

# 与第三方证书配置示例的安全Cisco Unified CME

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置](#)

[概略的配置步骤](#)

[详细配置示例](#)

[相关信息](#)

## 简介

许多网络管理员选择实现Cisco Unified Communications Manager Express (CME)以安全。而不是内置的IOS认证机关(IOS-CA)，网络管理员能选择集成与他们的现有公共密钥基础设施(PKI)基础设施的安全CME。本文描述如何配置安全CME运行与安全信令和媒体，通过第三方证书。

## [先决条件](#)

### [要求](#)

本文假设，Cisco Unified Communications Manager Express (CME)在您的环境运行和功能完备的。一定是可操作的在Secure Cisco Unified CME的所有电话需要能成功首先注册到CME。关于如何配置CME的信息，参考[Cisco Unified Communications Manager Express系统管理员指南](#)。

本文也假设，语音和安全功能启用。

### [使用的组件](#)

本文档中的信息根据Cisco Unified Communications Manager Express (CME)。

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。

### [规则](#)

有关文档规则的信息，请参阅 [Cisco 技术提示规则](#)。

# 配置

注意：使用[命令查找工具](#) ([仅限注册用户](#)) 可获取有关本部分所使用命令的详细信息。

## 概略的配置步骤

1. 创建IOS-CA实例。
2. 创建信任点有第三方CA证书。
3. 生成证书签名请求(CSR)从信任点。
4. 签署与服务器验证使用情况的CSR，并且获取CA证明。
5. 验证与CA证书的信任点，并且导入各自身份证书。
6. 验证第三方证书信任点。
7. 创建IOS CA CME信任点。
8. 配置证书信任列表(CTL)客户端。
9. 配置认证机关代理功能(CAPF)服务器。
10. 配置电话服务。
11. 配置测试电话。
12. 验证。

## 详细配置示例

1. 创建IOS-CA实例。IOS-CA实例生产使用签署电话的局部重要的证书的自签名证书(LSC)。

```
crypto key gen rsa label ios-ca mod 2048
The name for the keys will be: ios-ca
% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 17 seconds)

crypto pki server ios-ca
database level complete
grant auto
lifetime cert 7305
exit
ip http server
crypto pki trust ios-ca
enrollment url http://10.2.3.4:80
revo none
rsa key ios-ca
exit
crypto pki server ios-ca
no shut
%Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit
Password: Cisc0123
Re-enter password: Cisc0123
% Certificate Server enabled.
exit
```

2. 创建将生成第三方签字的CSR的信任点。这些信任点最终有第三方CA证书，以及身份证书，是CSR的结果。

```
crypto key generate rsa label tac-sast mod 2048
The name for the keys will be: tac-sast
% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 52 seconds)
```

```
crypto pki trust tac-sast
enroll term
serial-number none
fqdn none
ip-address none
subject-name CN=tac-sast
revo none
rsakeypair tac-sast
exit
```

### 3. 生成从信任点的CSR。crypto pki登记提供给第三方CA签字的命令生产CSR。

#### 示例 1 :

```
crypto pki enroll tac-sast
% Start certificate enrollment ..
% The subject name in the certificate will include: CN=tac-sast
% The fully-qualified domain name will not be included in the certificate
Display Certificate Request to terminal? [yes/no]: yes
Certificate Request follows:
MIICfjCCAAYCAQAwGDEWMBQGA1UEAxMNam9jYXNhbGUtc2FzdDCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBALLIyM0k5DmgWyljILHy+eaoJTU+OioaTfFO
V7SdNOFjoXCRpqCZwFavR82/Wukoho9HUXB7/oEQV6D2UoyHRh1lmzHv5AxuJuE1
0Qk9YHpBzLAcNEvRWvnyVnMaBSc6Fy9j7oabAUuOoWveK8Nrsor38WH2gIY3kUaM
8swgaomqlAj8LbmYE/PQdtfxOEneIF1FHHXj4R72dqkCaiBz7fc09sdxfrqi8jEf
UbndH9yZit912wXl4nxC2Wa2S30/p6vXEwKfQMGZe4nO7SJPtJ/vNHx/HNCKJxHV
H1V0JH7Affffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
ffffffffffffffffffffffffffffffffEAAAhMB8G
CSqGSIB3DQEJdJESMBAdGyDVR0PAQH/BAQDAgWgMA0GCSqGSIB3DQEBBAUAA4IB
AQB+utK7EpeGYyPfnALsXkPcbu+2kwi/TI+B2kT3ol/dxyX6hNh0jp3eOTQtS1
H7jRey4ew9GZVTEqq7cxwz1f7d6ZP4BRqzplf0HVvu7HC+bar0jB2FNvVan27zYu
XSP/GIaUiQDTbaEyDgGr8s5PlFSS2Ap4FvxsskjD/30geszhRs+N3cYfQVpnWjnj
TwbMF4998BXm1PIQigJBIInACY2SUszqcDih7NclY6viYaSiN0ZCuzEyKI2tjbuUU
EU/o0fcWMXsnBc44WQBAEPtBSLYFVb4kG19AgAyOW7q9ACiBTpmullkwuDyTPg5X
fCIWUjVftWoHizqxKSbLQ2nL
---End - This line not part of the certificate request---
Redisplay enrollment request? [yes/no]: no
```

#### 示例 2 :

```
crypto pki enroll tac-sast
% Start certificate enrollment ..
% The subject name in the certificate will include: CN=tac-sast
% The fully-qualified domain name will not be included in the certificate
Display Certificate Request to terminal? [yes/no]: yes
Certificate Request follows:
MIICfjCCAAYCAQAwGDEWMBQGA1UEAxMNam9jYXNhbGUtc2FzdDCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBALLIyM0k5DmgWyljILHy+eaoJTU+OioaTfFO
V7SdNOFjoXCRpqCZwFavR82/Wukoho9HUXB7/oEQV6D2UoyHRh1lmzHv5AxuJuE1
0Qk9YHpBzLAcNEvRWvnyVnMaBSc6Fy9j7oabAUuOoWveK8Nrsor38WH2gIY3kUaM
8swgaomqlAj8LbmYE/PQdtfxOEneIF1FHHXj4R72dqkCaiBz7fc09sdxfrqi8jEf
UbndH9ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
ffffffffffffffffffffffffffffffffHNCKJxHV
H1V0JH7AwWLDnUgEWGoSFOL5j/lwIHmemUDpSuL9IY+9EP622E0CAwEAAAhMB8G
CSqGSIB3DQEJdJESMBAdGyDVR0PAQH/BAQDAgWgMA0GCSqGSIB3DQEBBAUAA4IB
AQB+utK7EpeGYyPfnALsXkPcbu+2kwi/TI+B2kT3ol/dxyX6hNh0jp3eOTQtS1
H7jRey4ew9GZVTEqq7cxwz1f7d6ZP4BRqzplf0HVvu7HC+bar0jB2FNvVan27zYu
XSP/GIaUiQDTbaEyDgGr8s5PlFSS2Ap4FvxsskjD/30geszhRs+N3cYfQVpnWjnj
```







```
C/e28VwavV4piIXK4FuZKB1iltOo9MZAGH9PvVE0+yG8zpeIcwOgDq951qJejeBA
+N+ryCFy5TEbiMF3pwlXjdbBAProJlslQ0QcjoigPntPygRfehdlhMUo4NgC/svX
5VZSfxpagaBhdpUNVYo2s0ujXujuI/aTRpbDan2h7n27tMMBtDcocpQgPv6txDoR
b+Qb8CPZt3IvuEXAru4cRv101jYUWlY59ta5uELSnA+2WA36PiMxIyLu67WlRI05
1rFcB0mIQ8vTpqyNp8/TFOpOSnQMO30w9Fs=
-----END CERTIFICATE-----
quit
% Router Certificate successfully imported
```

- 一旦CA和身份证书装载到各自信任点，请验证每信任点的证书链。此步骤保证上一个步骤顺利地完成。

```
crypto pki cert validate tac-cme
Chain has 2 certificates
Certificate chain for tac-cme is valid
```

```
crypto pki cert validate tac-sast
Chain has 2 certificates
Certificate chain for tac-sast is valid
```

- 创建IOS CA CME信任点。

由于IOS-CA信任点不可能用于客户端验证(传输级安全性(TLS)连接用电话)，您在它必须创建另一信任点和放置IOS-CA证书。

此信任点用于只授权IP电话的要求TLS连接(因此他们能适当地注册)。

```
crypto pki trust ios-ca-cme
enroll url http://10.2.3.4:80
revo none
rsa key ios-ca
exit
```

```
crypto pki auth ios-ca-cme
Certificate has the following attributes:
Fingerprint MD5: 0120A3AB 44155DF9 091F31BF C3E26B80
Fingerprint SHA1: 90F9DDDE 20A792B5 3693A065 8BDAD50E 588E011C
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
```

- 配置CTL客户端。

```
ctl-client
server capf 10.2.3.4 trust tac-cme
server cme-tftp 10.2.3.4 trust tac-cme
sast1 trust tac-cme
sast2 trust tac-sast
regenerate
```

**Note:**保证CTL文件顺利地创建：

```
do sh flash | iCTL
58 8642 Aug 29 2012 13:57:22 +00:00 CTLFile.tlv
```

- 配置CAPF服务器。

```
capf-server
auth-mode null-string
cert-enroll-trust ios-ca pass 0 null
```

```
trustpoint-label tac-cme
source-addr 10.2.3.4
end
```

## 10. 配置电话服务。

```
confi t
Enter configuration commands, one per line. End with CNTL/Z.
telephony-service
secure-signaling trust tac-cme
tftp-server-credentials trust tac-cme
server-security-mode secure
cnf-file perphone
device-security-mode encrypted
exit
```

## 11. 配置测试电话(ephone)为了升级其证书和使用加密的模式。

```
ephone 1
capf-ip-in-cnf
cert-oper upgrade auth-mode null
device-security-mode encrypted
telephony-service
cre cnf
Creating CNF files
CNF-FILES: Clock is not set or synchronized, retaining old versionStamps
end
```

一旦配置完成，重置电话并且等待它注册。

**Note:**在电话重置前，请保证已经没有安全配置存在。如果安全配置存在，必须手工删除或在注册之前完成测试电话的出厂重置获取Cisco Unified CME。

要重置电话，请执行这些命令：

```
confi t
ephone 1
reset
end
```

一旦电话接收更新LSC，CERT操作升级验证模式空字符串命令删除。

```
do sh run | sec ephone
ephone 1
device-security-mode encrypted
mac-address ABCD.ABCD.ABCD
type 7960
capf-ip-in-cnf
button 1:1
sh ephone
```

## 12. 验证电话注册与验证和加密。

```
sh ephone
ephone-1[0] Mac:ABCD.ABCD.ABCD TCP
socket:[2] activeLine:0 whisperLine:0
REGISTERED in SCCP ver 11/9
max_streams=0 + Authentication + Encryption with TLS connection
mediaActive:0 whisper_mediaActive:0
startMedia:0 offhook:0 ringing:0 reset:0
reset_sent:0 paging 0 debug:0 caps:8
IP:10.2.3.10 * 51685 Telecaster 7960
keepalive 4 max_line 6 available_line 6
button 1: cw:1 ccw:(0 0)
dn 1 number 2090 CH1 IDLE CH2 IDLE
```

Preferred Codec: g711ulaw

Lpcor Type: none

安全Cisco Unified CME应该是功能完备的与第三方证书。

## 相关信息

- [Cisco Unified Communications Manager Express 系统管理员指南](#)
- [在Cisco TAC维基的安全语音](#)
- [技术支持和文档 - Cisco Systems](#)