使用CUCM在IP电话上配置LSC

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

- MIC 与 LSC

配置

- 网络拓扑

验证

LSC 批量安装

故障排除

- 无有效 CAPF 服务器
- LSC：连接失败
- LSC：失败
- LSC：操作挂起

相关信息

简介

本文档介绍如何在思科互联网协议电话（思科 IP 电话）上安装本地有效证书 (LSC)。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco Unified Communications Manager (CUCM) 集群安全模式选项
- X.509 证书
- 制造商安装证书 (MIC)
- LSC
- 证书颁发机构代理功能 (CAPF) 证书操作
- 默认安全设置 (SBD)

- 初始信任列表 (ITL) 文件

使用的组件

本文档中的信息基于支持 SBD 的 CUCM 版本，即 CUCM 8.0(1) 及更高版本。

注意：它仅适用于支持默认安全设置 (SBD) 的电话。 例如，7940 和 7960 电话不支持 SBD，7935、7936 和 7937 会议电话也不支持 SBD。如需查看您的 CUCM 版本中支持 SBD 的设备列表，请依次导航至 Cisco Unified Reporting > 系统报告 > Unified CM 电话功能列表，然后运行有关“功能：默认安全设置”的报告。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

思科证书颁发机构代理功能 (CAPF) 服务仅在发布方节点上运行。发布方充当 LSC 的证书颁发机构 (CA) 或签名者。

MIC 与 LSC

如果针对 802.1X 或 AnyConnect Phone VPN 使用基于证书的身份验证，则必须了解 MIC 与 LSC 之间的区别。

每部思科电话出厂时均预安装有 MIC。此证书由其中一项思科制造 CA 证书（思科制造 CA、思科制造 CA SHA2、CAP-RTP-001 或 CAP-RTP-002 证书）签署。当电话提供此证书时，会证明它是有效的Cisco电话，但这不会验证电话是否属于特定用户或CUCM集群。它可能是从公开市场购买或从其他地方带来的非法所得电话。

相反，LSC 由管理员特意安装在电话上，并由 CUCM 发布方的 CAPF 证书签署。您可以将 802.1X 或 AnyConnect VPN 配置为仅信任由已知 CAPF 证书颁发机构颁发的 LSC。基于 LSC 而不是 MIC 进行证书身份验证，便于更精细地控制受信任的电话设备。

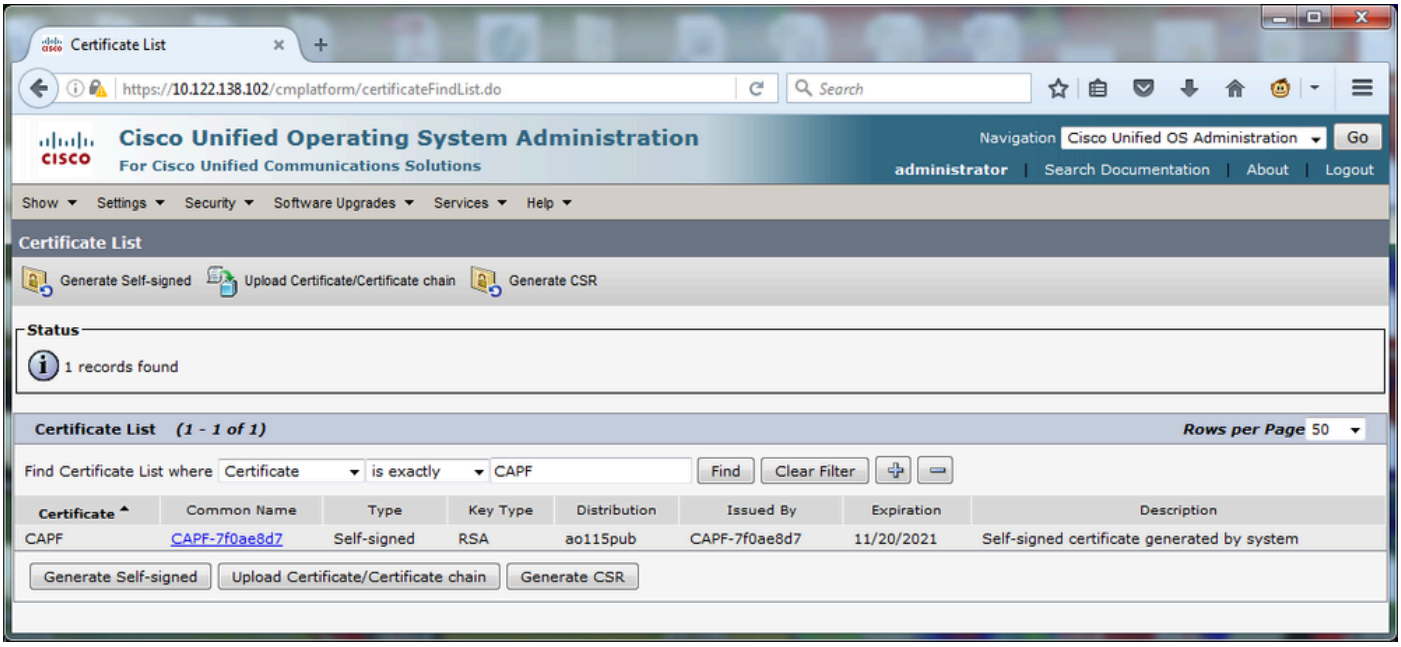
配置

网络拓扑

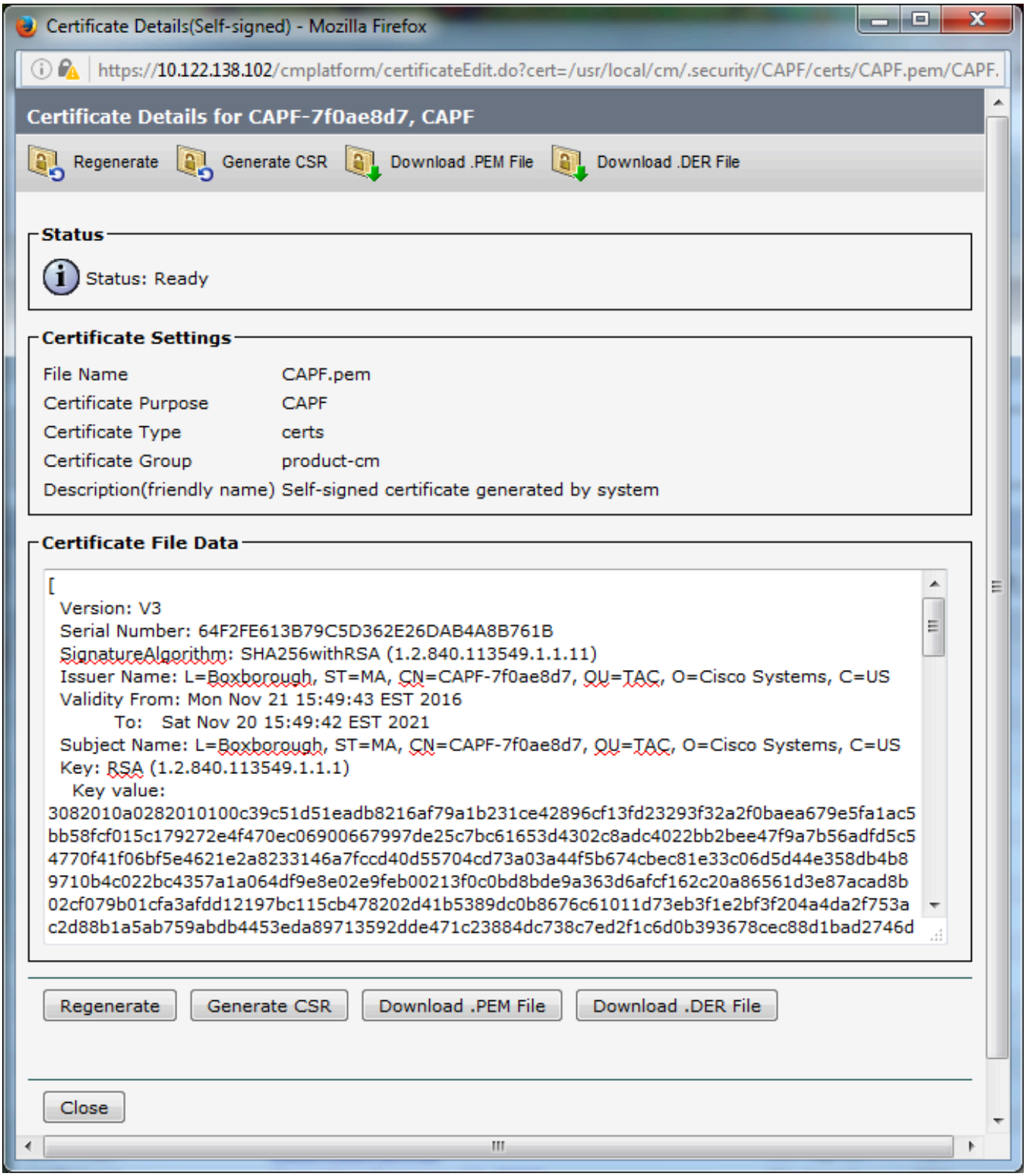
本文档使用了以下 CUCM 实验室服务器：

- CUCM 发布方和 TFTP 服务器
- CUCM 订用方和 TFTP 服务器

验证 CAPF 证书尚未到期，也不会在近期到期。依次导航至 Cisco Unified OS Administration > 安全 > 证书管理，然后导航至查找证书恰好是 CAPF 的证书列表，如图所示。



点击通用名称打开“证书详细信息”页面。检查证书文件数据窗格中的“有效期开始日期”和“有效期结束日期”，以确定证书何时到期，如图所示。



如果 CAPF 证书已到期或即将到期，请重新生成该证书。请勿使用已到期或即将到期的 CAPF 证书继续执行 LSC 安装流程。这样可避免在不久的将来由于 CAPF 证书到期而需要重新颁发 LSC。有关如何重新生成 CAPF 证书的信息，请参阅文章 CUCM 证书重新生成/续约流程。

同样，如果需要第三方证书颁发机构签署 CAPF 证书，则可在此阶段做出选择。立即完成证书签名请求 (CSR) 文件生成和已签名 CAPF 证书的导入，或者使用自签名 LSC 继续完成配置以进行初步测试。如果您需要第三方签名的 CAPF 证书，通常明智的做法是先使用自签名 CAPF 证书配置此功

能，测试并验证，然后重新部署由第三方签名的 CAPF 证书签署的 LSC。使用第三方签名的 CAPF 证书测试失败时，这可简化后续的故障排除。

警告：如果在 CAPF 服务已激活并启动时重新生成 CAPF 证书或导入第三方签名的 CAPF 证书，则 CUCM 会自动重置电话。当重置电话可接受时，在维护窗口中完成这些操作步骤。有关参考信息，请参阅思科漏洞 ID CSCue55353 - 在重新生成电话重置的 TVS/CCM/CAPF 证书时添加警告。

注意：如果您的 CUCM 版本支持 SBD，则无论 CUCM 集群是否设置为混合模式，此 LSC 安装操作步骤均适用。SBD 是 CUCM 8.0(1) 及更高版本的一部分。在这些版本的 CUCM 中，ITL 文件包含有关 CUCM 发布方服务器上的 CAPF 服务的证书。这允许将电话连接到 CAPF 服务以支持证书操作，例如安装/升级和故障排除。

在先前版本的 CUCM 中，需要将集群配置为混合模式才能支持证书操作。由于目前已不再需要这种模式，因此减少了对将 LSC 用作 802.1X 身份验证或 AnyConnect VPN 客户端身份验证的电话身份证书的阻碍。

在 CUCM 集群中的所有 TFTP 服务器上运行 show itl 命令。观察 ITL 文件是否包含 CAPF 证书。

例如，以下是实验 CUCM Subscriber ao115sub 的 show itl 输出内容节选。

注意：此文件中有一个功能为 CAPF 的 ITL 记录条目。

注意：如果您的 ITL 文件没有 CAPF 条目，请登录到 CUCM 发布方服务器并确认 CAPF 服务是否已激活。为了确认这一点，请依次导航至 Cisco Unified Serviceability > 工具 > 服务激活 > CUCM 发布方 > 安全，然后激活思科证书颁发机构代理功能服务。如果该服务已停用并且您刚刚重新激活该服务，请依次导航至 Cisco Unified Serviceability > 工具 > 控制中心 – 功能服务 > 服务器 > CM 服务，然后在 CUCM 集群中的所有 TFTP 服务器上重新启动 Cisco TFTP 服务，以重新生成 ITL 文件。此外，请确保不会遇到思科漏洞 ID CSCuj78330。

注：完成后，在 CUCM 集群中的所有 TFTP 服务器上运行 show itl 命令，以验证当前 CUCM 发布方 CAPF 证书现在是否包含在文件中。

<#root>

```
ITL Record #:1
```

```
 ----

BYTEPOS TAG LENGTH VALUE

------- --- ------ -----

1 RECORDLENGTH 2 727

2 DNSNAME 2

3 SUBJECTNAME 64 CN=CAPF-7f0ae8d7;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US

4 FUNCTION 2 CAPF

5 ISSUERNAME 64 CN=CAPF-7f0ae8d7;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US

6 SERIALNUMBER 16 64:F2:FE:61:3B:79:C5:D3:62:E2:6D:AB:4A:8B:76:1B

7 PUBLICKEY 270

8 SIGNATURE 256

11 CERTHASH 20 C3 E6 97 D0 8A E1 0B F2 31 EC ED 20 EC C5 BC 0F 83 BC BC 5E

12 HASH ALGORITHM 1 null
```

```
 ITL Record #:2
 ----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 717
2 DNSNAME 2
3 SUBJECTNAME 59 CN=ao115pub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
4 FUNCTION 2 TVS
5 ISSUERNAME 59 CN=ao115pub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
6 SERIALNUMBER 16 6B:99:31:15:D1:55:5E:75:9C:42:8A:CE:F2:7E:EA:E8
7 PUBLICKEY 270
8 SIGNATURE 256
11 CERTHASH 20 05 9A DE 20 14 55 23 2D 08 20 31 4E B5 9C E9 FE BD 2D 55 87
12 HASH ALGORITHM 1 null

 ITL Record #:3
 ----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1680
2 DNSNAME 2
3 SUBJECTNAME 71 CN=ITLRECOVERY_ao115pub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 71 CN=ITLRECOVERY_ao115pub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
6 SERIALNUMBER 16 51:BB:2F:1C:EE:80:02:16:62:69:51:9A:14:F6:03:7E
7 PUBLICKEY 270
8 SIGNATURE 256
9 CERTIFICATE 963 DF 98 C1 DB E0 61 02 1C 10 18 D8 BA F7 1B 2C AB 4C F8 C9 D5 (SHA1 Hash HEX)
This etoken was not used to sign the ITL file.

 ITL Record #:4
 ----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 717
2 DNSNAME 2
3 SUBJECTNAME 59 CN=ao115sub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
4 FUNCTION 2 TVS
5 ISSUERNAME 59 CN=ao115sub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
6 SERIALNUMBER 16 65:E5:10:72:E7:F8:77:DA:F1:34:D5:E3:5A:E0:17:41
7 PUBLICKEY 270
8 SIGNATURE 256
11 CERTHASH 20 00 44 54 42 B4 8B 26 24 F3 64 3E 57 8D 0E 5F B0 8B 79 3B BF
12 HASH ALGORITHM 1 null

 ITL Record #:5
 ----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1652
2 DNSNAME 2
3 SUBJECTNAME 59 CN=ao115sub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 59 CN=ao115sub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
6 SERIALNUMBER 16 48:F7:D2:F3:A2:66:37:F2:DD:DF:C4:7C:E6:B9:CD:44
7 PUBLICKEY 270
8 SIGNATURE 256
9 CERTIFICATE 959 20 BD 40 75 51 C0 61 5C 14 0D 6C DB 79 E5 9E 5A DF DC 6D 8B (SHA1 Hash HEX)
This etoken was used to sign the ITL file.
```

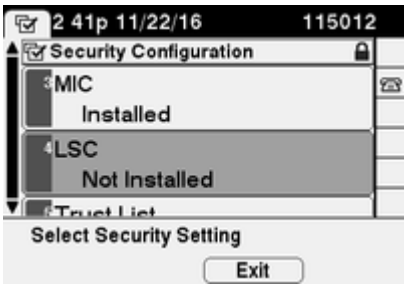
```
 ITL Record #:6
 ----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1652
2 DNSNAME 2
3 SUBJECTNAME 59 CN=ao115sub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
4 FUNCTION 2 TFTP
5 ISSUERNAME 59 CN=ao115sub;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
6 SERIALNUMBER 16 48:F7:D2:F3:A2:66:37:F2:DD:DF:C4:7C:E6:B9:CD:44
7 PUBLICKEY 270
8 SIGNATURE 256
9 CERTIFICATE 959 20 BD 40 75 51 C0 61 5C 14 0D 6C DB 79 E5 9E 5A DF DC 6D 8B (SHA1 Hash HEX)

 ITL Record #:7
 ----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1031
2 DNSNAME 9 ao115sub
3 SUBJECTNAME 62 CN=ao115sub-EC;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
4 FUNCTION 2 TFTP
5 ISSUERNAME 62 CN=ao115sub-EC;OU=TAC;O=Cisco Systems;L=Boxborough;ST=MA;C=US
6 SERIALNUMBER 16 53:CC:1D:87:BA:6A:28:BD:DA:22:B2:49:56:8B:51:6C
7 PUBLICKEY 97
8 SIGNATURE 103
9 CERTIFICATE 651 E0 CF 8A B3 4F 79 CE 93 03 72 C3 7A 3F CF AE C3 3E DE 64 C5 (SHA1 Hash HEX)

The ITL file was verified successfully.
```

将 CAPF 条目确认为 ITL 中的条目后，可以在电话上完成证书操作。在本例中，使用 Null 字符串身份验证安装 2048 位 RSA 证书。

在电话上，验证是否尚未安装 LSC，如图所示。例如，在 79XX 系列电话上，请导航至设置 > 4 - 安全配置 > 4 - LSC 。

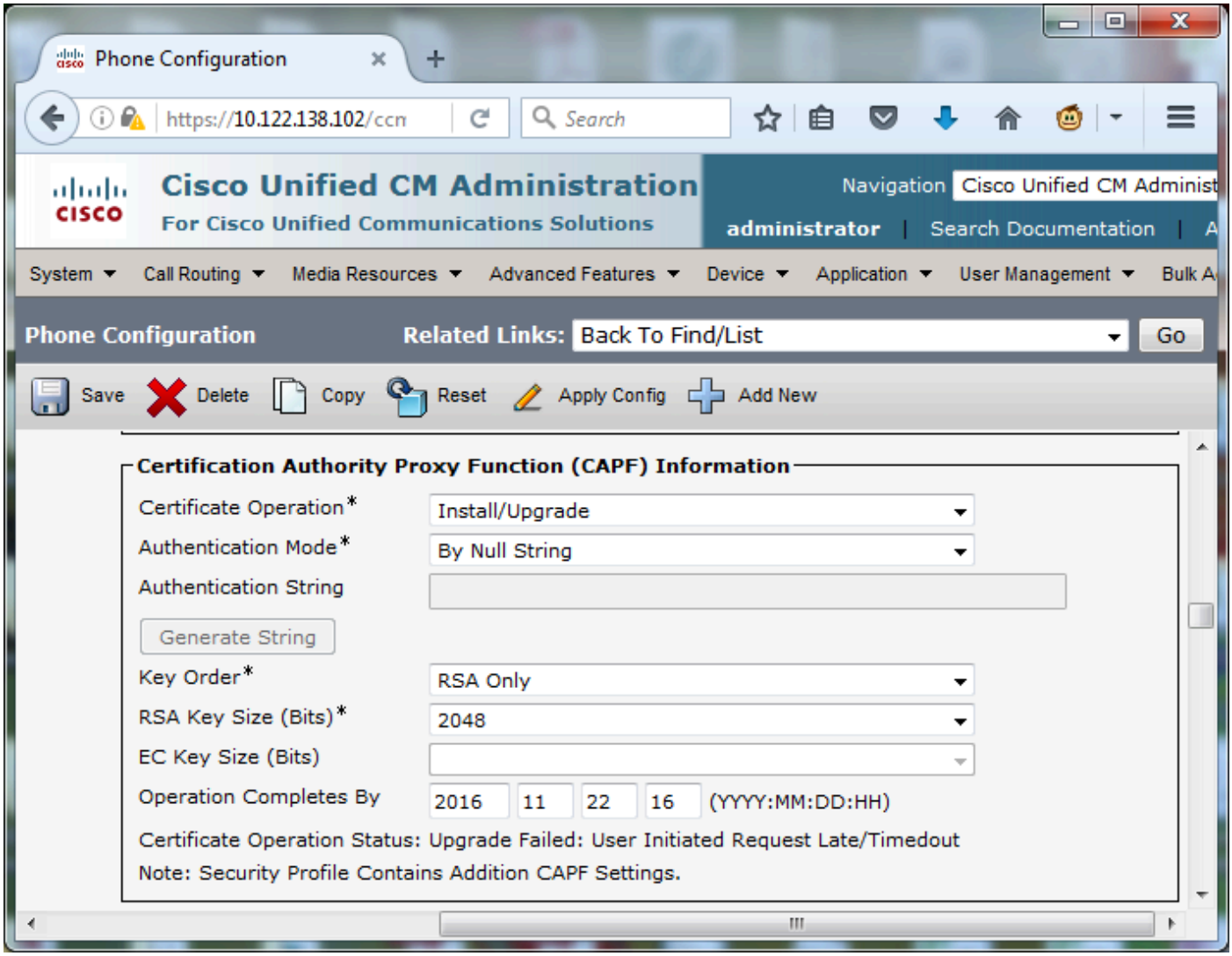


打开电话的电话配置页面。依次导航至 Cisco Unified CM 管理 > 设备 > 电话。

将以下详细信息输入电话配置的“CAPF 信息”部分，如图所示：

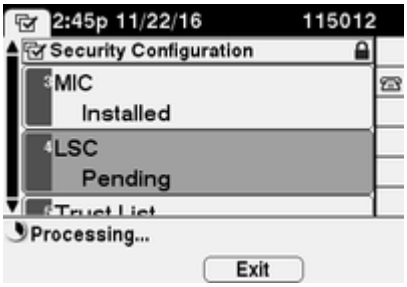
- 对于证书操作，请选择安装/升级。
- 对于身份验证模式，请选择按 Null 字符串。

- 对于本例，密钥顺序、RSA 密钥大小（位）和 EC 密钥大小（位）保留为系统默认设置。
- 对于操作完成时间，请输入至少一小时后的日期和时间。

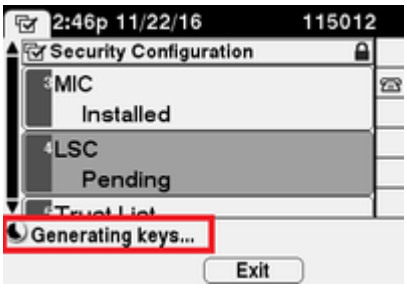


保存配置更改，然后单击Apply Config。

电话上的 LSC 状态更改为“待处理”，如图所示。



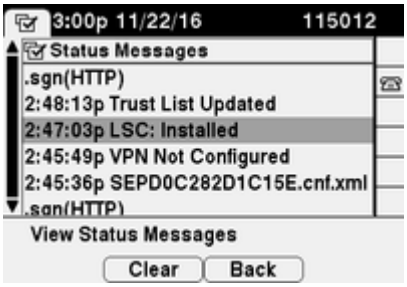
电话将生成密钥，如图所示。



电话将重置，并且重置完成后，电话 LSC 状态更改为已安装，如图所示。



这也可在电话的“状态消息”下看到，如图所示。



验证

使用本部分可确认配置能否正常运行。

要验证多部电话上的 LSC 证书安装情况，请参阅 Cisco Unified Communications Manager 管理指南版本 11.0(1) 的生成 CAPF 报告部分。 或者，您可以使用按 LSC 状态或身份验证字符串查找电话操作步骤在 CUCM 管理 Web 界面中查看相同的数据。

要获取电话中安装的 LSC 证书的副本，请参阅文章如何从思科 IP 电话检索证书。

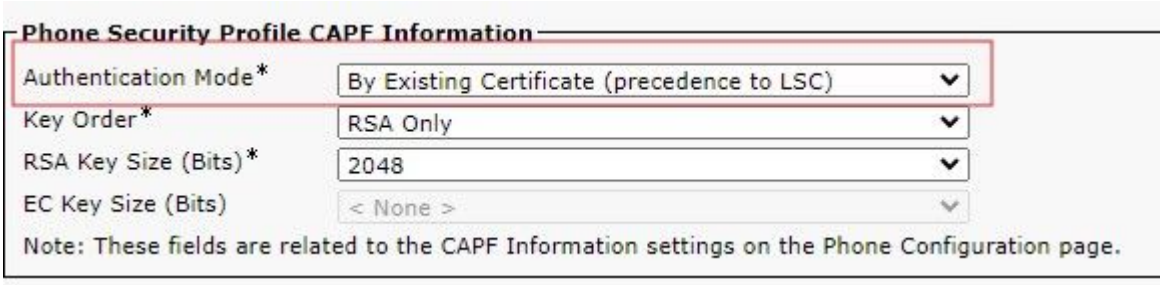
LSC 批量安装

根据此部分的说明将 LCS 批量上传到相同型号的电话。

1. 依次导航至批量管理 > 电话 > 更新电话 > 查询。
2. 查找设备类型包含 <enter four digit model number> 的电话，选择查找，然后选择下一步 。
3. 滚动到证书颁发机构代理功能 (CAPF) 信息部分。
4. 在下拉部分中，选择安装/升级。

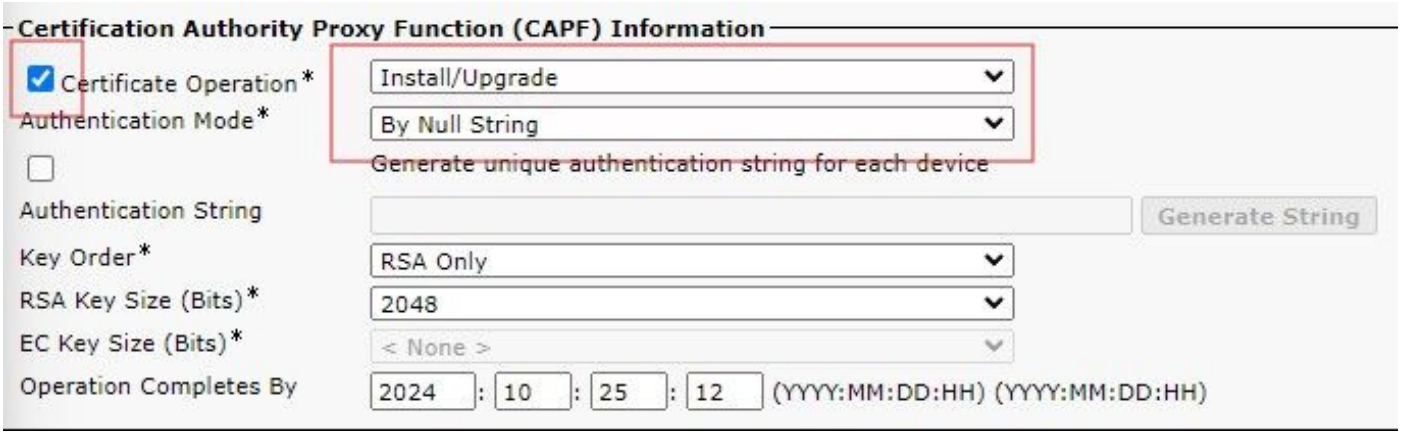
使用批量管理并选择身份验证模式时，身份验证模式必须与电话安全配置文件的操作匹配。 如果存在不匹配项，例如电话安全配置文件中的“按 Null 字符串批量执行”和“按现有证书（优先于 LSC）”，则操作无法完成。

检查电话安全配置文件和身份验证模式，以确保您使用的是正确的模式。



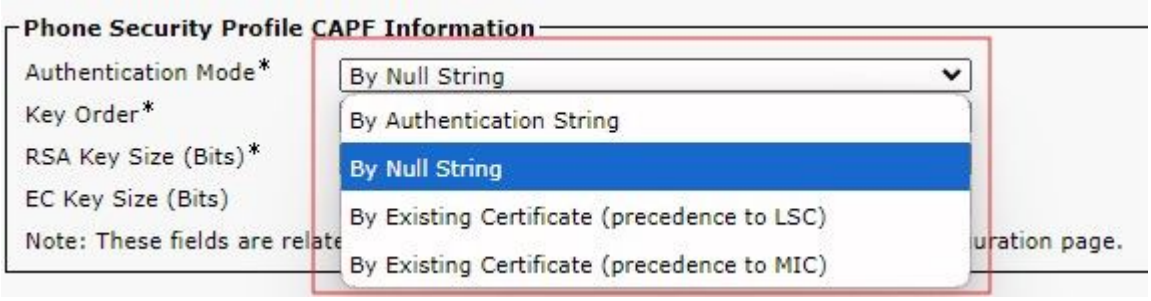
按 LSC 优先级排序的 LSC

要设置批量配置，请在下拉列表中选择与电话安全配置文件匹配的身份验证模式 。



批量选择

如果更改电话安全配置文件身份验证模式，则需要保存，然后应用配置。 这可能会导致使用特定电话安全配置文件的设备重新启动。



身份验证选择

故障排除

本部分提供了可用于对配置进行故障排除的信息。

无有效 CAPF 服务器

LSC 安装失败。电话的状态消息显示“无有效的 CAPF 服务器”。 这表示 ITL 文件中没有 CAPF 条目。验证 CAPF 服务是否已激活，然后重新启动 TFTP 服务。重新启动后，验证 ITL 文件是否包含 CAPF 证书，重置电话以获取最新的 ITL 文件，然后重试证书操作。如果电话安全设置菜单中的 CAPF 服务器条目显示为主机名或完全限定域名，请确认电话能够将该条目解析为 IP 地址。

LSC：连接失败

LSC 安装失败。电话的状态消息显示“LSC：连接失败”。 这可能表示存在下列其中一种情况：

- ITL 文件中的 CAPF 证书与当前证书不匹配，CAPF 服务正在使用中。
- CAPF 服务已停止或已停用。
- 电话无法通过网络访问 CAPF 服务。

验证 CAPF 服务是否已激活，重新启动 CAPF 服务以及已启动的 TFTP 服务，重置电话以获取最新的 ITL 文件，然后重试证书操作。如果问题仍然存在，请从电话和 CUCM 发布方处捕获数据包并进行分析，以查看端口 3804（默认的 CAPF 服务端口）上是否存在双向通信。如果不存在双向通信，则可能是网络问题。

LSC：失败

LSC 安装失败。电话的状态消息显示“LSC：失败”。 “电话配置”网页显示“证书操作状态：升级失败:用户发起的请求延迟/超时”。 这表明操作完成时间和日期已到期或已经过去。输入至少一小时后的日期和时间，然后重试证书操作。

LSC：操作挂起

LSC 安装失败。电话的状态消息显示“LSC：连接失败”。 “电话配置”页面显示“证书操作状态：操作待处理”。 用户可以看到“证书操作状态：操作待处理”状态的原因各不相同。其中一些措施包括：

- 电话上的 ITL 与当前在已配置 TFTP 服务器上使用的 ITL 不同。
- 损坏的 ITL 存在问题。发生这种情况时，设备将失去受信任状态，需要从 CUCM 发布方运行命令 utils itl reset localkey 以强制电话立即使用 ITLRecovery 证书。如果集群处于混合模式，则需要使用命令 utils ctl reset localkey。接下来，您会看到一个示例，说明当您尝试从 CUCM 的 CLI 查看损坏的 ITL 时可以看到的内容。如果在尝试查看 ITL 并尝试运行 utils itl reset localkey 命令时出现错误，但看到的是第二个错误，则这可能是思科漏洞 ID CSCus33755。 确认 CUCM 的版本是否受到影响。

```
admin:show itl
Length of ITL file: 0
ITL File not found. To generate an ITL file, activate or restart the Cisco TFTP service as this command is only valid on tftp
servers.
Error parsing the ITL File.
```

```
admin:utils itl reset localkey
Enter CCM Administrator password :

Locating active Tftp servers in the cluster.....

Unable to determine the active and running  TFTP nodes in the cluster
Ensure that the DB replication is working on all nodes and the correct Password has been entered
Then retry the command

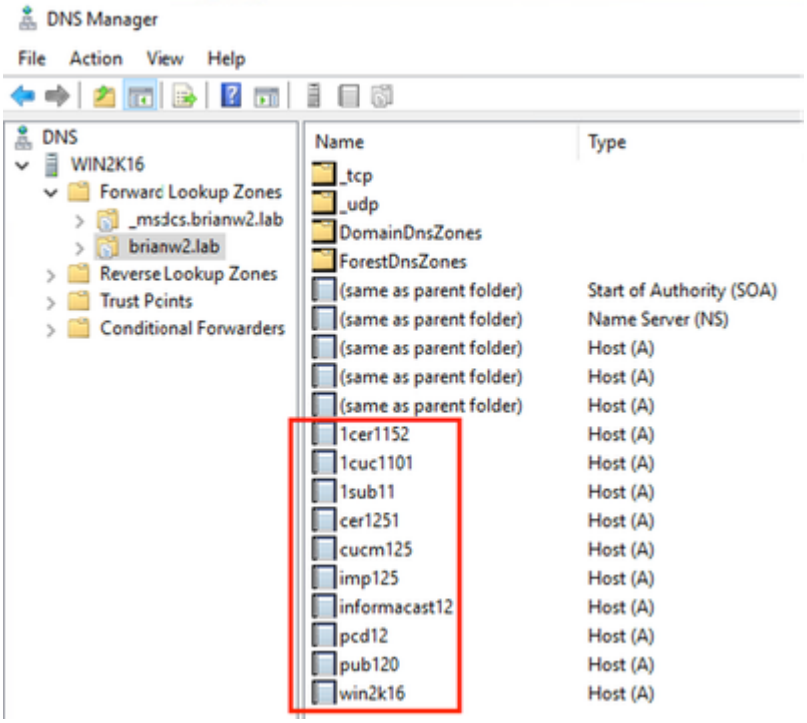
Executed command unsuccessfully
chmod: changing permissions of `/var/log/active/cm/trace/dbl/sdi/replication_scripts_output.log': Operation not permitted
```

- 由于 TVS 故障，电话未能对新 LSC 进行身份验证。
- 电话将使用 MIC 证书，但电话配置页面上的“证书颁发机构代理功能 (CAPF) 信息”部分会将“身份验证模式”设置为“按现有证书（优先于 LSC）”。
- 电话无法解析 CUCM 的 FQDN。

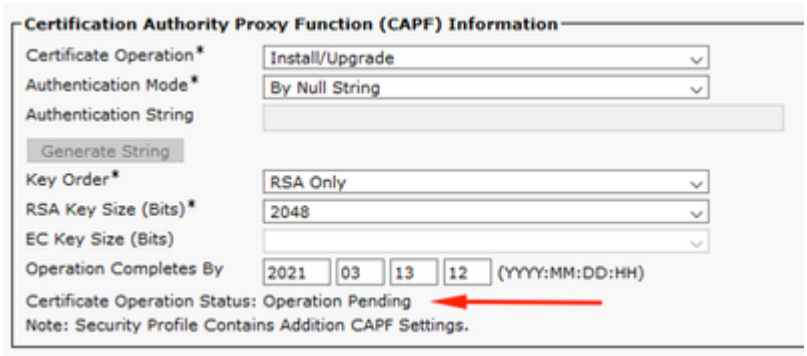
对于最后一个场景，设置了一个实验环境来模拟在电话无法解析 CUCM 的 FQDN 时日志中将会显示的内容。目前，该实验设置了以下服务器：

- 运行版本 11.5.1.15038-2 的 CUCM 发布方和订用方
- 设置为用户的 DNS 服务器的 Windows 2016 Server

对于测试，没有配置 PUB11 CUCM 服务器的 DNS 条目。



已在实验中尝试将 LSC 推送到其中一部电话 (8845)。查看它是否仍显示“证书操作状态：操作挂起.



在电话控制台日志中，查看电话是否尝试查询其本地缓存 (127.0.0.1)，然后再将查询转发到已配置的 DNS 服务器地址。

```
0475 INF Mar 12 15:07:53.686410 dnsmasq[12864]: query[A] PUB11.brianw2.lab from 127.0.0.1
0476 INF Mar 12 15:07:53.686450 dnsmasq[12864]: forwarded PUB11.brianw2.lab to X.X.X.X
0477 INF Mar 12 15:07:53.694909 dnsmasq[12864]: forwarded PUB11.brianw2.lab to X.X.X.X
```

```
0478 INF Mar 12 15:07:53.695263 dnsmasq[12864]: reply PUB11.brianw2.lab is NXDOMAIN-IPv4
0479 INF Mar 12 15:07:53.695833 dnsmasq[12864]: query[A] PUB11.brianw2.lab from 127.0.0.1
0480 INF Mar 12 15:07:53.695865 dnsmasq[12864]: cached PUB11.brianw2.lab is NXDOMAIN-IPv4
0481 WRN Mar 12 15:07:53.697091 (12905:13036) JAVA-configmgr MQThread|NetUtil.traceIPv4DNSErrors:? - DN

++ However, we see that the phone is not able to resolve the FQDN of the CUCM Publisher. This is becaus

0482 ERR Mar 12 15:07:53.697267 (12905:13036) JAVA-configmgr MQThread|cip.sec.TvsProperty:? - Failed to

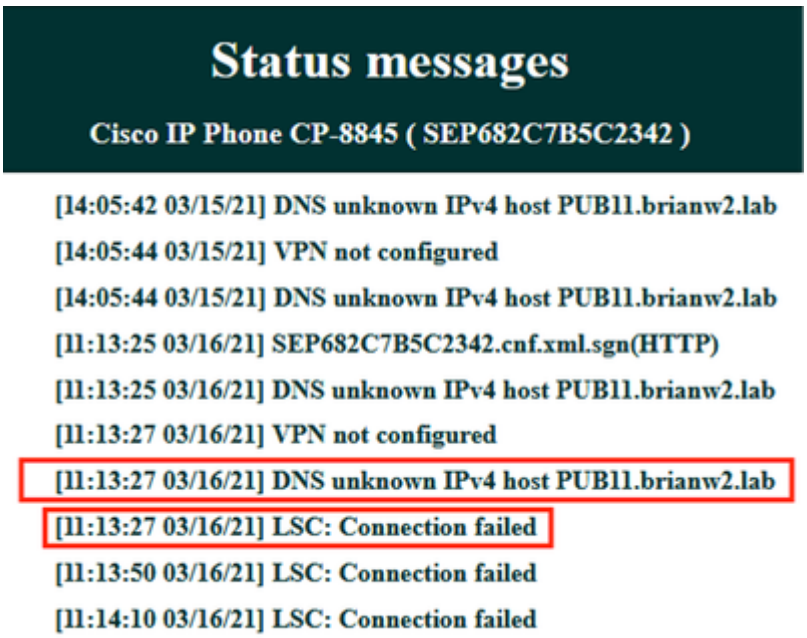
++ Afterwards, we see the CAPF operation fail. This is expected because we do not have a DNS mapping fo

0632 NOT Mar 12 15:07:55.760715 (12905:13036) JAVA-configmgr MQThread|cip.sec.CertificateProperty:? - C
0633 NOT Mar 12 15:07:55.761649 (322:17812) SECUREAPP-RCAPF_START_MODE: Start CAPF - mode:[1]([NULL_STR
0634 NOT Mar 12 15:07:55.761749 (322:17812) SECUREAPP-CAPF_CLNT_INIT:CAPF clnt initialized
0635 NOT Mar 12 15:07:55.761808 (322:17812) SECUREAPP-CAPFClnt: SetDelayTimer - set with value <0>
0636 ERR Mar 12 15:07:55.761903 (322:17812) SECUREAPP-Sec create BIO - invalid parameter.
0637 ERR Mar 12 15:07:55.761984 (322:17812) SECUREAPP-SEC_CAPF_BIO_F: CAPF create bio failed
0638 ERR Mar 12 15:07:55.762040 (322:17812) SECUREAPP-SEC_CAPF_OP_F: CAPF operation failed, ret -7
0639 CRT Mar 12 15:07:55.863826 (12905:13036) JAVA-configmgr MQThread|cip.sec.CertificateProperty$1:? -

++ What we would expect to see is something similar to the following where DNS replies with the IP addr

4288 INF Mar 12 16:34:06.162666 dnsmasq[12864]: query[A] PUB11.brianw2.lab from 127.0.0.1
4289 INF Mar 12 16:34:06.162826 dnsmasq[12864]: forwarded PUB11.brianw2.lab to X.X.X.X
4290 INF Mar 12 16:34:06.164908 dnsmasq[12864]: reply PUB11.brianw2.lab is X.X.X.X
4291 NOT Mar 12 16:34:06.165024 (12905:13036) JAVA-configmgr MQThread|cip.sec.TvsProperty:? - Resolve T
```

在电话状态消息中，可看到电话无法解析 PUB11.brianw2.lab。之后，可看到“LSC：连接”失败消息。



需要考虑的缺陷：

思科漏洞 ID CSCub62243 - LSC 安装间歇性失败，随后冻结 CAPF 服务器。

需要考虑的增强功能缺陷：

思科漏洞 ID CSCuz18034 - 需要报告安装了 LSC 的终端以及到期状态。

相关信息

这些文档提供了有关在 AnyConnect VPN 客户端身份验证和 802.1X 身份验证情景中使用 LSC 的更多信息。

- AnyConnect VPN 电话 - IP 电话、ASA 和 CUCM 故障排除
- 基于身份的网络服务：支持 IEEE 802.1X 网络中的 IP 电话部署和配置指南

还有一种高级类型的 LSC 配置，其中 LSC 证书由第三方证书颁发机构而不是 CAPF 证书直接签署。

有关详细信息，请参阅：CUCM 第三方 CA 签名的 LSC 生成和导入配置示例

- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。