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](#)
[本地重要证书](#)
[无线局域网控制器 (WLC) 上的证书调配](#)
[LWAPP AP 上的证书调配](#)
[无线局域网控制器 (WLC) 和轻型接入点 (LAP) 上的 LSC 支持](#)
[Configure](#)
[网络设置](#)
[CA 和 SCEP 设置过程](#)
[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

本文档介绍如何配置无线局域网控制器 (WLC) 和轻型接入点 (LAP) 来使用本地重要证书功能。无线局域网控制器版本 5.2 引入了此功能。借助此功能，如果您选择控制公钥基础架构 (PKI)，可以在无线接入点和控制器上生成本地重要证书，然后可以使用这些证书实现 WLC 和 LAP 之间的相互身份验证。

Prerequisites

Requirements

尝试进行此配置之前，请确保满足以下要求：

- 了解如何配置 WLC、LAP 和无线客户端卡执行基本操作
- 了解如何配置和使用 Microsoft Windows 2003 CA 服务器
- 了解公钥基础架构和数字证书

Components Used

本文档中的信息基于以下软件和硬件版本：

- 运行固件版本 5.2 的思科 4400 系列 WLC
- 思科 Aironet 1130 AG 系列轻型接入点 (LAP)
- Microsoft Windows 2003 服务器配置为域控制器以及证书授权机构服务器
- 运行固件 4.2 版的 Cisco Aironet 802.11 a/b/g 客户端适配器
- 运行固件版本 4.2 的思科 Aironet 桌面实用程序 (ADU)

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.

本地重要证书

在版本 5.2.157.0 之前的控制器软件中，控制器可以使用自签名证书 (SSC) 对无线接入点进行身份验证，或者如果无线接入点有厂商预装证书 (MIC)，则向 RADIUS 服务器发送授权信息。在控制器软件版本 5.2.157.0 中，您可以配置控制器来使用本基地重要证书 (LSC)。如果希望自己的公钥基础架构 (PKI) 提供更好的安全性，可以使用 LSC；控制您的证书授权机构 (CA)、定义策略、限制以及生成证书的使用。

首先需要在控制器上调配新的 LSC 证书，然后再在证书授权机构 (CA) 服务器的 LAP 上进行调配。

LAP 会使用 CAPWAP 协议与控制器 (WLC) 通信。必须从 WLC 发起签名证书以及为 LAP 和 WLC 本身颁发 CA 证书的任何请求。LAP 不直接与 CA 服务器通信。WLC 充当 LWAPP AP 的 CA 代理。必须在 WLC 上配置 CA 服务器详细信息，并且必须保证可访问这些详细信息。

控制器使用简单证书注册协议 (SCEP) 将设备上生成的 certReqs 转发给 CA，然后重新使用 SCEP 从 CA 获取经过签名的证书。

SCEP 是公钥基础架构 (PKI) 客户端和证书授权机构服务器用于支持证书注册和撤销的证书管理协议。此协议在思科的应用十分广泛，并且受很多 CA 服务器支持。在 SCEP 协议中，HTTP 用作 PKI 消息的传输协议。SCEP 的主要目标是向网络设备安全地颁发证书。SCEP 可以执行的操作很多，但针对此项目和版本，SCEP 用于以下操作。

- CA 和 RA 公钥分配
- 证书注册

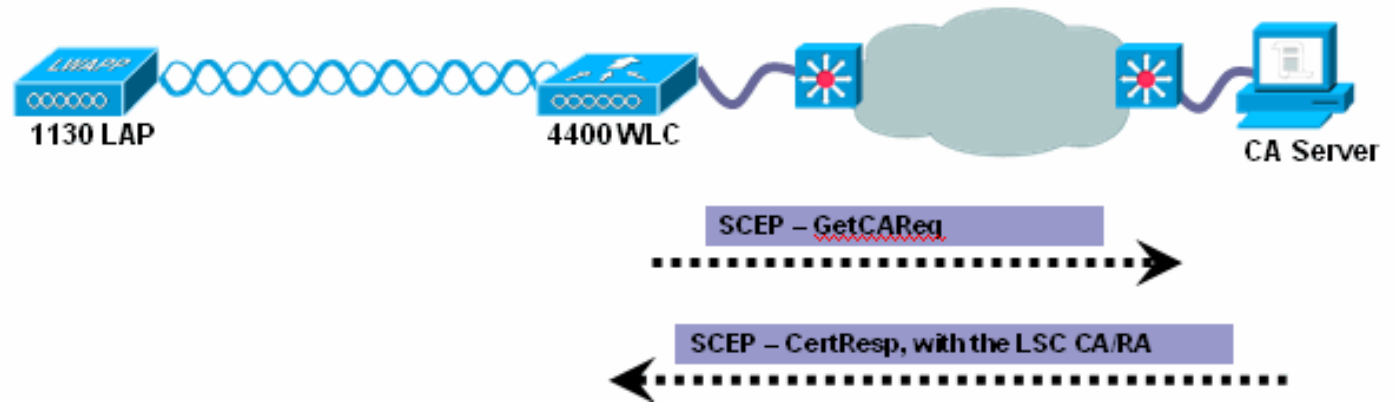
所有 SCEP 事务都在自动模式下发生。不支持吊销证书。

Note: 配置为网桥模式的无线接入点不支持 LSC。

无线局域网控制器 (WLC) 上的证书调配

新的 LSC 证书（CA 和设备证书）必须安装在控制器上。

使用 SCEP 协议从 CA 服务器接收 CA 证书。此时，控制器上没有任何证书，此操作明显是 Get 操作。这些证书安装在控制器上。此外，如果使用 LSC 调配 AP，这些相同的 CA 证书还会被推送到 AP 中。



设备证书注册操作

对于请求 CA 签名证书的 LAP 和控制器，certRequest 是作为 PKCS#10 消息发送的。CertRequest 包含主题名称、PublicKey 以及 X.509 证书中要包含的其他属性，并由请求者的 PrivateKey 进行数字签名。这些内容必须发送至 CA，CA 会将 certRequest 转换为 X.509 证书。

接收 PKCS#10 certRequest 的 CA 需要其他信息才能对请求者的身份进行验证，并验证请求是否保持不变。PKCS#10 经常与其他方法（例如 PKCS#7）相结合来发送和接收 Cert Reqs/Resps。

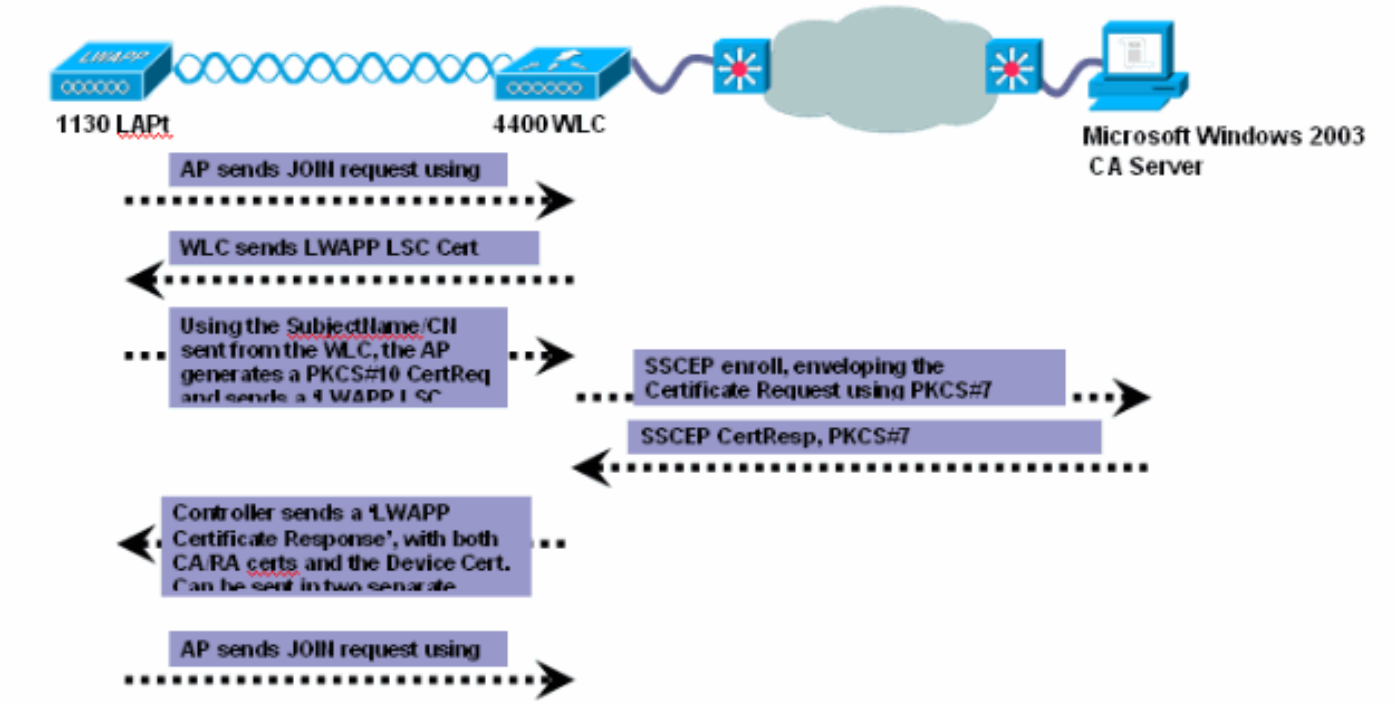
这里，PKCS#10 包装为 PKCS#7 SignedData 消息类型。这作为 SCEP 客户端功能的一部分，在向控制器发送 PKCSReq 消息时受支持。

成功完成注册操作后，CA 和设备证书现在均在控制器上。

LWAPP AP 上的证书调配

要在 CAPWAP 模式下在 LAP 上调配新证书，LAP 必须能够获取新的已签名的 X.509 证书。为此，LAP 会向控制器（充当 CA 代理，可帮助为 LAP 获取由 CA 签名的 certRequest）发送 certRequest。

certReq 和 certResponses 通过 LWAPP 负载发送至 LAP。下图显示 LAP 调配 LSC 的工作流。



以下是详细步骤：

1. 当 LAP 处于“运行”状态下，并且已使用其当前的 MIC/SSC 加入 WLC 后，才能调配更新的 LSC。在 LSC 调配阶段，即使 AP 处于“运行”状态，无线电也会强制关闭。
2. 必须在 WLC 上启用使用和部署 LSC。此过程包括启用 LSC、添加 CA 服务器，以及配置其他参数。LSC 证书参数命令请求从控制器发送至 LAP，其中负载中设置有主题名称、有效时间和 Keysize。LAP 会在创建 certRequest 时使用这些字段。此外，负载也会指明 LAP 必须创建 certRequest，并将其发送回控制器。
3. LAP 生成所配置的 keysize 公用/专用 RSA 密钥对。在生成密钥对后，配置好从控制器接收的 SubjectName 后会生成 certRequest。CN 将使用现有的 SSC/MIC 格式“Cxxxx-EtherMacAddr”自动生成。LAP 生成 PKCS#10 CertReq 并将其作为负载（LSC 证书请求）发送至控制器。
4. 然后，控制器创建 SSCEP PKCSReq 消息（PKCS#7 格式的消息）并代表 LAP 将其发送给 CA，以便让配置好的 CA 为证书请求签名。所安装的 CA/RA 证书用于加密 certReq。
5. 如果 CA 能够审批证书请求，会以 PKCS#7 格式重新向 SSCEP 客户端（控制器）发送状态=成功的 CertRep 消息。证书响应作为 PEM 格式的证书在本地写入到文件中。
6. 因为此 CertResp 是供 LAP 使用的，WLC 会通过负载“证书响应”向 LAP 发送证书。首先使用同一负载发送 CA 证书，然后通过单独的负载发送设备证书。

LSC CA 和 LAP 设备证书均安装在 LAP 中，系统自动重启。在下一次启动时，因为 AP 配置为使用 LSC，它会将 LSC 设备证书作为加入请求的一部分发送到控制器。控制器会将其新的设备证书作为加入响应的一部分发送，同时使用新的 CA 根证书验证入站 LAP 证书。

Note: 配置为网桥模式的无线接入点不支持 LSC。

无线局域网控制器 (WLC) 和轻型接入点 (LAP) 上的 LSC 支持

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

思科 Aironet C1130、C1140、C1240、C1252 无线接入点和任何新的接入点支持 LSC。

网状 AP（1510 和 1522）以及网桥模式 AP 不支持 LSC。

本文档通过配置示例介绍如何使用本地重要证书启用 LAP 并对其进行身份验证。

Configure

Note: 本地重要证书功能可通过控制器上的 GUI 或 CLI 启用。

Note: 控制器上的 LSC 功能不使用密码质询。因此，为使 LSC 正常工作，您必须在 CA 服务器上禁用密码质询。此外，您无法将 Microsoft Windows Server 2008 用作 CA 服务器，因为无法在其上禁用密码质询。

网络设置

在本示例中，您需要配置 4400 无线局域网控制器和 1130 系列轻型接入点来使用本地重要证书 (LSC)。为此，您必须使用证书颁发机构 (CA) 服务器的 LSC 调配无线局域网控制器和 LAP。

本文档将 Microsoft Windows 2003 服务器用作 CA 服务器。

CA 和 SCEP 设置过程

本文档假设已在 Microsoft Windows 2003 服务器上配置 CA 服务器。以下是 CA 和 SCEP 设置过程的步骤摘要：

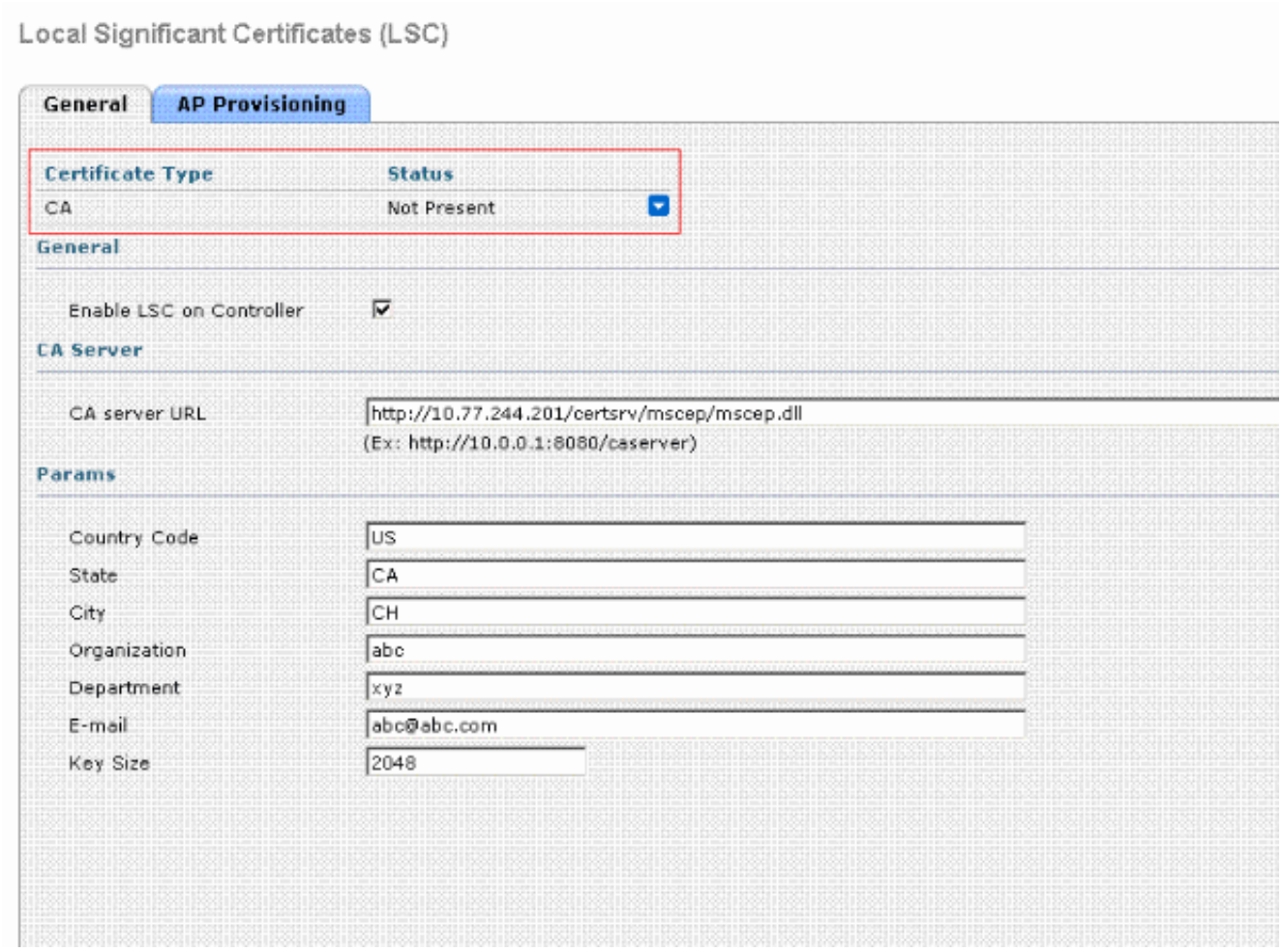
1. 设置 Windows 2003 和 CA 服务器，确保 *http://ca-server/certsrv* 正常工作
2. 从 Microsoft 网站下载 *cepsetup.exe*
3. 安装 cepsetup.exe，取消选中“需要 SCEP *质询短语*”，因为 WLC 现在无法支持质询注册模式。
4. 提供姓名、邮箱地址、国家/地区、所在城市和其他详细信息。
5. 确保 *http://ca-server/certsrv/mscep/mscep.dll* 可如期正常工作。

Note: 您将需要创建一个用户账户，并为 IPSec（离线请求）模板分配读取和注册权限，并使其成为 IIS_WPG 组的一员。有关完整的详细信息，请参阅 Microsoft 网站，了解安装和配置 SCEP

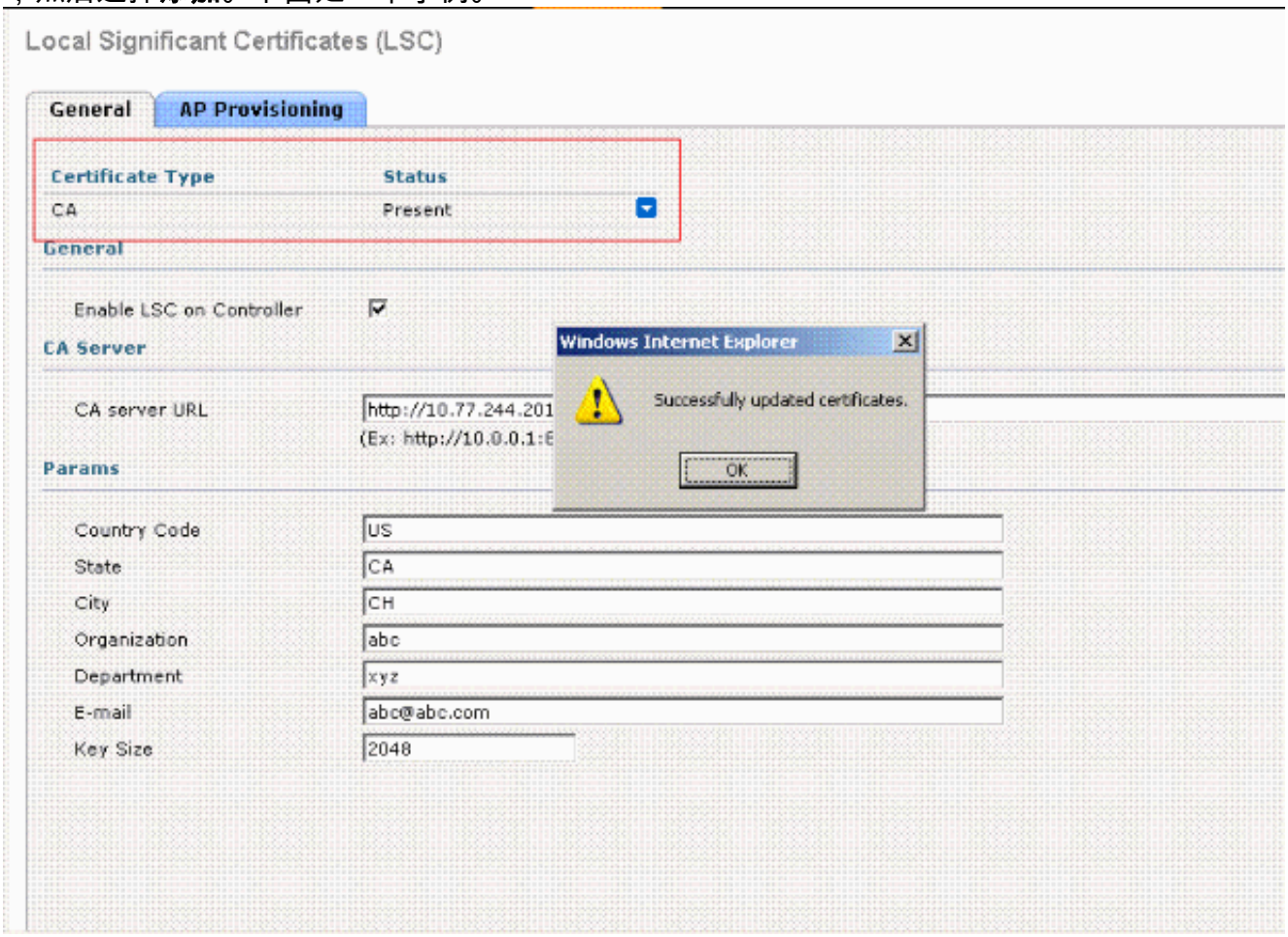
通过 GUI 配置无线局域网控制器

完成这些步骤：

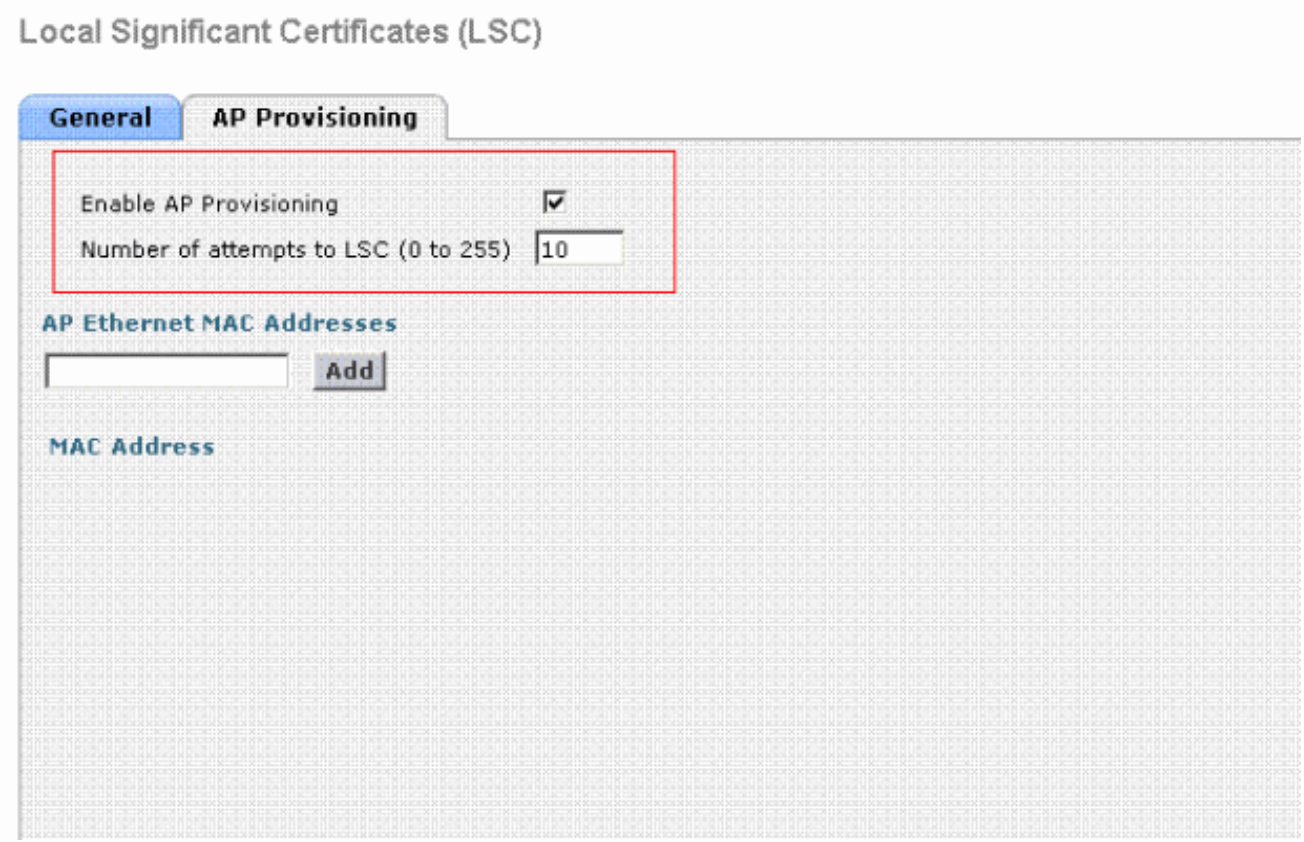
1. 从无线局域网控制器 GUI 中，点击**安全 > 证书 > LSC**，打开“本地重要证书 (LSC)”页面。
2. 点击**常规**选项卡。
3. 要在系统上启用 LSC，请选中**在控制器上启用 LSC** 复选框。
4. 在“CA 服务器 URL”字段中，输入 CA 服务器的 URL。您可以输入域名或 IP 地址。
5. 在“参数”字段中，输入设备证书的参数。密钥大小为 384 到 2048（位数）之间的值，默认值为 2048。
6. 单击 **Apply** 以提交更改。



7. 要将 CA 证书添加到控制器的 CA 证书数据库中，请将光标悬停在证书类型的蓝色下拉箭头上，然后选择**添加**。下面是一个示例。



8. 要在无线接入点上调配 LSC，请点击 **AP 调配**选项卡，然后选中**启用 AP 调配**复选框。
9. 要将无线接入点添加到调配列表中，请在“AP 以太网 MAC 地址”字段中输入无线接入点的 MAC 地址，然后点击**添加**。要从调配列表中删除无线接入点，请将光标悬停在无线接入点的蓝色下拉箭头上，然后选择**删除**。如果您配置无线接入点调配列表，则启用 AP 调配时仅会调配调配列表中的无线接入点。如果未配置无线接入点调配列表，则使用 MIC 或 SSC 证书加入控制器的所有无线接入点都可以实现 LSC 调配。
10. 单击 **Apply** 以提交更改。



通过 CLI 配置无线局域网控制器

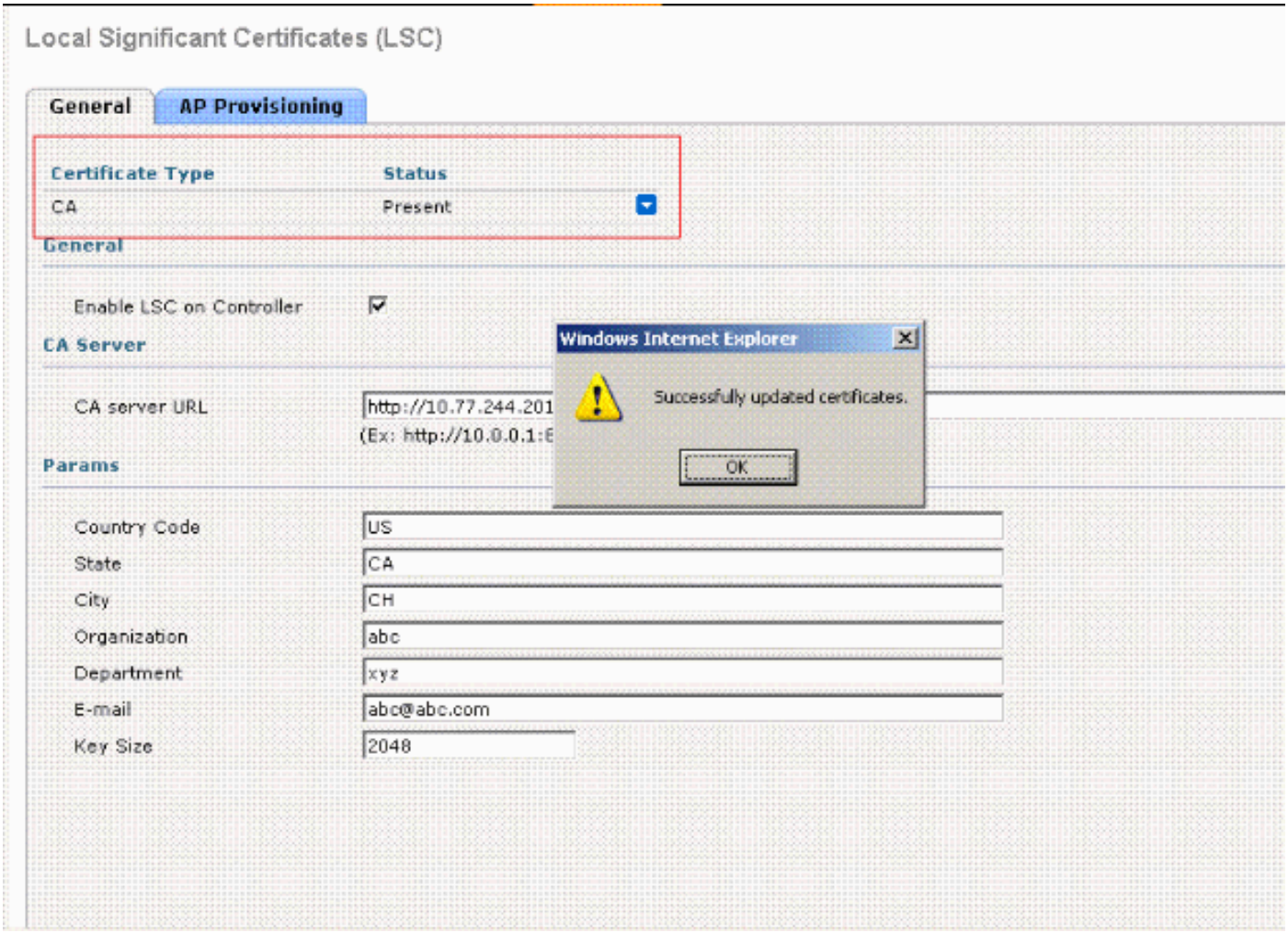
请参阅《思科无线局域网控制器配置指南版本 5.2》的**使用 CLI 配置 LSC** 部分，了解从控制器的 CLI 启用本地重要证书 (LSC) 功能。

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。

配置好无线局域网控制器和 CA 服务器后，无线局域网控制器会使用 SCEP 协议与 CA 服务器通信并获取 LSC 证书。以下是安装证书后的 WLC 的屏幕截图。



当 LAP 出现时，LAP 会借助第 2/3 层发现机制发现 WLC，并使用 MIC 证书向控制器发送加入请求。

然后，无线局域网控制器会向 LAP 发送 LSC 证书参数请求。

从 WLC 发送 SubjectName/CN 后，AP 会生成 PKCS #10 CertReq 并向 WLC 发送 'LWAPP LSC 证书请求'。

此请求由 WLC 转发到 CA 服务器。CA 服务器向控制器发送 LAP LSC 证书。然后，控制器将 LSC 发送到 LAP。

AP CLI 上会显示以下消息。

```
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 使用 LSC 发送加入请求。

发出 **debug capwap events enable 命令**以查看事件顺序。

当 LAP 使用 LSC 注册 WLC 后，您可以在 WLC GUI 上确认此事。

您还可以从 WLC CLI 使用这些命令进行验证。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
```

要查看使用 LSC 进行调配的无线接入点的详细信息，请输入以下命令：

```
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

本部分介绍如何对配置进行故障排除。您可以使用 **debug pm pki scep enable** 命令查看事件顺序。

以下是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 byteseded: Operation now in progress*emWeb: Nov 23 06:52:27.526:
scep: Http response is <HTTP/1.1 200 OK>
scep: Server returned status code 200.
scep: header info: <Connection: close>
scep: header info: <Date: Wed, 23 Nov 2011 06:52:30 GMT>
scep: header info: <Server: Microsoft-IIS/6.0>
scep: header info: <Content-Length: 3795>
scep: header info: <Content-Type: application/x-x509-ca-ra-cert>
scep: MIME header: application/x-x509-ca-ra-cert
scep: found certificate:
  subject: /DC=com/DC=ccie/CN=AD
  issuer: /DC=com/DC=ccie/CN=AD
  usage: Digital Signature, Certificate Sign, CRL Sign
scep: found certificate:
  subject: /C=CN/ST=BJ/L=BJ/O=Cisco/OU=BN/CN=tls/emailAddress=tls@ccie.com
  issuer: /DC=com/DC=ccie/CN=AD
  usage: Key Encipherment
scep: found certificate:
  subject: /C=CN/ST=BJ/L=BJ/O=Cisco/OU=BN/CN=tls/emailAddress=tls@ccie.com
  issuer: /DC=com/DC=ccie/CN=AD
  usage: Digital Signature
scep: CA cert retrieved with fingerprint 639993FF7FF8FB12EF2FB09DEC7C5BED

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

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

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

```
scep: header info: <Content-Length: 2549>
scep: header info: <Content-Type: application/x-pki-message>
scep: MIME header: application/x-pki-message

scep: reading outer PKCS#706:53:13.488:
scep: PKCS#7 payload size: 2549 bytes8:
scep: PKCS#7 contains 2023 bytes of enveloped data
scep: verifying signature 06:53:13.489:
scep: signature ok Nov 23 06:53:13.490:
scep: finding signed attributes:13.490:
scep: finding attribute transId:13.490:
scep: allocating 32 bytes for attribute.
scep: reply transaction id: A984A2DFE20DA7E0FE702DC8EC307F33
scep: finding attribute messageType490:
scep: allocating 1 bytes for attribute.
scep: reply message type is good13.490:
scep: finding attribute senderNonce490:
scep: allocating 16 bytes for attribute.
scep: finding attribute recipientNonce:
scep: allocating 16 bytes for attribute.
scep: finding attribute pkiStatus3.491:
scep: allocating 1 bytes for attribute.
scep: pkistatus: SUCCESS3 06:53:13.491:
scep: reading inner PKCS#706:53:13.491:
scep: decrypting inner PKCS#753:13.492:
scep: found certificate:
  subject: /serialNumber= PID:AIR-LAP1262N-A-K9
    SN:FTX1433K60R/C=CN/ST=BJ/L=BJ/O=Cisco/OU=BN/CN=AP3G1-f866f267577e/emailAddress=
tls@ccie.com
  issuer: /DC=com/DC=ccie/CN=AD
scep: PKCS#7 payload size: 1580 bytes:53:13.518:

Digital Signature, Key Encipherment
scep: waiting for 10 secs 06:53:13.520:
```

以下是失败示例：

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

scep: reading outer PKCS#718:07:14.133:
scep: PKCS#7 payload size: 540 bytes33:
scep: PKCS#7 contains 1 bytes of enveloped data
scep: verifying signature 18:07:14.134:
scep: signature ok Nov 22 18:07:14.135:
scep: finding signed attributes:14.135:
scep: finding attribute transId:14.135:
scep: allocating 32 bytes for attribute.
scep: reply transaction id: 3DA1646840CD4FFEB1534EA8F1D45F76
scep: finding attribute messageType135:
scep: allocating 1 bytes for attribute.
scep: reply message type is good14.135:
scep: finding attribute senderNonce135:
```

```
scep: allocating 16 bytes for attribute.
scep: finding attribute recipientNonce:
scep: allocating 16 bytes for attribute.
scep: finding attribute pkiStatus4.136:
scep: allocating 1 bytes for attribute.
scep: pkistatus: FAILURE2 18:07:14.136:
scep: finding attribute failInfo14.136:
scep: allocating 1 bytes for attribute.
scep: reason: Transaction not permitted or supported
scep: waiting for 10 secs 18:07:14.136:
scep: waiting for 10 secs 18:07:27.144:
scep: waiting for 10 secs 18:07:40.152:
scep: waiting for 10 secs 18:07:53.160:
scep: waiting for 10 secs 18:08:06.168:
scep: waiting for 10 secs 18:08:19.176:
scep: waiting for 10 secs 18:08:32.184:
scep: waiting for 10 secs 18:08:45.192:
scep: waiting for 10 secs 18:08:58.200:
scep: waiting for 10 secs 18:09:11.208:
```

Related Information

- Cisco 无线局域网控制器配置指南 5.2 版
- 在无线局域网控制器上为第三方证书生成证书签名请求 (CSR)
- 为第三方证书生成证书签名请求以及向 WLC 上传链式证书的程序
- 无线支持页
- Technical Support & Documentation - Cisco Systems