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

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。

- Cisco 5508 WLC ファームウェアのバージョン 8.3.102 を実行する
- 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

このドキュメントの情報は、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、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

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 認証からの信頼された CA 認証へ信頼のチェーンを確立することです。 CA はピア 認証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 認証が 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に考慮に入れます。

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 中間認証および CA ルート証明のサーバ証明の使用
- レベル 3 - WLC、2 つの CA 中間認証および CA ルート証明のサーバ証明の使用

WLC は連鎖された認証を WLC の 10KB よりもっとサポートしません。 ただし、この制約事項は WLC バージョン 7.0.230.0 およびそれ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。

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、連鎖された認証だけ Web 認証のための WLC でサポートされます。

チェーンされていない証明書を WLC 上で使用する方法については、「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」を参照してください。

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 以降は単独で認証の 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 のためのサポートはまた（Cisco バグ ID CSCti65315 を- OpenSSL v1.0 を使用して生成される認証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 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、それのこの 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** として構成のこの修正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。 認証（Common Name）を作成するのに使用するホスト名が WLC の仮想インターフェイス IP アドレスのための Domain Name System（DNS）ホスト名項目とおよびその DNS で同様に存在 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に Virtual IP（VIP）への変更をインターフェイスさせる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 またはそれ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; 従って決して外界で露出されません。

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、生じる認証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認証がなかったが、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
DAYDVQQKDAVDaXNjbzEMMAoGA1UECwwDVEFDMSUwIwYDVQQDDBxteXdlYmF1dGhw
b3J0YWwud2lyZWxlc3MuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEAnssc0BxlJ2ULa3xgJH5lAUtbd9CuQVqqf2nflh+V1tu82rzTvz38bjF3g+MX
JiaBbKMA27VJH1J2K2ycDMlhjyYpH9N59T4fXvZr3JNGVfmHIRuYDnCSdil0ookK
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 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ないのと同じ認証を再インストールできません。

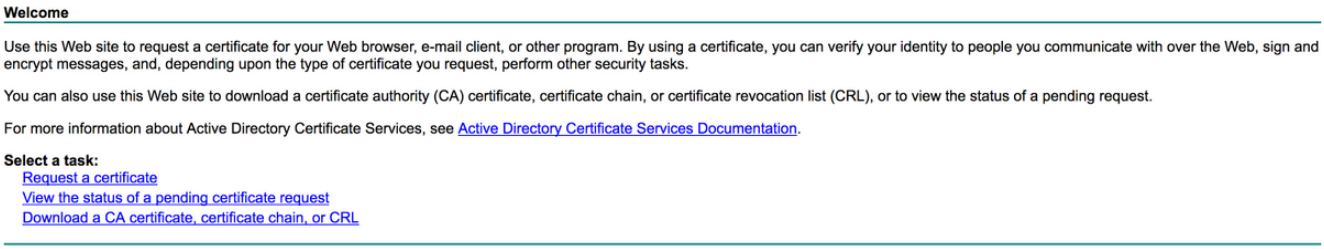
サード パーティ 署名 権限か企業 公開鍵インフラストラクチャ（PKI）にそれからこの CSR を引き渡さなければなりません。

ステップ 2.認証を署名される得て下さい

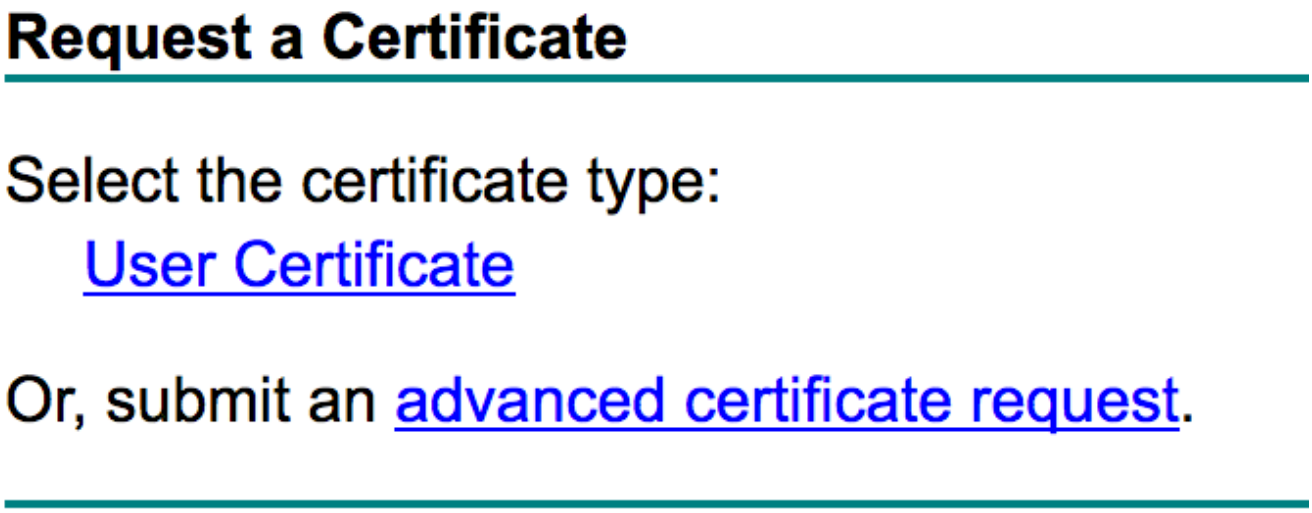
オプション A: 企業 CA からの Final.pem ファイルを得て下さい

この例は既存の企業 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。

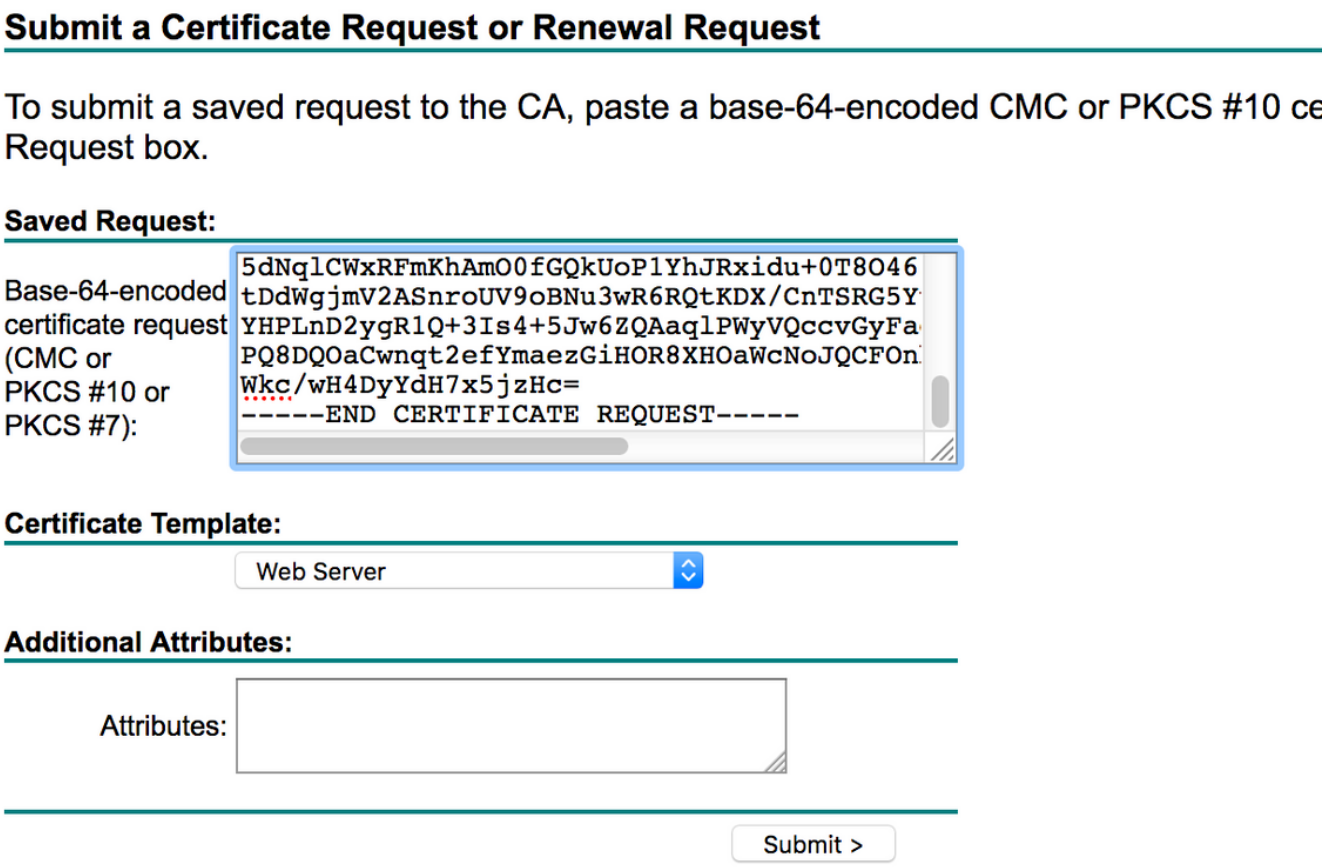
1. ブラウザ（通常 https:// <CA-ip>/certsrv）の enteprrise CA ページに行き、『Request a certificate』 をクリック して下さい。



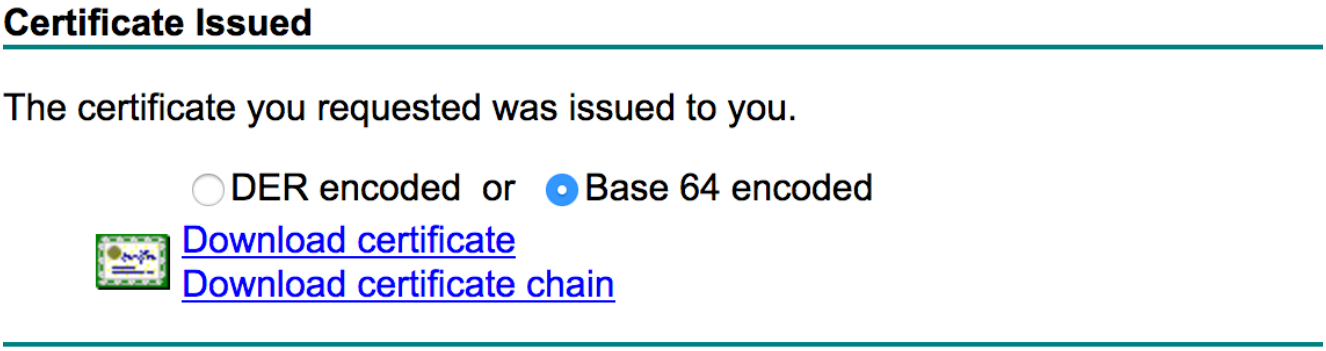
2. [Advanced certificate request] をクリックします。



3. WLC か 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。



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



5. ダウンロードされた認証が型 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 であるデバイス認証のプライベートキー、 ）プライベートキーと証明書 チェーン （ この例で、「全certs.pem」指名されます ）認証を結合して下さい。 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 への認証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。 オプション B のステップどのようにのように見える必要があるか見る 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 つの認証だけを見る場合、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（単なるコピー貼り付けによって）追加 する必要。

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 認証に署名し、電子メールを通して署名入り認証 チェーンを送信 します。 連鎖された認証の場合には、CA から認証の全体のチェーンを受け取ります。 1 中間認証 次がこの例あるただ場合、CA からこの 3 つの認証を受け取ります:

   Root certificate.pemIntermediate certificate.pemDevice certificate.pem**注:** 認証がセキュアハッシュアルゴリズム 1（SHA1）暗号化と Apache 互換性があることを確かめて下さい。
2. 3 つの認証がすべてあったら、この順序で別のファイルに各 .pem ファイルのコンテンツをコピー 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 認証のプライベートキー、) プライベートキーと全certs.pem 認証を結合して下さい。 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 認証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 の値がと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 パスワードでであって下さい（ 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 認証をダウンロードして下さい

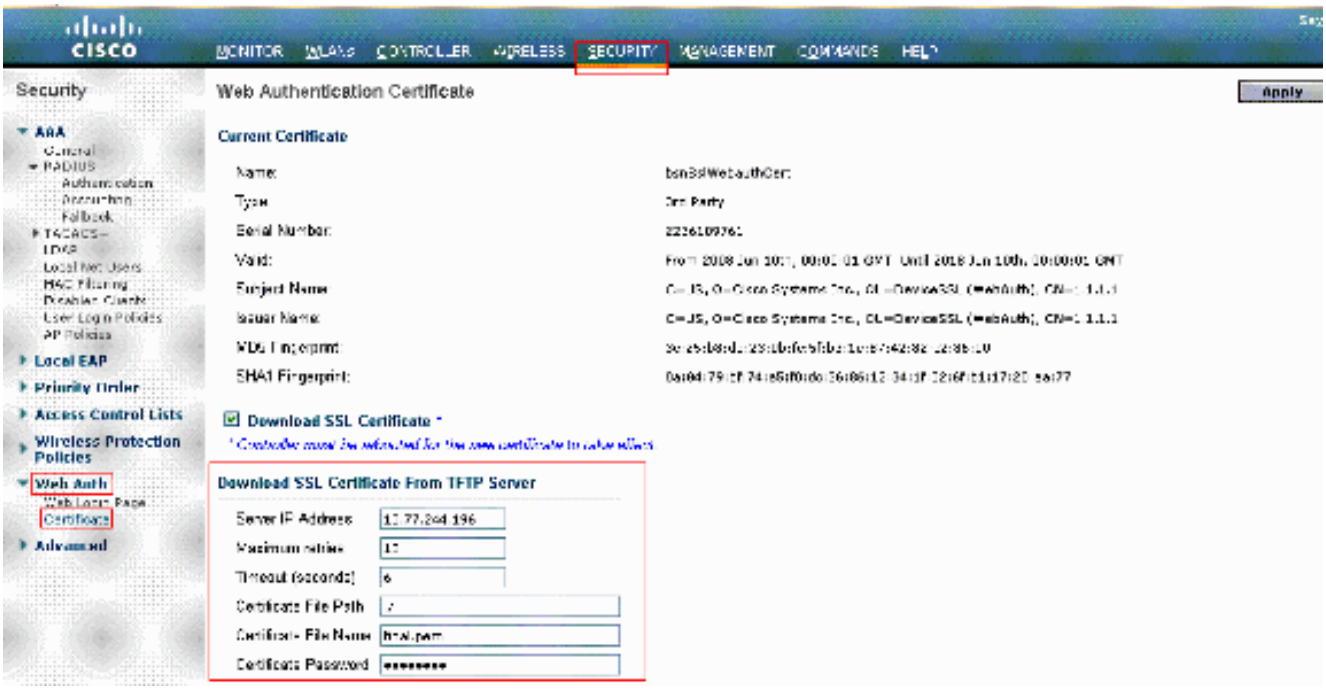
GUI の WLC にチェーン証明書をダウンロードするためにこれらのステップを完了して下さい:

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、コントローラをリブートします。

トラブルシューティング

多分提起する何が問題は WLC の認証のインストールです。 解決し、WLC のコマンド・ラインを開き、**デバッグ転送をすべてのイネーブル**入力し、次にダウンロード認証 プロシージャを完了するため。

```
(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 認証しかアップ ロードなできます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。

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