

在无线局域网控制器上局部重要的证书的配置示例

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Conventions](#)

[局部重要的证书](#)

[在无线局域网控制器\(WLCs\)的认证设置](#)

[在LWAPP AP的认证设置](#)

[在无线局域网控制器\(WLCs\)和轻量级接入点\(膝部\)的LSC技术支持](#)

[Configure](#)

[网络设置](#)

[CA和SCEP设置进程](#)

[通过GUI配置无线局域网控制器](#)

[通过CLI配置无线局域网控制器](#)

[Verify](#)

[Troubleshoot](#)

[Related Information](#)

[Introduction](#)

本文解释如何配置无线局域网控制器(WLC)和轻量级接入点(膝部)使用局部重要的认证功能。此功能被引入无线局域网控制器版本5.2。使用此功能，如果选择控制公共密钥基础设施(PKI)，您在接入点和控制器能生成局部重要的证书(LSC)。这些证书可能然后用于相互验证WLC和LAP。

[Prerequisites](#)

[Requirements](#)

尝试进行此配置之前，请确保满足以下要求：

- 知识如何配置WLC、LAP和无线客户端卡基本操作的
- 知识如何配置和使用微软视窗2003 CA服务器
- 公共钥匙结构和数字证书知识

[Components Used](#)

本文档中的信息基于以下软件和硬件版本：

- 运行固件5.2的Cisco 4400系列WLC
- Cisco Aironet 1130 AG系列轻量级接入点(LAP)
- 作为认证机关服务器被配置的作为域控制器和微软视窗2003服务器。
- 运行固件 4.2 版的 Cisco Aironet 802.11 a/b/g 客户端适配器
- Cisco Aironet Desktop软件(ADU)该运行固件版本4.2

The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to [Cisco Technical Tips Conventions](#) for more information on document conventions.

局部重要的证书

在控制器软件版本中早于5.2.157.0，控制器能使用自署名的认证(SSCs)验证接入点或发送授权信息到RADIUS服务器，如果接入点有出厂时安装的证书(MICs)。在控制器软件版本5.2.157.0中，您能配置控制器使用一个本地重大的认证(LSC)。如果希望您自己的公共密钥基础设施(PKI)提供更好的安全，您能使用LSC;有您的Certificate Authority (CA)控制和定义策略、限制和使用方法在生成的证书。

新的LSC证书在控制器需要首先然后设置从Certificate Authority (CA)服务器的LAP。

LAP与控制器(WLC)联络有CAPWAP协议的。必须从WLC起所有请求签署认证和发行CA证书LAP的和WLC的。LAP不直接地与CA服务器联络。WLC正常运行作为CA代理对LWAPP的AP。在WLC必须配置CA服务器详细资料，并且一定可及的。

控制器利用简单认证登记协议(SCEP)转发在设备生成的certReqs对CA并且再利用SCEP从CA获得签名的证书。

SCEP是公共密钥基础设施(PKI)客户端和认证机关服务器使用支持证书登记和撤销的证书管理协议。在Cisco中是用途广泛并且许多CA服务器支持它。在SCEP协议，HTTP使用作为传输协议PKI消息。SCEP的主要目标是证书安全的出版物到网络设备。SCEP有能力在许多操作上，但是对于此项目和版本，SCEP为这些操作使用。

- CA和RA公开密钥分发
- 证书登记

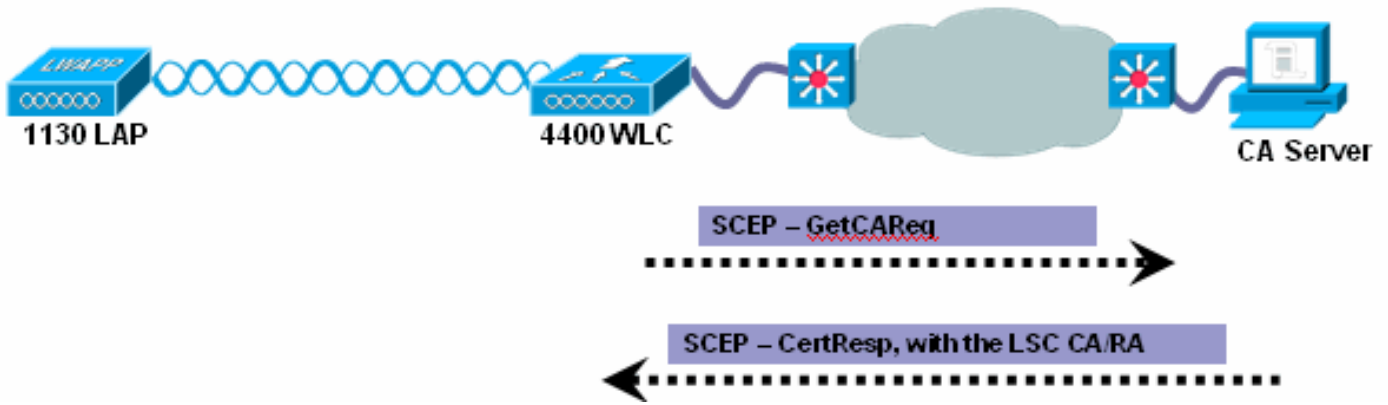
所有SCEP事务在自动化模式下发生。不支持认证吊销。

Note: 为网桥模式被配置的接入点不支持LSCs。

在无线局域网控制器(WLCs)的认证设置

必须在控制器上安装新的LSC证书，CA和设备证书。

使用SCEP协议，CA证书从CA服务器被接受。从这时，没有证书在控制器，此操作是确切获得操作。这些在控制器上安装。当APs配置有LSCs时，这些同样CA证书也被推进对APs。



设备证书登记操作

对于LAP和请求CA签名的证书的控制器， certRequest被发送作为PKCS-10消息。certRequest包含请求方的PrivateKey和其他属性将包括在X.509证书和数字式地签字的主题名称、Publickey。必须发送这些到CA，变换certRequest成X.509证书。

接受certRequest—的PKCS-10的CA要求其他信息验证请求方身份和验证请求是未改变的。与其他途径一起的许多时期PKCS-10，例如PKCS-7，发送和接受Cert Reqs/Resps。

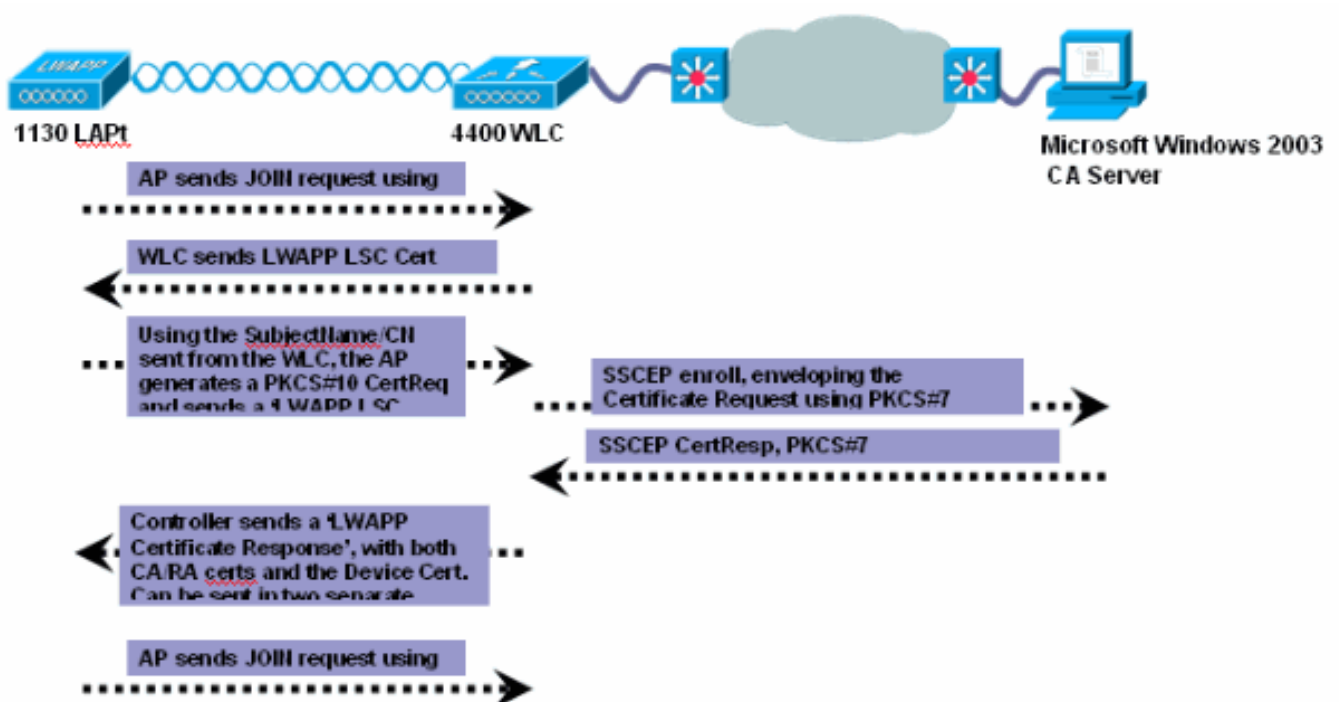
这里， PKCS-10在PKCS-7 SignedData消息类型包裹。而PKCSReq信息传送到控制器，作为SCEP客户端功能一部分，这支持。

在成功的登记操作， CA和设备认证当前是存在控制器。

在LWAPP AP的认证设置

为了在LAP能将设置的新证书，而在CAPWAP模式LAP一定能获得新的签字的X.509证书。为了执行此，它发送—certRequest到控制器，作为CA代理，并且帮助获得LAP的CA签字的certRequest。

certReq和certResponses被发送到与LWAPP有效载荷的LAP。此图表显示LAP的流能设置LSC。



这详细是步骤：

1. LAP的设置与更新的LSCs的发生，一旦LAP在UP状态，在加入了与其当前MIC/SSC后的WLC。在LSC设置阶段，即使AP在UP状态，无线电强迫被关闭。
2. 在WLC必须启用使用 and 提供LSC。此进程包括对enable (event) LSC，添加CA服务器，并且配置其他参数。LSC认证参数订单请求从控制器被发送到LAP， subject-name，在有效载荷和KeySize设置的正确性时间。当certRequest被创建时，LAP使用这些字段。有效载荷也表明LAP必须创建certRequest和送回它到控制器。
3. LAP生成被配置的keySize公共/专用的RSA密钥对。在密钥对以后的生成， certRequest在从控制器接收的SubjectName以后生成被配置。CN主动生成与现有的SSC/MIC格式，“Cxxxx-EtherMacAddr”。LAP生成—PKCS-10 CertReq并且发送它作为有效载荷，LSC证书请求，到控制器。
4. 控制器然后创建一个SSCEP PKCSReq消息，PKCS-7格式化信息，并且发送它到CA代表：LAP，为了获得证书请求签字由被配置的CA。安装的CA/RA certs用于加密certReq。
5. 如果CA能审批证书请求，与Status=SUCCESS的一个CertRep消息被退还到SSCEP客户端(控制器)以PKCS-7格式。Cert回应被写本地到文件作为PEM格式认证。
6. 因为此CertResp是为LAP，WLC发送认证到与有效载荷“认证回应的”LAP。CA cert用同一有效载荷首先传送，然后设备认证在分开的有效载荷被发送。

LSC CA和LAP设备证书安装到LAP和系统自重新启动。当下次它出现，因为配置使用LSCs，作为加入请求一部分，AP发送LSC设备认证到控制器。作为加入回应一部分，控制器发送其新设备认证并且验证与新的CA根证明的入站LAP认证。

Note: 为网桥模式被配置的接入点不支持LSCs。

[在无线局域网控制器\(WLCs\)和轻量级接入点\(膝部\)的LSC技术支持](#)

这些WLC平台支持LSC：

- Cisco 4400 系列无线局域网控制器
- 思科2100系列无线局域网控制器
- Cisco Catalyst 6500 Series无线服务模块(WISM)
- Cisco Catalyst 3750G集成无线局域网控制器
- Cisco 无线局域网控制器模块

Cisco Aironet C1130、C1140、C1240，C1252接入点和所有新的接入点支持LSC。

网AP (1510，1522)不支持LSC，网桥模式AP。

本文如何解释与配置示例，对enable (event)并且验证与局部重要的证书的膝部。

[Configure](#)

Note: 局部重要的认证功能可以是启用的通过[GUI](#)或[CLI](#)在控制器。

Note: 在控制器的LSC功能不采取密码挑战。所以，为了LSC能工作，您必须禁用在CA服务器的密码挑战。并且，因为禁用对此的密码挑战是不可能的您不能使用微软视窗服务器2008作为CA服务器。

[网络设置](#)

在本例中，您配置—4400无线局域网控制器和1130系列轻量级接入点使用局部重要的证书(LSCs)。

为了完成此，您必须设置无线局域网控制器和LAP与LSCs从Certificate Authority (CA)服务器。

本文使用微软视窗2003服务器作为CA服务器。

[CA和SCEP设置进程](#)

本文假设，在微软视窗2003服务器的CA服务器配置到位。这是步骤的汇总CA和SCEP的设置进程：

1. 设置Windows 2003，并且CA服务器，确定`http://ca-server/certsrv`工作
2. 从Microsoft网站的下载`cepsetup.exe`
3. 因为WLC不可能支持挑战当前，登记模式安装`cepsetup.exe`，不选定“RequireSCEP挑战说明”。
4. 提供名字、电子邮件、国家、城市和其他细节。
5. 保证`http://ca-server/certsrv/mscep/mscep.dll`工作正如所料。

Note: 您将需要创建用户帐户，分配它请读并且登记IPSec (脱机请求)模板的权限，并且做它成员IIS_WPG组。关于完全详细资料请参见[安装和配置的SCEP](#) Microsoft网站

[通过GUI配置无线局域网控制器](#)

完成这些步骤：

1. 从无线局域网控制器GUI，请点击**安全>认证> LSC**为了打开本地重大的证书(LSC)页。
2. 点击**一般**选项。
3. 为了在系统的enable (event) LSC，检查在**控制器**复选框的**Enable (event) LSC**。
4. 在CA服务器URL字段，请输入URL到CA服务器。您能输入域名或IP地址。
5. 在**密钥**字段，请输入设备认证的参数。密钥大小是从384的值到2048 (在位)，并且DEFAULT值是2048。
6. 单击 **Apply** 以提交更改。

Local Significant Certificates (LSC)

General **AP Provisioning**

| Certificate Type | Status |
|------------------|----------------------------|
| CA | Not Present ▼ |

General

Enable LSC on Controller

CA Server

CA server URL
(Ex: http://10.0.0.1:8080/caserver)

Params

Country Code
State
City
Organization
Department
E-mail
Key Size

7. 为了添加CA证书到控制器的CA证书数据库，盘旋您的在蓝色下拉箭头的光标证书类型的和选择添加。下面是一个示例。

Local Significant Certificates (LSC)

General **AP Provisioning**

| Certificate Type | Status |
|------------------|------------------------|
| CA | Present ▼ |

General

Enable LSC on Controller

CA Server

CA server URL
(Ex: http://10.0.0.1:8080/caserver)

Params

Country Code
State
City
Organization
Department
E-mail
Key Size

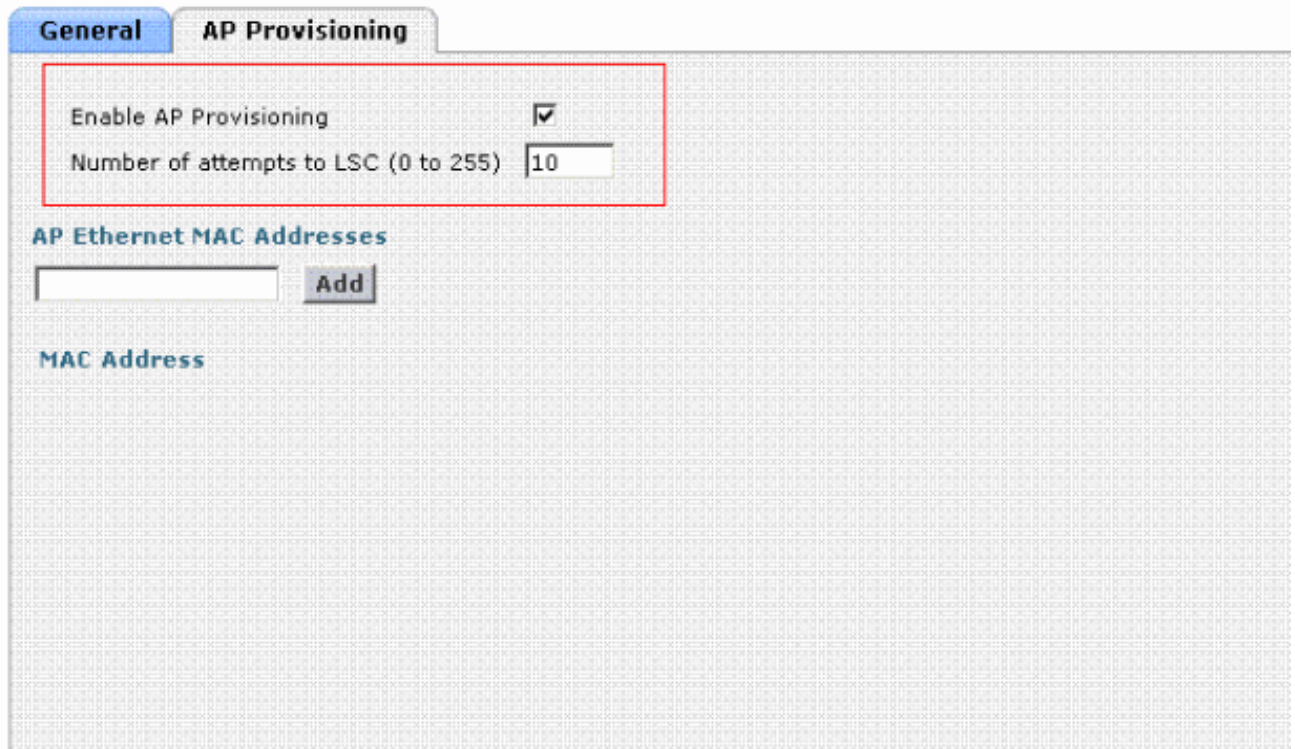
Windows Internet Explorer

Successfully updated certificates.

OK

8. 为了设置在接入点的LSC，请点击**AP Provisioning**选项，并且检查**设置**复选框的**Enable (event) AP**。
9. 为了添加对提供列表的接入点，输入接入点MAC地址在AP以太网MAC地址字段和点击**添加**。为了从提供列表取消接入点，盘旋您的在蓝色下拉箭头的光标接入点的和选择**去除**。如果配置一张接入点提供列表，只有在提供列表的接入点设置，当您enable (event) AP设置。如果不配置一张接入点提供列表，加入控制器的所有接入点有MIC或SSC认证的是设置的LSC。
10. 单击 **Apply** 以提交更改。

Local Significant Certificates (LSC)



The screenshot shows the configuration page for Local Significant Certificates (LSC) under the 'AP Provisioning' tab. The 'Enable AP Provisioning' checkbox is checked, and the 'Number of attempts to LSC (0 to 255)' is set to 10. Below this, there is a section for 'AP Ethernet MAC Addresses' with an 'Add' button and a 'MAC Address' label.

[通过CLI配置无线局域网控制器](#)

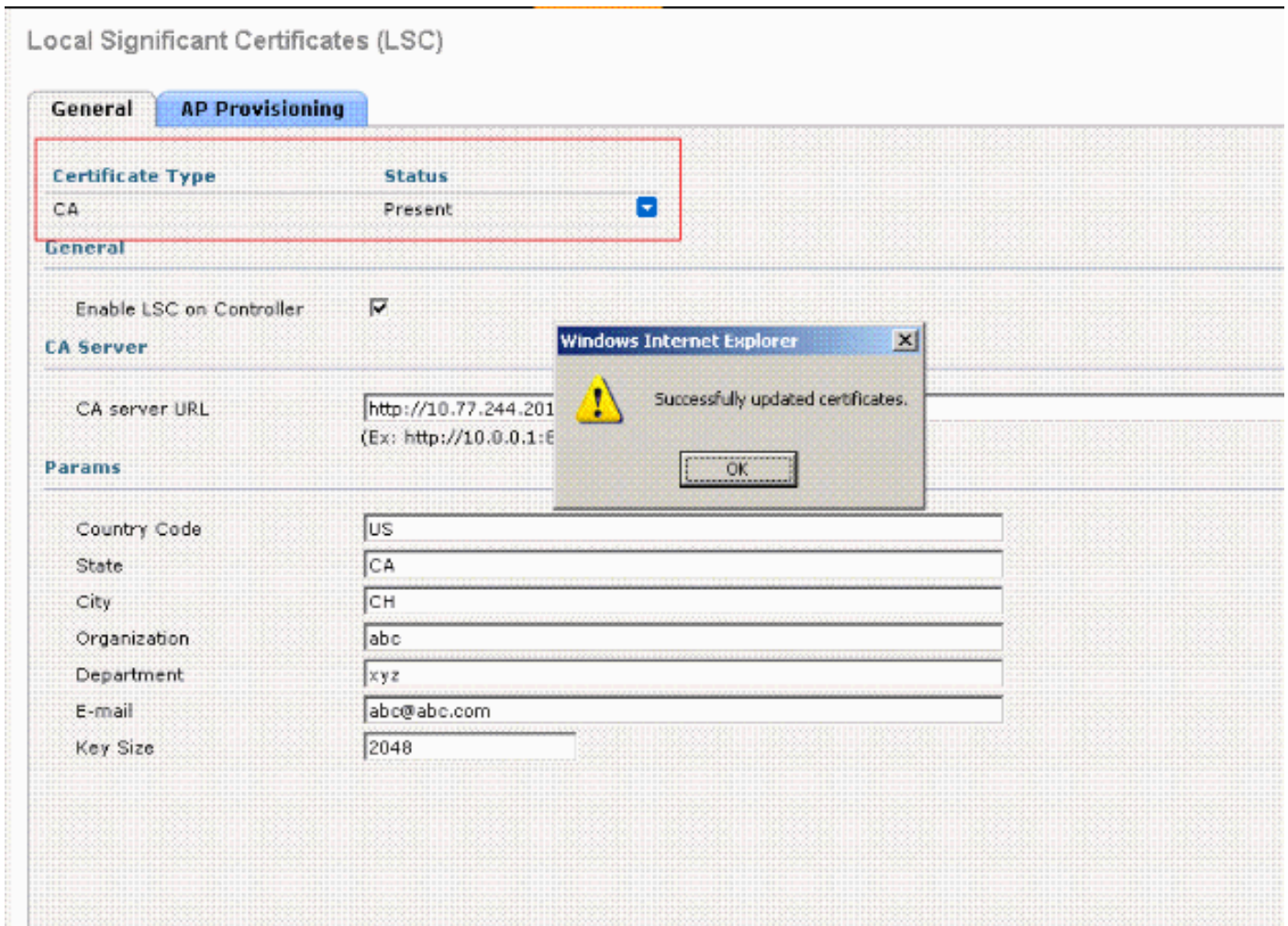
请参见[使用CLI配置Cisco无线LAN控制器配置指南的LSC部分](#)，[版本5.2](#)关于程序的信息到enable (event)从CLI的局部重要的认证(LSC)功能在控制器。

[Verify](#)

Use this section to confirm that your configuration works properly.

[命令输出解释程序 \(仅限注册用户\)](#) (OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

一旦配置无线局域网控制器，并且CA服务器到位，无线局域网控制器使用SCEP协议为了与CA服务器沟通和获取LSC认证。这是WLC的屏幕画面，一旦安装认证。



当LAP出现时，LAP发现与第二层/第三层发现机制的WLC并且发送加入请求到有MIC认证的控制器。

无线局域网控制器然后发送LSC验证参数请求到LAP。

使用从WLC发送的SubjectName/CN，AP生成PKCS-10 CertReq并且发送“LWAPP LSC证书请求”对WLC。

此请求反过来被对CA服务器的WLC转发。CA服务器发送LAP LSC认证到控制器。控制器然后发送LSC到LAP。

此消息出现在AP CLI。

```
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
```

最后，LAP发送与LSC的一个加入请求。

发出enable命令调试capwap的事件为了查看此事件顺序。

一旦LAP向与LSC的WLC登记，您在WLC GUI能确认此。

All APs

Search by AP MAC

| AP Name | AP MAC | AP Up Time | Admin Status | Operational Status | AP Mode | Certificate Type | AP Sub Mode |
|---------|-------------------|---------------------|--------------|--------------------|---------|------------------|-------------|
| AP1130 | 00:10:c7:a0:eb:3e | 0 d, 00 h 01 m 20 s | Enable | REG | Local | LSC | None |

您能也使用从WLC CLI的这些命令为了验证此。示例如下：

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
```

为了查看关于配置有LSC的接入点的详细资料，输入此命令：

show certificate lsc ap-provision

Information similar to the following appears:

```
LSC AP-Provisioning..... Yes
Provision-List..... Present
```

IdxMac Address

```
-----
100:18:74:c7:c0:90
```

Troubleshoot

此部分说明如何排除您的配置故障。您能使用enable命令调试pm pki的scep为了查看事件顺序。

这是一本成功的调试日志的示例：

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 bytesesed: 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 bytesesed: 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:

这是发生故障案件的示例：

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 bytesesd: 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:
```

[Related Information](#)

- [Cisco 无线局域网控制器配置指南 5.2 版](#)
- [认证一个第三方认证的署名请求\(CSR\)生成在WLAN控制器\(WLC\)](#)
- [认证第三方认证和方法的署名请求生成加载被串连的证书到WLC](#)
- [无线支持页](#)
- [Technical Support & Documentation - Cisco Systems](#)