サードパーティの証明書を使用したセキュアな Cisco Unified CME の設定例

目次

概要

多くのネットワーク管理者は、セキュリティを備えた Cisco Unified Communications Manager Express（CME）を実装することを選びます。 ネットワーク管理者は、組み込みの IOS 認証局（IOS-CA）の代わりに、Secure CME を既存のパブリック キー インフラストラクチャ（PKI）に統合できます。 このドキュメントでは、サードパーティ証明書を使用してセキュア シグナリングおよびメディアを操作するように Secure CME を設定する方法について説明します。

前提条件

要件

このドキュメントは、ご使用の環境で Cisco Unified Communications Manager Express（CME）が稼働しており、完全に機能することを前提としています。 Secure Cisco Unified CME で動作する必要がある電話機はすべて、最初に CME への登録が正常に完了できる必要があります。 CME の設定方法の詳細については、『Cisco Unified Communications Manager Express System Administrator Guide』を参照してください。

また、このドキュメントでは音声機能とセキュリティ機能の両方が有効であることも前提としています。

使用するコンポーネント

このドキュメントの情報は、Cisco Unified Communications Manager Express（CME）に基づくものです。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

設定

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

設定手順の概要

1. IOS-CA インスタンスを作成します。
2. サード パーティの CA 証明書を維持するトラストポイントを作成します。
3. トラストポイントから証明書署名要求（CSR）を生成します。
4. サーバ認証を使用して CSR に署名し、CA 証明書を取得します。
5. CA 証明書を使用してトラストポイントを認証し、該当する ID 証明書をインポートします。
6. サード パーティ証明書トラストポイントを検証します。
7. IOS CA CME トラストポイントを作成します。
8. 証明書信頼リスト（CTL）クライアントを設定します。
9. 認証局プロキシ機能（CAPF）サーバを設定します。
10. テレフォニー サービスを設定します。
11. テスト電話機を設定します。
12. 検証を行います。

詳しい設定の例

1. IOS-CA インスタンスを作成します。 IOS-CA インスタンスにより作成される自己署名証明書は、電話機のローカルで有効な証明書（LSC）の署名に使用されます。

```
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
```

```
rsakey 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: Cisco123
Re-enter password: Cisco123
% Certificate Server enabled.
exit
```

2. サード パーティ署名用 CSR を生成するトラストポイントを作成します。 これらのトラストポイントは、最終的にサード パーティの CA 証明書と、CSR の結果作成される ID 証明書を保持します。

```
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. トラストポイントから CSR を生成します。 **crypto pki enroll** コマンドは、サード パーティ CA に署名のために提供される CSR を作成します。

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:
MIICfjCCAWYCAQAwGDEWMBQGA1UEAxMNam9jYXNhbGUtc2FzdDCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBALLIyM0k5DmgWy1jILHy+eaoJTU+OioaTfFO
V7SdNOfjoXCRpqCZwFavR82/Wukoho9HUXB7/oEQV6D2UoyHRhl1mzHv5AxuJuE1
0Qk9YHpBzLAcNEvRWvnyVnMaBSc6Fy9j7oabAUuOoWveK8NrsoR38WH2gIY3kUaM
8swgaomqlAj8LbmYE/PQdtfxOEneIF1FHHXj4R72dqkCaiBz7fcO9sdxfRqi8jEf
UbndH9yZit912wX14nxC2Wa2S3O/p6vXEwKfQMGZe4nO7SJPtJ/vNHx/HNCkJxHV
H1V0JH7Affffffffffffffffffffffffffffffffffffffffffffffffffffff
ffffffffffffffffffffffffffffffEAAaAhMB8G
CSqGSIb3DQEJDjESMBAwDgYDVR0PAQH/BAQDAgWgMA0GCSqGSIb3DQEBBAUAA4IB
AQB++utK7EpeGYYyPfNALsXkPcbu+2kwi/TI+B2kT3ol/dxyX6hNh0jp3eOTQtSl
H7jRey4ew9GZVTeqq7cxwz1f7d6ZP4BRqzp1f0HVvu7HC+bAR0jB2FNvVaN27zYu
XSP/GIaUiQDTbaEyDgGr8s5PlFSS2Ap4FvxsskjD/30geszhRs+N3cYfQVpnWjnq
TwbMF4998BXmlPIQigJBInACY2SUszqcDih7Nc1Y6viYaSiN0ZCuzEyKI2tjbwUU
EU/o0fcWMXsnBc44WQBAEpTBSLYFVb4kGl9AgAyOW7q9ACiBTpmul1kwuDyTPg5X
fCIWUjVfTWoHizqxKSbLQ2nL
---End - This line not part of the certificate request---
Redisplay enrollment request? [yes/no]: no
```

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:
MIICfjCCAWYCAQAwGDEWMBQGA1UEAxMNam9jYXNhbGUtc2FzdDCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBALLIyM0k5DmgWy1jILHy+eaoJTU+OioaTfFO
V7SdNOfjoXCRpqCZwFavR82/Wukoho9HUXB7/oEQV6D2UoyHRhl1mzHv5AxuJuE1
0Qk9YHpBzLAcNEvRWvnyVnMaBSc6Fy9j7oabAUuOoWveK8NrsoR38WH2gIY3kUaM
8swgaomqlAj8LbmYE/PQdtfxOEneIF1FHHXj4R72dqkCaiBz7fcO9sdxfRqi8jEf
UbndH9fffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
ffffffffffffffffffffffffffffHNCkJxHV
H1V0JH7AwWLdnUgEWGoSFOL5j/lwIHmemUDpSuL9IY+9EP622E0CAwEAAaAhMB8G
CSqGSIb3DQEJDjESMBAwDgYDVR0PAQH/BAQDAgWgMA0GCSqGSIb3DQEBBAUAA4IB
AQB++utK7EpeGYYyPfNALsXkPcbu+2kwi/TI+B2kT3ol/dxyX6hNh0jp3eOTQtSl
H7jRey4ew9GZVTeqq7cxwz1f7d6ZP4BRqzp1f0HVvu7HC+bAR0jB2FNvVaN27zYu
XSP/GIaUiQDTbaEyDgGr8s5PlFSS2Ap4FvxsskjD/30geszhRs+N3cYfQVpnWjnq
TwbMF4998BXmlPIQigJBInACY2SUszqcDih7Nc1Y6viYaSiN0ZCuzEyKI2tjbwUU
EU/o0fcWMXsnBc44WQBAEpTBSLYFVb4kGl9AgAyOW7q9ACiBTpmul1kwuDyTPg5X
fCIWUjVfTWoHizqxKSbLQ2nL
---End - This line not part of the certificate request---
Redisplay enrollment request? [yes/no]: no
```

4. サーバ認証許可を使用して証明書を生成するには、2 つの CSR を使用します。
   注： CA からの 2 つの証明書のいずれかの完全な証明書チェーンが取得されるということが重要です。 証明書チェーンは、署名 CA から CA 証明書と ID 証明書の両方を提供します。証明書が Base 64 形式でダウンロードされていることを確認します。CA 証明書は各トラストポイントの認証用に使用され、ID 証明書がその順序で各トラストポイントにインポートされることが重要です。
5. CA 証明書を使用してトラストポイントを認証し、SAST ID 証明書をインポートします。

   例 1：

```
crypto pki auth tac-sast
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
-----BEGIN CERTIFICATE-----
MIIFQTCCBCmgAwIBAgIQUt2XjpaAwaJIEkcOebj7AjANBgkqhkiG9w0BAQUFADBs
MRMwEQYKCZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFY2lzY28xIjAg
BgoJkiaJk/IsZAEZFhJqeW91bmd0YS1sYWJkb21haW4xGjAYBgNVBAMTEWp5b3Vu
Z3RhLWNhc2VydmVyMB4XDTEyMDgxMzE1NTczM1oXDTE3MDgxNDE2MDY0M1owbDET
MBEGCgmSJomT8ixkARkWA2NvbTEVMBMGCgmSJomT8ixkARkWBWNpc2NvMSIwIAYK
CZImiZPyLGQBGRYSanlvdW5ndGEtbGFiZG9tYWluMRowGAYDVQQDExFqeW91bmd0
YS1jYXNlcnZlcjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJ2Cxwm6
uX3/t3Ip9A5OnbKS1IL4MaTCVzev7tlZbusWLQcfJwOhjFNxJJpgY2yE8CjBsL4H
eryNvcvUFeA90kXbEncl1uoI7t1JEf5ifQBopqGO54E0t1YUHrcT5LgXdBU839yp
lNm9VtFfffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
ffffffffffffffffffffffo45wsFTRpp8
DC7nGuW0erm2/ISnfoNs/mUmfWbmoAbJjIrU+RHaQ7RrcXPWB3mEqC40eQtYJFZl
tRE7DNwPriVBTpWCV+wo94DkHtn8/nc3FOWD0RIjU7Y66jG+umWSeqJh0xdZBak2
+L9A6ZwCxyeuzg0CAwEAAaOCAd0wggHZMBMGCSsGAQQBgjcUAgQGHgQAQwBBMAsG
A1UdDwQEAwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBSy5dc14lYuF1hq
yYnbrQAHPsISWzCCAUoGA1UdHwSCAUEwggE9MIIBOaCCATWgggExhoHWbGRhcDov
Ly9DTj1qeW91bmd0YS1jYXNlcnZlcixDTj1qeW91bmd0YS1jYXNlcnZlcixDTj1D
RFAsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZXMsQ049Q29u
ZmlndXJhdGlvbixEQz1qeW91bmd0YS1sYWJkb21haW4sREM9Y2lzY28sREM9Y29t
P2NlcnRpZmljYXRlUmV2b2NhdGlvbkxpc3Q/YmFzZT9vYmplY3RDbGFzcz1jUkxE
aXN0cmlifffffffffffffffffffffffffffffffffffffffffffffffffffffffff
ffffffffffffffffffffffffffffyLmp5b3Vu
Z3RhLWxhYmRvbWFpbi5jaXNjby5jb20vQ2VydEVucm9sbC9qeW91bmd0YS1jYXNl
```

```
cnZlci5jcmwwEgYJKwYBBAGCNxUBBAUCAwEAATAjBgkrBgEEAYI3FQIEFgQUWjZQ
/W2X5GoSeibbuvAKHH8/97MwDQYJKoZIhvcNAQEFBQADggEBAI8nivQcicltdXnt
X30+QO+FKK0Cu6WWFIozqKE0eeSJ0C3fPv88jjkae4+YjF/gK2wPt/mezWeQm0MO
S4m0LHnMMZGU7ezAHTd+yh5oWI2Q2iBFnslvSIUboJZazNkDEFm7Dl8gDKajEvE/
JUNtebgOJPJUXvV/v0Rpry1Nckxrn3tsiCF62acgAZke1hSrscoeqzkygk8vIr1K
lv9W2Vy2TPa6i8ZWG8at36jAsNAk5HJUEl7mFyirMIJcc+diZ12WPoRqrQ+CE7ZL
Mw+ydSS5x0XvFqily0VE649TsvtKCOMkJjbLLX8wZp9SU2AgXutHr3CdlrVlaElC
ZW4J3cQ=
-----END CERTIFICATE-----
quit
Certificate has the following attributes:
Fingerprint MD5: C198A185 83575520 EBE6E03D 33BA9B2C
Fingerprint SHA1: B0A9668D 42D36311 E82B0A33 480127B5 BEB02B60
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported


crypto pki import tac-sast cert
% The fully-qualified domain name will not be included in the certificate
Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself
-----BEGIN CERTIFICATE-----
MIIGpzCCBY+gAwIBAgIKGdhyPgABAAABpDANBgkqhkiG9w0BAQUFADBsMRMwEQYK
CZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFY2lzY28xIjAgBgoJkiaJ
k/IsZAEZFhJqeW91bmd0YS1sYWJkb21haW4xGjAYBgNVBAMTEWp5b3VuZ3RhLWNh
c2VydmVyMB4XDTEyMDgyOTEzMzIyOVoXDTE0MDgyOTEzMzIyOVowGDEWMBQGA1UE
AxMNam9jYXNhbGUtc2FzdDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
ALLIyM0k5DmgWy1jILHy+eaoJTU+OioaTfFOV7SdNOfjoXCRpqCZwFavR82/Wuko
ho9HUXB7/oEQV6D2UoyHRhl1mzHv5AxuJuE10Qk9YHpBzLAcNEvRWvnyVnMaBSc6
Fy9j7oabAUuOoWveK8NrsoR38WH2gIY3kUaM8swgaomqlAj8LbmYE/PQdtfxOEne
IF1FHHXj4ffffffffffffffffffffffffffffffffffffffffffffffffffffffff
ffffffffffffffffffffffWa2S3O/
p6vXEwKfQMGZe4nO7SJPtJ/vNHx/HNCkJxHVH1V0JH7AwWLdnUgEWGoSFOL5j/lw
IHmemUDpSuL9IY+9EP622E0CAwEAAaOCA50wggOZMA4GA1UdDwEB/wQEAwIFoDAd
BgNVHQ4EFgQUtP6NbC/kpe3uSa2oeZy9rTDGMHAwHwYDVR0jBBgwFoAUsuXXNeJW
LhdYasmJ260ABz7CElswggGYBgNVHR8EggGPMIIBizCCAYegggGDoIIBf4aB2Wxk
YXA6Ly8vQ049anlvdW5ndGEtY2FzZXJ2ZXIoMSksQ049anlvdW5ndGEtY2FzZXJ2
ZXIsQ049Q0RQLENOPVB1YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2Vz
LENOPUNvbmZpZ3VyYXRpb24sREM9anlvdW5ndGEtbGFiZG9tYWluLERDPWNpc2Nv
LERDPWNvbT9jZXJ0aWZpY2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Q2xh
c3M9Y1JMRGlzdHJpYnV0aW9uUG9pbnSGWWh0dHA6Ly9qeW91bmd0YS1jYXNlcnZl
ci5qeW91bmd0YS1sYWJkb21haW4uY2lzY28uY29tL0NlcnRFbnJvbGwvanlvdW5n
dGEtY2FzZXJ2ZXIoMSkuY3JshkZodHRwOi8vanlvdW5ndGEtY2FzZXJ2ZXIuY2lz
Y28uY29tL0NlcnRFbnJvbGwvanlvdW5ndGEtY2FzZXJ2ZXIoMSkuY3JsMIIBcQYI
KwYBBQUHAQEEggFjMIIBXzCBxAYIKwYBBQUHMAKGgbdsZGFwOi8vL0NOPWp5b3Vu
Z3RhLWNhc2VydmVyLENOPUFJQSxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxD
Tj1TZXJ2aWfffffffffffffffffffffffffffffffffffffffffffffffffffffffff
ffffffffffffffffffffffLWxhYmRvbWFp
bixEQz1jaXNjbyxEQz1jb20/Y0FDZXJ0aWZpY2F0ZT9iYXNlP29iamVjdENsYXNz
PWNlcnRpZmljYXRpb25BdXRob3JpdHkwgZUGCCsGAQUFBzAChoGIaHR0cDovL2p5
b3VuZ3RhLWNhc2VydmVyLmp5b3VuZ3RhLWxhYmRvbWFpbi5jaXNjby5jb20vQ2Vy
dEVucm9sbC9qeW91bmd0YS1jYXNlcnZlci5qeW91bmd0YS1sYWJkb21haW4uY2lz
Y28uY29tX2p5b3VuZ3RhLWNhc2VydmVyKDEpLmNydDAhBgkrBgEEAYI3FAIEFB4S
AFcAZQBiAFMAZQByAHYAZQByMBMGA1UdJQQMMAoGCCsGAQUFBwMBMA0GCSqGSIb3
DQEBBQUAA4IBAQCayeYa7pauRGAgGPHmAHQt6iiqBsS+uVwArgO1u0HEjs4EkPm8
xQZNexVBOmGyzTwlwjpD8jTDIO1AEWP67b/gB2xViktVqvaVfKfMR+3cxODoTUNJ
DbMKR7tOyLrfv+7hNVcsKlAo+XpohVKdP4XOPXeEquYrTmzInsB55PtMxJ7qnYU6
29kJUZdVQZUjZSy4dVhtVYVO9Gmj5XIkzUneS4QC7N/3CXGZQilH11PzulUvAAFh
h2o6c7QgKtHGxOwrkXuPl6+GN4mV+uFXh1B5DTEXG7/yJNNE2yNN+Flb05yLcyEA
Y0p/cksKkNhpRDh+YNT1uHa0AjY8fa1AJqpp
-----END CERTIFICATE-----
quit
% Router Certificate successfully imported
```

例 2：

```
crypto pki auth tac-cme
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
-----BEGIN CERTIFICATE-----
MIIFQTCCBCmgAwIBAgIQUt2XjpaAwaJIEkcOebj7AjANBgkqhkiG9w0BAQUFADBs
MRMwEQYKCZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFY2lzY28xIjAg
BgoJkiaJk/IsZAEZFhJqeW91bmd0YS1sYWJkb21haW4xGjAYBgNVBAMTEWp5b3Vu
Z3RhLWNhc2VydmVyMB4XDTEyMDgxMzE1NTczM1oXDTE3MDgxNDE2MDY0M1owbDET
MBEGCgmSJomT8ixkARkWA2NvbTEVMBMGCgmSJomT8ixkARkWBWNpc2NvMSIwIAYK
CZImiZPyLGQBGRYSanlvdW5ndGEtbGFiZG9tYWluMRowGAYDVQQDExFqeW91bmd0
YS1jYXNlcnZlcjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJ2Cxwm6
uX3/t3Ip9A5OnbKS1IL4MaTCVzev7tlZbusWLQcfJwOhjFNxJJpgY2yE8CjBsL4H
eryNvcvUFfffffffffffffffffffffffffffffffffffffffffffffffffffffffff
fffffffffffffffffffffffU839yp
lNm9VtF+MXC0L7dIpu1XRT7/lJgLDAI5alZg5wW6zC9xrgNS88cR1o45wsFTRpp8
DC7nGuW0erm2/ISnfoNs/mUmfWbmoAbJjIrU+RHaQ7RrcXPWB3mEqC40eQtYJFZl
tRE7DNwPriVBTpWCV+wo94DkHtn8/nc3FOWD0RIjU7Y66jG+umWSeqJh0xdZBak2
+L9A6ZwCxyeuzg0CAwEAAaOCAd0wggHZMBMGCSsGAQQBgjcUAgQGHgQAQwBBMAsG
A1UdDwQEAwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBSy5dc14lYuF1hq
yYnbrQAHPsISWzCCAUoGA1UdHwSCAUEwggE9MIIBOaCCATWgggExhoHWbGRhcDov
Ly9DTj1qeW91bmd0YS1jYXNlcnZlcixDTj1qeW91bmd0YS1jYXNlcnZlcixDTj1D
RFAsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZXMsQ049Q29u
ZmlndXJhdGlvbixEQz1qeW91bmd0YS1sYWJkb21haW4sREM9Y2lzY28sREM9Y29t
P2NlcnRpZmffffffffffffffffffffffffffffffffffffffffffffffffffffffff
fffffffffffffffffffffffffffjUkxE
aXN0cmlidXRpb25Qb2ludIZWaHR0cDovL2p5b3VuZ3RhLWNhc2VydmVyLmp5b3Vu
Z3RhLWxhYmRvbWFpbi5jaXNjby5jb20vQ2VydEVucm9sbC9qeW91bmd0YS1jYXNl
cnZlci5jcmwwEgYJKwYBBAGCNxUBBAUCAwEAATAjBgkrBgEEAYI3FQIEFgQUWjZQ
/W2X5GoSeibbuvAKHH8/97MwDQYJKoZIhvcNAQEFBQADggEBAI8nivQcicltdXnt
X30+QO+FKK0Cu6WWFIozqKE0eeSJ0C3fPv88jjkae4+YjF/gK2wPt/mezWeQm0MO
S4m0LHnMMZGU7ezAHTd+yh5oWI2Q2iBFnslvSIUboJZazNkDEFm7Dl8gDKajEvE/
JUNtebgOJPJUXvV/v0Rpry1Nckxrn3tsiCF62acgAZke1hSrscoeqzkygk8vIr1K
lv9W2Vy2TPa6i8ZWG8at36jAsNAk5HJUEl7mFyirMIJcc+diZ12WPoRqrQ+CE7ZL
Mw+ydSS5x0XvFqily0VE649TsvtKCOMkJjbLLX8wZp9SU2AgXutHr3CdlrVlaElC
ZW4J3cQ=
-----END CERTIFICATE-----
quit
Certificate has the following attributes:
Fingerprint MD5: C198A185 83575520 EBE6E03D 33BA9B2C
Fingerprint SHA1: B0A9668D 42D36311 E82B0A33 480127B5 BEB02B60
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

crypto pki import tac-cme cert
% The fully-qualified domain name will not be included in the certificate
Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself
-----BEGIN CERTIFICATE-----
MIIGpjCCBY6gAwIBAgIKGdmLjgABAAABpTANBgkqhkiG9w0BAQUFADBsMRMwEQYK
CZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFY2lzY28xIjAgBgoJkiaJ
k/IsZAEZFhJqeW91bmd0YS1sYWJkb21haW4xGjAYBgNVBAMTEWp5b3VuZ3RhLWNh
c2VydmVyMB4XDTEyMDgyOTEzMzM0MVoXDTE0MDgyOTEzMzM0MVowFzEVMBMGA1UE
AxMMam9jYXNhbGUtY21lMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
uVz/50eRaTmlnvOKRFp9ZcZuqw3We6DVqsBMuTpQg0Bg/VQTgCa9NFD8LW2UXGO8
YFANV8ABVn9q/1TET6Fg5YbcTePsd5/lNlL1zpSHiAtBuwfGzKKiMgZJ1XFYeb9p
heqpTj2d22CoghFQnKbRUOPpjfPcElFq07/z5m7blEkAmsAQh2y+bIH5T7UNdgtf
smLqWZMqIsMEvNEi3gbkPUTatmZlgFac1TXvxyIIv95rIeqs07WZXn0GsgkNsO3i
CjcFY1UXxxYV5Wg/uPQlFnbRpTefd5Ms253Dm9Ey2E8v+E3HsOfn0JvpY4vIkKz2
KDesetXsIOw747tf1wXHmQIDAQABo4IDnTCCA5kwDgYDVR0PAQH/BAQDAgWgMB0G
A1UdDgQWBBR8xG8ZaDVcquSU+0n40KSH+7SmSDAfBgNVHSMEGDAWgBSy5dc14lYu
```

```
F1hqyYnbrQAHPsISWzCCAZgGA1UdHwSCAY8wggGLMIIBh6CCAYOgggF/hoHZbGRh
cDovLy9DTj1qeW91bmd0YS1jYXNlcnZlcigxKSxDTj1qeW91bmd0YS1jYXNlcnZl
cixDTj1DRFAsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZXMs
Q049Q29uZmlndXJhdGlvbixEQz1qeW91bmd0YS1sYWJkb21haW4sREM9Y2lzY28s
REM9Y29tP2NlcnRpZmljYXRlUmV2b2NhdGlvbkxpc3Q/YmFzZT9vYmplY3RDbGFz
cz1jUkfffffffffffffffffffffffffffffffffffffffffffffffffcDovL2
p5b3VuZ3RhLWNhc2VydmVy
Lmp5b3VuZ3RhLWxhYmRvbWFpbi5jaXNjby5jb20vQ2VydEVucm9sbC9qeW91bmd0
YS1jYXNlcnZlcigxKS5jcmyGRmh0dHA6Ly9qeW91bmd0YS1jYXNlcnZlci5jaXNj
by5jb20vQ2VydEVucm9sbC9qeW91bmd0YS1jYXNlcnZlcigxKS5jcmwwggFxBggr
BgEFBQcBAQSCAWMwggFfMIHEBggrBgEFBQcwAoaBt2xkYXA6Ly8vQ049anlvdW5n
dGEtY2FzZXJ2ZXIsQ049QUlBLENOPVB1YmxpYyUyMEtleSUyMFNlcnZpY2VzLENO
PVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRpb24sREM9anlvdW5ndGEtbGFiZG9tYWlu
LERDPWNpc2NvLERDPWNvbT9jQUNlcnRpZmljYXRlP2Jhc2U/b2JqZWN0Q2xhc3M9
Y2VydGlmaWNhdGlvbkF1dGhvcml0eTCBlQYIKwYBBQUHMAKGgYhodHRwOi8vanlv
dW5ndGEtY2FzZXJ2ZXIuanlvdW5ndGEtbGFiZG9tYWluLmNpc2NvLmNvbS9DZXJ0
RW5yb2xsL2p5b3VuZ3RhLWNhcffffffffffffffffffffffffffffffffffffffff
ffffffffffffffffFpbi5jaXNj
by5jb21fanlvdW5ndGEtY2FzZXJ2ZXIoMSkuY3J0MCEGCSsGAQQBgjcUAgQUHhIA
VwBlAGIAUwBlAHIAdgBlAHIwEwYDVR0lBAwwCgYIKwYBBQUHAwEwDQYJKoZIhvcN
AQEFBQADggEBAHNVNEMcys1z4sXGiI2jZzT5Nt/q8dLl4LCJ2iZkmS3F8tG14UEf
C/e28VWavV4piIXK4FuZKB1iltOo9MZAGH9PvVEO+yG8zpeIcwOgDq951qJejeBA
+N+ryCFy5TEbiMF3pw1XjdbBAProJ1s1Q0QcjoigPNtPyqRfehdlhMUo4NgC/svX
5VZSfxpagaBhdpUNVYo2s0ujXujuI/aTRpbDan2h7n27tMMBtDcocpQgPv6txDoR
b+Qb8CPZt3IvuEXAru4cRv1O1jYUWlY59ta5uELSnA+2WA36PiMxIyLu67W1RI05
1rFcBOmIQ8vTpqyNp8/TFOpOSnQMO30w9Fs=
-----END CERTIFICATE-----
quit
% Router Certificate successfully imported
```

6. CA 証明書と ID 証明書の両方がそれぞれ該当するトラストポイントにロードされたら、各トラストポイントの証明書チェーンを検証します。 この手順により、これより前の手順が正常に完了していることを確認できます。

```
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
```

7. IOS CA CME トラストポイントを作成します。

   IOS-CA トラストポイントはクライアント認証（電話機との Transport Level Security（TLS）接続）には使用できないため、別のトラストポイントを作成し、そのトラストポイントに IOS-CA 証明書を配置する必要があります。

   このトラストポイントは、IP フォンによる TLS 接続要求の許可だけに使用されます（これにより、正しく登録されます）。

```
crypto pki trust ios-ca-cme
enroll url http://10.2.3.4:80
revo none
rsakey 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.
```

8. CTL クライアントを設定します。

```
ctl-client
server capf 10.2.3.4 trust tac-cme
server cme-tftp 10.2.3.4 trust tac-cme
sast1 trust tac1-cme
sast2 trust tac-sast
regenerate
```

注: CTL ファイルが正常に作成されたことを確認します。

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

9. CAPF サーバを設定します。

```
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. テレフォニー サービスを設定します。

```
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. 証明書をアップグレードし、暗号化モードを使用するように、テスト電話機（ephone）を設定します。

```
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
```

設定が完了したら電話機をリセットし、登録されるまで待ちます。

注: 電話機をリセットする前に、セキュリティの設定がすでに存在していないことを確認してください。 セキュリティの設定が存在している場合は、Secure Cisco Unified CME への登録前に、そのセキュリティ設定を手動で削除するか、電話機を工場出荷時状態にリセットする必要があります。

電話機をリセットするには、次のコマンドを実行します。

```
confi t
```

```
ephone 1
reset
end
```

電話機が更新された LSC を受信すると、**cert-oper upgrade auth-mode null-string** コマンドは削除されます。

```
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. 電話機が認証と暗号化の両方に登録されていることを確認します。

```
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
```

Secure Cisco Unified CME がサードパーティの証明書を使用して完全に機能する必要があります。

関連情報

- Cisco Unified Communications Manager Express システム アドミニストレータ ガイド
- セキュアな音声（Cisco TAC Wiki）
- テクニカル サポートとドキュメント – Cisco Systems