証明書の管理

外部で生成した SSL 証明書のロード

TFTP サーバなどのサポートされている転送方法を使用して、外部で生成された SSL 証明書をコントローラにダウンロードできます。TFTP を使用する際の注意事項は次のとおりです。

- サービス ポート経由で証明書をロードする場合、サービス ポートはルーティングできないため、TFTP サーバはコントローラと同じサブネット上になければなりません。そうでない場合は、コントローラ上に静的ルートを作成する必要があります。また、証明書をディストリビューション システム ネットワーク ポート経由でロードする場合は、TFTP サーバはどのサブネットに存在していてもかまいません。
- サードパーティの TFTP サーバを Cisco Prime Infrastructure と同じ PC 上で実行することはできません。Prime Infrastructure 内蔵 TFTP サーバとサードパーティの TFTP サーバのどちらも、同じ通信ポートを使用するからです。

（注） チェーン証明書は Web 認証と管理証明書に対してサポートされています。

関連資料

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 [英語]：
https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/109597-csr-chained-certificates-wlc-00.html

SSL 証明書のロード（GUI）

手順

ステップ 1 **[Security]** > **[Web Auth]** > **[Certificate]** を選択します。

ステップ 2 [Web Authentication Certificate] ページで、 [Download SSL Certificate] チェックボックスをオンにします。

（注） コントローラの GUI で TFTP 転送モードのみが使用されます。コントローラ CLI では、FTP などの他の方式も使用できます。

ステップ 3 [Server IP Address] フィールドに、TFTP サーバの IP アドレスを入力します。

ステップ 4 [Maximum Retries] フィールドに、TFTP サーバによる証明書のダウンロードの最大試行回数を入力します。

ステップ 5 [Timeout] フィールドに、TFTP サーバによる証明書のダウンロードの試行時間（秒単位）を入力します。

ステップ 6 [Certificate 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。

ステップ 7 [Certificate File Name] フィールドに、証明書の名前（webadmincert_name.pem）を入力します。

ステップ 8 （オプション）[Certificate Password] フィールドに、証明書を暗号化するためのパスワードを入力します。

ステップ 9 設定を保存します。

ステップ 10 **[Commands]** > **[Reboot]** > **[Reboot]** > **[Save and Reboot]** を選択し、コントローラをリブートして変更内容を反映します。

SSL 証明書のロード（CLI）

この項で説明する手順は webauthcert のインストールと webadmincert のインストールの両方に似ていますが、データタイプのダウンロードに違いがあります。

手順

ステップ 1 パスワードを使用して、.PEM エンコードファイル形式の HTTPS 証明書を暗号化します。PEM エンコード ファイルは、Web アドミニストレーション証明書ファイル（`webadmincert_name.pem`）と呼ばれます。

ステップ 2 webadmincert_name.pem ファイルを TFTP サーバ上のデフォルト ディレクトリに移動します。

ステップ 3 現在のダウンロードの設定を表示するには、次のコマンドを入力してプロンプトに**n**と応答します。

transfer download start

以下に類似した情報が表示されます。

```
Mode..................................... TFTP
Data Type................................ Admin Cert
TFTP Server IP........................... xxx.xxx.xxx.xxx
TFTP Path................................ <directory path>
TFTP Filename.............................
Are you sure you want to start? (y/n) n
Transfer Canceled
```

ステップ 4 次のコマンドを使用して、ダウンロード設定を変更します。

transfer download mode *tftp*

transfer download datatype *webadmincert*

transfer download serverip *TFTP_server IP_address*

transfer download path *absolute_TFTP_server_path_to_the_update_file*

transfer download filename *webadmincert_name.pem*

ステップ 5 オペレーティング システムが Web アドミニストレーション SSL キーおよび証明書の暗号化を解除できるように、.PEM ファイルのパスワードを設定するには、次のコマンドを入力します。

transfer download certpassword *private_key_password*

ステップ 6 現在のダウンロードの設定を確認して証明書とキーのダウンロードを開始するには、次のコマンドを入力して、プロンプトに **y** と応答します。

transfer download start

以下に類似した情報が表示されます。

```
Mode..................................... TFTP
Data Type................................ Site Cert
TFTP Server IP........................... xxx.xxx.xxx.xxx
TFTP Path................................ directory path
TFTP Filename............................ webadmincert_name
Are you sure you want to start? (y/n) y
TFTP Webadmin cert transfer starting.
Certificate installed.
Please restart the switch (reset system) to use the new certificate.
```

ステップ 7 リブート後も変更内容が維持されるように、SSL 証明書、キー、セキュア Web パスワードを NVRAM に保存するには、次のコマンドを入力します。

save config

ステップ 8 コントローラをリブートするには、次のコマンドを入力します。

reset system

デバイスの証明書のダウンロード

各無線デバイス（コントローラ、アクセスポイント、およびクライアント）には独自のデバイスの証明書があります。たとえば、コントローラには、シスコによりインストールされたMICデバイスの証明書が付属しています。

（注） ローカル EAP の設定の詳細については、「ローカル EAP の設定」セクションを参照してください。

この項の手順に従って、GUIまたはCLIのいずれかを使用して、ベンダー固有のデバイスの証明書をコントローラにダウンロードします。ただし、ダウンロードを開始する前に、証明書のダウンロードに TFTP または FTP サーバを使用できることを確認します。TFTP または FTP サーバをセットアップする場合は、次のガイドラインに従ってください。

- サービス ポート経由でアップグレードする場合、サービス ポートはルーティングできないため、TFTPまたはFTPサーバはサービス ポートと同じサブネット上になければなりません。あるいは、コントローラ上に静的ルートを作成する必要があります。
- ディストリビューション システム ネットワーク ポートを経由してアップグレードする場合、ディストリビューション システム ポートはルーティング可能なので、TFTP または FTPサーバは同じサブネット上にあっても、別のサブネット上にあってもかまいません。
- Prime Infrastructure 内蔵 TFTP または FTP サーバとサードパーティの TFTP または FTP サーバは同じ通信ポートを使用する必要があるため、サードパーティの TFTP または FTP サーバは Cisco Prime Infrastructure と同じコンピュータ上で実行できません。

（注） コントローラにダウンロードする証明書はすべて、PEM形式でなければなりません。

（注） デフォルト（ゼロタッチ設定）サプリカントで Microsoft Windows 10 を使用しているクライアントは、サーバ証明書を検証するための CA 証明書が存在しない場合、コントローラへの接続に失敗します。これは、サプリカントではサーバ証明書を受け入れるためのウィンドウがポップアップ表示されず、802.1 X 認証がサイレントに拒否されるためです。したがって、次のいずれかを実行することをお勧めします。

- Microsoft Windows 10 を使用しているクライアントが信頼できるサードパーティの CA 証明書を AAA サーバに手動でインストールします。
- サーバ証明書を信頼するか、信頼しないかを選択するウィンドウがポップアップ表示される、その他のサプリカント（Cisco AnyConnect など）を使用します。信頼できる証明書を受け入れると、クライアントが認証されます。

関連トピック

ローカル EAP について

デバイスの証明書のダウンロード（GUI）

手順

ステップ 1 サーバ上のデフォルト ディレクトリにデバイス証明書をコピーします。

ステップ 2 [Commands] > [Download File] の順に選択して、[Download File to Controller] ページを開きます。

ステップ 3 [File Type] ドロップダウン リストから、[Vendor Device Certificate] を選択します。

ステップ 4 [Certificate Password] テキスト ボックスに、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。

ステップ 5 [Transfer Mode] ドロップダウン リストで、次のオプションから選択します。

- **TFTP**
- **FTP**
- SFTP（7.4 以降のリリースで利用可能）

ステップ 6 [IP Address] テキスト ボックスに、サーバの IP アドレスを入力します。

TFTP サーバを使用している場合は、[Maximum Retries] テキスト ボックスの 10 回の再試行および [Timeout] テキスト ボックスの 6 秒というデフォルト値は、調整しなくても適切に機能します。ただし、これらの値は変更できます。

ステップ 7 TFTP サーバが証明書のダウンロードを試行する最大回数を [Maximum Retries] テキスト ボックスに入力し、TFTP サーバが証明書のダウンロードを試行する時間（秒単位）を [Timeout] テキスト ボックスに入力します。

ステップ 8 [File Path] テキスト ボックスに、証明書のディレクトリ パスを入力します。

ステップ 9 [File Name] テキスト ボックスに、証明書の名前を入力します。

ステップ 10 FTP サーバを使用している場合は、次の手順に従います。

a) [Server Login Username] テキスト ボックスに、FTP サーバにログインするためのユーザ名を入力します。

b) [Server Login Password] テキスト ボックスに、FTP サーバにログインするためのパスワードを入力します。

c) [Server Port Number] テキスト ボックスに、ダウンロードが発生する FTP サーバのポート番号を入力します。デフォルト値は 21 です。

ステップ 11 [Download] をクリックして、デバイスの証明書をコントローラにダウンロードします。ダウンロードのステータスを示すメッセージが表示されます。

ステップ 12 ダウンロードの完了後、**[Commands]** > **[Reboot]** > **[Reboot]** の順に選択します。

ステップ 13 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。

ステップ 14 [OK] をクリックし、変更内容を確定してコントローラをリブートします。

デバイスの証明書のダウンロード（CLI）

手順

ステップ 1 コントローラ CLI にログインします。

ステップ 2 次のコマンドを入力して、設定ファイルのダウンロードに使用する転送モードを指定します。

transfer download mode {**tftp** | **ftp** | **sftp**}

ステップ 3 次のコマンドを入力して、ダウンロードするファイルのタイプを指定します。

transfer download datatype eapdevcert

ステップ 4 次のコマンドを入力して、証明書の秘密キーを指定します。

transfer download certpassword *password*

ステップ 5 次のコマンドを入力して、TFTP または FTP サーバの IP アドレスを指定します。

transfer download serverip *server-ip-address*

ステップ 6 次のコマンドを入力して、ダウンロードする設定ファイルの名前を指定します。

transfer download path *server-path-to-file*

ステップ 7 次のコマンドを入力して、設定ファイルのディレクトリ パスを指定します。

transfer download filename *filename.pem*

ステップ 8 （オプション）TFTP サーバを使用している場合は、次のコマンドを入力します。

- **transfer download tftpMaxRetries retries**
- **transfer download tftpPktTimeout timeout**

（注） 10回の再試行および6秒のタイムアウトというデフォルト値は、調整しなくても適切に機能します。ただし、これらの値は変更できます。値を変更するには、TFTPサーバがソフトウェアのダウンロードを試行する最大回数を*retries*パラメータ、ソフトウェアのダウンロードを試行する時間の合計（秒単位）を*timeout*パラメータに入力します。

ステップ9 FTPサーバを使用している場合は、次のコマンドを入力します（FTPサーバを使用していない場合は、このステップをスキップします）。

- **transfer download username** *username*
- **transfer download password** *password*
- **transfer download port** *port*

（注） portパラメータのデフォルト値は21です。

ステップ10 **transfer download start** コマンドを入力して、更新された設定を表示します。現在の設定を確認してダウンロードプロセスを開始するプロンプトが表示されたら、**y** と答えます。

ステップ11 次のコマンドを入力して、コントローラをリブートします。

reset system

デバイスの証明書のアップロード

デバイスの証明書のアップロード（GUI）

手順

ステップ1 **[Commands]** > **[Upload File]** の順に選択して、[Upload File from Controller] ページを開きます。

ステップ2 [File Type] ドロップダウン リストから、[IPSec Device Certificate] を選択します。

ステップ3 [Transfer Mode] ドロップダウン リストで、次のオプションから選択します。

- **TFTP**
- **FTP**
- **SFTP**

ステップ4 [IP Address] テキスト ボックスに、サーバのIPアドレスを入力します。

ステップ5 [File Path] テキスト ボックスに、証明書のディレクトリ パスを入力します。

ステップ6 [File Name] テキスト ボックスに、証明書の名前を入力します。

ステップ7 FTPサーバを使用している場合は、次の手順に従います（FTPサーバを使用していない場合は、このステップをスキップします）。

a) [Server Login Username] テキスト ボックスに、FTP サーバにログインするためのユーザ名を入力します。
b) [Server Login Password] テキスト ボックスに、FTP サーバにログインするためのパスワードを入力します。
c) [Server Port Number] テキスト ボックスに、ダウンロードが発生する FTP サーバのポート番号を入力します。デフォルト値は 21 です。SFTP のデフォルト値は 22 です。

ステップ 8 [Upload] をクリックして、コントローラから CA 証明書をアップロードします。アップロードのステータスを示すメッセージが表示されます。

ステップ 9 アップロードの完了後、**[Commands]** > **[Reboot]** > **[Reboot]** を選択します。

ステップ 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。

ステップ 11 [OK] をクリックし、変更内容を確定してコントローラをリブートします。

デバイスの証明書のアップロード（CLI）

手順

ステップ 1 コントローラ CLI にログインします。

ステップ 2 次のコマンドを入力して、ダウンロードするファイルのタイプを指定します。

transfer upload datatype ipsecdevcert

ステップ 3 次のコマンドを入力して、設定ファイルのアップロードに使用する転送モードを指定します。

transfer upload mode {**tftp** | **ftp** | **sftp**}

ステップ 4 次のコマンドを入力して、TFTP または FTP サーバの IP アドレスを指定します。

transfer upload serverip *server-ip-address*

ステップ 5 次のコマンドを入力して、ファイルのディレクトリ パスを指定します。

transfer upload path *server-path-to-file*

ステップ 6 次のコマンドを入力して、アップロードするファイルの名前を指定します。

transfer upload filename *filename*

ステップ 7 FTP サーバを使用している場合は、次のコマンドを入力します（FTP サーバを使用していない場合は、このステップをスキップします）。

- **transfer upload username** *username*
- **transfer upload password** *password*
- **transfer upload port** *port*

（注） port パラメータのデフォルト値は 21 です。SFTP のデフォルト値は 22 です。

ステップ 8 **transfer upload start** コマンドを入力して、更新された設定を表示します。現在の設定を確認してアップロード プロセスを開始するプロンプトが表示されたら、y と答えます。

ステップ 9 **reset system** コマンドを入力して、コントローラをリブートします。

CA 証明書のダウンロード

コントローラとアクセス ポイントは、デバイス証明書の署名と検証に使用される、認証局（CA）証明書を備えています。コントローラには、シスコによりインストールされた CA 証明書が付属しています。この証明書は、ローカル EAP 認証時にワイヤレス クライアントの認証を行うために、EAP-FAST（PAC を使用していない場合）、EAP-TLS、PEAP-GTC、および PEAP-MSCHAPv2 により使用できます。ただし、ご自身のベンダー固有の CA 証明書を使用する場合は、証明書をコントローラにダウンロードする必要があります。

（注） ローカル EAP の設定の詳細については、「ローカル EAP の設定」セクションを参照してください。

この項の手順に従って、GUI または CLI のいずれかを介して、CA 証明書をコントローラにダウンロードします。ただし、ダウンロードを開始する前に、証明書のダウンロードに TFTP または FTP サーバを使用できることを確認します。TFTP または FTP サーバをセットアップする場合は、次のガイドラインに従ってください。

- サービス ポート経由でアップグレードする場合、サービス ポートはルーティングできないため、TFTP または FTP サーバはサービス ポートと同じサブネット上になければなりません。あるいは、コントローラ上に静的ルートを作成する必要があります。
- ディストリビューション システム ネットワーク ポートを経由してアップグレードする場合、ディストリビューション システム ポートはルーティング可能なので、TFTP または FTP サーバは同じサブネット上にあっても、別のサブネット上にあってもかまいません。
- Prime Infrastructure 内蔵 TFTP または FTP サーバとサードパーティの TFTP または FTP サーバは同じ通信ポートを使用する必要があるため、サードパーティの TFTP または FTP サーバは Cisco Prime Infrastructure と同じコンピュータ上で実行できません。

（注） コントローラにダウンロードする証明書はすべて、PEM 形式でなければなりません。

CA 証明書のダウンロード（GUI）

手順

ステップ 1 サーバ上のデフォルト ディレクトリに CA 証明書をコピーします。

ステップ 2 **[Commands]** > **[Download File]** を選択して、[Download File to Controller] ページを開きます。

ステップ 3 [File Type] ドロップダウン リストから、[Vendor CA Certificate] を選択します。

ステップ 4 [Transfer Mode] ドロップダウン リストで、次のオプションから選択します。

- **TFTP**
- **FTP**
- SFTP（7.4 以降のリリースで利用可能）

ステップ 5 [IP Address] テキスト ボックスに、サーバの IP アドレスを入力します。

TFTP サーバを使用している場合は、[Maximum Retries] テキスト ボックスの 10 回の再試行および [Timeout] テキスト ボックスの 6 秒というデフォルト値は、調整しなくても適切に機能します。ただし、これらの値は変更できます。

ステップ 6 TFTP サーバが証明書のダウンロードを試行する最大回数を [Maximum Retries] テキスト ボックスに入力し、TFTP サーバが証明書のダウンロードを試行する時間（秒単位）を [Timeout] テキスト ボックスに入力します。

ステップ 7 [File Path] テキスト ボックスに、証明書のディレクトリ パスを入力します。

ステップ 8 [File Name] テキスト ボックスに、証明書の名前を入力します。

ステップ 9 FTP サーバを使用している場合は、次の手順に従います。

a) [Server Login Username] テキスト ボックスに、FTP サーバにログインするためのユーザ名を入力します。

b) [Server Login Password] テキスト ボックスに、FTP サーバにログインするためのパスワードを入力します。

c) [Server Port Number] テキスト ボックスに、ダウンロードが発生する FTP サーバのポート番号を入力します。デフォルト値は 21 です。

ステップ 10 [Download] をクリックして、CA 証明書をコントローラにダウンロードします。ダウンロードのステータスを示すメッセージが表示されます。

ステップ 11 ダウンロードの完了後、**[Commands]** > **[Reboot]** > **[Reboot]** の順に選択します。

ステップ 12 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。

ステップ 13 [OK] をクリックし、変更内容を確定してコントローラをリブートします。

CA 証明書のダウンロード（CLI）

手順

ステップ 1 コントローラ CLI にログインします。

ステップ 2 次のコマンドを入力して、設定ファイルのダウンロードに使用する転送モードを指定します。

transfer download mode {**tftp** | **ftp** | **sftp**}

ステップ 3 次のコマンドを入力して、ダウンロードするファイルのタイプを指定します。

transfer download datatype eapdevcert

ステップ 4 次のコマンドを入力して、TFTP または FTP サーバの IP アドレスを指定します。

transfer download serverip *server-ip-address*

ステップ 5 次のコマンドを入力して、設定ファイルのディレクトリ パスを指定します。

transfer download path *server-path-to-file*

ステップ 6 次のコマンドを入力して、ダウンロードする設定ファイルの名前を指定します。

transfer download filename *filename*

ステップ 7 （オプション）TFTP サーバを使用している場合は、次のコマンドを入力します。

- **transfer download tftpMaxRetries** *retries*
- **transfer download tftpPktTimeout** *timeout*

（注） 10回の再試行および6秒のタイムアウトというデフォルト値は、調整しなくても適切に機能します。ただし、これらの値は変更できます。値を変更するには、TFTPサーバがソフトウェアのダウンロードを試行する最大回数を*retries*パラメータ、ソフトウェアのダウンロードを試行する時間の合計（秒単位）を *timeout* パラメータに入力します。

ステップ 8 FTPサーバを使用している場合は、次のコマンドを入力します（FTPサーバを使用していない場合は、このステップをスキップします）。

- **transfer download username** *username*
- **transfer download password** *password*
- **transfer download port** *port*

（注） port パラメータのデフォルト値は 21 です。

ステップ 9 **transfer download start** コマンドを入力して、更新された設定を表示します。現在の設定を確認してダウンロード プロセスを開始するプロンプトが表示されたら、y と答えます。

ステップ 10 **reset system** コマンドを入力して、コントローラをリブートします。

CA 証明書のアップロード

CA 証明書のアップロード（GUI）

手順

ステップ 1 **[Commands]** > **[Upload File]** の順に選択して、[Upload File from Controller] ページを開きます。

ステップ 2 [File Type] ドロップダウン リストから、[IPSec CA Certificate] を選択します。

ステップ 3 [Transfer Mode] ドロップダウン リストで、次のオプションから選択します。

- **TFTP**
- **FTP**
- **SFTP**

ステップ 4 [IP Address] フィールドにサーバの IP アドレスを入力します。

ステップ 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。

ステップ 6 [File Name] フィールドに、証明書の名前を入力します。

ステップ 7 （オプション）FTP サーバを使用している場合は、次の手順に従います（FTP サーバを使用していない場合は、このステップをスキップします）。

a) [Server Login Username] フィールド、FTP サーバにログオンするためのユーザ名を入力します。

b) [Server Login Password] フィールドに、FTP サーバにログオンするためのパスワードを入力します。

c) [Server Port Number] フィールドに、FTP サーバ上のダウンロードが行われるポート番号を入力します。デフォルト値は 21 です。SFTP のデフォルト値は 22 です。

ステップ 8 [Upload] をクリックして、コントローラから CA 証明書をアップロードします。アップロードのステータスを示すメッセージが表示されます。

ステップ 9 アップロードの完了後、**[Commands]** > **[Reboot]** > **[Reboot]** を選択します。

ステップ 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。

ステップ 11 [OK] をクリックし、変更内容を確定してコントローラをリブートします。

CA 証明書のアップロード（CLI）

手順

ステップ 1 コントローラ CLI にログインします。

ステップ 2 次のコマンドを入力して、ダウンロードするファイルのタイプを指定します。

transfer upload datatype ipseccacert

ステップ 3 次のコマンドを入力して、設定ファイルのアップロードに使用する転送モードを指定します。

transfer upload mode {**tftp** | **ftp** | **sftp**}

ステップ 4 次のコマンドを入力して、TFTP または FTP サーバの IP アドレスを指定します。

transfer upload serverip *server-ip-address*

ステップ 5 次のコマンドを入力して、ファイルのディレクトリ パスを指定します。

transfer upload path *server-path-to-file*

ステップ 6 次のコマンドを入力して、アップロードするファイルの名前を指定します。

transfer upload filename *filename*

ステップ 7 （オプション）FTP サーバを使用している場合は、次のコマンドを入力します（FTP サーバを使用していない場合は、このステップをスキップします）。

- **transfer upload username** *username*
- **transfer upload password** *password*
- **transfer upload port** *port*

（注） port パラメータのデフォルト値は 21 です。SFTP のデフォルト値は 22 です。

ステップ 8 **transfer upload start** コマンドを入力して、更新された設定を表示します。現在の設定を確認してアップロード プロセスを開始するプロンプトが表示されたら、y と答えます。

ステップ 9 **reset system** コマンドを入力して、コントローラをリブートします。

証明書署名要求の生成

このセクションでは、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、およびコントローラにチェーン証明書をダウンロードする方法について説明します。CSR は、次のいずれかの方法を使用して生成できます。

- OpenSSL を使用する
- コントローラ自体を使用する

関連資料

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 [英語] : https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/109597-csr-chained-certificates-wlc-00.html

OpenSSL を使用した証明書署名要求の生成

手順

ステップ 1 OpenSSL のアプリケーションをインストールして開きます。

ステップ 2 次のコマンドを入力します。

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

コントローラ自体で CSR を生成する場合は 2048 ビットのキー サイズが使用されますが、ECDSA の最大キー サイズは 256 ビットです。

（注） 正しい共通名を指定する必要があります。証明書の作成に使用されるホスト名（共通名）が、コントローラの仮想インターフェイス IP に対するドメイン ネーム システム（DNS）のホスト名エントリに一致することを確認します。この名前は、DNS にも存在する必要があります。また、VIP インターフェイスへの変更後には、この変更を反映するためにシステムをリブートする必要があります。

コマンド投入後に、国、州、都市などの情報を入力するように促されます。

以下に類似した情報が表示されます。

```
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>
```

すべての必要な詳細を入力すると、2 つのファイルが生成されます。

- 名前 *mykey.pem* を含む新しい秘密キー

- 名前 *myreq.pem* を含む CSR

ステップ 3 証明書署名要求（CSR）の情報をコピーして CA の登録ツールに貼り付けます。サードパーティ CA に CSR を送信すると、サードパーティ CA は証明書にデジタル署名して、電子メールで署名付き証明書チェーンを返します。チェーン証明書の場合、CA から証明書のチェーン全体を受信します。上記の例のように中間証明書が 1 つのみであれば、CA から次の 3 種類の証明書を受信します。

- ルート証明書（.pem）
- 中間証明書（.pem）
- デバイス証明書（.pem）

（注） 証明書が SHA1 暗号化との Apache 互換であることを確認します。

ステップ 4 3つすべての証明書を取得したら、次の順序で各 .pem ファイルの内容をコピーして別のファイルに貼り付けます。

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

ステップ 5 ファイルを *All-certs.pem* という名前で保存します。

ステップ 6 All-certs.pem 証明書を、CSR ととも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）と組み合わせて、final.pem という名前でファイルを保存します。

ステップ 7 次のコマンドを入力して、All-certs.pem ファイルおよび final.pem ファイルを作成します。

```
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
```

final.pem ファイルをコントローラにダウンロードする必要があります。

（注） **-passin** および **-passout** パラメータのパスワードを入力する必要があります。**-passout** パラメータに対して設定されたパスワードは、コントローラに設定されている certpassword パラメータと一致する必要があります。上記の例では、**-passin** と **-passout** の両方のパラメータに対して設定されるパスワードは check123 です。

次のタスク

CLI または GUI を使用してコントローラに final.pem ファイルをダウンロードします。

シスコ ワイヤレス コントローラを使用した証明書署名要求の生成（GUI）

リリース 8.3 以降では、コントローラ自体でより安全なオプションを使用して CSR が生成されます。

CSR を生成し、生成された証明書をインストールしないと、次のリブート後に HTTPS 経由でコントローラにアクセスできなくなります。これは、リブート後に、コントローラが新たに生成された CSR キーを探すためです。

手順

ステップ 1 **[Security]** > **[Certificate]** > **[CSR]** を選択します。

ステップ 2 [CSR] ページで、次の詳細情報を指定します。

- Certificate Type
- Country Code
- State
- City
- Organization
- Department
- Common Name
- E-mail
- Key Type

ステップ 3 [Generate] をクリックします。

次のタスク

[Commands] > **[Upload File]** に移動して、生成された CSR 証明書ファイルをダウンロードします。

シスコ ワイヤレス コントローラを使用した証明書署名要求の生成（CLI）

リリース 8.3 以降では、コントローラ自体でより安全なオプションを使用して CSR が生成されます。

CSR を生成し、生成された証明書をインストールしないと、次のリブート後に HTTPS 経由でコントローラにアクセスできなくなります。これは、リブート後に、コントローラが新たに生成された CSR キーを探すためです。

手順

- 次のコマンドを入力して、CSR を生成します。

  config certificate generate csr-webauth {**csr-webauth** | **csr-webadmin**} *country state city organization department common-name e-mail*

  コマンドを入力すると、端末に CSR が表示されます。

次のタスク

端末に表示された CSR をコピーして、自分のコンピュータ上のファイルに貼り付ける必要があります。CSR は、サードパーティの署名機関またはエンタープライズ公開キー インフラストラクチャ（PKI）に引き渡す必要があります。

生成されたキーは、次の CSR が生成されるまでコントローラに残ります（以前生成された CSR は上書きされます）。（RMA）の後で、コントローラ ハードウェアを変更した場合は、同じ証明書を再インストールすることはできません。代わりに、新しいコントローラ上で新たに証明書を生成する必要があります。

サードパーティ証明書のダウンロード

サードパーティ証明書のダウンロード（GUI）

手順

ステップ 1 デバイス証明書 final.pem を TFTP サーバのデフォルト ディレクトリにコピーします。

ステップ 2 [Security] > [Web Auth] > [Certificate] を選択して、[Web Authentication Certificate] ページを開きます。

ステップ 3 [Download SSL Certificate] チェックボックスをオンにして、Download SSL Certificate From Server パラメータを表示します。

ステップ 4 [Server IP Address] テキスト ボックスに、TFTP サーバの IP アドレスを入力します。

ステップ 5 [File Path] テキスト ボックスに、証明書のディレクトリ パスを入力します。

ステップ 6 [File Name] テキスト ボックスに、証明書の名前を入力します。

ステップ 7 [Certificate Password] テキスト ボックスに、証明書の保護に使用されたパスワードを入力します。

ステップ 8 [Apply] をクリックします。

ステップ 9 ダウンロードが完了したら、[Commands] > [Reboot] の順に選択して、[Save and Reboot] をクリックします。

ステップ 10 変更を確定してコントローラをリブートするために [OK] をクリックします。

サードパーティ証明書のダウンロード（CLI）

手順

ステップ 1 *final.pem* ファイルを TFTP サーバ上のデフォルトディレクトリに移動します。次のコマンドを入力して、ダウンロードの設定を変更します。

```
(Cisco Controller) > transfer download mode tftp
(Cisco Controller) > transfer download datatype webauthcert
(Cisco Controller) > transfer download serverip <TFTP server IP address>
(Cisco Controller) > transfer download path <absolute TFTP server path to the update
file>
(Cisco Controller) > transfer download filename final.pem
```

ステップ 2 オペレーティング システムが 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。

```
(Cisco Controller) > transfer download certpassword password
```

（注） *certpassword* の値が、CSR を生成する **-passout** パラメータと同じであることを確認します。

ステップ 3 次のコマンドを入力して、証明書およびキーのダウンロードを開始します。

transfer download start

例：

```
(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.
```

ステップ 4 コントローラをリブートします。