配置在Cisco IP电话的LSC与CUCM

目录

简介

本文描述如何安装一局部重要的证书(LSC)在思科互联网协议电话(Cisco IP电话)。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco Unified Communications Manager (CUCM)团星安全模式选项
- X.509证书
- 制造的已安装证书(MICs)
- LSCs
- 认证机关代理功能(CAPF)证书操作
- 默认情况下安全(SBD)
- 最初的托拉斯列表(ITL)文件

使用的组件

本文档中的信息根据支持SBD，即CUCM 8.0(1)以上的CUCM版本。

> **Note**:它只也适合于到支持SBD的电话。例如， 7940个和7960个电话不支持SBD，亦不7935个， 7936个和7937个会议电话。对于支持在CUCM您的版本的SBD设备的列表，请导航对**报告>System报告的Cisco Unified >统一CM电话功能列表**并且送关于**功能的**一报告：**安全默认情况下**。

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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

MICs与LSCs

如果使用身份验证802.1X或Anyconnect电话的VPN基于验证，它是重要了解在MICs和LSCs之间的区别。

每个Cisco电话附有MIC被事先装配在出厂。此证书由制造CA证书，由思科制造CA，思科的一个思科签字制造CA SHA2、CAP-RTP-001或者CAP-RTP-002证书。当电话提交此证书时，证明，它是一个有效Cisco电话，但是这不验证电话属于一特定客户或CUCM集群。它能潜在是从一个不同的站点采购在开放的市场或带来的一个恶意电话。

LSCs，另一方面，在电话故意地安装由管理员和由CUCM发行商的CAPF证书签字。您会配置802.1X或Anyconnect VPN只委托已知CAPF证书权限发出的LSCs。根据证书验证而不是MICs的LSCs提供您电话设备是委托的一更加粒状的控制。

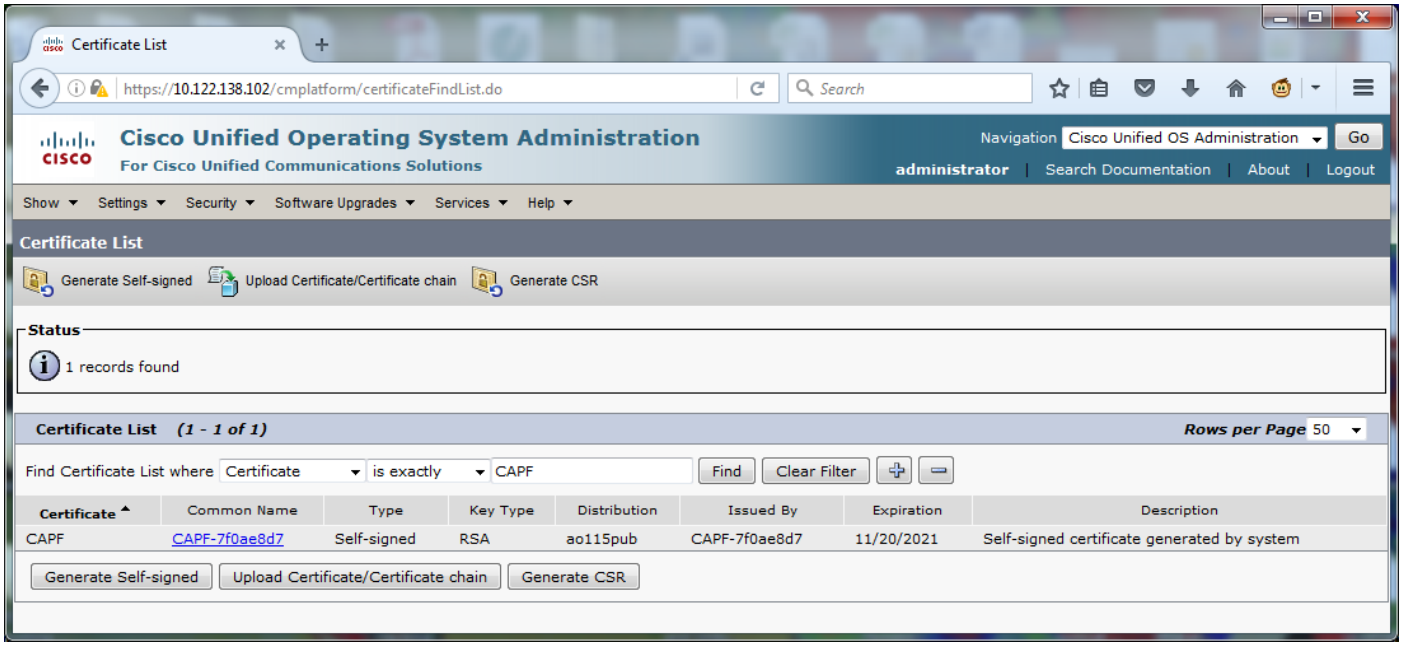
配置

网络拓扑

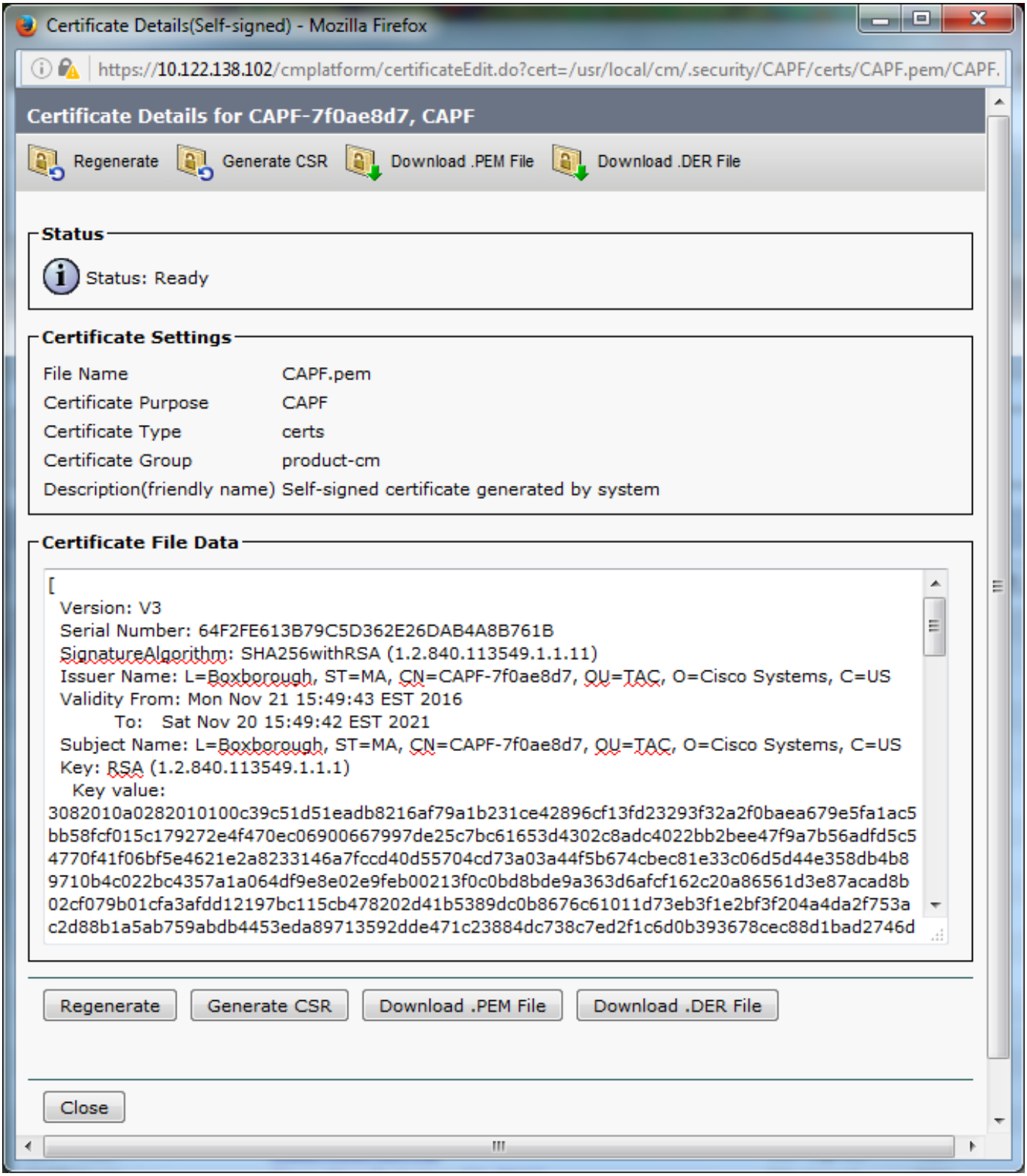
这些CUCM实验室服务器使用了本文：

- ao115pub - 10.122.138.102 - CUCM发行商& TFTP server
- ao115sub - 10.122.138.103 - CUCM用户& TFTP server

验证CAPF证书未超时，亦不在不久的将来超时。导航对**Cisco Unified OS管理> Security > Certificate Management**，然后**查找**如镜像所显示，**证书正确地是CAPF的证书列表**。



点击**公用名称**为了打开证书详细信息页。检查正确性**从：**并且**对：**在**证书文件数据**窗格的日期为了确定，当证书超时如镜像所显示。



如果CAPF证书超时或者很快是超时，重新生成该证书。请勿移动向前与与已到期的LSC安装进程也很快请勿超时CAPF证书。这避免需要在不久的将来补发LSCs由于CAPF证书到期。关于如何重新生成CAPF证书的信息，请参考CUCM证书重新生成/更新过程条款。

同样地，如果需要安排您的CAPF证书签字由第三方认证机关，您有在此阶段做一的选择。当前请完成签字的CAPF证书的证书签名请求(CSR)文件生成和进口或者继续与一自已签署的LSC的配置初试的。 如果需要第三方签字的CAPF证书，通常是易于的首先配置此功能与一自已签署的CAPF证书，测验和验证，然后调遣由第三方签字的CAPF证书签字的LSCs。如果与第三方的测验签署了CAPF证书失败，这简化最新故障排除。

警告：如果重新生成CAPF证书或导入一第三方签字的CAPF证书，当CAPF服务被启动并且开始时，电话由CUCM自动地重置。当重置时，电话是可接受的请完成在维护窗口的这些步骤。关于参考，请参阅CSCue55353 -请添加警告，当重新生成该时TVS/CCM/CAPF的证书给重置打电话。

Note:如果您的CUCM版本支持SBD，此LSC安装程序不管怎么样应用，如果您的CUCM集群设置对混合模式。SBD是CUCM版本8.0(1)和以上的部分。在CUCM中这些版本，ITL文件包含CAPF服务的证书在CUCM发行商。这允许电话连接到CAPF服务为了支持证书操作例如安装/升级并且排除故障。

在CUCM中以前版本，配置混合模式的集群为了支持证书操作是必要的。因为这不再是必要的，这使障碍降低到使用LSCs作为电话身份证书802.1X验证的或AnyConnect VPN客户端验证的。

运行**显示itl** on命令在CUCM集群的所有TFTP服务器。注意到ITL文件包含CAPF证书。

例如，这是从实验室CUCM用户输出的**显示itl的**摘要ao115sub。

Note:有在此文件的一个ITL记录条目有CAPF的功能的。

Note:如果您的ITL文件没有一个CAPF条目，登陆给您的CUCM发行商并且确认CAPF服务被启动。为了确认此，导航对**Cisco Unified维护性> Tools > Service激活> CUCM发行商> Security**，然后启动**思科认证机关代理功能服务**。如果撤销了服务，并且激活它，请导航对**Cisco Unified维护性> Tools > Control Center –以Services> Server> CM服务为特色**，则重新启动在所有TFTP服务器的Cisco Tftp服务在CUCM集群重新生成ITL文件。并且，请保证您不点击CSCuj78330。

Note: 在您执行后，请运行**显示itl** on命令在CUCM集群的所有TFTP服务器为了验证当前CUCM发行商CAPF证书在文件当前包括。

```
 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
```

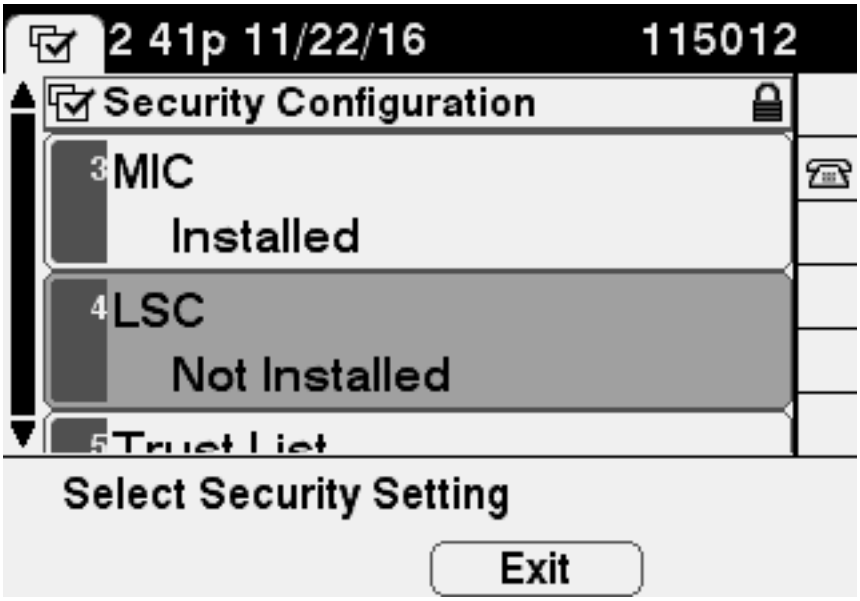
```
7 PUBLICKEY 270
8 SIGNATURE 256
9 CERTIFICATE 959 20 BD 40 75 51 C0 61 5C 14 0D 6C DB 79 E5 9E 5A DF DC 6D 8B (SHA1 Hash HEX)

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.
```

当CAPF条目被确认作为在ITL的一个条目，您能完成在电话的一证书操作。在本例中，一2048个位RSA证书利用空字符串验证安装。

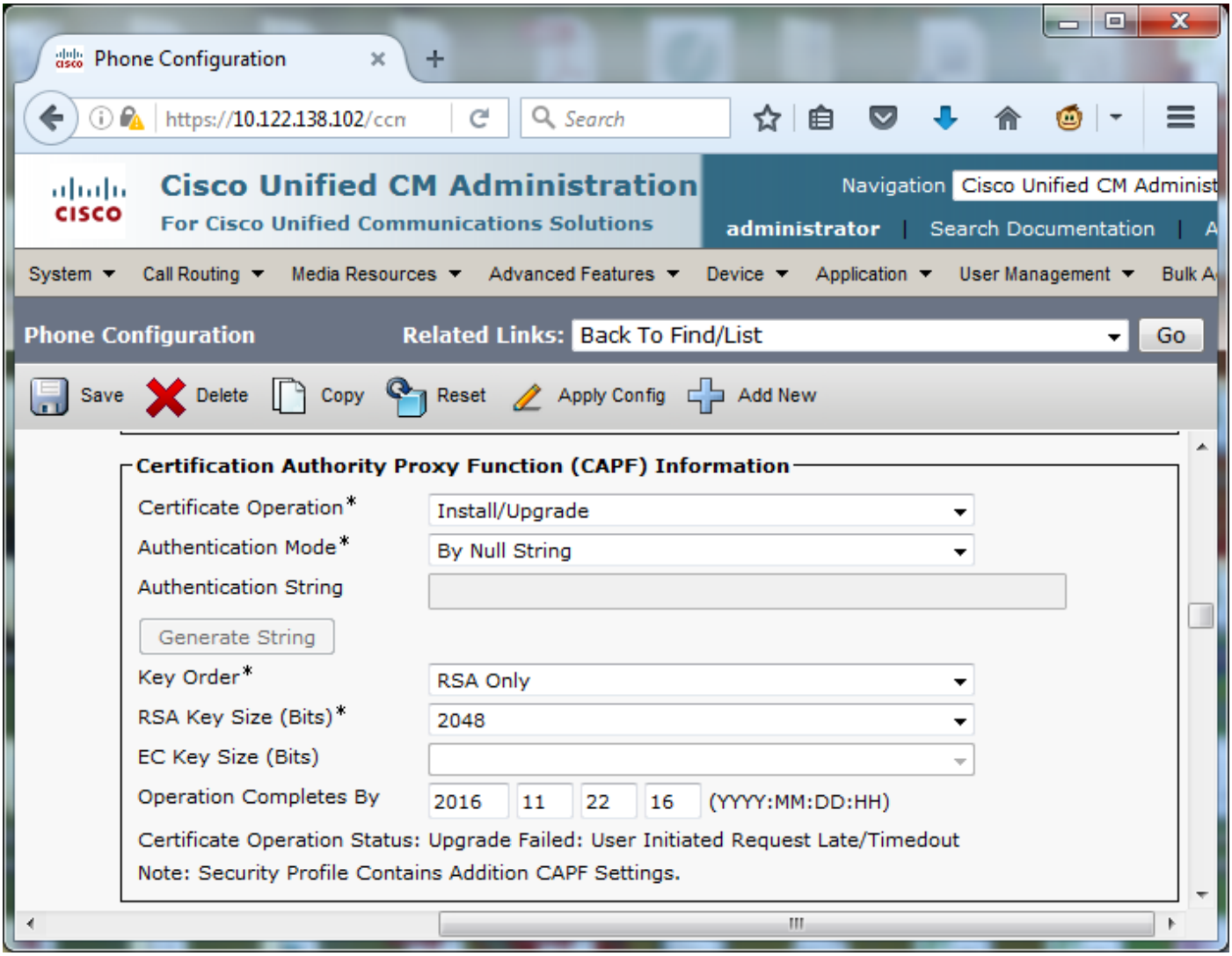
在电话上，请验证如镜像所显示， LSC没有安装。例如，在79XX系列打电话，导航对**设置> 4 -安全配置> 4 - LSC**。



打开您的电话的Phone Configuration页。导航对**Cisco Unified CM Administration > Device > Phone**。

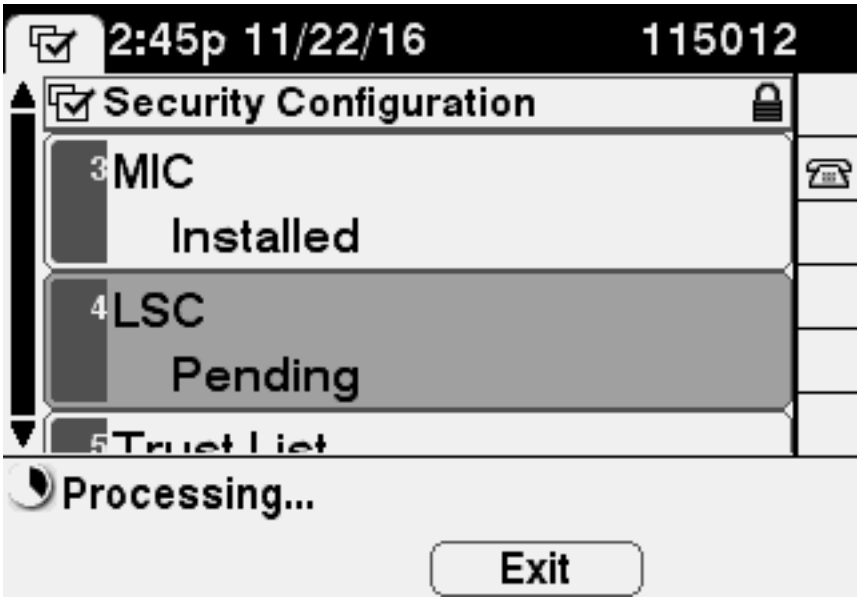
如镜像所显示，输入这些详细信息对电话配置的CAPF信息部分， ：

- 对于证书操作，请选择**安装/升级**
- 对于认证模式，请**由空字符串**选择
- 对于此示例，请留下关键命令、RSA密钥大小(比特)和EC密钥大小(比特)集给**系统默认**。
- 对于操作完成由，输入是至少一个小时对未来的日期和时间。

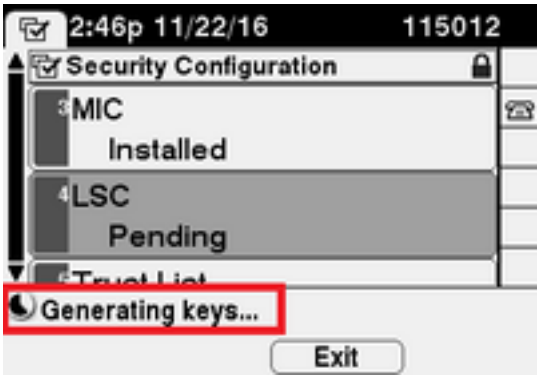


保存您的配置更改，然后**运用设置**。

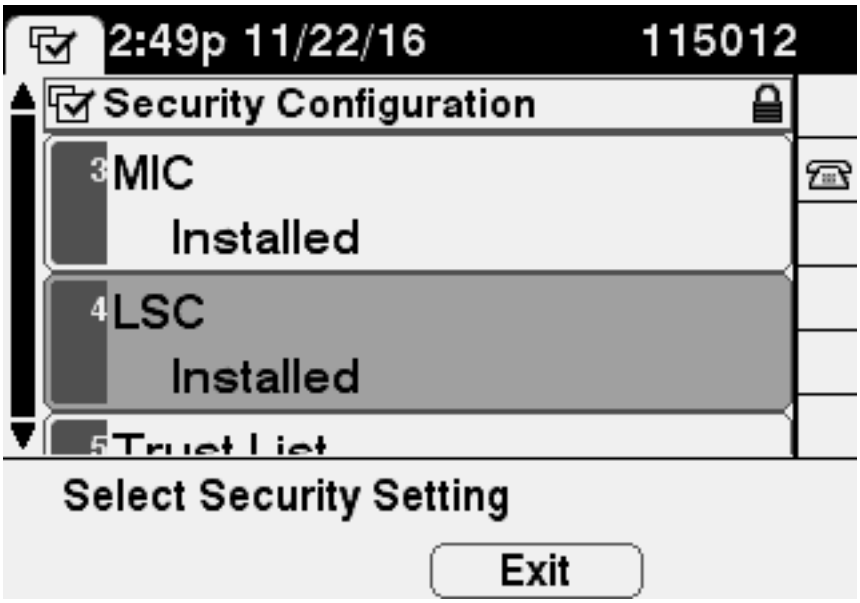
如镜像所显示，在电话的LSC状态更改对**待定**。



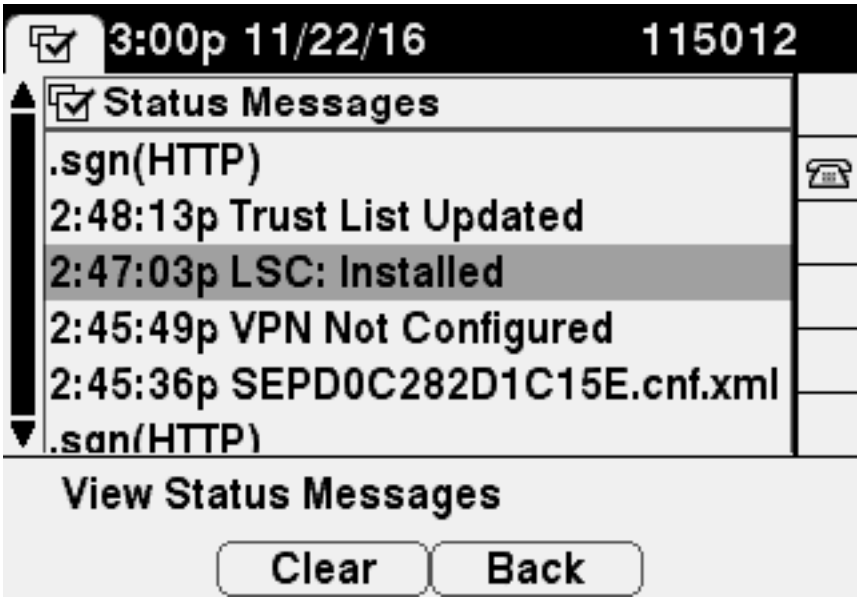
如镜像所显示，电话生成密钥。



电话重置，和，当重置完成，对**已安装的**电话LSC状态变化如镜像所显示。



如镜像所显示，这也是在电话的可视下面**状态消息**。



验证

使用本部分可确认配置能否正常运行。

为了验证多个电话的LSC认证安装，为Cisco Unified Communications Manager请参考安全指南生

成CAPF报告栏，版本11.0(1)。或者，您可以利用查找电话查看在CUCM管理Web接口内的同一个数据由LSC状态或认证字符串步骤。

为了得到在电话安装的LSC证书的复制，请参考如何从思科IP phonesarticle获取证书。

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不能安装。电话的状态消息不显示**有效CAPF服务器**。这表明没有在ITL文件的CAPF条目。验证CAPF服务被启动了，然后重新启动TFTP服务。验证ITL文件包含CAPF证书，在重新启动，重置电话拾起最新的ITL文件后，然后再试您的证书操作。如果在电话的安全设置菜单显示的CAPF服务器项作为主机名或完全限定域名，确认电话能解决条目到IP地址。

LSC ：连接失败

LSC不能安装。电话的状态消息显示**LSC ：连接失败**。这可能指示这些情况之一：

- CAPF证书在ITL文件和当前证书之间的一不匹配， CAPF服务是在使用中的。
- CAPF服务被终止或被撤销。
- 电话不能到达在网络的CAPF服务。

验证CAPF服务激活，重新启动CAPF服务，重新启动TFTP服务集群域内，重置电话拾起最新的ITL文件，然后再试您的证书操作。如果问题持续，请采取从电话和CUCM发行商的一数据包捕获，并且分析为了发现是否有在端口3804的双向通信，默认CAPF服务端口。否则，可能有网络问题。

LSC ：失败

LSC不能安装。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：失败的升级：用户发起的请求后/Timedout**。这表明操作在时间与日期之前完成以前超时或是。输入是至少一个小时对未来的日期和时间，然后再试您的证书操作。

相关信息

这些文档在使用提供更多信息LSCs在上下文为AnyConnect VPN客户端验证和802.1X验证。

- AnyConnect VPN电话- IP电话， ASA和CUCM排除故障
- 基于身份的网络服务：在IEEE 802.1X启用的网络部署和配置指南的IP电话

也有LSC配置的一种先进的类型， LSC证书直接地由第三方签字认证机关，不是CAPF证书。

关于详细信息，请参考： CUCM第三方CA签名的LSCs生成和导入配置示例

- **技术支持和文档 - Cisco Systems**