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。

- ファームウェア バージョン 5.1.151.0 が稼働している Cisco 4400 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

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

先のコントローラ バージョン バージョン 5.1.151.0 よりでは、Web 認証 認証はデバイス 認証だけである場合もあり、デバイス 認証 (連鎖された認証無し) に連鎖される CA ルートが含まれていないはずです。 バージョン 5.1.151.0 以降のコントローラの場合は、デバイス証明書を Web 認証用のチェーン証明書としてダウンロードできます。

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 原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 原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 原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

先のソフトウェア バージョン バージョン 5.1.151.0 よりとの WLCs に関しては、回避策はこれらのオプションの 1 つを使用することです:

- チェーンされていない証明書を CA から入手します。これは、署名ルートを証明できることを意味します。
- すべての有効な中間 CA ルート証明書 (信頼できるかできないかを問わない) をクライアントにインストールします。

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。

CSR の生成

CSR を生成するには、次の手順を実行します。

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追加されました（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）。

2. 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
   ```

   注: WLCs サポート 2,048 ビットの最大キーサイズ。

3. 時々新しい CSR を生成することを試みるとき **req で /usr/local/ssl/openssl.cnf エラーから構成ヒントをロードすることが不可能な**エラーを受け取るかもしれません。 これは openssl.cfg（か openssl.cnf）ファイルの位置がデフォルト OpenSSL フォルダにない場合起こる場合があります。 この問題を解決するために、コマンドの openssl.cfg ファイルに CSR を生成するために全体のパス名を規定 しなければなりません。 次に例を示します。

   ```
   OpenSSL> req -config "C:\Open SSL1\OpenSSL\bin\openssl.cfg" -new -newkey rsa:
   1024 -nodes -keyout mykey.pem -out myreq.pem
   ```

   このパスは、OpenSSL Config ファイルの < C:\Open SSL1\OpenSSL\bin\openssl.cfg >、ファイルロケーションに基づいて異なるかもしれません。

4. 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
   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>
```

5. 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

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。 この例のような 1 つの中間認証があるただ場合、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:

```
------BEGIN CERTIFICATE------
*Device cert*
------END CERTIFICATE------
------BEGIN CERTIFICATE------
*Intermediate CA cert *
------END CERTIFICATE--------
------BEGIN CERTIFICATE------
*Root CA cert *
------END CERTIFICATE------
```

3. *All-certs.pem* としてファイルを保存します。

4. All-certs.pem 証明書を CSR と同時に生成した秘密キー (デバイス証明書の秘密キー、この例では mykey.pem) と結合し、ファイルを *final.pem* として保存します。

   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 WLC にダウンロードする必要があるファイル**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。

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 に対する値が、「**CSR の生成**」のステップ 4 で設定した **-passout** パラメータのパスワードと同一であることを確認してください。 この例では、**certpassword** は **check123** である必要があります。

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
```

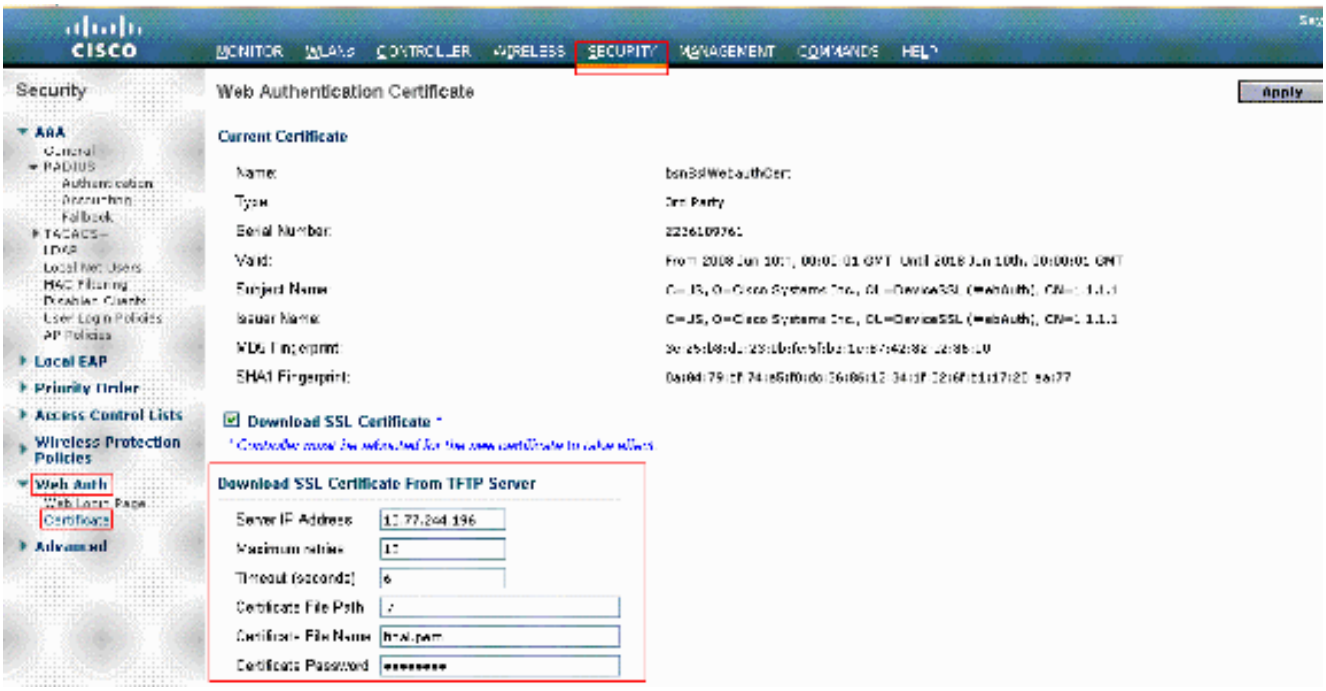
```
Mode..................................... TFTP
Data Type................................ Site Cert
TFTP Server IP........................... 10.77.244.196
TFTP Packet Timeout...................... 6
TFTP Max Retries......................... 10
TFTP Path......................................./
TFTP Filename............................ final.pem

This may 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。

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。

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