

# サードパーティ証明書用 CSR の生成とチェーン証明書の WLC へのダウンロード

## 目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[チェーン証明書](#)

[チェーン証明書のサポート](#)

[証明書のレベル](#)

[ステップ 1. CSR を生成して下さい](#)

[OpenSSL のオプション A. CSR](#)

[WLC によるオプション B. CSR Generated](#)

[ステップ 2. 証明書を署名される得て下さい](#)

[オプション A: エンタープライズ CA からの Final.pem ファイルを得て下さい](#)

[オプション B: サードパーティ CA からの Final.pem ファイルを得て下さい](#)

[ステップ 3 CLI. CLI の WLC にサードパーティ証明書をダウンロードして下さい](#)

[ステップ 3 GUI. GUI の WLC にサードパーティ証明書をダウンロードして下さい](#)

[トラブルシューティング](#)

[関連情報](#)

## 概要

このドキュメントでは、サードパーティの証明書を取得するための証明書署名要求 ( CSR ) の生成方法およびワイヤレス LAN ( WLAN ) コントローラ ( WLC ) へのチェーン証明書のダウンロード方法を説明します。

## 前提条件

### 要件

この設定を試みる前に、これらのトピックのナレッジがあるはずです:

- WLC、Lightweight アクセスポイント ( LAP )、および基本動作のための無線クライアントカードの設定方法
- OpenSSL アプリケーションの使用方法
- 公開鍵インフラストラクチャおよびデジタル証明書

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- ファームウェア バージョン 8.3.102 を実行する Cisco 5508 WLC
- Microsoft Windows 用の OpenSSL アプリケーション
- サードパーティの認証局 ( CA ) 固有の登録ツール

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、初期 ( デフォルト ) 設定の状態から起動しています。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

## チェーン証明書

証明書チェーンはシーケンスになった証明書です。チェーン内の各証明書は、後続の証明書によって署名されています。証明書チェーンの目的はピア証明書からの信頼された CA 認証へ信頼のチェーンを確立することです。CA はピア証明書の識別のためにそれに署名するとき保証します。この CA が信頼できる CA の 1 つであれば、つまり CA 証明書のコピーがルート証明書ディレクトリにあれば、署名されたピア証明書も信頼できることになります。

クライアントは、既知の CA によって作成された証明書でなければ受け入れないことがあります。通常、クライアントでは、証明書の妥当性を確認できないと示します。これは、証明書の署名がクライアントのブラウザに設定されていない中間 CA による場合です。その場合は、チェーン SSL 証明書または証明書グループを使用する必要があります。

### チェーン証明書のサポート

コントローラはデバイス証明書が Web 認証のためのチェーン証明書としてダウンロードされることができるよう考慮に入れます。

### 証明書のレベル

- レベル 0 - WLC のサーバ証明だけの使用
- レベル 1 - WLC および CA ルート証明のサーバ証明の使用
- レベル 2 - WLC、1 つの単一 CA 中間証明書および CA ルート証明のサーバ証明の使用
- レベル 3 - WLC、2 つの CA 中間証明書および CA ルート証明のサーバ証明の使用

WLC は連鎖された証明書を WLC の 10KB よりもっとサポートしません。ただし、この制限は WLC バージョン 7.0.230.0 および以降で取除かれました。

**注:** チェーン証明書は、Web 認証のみでサポートされています。管理証明書ではサポートされていません。

**注:** ワイルドカード証明書はローカル EAP、管理または webauthentication のためにフルサポートされます

次の任意の Web 認証証明書を使用できます。

- チェーン証明書
- チェーンされていない証明書
- 自動生成される

**注:** WLC バージョン 7.6 および それ 以降では、連鎖された証明書だけ Web 認証のための

WLC でサポートされます。

管理目的で解放された証明書を生成するために検知する場合この資料に続き、証明書が CA 認証と結合される部品を無視できます。

このドキュメントでは、チェーン Secure Socket Layer ( SSL ) 証明書を WLC に適切にインストールする方法を説明します。

## ステップ 1. CSR を生成して下さい

CSR を生成する 2 つの方法があります。手動で OpenSSL ( pre-8.3 WLC ソフトウェアの可能な限り唯一の方法 ) または CSR を ( 8.3.102 ) の後で利用可能な生成するのに WLC 自体を使用することと。

### OpenSSL のオプション A. CSR

注: Chrome バージョン 58 および それ以降は単独で証明書の Common Name を信頼しないし、また認証対象代替名をあるように要求します。以降のセクションはこのブラウザのための新しい要件である OpenSSL CSR に SAN フィールドを追加する方法を説明します。

OpenSSL の CSR を生成するためにこれらのステップを完了して下さい:

1. [OpenSSL をインストール](#)し、開いて下さい。

Microsoft Windows では、デフォルトで、openssl.exe は C:\> openssl > ビンにあります。

注: OpenSSL バージョン 0.9.8 は古い WLC リリースのための推奨されるバージョンです; ただし、バージョン 7.5 現在で、OpenSSL バージョン 1.0 のサポートはまた ( Cisco バグ ID [CSCti65315](#) を - OpenSSL v1.0 を使用して生成される証明書のための必要性サポート参照して下さい ) 追加され、使用するべき推奨されるバージョンです。OpenSSL はまた 1.1 作業テストされ、8.x およびそれ以降の WLC リリースの偉大な人をはたらかせます。

2. OpenSSL config ファイルを取付け、そのこの CSR のためにそれを編集するためにコピーを撮って下さい。以降のセクションを追加するためにコピーを編集して下さい:

- 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
```

"DNS.1" から開始するラインは "DNS.2" 等証明書が持っているすべての代替名が含まれているはずですが。それから WLC のために使用する可能性のある URL を書くことができます。太字の上の行はありませんでしたし、またはラボ openssl バージョンでコメントされませんでした、オペレーティングシステムおよび openssl バージョンによって非常に変わるかもしれません。この例のための openssl-san.cnf として構成のこの変更バージョンを保存します。

4. 新しい CSR を生成するためにこのコマンドを発行して下さい:

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

注: WLCs サポート 2,048 ビットの最大キー サイズ。

5. このコマンドを発行すると、複数の情報を求めるメッセージが表示されます。国名、州、都市などです。必要な情報を入力します。

注: 正しい Common Name を入力することが重要です。証明書 ( Common Name ) を作成するのに使用するホスト ネームが WLC の仮想インターフェイス IP アドレスのためのドメイン ネーム システム ( DNS ) ホスト ネーム エントリとおよびその DNS でまた存在する名前一致するようにして下さい。またこの変更が実施されることができるよう Virtual IP ( VIP ) インターフェイスへの変更を行なった後、システムをリブートして下さい。次に例を示します。

```
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. - csrfilename の... -テキスト- noout openssl req が付いている CSR を ( 特に SAN のために存在を帰因させます ) 確認できます
7. 必須詳細すべてを提供した後、2 つのファイルは生成されます:

mykey.pem という名前を含む新しい秘密キー myreq.pem という名前を含む CSR

## WLC によるオプション B. CSR Generated

WLC がソフトウェア バージョン 8.3.102 か以降を実行する場合、より多くのセキュアなオプション ( および最も容易の余りに ) CSR を生成するには WLC を使用することです。長所はキーが WLC で生成されなく、決して WLC を去らないことです; 従って決して外部で露出されません。

現在、この方式はある特定のブラウザにおいての問題の原因となるかもしれない CSR の SAN を設定することを割り当てません SAN アトリビュートの存在を必要とする。署名時に SAN フィールドを挿入する CA 割り当てに従ってそれは CA とチェックするよい概念です。

**注:** CSR 世代別コマンドを実行し、生じる証明書をまだインストールしない場合、WLC は再度ブートするにそれと合っている証明書がなかったが、後 WLC が最近生成された CSR キーを使用するので、次の再度ブートするで HTTPS で全く届かないです。

Web 認証のための CSR を生成するために、このコマンドを入力して下さい:

( WLC ) >config certificate generate CSRwebauth は BR ブリュッセル Cisco TAC  
mywebauthportal.wireless.com tac@cisco.com です

-----BEGIN CERTIFICATE REQUEST-----

```
MIICqjCCAZICAQAwZTELMaKGA1UECAwCQlIxETAPBgNVBACMCEJydXNzZWxzMQ4w
DAYDVQQKDAVDaXNjbzEMMAoGA1UECwwDVEFDMSUwIwYDVQQDDDBxteXdIYmF1dGhw
b3J0YWwud2lyZWxlc3MuY29tMIIBljANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCGKC
AQEAnssc0BxlJ2ULa3xgJH5IAUtbd9CuQVqqf2nflh+V1tu82rzTvz38bjF3g+MX
JiaBbKMA27VJH1J2K2ycDMIhJyYpH9N59T4fXvZr3JNGVfmHIRuYDnCSdil0ookK
FU4sDwXyOxR6gfB6m+Uv5SCOuzfBsTz5bfQ1NIZqg1hNemnhqVgbXEd90sgJmaF2
0tsL0jUhbLosdwMLUbZ5LUa34mvufoI3VAKA0cmWZh2WzMJial2JpbO0afRO3kSg
x3XDkZiR7Z9a8rK6Xd8rwDlx0TcMFWdWVcKMDgh7Tw+Ba1cUjIMzKT6OOjFGOGu
yNkgYefrBN+WkDdc6c55bxErwIDAQABoAAwDQYJKoZIhvcNAQELBQADggEBAB0K
ZvEpAafoovphlcXIEIL2DSwVzjlb9u7T5JRGgqri1I9/0wzxFjTymQofga427mj
5dNqlCWxRFmKhAmO0fGQkUoP1YhJRxidU+0T8O46s/stbhj9nulnmoTgPaA0s3YH
tDdWgjmV2ASnroUV9oBNu3wR6RQtKDX/CnTSRG5YufTWOVf9IRnL9LkU6pzA69Xd
YHPLnD2ygR1Q+3ls4+5Jw6ZQAaqIPWyVQccvGyFacscA7L+nZK3SSITzGt9B2HAa
PQ8DQOaCwnqt2efYmaezGiHOR8XHOaWcNoJQCFOnb4KK6/1aF/7eOS4LMA+jSzt4
Wkc/wH4DyYdH7x5jzHc=
```

-----END CERTIFICATE REQUEST-----

webadmin のための CSR を生成するために、コマンドはやっと変更します:

( WLC ) >config certificate generate CSRwebadmin は BR ブリュッセル Cisco TAC  
mywebauthportal.wireless.com tac@cisco.com です

**注:** CSR はターミナルでコマンドを入力した後印刷されます。それを取得する他の方法がありません; WLC からそれをアップロードすることはできませんそれを保存するそれは可能な限りあります。コマンドを入力した後/貼り付けそれコンピュータのファイルへコピーするためになります。生成されたキーは WLC に次の CSR が生成されるまでとどまります ( キーはこうして上書きされます )。 ( RMA ) WLC ハードウェアを後の方で変更しなければならなければ、New 鍵および CSR が新しい WLC で生成されなければならぬのと同

じ証明書を再インストールできません。

サードパーティ署名権限がエンタープライズ Public Key Infrastructure ( PKI ) にそれからこの CSR を引き渡さなければなりません。

## ステップ 2. 証明書を署名される得て下さい

### オプション A: エンタープライズ CA からの Final.pem ファイルを得て下さい

この例は既存のエンタープライズ CA だけ ( この例の Windows サーバ 2012 ) を展示し、Windows サーバ CA を全く最初から設定するためにステップをカバーしないものです。

1. ブラウザ ( 通常 [https:// <CA-ip>/certsrv](https://<CA-ip>/certsrv) ) の enterprise CA ページに行き、『Request a certificate』をクリックして下さい。

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. [Advanced certificate request] をクリックします。

## Request a Certificate

---

Select the certificate type:

[User Certificate](#)

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

---

3. WLC が OpenSSL から得た CSR を入力して下さい。証明書のテンプレート ドロップダウン リストで、『Web Server』を選択して下さい。

## 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):

```
5dNq1CWxRFmKhAm00fGQkUoP1YhJRxiDu+0T8046
tDdWgjmV2ASnroUV9oBNu3wR6RQtKDX/CnTSRG5Y
YHPLnD2ygR1Q+3Is4+5Jw6ZQAaqlPWYVQccvGyFa
PQ8DQ0aCwnqt2efYmaezGiHOR8XHOaWcNoJQCFOn
Wkc/wH4DyYdH7x5jzHc=
-----END CERTIFICATE REQUEST-----
```

### Certificate Template:

Web Server

### Additional Attributes:

Attributes:

Submit >

4. Base 64 encoded オプション・ ボタンをクリックして下さい。

## Certificate Issued

---

The certificate you requested was issued to you.

DER encoded or  Base 64 encoded



[Download certificate](#)

[Download certificate chain](#)

5. ダウンロードされた証明書がタイプ PKCS7 ( .p7b ) なら、PEM にそれを変換する必要があります ( 下記の例でファイル名 "All-certs.p7b" として証明書 チェーンをダウンロードしました ) :

```
openssl pkcs7 - print_certs -全certs.pem All-certs.p7b の... -
```

6. CSR ( オプション A ( すなわち、CSR を生成するのに OpenSSL を使用しました ) と行った生成し、と共に final.pem としてファイルを保存します場合この例の mykey.pem であるデバイス証明書のプライベート キー、 ) プライベート キーによって証明書 チェーン ( この例で、「全 certs.pem」 指名されます ) 証明書を結合して下さい。WLC ( B ) オプションからの CSR を直接生成したらこのステップをスキップできます。

All-certs.pem ファイルおよび final.pem ファイルを作成するには、OpenSSL アプリケーションで以下のコマンドを発行します。

```
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:** このコマンドでは、パラメータ **-passin** および **-passout** に対してパスワードを入力する必要があります。 **-passout** パラメータに設定するパスワードは、WLC 上で設定する **certpassword** パラメータと一致している必要があります。この例では、**-passin** と **-passout** の両方のパラメータに対してパスワード **check123** を設定しています。

Final.pem は「OpenSSL をオプション A. CSR」の後に記入した場合 WLC にダウンロードする必要があるファイルです。「WLC 自体によって」に生成されたオプション B. CSR 続いた場合全certs.pem WLC にダウンロードする必要があるファイルはです。次の手順では、このファイルを WLC にダウンロードします。

**注:** WLC への証明書のアップロードが失敗した場合、pem ファイルの全体チェーンがなかったらことであるかもしれません。どのようにのように見える必要があるか見るためにオプション B のステップ 2 を ( サードパーティ CA からの final.pem を得て下さい ) 下記に参照して下さい。ファイルの 1 つの証明書だけを見る場合、手動ですべての中間物およびルートCA認証ファイルをダウンロードし、チェーンを作成するためにファイルに ( 単なるコピーペーストによって ) 付ける必要性。

## オプション B: サードパーティ CA からの Final.pem ファイルを得て下さい

1. CSR の情報をコピーして、任意の CA の登録ツールに貼り付けます。

サードパーティ CA に CSR を入れた後、サードパーティ CA はデジタルで証明書に署名し、メールを通して署名入り認証チェーンを送信します。連鎖された証明書の場合には、CA から証明書の全体のチェーンを受け取ります。1 中間証明書次がこの例あるただ場合、CA からこの 3 つの証明書を受け取ります:

Root certificate.pem  
Intermediate certificate.pem  
Device certificate.pem  
**注:** 証明書が 1 ( SHA1 ) 暗号化と Secure Hash Algorithm ( SHA ) Apache 互換性があることを確かめて下さい。

2. 3 つの証明書がすべてあったら、この順序で別のファイルに各 .pem ファイルの内容をコピーアンドペーストして下さい:

```
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. All-certs.pem としてファイルを保存します。

4. CSR ( オプション A ( すなわち、CSR を生成するのに OpenSSL を使用しました ) と行った生成し、と共に final.pem としてファイルを保存します場合この例の mykey.pem であるデバイス 証明書のプライベート キー、 ) プライベート キーによって全certs.pem 証明書を結合して下さい。WLC ( B ) オプションからの CSR を直接生成したらこのステップをスキップできます。

All-certs.pem ファイルおよび final.pem ファイルを作成するには、OpenSSL アプリケーションで以下のコマンドを発行します。

```
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: このコマンドでは、パラメータ **-passin** および **-passout** に対してパスワードを入力する必要があります。 **-passout** パラメータに設定するパスワードは、WLC 上で設定する **certpassword** パラメータと一致している必要があります。この例では、**-passin** と **-passout** の両方のパラメータに対してパスワード **check123** を設定しています。Final.pem は「OpenSSL をオプション A. CSR」の後に記入した場合 WLC にダウンロードする必要があるファイルです。「WLC 自体によって」に生成されたオプション B. CSR 続いた場合全certs.pem WLC にダウンロードする必要があるファイルはです。次の手順では、このファイルを WLC にダウンロードします。

注: SHA2 はまたサポートされます。Cisco バグ ID [CSCuf20725](#) は SHA512 サポートのための要求です。

## ステップ 3 CLI. CLI の WLC にサードパーティ 証明書をダウンロードして下さい

CLI の WLC にチェーン証明書をダウンロードするためにこれらのステップを完了して下さい:

1. TFTP サーバ上のデフォルト ディレクトリに final.pem ファイルを移動します。
2. ダウンロード設定を変更するために、CLI で以下のコマンドを発行します。

```
>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. オペレーティング システムで SSL キーと証明書を復号化できるように、.pem ファイルのパスワードを入力します。

```
>transfer download certpassword password
```

注: certpassword の値が同じであること [生成する](#) のステップ 4 で設定された確実な-passout パラメータ パスワードで下さい (または 5) [CSR](#) セクション。この例では、certpassword は check123 である必要があります。B を『Option』を選択したら WLC 自体を使用しなさい (すなわち、CSR を生成すればのに) certpassword フィールドは空白を残すことができる。

4. transfer download start コマンドを発行して、更新された設定を表示します。次に、プロンプトで y と入力して、現在のダウンロード設定を確認し、証明書とキーのダウンロードを開始します。次に例を示します。

```
(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.
```

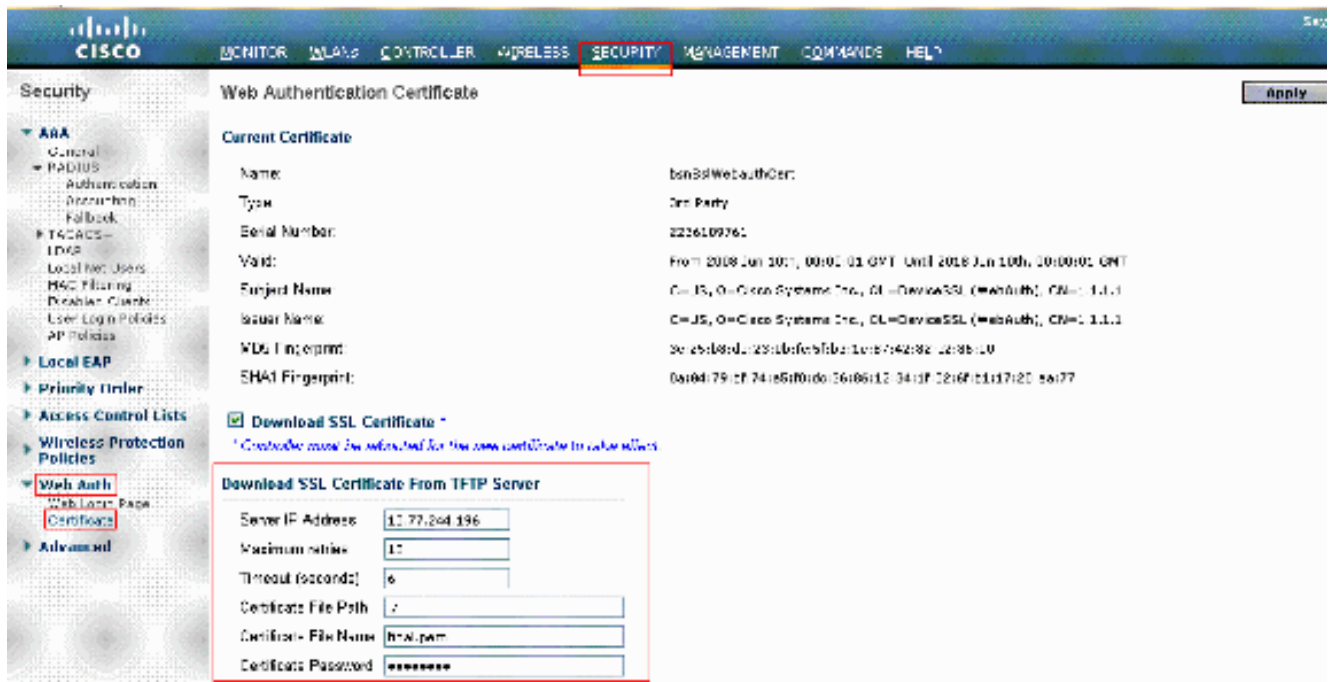
```
Certificate installed.
Reboot the switch to use new certificate.
```

5. 変更を有効にするために、WLC をリブートします。

## ステップ 3 GUI. GUI の WLC にサードパーティ 証明書をダウンロードして下さい

GUI の WLC にチェーン証明書をダウンロードするためにこれらのステップを完了して下さい:

1. デバイスの証明書 final.pem を TFTP サーバ上のデフォルト ディレクトリにコピーします。
2. [Security] > [Web Auth] > [Cert] を選択して [Web Authentication Certificate] ページを開きます。
3. [Download SSL Certificate] チェック ボックスをオンにして、[Download SSL Certificate From TFTP Server] のパラメータを表示します。
4. [IP Address] フィールドに、TFTP サーバの IP アドレスを入力します。



5. [File Path] フィールドに、証明書のディレクトリパスを入力します。
6. [File Name] フィールドに、証明書の名前を入力します。
7. [Certificate Password] フィールドに、証明書を保護するために使用されたパスワードを入力します。
8. [Apply] をクリックします。
9. ダウンロードの完了後、[Commands] > [Reboot] > [Reboot] の順に選択します。
10. 変更を保存するように求めるプロンプトが表示されたら、[Save and Reboot] をクリックします。
11. 変更内容を確定するために [OK] をクリックして、コントローラをリポートします。

## トラブルシューティング

多分提起する何が問題は WLC の証明書のインストールです。 解決するために、WLC のコマンド・ラインを開き、デバッグ転送をすべて入力するために pm PKI それから完了しますダウンロード証明書 プロシージャを有効にし、。

```
(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.

証明書フォーマットおよびそして連鎖を確認する必要があります。バージョン 7.6 より WLCs 以降は全体チェーンがあるように要求する従って単独で WLC 証明書しかアップロードできませんことを覚えていて下さい。ルートCA までのチェーンはファイルにある必要があります。

中間 CA が不正確なときデバッグの例はここにあります:

```
(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.

## 関連情報

- [サードパーティ証明書用 CSR の生成とチェーンされていない証明書の WLC へのダウンロード](#)
- [Wireless Control System \( WCS \) でのサードパーティ証明書のための証明書署名要求 \( CSR \) の生成](#)
- [Linux サーバ上にインストールされた Wireless Control System \( WCS \) 証明書署名要求 \( CSR \) の設定例](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)