# 9800 WLCでのローカルで有効な証明書プロビジ ョニングのためのSCEPの設定

## 内容

概要 前提条件 要件 <u>使用するコンポーネント</u> 背景説明 設定 ネット<u>ワーク図</u> Windows ServerでのSCEPサービスの有効化 SCEP 登録チャレンジ パスワードの要件の無効化 証明書テンプレートとレジストリの設定 9800デバイスのトラストポイントの設定 AP登録パラメータと更新管理トラストポイントの定義 確認 コントローラ証明書のインストールの確認 9800 WLC LSC設定の確認 アクセスポイント証明書のインストールの確認 トラブルシュート 一般的な問題 debugおよびlogコマンド 登録の成功例

### 概要

## 前提条件

Windows ServerでSCEPを正常に実行するには、9800 WLCが次の要件を満たしている必要があります。

- •コントローラとサーバの間に到達可能性がある必要があります。
- コントローラとサーバは同じNTPサーバに同期されているか、同じ日付とタイムゾーンを共有しています(CAサーバとAPからの時刻が異なる場合、APは証明書の検証とインストールに問題があります)。

Windows Serverでは、インターネットインフォメーションサービス(IIS)が以前に有効になってい る必要があります。

### 要件

次のテクノロジーに関する知識があることが推奨されます。

- 9800 Wireless LAN Controllerバージョン16.10.1以降。
- Microsoft Windows Server 2012 Standard.
- ・秘密キーインフラストラクチャ(PKI)と証明書。

#### 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いています。

- 9800-L WLCソフトウェアバージョン17.2.1。
- Windows Server 2012 Standard R2.
- •3802アクセスポイント

**注**:このドキュメントのサーバ側の設定は、特にWLC SCEPです。詳細、セキュリティ、 および証明書サーバの設定については、Microsoft TechNetを参照してください。

#### 背景説明

新しいLSC証明書(認証局(CA)ルート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 ールして、最終的にAPにダウンロードする必要があります。SCEPでは、CA証明書とデバイス証 明書がCAサーバから受信され、後でコントローラに自動的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、同じ認証プロセスが実行されます。そのためには、コン トローラがCAプロキシとして機能し、CAによって署名されたAPの証明書要求(自己生成)を取 得するのに役立ちます。

### 設定

ネットワーク図



Windows ServerでのSCEPサービスの有効化

**ステップ1:サーバマネージャ**アプリケーションで、[管理]メニ**ューを選択**し、[役割と機能の追**加** ]**オプションを選択し**て、役割の役割と機能構成ウィザードを開きます。そこから、SCEPサーバ 登録に使用されるサーバインスタンスを選択します。

ステップ2:[Certification Authority]、[Network Device Enrollment Service]、および[Online Responder]の機能が選択されていることを確認し、[Next]を選択します。

L.	Add Roles and Features Wizard	_ <b>D</b> X
Before You Begin Installation Type Server Selection Server Roles Features	Add Roles and Features Wizard Select one or more roles to install on the selected server. Roles  Certification Authority (Installed) Certification Authority (Installed) Certification Services (1 of 6 installed)	DESTINATION SERVER Chuu-Win12.chuu-domain.local Description Windows Server Essentials Experience sets up the IT infrastructure and provides powerful functions such as PC backups that below sortext data and Permete Web
Confirmation Results	<ul> <li>✓ Certificate Enrollment Policy Web Service</li> <li>✓ Certificate Enrollment Web Service</li> <li>✓ Certification Authority Web Enrollment</li> <li>✓ Certification Authority Web Enrollment</li> <li>✓ Network Device Enrollment Service</li> <li>✓ Online Responder</li> <li>✓ Active Directory Domain Services (Installed)</li> <li>△ Active Directory Federation Services</li> <li>△ Active Directory Lightweight Directory Services</li> <li>△ Active Directory Rights Management Services</li> <li>△ Application Server</li> <li>✓ DHCP Server (Installed)</li> <li>○ Fax Server</li> </ul>	helps protect data, and Remote Web Access that helps access business information from virtually anywhere.
	< Previous	Next > Install Cancel

**ステップ3:[**次へ]を2回選択し、[完了]を選択して構成ウィザードを終了します。サーバーが機能の インストールプロセスを完了するまで待ってから、[閉じる]を選択してウィザードを閉じます。

ステップ4:インストールが完了すると、[Server Manager Notification]アイコンに警告アイコンが 表示されます。これを選択し、[AD CS構成ウィザード]メニューを開くには、[接続先サーバー上 のActive Directoryサービスの構成]オプションリンクを選択してください。

-	Server Manager	
€ ∵ Server M	lanager • Dashboard	- ②   🏹 Manage
III Dashboard	WELCOME TO SERVER MANAGER	Post-deployment Configuration     Configuration     Configuration required for Active Directory
Local Server     All Servers     All CS	1 Configure this local server	Configure Active Directory Certificate Services on th Configure Active Directory Certificate Services on th  Feature installation
間 AD DS 覧 DHCP	2 Add roles and features	Configuration required. Installation succeeded on Chuis-Win12 dhuis-domain.local.
B DNS ■ File and Storage Services ▷	3 Add other servers to manage	Add Roles and Features
ED IIS PL NAP	4 Create a server group	Task Details

**ステップ5**:メニューで構成するNetwork Device Enrollment ServiceとOnline Responderの役割サ ービスを選択し、[次へ]を選**択します**。

**ステップ6:NDESの**サービスアカウントで、組み込みのアプリケーションプールとサービスアカ ウントの間のオプションを選択し、[次へ]を選択します。

**注**:サービスアカウントの場合は、そのアカウントがIIS\_IUSRSグループに属していること を確認してください。



**ステップ7**:次の画面で[Next]を選択し、インストール処理を終了します。インストール後、 SCEP URLは任意のWebブラウザで使用できます。URL http://<server ip>/certsrv/mscep/mscep.dllに移動し、サービスが利用可能であることを確認します。

9	Netw	ork Dev	rice Enrollment Servic × +	L-	-   י		x
÷	$\rightarrow$	C	No seguro   172.16.80.8/certsrv/mscep/mscep	dll ☆		Ð	:
Netv	Network Device Enrollment Service						

Network Device Enrollment Service allows you to obtain certificates for routers or other network devices using the Simple Certificate Enrollment Protocol (SCEP).

This URL is used by network devices to submit certificate requests.

To obtain an enrollment challenge password, go to the admin URL. By default, the admin URL is <u>http://Chuu-Win12/CertSrv/mscep\_admin</u>

For more information see Using Network Device Enrollment Service.

#### SCEP 登録チャレンジ パスワードの要件の無効化

デフォルトでは、Windows Serverは動的チャレンジパスワードを使用して、Microsoft SCEP(MSCEP)に登録する前にクライアント要求とエンドポイント要求を認証します。 そのため には、管理者アカウントがWeb GUIを参照し、各要求のオンデマンドパスワードを生成する必要 があります(パスワードは要求に含める必要があります)。コントローラは、サーバに送信する 要求にこのパスワードを含めることはできません。この機能を削除するには、NDESサーバのレ ジストリキーを変更する必要があります。

**ステップ1:レジス**トリエディットフォームを開き、[スタート]メニ**ュー**から[Regedit]**を検索**します。

ステップ2:[Computer] > [HKEY\_LOCAL\_MACHINE] > [SOFTWARE] > [Microsoft] > [Cryptography] > [MSCEP] > [EnforcePassword]に移動します

ステップ3:EnforcePasswordの値を0に変更します。すでに0の場合は、そのまま残します。

<b>B</b>		Registry Editor		_ 🗆 🗙
File Edit View Favorites Help				
- MSCEP	^	Name	Туре	Data
— 👢 САТуре		(Default)	REG SZ	(value not set)
CertsInMYStore		EnforcePassword	REG_DWORD	0x00000000 (0)
EnforcePassword		,		
PasswordVDir				
UseSinglePassword				
- OID	Ξ			
- Protect	_			
- Providers				
CTE				
DataAccess				
DevDiv				
Device Association Framework				N
Dfra				4
DFS				
DHCPMibAgent				
DirectDraw				
DirectInput				
DirectPlay8				
DirectPlayNATHelp	$\sim$			
<		<	111	>
Computer\HKEY_LOCAL_MACHINE\	SOFT	WARE\Microsoft\Crypt	ography\MSCEP\Enfor	cePassword

### 証明書テンプレートとレジストリの設定

証明書とその関連キーは、CAサーバ内のアプリケーションポリシーによって定義される異なる目 的で、複数のシナリオで使用できます。アプリケーションポリシーは、証明書の拡張キー使用法 (EKU)フィールドに保存されます。このフィールドはオーセンティケータによって解析され、意 図した目的でクライアントによって使用されていることを確認します。適切なアプリケーション ポリシーがWLCおよびAP証明書に統合されていることを確認するには、適切な証明書テンプレー トを作成し、それをNDESレジストリにマッピングします。

ステップ1:[Start] > [Administrative Tools] > [Certification Authority]に移動します。

**ステップ2:CA** Serverフォルダツリーを展開し、[Certificate Templates]フォルダを右クリックして [Manage]を選択します。

**ステップ3:ユ**ーザー証明書テンプレートを右クリックして、コンテキストメニューで[Duplicate Template]を選択します。

**ステップ4:**[General]タブに移動し、テンプレート名と有効期間を必要に応じて変更し、その他の オプションはすべてオフのままにします。

**注意**:有効期間を変更する場合は、証明機関のルート証明書の有効期間より大きくないこと を確認してください。

Pro	perties	of New	Template	X
Subject Name	Ser	ver	Issuance R	equirements
Superseded Templa	ites	Exte	ensions	Security
Compatibility General	Request	Handling	Cryptography	Key Attestation
Template display name				
9800-LSC				
Template name:				
9800-LSC				
Validity period:		Renewa	l period:	
2 unam		C C C	weeke v	
2 years V			weeks v	
Publish certificate in	Active Di	rectory		
Do not automatic	cally reenro	oll if a dupli	cate certificate e	exists in Active
Directory				
OK	(	Cancel	Apply	Help

**ステップ5:「**サブジェクト名」タブに**移動し**て、「要求**内の供給」が選択されていることを**確認 します。証明書の署名を取得するために管理者の承認が必要ないことを示すポップアップが表示 されたら、[OK]を選択**します**。

Properties of New Template					
Compatibility	General	Request	Handling	Cryptography	Key Attestation
Supersec	ded Templa	tes	Exte	ensions	Security
Subject N	lame	Sen	ver	Issuance Re	equirements
Supply in the request     Use subject information from existing certificates for autoenrollment     renewal requests (*)					
O Build from this Active Directory information					
Select this option to enforce consistency among subject names and to simplify certificate administration.					

**ステップ6:[**Extensions]タブに移動し、[Application Policies]オプシ**ョンを選択**し、[**Edit...]ボタンを** 選択します。[Application Policies]ウィ**ンドウにクラ**イアント認証が表示**されていることを確認**し ます。それ以外の場合は、[Add] を選択して追加します。

	Pro	perties	of New	Template	X		
Compatibility	General	Request	equest Handling Cryptography Key Attestati				
Subject N	Name	Ser	ver	Issuance Re	equirements		
Superse	ded Templa	tes	Exte	insions	Security		
To modify an extension, select it, and then click Edit.							
Applicat	ion Policies						
Edit Application Policies Extension							
An application policy defines how a certificate can be used.							
Application policies: Client Authentication Encrypting File System Secure Email							

ステップ7:[Security]タブに移動し、Windows ServerでSCEPサービスを有効にするステップ6で定 義したサービスアカウントにテンプレートのフルコントロール権限があることを確認して、 [Apply]、[OK]を選択します。

Compatibility General	1			
	Request	Handling	Cryptography	Key Attestation
Subject Name	Serv	er	Issuance Re	equirements
Superseded Temp	lates	Exte	ensions	Security
Group or user names:				
& Authenticated Us	ers			
Administrator				
B Domain Admins (	CHUU-DOM	AIN\Dom	ain Admins)	
😹 Domain Users (C	HUU-DOMA	IN\Domai	in Users)	
Senterprise Admin	s (CHUU-DO	MAIN\En	terprise Admins)	
		Г	Add	Remove
Permissions for Admini	strator		Allow	Deny
Full Control			>	
Read			>	
Write			✓	
Enroll			✓	
Autoenroll			✓	
For enabled normination	or advace	ad eatting	aliak	
Advanced. Advanced settings, click Advanced				

**ステップ8:[Certification Authority]ウ**ィンドウに戻り、[**Certificate Templates**]フォルダを右クリックし、[**New**] > [**Certificate Template to Issue]を選択します**。

**ステップ9:**前に作成した証明書テンプレートを選択します。この例では、9800-LSCです。次に、 [**OK**]を選択**します**。

**注**:新しく作成した証明書テンプレートは、すべてのサーバで複製する必要があるため、複数のサーバ展開でリストに表示するには時間がかかる場合があります。

	Enable Certificate Templates	X
Select one Certificate Template to Note: If a certificate template that information about this template has All of the certificate templates in the For more information, see <u>Cert</u>	enable on this Certification Authority. was recently created does not appear on this list, you may need to wait until been replicated to all domain controllers. e organization may not be available to your CA. <u>ifficate Template Concepts.</u>	
Name	Intended Purpose	~
9800-LSC     CA Exchange     Code Signing     Cross Certification Authority     Enrollment Agent     Enrollment Agent (Computer)     Exchange Signature Only     Exchange Liter	Client Authentication, Secure Email, Encrypting File System Private Key Archival Code Signing <all> Certificate Request Agent Certificate Request Agent Secure Email Secure Email</all>	=
Exchange Oser     IPSec     Key Recovery Agent     OCSP Response Signing	IP security IKE intermediate Key Recovery Agent OCSP Signing	<ul><li>✓</li></ul>

### 新しい証明書テンプレートが[証明書テンプレート]フォルダの内容**にリスト**されます。

💭 certsrv - [Cer	tification Authority (Local)\CHUU-WIN	N12-CA\Certificate Templates]	. 🗆 X
File Action View Help			
🗢 🔿 🙎 🙆 📓			
Certification Authority (Local)	Name 9800-LSC Authenticated Session Exchange Enrollment Agent (Offline r IPSec (Offline request) CEP Encryption Directory Email Replication Domain Controller Authentication Kerberos Authentication EFS Recovery Agent Basic EFS Domain Controller Web Server Computer User Subordinate Certification Authority Administrator	Intended Purpose Client Authentication, Secure Email, En Client Authentication Certificate Request Agent IP security IKE intermediate Certificate Request Agent Directory Service Email Replication Client Authentication, Server Authentic Client Authentication, Server Authentic File Recovery Encrypting File System Client Authentication, Server Authentic Server Authentication Client Authentication Client Authentication, Server Authentic Encrypting File System, Secure Email, Cl <all> Microsoft Trust List Signing, Encrypting</all>	

ステップ10:レジストリージエディタ(Registry Editor)ウィンドウに戻り、[Computer] >

[HKEY\_LOCAL\_MACHINE] > [SOFTWARE] > [Microsoft] > [Cryptography] > [MSCEP]に移動します。

**ステップ11**: EncryptionTemplate、GeneralPurposeTemplate、およびSignatureTemplateレジスト リを編集して、新しく作成された証明書テンプレートを指定します。

đ		Registry Editor		_ 🗆 🗙
File	Edit View Favorites Help			
	<ul> <li>CertificateTemplateCa</li> <li>Defaults</li> <li>MSCEP</li> <li>CAType</li> <li>CAType</li> <li>CertsInMYStore</li> <li>EnforcePassword</li> <li>PasswordVDir</li> <li>UseSinglePassworc</li> <li>OID</li> <li>Protect</li> <li>Providers</li> <li>Services</li> <li>UserInterface</li> <li>CTF</li> <li>DataAccess</li> <li>DevDiv</li> <li>Device Association Frame</li> <li>Dfrg</li> <li>DFS</li> <li>DHCPMibAgent</li> <li>DirectDraw</li> <li>DirectInput</li> </ul>	Name (Default) (Defa	Type REG_SZ REG_SZ REG_SZ	Data (value not set) 9800-LSC 9800-LSC 9800-LSC
<				>
Compi	uter\HKEY_LOCAL_MACHINE\SOFT	WARE\Microsoft\Crypto	ography\MSCEP	.:1

**ステップ12:**NDESサーバをリブートし、[**Certification Authority]ウィンドウに戻**り、サーバ名を選択し、[**Stop** and **Play**]ボタンを簡潔に選択します。

🦕 c	ertsrv - [Certification Authority (Local)\CHUU-WIN12-CA]
File Action View Help	> <b></b>
Certification Authority (Local)	Name         Revoked Certificates         Issued Certificates         Pending Requests         Failed Requests         Certificate Templates

9800デバイスのトラストポイントの設定

コントローラは、APがプロビジョニングされたら、APを認証するためにトラストポイントを定 義する必要があります。トラストポイントには、同じCAサーバ(この例ではMicrosoft CA)から 取得したCAルート証明書とともに、9800デバイス証明書が含まれます。 証明書をトラストポイ ントにインストールするには、サブジェクト属性とそれに関連付けられたRSA鍵のペアが含まれ ている必要があります。設定は、Webインターフェイスまたはコマンドラインを使用して実行さ れます。

ステップ1:[Configuration] > [Security] > [PKI Management]に移動し、[RSA Keypair Generation]タ ブを選択します。[+ Add]ボタンを選択します。

ステップ2:キーペアに関連付けられたラベルを定義し、[エクスポート可能(Exportable)]チェック ボックスが選択されていることを確認します。

onfiguration • > Security • >	PKI Management				
A Server RSA Keypair Gene	ration Trustpoin	t			
+ Add	_				
Key Label	Key Exportable	Zeroise RSA Key	(		
TP-self-signed-1997188793	No	E Zeroise	Key Label*	AP-LSC	
AP-KEY	Yes	2eroise	Madulua Cizat	2049	
chaincert.pfx	No	🗎 Zeroise	Modulus Size*	2040	
TP-self-signed-1997188793.serve	No	2 Zeroise	Key Exportable*		
CISCO_IDEVID_SUDI_LEGACY	No	2 Zeroise	D Cancel		✓ Generate
CISCO_IDEVID_SUDI	No	2 Zeroise	Contoch		Concrato
SLA-KeyPair	Yes	2 Zeroise			
SLA-KeyPair2	Yes	2 Zeroise			
ii i i ⊨ i 10	<ul> <li>items per page</li> </ul>	1 - 8 of 8 items			

ステップ1と2のCLI設定。この設定例では、ラベルAP-LSCとモジュラスサイズ2048ビットでキー ペアが生成されます。

9800-L(config) # crypto key generate rsa exportable general-keys modulus

The name for the keys will be: AP-LSC

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be exportable...
[OK] (elapsed time was 1 seconds)
フニップの目じょクション・ロズ 「トニフト ポイン・トルクブを認

**ステップ3**:同じセクション内で、[トラストポイ**ント]**タブを選択し、[+ Add]ボタン**を選択**します。

ステップ4:トラストポイントの詳細にデバイス情報を入力し、[Apply to Device]を選択します。

- [Label] フィールドは、トラストポイントに関連付けられた名前です
- ・登録URLの場合は、「Windows ServerでSCEPサービスを有効にする」セクションのステップ7で定義したURLを使用します
- [Authenticate]チェックボックスをオンにし、CA証明書をダウンロードします
- [ドメイン名]フィールドは、証明書要求の共通名属性として配置されます

- [Key Generated]チェ**ックボックス**をオンにすると、ドロップダウンメニューが表示され、ス テップ2で生成されたキーペアが選択されます
- [Enroll Trustpoint]チェックボ**ックスをオン**にすると、2つのパスワードフィールドが表示され ます。パスワードを入力します。これは、デバイス証明書とCA証明書で証明書キーをチェー ンするために使用されます

警告:9800コントローラはLSCインストールの多層サーバチェーンをサポートしていない ため、ルートCAは、コントローラとAPからの証明書要求に署名するルートCAである必要 があります。

Add Trustpoint				×
Label*	9800-LSC		Enrollment URL	certsrv/mscep/mscep.dll
Authenticate		_		
Subject Name				
Country Code	MX		State	CDMX
Location	Juarez		Organisation	Wireless TAC
Domain Name	chuu-domain.local		Email Address	jesuherr@cisco.com
Key Generated	<ul> <li>Image: A start of the start of</li></ul>	1		
Available RSA Keypairs	AP-LSC 🔻	)		
Enroll Trustpoint				
Password	•••••	]		
Re-Enter Password	******	]		
Cancel				Apply to Device

#### ステップ3と4のCLI設定:

**注意**:subject-name設定行は、LDAP構文でフォーマットする必要があります。フォーマットしない場合、コントローラで受け入れられません。

9800-L(config)#crypto pki trustpoint

```
9800-L(ca-trustpoint)#enrollment url http://
```

```
9800-L(ca-trustpoint)#rsakeypair
```

```
9800-L(ca-trustpoint)#revocation-check none
9800-L(ca-trustpoint)#exit
9800-L(config)#crypto pki authenticate
```

```
Certificate has the following attributes:
    Fingerprint MD5: E630EAE6 FB824658 690EB0F5 638D7224
    Fingerprint SHA1: 97070ACD CAD03D5D 0C1A6085 19992E0D 6B8C4D8B
* Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
9800-L(config)#crypto pki enroll <trustpoint name>
*
* 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.
Password:
Re-enter password:
* The subject name in the certificate will include: C=MX, ST=CDMX, L=Juarez, O=Wireless TAC,
```

CN=9800-L.chuu-domain.local/emailAddress=jesuherr@cisco.com
% The subject name in the certificate will include: 9800-L.alzavala.local
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose AP-LSC' commandwill show the fingerprint.

### AP登録パラメータと更新管理トラストポイントの定義

AP登録では、以前に定義したトラストポイントの詳細を使用して、コントローラが証明書要求を 転送するサーバの詳細を決定します。コントローラは証明書登録のプロキシとして使用されるた め、証明書要求に含まれるサブジェクトのパラメータを認識する必要があります。設定は、 Webインターフェイスまたはコマンドラインを使用して実行されます。

ステップ1:[Configuration] > [Wireless] > [Access Points]に移動し、[LSC Provision]メニューを展 開します。

ステップ2:AP証明書要求に入力された属性を[Subject Name Parameters]に入力し、[Apply]を選択 します。

### Subject Name Parameters

Country	MX
State	CDMX
City	Juarez
	·
Organisation	Cisco TAC
	·
Department	Wireless TAC
	1
Email Address	jesuherr@cisco.com
	1

ステップ1と2のCLI設定:

9800-L(config) **#ap lsc-provision subject-name-parameter country** 

**注**:9800 WLCでは属性が検証されないため、国番号などの2文字に制限されたサブジェクト 名パラメータは厳密に尊重する必要があります。 詳細については、不具合<u>CSCvo72999</u>を参照してください 参照として

**ステップ3**:同じメニュー内で、ドロップダウンリストから以前に定義したトラストポイントを選択し、AP加入の試行回数(MICを再度使用する前の加入試行回数を定義します)を指定し、証明 書キーサイズを設定します。次に、[Apply] をクリックします。

Status	Disabled •	Subject Name Parameters		🖺 Apply
Trustpoint Name	AP-LSC × •	P d d H d d s		
Number of Join Attemats	10	Country	MX	
Number of Join Alteripts		State	CDMX	
Key Size	2048 •	City	Juarez	
Add APs to LSC Provision				
List		Organisation	Cisco TAC	

ステップ3のCLI設定:

9800-L(config)#ap lsc-provision join-attempt

9800-L(config)#ap lsc-provision trustpoint

```
9800-L(config)#ap lsc-provision key-size
```

ステップ4:(オプション)コントローラに加入しているすべてのAPまたはMACアドレスリストに 定義されている特定のAPに対して、APLSCプロビジョニングをトリガーできます。同じメニュ ーで、テキストフィールドにAPイーサネットMACアドレスをxxxx.xxxxの形式で入力し、 +記号をクリックします。または、APのMACアドレスを含むcsvファイルをアップロードし、フ ァイルを選択してから[ファイルのアップロード]を選択します。

**注**:コントローラは、CSVファイル内で、参加しているAPリストから認識されないMACア ドレスをスキップします。

Add APs to LSC Provision List

	Select File		
	Select CSV File		
AP MAC Address	Q Enter MAC/Sear	+	
APs in Provision List :	1		
	286f.7fcf.53ac	Û	
	286f.7fcf.53ac	Û	

ステップ4のCLI設定:

**ステップ 5**: [Status]ラベルの横のドロップダウンメニューから[Enabled]または[Provision List]を 選択して、[Apply to Trigger AP LSC enrollement]をクリックします。

注:APは、証明書要求、ダウンロード、およびインストールを開始します。証明書が完全 にインストールされると、APはリブートし、新しい証明書を使用して加入プロセスを開始 します。

**ヒント**:プロビジョンリストとともに実稼働前のコントローラを使用してAP LSCプロビジ ョニングを行う場合は、証明書がプロビジョニングされたらAPエントリを削除しないでく ださい。これを行い、APがMICにフォールバックして同じ実稼働前コントローラに加入す ると、LSC証明書が消去されます。

Status Enabled	<ul> <li>LSC Provision</li> </ul>				
	Status	Enabled	•	Subject Name	

ステップ5のCLI設定:

9800-L(config)#ap lsc-provision

In Non-WLANCC mode APs will be provisioning with RSA certificates with specified key-size configuration. In WLANCC mode APs will be provisioning with EC certificates with a 384 bit key by-default or 256 bit key if configured.

Are you sure you want to continue? (y/n): y If specific AP list provisioning is preferred then use: 9800-L(config)#ap lsc-provision provision-list

**ステップ6:[Configuration] > [Interface] > [Wireless]に移動し**て、管理インターフェイスを選択しま す。[トラストポイント]フィールドで、ドロップダウンメニューから新しいトラストポイントを選 択し、[Update & Apply to Device]をクリックします。

注意:LSCが有効で、9800 WLCのトラストポイントがMICまたはSSCを参照している場合 、APは設定された数の加入の試行に対してLSCへの加入を試行します。最大試行回数に達 すると、APはMICにフォールバックして再度参加しますが、LSCプロビジョニングが有効 になっているため、APは新しいLSCを要求します。これにより、CAサーバが同じAPに対し て常に証明書に署名し、APがjoin-request-rebootループに留まるというループが発生します。

注:LSC証明書を使用するように管理トラストポイントが更新されると、新しいAPは MICを使用してコントローラに参加できなくなります。現在、プロビジョニングウィンドウ を開くサポートはありません。新しいAPをインストールする必要がある場合は、管理トラ ストポイント内のAPと同じCAによって署名されたLSCを事前にプロビジョニングしておく 必要があります。

Edit Management Interface		×
Interface	Vlan2622 🔻	
Trustpoint	AP-LSC X V	
NAT Status	DISABLED	
Cancel	📑 Update	& Apply to Device

ステップ6のCLI設定:

9800-L(config)#wireless management trustpoint



### コントローラ証明書のインストールの確認

9800 WLCトラストポイントにLSC情報があることを確認するために、**show crypto pki certificates verbose <trustpoint name>コマンドを発行します。**2つの証明書が、LSCのプロビジョ ニングと登録のために作成されたトラストポイントに関連付けられます。この例では、トラスト 9800-L#show crypto pki certificates verbose microsoft-ca Certificate Status: Available Version: 3 Certificate Usage: General Purpose Issuer: cn=CHUU-WIN12-CA dc=chuu-domain dc=local Subject: Name: 9800-L.alzavala.local cn=9800-L.chuu-domain.local/emailAddress=jesuherr@cisco.com o=Wireless TAC l=Juarez st=CDMX c=MX hostname=9800-L.alzavala.local CRL Distribution Points: ldap:///CN=CHUU-WIN12-CA,CN=Chuu-Win12, CN=CDP, CN=Public%20Key%20Services, CN=Services, CN=Coint Validity Date: start date: 04:25:59 Central May 11 2020 end date: 04:25:59 Central May 11 2022 Subject Key Info: Public Key Algorithm: rsaEncryption RSA Public Key: (2048 bit) Signature Algorithm: SHA256 with RSA Encryption [...] Authority Info Access: CA ISSUERS: ldap:///CN=CHUU-WIN12-CA, CN=AIA, CN=Public%20Key%20Services, CN=Services, CN=Configuration, DC=chuudomain, DC=local?cACertificate?base?objectClass=certificationAuthority [...] CA Certificate Status: Available Version: 3 Certificate Serial Number (hex): 37268ED56080CB974EF3806CCACC77EC Certificate Usage: Signature Issuer: cn=CHUU-WIN12-CA dc=chuu-domain dc=local Subject: cn=CHUU-WIN12-CA dc=chuu-domain dc=local Validity Date: start date: 05:58:01 Central May 10 2019 end date: 06:08:01 Central May 10 2024 Subject Key Info: Public Key Algorithm: rsaEncryption RSA Public Key: (2048 bit) Signature Algorithm: SHA256 with RSA Encryption

#### 9800 WLC LSC設定の確認

ワイヤレス管理トラストポイントに関する詳細を確認するには、show wireless management trustpointコマンドを実行して、正しいトラストポイント(LSCの詳細を含むトラストポイント、 この例ではAP-LSC)が使用中であり、[Available:

9800-L#show wireless management trustpoint

AP LSCプロビジョニング設定に関する詳細を、プロビジョンリストに追加されたAPのリストと

ともに確認するには、show ap lsc-provision summary**コマンドを実行し**ます。正しいプロビジョ ニング状態が表示されていることを確認します。

9800-L#show ap lsc-provision summary AP LSC-provisioning : Enabled for all APs Trustpoint used for LSC-provisioning : AP-LSC LSC Revert Count in AP reboots : 10

#### **AP LSC Parameters :**

Country : MX State : CDMX City : Juarez Orgn : Cisco TAC Dept : Wireless TAC Email : josuvill@cisco.com Key Size : 2048 EC Key Size : 384 bit

AP LSC-provision List :

Total number of APs in provision list: 2

Mac Addresses : -----xxxx.xxxx.xxxx xxxx.xxxx.xxxx

### アクセスポイント証明書のインストールの確認

APにインストールされている証明書を確認するには、AP CLIから**show crypto**コマンドを実行し 、CAルート証明書とデバイス証明書の両方が存在することを確認します(出力には関連するデー タだけが表示されます)。

AP3802#**show crypto** 

[...] ----- LSC: Enabled ----- Device Certificate -----Certificate: Data: Version: 3 (0x2) Serial Number: 73:00:00:00:0b:9e:c4:2e:6c:e1:54:84:96:00:00:00:00:00:0b Signature Algorithm: sha256WithRSAEncryption Issuer: DC=local, DC=chuu-domain, CN=CHUU-WIN12-CA Validity Not Before: May 13 01:22:13 2020 GMT Not After : May 13 01:22:13 2022 GMT Subject: C=MX, ST=CDMX, L=Juarez, O=Cisco TAC, CN=ap3g3-286F7FCF53AC/emailAddress=josuvill@cisco.com Subject Public Key Info: Public Key Algorithm: rsaEncryption Public-Key: (2048 bit) ----- Root Certificate -----Certificate: Data: Version: 3 (0x2) Serial Number: 32:61:fb:93:a8:0a:4a:97:42:5b:5e:32:28:29:0d:32

```
Signature Algorithm: sha256WithRSAEncryption

Issuer: DC=local, DC=chuu-domain, CN=CHUU-WIN12-CA

Validity

Not Before: May 10 05:58:01 2019 GMT

Not After : May 10 05:58:01 2024 GMT

Subject: DC=local, DC=chuu-domain, CN=CHUU-WIN12-CA

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

スイッチポートdot1x認証用のLSCが使用されている場合、APからポート認証が有効になってい
```

人イッナホートdot1x認証用のLSCか使用されている場合、APからホート認証か有効になってい るかどうかを確認できます。

AP3802#**show ap authentication status** AP dot1x feature is disabled.

> **注**:APのポートdot1xを有効にするには、APプロファイルまたはダミー値を使用したAP設 定自体で、APのdot1xクレデンシャルを定義する必要があります。

## トラブルシュート

#### 一般的な問題

- 1. テンプレートがサーバレジストリに正しくマッピングされていない場合、またはサーバにパ スワードのチャレンジが必要な場合は、9800 WLCまたはAPの証明書要求は拒否されます。
- IISのデフォルトサイトが無効になっている場合、SCEPサービスも無効になっているため、 トラストポイントで定義されたURLに到達できず、9800 WLCは証明書要求を送信しません
   。
- 3. サーバと9800 WLCの間で時刻が同期されていない場合、時刻の妥当性チェックが失敗する ため、証明書はインストールされません。

#### debugおよびlogコマンド

9800コントローラ証明書の登録をトラブルシューティングするには、次のコマンドを使用します 。

9800-L#debug crypto pki transactions 9800-L#debug crypto pki validation 9800-L#debug crypto pki scep AP登録のトラブルシューティングと監視には、次のコマンドを使用します。

AP3802#debug capwap client payload AP3802#debug capwap client events APコマンドラインから、show loggingは、APに証明書のインストールに問題があったかどうかを 表示し、証明書がインストールされなかった理由の詳細を表示します。

[...]
Mar 19 19:39:13 kernel: \*03/19/2020 19:39:13.3429] AP has joined controller 9800-L Mar 19
19:39:13 kernel: 03/19/2020 19:39:13.3500] SELinux: initialized (dev mtd\_inodefs, type
mtd\_inodefs), not configured for labeling Mar 19 19:39:13 kernel: \*03/19/2020 19:39:13.5982]

Generating a RSA private key Mar 19 19:39:14 kernel: \*03/19/2020 19:39:13.5989] ..... Mar 19 19:39:15 kernel: \*03/19/2020 19:39:14.4179] .. Mar 19 19:39:15 kernel: \*03/19/2020 19:39:15.2952] writing new private key to '/tmp/lsc/priv\_key' Mar 19 19:39:15 kernel: \*03/19/2020 19:39:15.2955] ----- Mar 19 19:39:15 kernel: \*03/19/2020 19:39:15.5421] cen\_validate\_lsc: Verification failed for certificate: Mar 19 19:39:15 kernel: \*03/19/2020 19:39:15.5421] countryName = MX Mar 19 19:39:15 kernel: \*03/19/2020 19:39:15.5421] stateOrProvinceName = CDMX Mar 19 19:39:15 kernel: \*03/19/2020 19:39:15.5421] localityName = Juarez Mar 19 19:39:15 kernel: \*03/19/2020 19:39:15.5421] organizationName = cisco-tac Mar 19 19:39:15 kernel: \*03/19/2020 19:39:15.5421] commonName = ap3g3- Mar 19 19:39:15 kernel: \*03/19/2020 19:39:15.5421] emailAddress = jesuherr@cisco.com Mar 19 19:39:15 kernel: \*03/19/2020 19:39:15.5427] LSC certificates/key failed validation! Mar 19 19:39:15 kernel: \*03/19/2020 19:39:15.5427]

#### 登録の成功例

#### これは、コントローラとそれに関連するAPの両方の登録が成功した場合の、前述のデバッグの出 力です。

#### 9800 WLCへのCAルート証明書のインポート:

#### [...]

Certificate has the following attributes: Fingerprint MD5: E630EAE6 FB824658 690EB0F5 638D7224 Fingerprint SHA1: 97070ACD CAD03D5D 0C1A6085 19992E0D 6B8C4D8B % Do you accept this certificate? [yes/no]: yes CRYPTO\_PKI\_SCEP: Client sending GetCACert request CRYPTO\_PKI: Sending CA Certificate Request: GET /certsrv/mscep/mscep.dll/pkiclient.exe?operation=GetCACert&message=AP-LSC HTTP/1.0 User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI) Host: 172.16.80.8 CRYPTO\_PKI: locked trustpoint AP-LSC, refcount is 1 CRYPTO\_PKI: http connection opened CRYPTO\_PKI: Sending HTTP message CRYPTO\_PKI: Reply HTTP header: HTTP/1.0 User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI) Host: 172.16.80.8 CRYPTO\_PKI: unlocked trustpoint AP-LSC, refcount is 0 CRYPTO\_PKI: locked trustpoint AP-LSC, refcount is 1 CRYPTO\_PKI: Header length received: 192 CRYPTO\_PKI: parse content-length header. return code: (0) and content-length : (3638) CRYPTO\_PKI: Complete data arrived CRYPTO\_PKI: unlocked trustpoint AP-LSC, refcount is 0 CRYPTO\_PKI: Reply HTTP header: HTTP/1.1 200 OK Content-Type: application/x-x509-ca-ra-cert Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Tue, 19 May 2020 21:47:34 GMT Connection: close Content-Length: 3638 Content-Type indicates we have received CA and RA certificates. CRYPTO\_PKI\_SCEP: Client received CA and RA certificate CRYPTO\_PKI:crypto\_process\_ca\_ra\_cert(trustpoint=AP-LSC) The PKCS #7 message contains 3 certificates. CRYPTO\_PKI:crypto\_pkcs7\_extract\_ca\_cert found cert CRYPTO\_PKI: Bypassing SCEP

[...] CRYPTO\_PKI: using private key AP-LSC for enrollment CRYPTO\_PKI\_SCEP: Client sending GetCACert request CRYPTO\_PKI: Sending CA Certificate Request: GET /certsrv/mscep/mscep.dll/pkiclient.exe?operation=GetCACert&message=AP-LSC HTTP/1.0 User-Agent:

#### 9800 WLCデバイス登録:

crypto\_pki\_get\_cert\_record\_by\_cert() CRYPTO\_PKI: crypto\_pki\_authenticate\_tp\_cert() CRYPTO\_PKI: trustpoint AP-LSC authentication status = 0 Trustpoint CA certificate accepted.

Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI) Host: 172.16.80.8 CRYPTO\_PKI: locked trustpoint AP-LSC, refcount is 1 CRYPTO\_PKI: http connection opened CRYPTO\_PKI: Sending HTTP message CRYPTO\_PKI: Reply HTTP header: HTTP/1.0 User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI) Host: 172.16.80.8 CRYPTO\_PKI: unlocked trustpoint AP-LSC, refcount is 0 CRYPTO\_PKI: locked trustpoint AP-LSC, refcount is 1 CRYPTO\_PKI: Header length received: 192 CRYPTO\_PKI: parse content-length header. return code: (0) and content-length : (3638) CRYPTO\_PKI: Complete data arrived CRYPTO\_PKI: unlocked trustpoint AP-LSC, refcount is 0 CRYPTO\_PKI: Reply HTTP header: HTTP/1.1 200 OK Content-Type: application/x-x509-ca-ra-cert Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Tue, 19 May 2020 21:48:33 GMT Connection: close Content-Length: 3638 Content-Type indicates we have received CA and RA certificates. CRYPTO\_PKI\_SCEP: Client received CA and RA certificate CRYPTO\_PKI:crypto\_process\_ca\_ra\_cert(trustpoint=AP-LSC) The PKCS #7 message

contains 3 certificates. CRYPTO\_PKI:crypto\_pkcs7\_insert\_ra\_certs found RA certs

certificate received. CRYPTO\_PKI: CA certificate received. CRYPTO\_PKI:

capabilities request 0 CRYPTO\_PKI: transaction CRYPTO\_REQ\_CA\_CERT completed CRYPTO\_PKI: CA

CRYPTO\_PKI:crypto\_pkcs7\_insert\_ra\_certs found RA certs CRYPTO\_PKI\_SCEP: Client Sending GetCACaps request with msg = GET /certsrv/mscep/mscep.dll/pkiclient.exe?operation=GetCACaps&message=AP-LSC HTTP/1.0 User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI) Host: 172.16.80.8 CRYPTO\_PKI: locked trustpoint AP-LSC, refcount is 1 CRYPTO\_PKI: http connection opened CRYPTO\_PKI: Sending HTTP message CRYPTO\_PKI: Reply HTTP header: HTTP/1.0 User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI) Host: 172.16.80.8 CRYPTO\_PKI: unlocked trustpoint AP-LSC, refcount is 0 CRYPTO\_PKI: locked trustpoint AP-LSC, refcount is 1 CRYPTO\_PKI: Header length received: 171 CRYPTO\_PKI: parse content-length header. return code: (0) and content-length : (34) CRYPTO\_PKI: Complete data arrived CRYPTO\_PKI: unlocked trustpoint AP-LSC, refcount is 0 CRYPTO\_PKI: Reply HTTP header: HTTP/1.1 200 OK Content-Type: text/plain Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Tue, 19 May 2020 21:48:33 GMT Connection: close Content-Length: 34 CRYPTO\_PKI: HTTP header content length is 34 bytes CRYPTO\_PKI\_SCEP: Server returned capabilities: 92 CA\_CAP\_RENEWAL CA\_CAP\_S alz\_9800(config)#HA\_1 CA\_CAP\_SHA\_256 CA\_CAP\_SHA\_512 CRYPTO\_PKI: transaction CRYPTO\_REQ\_CERT completed CRYPTO\_PKI: status: %PKI-6-CSR\_FINGERPRINT: CSR Fingerprint MD5 : 9BFBA438303487562E888087168F05D4 CSR Fingerprint SHA1: 58DC7DB84C632A7307631A97A6ABCF65A3DEFEEF CRYPTO\_PKI: Certificate Request Fingerprint MD5: 9BFBA438 30348756 2E888087 168F05D4 CRYPTO\_PKI: Certificate Request Fingerprint SHA1: 58DC7DB8 4C632A73 07631A97 A6ABCF65 A3DEFEEF PKI:PKCS7 to issuer cn=CHUU-WIN12-CA,dc=chuu-domain,dc=local serial 18 00 00 00 38 DB 68 64 CO 52 CO 0F 0E 00 00 00 00 38 CRYPTO PKI: Deleting cached key having key id 65 CRYPTO\_PKI: Attempting to insert the peer's public key into cache CRYPTO\_PKI: Peer's public inserted successfully with key id 66 CRYPTO\_PKI: Expiring peer's cached key with key id 66 PKI: Trustpoint AP-LSC has no router cert PKI: Signing pkcs7 with AP-LSC trustpoint temp self-signed cert CRYPTO\_PKI\_SCEP: Client sending PKCSReq CRYPTO\_PKI: locked trustpoint AP-LSC, refcount is 1 CRYPTO\_PKI: http connection opened CRYPTO\_PKI: Sending HTTP message CRYPTO\_PKI: Reply HTTP header: HTTP/1.0 Host: 172.16.80.8 CRYPTO\_PKI: unlocked trustpoint AP-LSC, refcount is 0 CRYPTO\_PKI: locked trustpoint AP-LSC, refcount is 1 CRYPTO\_PKI: locked trustpoint AP-LSC, refcount is 2 CRYPTO\_PKI: Header length received: 188 CRYPTO\_PKI: parse content-length header. return code: (0) and content-length : (2807) CRYPTO\_PKI: Complete data arrived CRYPTO\_PKI: unlocked trustpoint AP-LSC, refcount is 1 CRYPTO\_PKI: received msg of 2995 bytes CRYPTO\_PKI: Reply HTTP header: HTTP/1.1 200 OK Content-Type: application/x-pkimessage Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Tue, 19 May 2020 21:48:33 GMT Connection: close Content-Length: 2807 CRYPTO\_PKI: Prepare global revocation service providers CRYPTO\_PKI: Deleting cached key having key id 66 CRYPTO\_PKI: Attempting to insert the peer's public key into cache CRYPTO\_PKI:Peer's public inserted successfully with key id 67 CRYPTO\_PKI: Expiring peer's cached key with key id 67 CRYPTO\_PKI: Remove global revocation service providers The PKCS #7 message has 1 verified signers. signing cert: issuer cn=CHUU-WIN12-CA,dc=chuudomain,dc=local serial 1800037A239DF5180C0672C0000037 Signed Attributes: CRYPTO PKI SCEP: Client received CertRep - GRANTED (AF58BA9313638026C5DC151AF474723F) CRYPTO PKI: status = 100: certificate is granted The PKCS #7 message contains 1 certs and 0 crls. Newly-issued Router Cert: issuer=cn=CHUU-WIN12-CA,dc=chuu-domain,dc=local serial=1800043245DC93E1D943CA70000043 start date: 21:38:34 Central May 19 2020 end date: 21:38:34 Central May 19 2022 Router date: 21:48:35 Central May 19 2020 %PKI-6-CERT\_INSTALL: An ID certificate has been installed under Trustpoint : AP-LSC Issuer-name : cn=CHUU-WIN12-CA,dc=chuu-domain,dc=local Subject-name : cn=9800-L.chuu-domain.local/emailAddress=jesuherr@cisco.com,o=Wireless

TAC,l=Juarez,st=CDMX,c=MX,hostname=alz\_9800.alzavala.local Serial-number:

1800000043245DC93E1D943CA700000000043 End-date : 2022-05-19T21:38:34Z Received router cert from CA CRYPTO\_PKI: Not adding alz\_9800.alzavala.local to subject-alt-name field because : Character allowed in the domain name. Calling pkiSendCertInstallTrap to send alert CRYPTO\_PKI: All enrollment requests completed for trustpoint AP-LSC

#### コントローラ側からのAP登録デバッグ出力では、9800 WLCに加入しているAPごとに、次の出力 が複数回繰り返されます。

#### [...]

CRYPTO\_PKI: (A6964) Session started - identity selected (AP-LSC) CRYPTO\_PKI: Doing re-auth to fetch RA certificate. CRYPTO\_PKI\_SCEP: Client sending GetCACert request CRYPTO\_PKI: Sending CA Certificate Request: GET /certsrv/mscep/mscep.dll/pkiclient.exe?operation=GetCACert&message=AP-LSC HTTP/1.0 User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI) Host: 172.16.80.8 CRYPTO\_PKI: locked trustpoint AP-LSC, refcount is 2 CRYPTO\_PKI: http connection opened CRYPTO\_PKI: Sending HTTP message CRYPTO\_PKI: Reply HTTP header: HTTP/1.0 User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI) Host: 172.16.80.8 CRYPTO\_PKI: unlocked trustpoint AP-LSC, refcount is 1 CRYPTO\_PKI: locked trustpoint AP-LSC, refcount is 2 CRYPTO\_PKI: Header length received: 192 CRYPTO\_PKI: parse content-length header. return code: (0) and content-length : (3638) CRYPTO\_PKI: Complete data arrived CRYPTO\_PKI: unlocked trustpoint AP-LSC, refcount is 1 CRYPTO\_PKI: Reply HTTP header: HTTP/1.1 200 OK Content-Type: application/x-x509-ca-ra-cert Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Tue, 19 May 2020 21:51:03 GMT Connection: close Content-Length: 3638 Content-Type indicates we have received CA and RA certificates. CRYPTO\_PKI\_SCEP: Client received CA and RA certificate

CRYPTO\_PKI:crypto\_process\_ca\_ra\_cert(trustpoint=AP-LSC) The PKCS #7 message contains 3 certificates. CRYPTO\_PKI:crypto\_pkcs7\_insert\_ra\_certs found RA certs

CRYPTO PKI:crypto\_pkcs7\_insert\_ra\_certs found RA\_certs CRYPTO\_PKI: Capabilites already obtained CA\_CAP\_RENEWAL CA\_CAP\_SHA\_1 CA\_CAP\_SHA\_256 CA\_CAP\_SHA\_512 PKCS10 request is compulsory CRYPTO\_PKI: byte 2 in key usage in PKCS#10 is 0x5 May 19 21: alz\_9800(config)#51:04.985: CRYPTO\_PKI: all usage CRYPTO\_PKI: key\_usage is 4 CRYPTO\_PKI: creating trustpoint clone Proxy-AP-LSC8 CRYPTO\_PKI: Creating proxy trustpoint Proxy-AP-LSC8 CRYPTO\_PKI: Proxy enrollment request trans id = 7CBB299A2D9BC77DBB1A8716E6474C0C CRYPTO\_PKI: Proxy forwading an enrollment request CRYPTO\_PKI: using private key AP-LSC for enrollment CRYPTO\_PKI: Proxy send CA enrollment request with trans id: 7CBB299A2D9BC77DBB1A8716E6474C0C CRYPTO\_PKI: No need to re-auth as we have RA in place CRYPTO\_PKI: Capabilites already obtained CA\_CAP\_RENEWAL CA\_CAP\_SHA\_1 CA\_CAP\_SHA\_256 CA\_CAP\_SHA\_512 CRYPTO\_PKI: transaction CRYPTO\_REQ\_CERT completed CRYPTO\_PKI: status: PKI:PKCS7 to issuer cn=CHUU-WIN12-CA,dc=chuu-domain,dc=local serial 18 00 00 00 38 DB 68 64 C0 52 C0 OF 0E 00 00 00 00 00 38 CRYPTO PKI: Deleting cached key having key id 67 CRYPTO PKI: Attempting to insert the peer's public key into cache CRYPTO\_PKI:Peer's public inserted successfully with key id 68 CRYPTO\_PKI: Expiring peer's cached key with key id 68 PKI: Trustpoint Proxy-AP-LSC8 has no router cert and loaded PKI: Signing pkcs7 with Proxy-AP-LSC8 trustpoint temp self-signed cert CRYPTO\_PKI\_SCEP: Client sending PKCSReq CRYPTO\_PKI: locked trustpoint Proxy-AP-LSC8, refcount is 2 CRYPTO\_PKI: http connection opened CRYPTO\_PKI: Sending HTTP message CRYPTO\_PKI: Reply HTTP header: HTTP/1.0 Host: 172.16.80.8 CRYPTO\_PKI: unlocked trustpoint Proxy-AP-LSC8, refcount is 1 CRYPTO\_PKI: locked trustpoint Proxy-AP-LSC8, refcount is 2 CRYPTO\_PKI: locked trustpoint Proxy-AP-LSC8, refcount is 3 CRYPTO\_PKI: Header length received: 188 CRYPTO\_PKI: parse content-length header. return code: (0) and content-length : (2727) CRYPTO\_PKI: Complete data arrived CRYPTO\_PKI: unlocked trustpoint Proxy-AP-LSC8, refcount is 2 CRYPTO\_PKI: received msg of 2915 bytes CRYPTO\_PKI: Reply HTTP header: HTTP/1.1 200 OK Content-Type: application/x-pki-message Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Tue, 19 May 2020 21:51:03 GMT Connection: close Content-Length: 2727 CRYPTO\_PKI: Prepare global revocation service providers CRYPTO\_PKI: Deleting cached key having key id 68 CRYPTO\_PKI: Attempting to insert the peer's public key into cache CRYPTO\_PKI:Peer's public inserted successfully with key id 69 CRYPTO\_PKI: Expiring peer's cached key with key id 69 CRYPTO\_PKI: Remove global revocation service providers The PKCS #7 message has 1 alz\_9800(config)# verified signers. signing cert: issuer cn=CHUU-WIN12-CA,dc=chuudomain,dc=local serial 1800037A239DF5180C0672C0000037 Signed Attributes: CRYPTO PKI SCEP: Client received CertRep - GRANTED (7CBB299A2D9BC77DBB1A8716E6474C0C) CRYPTO\_PKI: status = 100: certificate is granted The PKCS #7 message contains 1 certs and 0 crls. Received router cert from CA CRYPTO\_PKI: Enrollment poroxy callback status: CERT\_REQ\_GRANTED CRYPTO\_PKI: Proxy received router cert from CA CRYPTO\_PKI: Rcvd request to end PKI session A6964. CRYPTO\_PKI: PKI session A6964 has ended. Freeing all resources. CRYPTO\_PKI: unlocked trustpoint AP-LSC, refcount is 0 CRYPTO\_PKI: Cleaning RA certificate for TP : AP-LSC CRYPTO\_PKI: All enrollment requests completed for trustpoint Proxy-AP-LSC8. CRYPTO\_PKI: All enrollment requests completed for trustpoint Proxy-AP-LSC8. CRYPTO\_PKI: unlocked trustpoint Proxy-AP-LSC8, refcount is 1 CRYPTO\_PKI: All enrollment requests completed for trustpoint Proxy-AP-LSC8. CRYPTO\_CS: removing trustpoint clone Proxy-AP-LSC8

#### AP側からのAP登録デバッグ出力:

[DEC] CAPWAP\_CONFIGURATION\_UPDATE\_REQUEST(7) seq 40 len 407 ..Vendor Type: SPAM\_VENDOR\_ID\_PAYLOAD(104) vendId 409600 ...Vendor SubType: CERTIFICATE\_PARAMETER\_PAYLOAD(63) vendId 409600 LSC set retry number from WLC: 1

Generating a RSA private key

writing new private key to '/tmp/lsc/priv\_key'
----[ENC] CAPWAP\_WTP\_EVENT\_REQUEST(9)
...Vendor SubType: LSC\_CERTIFICATE\_PAYLOAD(64) Len 1135 Total 1135
[ENC] CAPWAP\_CONFIGURATION\_UPDATE\_RESPONSE(8)

.Msg Elem Type: CAPWAP\_MSGELE\_RESULT\_CODE(33) Len 8 Total 8 [DEC] CAPWAP\_CONFIGURATION\_UPDATE\_REQUEST(7) seq 41 len 20 ..Vendor Type: SPAM\_VENDOR\_ID\_PAYLOAD(104) vendId 409600 ...Vendor SubType: LSC\_CERTIFICATE\_PAYLOAD(64) vendId 409600 LSC\_CERT\_ENROLL\_PENDING from WLC

[ENC] CAPWAP\_CONFIGURATION\_UPDATE\_RESPONSE(8) .Msg Elem Type: CAPWAP\_MSGELE\_RESULT\_CODE(33) Len 8 Total 8 Received Capwap watchdog update msg. [DEC] CAPWAP\_CONFIGURATION\_UPDATE\_REQUEST(7) seq 42 len 1277 ..Vendor Type: SPAM\_VENDOR\_ID\_PAYLOAD(104) vendId 409600 ...Vendor SubType: LSC\_CERTIFICATE\_PAYLOAD(64) vendId 409600 LSC\_ENABLE: saving ROOT\_CERT

[ENC] CAPWAP\_CONFIGURATION\_UPDATE\_RESPONSE(8) .Msg Elem Type: CAPWAP\_MSGELE\_RESULT\_CODE(33) Len 8 Total 8 [DEC] CAPWAP\_CONFIGURATION\_UPDATE\_REQUEST(7) seq 43 len 2233 ..Vendor Type: SPAM\_VENDOR\_ID\_PAYLOAD(104) vendId 409600 ...Vendor SubType: LSC\_CERTIFICATE\_PAYLOAD(64) vendId 409600 LSC\_ENABLE: saving DEVICE\_CERT

SC private key written to hardware TAM

root: 2: LSC enabled AP Rebooting: Reset Reason - LSC enabled これで、SCEPによるLSC登録の設定例は終了です。