ローカルで有効な証明書

ローカルで有効な証明書 （LSC）について

このモジュールでは、ローカルで有効な証明書（LSC）を使用するように Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラおよび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。LSC を使用する公開キーインフラストラクチャ（PKI）を選択した場合は、AP と組み込みワイヤレスコントローラで LSC を生成でき、証明書を使用して組み込みワイヤレスコントローラと AP を手動で認証できます。

シスコ 組み込みワイヤレスコントローラでは、LSC を使用するように組み込みワイヤレスコントローラを設定できます。独自の PKI でセキュリティを強化して認証局（CA）を管理し、生成された証明書でポリシー、制約事項、および使用方法を定義する場合は、LSC を使用します。

組み込みワイヤレスコントローラで新しい LSC 証明書をプロビジョニングし、CA サーバーから Lightweight アクセスポイント（LAP）を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組み込みワイヤレスコントローラと通信します。証明書への署名と、LAP および組み込みワイヤレスコントローラ自体の CA 証明書の発行についての要求は、組み込みワイヤレスコントローラから開始する必要があります。LAP は CA サーバーと直接通信しません。CA サーバーの詳細が組み込みワイヤレスコントローラで設定されていて、アクセス可能である必要があります。

組み込みワイヤレスコントローラは、デバイス上で生成された certReqs を CA に転送するために Simple Certificate Enrollment Protocol（SCEP）を使用し、CA から署名済み証明書を取得するために SCEP を再度使用します。

SCEP は、証明書の登録と失効をサポートするために PKI クライアントと CA サーバーで使用される証明書管理プロトコルです。SCEP はシスコで広く使用され、多くの CA サーバーでサポートされています。SCEP では、HTTP は PKI メッセージのトランスポート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安全に発行することです。SCEP は多くの操作に対応していますが、このリリースでは次の操作に使用されています。

- CA およびルータアドバタイズメント（RA）公開キーの配布
- 認証登録

コントローラ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 を使用する場合、CA 証明書は CA サーバーから受け取ります。この時点では、コントローラに証明書は存在しません。CA 証明書は get 操作で取得後、コントローラにインストールされます。AP が LSC でプロビジョニングされるときに、同じ CA 証明書が AP にもプッシュされます。

製造元でインストールされる証明書の期限切れの防止

製造元でインストールされる証明書（MIC）の期限切れによる失敗を防ぐには、次に示すようにポリシーを設定してください。

- 証明書マップを作成し、ルールを追加します。

```
configure terminal
crypto pki certificate map map1 1
issuer-name co Cisco Manufacturing CA
```

注 同じマップの下に、複数のルールとフィルタを追加できます。前述の例に記載されているルールでは、発行者名に Cisco Manufacturing CA（大文字と小文字を区別しない）が含まれているすべての証明書がこのマップの下で選択されることが指定されています。

- Trustpool ポリシーの下で証明書マップを使用します。

```
configure terminal
crypto pki trustpool policy
match certificate map1 allow expired-certificate
```

デバイスの証明書の登録操作

CA 署名付き証明書を要求する LAP とコントローラの両方に対して、certRequest が PKCS#10 メッセージとして送信されます。certRequest には、X.509 証明書に含まれる件名、公開キー、およびその他の属性が含まれています。また、要求者の秘密キーでデジタル署名される必要があります。これらは CA に送信され、そこで certRequest が X.509 証明書に変換されます。

PKCS#10 certRequest を受け取る 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（証明書の要求や応答を送受信するために、PKCS#10 は PKCS#7 などの他のアプローチと組み合わされることがあります）。

PKCS#10 は PKCS#7 Signed Data 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、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で使用可能になります。

Lightweight アクセス ポイントでの証明書プロビジョニング

LAP で新しい証明書をプロビジョニングするには、CAPWAP モードの間に 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。そのために、LAP はコントローラに certRequest を送信します。コントローラは CA プロキシとして機能し、CA により署名された LAP 用の certRequest を取得を支援します。

certReq および certResponse は LWAPP ペイロードを使用して LAP に送信されます。

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、システムが自動的に再起動します。システムは、次回起動時には LSC を使用するように設定されているため、AP は join 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。join 応答の一部として、コントローラは新しいデバイス証明書を送信し、新しい CA ルート証明書を使用して受信 LAP 証明書も検証します。

（注） LSC は、コントローラとすべての Cisco Aironet アクセスポイントでサポートされています。

LSC ワークフローは、FIPS + WLANCC モードでは異なります。CA サーバーは EST プロトコルをサポートし、FIPS + WLANCC モードで EC 証明書を発行できる必要があります。

また、LSC はコントローラで有効になっています（GUI および CLI）。

次の作業

コントローラおよび AP の既存の PKI インフラストラクチャを使用して証明書の登録を設定、許可、および管理するには、LSC プロビジョニング機能を使用する必要があります。

ローカルで有効な証明書のプロビジョニング

PKI トラストポイントの RSA キーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**crypto key generate rsa** [**exportable**] **general-keys modulus** *key_size* **label** *RSA_key* 例： `デバイス(config)# crypto key generate rsa exportable general-keys modulus 2048 label ewlc-tp1`	PKI トラストポイントの RSA キーを設定します。 **exportable** はオプションのキーワードです。エクスポート可能なキーの設定は任意です。選択すると、必要に応じて、ボックスから出してキーをエクスポートできます。 • key_size：キー係数のサイズ。有効な範囲は 2048 ～ 4096 です。 • RSA_key：RSA キーペアのラベル。
ステップ 3	**end** 例： `デバイス(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

PKI トラストポイントパラメータの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**crypto pki trustpoint** *trustpoint_name* 例： `デバイス(config)# crypto pki trustpoint microsoft-ca`	外部CAサーバーの新しいトラストポイントを作成します。*trustpoint_name* はトラストポイント名を指します。
ステップ 3	**enrollment url** *HTTP_URL* 例： `デバイス(ca-trustpoint)# enrollment url http://CA_server/certsrv/mscep/mscep.dll`	ルータが証明書要求を送信する CA の URL を指定します。 url url：ルータが証明書要求を送信するファイルシステムの URL。URL 内の IPv6 アドレスは括弧で囲む必要があります。たとえば、http://[2001:DB8:1:1::1]:80 です。登録方式オプションの詳細については、「enrollment url (ca-trustpoint)」コマンド ページを参照してください。
ステップ 4	**subject-name** *subject_name* 例： `デバイス(ca-trustpoint)# subject-name C=IN, ST=KA, L=Bengaluru, O=Cisco, CN=eagle-eye/emailAddress=support@abc.com`	トラストポイントの件名パラメータを作成します。
ステップ 5	**rsakeypair** *RSA_key key_size* 例： `デバイス(ca-trustpoint)# rsakeypair ewlc-tp1`	RSA キーをトラストポイントの RSA キーにマッピングします。 • RSA_key：RSA キーペアのラベル。 • key_size：署名キーの長さ。範囲は 360 ～ 4096 です。
ステップ 6	**revocation** {**crl** | **none** | **ocsp**} 例： `デバイス(ca-trustpoint)# revocation none`	失効を確認します。
ステップ 7	**end** 例： `デバイス(ca-trustpoint)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

PKI トラストポイントの認証と登録（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[PKI Management]** を選択します。

ステップ 2 [PKI Management] ウィンドウで、[Trustpoints] タブをクリックします。

ステップ 3 [Add Trustpoint] ダイアログボックスで、次の情報を入力します。

a) [Label] フィールドに、RSA キーラベルを入力します。
b) [Enrollment URL] フィールドに、登録 URL を入力します。
c) [Authenticate] チェックボックスをオンにして、登録 URL の公開証明書を認証します。
d) [Subject Name] セクションで、[Country Code]、[State]、[Location]、[Organisation]、[Domain Name]、および [Email Address] を入力します。
e) [Key Generated] チェック ボックスをオンにして、使用可能な RSA キーペアを表示します。[Available RSA Keypairs] ドロップダウンリストからオプションを選択します。
f) [Enroll Trustpoint] チェックボックスをオンにします。
g) [Password] フィールドにパスワードを入力します。
h) [Re-Enter Password] フィールドで、パスワードを確認します。
i) [Apply to Device] をクリックします。

新しいトラストポイントがトラストポイント名リストに追加されます。

CA サーバーを使用した PKI トラストポイントの認証と登録（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**crypto pki authenticate** *trustpoint_name* 例： `デバイス(config)# crypto pki authenticate microsoft-ca`	CA 証明書を取得します。
ステップ 3	**yes** 例： `デバイス(config)# % Do you accept this certificate? [yes/no]: yes Trustpoint CA certificate accepted.`	

	コマンドまたはアクション	目的
ステップ 4	**crypto pki enroll** *trustpoint_name* 例： デバイス(config)# **crypto pki enroll microsoft-ca** **%** **% Start certificate enrollment ..** **% Create a challenge password. You will need to verbally provide this password to the CA Administrator in order to revoke your certificate.** **For security reasons your password will not be saved in the configuration.** **Please make a note of it.**	クライアント証明書を登録します。
ステップ 5	**password** 例： デバイス(config)# **abcd123**	CA サーバーへのチャレンジパスワードを入力します。
ステップ 6	**password** 例： デバイス(config)# **abcd123**	CA サーバーへのチャレンジパスワードを再入力します。
ステップ 7	**yes** 例： デバイス(config)# **% Include the router serial number in the subject name? [yes/no]: yes**	
ステップ 8	**no** 例： デバイス(config)# **% Include an IP address in the subject name? [no]: no**	
ステップ 9	**yes** 例： デバイス(config)# **Request certificate from CA? [yes/no]: yes** **% Certificate request sent to Certificate Authority** **% The 'show crypto pki certificate verbose client' commandwill show the fingerprint.**	
ステップ 10	**end** 例：	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コ

	コマンドまたはアクション	目的
	デバイス(config)# **end**	ンフィギュレーションモードを終了できます。

LSC 証明書による AP の接続試行回数の設定（GUI）

手順

ステップ 1 [Configuration] > [Wireless] > [Access Points] > > の順に選択します。
ステップ 2 [All Access Points] ウィンドウで LSC プロビジョンの名前をクリックします。
ステップ 3 [Status] ドロップダウンリストから、LSC を有効にするステータスを選択します。
ステップ 4 [Trustpoint Name] ドロップダウンリストからトラストポイントを選択します。
ステップ 5 [Number of Join Attempts] フィールドに、許可される再試行回数を入力します。
ステップ 6 [Apply] をクリックします。

LSC 証明書による AP の接続試行回数の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap lsc-provision join-attempt** *number_of_attempts* 例： デバイス(config)# **ap lsc-provision join-attempt 10**	新たにプロビジョニングされた LSC 証明書を使用した AP の接続失敗の最大試行回数を指定します。 AP の接続回数が指定の制限を超えると、AP は製造元でインストールされる証明書（MIC）を使用して再接続します。
ステップ 3	**end** 例： デバイス(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

LSC 証明書の件名パラメータの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap lsc-provision subject-name-parameter country** *country-str* **state** *state-str* **city** *city-str* **domain** *domain-str* **org** *org-str* **email-address** *email-addr-str* 例： `デバイス(config)# ap lsc-provision subject-name-parameter country India state Karnataka city Bangalore domain domain1 org Right email-address adc@gfe.com`	AP によって生成された証明書要求の件名パラメータに含める属性を指定します。
ステップ 3	**end** 例： `デバイス(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

LSC 証明書のキー サイズの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap lsc-provision key-size**{ **2048** | **3072** | **4096}**} 例： `デバイス(config)# ap lsc-provision key-size 2048`	AP 上の LSC に対して生成されるキーのサイズを指定します。
ステップ 3	**end** 例： `デバイス(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

アクセスポイントでの LSC プロビジョニング用トラストポイントの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap lsc-provision trustpoint** *tp-name* 例： `デバイス(config)# ap lsc-provision trustpoint microsoft-ca`	LCS を AP にプロビジョニングする際に使用するトラストポイントを指定します。 tp-name：トラストポイント名。
ステップ 3	**end** 例： `デバイス(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

AP LSC プロビジョンリストの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Wireless]** > **[Access Points]** 選択します。

ステップ 2 [All Access Points] ウィンドウで、対応する LSC プロビジョンの名前をクリックします。

ステップ 3 [Status] ドロップダウンリストから、LSC を有効にするステータスを選択します。

ステップ 4 [Trustpoint Name] ドロップダウンリストからトラストポイントを選択します。

ステップ 5 [Number of Join Attempts] フィールドに、許可される再試行回数を入力します。

ステップ 6 [Key Size] ドロップダウンリストから、キーを選択します。

ステップ 7 [Edit AP Join Profile] ウィンドウで [CAPWAP] タブをクリックします。

ステップ 8 [Add APs to LSC Provision List] セクションで [Select File] をクリックして、AP の詳細を含む CSV ファイルをアップロードします。

ステップ 9 [**Upload File**（ファイルのアップロード）] をクリックします。

ステップ 10 [AP MAC Address] フィールドに、AP の MAC アドレスを入力して、追加します（プロビジョンリストに追加された AP は、[APs in Provision List] に表示されます）。

ステップ 11 [Subject Name Parameters] セクションに、次の詳細情報を入力します。

- 国

- **State**
- **市区町村郡（City）**
- **Organisation**
- **部署名（Department）**
- **電子メール アドレス（Email Address）**

ステップ 12 [Apply] をクリックします。

AP LSC プロビジョンリストの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[**no**] **ap lsc-provision mac-address** *mac-addr* 例： `デバイス(config)# no ap lsc-provision mac-address 001b.3400.02f0`	LSC プロビジョンリストに AP を追加します。 （注） **ap lsc-provision provision-list** コマンドを使用して AP のリストをプロビジョニングできます。 （または） **ap lsc-provision** コマンドを使用してすべての AP をプロビジョニングできます。
ステップ 3	**end** 例： `デバイス(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

すべての AP に対する LSC プロビジョニングの設定（GUI）

手順

ステップ 1 [Configuration] > [Wireless] > [Access Points] > > の順に選択します。

ステップ 2 [Access Points] ウィンドウで [LSC Provision] セクションを展開します。

ステップ 3 [Status] を [Enabled] 状態に設定します。

（注） [Status] を [Provision List] に設定すると、そのプロビジョンリストに含まれている AP に対してのみ LSC プロビジョニングが設定されます。

ステップ 4 [Trustpoint Name] ドロップダウンリストから、すべての AP に対して適切なトラストポイントを選択します。

ステップ 5 [Number of Join Attempts] フィールドに、AP が組み込みワイヤレスコントローラへの参加を再試行できる回数を入力します。

ステップ 6 [Key Size] ドロップダウンリストから、証明書のキーサイズを選択します。

- **2048**
- **3072**
- **4096**

ステップ 7 [Add APs to LSC Provision List] セクションで [Select File] をクリックして、AP の詳細を含む CSV ファイルをアップロードします。

ステップ 8 [**Upload File**（ファイルのアップロード）] をクリックします。

ステップ 9 [AP MAC Address] フィールドに、AP の MAC アドレスを入力します（プロビジョンリストに追加された AP は、[APs in Provision List] セクションに表示されます）。

ステップ 10 [Subject Name Parameters] セクションに、次の詳細情報を入力します。

1. **国**
2. **State**
3. **市区町村郡（City）**
4. **Organization**
5. **部署名（Department）**
6. **電子メール アドレス（Email Address）**

ステップ 11 [Apply] をクリックします。

すべての AP に対する LSC プロビジョニングの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[**no**] **ap lsc-provision** 例： `デバイス(config)# no ap lsc-provision`	すべての AP に対して LSC プロビジョニングを有効にします。 デフォルトでは、LSC プロビジョニングはすべての AP に対して無効になっています。
ステップ 3	**end** 例： `デバイス(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

プロビジョンリストに含まれる AP に対する LSC プロビジョニングの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap lsc-provision provision-list** 例： `デバイス(config)# ap lsc-provision provision-list`	プロビジョンリストに設定されている一連の AP に対して LSC プロビジョニングを有効にします。
ステップ 3	**end** 例： `デバイス(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

ローカルで有効な証明書のプロビジョニング解除

ローカルで有効な証明書（LSC）のプロビジョニングを解除するには、次の手順を実行します。

1. シャーシを WLAN コモンクライテリア（WLANCC）モードに移行します。
2. LSC とワイヤレス管理トラストポイントをプロビジョニングして、AP をリロードします。詳細については、LSC プロビジョニングおよび管理トラストポイントの設定（14 ページ）を参照してください。
3. 連邦情報処理標準（FIPS）と WLANCC を削除します。詳細については、FIPS および WLAN コモンクライテリアの削除（15 ページ）を参照してください。
4. LSC プロビジョニングを削除します。詳細については、LSC プロビジョニングの削除（16 ページ）を参照してください。

LSC プロビジョニングおよび管理トラストポイントの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap lsc-provision** 例： `Device(config)# ap lsc-provision`	AP LSC プロビジョニングパラメータを設定します。
ステップ 3	**wireless management trustpoint** *trustpoint_name* 例： `Device(config)# wireless management trustpoint trustpoint-name`	LSC の管理トラストポイントを設定します。
ステップ 4	**do write** 例： `Device(config)# do write`	実行コンフィギュレーションをメモリ、ネットワーク、または端末に書き込みます。

FIPS および WLAN コモンクライテリアの削除

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap dtls-version dtls_1_2** 例： `Device(config)# ap dtls-version dtls_1_2`	AP DTLS バージョンを設定します。
ステップ 3	**ap dtls-cipher** *ECDHE-ECDSA-AES256-GCM-SHA384* 例： `Device(config)# ap dtls-cipher ECDHE-ECDSA-AES256-GCM-SHA384`	AP DTLS 暗号スイートを設定します。
ステップ 4	**no wireless wlancc** 例： `Device(config)# no wireless wlancc`	コントローラの WLAN CC を無効にします。
ステップ 5	**no fips authorization-key** 例： `Device(config)# no fips authorization-key`	FIPS の認証キーを無効にします。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**write memory** 例： `Device# write memory`	設定を保存します。
ステップ 8	**reload** 例： `Device# reload`	内部 AP をリロードして、非 FIPS および非 CC モードに移行します。

LSC プロビジョニングの削除

始める前に

スタンバイ AP が起動するのを待ちます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no ap lsc-provisioning** 例： `Device(config)# no ap lsc-provisioning`	AP LSC プロビジョニングパラメータを無効にします。
ステップ 3	**shutdown** 例： `Device(config)# shutdown`	スタンバイ AP をリロードします。 （注） マスター AP の次のリロードも待ちます。
ステップ 4	**no ap dtls-cipher ECDHE-ECDSA-AES256-GCM-SHA384** 例： `Device(config)# no ap dtls-cipher ECDHE-ECDSA-AES256-GCM-SHA384`	AP DTLS 暗号スイートを無効にします。
ステップ 5	**no ap dtls-version dtls_1_2** 例： `Device(config)# no ap dtls-version dtls_1_2`	DTLS バージョンを無効にします。
ステップ 6	**no wireless management trustpoint** 例： `Device(config)# no wireless management trustpoint`	ワイヤレス管理トラストポイントを無効にします。
ステップ 7	**reload** 例： `Device# reload`	内部 AP をリロードします。

Trustpool への CA 証明書のインポート（GUI）

PKI Trustpool Management は、コントローラ上のさまざまなサービスによって使用される信頼できる証明書（ダウンロードまたは組み込み）のリストを保存するために使用されます。また、マルチレベル CA 証明書の認証にも使用されます。PKI Trustpool 内の組み込み CA 証明書バンドルが最新のものではない、破損している、または特定の証明書を更新する必要がある場合、シスコから自動更新を受信します。

PKI Trustpool の CA 証明書を手動で更新するには、このタスクを実行します。

（注） LSC が中間 CA によって発行されている場合は、CA 証明書の完全なチェーンを Trustpool にインポートする必要があります。インポートせず、コントローラに完全なチェーンが存在しない状態では AP をプロビジョニングできません。証明書がルート CA によって発行されている場合、インポート手順を実行する必要はありません。

手順

ステップ 1 **[Configuration]** > **[Security]** > **[PKI Management]** を選択します。

ステップ 2 [PKI Management] ウィンドウで、[Trustpoint] タブをクリックします。

ステップ 3 [Import] をクリックします。

ステップ 4 [CA Certificate] フィールドで、CA 証明書をコピーして貼り付けます。複数の CA 証明書（.pem 形式）をリンクします。

ステップ 5 [Apply to Device] をクリックします。

Trustpool への CA 証明書のインポート（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 2	**crypto pki trust pool import terminal**
	例：
	`デバイス(config)# crypto pki trust pool import terminal`
	`% Enter PEM-formatted CA certificate.`
	`% End with a blank line or "quit" on a line by itself.`
		ルート証明書をインポートします。インポートするためには、digicert.com から CA 証明書を貼り付ける必要があります。

	コマンドまたはアクション	目的
	-----BEGIN CERTIFICATE----- **-----END CERTIFICATE-----** **-----BEGIN CERTIFICATE-----** **-----END CERTIFICATE-----** **-----BEGIN CERTIFICATE-----** **-----END CERTIFICATE-----** **Aug 23 02:47:33.450:** **%PKI-6-TRUSTPOOL_DOWNLOAD_SUCCESS:** **Trustpool Download is successful**	
ステップ 3	**end** 例： デバイス(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

Trustpool にインポートされた CA 証明書のクリーニング（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[PKI Management]** を選択します。

ステップ 2 [PKI Management] ウィンドウで、[Trustpoint] タブをクリックします。

ステップ 3 [Clean] をクリックします。

（注） ダウンロードした CA 証明書バンドルが消去されますが、組み込みの CA 証明書バンドルは消去されません。

ステップ 4 **[はい（Yes）]** をクリックします。

Trustpool にインポートされた CA 証明書のクリーニング（CLI）

特定の CA 証明書を Trustpool から削除することはできません。ただし、Trustpool にインポートされた CA 証明書はすべてクリアできます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**crypto pki trustpool clean** 例： `デバイス(config)# crypto pki trustpool clean`	ダウンロードしたCA証明書バンドルが消去されますが、組み込みのCA証明書バンドルは消去されません。
ステップ 3	**end** 例： `デバイス(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

単一の CA 証明書専用の新しいトラストポイントの作成

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**crypto pki trustpoint** *tp-name* 例： `デバイス(config)# crypto pki trustpoint tp_name`	トラストポイントを作成します。
ステップ 3	**enrollment terminal** 例： `デバイス(ca-trustpoint)# enrollment terminal`	トラストポイントの登録端末を作成します。
ステップ 4	**exit** 例： `デバイス(ca-trustpoint)# exit`	トラストポイント設定を終了します。

ステップ 5	**crypto pki authenticate** *tp-name*
	例：
	`デバイス(config)# crypto pki authenticate tp_name`
	`<<< PASTE CA-CERT in PEM format followed by quit >>>`
		トラストポイントを認証します。

LSC 設定の確認

ワイヤレス管理トラストポイントの詳細を表示するには、次のコマンドを使用します。

```
Device# show wireless management trustpoint

Trustpoint  Name : microsoft-ca
Certificate Info : Available
Certificate Type : LSC
Certificate Hash : 9e5623adba5307facf778e6ea2f5082877ea4beb
 Private key Info : Available
```

AP の LSC プロビジョン関連の設定に関する詳細を表示するには、次のコマンドを使用します。

```
Device# show ap lsc-provision summary

AP LSC-provisioning : Disabled
Trustpoint used for LSC-provisioning : microsoft-ca
LSC Revert Count in AP reboots : 10

AP LSC Parameters :
Country : IN
State : KA
City : BLR
Orgn : ABC
Dept : ABC
Email : support@abc.com
Key Size : 2048

AP LSC-provision List : Enabled
Total number of APs in provision list: 3

Mac Address
-----------
0038.df24.5fd0
2c5a.0f22.d4ca
e4c7.22cd.b74f
```

```
Device# show ap lsc-provision summary

AP LSC-provisioning : Disabled
Trustpoint used for LSC-provisioning : lsc-root-tp
Certificate chain status : Available
Number of certs on chain : 2
Certificate hash : 7f9d05183deecac4e5a79db65d538245685e8e30
LSC Revert Count in AP reboots : 1

AP LSC Parameters :
Country : IN
State : KA
City : BLR
Orgn : ABC
Dept : ABC
Email : support@abc.com
Key Size : 2048
EC Key Size : 384 bit

AP LSC-provision List :

Total number of APs in provision list: 2
```

```
Mac Addresses :
--------------
1880.90f5.1540
2c5a.0f70.84dc
```

LSC の管理トラストポイントの設定（GUI）

手順

ステップ 1 **[Administration]** > **[Management]** > **[HTTP/HTTPS]** の順に選択します。

ステップ 2 [HTTP Trust Point Configuration] セクションで、[Enable Trust Point] を [Enabled] 状態に設定します。

ステップ 3 [Trust Points] ドロップダウンリストから、適切なトラストポイントを選択します。

ステップ 4 設定を保存します。

LSC の管理トラストポイントの設定（CLI）

LSC のプロビジョニング後、AP は自動的に再起動し、ブートアップ後に LSC モードで参加します。同様に、AP LSC のプロビジョニングを削除すると、AP は再起動し、非 LSC モードで接続します。

EWC では、内部 AP は自動的には再起動しません。LSC モードと非 LSC モードで動作させるには、内部 AP を手動で再起動する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** **例**： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wireless management trustpoint** *trustpoint_name* **例**： `デバイス(config)# wireless management trustpoint microsoft-ca`	LSC の管理トラストポイントを設定します。 内部 AP はリロードの前に参加できなくなるため、次の手順を実行して内部 AP をリロードします。
ステップ 3	**write memory** **例**： `Device(config)# write memory`	設定を保存します。

	コマンドまたはアクション	目的
ステップ 4	**wireless ewc-ap ap reload** 例： `Device(config)# write memory`	内部 AP をリロードします。これにより、AP 上のコントローラもリロードされます。
ステップ 5	**end** 例： `デバイス(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

コントローラに接続する MIC および LSC アクセスポイントに関する情報

コントローラに接続する MIC および LSC アクセスポイントのサポートの概要

Cisco IOS XE Bengaluru 17.4.1 以前のリリースでは、デフォルトの証明書（製造元でインストールされる証明書（MIC）または Secure Unique Device Identifier（SUDI））を持つ AP は、ローカルで有効な証明書（LSC）が展開されたコントローラには接続できません。このコントローラの管理証明書は LSC です。この問題を解決するには、LSC が展開されたコントローラに移動する前に、プロビジョニング コントローラを使用してそれらの AP に LSC をプロビジョニングする必要があります。

Cisco IOS XE Bengaluru 17.5.1 以降では、新しい認証ポリシー設定により、MIC AP が LSC が展開されたコントローラに接続でき、LSC と MIC AP がコントローラ内で同時に共存できるようになりました。

推奨事項および制約事項

- CA サーバーが証明書署名要求（CSR）を受け入れるように手動登録（手動介入）で構成されている場合、コントローラは CA サーバーが保留中の応答を送信するのを待ちます。10 分間 CA サーバーからの応答がない場合、フォールバックモードが有効になります。
  - Cisco Wave 2 AP が CSR を再生成し、新しい CSR が CA サーバーに送信されます。
  - Cisco IOS AP が再起動すると、Cisco IOS AP から新しい CSR が送信され、CA サーバーにも送信されます。
- コントローラのローカルで有効な証明書（LSC）は、パスワードチャレンジでは機能しません。このため、LSC を機能させるには、CA サーバーでパスワードの確認を無効にする必要があります。

- Microsoft CA を使用している場合は、CA サーバーとして Windows Server 2012 以降を使用することをお勧めします。

設定ワークフロー

1. コントローラでの LSC の設定（CLI） （23 ページ）
2. AP での AP 証明書ポリシーの有効化（CLI） （24 ページ）
3. AP ポリシー証明書の設定（GUI） （25 ページ）
4. コントローラに接続するための AP の許可リストの設定（CLI） （25 ページ）

コントローラでの LSC の設定（CLI）

CAPWAP-DTLS のコントローラによって使用されるサーバー証明書は、次の設定に基づいています。

始める前に

- 次のワイヤレス管理サービスに適切なトラストポイントを設定して、LSC を有効にしてください。
  - AP 接続プロセス：CAPWAP DTLS サーバー証明書
  - モビリティ接続：モビリティ DTLS 証明書
  - NMSP および CMX 接続：NMSP TLS 証明書

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**[no] wireless management trustpoint** *trustpoint-name* 例： `Device(config)# wireless management trustpoint trustpoint-name`	LSC 展開コントローラで LSC トラストポイントを設定します。

AP での AP 証明書ポリシーの有効化（CLI）

- 管理トラストポイントが LSC の場合、デフォルトでは、MIC AP はコントローラに接続できません。この設定は、MIC AP がコントローラに接続できるようにするコンフィギュレーションノブの有効化または無効化として機能します。
- この設定は、DTLS ハンドシェイク時に AP が MIC に接続できるようにするコントローラ認証です。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap auth-list ap-cert-policy allow-mic-ap trustpoint** *trustpoint-name* 例： `Device(config)# ap auth-list ap-cert-policy allow-mic-ap trustpoint trustpoint-name`	コントローラ証明書チェーンのトラストポイント名を設定します。 （注） **allow-mic-ap trustpoint** コマンドは、仮想コントローラ（クラウド向け Cisco Catalyst 9800-CL ワイヤレスコントローラ）にのみ必要です。他のすべてのアプライアンス コントローラ プラットフォームでは、デフォルトの証明書が選択されています。このデフォルトの証明書は、製造元がインストールした SUDI です。
ステップ 3	**ap auth-list ap-cert-policy allow-mic-ap** 例： `Device(config)# ap auth-list ap-cert-policy allow-mic-ap`	CAPWAP-DTLS ハンドシェイク中に AP 証明書ポリシーを有効にします。
ステップ 4	**ap auth-list ap-cert-policy** {**mac-address** *H.H.H* | **serial-number** *serial-number-ap*} **policy-type mic** 例： `Device(config)# ap auth-list ap-cert-policy mac-address 1111.1111.1111 policy-type mic`	AP 証明書ポリシーを MIC として有効にします。

AP ポリシー証明書の設定（GUI）

手順

ステップ 1 [Configuration] > [Wireless] > [Access Points] を選択します。

ステップ 2 [All Access Points] ウィンドウで、[AP Certificate Policy] をクリックします。

ステップ 3 [AP Policy Certificate] ウィンドウで、以下のアクションを実行します。

a) [Authorize APs join with MIC] トグルボタンをクリックして、AP 認証を有効にします。

b) [Trustpoint Name] ドロップダウンリストから、必要なトラストポイントを選択します。

c) [Add MAC or Serial Number] をクリックして、MAC アドレスまたはシリアル番号を手動で追加するか、.csv ファイルを使用して追加します。
[Add MAC or Serial Number] ウィンドウが表示されます。

d) [AP Authlist Type] をクリックし、MAC アドレスまたはシリアル番号を入力します。.csv ファイルをアップロードするか、リストボックスに MAC アドレスを入力します。
新しく追加された MAC アドレスとシリアル番号は、[List of MAC Address and Serial Numbers] の下に表示されます。

e) [Apply] をクリックします。

AP 証明書ポリシーが [AP Inventory] ウィンドウに追加されます。

（注） MIC を使用して新しい AP を追加するには、「AP ポリシー証明書の設定（GUI）」の項で説明されているステップ 1 ～ 3 を実行します。LSC を使用して新しい AP を追加するには、「AP LSC プロビジョンリストの設定（GUI）」と「AP ポリシー証明書の設定（GUI）」のステップ 1 ～ 3 で説明されている手順を実行します。

コントローラに接続するための AP の許可リストの設定（CLI）

AP の許可リストは、イーサネット MAC アドレスまたは AP のシリアル番号に基づいて入力できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap auth-list ap-cert-policy** {**mac-address** *AP-Ethernet-MAC-address* | **serial-number** *AP-serial-number*} **policy-type mic** 例：	イーサネット MAC アドレスまたは AP のアセンブリシリアル番号に基づいて AP 証明書ポリシーを設定します。

	コマンドまたはアクション	目的
	`Device# ap auth-list ap-cert-policy mac-address 00b0.e192.0d98 policy-type mic`	

設定ステータスの確認

AP が AP 証明書ポリシーによって承認されているかどうかを確認するには、次のコマンドを使用します。

```
Device# show ap auth-list ap-cert-policy
Authorize APs joining with MIC : ENABLED
MIC AP policy trustpoint
Name : CISCO_IDEVID_SUDI
Certificate status : Available
Certificate Type : MIC
Certificate Hash : xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

AP の MAC アドレスとシリアル番号に関する AP 証明書ポリシーを確認するには、次のコマンドを使用します。

```
Device# show ap auth-list ap-cert-policy mac-address
MAC address      AP cert policy
---------------------------------
1111.2222.3333   MIC

Device# show ap auth-list ap-cert-policy serial-number
Serial number    AP cert policy
---------------------------------
F1234567890      MIC
```

（注） 無効なトラストポイント（SSC以外）を設定すると、**allow-mic-ap policy** は有効になりません。無効なトラストポイントを設定すると、次のエラーがコンソールに表示されます。

```
Device(config)# ap auth-list ap-cert-policy allow-mic-ap trustpoint lsc-root-tp
Dec 18 07:38:29.944: %CERT_MGR_ERRMSG-3-CERT_MGR_GENERAL_ERR: Chassis 1 R0/0: wncd:
General error: MIC AP Policy trustpoint: 'lsc-root-tp' cert-chain type is LSC, It must
be either MIC or vWLC-SSC
```