# ワイヤレス LAN コントローラのローカルで有効な証明書の設定例

## 目次



## 概要

このドキュメントでは、ローカルで有効な証明書機能を使用するようにワイヤレス LAN コントローラ ( WLC ) と Lightweight アクセス ポイント ( LAP ) を設定する方法について説明します。 この機能は、ワイヤレス LAN コントローラ バージョン 5.2 で導入されました。 この機能を使用すると、公開キー インフラストラクチャ ( PKI ) を制御する場合に、アクセス ポイントとコントローラでローカルで有効な証明書 ( LSC ) を生成できます。 そうすれば、この証明書を使用して WLC と LAP を相互に認証することができます。

## 前提条件

### 要件

この設定を行う前に、次の要件が満たされていることを確認します。

- WLC、LAP、およびワイヤレス クライアント カードの基本動作の設定方法を理解している
- Microsoft Windows 2003 CA サーバを設定して使用する方法を理解している

- 公開キーのインフラストラクチャおよびデジタル証明書に関する知識

## 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 5.2 が稼働している Cisco 4400 シリーズ WLC
- Cisco Aironet 1130 AG シリーズ Lightweight アクセス ポイント（LAP）
- ドメイン コントローラおよび認証局サーバとして設定された Microsoft Windows 2003 サーバ
- ファームウェア リリース 4.2 が稼働する Cisco Aironet 802.11a/b/g クライアント アダプタ
- ファームウェア バージョン 4.2 が稼働する Cisco Aironet Desktop Utility（ADU）

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。

## 表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

# ローカルで有効な証明書

5.2.157.0 より前のコントローラ ソフトウェア リリースでは、コントローラが自己署名証明書（SSC）を使用してアクセス ポイントを認証することも、アクセス ポイントに製造元でインストールされた証明書（MIC）が存在する場合は認可情報を RADIUS サーバに送信することもできます。 コントローラ ソフトウェア リリース 5.2.157.0 以降では、ローカルで有効な証明書（LSC）を使用するようにコントローラを設定できます。 LSC は、セキュリティを強化する、認証局（CA）を制御する、または生成された証明書に関するポリシー、制約事項、および使用方法を定義するために、 独自の公開キー インフラストラクチャ（PKI）が必要な場合に使用できます。

新しい LSC 証明書は、最初に、コントローラにプロビジョニングしてから、認証局（CA）サーバから LAP にプロビジョニングする必要があります。

LAP は CAPWAP プロトコルを使用してコントローラ（WLC）と通信します。 証明書に署名して LAP 用と WLC 用の CA 証明書を発行するための要求を WLC から開始する必要があります。 LAP は直接 CA サーバと通信しません。 WLC は LWAPP の AP に対する CA プロキシとして機能します。 CA サーバの詳細を WLC 上で設定して、到達可能にする必要があります。

コントローラは、Simple Certificate Enrollment Protocol（SCEP）を使用してデバイス上で生成された certReqs を CA に転送してから、再度 SCEP を使用して CA から署名付き証明書を取得します。

SCEP は、公開キー インフラストラクチャ（PKI）クライアントと認証局サーバが証明書の登録と失効に使用する証明書管理プロトコルです。 これは、シスコで広く使用されており、多くの CA サーバでサポートされています。 SCEP プロトコルでは、HTTP が PKI メッセージの転送プロトコルとして使用されます。 SCEP の主な目的は、ネットワーク デバイスに証明書を確実に発行することです。 SCEP はさまざまな操作が可能ですが、このプロジェクトとリリースでは、SCEP が次の操作に使用されます。

- CA と RA の公開キーの配布
- 証明書の登録

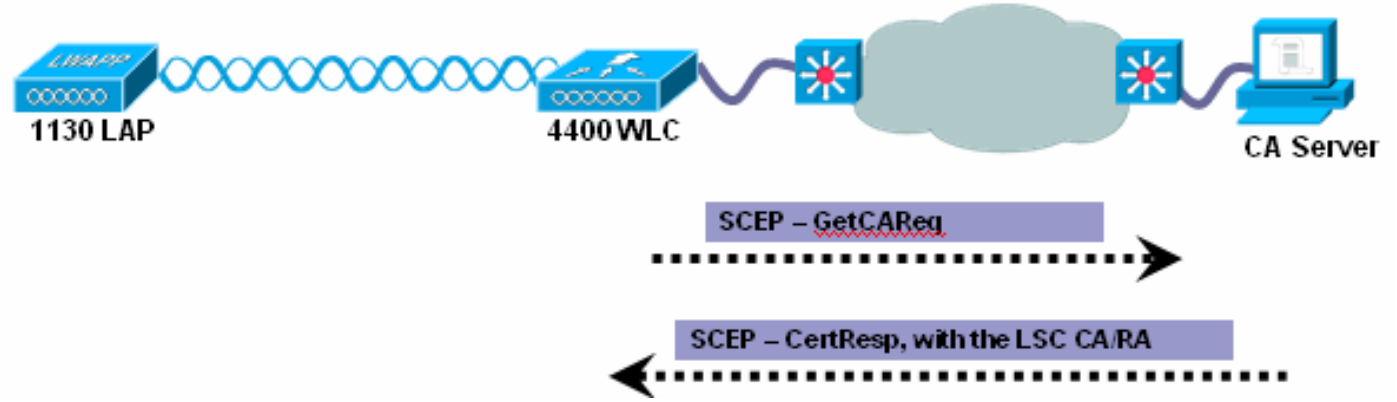
すべての SCEP トランザクションが自動モードで発生します。 証明書の失効はサポートされません。

**注:** LSC は、ブリッジ モードに設定されたアクセス ポイントではサポートされません。

## ワイヤレス LAN コントローラ（WLC）での証明書プロビジョニング

新しい LSC 証明書（CA 証明書とデバイス証明書の両方）をコントローラにインストールする必要があります。

SCEP プロトコルを使用している場合は、CA 証明書が CA サーバから送られてきます。 それ以降は、コントローラ上に証明書が存在しないため、この操作は純粋な取得操作です。 この証明書がコントローラにインストールされます。 この同じ CA 証明書が、LSC を使用してプロビジョニングされた AP にもプッシュされます。




**デバイスの証明書登録操作**

LAP と CA 署名付き証明書を要求するコントローラの両方で、certRequest が PKCS#10 メッセージとして送信されます。 certRequest には、X.509 証明書に追加され、要求者の秘密キーによってデジタル署名されるサブジェクト名、公開キー、およびその他の属性が含まれています。 これらは CA に送信され、certRequest から X.509 証明書に変換される必要があります。

PKCS#10 certRequest を受信した CA には、要求者の ID を認証し、要求が変更されていないことを確認するための追加情報が必要です。 多くの場合、PKCS#10 と他のアプローチ（PKCS#7 など）を使用して、Cert Reqs/Resps の送受信が行われます。

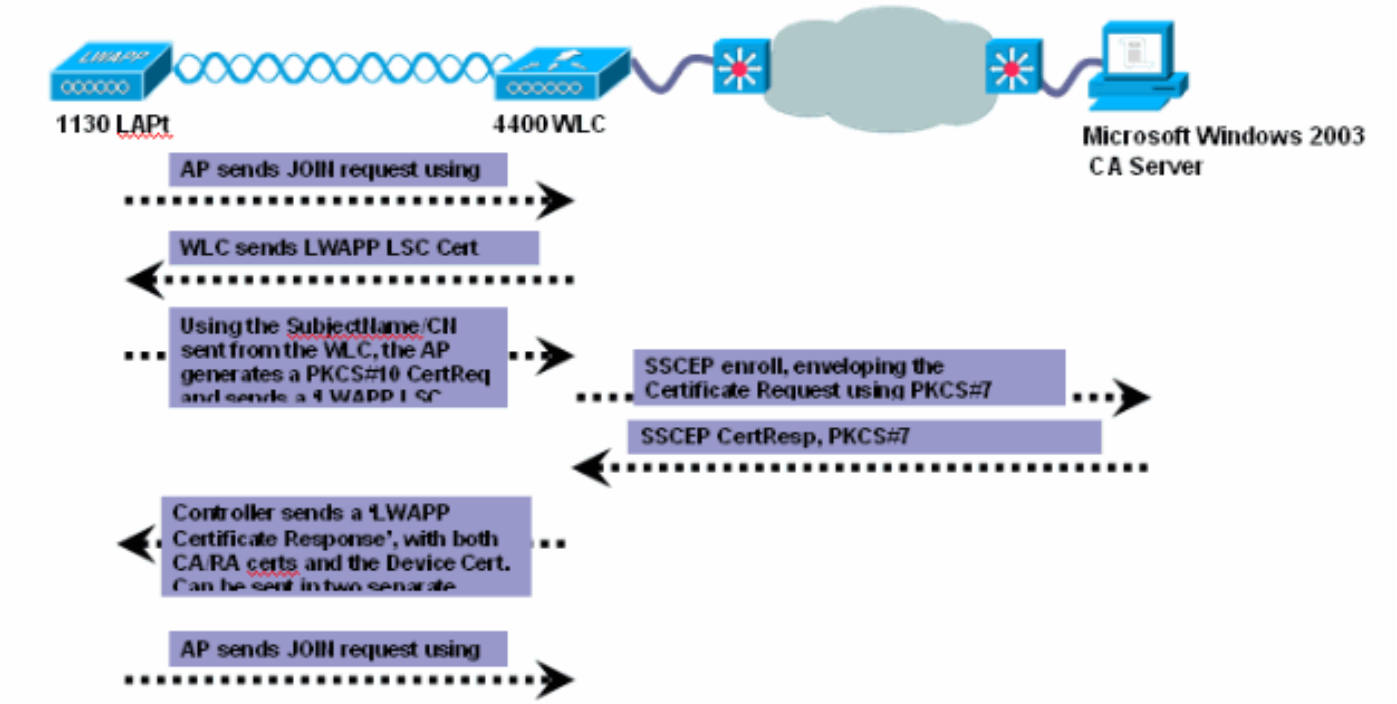
ここで、PKCS#10 が PKCS#7 SignedData メッセージ タイプでラップされます。 これは、SCEP クライアント機能の一部としてサポートされますが、PKCSReq メッセージがコントローラに送信されます。

登録操作が成功すると、CA 証明書とデバイス証明書の両方がコントローラに存在しています。

## LWAPP AP での証明書プロビジョニング

新しい証明書を LAP にプロビジョニングするには、CAPWAP モードの LAP が新しい署名付き X.509 証明書を取得できる必要があります。 これを実現するために、LAP は、CA プロキシとして機能し、CA によって署名された LAP 用の certRequest の取得を支援するコントローラに certRequest を送信します。

certReq と certResponses は LWAPP ペイロードを使用して LAP に送信されます。 次の図に、LAP が LSC をプロビジョニングするフローを示します。




ここで、手順の詳細を示します。

1. より新しい LSC を使用した LAP のプロビジョニングは、LAP が現在の MIC/SSC を使用して WLC を参加させてから、LAP がアップ状態になったときに実行されます。 LSC プロビジョニング フェーズでは、AP がアップ状態であっても、無線が強制的にシャット ダウンされます。
2. LSC の使用とプロビジョニングは WLC で有効にする必要があります。 このプロセスには、LSC の有効化、CA サーバの追加、およびその他のパラメータの設定が含まれます。 ペイロード内にサブジェクト名、有効期間、およびキー サイズが設定された LSC 証明書パラメータ コマンド要求が、コントローラから LAP に送信されます。 これらのフィールドは、LAP によって certRequest の作成時に使用されます。 ペイロードは、LAP が certRequest を作成して、コントローラに送り返す必要があることも示します。
3. LAP が、設定されたキー サイズの公開/秘密 RSA キーのペアを生成します。 キー ペアが生成されると、コントローラから受信された SubjectName の設定後に、certRequest が生成されます。 CN は、既存の SSC/MIC 形式 "Cxxxx-EtherMacAddr" を使用して自動生成されます。 LAP が、PKCS#10 CertReq を生成して、それをペイロード LSC 証明書要求としてコントローラに送信します。
4. コントローラは、SSCEP PKCSReq メッセージ（PKCS#7 形式のメッセージ）を作成して、それを LAP の代わりに CA に送信し、 設定された CA によって署名された証明書要求を取得します。 インストールされている CA/RA 証明書が certReq の暗号化に使用されます。
5. CA が証明書要求を承認できる場合は、Status=SUCCESS になっている CertRep メッセージが PKCS#7 形式で SSCEP クライアント（コントローラ）に送り返されます。 証明書応答が PEM 形式の証明書としてローカルでファイルに書き込まれます。
6. この CertResp は LAP 用のため、WLC はペイロード "Certificate Response" 付きの証明書を LAP に送信します。 最初に、CA 証明書が同じペイロードを使用して送信されてから、デバイス証明書が別のペイロードで送信されます。

LSC CA 証明書と LAP デバイス証明書の両方が LAP にインストールされ、システムが自動リブートします。 次にシステムが起動したときは、LSC を使用するように設定されているため、AP

が参加要求の一部として LSC デバイス証明書をコントローラに送信します。 参加応答の一部として、コントローラが、新しいデバイス証明書を送信すると同時に、新しい CA ルート証明書で受信 LAP 証明書を検証します。

**注:** LSC は、ブリッジ モードに設定されたアクセス ポイントではサポートされません。

## ワイヤレス LAN コントローラ（WLC）と Lightweight アクセス ポイント（LAP）での LSC サポート

LSC は、次の WLC プラットフォームでサポートされます。

- Cisco 4400 シリーズ ワイヤレス LAN コントローラ
- Cisco 2100 シリーズ ワイヤレス LAN コントローラ
- Cisco Catalyst 6500 シリーズ ワイヤレス サービス モジュール（WiSM）
- Cisco Catalyst 3750G 統合ワイヤレス LAN コントローラ
- Cisco ワイヤレス LAN コントローラ モジュール

LSC は、Cisco Aironet C1130、C1140、C1240、C1252 アクセス ポイント、および新しい任意のアクセス ポイントでサポートされます。

ただし、メッシュ AP（1510、1522）とブリッジ モード AP ではサポートされません。

このドキュメントでは、LAP を有効にして、ローカルで有効な証明書を使用して認証する方法と設定例について説明します。

# 設定

**注:** ローカルで有効な証明書機能は、コントローラ上の GUI または CLI を介して有効にすることができます。

**注:** コントローラ上の LSC 機能はパスワードの確認を行いません。 このため、LSC を機能させるには、CA サーバでパスワードの確認を無効にする必要があります。 Microsoft Windows Server 2008 ではパスワードの確認を無効に設定できないため、それを CA サーバとして使用することはできません。

## ネットワーク構成

この例では、ローカルで有効な証明書（LSC）を使用するように 4400 ワイヤレス LAN コントローラと 1130 シリーズ Lightweight アクセス ポイントを設定します。 これを実現するには、認証局（CA）サーバからの LSC を使用してワイヤレス LAN コントローラと LAP をプロビジョニングする必要があります。

このドキュメントでは、CA サーバとして Microsoft Windows 2003 サーバを使用します。

## CA と SCEP のセットアップ プロセス

このドキュメントでは、Microsoft Windows 2003 サーバ上で CA サーバ設定が構成されていることを前提とします。 ここで、CA と SCEP のセットアップ プロセスに関する手順の概要を示します。

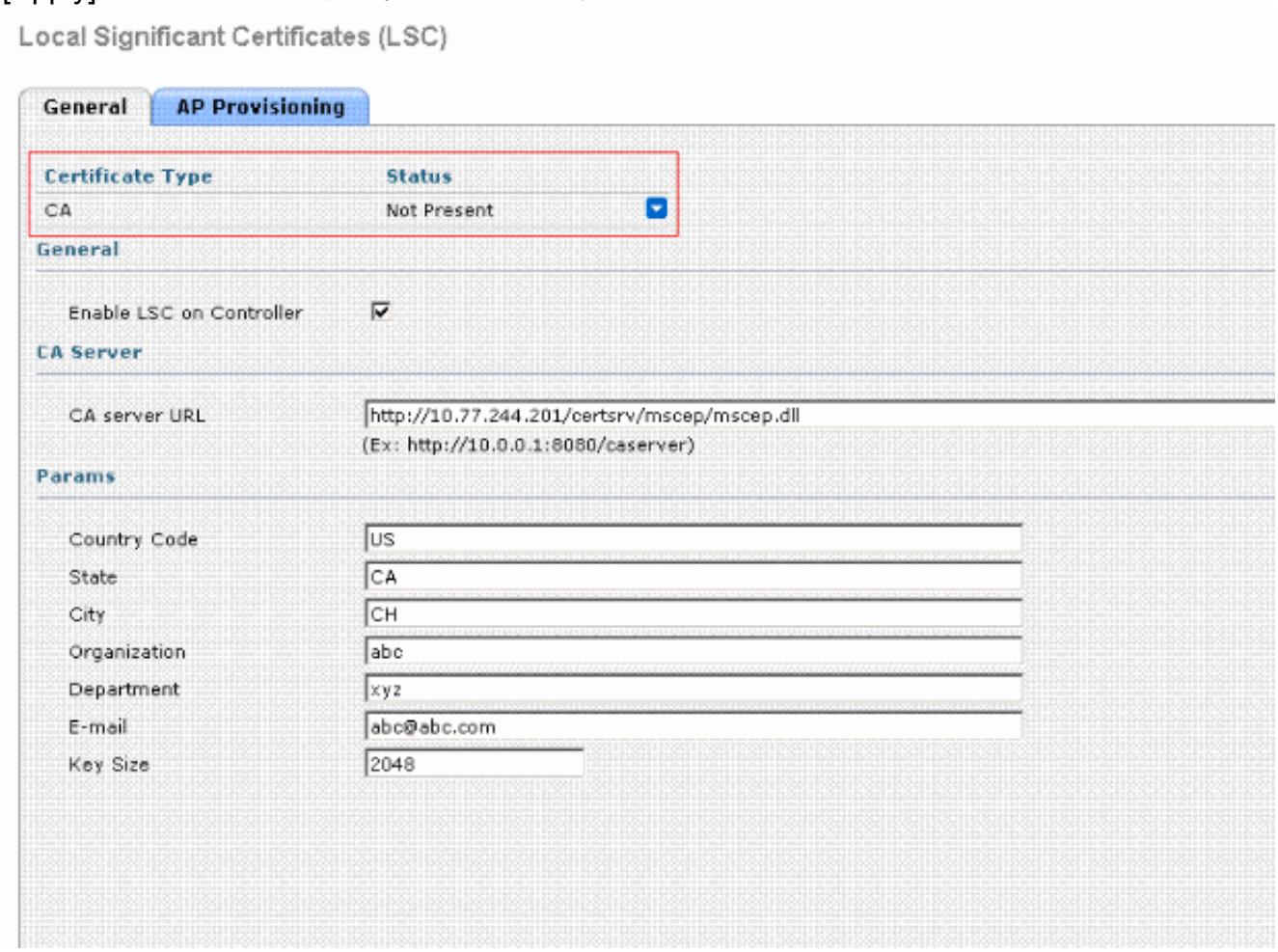
1. Windows 2003 サーバと CA サーバのセットアップ、*http://ca-server/certsrv* の動作の確認
2. Microsoft Web サイトからの *cepsetup.exe* のダウンロード
3. cepsetup.exe のインストール、[RequireSCEP Challenge Phrase] のオフ（この時点で WLC がチャレンジ登録モードをサポートできないため）
4. 名前、電子メール、国、都市などの詳細の指定
5. *http://ca-server/certsrv/mscep/mscep.dll* が想定どおりに動作することの確認

**注:** ユーザ アカウントを作成して、それに IPSec（オフライン要求）テンプレートの読み取り権限と登録権限を割り当て、IIS_WPG グループのメンバーにする必要があります。 詳細については、Microsoft の Web サイトで、『SCEP のインストールと構成』を参照してください。

## GUI 経由のワイヤレス LAN コントローラの設定

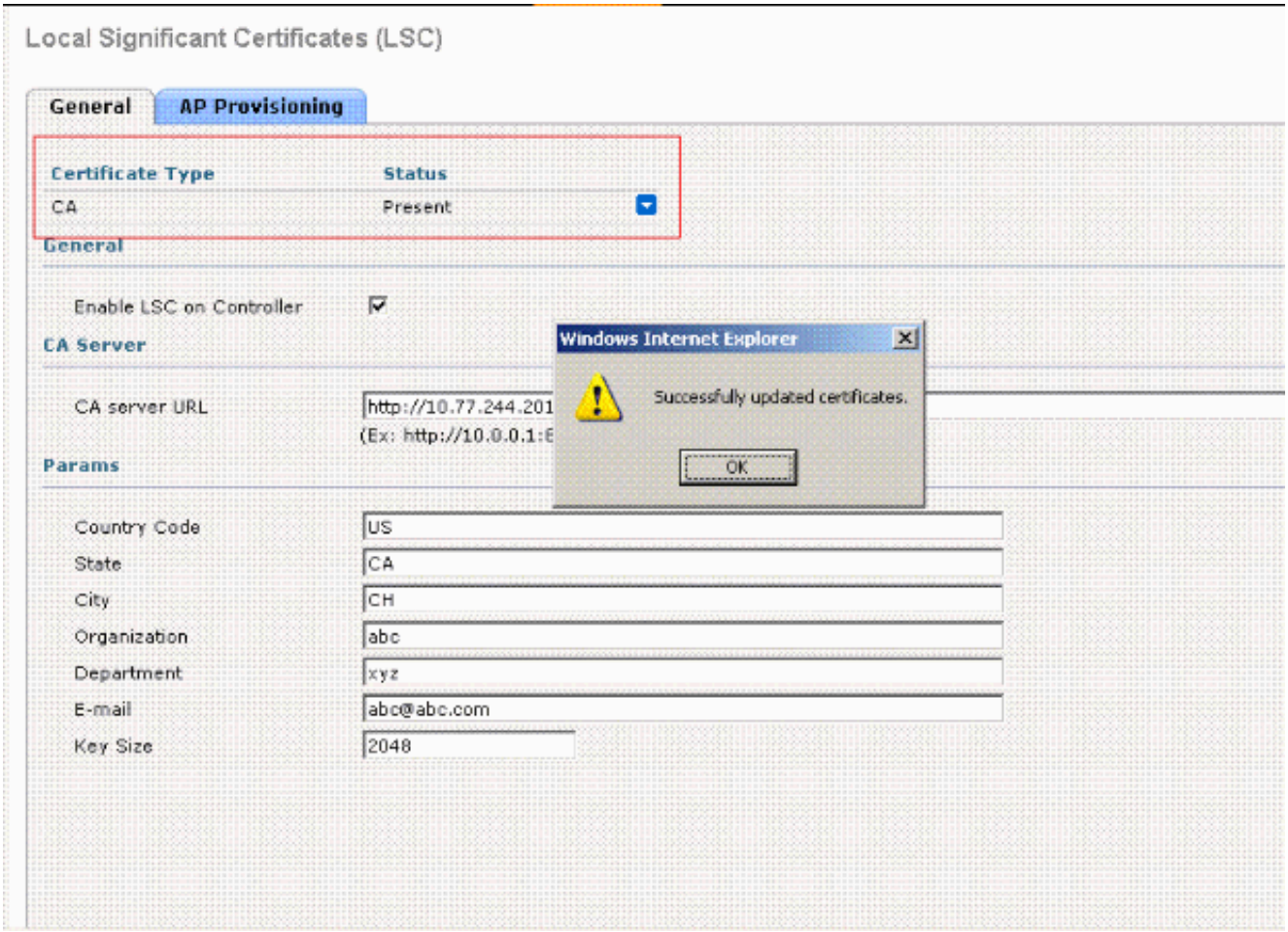
次の手順を実行します。

1. ワイヤレス LAN コントローラの GUI から、[Security] > [Certificate] > [LSC] の順にクリックして、[Local Significant Certificate (LSC)] ページを開きます。
2. [General] タブをクリックします。
3. システム上で LSC を有効にするために、[Enable LSC on Controller] チェック ボックスをオンにします。
4. [CA Server URL] フィールドに、CA サーバへの URL を入力します。 ドメイン名を入力することも IP アドレスを入力することもできます。
5. [Params] フィールドに、デバイス証明書のパラメータを入力します。 キーのサイズは 384 ~ 2048（ビット）の範囲であり、デフォルト値は 2048 です。
6. [Apply] をクリックして、変更を確定します。

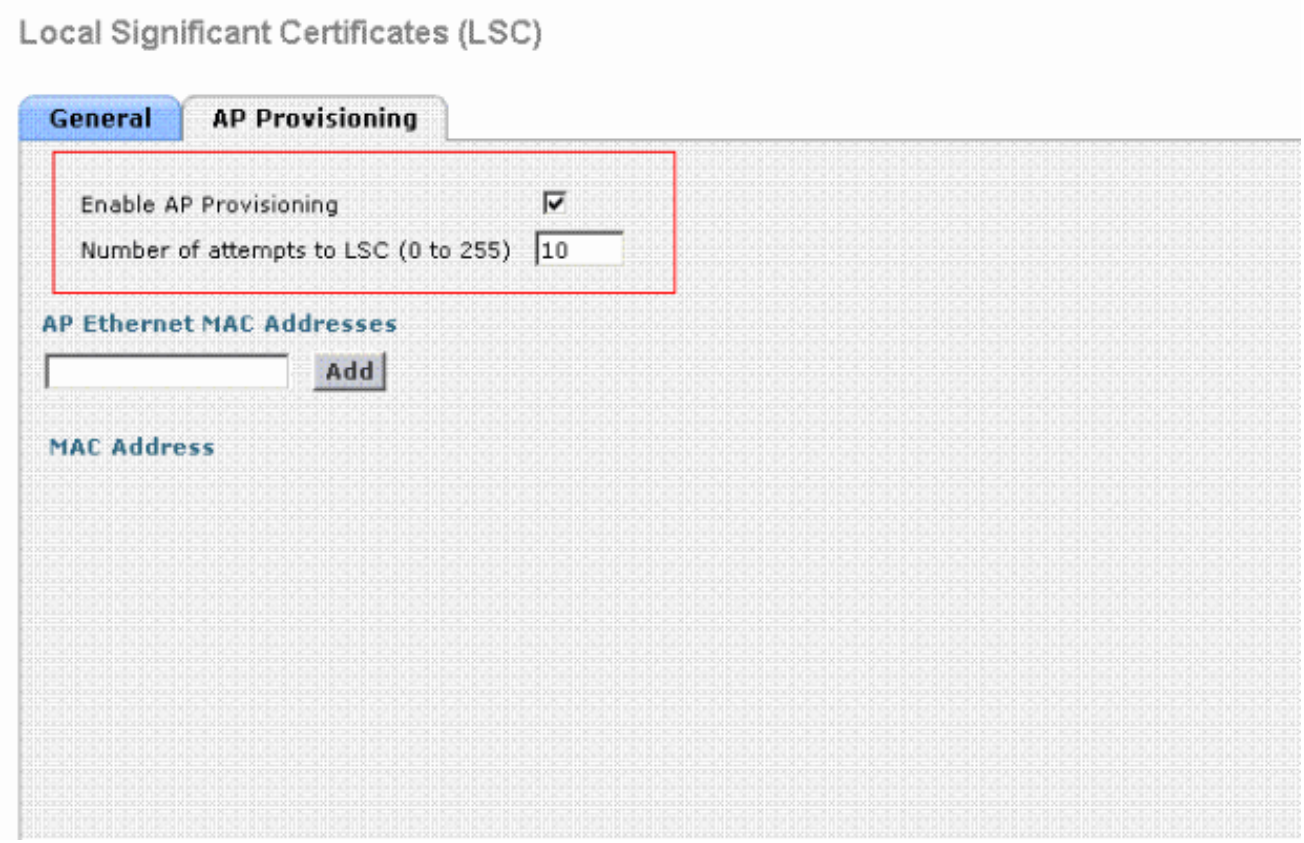



7. コントローラの CA 証明書データベースに CA 証明書を追加するには、証明書タイプの青色

のドロップダウン矢印の上にカーソルを移動して、[Add] を選択します。 次に例を示します。




8. アクセス ポイント上で LSC をプロビジョニングするには、[AP Provisioning] タブをクリックして、[Enable AP Provisioning] チェック ボックスをオンにします。
9. プロビジョン リストにアクセス ポイントを追加するには、[AP Ethernet MAC Addresses] フィールドにアクセス ポイントの MAC アドレスを入力して、[Add] をクリックします。 プロビジョン リストからアクセス ポイントを削除するには、そのアクセス ポイントの青色のドロップダウン矢印の上にカーソルを移動して、[Remove] を選択します。アクセス ポイント プロビジョン リストを設定すると、AP プロビジョニングを有効にした場合に、プロビジョン リスト内のアクセス ポイントのみがプロビジョニングされます。 アクセス ポイント プロビジョン リストを設定しない場合、コントローラに join する MIC または SSC 証明書を持つすべてのアクセス ポイントが LSC でプロビジョニングされます。
10. [Apply] をクリックして、変更を確定します。




## CLI 経由のワイヤレス LAN コントローラの設定

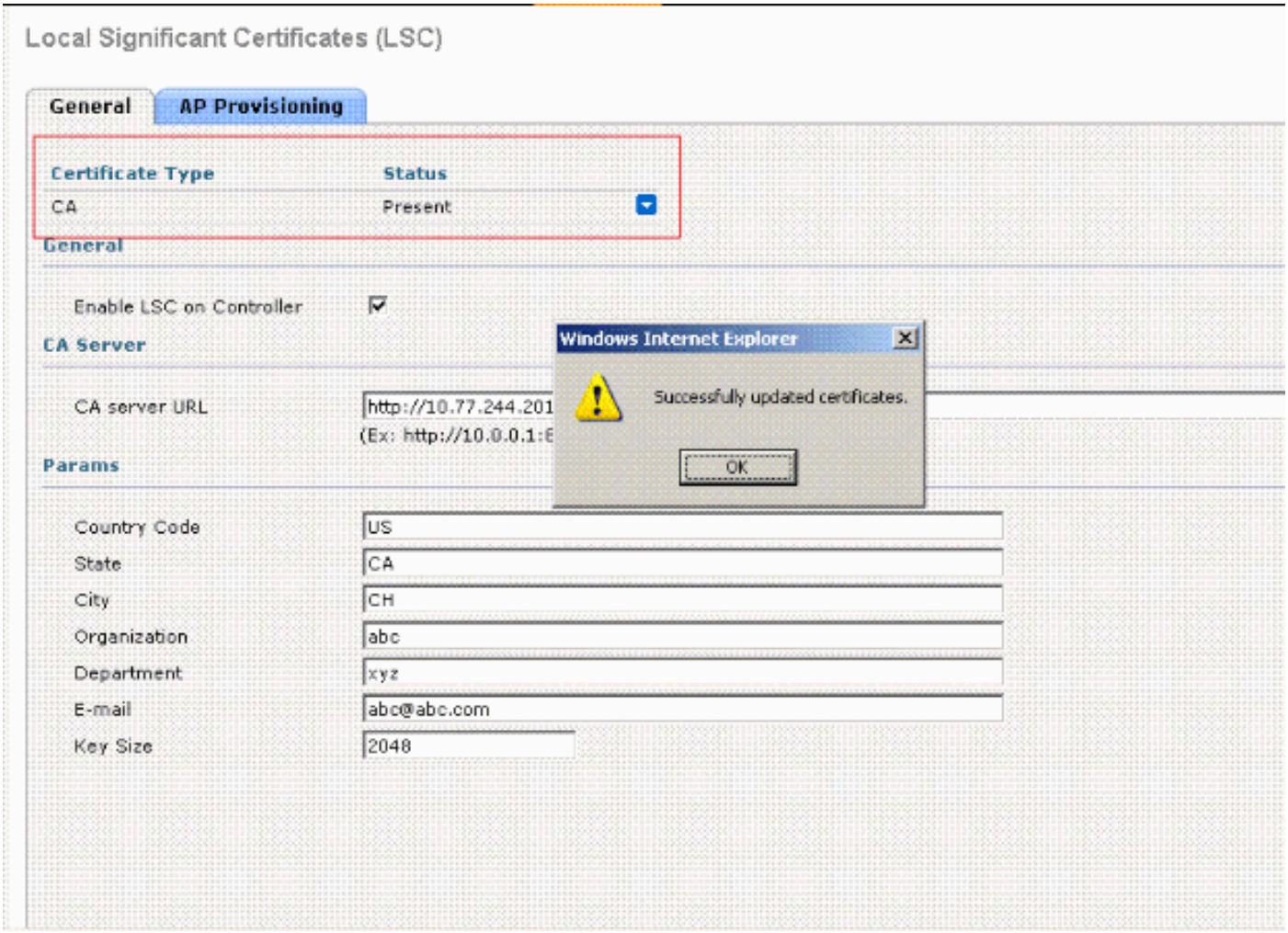
コントローラの CLI からローカルで有効な証明書（LSC）機能を有効にする手順については、『Cisco Wireless LAN Controller コンフィギュレーション ガイド、リリース 5.2』の「**CLI を使用した LSC の設定**」の項を参照してください。

# 確認

ここでは、設定が正常に動作していることを確認します。

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

ワイヤレス LAN コントローラが設定され、CA サーバが設置されたら、ワイヤレス LAN コントローラが SCEP プロトコルを使用して CA サーバと通信し、LSC 証明書を取得します。 ここで、証明書がインストールされた WLC のスクリーンショットを示します。




LAP がアップすると、レイヤ 2/レイヤ 3 検出メカニズムを使用して WLC を検出し、MIC 証明書と一緒に参加要求をコントローラに送信します。

その後で、ワイヤレス LAN コントローラが LSC 証明書パラメータ要求を LAP に送信します。

WLC から送信されたサブジェクト名/CN を使用して、AP が PKCS #10 CertReq を生成し、LWAPP LSC 証明書要求を WLC に送信します。

この要求は WLC によって次の CA サーバに転送されます。 CA サーバが LAP LSC 証明書をコントローラに送信します。 その後で、コントローラが LSC を LAP に送信します。

このメッセージが AP CLI に表示されます。

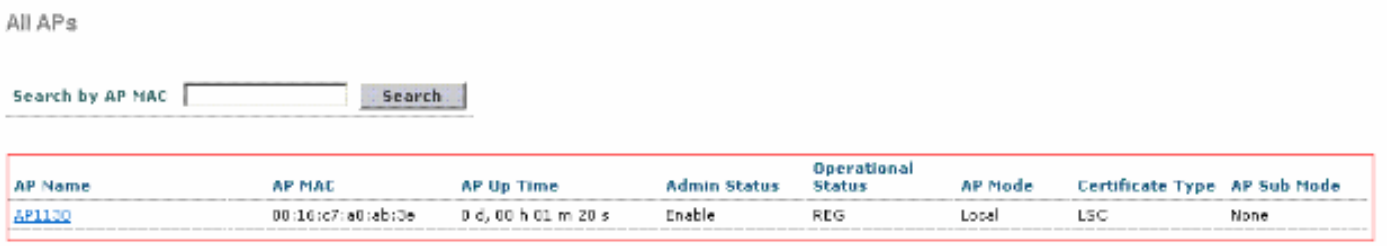
```
The name for the keys will be: Cisco_IOS_LSC_Keys

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]
LSC CA cert successfully imported
LSC device cert successfully imported
```

最後に、LAP が LSC への参加要求を送信します。

このイベントのシーケンスを表示するには、**debug capwap events enable コマンド**を発行します。

LAP が LSC を使用して WLC に登録したら、それを WLC GUI で確認することができます。




WLC CLI から次のコマンドを使用して、これを確認することもできます。 次に例を示します。

```
show certificate lsc summary Information similar to the following appears: LSC
Enabled..................................... Yes LSC CA-
Server...................................... http://10.77.244.201:8080/caserver LSC AP-
Provisioning................................ Yes Provision-
List............................... Not Configured LSC Revert Count in AP
reboots.................. 3 LSC Params: Country..................................... 4
State....................................... ca
City........................................ ch
Orgn........................................ abc
Dept........................................ xyz
Email....................................... abc@abc.com
KeySize..................................... 2048 LSC Certs: CA
Cert........................................ Not Configured RA
Cert..................................... Not Configured
```

LSC を使用してプロビジョニングされたアクセス ポイントの詳細を表示するには、次のコマンドを入力します。

```
show certificate lsc ap-provision Information similar to the following appears: LSC AP-
Provisioning.......................... Yes Provision-List.............................
Present Idx Mac Address --- ------------ 1 00:18:74:c7:c0:90
```

## トラブルシューティング

ここでは、設定のトラブルシューティング方法について説明します。 **debug pm pki scep enable コマンド**を使用すれば、イベントのシーケンスを表示できます。

ここで、正常なデバッグ ログの例を示します。

```
Success log:

WLC

(Cisco Controller) >

scep: waiting for 10 secsmLscScepTask: Nov 23 06:52:21.455:
scep: : Nov 23 06:52:27.519:

===== SCEP_OPERATION_GETCAPS =====
scep: Failed to get SCEP Capabilities from CA. Some CA's do not support this.
scep: Getting CA Certificate(s).
scep: : Nov 23 06:52:27.519:

===== SCEP_OPERATION_GETCA =====
scep: requesting CA certificate

scep: Sent 82 byteseded: Operation now in progress*emWeb: Nov 23 06:52:27.526:
scep: Http response is <HTTP/1.1 200 OK>
```

```
scep: Server returned status code 200.
scep: header info: <Connection: close>
scep: header info: <Date: Wed, 23 Nov 2011 06:52:30 GMT>
scep: header info: <Server: Microsoft-IIS/6.0>
scep: header info: <Content-Length: 3795>
scep: header info: <Content-Type: application/x-x509-ca-ra-cert>
scep: MIME header: application/x-x509-ca-ra-cert
scep: found certificate:
  subject: /DC=com/DC=ccie/CN=AD
  issuer: /DC=com/DC=ccie/CN=AD
  usage: Digital Signature, Certificate Sign, CRL Sign
scep: found certificate:
  subject: /C=CN/ST=BJ/L=BJ/O=Cisco/OU=BN/CN=tls/emailAddress=tls@ccie.com
  issuer: /DC=com/DC=ccie/CN=AD
  usage: Key Encipherment
scep: found certificate:
  subject: /C=CN/ST=BJ/L=BJ/O=Cisco/OU=BN/CN=tls/emailAddress=tls@ccie.com
  issuer: /DC=com/DC=ccie/CN=AD
  usage: Digital Signature
scep: CA cert retrieved with fingerprint 639993FF7FF8FB12EF2FB09DEC7C5BED

scep: waiting for 10 secs 06:52:34.463:

AP
(Cisco Controller) >
scep: waiting for 10 secsmLscScepTask: Nov 23 06:52:47.471:
scep: waiting for 10 secs 06:53:00.479:
scep: AP MAC: 58:bc:27:13:4a:d0 Starting new enrollment request.
scep: creating inner PKCS#7:01.542:
scep: data payload size: 797 bytes:
scep: successfully encrypted payload
scep: envelope size: 1094 bytes545:
scep: Sender Nonce before send: 089AC8C4604FCEB10C1F30E045073B10
scep: creating outer PKCS#7:01.545:
scep: signature added successfully:
scep: adding signed attributes.545:
scep: adding string attribute transId
scep: adding string attribute messageType
scep: adding octet attribute senderNonce
scep: PKCS#7 data written successfully
scep: applying base64 encoding.565:
scep: base64 encoded payload size: 3401 bytes

scep: Sent 3646 bytesed: Operation now in progress*sshpmLscTask: Nov 23 06:53:01.613:
scep: SenderNonce in reply: BF4EE64D4169584D90B2502ECCC0C133
scep: recipientNonce in reply: 089AC8C4604FCEB10C1F30E045073B10
scep: Http response is <HTTP/1.1 200 OK>
scep: Server returned status code 200.:
scep: header info: <Connection: close>:
scep: header info: <Date: Wed, 23 Nov 2011 06:53:02 GMT>
scep: header info: <Server: Microsoft-IIS/6.0>
scep: header info: <Content-Length: 2549>
scep: header info: <Content-Type: application/x-pki-message>
scep: MIME header: application/x-pki-message

scep: reading outer PKCS#706:53:13.488:
scep: PKCS#7 payload size: 2549 bytes8:
scep: PKCS#7 contains 2023 bytes of enveloped data
scep: verifying signature 06:53:13.489:
scep: signature ok Nov 23 06:53:13.490:
scep: finding signed attributes:13.490:
scep: finding attribute transId:13.490:
scep: allocating 32 bytes for attribute.
scep: reply transaction id: A984A2DFE20DA7E0FE702DC8EC307F33
```

scep: finding attribute messageType490:
scep: allocating 1 bytes for attribute.
scep: reply message type is good13.490:
scep: finding attribute senderNonce490:
scep: allocating 16 bytes for attribute.
scep: finding attribute recipientNonce:
scep: allocating 16 bytes for attribute.
scep: finding attribute pkiStatus3.491:
scep: allocating 1 bytes for attribute.
scep: pkistatus: **SUCCESS3** 06:53:13.491: scep: reading inner PKCS#706:53:13.491: scep: decrypting inner PKCS#753:13.492: scep: **found certificate:** subject: /serialNumber= PID:AIR-LAP1262N-A-K9 SN:FTX1433K60R/C=CN/ST=BJ/L=BJ/O=Cisco/OU=BN/CN=AP3G1-f866f267577e/emailAddress= tls@ccie.com issuer: /DC=com/DC=ccie/CN=AD scep: PKCS#7 payload size: 1580 bytes:53:13.518: Digital Signature, Key Encipherment scep: waiting for 10 secs 06:53:13.520:

次に、失敗した場合の例を示します。

Fail log
WLC
(Cisco Controller) >debug pm pki scep detail enable
scep: waiting for 10 secsmLscScepTask: Nov 23 00:57:52.407:
scep: waiting for 10 secs 00:58:05.415:
scep: waiting for 10 secs 00:58:18.423:
scep: waiting for 10 secs 00:58:31.431:
scep: waiting for 10 secs 00:58:44.439:
scep: waiting for 10 secs 00:58:57.447:
scep: waiting for 10 secs 00:59:10.455:
scep: : Nov 23 00:59:22.479:
===== SCEP_OPERATION_GETCAPS =====
scep: Failed to get SCEP Capabilities from CA. Some CA's do not support this.
scep: Getting CA Certificate(s).
scep: : Nov 23 00:59:22.479:
===== SCEP_OPERATION_GETCA =====
scep: requesting CA certificate

scep: Sent 82 byteseded: Operation now in progress*emWeb: Nov 23 00:59:22.486:
scep: Http response is <HTTP/1.1 200 OK>
scep: Server returned status code 200.
scep: header info: <Connection: close>
scep: header info: <Date: Wed, 23 Nov 2011 00:59:22 GMT>
scep: header info: <Server: Microsoft-IIS/6.0>
scep: header info: <Content-Length: 3795>
scep: header info: <Content-Type: application/x-x509-ca-ra-cert>
scep: MIME header: application/x-x509-ca-ra-cert
scep: found certificate:
  subject: /DC=com/DC=ccie/CN=AD
  issuer: /DC=com/DC=ccie/CN=AD
  usage: Digital Signature, Certificate Sign, CRL Sign
scep: found certificate:
  subject: /C=CN/ST=BJ/L=BJ/O=Cisco/OU=BN/CN=tls/emailAddress=tls@ccie.com
  issuer: /DC=com/DC=ccie/CN=AD
  usage: Key Encipherment
scep: found certificate:
  subject: /C=CN/ST=BJ/L=BJ/O=Cisco/OU=BN/CN=tls/emailAddress=tls@ccie.com
  issuer: /DC=com/DC=ccie/CN=AD
  usage: Digital Signature
scep: CA cert retrieved with fingerprint 639993FF7FF8FB12EF2FB09DEC7C5BED

scep: waiting for 10 secs 00:59:23.463:

AP:
(Cisco Controller) >debug pm pki scep detail enable
scep: waiting for 10 secsmLscScepTask: Nov 22 18:06:22.100:
scep: waiting for 10 secs 18:06:35.108:

```
scep: waiting for 10 secs 18:06:48.116:
scep: waiting for 10 secs 18:07:01.124:
scep: AP MAC: 58:bc:27:13:4a:d0 Starting new enrollment request.
scep: creating inner PKCS#7:04.631:
scep: data payload size: 536 bytes:
scep: successfully encrypted payload
scep: envelope size: 838 bytes.633:
scep: Sender Nonce before send: F8BBA9EB06579188A62635A1DFA6510A
scep: creating outer PKCS#7:04.634:
scep: signature added successfully:
scep: adding signed attributes.634:
scep: adding string attribute transId
scep: adding string attribute messageType
scep: adding octet attribute senderNonce
scep: PKCS#7 data written successfully
scep: applying base64 encoding.655:
scep: base64 encoded payload size: 3055 bytes

scep: Sent 3280 bytesed: Operation now in progress*sshpmLscTask: Nov 22 18:07:04.690:
scep: SenderNonce in reply: 69A4BF610ED41746B1066B5BEC4427F0
scep: recipientNonce in reply: F8BBA9EB06579188A62635A1DFA6510A
scep: Http response is <HTTP/1.1 200 OK>
scep: Server returned status code 200.:
scep: header info: <Connection: close>:
scep: header info: <Date: Tue, 22 Nov 2011 18:07:04 GMT>
scep: header info: <Server: Microsoft-IIS/6.0>
scep: header info: <Content-Length: 540>
scep: header info: <Content-Type: application/x-pki-message>
scep: MIME header: application/x-pki-message

scep: reading outer PKCS#718:07:14.133:
scep: PKCS#7 payload size: 540 bytes33:
scep: PKCS#7 contains 1 bytes of enveloped data
scep: verifying signature 18:07:14.134:
scep: signature ok Nov 22 18:07:14.135:
scep: finding signed attributes:14.135:
scep: finding attribute transId:14.135:
scep: allocating 32 bytes for attribute.
scep: reply transaction id: 3DA1646840CD4FFEB1534EA8F1D45F76
scep: finding attribute messageType135:
scep: allocating 1 bytes for attribute.
scep: reply message type is good14.135:
scep: finding attribute senderNonce135:
scep: allocating 16 bytes for attribute.
scep: finding attribute recipientNonce:
scep: allocating 16 bytes for attribute.
scep: finding attribute pkiStatus4.136:
scep: allocating 1 bytes for attribute.
scep: pkistatus: FAILURE2 18:07:14.136:
scep: finding attribute failInfo14.136: scep: allocating 1 bytes for attribute. scep: reason:
Transaction not permitted or supported scep: waiting for 10 secs 18:07:14.136: scep: waiting for
10 secs 18:07:27.144: scep: waiting for 10 secs 18:07:40.152: scep: waiting for 10 secs
18:07:53.160: scep: waiting for 10 secs 18:08:06.168: scep: waiting for 10 secs 18:08:19.176:
scep: waiting for 10 secs 18:08:32.184: scep: waiting for 10 secs 18:08:45.192: scep: waiting
for 10 secs 18:08:58.200: scep: waiting for 10 secs 18:09:11.208:
```

## 関連情報

- Cisco ワイヤレス LAN コントローラ コンフィギュレーション ガイド、リリース 5.2
- WLAN コントローラ（WLC）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
- サードパーティ証明書の証明書署名要求生成とチェーン証明書を WLC にアップロードする

ための手順

- ワイヤレスに関するサポート ページ
- テクニカルサポートとドキュメント - Cisco Systems