test123
An optional company name []:OpenSSL>
```

6. 您可以通过openssl req -text -noout -in csrfilename验证CSR（尤其是对于SAN属性

presentE）。

7. 提供所有必需的详细信息后，系统将生成两个文件：
    - 包含名称mykey.pem的新私钥。
    - 包含名称myreq.pem的CSR。

选项 B. 通过 WLC 生成 CSR

如果您的WLC运行软件版本8.3.102或更高版本，则更安全的选项是使用WLC生成CSR。优点是密钥在WLC上生成，不会离开WLC；因此不会暴露在外界中。

到目前为止，此方法不允许在CSR中配置SAN，已知这会导致某些浏览器出现问题，需要存在SAN属性。有些CA允许在签名时插入SAN字段，因此最好与您的CA进行检查。

WLC自身生成CSR所用的密钥大小为2048位，ecdsa密钥大小为256位。

注意：如果您运行csr generation命令并且未安装后续证书，则您的WLC将在下次重新启动时在HTTPS上完全无法访问，因为WLC在重新启动后使用新生成的CSR密钥，但是没有随附的证书。

要生成用于Web身份验证的CSR，请输入以下命令：

```
(WLC) >config certificate generate csr-webauth BE BR Brussels Cisco TAC
mywebauthportal.wireless.com tac@cisco.com
-----BEGIN CERTIFICATE REQUEST-----
MIICqjCCAZICAQAwZTELMAkGA1UECAwCQllxETAPBgNVBAcMCEJydXNzZWxzMQ4w
DAYDVQQKDAVDaXNjbzEMMAoGA1UECwDVEFDMSUwIwYDVQQDDBxteXdlYmF1dGhw
b3J0YWud2lyZWxlc3MuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEAnssc0BxlJ2ULa3xgJH5lAUtbd9CuQVqqf2nflh+V1tu82rzTvz38bjF3g+MX
JiaBbKMA27VJH1J2K2ycDMlhjyYpH9N59T4fXvZr3JNGVfmHIRuYDnCSdil0ookK
FU4sDwXyOxR6gfB6m+Uv5SCOuzfBsTz5bfQ1NlZqg1hNemnhqVgbXEd90sgJmaF2
0tsL0jUhbLosdwMLUbZ5LUa34mvufoI3VAKA0cmWZh2WzMJiaI2JpbO0afRO3kSg
x3XDkZiR7Z9a8rK6Xd8rwDlx0TcMFWdWVcKMDgh7Tw+Ba1cUjjIMzKT6OOjFGOGu
yNkgYefrrBN+WkDdc6c55bxErwIDAQABoAAwDQYJKoZIhvcNAQELBQADggEBAB0K
ZvEpAafoovphlcXIEl2DSwVzjlbd9u7T5JRGgqri1l9/0wzxFjTymQofga427mj
5dNqlCWxRFmKhAmO0fGQkUoP1YhJRxidu+0T8O46s/stbhj9nuInmoTgPaA0s3YH
tDdWgjmV2ASnroUV9oBNu3wR6RQtKDX/CnTSRG5YufTWOVf9IRnL9LkU6pzA69Xd
YHPLnD2ygR1Q+3Is4+5Jw6ZQAaqlPWyVQccvGyFacscA7L+nZK3SSITzGt9B2HAa
PQ8DQOaCwnqt2efYmaezGiHOR8XHOaWcNoJQCFOnb4KK6/1aF/7eOS4LMA+jSzt4
Wkc/wH4DyYdH7x5jzHc=
-----END CERTIFICATE REQUEST-----
```

为了生成Webadmin的CSR，该命令更改为：

```
 (WLC) >config certificate generate csr-webadmin BE BR Brussels Cisco TAC
mywebauthportal.wireless.com tac@cisco.com
```

注意：输入命令后，CSR会打印在终端上。没有其他方法可以检索它；无法从WLC上传它，也无法保存它。输入命令后，必须将其复制/粘贴到计算机上的文件。生成的密钥将保留在 WLC 上，直到生成下一个 CSR（因此该密钥将被覆盖）。如果稍后必须更改WLC硬件(RMA)，您将无法重新安装新密钥的相同证书，并且CSR会在新WLC上生成。

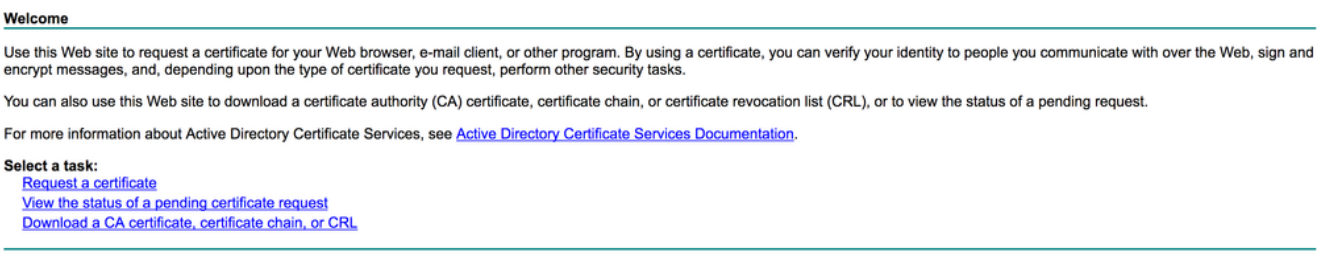
然后，您必须将此 CSR 移交给第三方签名机构或企业公钥基础设施 (PKI)。

第二步：获取证书签名

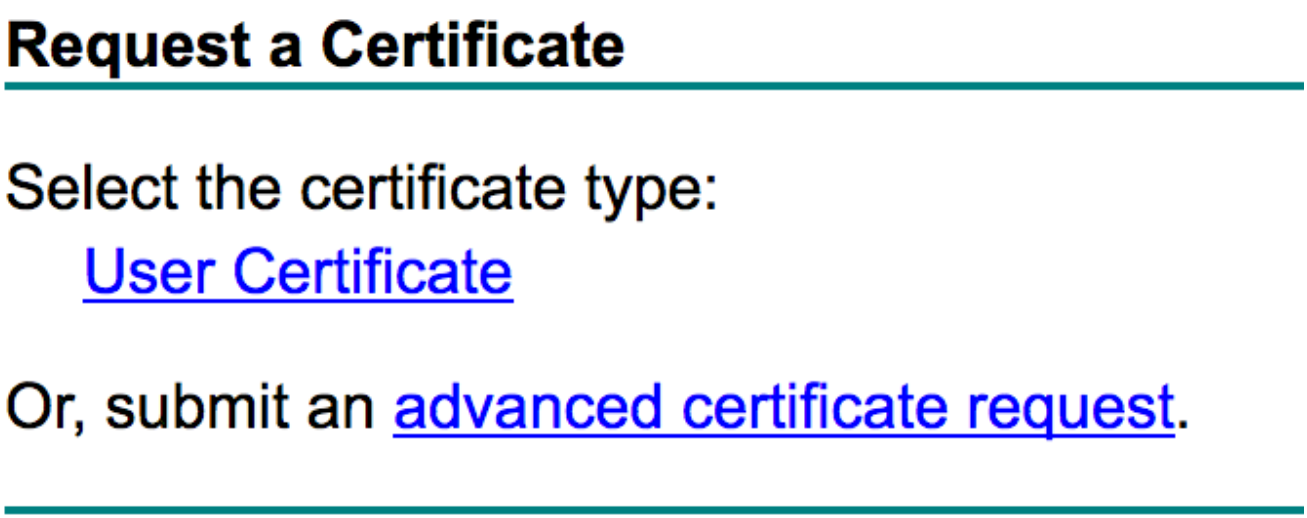
选项A：从您的企业CA获取Final.pem文件

本示例仅展示当前企业CA（本示例中为Windows Server 2012），不包括从头开始设置Windows Server CA的步骤。

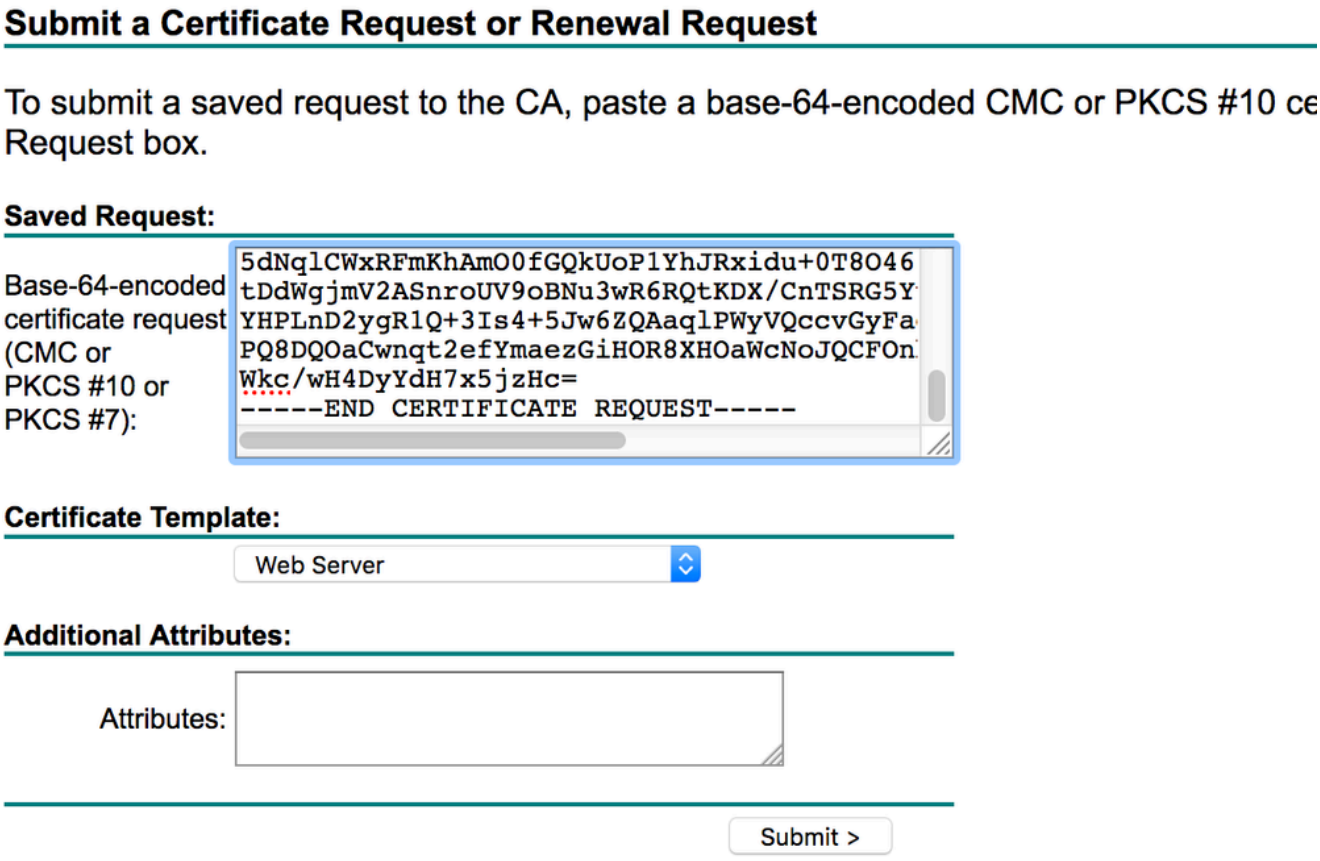
1. 转到浏览器(通常为https://<CA-ip>/certsrv)中的企业CA页面，然后单击“请求证书”。



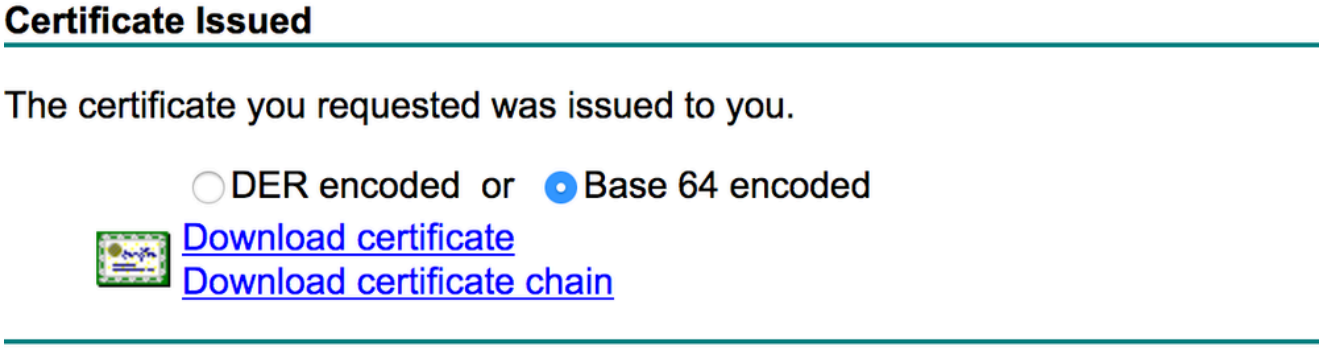
2. 单击高级证书请求。



3. 输入从WLC或OpenSSL获取的CSR。在Certificate Template（证书模板）下拉列表中，选择Web Server（Web服务器）。



4. 单击Base 64 encodedradio按钮。



5. 如果下载的证书类型为PKCS7 (.p7b)，请将其转换为PEM（在下一个示例中，证书链下载为文件名“All-certs.p7b”）：

```
openssl pkcs7 -print_certs -in All-certs.p7b -out All-certs.pem
```

6. 如果选择了选项A（使用OpenSSL生成CSR），则将证书链（在本示例中名为“All-certs.pem”）证书与与CSR（设备证书的私钥，在本示例中为mykey.pem）一起生成的私钥合并，并将文件另存为final.pem。如果直接从WLC生成CSR（选项B），请跳过此步骤。

在OpenSSL应用程序中输入以下命令以创建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。

如果您遵循“选项A.使用OpenSSL的CSR”，则Final.pem是下载到WLC的文件。

如果遵循了“选项B.由WLC自身生成的CSR”，则All-certs.pem是要下载到WLC的文件。下一步是将此文件下载到 WLC。

注意：如果证书上传到WLC失败，请验证pem文件中是否具有整个链。请参阅选项B的步骤 2（从第三方CA获取final.pem）查看其外观。如果您在该文件中仅看到一个证书，则需要手动下载所有中间证书和根 CA 证书文件，并将它们（通过简单的复制粘贴）附加到该文件中以创建链。

选项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。

   将 CSR 提交给第三方 CA 后，第三方 CA 会对证书进行数字签名，并通过电子邮件发回签名的证书链。对于链式证书，您会从CA接收整个证书链。如果只有一个中间证书（如本例所示），您会从 CA 收到以下三个证书：

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

   注意：确保证书与Apache兼容并采用Secure Hash Algorithm 1 (SHA1)加密。

2. 拥有全部三个证书后，请按以下顺序将每个.pem文件的内容复制并粘贴到另一个文件中：

```
------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. 如果使用选项A（使用OpenSSL生成CSR），请将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，并将文件另存为final.pem。如果直接从WLC生成CSR（选项B），请跳过此步骤。

   在OpenSSL应用程序中输入以下命令以创建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。在本例中，为 -passin 和 -passout 参数配置的密码均为 check123。

   如果您遵循“选项A.使用OpenSSL的CSR”，则Final.pem是下载到WLC的文件。 如果遵循“选项B.由WLC自身生成的CSR”，则All-certs.pem是必须下载到WLC的文件。 下一步是将此文件下载到 WLC。

注意：也支持SHA2。Cisco Bug ID CSCuf20725是SHA512支持请求。

第 3 步 CLI.使用CLI将第三方证书下载到WLC

使用CLI完成以下步骤，将链接证书下载到WLC：

1. 将 final.pem 文件移到 TFTP 服务器上的默认目录。

2. 在CLI中，输入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部分的步骤4（或5）中设置的-passout参数口令相同。在本示例中，certpassword必须为check123。如果您选择了选项B（即，使用WLC自身生成CSR），请将certpassword字段留空。

4. 输入命令**transfer download start**查看更新后的设置。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。例如：

```
(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 start.

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

5. 重新启动 WLC，以使更改生效。

第 3 步 GUI.使用GUI将第三方证书下载到WLC

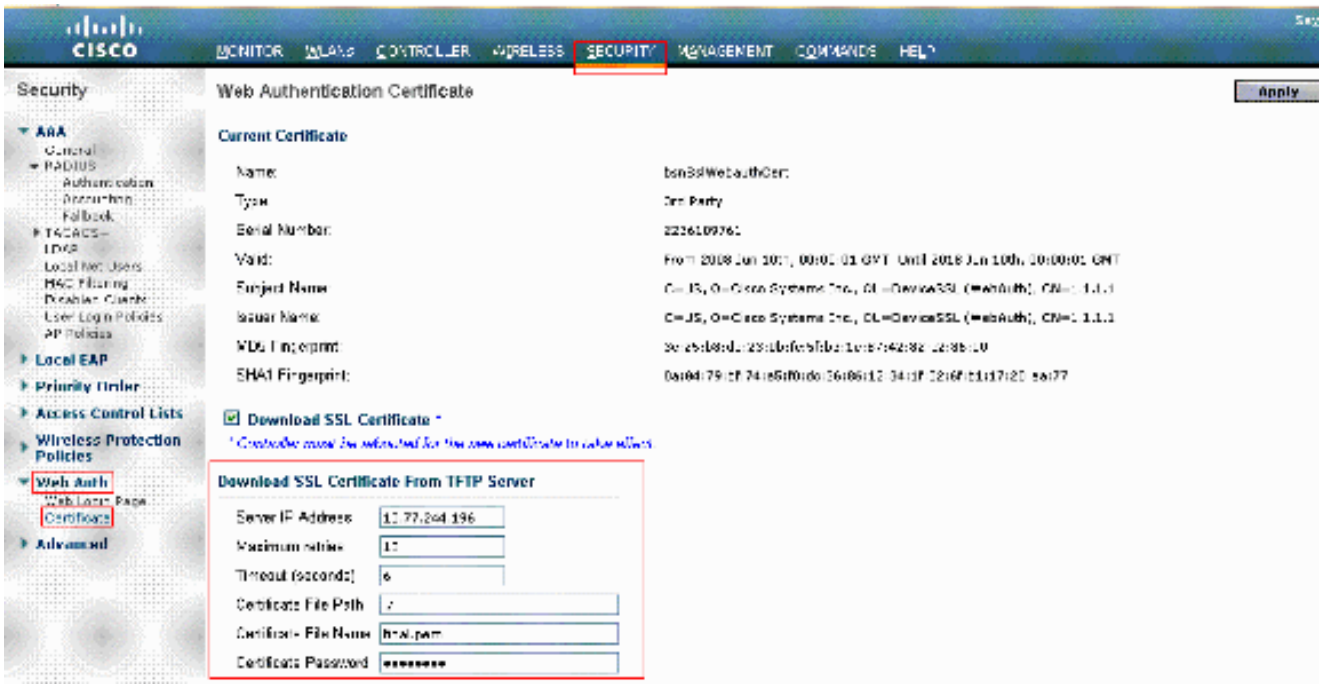
要使用GUI将链接证书下载到WLC，请完成以下步骤：

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

为了排除在WLC上安装证书的故障，请在WLC上打开命令行并输入 **debug transfer all enable** **debug pm pki**

enable ，然后完成下载证书过程。

```
In some cases, the logs only say that the certificate installation failed:

*TransferTask: Sep 09 08:37:17.415: RESULT_STRING: TFTP receive complete... Installing
 Certificate.

*TransferTask: Sep 09 08:37:17.415: RESULT_CODE:13


TFTP receive complete... Installing Certificate.

*TransferTask: Sep 09 08:37:21.418: Adding cert (1935 bytes) with certificate key password.

*TransferTask: Sep 09 08:37:21.421: RESULT_STRING: Error installing certificate.
```

验证证书格式和链。请记住，高于7.6版本的WLC要求存在整个链，因此不能仅上传WLC证书。到根CA的链必须存在于文件中。

以下是中间CA不正确时的调试示例：

```
*TransferTask: Jan 04 19:08:13.338: Add WebAuth Cert: Adding certificate & private key using password ch
*TransferTask: Jan 04 19:08:13.338: Add ID Cert: Adding certificate & private key using password check1
*TransferTask: Jan 04 19:08:13.338: Add Cert to ID Table: Adding certificate (name: bsnSslWebauthCert)
*TransferTask: Jan 04 19:08:13.338: Add Cert to ID Table: Decoding PEM-encoded Certificate (verify: YES)
*TransferTask: Jan 04 19:08:13.338: Decode & Verify PEM Cert: Cert/Key Length was 0, so taking string le
*TransferTask: Jan 04 19:08:13.338: Decode & Verify PEM Cert: Cert/Key Length 7148 & VERIFY
*TransferTask: Jan 04 19:08:13.342: Decode & Verify PEM Cert: X509 Cert Verification return code: 0
*TransferTask: Jan 04 19:08:13.342: Decode & Verify PEM Cert: X509 Cert Verification result text: unable
*TransferTask: Jan 04 19:08:13.342: Decode & Verify PEM Cert: Error in X509 Cert Verification at 0 depth
*TransferTask: Jan 04 19:08:13.343: Add Cert to ID Table: Error decoding (verify: YES) PEM certificate
*TransferTask: Jan 04 19:08:13.343: Add ID Cert: Error decoding / adding cert to ID cert table (verifyCh
*TransferTask: Jan 04 19:08:13.343: Add WebAuth Cert: Error adding ID cert
```

高可用性(HA SSO)注意事项

如 WLC HA SSO 部署指南中所述，在 HA SSO 场景中，不会将证书从主控制器复制到辅助控制器。

这意味着在形成HA对之前，您必须将所有证书导入到辅助设备。

另一个注意事项是，如果在主WLC上生成CSR（因此是在本地创建密钥），则此操作不起作用，因为无法导出该密钥。

唯一的方法是使用 OpenSSL 为主 WLC 生成 CSR（因此将密钥附加到证书），然后在两个 WLC 上导入该证书/密钥组合。

相关信息

- 在无线控制系统 (WCS) 上为第三方证书生成证书签名请求 (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
- WLC HA SSO指南

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）。