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 Cisco Catalyst 9800 シリーズ 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 Public Key Infrastructure（PKI）を選択した場合は、AP とコントローラで LSC を生成できます。その後、証明書を使用してコントローラと AP を相互認証することができます。

シスコ コントローラは、LSC を使用するように設定できます。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 を使用できます。

コントローラで新しい LSC 証明書をプロビジョニングし、次に認証局（CA）サーバから 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コントローラと通信します。証明書への署名と、LAP およびコントローラ自体の CA 証明書の発行については、コントローラから要求を開始する必要があります。LAP は CA サーバと直接通信しません。CA サーバの詳細がコントローラに設定され、アクセス可能である必要があります。

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、PKI クライアントと認証局サーバが証明書の登録と失効をサポートするため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、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 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 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 プロトコルを使用する場合、CA 証明書は CA サーバから受け取ります。この時点ではコントローラに証明書が存在しないため、これは純粋な **Get** 操作です。これらの証明書はコントローラ上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。

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 証明書に組み込まれ、要求者の秘密キーでデジタル署名される件名、公開キー、およびその他の属性が含まれています。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 が要求者の 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には、追加情報が必要です。証明書の要求または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何度も組み合わされます。

ここで、PKCS#10 は 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、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上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 モードで 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 はコントローラに certRequest を送信します。このコントローラは CA プロキシとして機能し、CA により署名された LAP 用の certRequest の取得に対応します。

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、システムが自動リブートします。システムが次に起動するときには、LSC を使用するように設定されているため、AP は接続要求の一部として LSC デバイス証明書をコントローラに送信します。接続応答の一部として、コントローラは新しいデバイス証明書を送信すると同時に、新しい CA ルート証明書を使用して受信 LAP 証明書を検証します。

（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。

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： `Device(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。 • **key_size** には、キー係数のサイズを入力します。有効な範囲は 360 ～ 4096 です。 • **RSA_key** には、RSA キー ペアのラベルを入力します。
ステップ 3	**end** 例： `Device(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。
ステップ 2	**crypto pki trustpoint** *trustpoint_name* 例： `Device(config)# crypto pki trustpoint microsoft-ca`	外部 CA サーバの新しいトラスト 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： `Device(ca-trustpoint)# enrollment url http://CA_server/certsrv/mscep/mscep.dll`	トラストポイント登録パラメータを使用してトラストポイントを登録します。
ステップ 4	**subject-name** *subject_name* 例： `Device(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： `Device(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 ペアのラベルを指します。 • *key_size*：署名キーの長さを指します。範囲は 360 ～ 4096 です。
ステップ 6	**revocation** {**crl** | **none** | **ocsp**} 例： `Device(ca-trustpoint)# revocation none`	失効を確認します。
ステップ 7	**end** 例： `Device(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。

CA サーバを使用した 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 [Trustpoint] セクションで [Add] をクリックします。

ステップ 3 トラストポイントのラベルと登録 URL を入力します。

ステップ 4 [Authenticate] チェック ボックスをオンにして、トラストポイントのラベルを認証します。

ステップ 5 [Subject Name] セクションに、国コード、都道府県、場所、組織、ドメイン名、および電子メール アドレスを入力します。

ステップ 6 [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選択できます。

ステップ 7 [Enroll Trustpoint] チェック ボックスをオンにしてパスワードを入力し、確認します。

ステップ 8 [Save & Apply to Device] をクリックします。

CA サーバを使用した 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： `Device(config)# crypto pki authenticate microsoft-ca`	CA 証明書を取得します。

ステップ 3	**yes**
	例：
	`Device(config)# % Do you accept this certificate? [yes/no]: yes`
	`Trustpoint CA certificate accepted.`	

ステップ 4	**crypto pki enroll** *trustpoint_name*
	例：
	`Device(config)# crypto pki enroll microsoft-ca`
	`%`
	`% Start certificate enrollment ..`
		クライアント証明書を登録します。

	コマンドまたはアクション	目的
	% 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.	
ステップ 5	**password** 例： `Device(config)# abcd123`	パスワードを入力します。
ステップ 6	**password** 例： `Device(config)# abcd123`	パスワードを再入力します。
ステップ 7	**yes** 例： `Device(config)# % Include the router serial number in the subject name? [yes/no]: yes`	
ステップ 8	**no** 例： `Device(config)# % Include an IP address in the subject name? [no]: no`	
ステップ 9	**yes** 例： `Device(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： `Device(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] ページで LSC プロビジョンの名前をクリックします。
ステップ 3 [Status] ドロップダウンを使用して LSC を有効にします。
ステップ 4 [Trustpoint Name] ドロップダウンを使用して、トラストポイントを検索または選択します。
ステップ 5 [Number of Join Attempts] フィールドに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： `Device(config)# ap lsc-provision join-attempt 10`	新しくプロビジョニングされた LSC 証明書を使用した AP の接続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 MIC 証明書を使用して再接続します。
ステップ 3	**end** 例： `Device(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： `Device(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に含める属性を指定します。
ステップ 3	**end** 例： `Device(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**{**1024** | **2048**} 例： `Device(config)# ap lsc-provision key-size 1024`	AP 上の LSC 証明書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： `Device(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： `Device(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* はトラストポイント名を指します。
ステップ 3	**end** 例： `Device(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 の 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] > > の順に選択します。

ステップ 2 [All Access Points] ページで LSC プロビジョンの名前をクリックします。

ステップ 3 [Status] ドロップダウンを使用して LSC を有効にします。

ステップ 4 [Trustpoint Name] ドロップダウンを使用して、トラストポイントを検索または選択します。

ステップ 5 [Number of Join Attempts] フィールドに再試行回数を入力します。

ステップ 6 [Key Size] ドロップダウンを使用してキーを選択します。

ステップ 7

ステップ 8 [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 9 [Add APs to LSC Provision List] セクションで、[Select File] オプションを使用して AP の詳細を含む CSV ファイルをアップロードします。ファイルを選択したら [Upload File] をクリックします。

ステップ 10 [AP MAC Address] フィールドを使用して、MAC アドレスで AP を検索し、追加することもできます。プロビジョン リストに追加された AP は、[APs in provision List] リストボックスに表示されます。

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。

- Country
- 都道府県（State）
- 市区町村郡（City）
- Organisation
- department
- 電子メール アドレス

ステップ 12 [Apply] をクリックします。

AP の 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： `Device(config)# no ap lsc-provision mac-address 001b.3400.02f0`	LSC プロビジョン リストにアクセス ポイントを追加します。 （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： `Device(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。

すべてのアクセス ポイントに対する 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] ページで [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。

[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 がコントローラへの接続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を使用して、次のオプションから証明書の適切なキー 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] オプションをクリックして、AP の詳細を含む CSV ファイルをアップロードします。ファイルを選択したら [Upload File] をクリックします。

ステップ 8 [AP MAC Address] フィールドに AP の MAC アドレスを入力して AP を検索し、追加することもできます。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 9 [Subject Name Parameters] セクションに、次の詳細情報を入力します。

1. Country
2. 都道府県（State）
3. 市区町村郡（City）
4. マニュアルの構成
5. 部門
6. 電子メール アドレス

ステップ 10 [Apply] をクリックします。

すべてのアクセス ポイントに対する 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： `Device(config)# no ap lsc-provision`	すべてのアクセスポイントに対して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： `Device(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 リストに含まれるアクセス ポイントに対する 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： `Device(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アクセス ポイントに対して LSC プロビジョニングを有効にします。
ステップ 3	**end** 例： `Device(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 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 プロビジョンに関連する設定の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
```

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] フィールドを [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）

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： `Device(config)# wireless management trustpoint microsoft-ca`	LSC の管理トラストポイントを設定します。
ステップ 3	**end** 例： `Device(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。