Asegure el CME unificado Cisco con el ejemplo de configuración de los Certificados de las de otras compañías

Contenido

Introducción

Muchos administradores de la red eligen implementar el Cisco Unified Communications Manager Express (CME) con la Seguridad. En vez del Certificate Authority IOS del accesorio (IOS-CA), los administradores de la red pueden elegir integrar el CME seguro con su infraestructura existente del Public Key Infrastructure (PKI). Este documento describe cómo configurar el CME seguro para actuar con asegura la señalización, y los media, vía los Certificados de las de otras compañías.

Prerequisites

Requisitos

Este documento asume que el Cisco Unified Communications Manager Express (CME) en su entorno se está ejecutando y completamente - funcional. Todos los teléfonos que deben ser operativos en Cisco seguro unificaron la necesidad CME de poder primero registrarse con éxito al CME. Refiera a la guía de administrador de sistema del Cisco Unified Communications Manager Express para la información sobre cómo configurar el CME.

Este documento también asume que la Voz y las funciones de seguridad están habilitadas.

Componentes Utilizados

La información en este documento se basa en el Cisco Unified Communications Manager Express

(CME).

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener información sobre las convenciones sobre documentos.

Configurar

Note: Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Pasos para la configuración sumarios

1. Cree el caso IOS-CA.
2. Cree el trustpoints para sostener los Certificados de CA de las de otras compañías.
3. Genere los pedidos de firma de certificado (CSR) del trustpoints.
4. Firme los CSR con el uso de la autenticación de servidor, y obtenga la certificación de CA.
5. Autentique el trustpoints con el certificado de CA, e importe los certificados de identidad respectivos.
6. Valide el trustpoints del certificado de las de otras compañías.
7. Cree el trustpoint IOS CA CME.
8. Configure Certificate Trust List (Lista de confianza del certificado) al cliente (CTL).
9. Configure el servidor de la función de proxy del Certificate Authority (CAPF).
10. Configure el servicio de telefonía.
11. Configure el teléfono de prueba.
12. Verifique.

Ejemplo de la configuración detallada

1. Cree el caso IOS-CA. El caso IOS-CA presenta el certificado autofirmado que se utiliza para firmar el teléfono localmente - el certificado significativo (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
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. Cree el trustpoints que generará los CSR para la firma de las de otras compañías. Este trustpoints sostiene eventual el certificado de CA de las de otras compañías, así como los certificados de identidad, que son un resultado de los CSR.

```
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. Genere los CSR del trustpoints. El pki crypto alista el comando produce el CSR que se proporciona a las de otras compañías CA para firmar.

Ejemplo 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
H1V0JH7Affffffffffffffffffffffffffffffffffffffffffffffffffffffff
ffffffffffffffffffffffffffffffffEAAaAhMB8G
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
```

Ejemplo 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
ffffffffffffffffffffffffffffffHNCkJxHV
H1V0JH7AwWLdnUgEWGoSFOL5j/lwIHmemUDpSuL9IY+9EP622E0CAwEAAaAhMB8G
CSqGSIb3DQEJDjESMBAwDgYDVR0PAQH/BAQDAgWgMA0GCSqGSIb3DQEBBAUAA4IB
AQB++utK7EpeGYYyPfNALsXkPcbu+2kwi/TI+B2kT3ol/dxyX6hNh0jp3eOTQtSl
H7jRey4ew9GZVTeqq7cxwz1f7d6ZP4BRqzp1f0HVvu7HC+bAR0jB2FNvVaN27zYu
XSP/GIaUiQDTbaEyDgGr8s5P1FSS2Ap4FvxsskjD/30geszhRs+N3cYfQVpnWjnq
TwbMF4998BXmlPIQigJBInACY2SUszqcDih7Nc1Y6viYaSiN0ZCuzEyKI2tjbwUU
EU/o0fcWMXsnBc44WQBAEpTBSLYFVb4kGl9AgAyOW7q9ACiBTpmul1kwuDyTPg5X
fCIWUjVfTWoHizqxKSbLQ2nL
---End - This line not part of the certificate request---
Redisplay enrollment request? [yes/no]: no
```

4. Utilice los dos CSR para generar los Certificados con los permisos de la autenticación de servidor.

   Notas: Es esencial que la Cadena de certificados llena está obtenida para uno de los dos Certificados de CA. La Cadena de certificados proporciona CA y el certificado de identidad de CA de firma.Asegúrese de que los Certificados estén descargados en el formato del base 64.Es muy importante que el certificado de CA está utilizado para la autenticación para cada trustpoint y que los certificados de identidad están importados en cada trustpoint, en esa orden.
5. Autentique el trustpoints con los Certificados de CA, e importe los certificados de identidad SAST.

   Ejemplo 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
CZImiZPyLGQBGRYSanlvdW5ndGEtbGFiZG9tYW1uMRowGAYDVQQDExFqeW91bmd0
YS1jYXNlcnZlcjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJ2Cxwm6
uX3/t3Ip9A5OnbKS1IL4MaTCVzev7tlZbusWLQcfJwOhjFNxJJpgY2yE8CjBsL4H
eryNvcvUFeA90kXbEncl1uoI7t1JEf5ifQBopqGO54E0t1YUHrcT5LgXdBU839yp
lNm9VtFfffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
ffffffffffffffffffffffo45wsFTRpp8
DC7nGuW0erm2/ISnfoNs/mUmfWbmoAbJjIrU+RHaQ7RrcXPWB3mEqC40eQtYJFZl
tRE7DNwPriVBTpWCV+wo94DkHtn8/nc3FOWD0RIjU7Y66jG+umWSeqJh0xdZBak2
+L9A6ZwCxyeuzg0CAwEAAaOCAd0wggHZMBMGCSsGAQQBgjcUAgQGHgQAQwBBMAsG
```

```
A1UdDwQEAwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBSy5dc141YuF1hq
yYnbrQAHPsISWzCCAUoGA1UdHwSCAUEwggE9MIIBOaCCATWgggExhoHWbGRhcDov
Ly9DTj1qeW91bmd0YS1jYXNlcnZlcixDTj1qeW91bmd0YS1jYXNlcnZlcixDTj1D
RFAsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049U2Vydmljc2XMsQ049Q29u
ZmlndXJhdGlvbixEQz1qeW91bmd0YS1sYWJkb21haW4sREM9Y2lzY28sREM9Y29t
P2NlcnRpZmljYXRlUmV2b2NhdGlvbkxpc3Q/YmFzZT9vYmplY3RDbGFzcz1jUkxE
aXN0cmliffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
ffffffffffffffffffffffffffffffyLmp5b3Vu
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
IF1FHHXj4fffffffffffffffffffffffffffffffffffffffffffffffffffffffff
ffffffffffffffffffffffffWa2S3O/
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
h2o6c7QgKtHGxOwrkXuP16+GN4mV+uFXh1B5DTEXG7/yJNNE2yNN+Flb05yLcyEA
Y0p/cksKkNhpRDh+YNT1uHa0AjY8fa1AJqpp
-----END CERTIFICATE-----
quit
% Router Certificate successfully imported
```

Ejemplo 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
CZImiZPyLGQBGRYSanlvdW5ndGEtbGFiZG9tYW1uMRowGAYDVQQDExFqeW91bmd0
YS1jYXNlcnZlcjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJ2Cxwm6
uX3/t3Ip9A5OnbKS1IL4MaTCVzev7tlZbusWLQcfJwOhjFNkJJpgY2yE8CjBsL4H
eryNvcvUFfffffffffffffffffffffffffffffffffffffffffffffffffffffffff
ffffffffffffffffffffffffU839yp
lNm9VtF+MXC0L7dIpu1XRT7/lJgLDAI5alZg5wW6zC9xrgNS88cR1o45wsFTRpp8
DC7nGuW0erm2/ISnfoNs/mUmfWbmoAbJjIrU+RHaQ7RrcXPWB3mEqC40eQtYJFZl
tRE7DNwPriVBTpWCV+wo94DkHtn8/nc3FOWD0RIjU7Y66jG+umWSeqJh0xdZBak2
+L9A6ZwCxyeuzg0CAwEAAaOCAd0wggHZMBMGCSsGAQQBgjcUAgQGHgQAQwBBMAsG
A1UdDwQEAwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBSy5dc141YuF1hq
yYnbrQAHPsISWzCCAUoGA1UdHwSCAUEwggE9MIIBOaCCATWgggExhoHWbGRhcDov
Ly9DTj1qeW91bmd0YS1jYXNlcnZlcixDTj1qeW91bmd0YS1jYXNlcnZlcixDTj1D
RFAsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZXMsQ049Q29u
ZmlndXJhdGlvbixEQz1qeW91bmd0YS1sYWJkb21haW4sREM9Y2lzY28sREM9Y29t
P2NlcnRpZmffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
ffffffffffffffffffffffffffffffjUkxE
aXN0cmlidXRpb25Qb2ludDIZWaHR0cDovL2p5b3VuZ3RhLWNhc2VydmVyLmp5b3Vu
Z3RhLWxhYmRvbWFpbi5jaXNjby5jb20vQ2VydEVucm9sbC9qeW91bmd0YS1jYXN1
cnZlci5jcmwwEgYJKwYBBAGCNxUBBAUCAwEAATAjBgkrBgEEAYI3FQIEFgQUWjZQ
/W2X5GoSeibbuvAKHH8/97MwDQYJKoZIhvcNAQEFBQADggEBAI8nivQcicltdXnt
X30+QO+FKK0Cu6WWFIozqKE0eeSJ0C3fPv88jjkae4+YjF/gK2wPt/mezWeQm0MO
S4m0LHnMMZGU7ezAHTd+yh5oWI2Q2iBFnslvSIUboJZazNkDEFm7Dl8gDKajEvE/
JUNtebgOJPJUXvV/v0Rpry1Nckxrn3tsiCF62acgAZke1hSrscoeqzkygk8vIr1K
lv9W2Vy2TPa6i8ZWG8at36jAsNAk5HJUEl7mFyirMIJcc+diZ12WPoRqrQ+CE7ZL
Mw+ydSS5x0XvFqily0VE649TsvtKCOMkJjbLLX8wZp9SU2AgXutHr3CdlrVlaE1C
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
AxMMam9jYXNhbGUtY211MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
uVz/50eRaTmlnvOKRFp9ZcZuqw3We6DVqsBMuTpQg0Bg/VQTgCa9NFD8LW2UXGO8
YFANV8ABVn9q/1TET6Fg5YbcTePsd5/lNlL1zpSHiAtBuwfGzKKiMgZJ1XFYeb9p
heqpTj2d22CoghFQnKbRUOPpjfPcE1Fq07/z5m7blEkAmsAQh2y+bIH5T7UNdgtf
smLqWZMqIsMEvNEi3gbkPUTatmZlgFac1TXvxyIIv95rIeqs07WZXn0GsgkNsO3i
CjcFY1UXxxYV5Wg/uPQlFnbRpTefd5Ms253Dm9Ey2E8v+E3HsOfn0JvpY4vIkKz2
KDesetXsIOw747tf1wXHmQIDAQABo4IDnTCCA5kwDgYDVR0PAQH/BAQDAgWgMB0G
A1UdDgQWBBR8xG8ZaDVcquSU+0n40KSH+7SmSDAfBgNVHSMEGDAWgBSy5dc141Yu
F1hqyYnbrQAHPsISWzCCAZgGA1UdHwSCAY8wggGLMIIBh6CCAYOgggF/hoHZbGRh
cDovLy9DTj1qeW91bmd0YS1jYXNlcnZlcigxKSxDTj1qeW91bmd0YS1jYXNlcnZl
cixDTj1DRFAsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZXMs
Q049Q29uZmlndXJhdGlvbixEQz1qeW91bmd0YS1sYWJkb21haW4sREM9Y2lzY28s
REM9Y29tP2NlcnRpZmljYXRlUmV2b2NhdGlvbkxpc3Q/YmFzZT9vYmplY3RDbGFz
cz1jUkffffffffffffffffffffffffffffffffffffffffffffffffffffcDovL2
p5b3VuZ3RhLWNhc2VydmVy
Lmp5b3VuZ3RhLWxhYmRvbWFpbi5jaXNjby5jb20vQ2VydEVucm9sbC9qeW91bmd0
YS1jYXNlcnZlcigxKS5jcmyGRmh0dHA6Ly9qeW91bmd0YS1jYXNlcnZlci5jaXNj
by5jb20vQ2VydEVucm9sbC9qeW91bmd0YS1jYXNlcnZlcigxKS5jcmwwggFxBggr
BgEFBQcBAQSCAWMwggFfMIHEBggrBgEFBQcwAoaBt2xkYXA6Ly8vQ049anlvdW5n
dGEtY2FzZXJ2ZXIsQ049QUlBLENOPVB1YmxpYyUyMEtleSUyMFNlcnZpY2VzLENO
PVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRpb24sREM9anlvdW5ndGEtbGFiZG9tYW1u
LERDPWNpc2NvLERDPWNvbT9jQUNlcnRpZmljYXRlP2Jhc2U/b2JqZWN0Q2xhc3M9
Y2VydGlmaWNhdGlvbkF1dGhvcml0eTCBlQYIKwYBBQUHMAKGgYhodHRwOi8vanlv
dW5ndGEtY2FzZXJ2ZXIuanlvdW5ndGEtbGFiZG9tYW1uLmNpc2NvLmNvbS9DZXJ0
RW5yb2xsL2p5b3VuZ3RhLWNhcffffffffffffffffffffffffffffffffffffffffff
ffffffffffffffffffFpbi5jaXNj
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. Una vez que CA y los certificados de identidad se cargan en el trustpoints respectivo, valide la Cadena de certificados para cada trustpoint. Este paso se asegura de que los pasos anteriores fueran completados con éxito.

```
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. Cree el trustpoint IOS CA CME.

   Porque el trustpoint IOS-CA no se puede utilizar para la autenticación de cliente (conexión llana de la Seguridad del transporte (TLS) con los teléfonos), usted debe crear otro trustpoint y poner el certificado IOS-CA en él.

   Este trustpoint se utiliza para autorizar solamente el pedido del teléfono del IP una conexión TLS (así que los puede registrarse correctamente).

```
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. Configure al cliente CTL.

```
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
```

Note: Asegúrese de que el archivo CTL fuera creado con éxito:

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

9. Configure el servidor del CAPF.

```
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. Configure el servicio de telefonía.

```
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. Configure el teléfono de prueba (ephone) para actualizar su certificado y utilizar el modo cifrado.

```
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
```

Una vez que la configuración es completa, reajuste el teléfono y espérelo para registrarse.

Note: Antes de que se reajuste el teléfono, asegúrese de que no haya presente de la Configuración de seguridad ya. Si una Configuración de seguridad está presente, debe ser quitada o completar manualmente una restauración de la fábrica del teléfono de prueba antes del registro para asegurar el CME unificado Cisco.

Para reajustar el teléfono, ejecute estos comandos:

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

Una vez que el teléfono ha recibido el LSC actualizado, se quita el comando de la **cadena nula de la actualización auténtico-MODE de la CERT-operación**.

```
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. Verifique que el teléfono se haya registrado con la autenticación y el cifrado.

```
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
```

Asegure el CME unificado Cisco debe ser completamente - funcional con los Certificados de las de otras compañías.

Información Relacionada

- Guía de Administrador de Sistema de Cisco Unified Communications Manager Express
- Asegure la Voz en el TAC de Cisco Wiki
- Soporte Técnico y Documentación - Cisco Systems