Renueve el certificado SCEP RA en el Servidor Windows AD 2012 usado para BYOD en el ISE

Contenido

Introducción

Este documento describe cómo renovar dos Certificados que se utilicen para el protocolo simple certificate enrollment (SCEP): Intercambie el certificado del agente de la inscripción y del cifrado CEP en el Microsoft Active Directory 2012.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento básico de la configuración del Microsoft Active Directory
- Conocimiento básico de la clave pública Infrastracture (PKI)
- Conocimiento básico del Identity Services Engine (ISE)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión 2.0 del Cisco Identity Services Engine
- R2 del Microsoft Active Directory 2012

Problema

Cisco ISE utiliza el protocolo SCEP para soportar el registro del dispositivo personal (BYOD onboarding). Al usar un externo SCEP CA, este CA es definido por un perfil SCEP RA en el ISE. Cuando se crea un perfil SCEP RA, dos Certificados se agregan automáticamente al almacén de los certificados confiables:

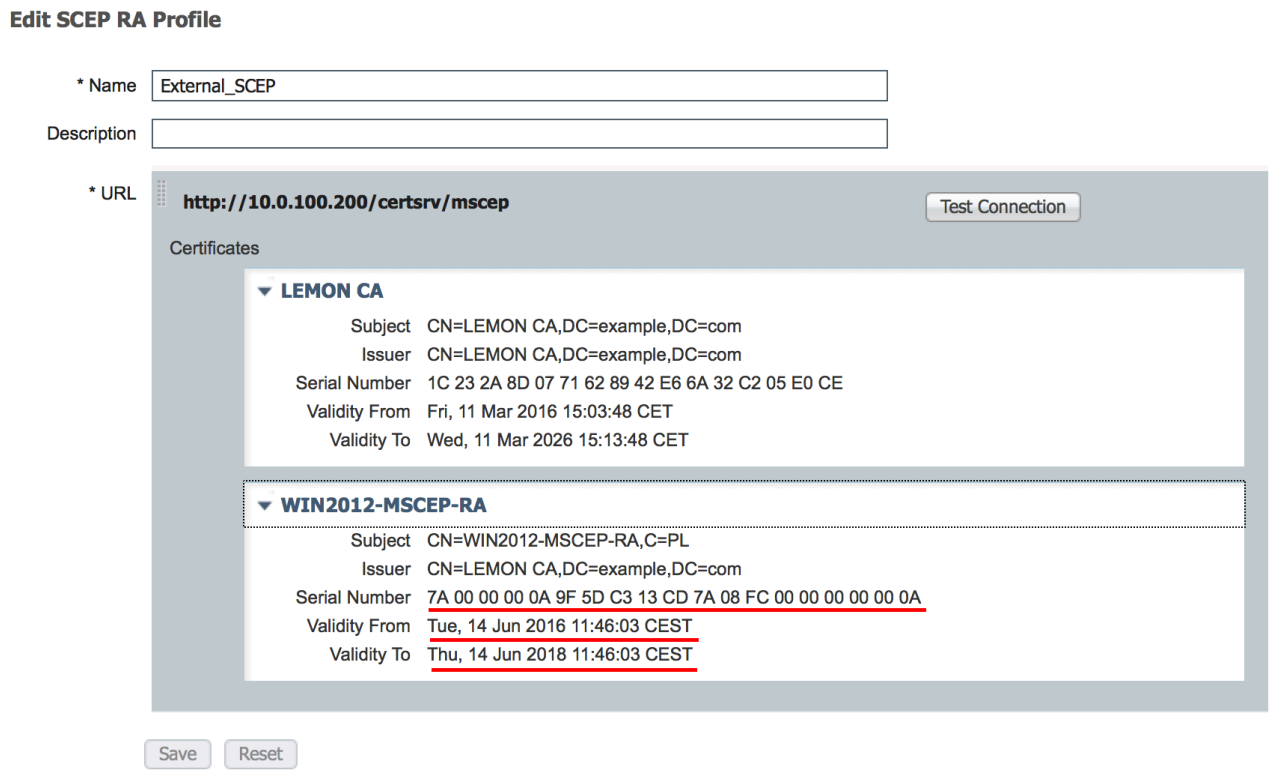
- Certificado raíz de CA,
- Certificado RA (autoridad de registro) que es firmado por CA.

El RA es responsable de recibir y de validar la petición del dispositivo de registro, y de remitirla a CA que publique el certificado del cliente.

Cuando expira el certificado RA, no se renueva automáticamente en el lado de CA (Servidor Windows 2012 en este ejemplo). Eso se debe hacer manualmente por el administartor activo Directory/CA.

Aquí está el ejemplo cómo alcanzar eso en el r2 del Servidor Windows 2012.

El SCEP inicial certifica visible en el ISE:



La suposición es que el CERTIFICADO MSCEP-RA está expirado y tiene que ser renovado.

Solución

Precaución: Cualquier cambio en el Servidor Windows se debe consultar con su

administrador primero.

1. Identifique las viejas claves privadas

Encuentre las claves del privite asociadas a los Certificados RA en el Active Directory usando la herramienta del **certutil**. Eso localiza después el **contenedor de claves.**

```
certutil -store MY %COMPUTERNAME%-MSCEP-RA
```

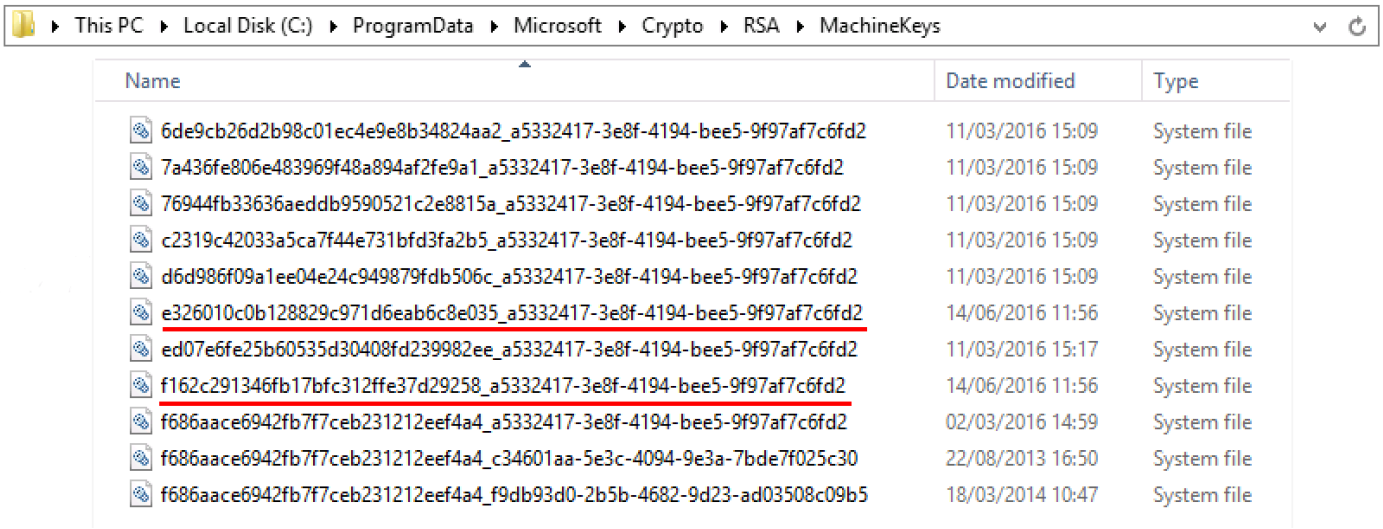
Observe por favor que si el nombre de su certificado inicial MSCEP-RA es diferente entonces debe ser ajustado en esta petición. Sin embargo, por abandono debe contener el nombre de computadora.

```
C:\Users\Administrator>certutil -store MY %COMPUTERNAME%-MSCEP-RA
MY "Personal"
================ Certificate 0 ================
Serial Number: 7a0000000940c8eb5d5aa4e373000000000009
Issuer: CN=LEMON CA, DC=example, DC=com
 NotBefore: 14/06/2016 11:46
 NotAfter: 14/06/2018 11:46
Subject: CN=WIN2012-MSCEP-RA, C=PL
Certificate Template Name (Certificate Type): EnrollmentAgentOffline
Non-root Certificate
Template: EnrollmentAgentOffline, Exchange Enrollment Agent (Offline request)
Cert Hash(sha1): f3 3a b8 a7 ae ba 8e b5 c4 eb ec 07 ec 89 eb 58 1c 5a 15 ca
  Key Container = f162c291346fb17bfc312ffe37d29258_a5332417-3e8f-4194-bee5-9f97a
f7c6fd2
  Simple container name: le-84278304-3925-4b49-a5b8-5a197ec84920
  Provider = Microsoft Strong Cryptographic Provider
Private key is NOT exportable
Signature test passed

================ Certificate 3 ================
Serial Number: 7a00000000a9f5dc313cd7a08fc000000000000a
Issuer: CN=LEMON CA, DC=example, DC=com
 NotBefore: 14/06/2016 11:46
 NotAfter: 14/06/2018 11:46
Subject: CN=WIN2012-MSCEP-RA, C=PL
Certificate Template Name (Certificate Type): CEPEncryption
Non-root Certificate
Template: CEPEncryption, CEP Encryption
Cert Hash(sha1): 0e e1 f9 11 33 93 c0 34 2b bd bd 70 f7 e1 b9 93 b6 0a 5c b2
  Key Container = e326010c0b128829c971d6eab6c8e035_a5332417-3e8f-4194-bee5-9f97a
f7c6fd2
  Simple container name: le-0955b42b-6442-40a8-97aa-9b4c0a99c367
  Provider = Microsoft Strong Cryptographic Provider
Private key is NOT exportable
Encryption test passed
CertUtil: -store command completed successfully.
```

2. Viejas claves privadas de la cancelación

Borre referir las claves manualmente de la carpeta abajo:

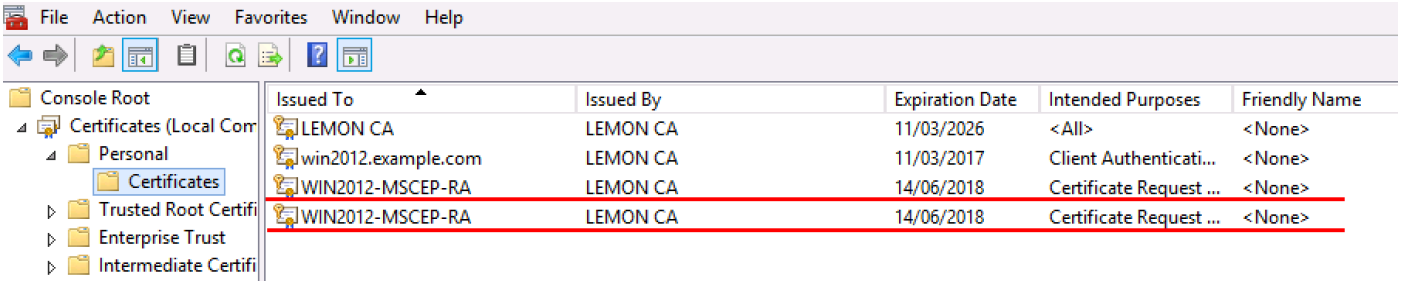
```
C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys
```



3. Borre los viejos ceritificates MSCEP-RA

Después de borrar las claves privadas, quite los ceritificates MSCEP-RA de la consola MMC.

El MMC > el archivo > Add/quitan Broche-en… > Add "Ceritificates" > cuenta > computadora local de la Computadora



4. Genere los nuevos Certificados para el SCEP

4.1. Genere el certificado de la inscripción del intercambio

4.1.1. Cree un archivo **cisco_ndes_sign.inf con el** contenido abajo. Esta información es utilizada más adelante por el certreq.exetool para generar el pedido de firma de certificado (CSR):

```
[NewRequest]
Subject = "CN=NEW-MSCEP-RA,OU=Cisco,O=Systems,L=Krakow,S=Malopolskie,C=PL"
Exportable = TRUE
KeyLength = 2048
KeySpec = 2
KeyUsage = 0x80
MachineKeySet = TRUE
ProviderName = "Microsoft Enhanced Cryptographic Provider v1.0
ProviderType = 1

[EnhancedKeyUsageExtension]
OID = 1.3.6.1.4.1.311.20.2.1

[RequestAttributes]
CertificateTemplate = EnrollmentAgentOffline
```

> Consejo: Si usted copia esta plantilla del archivo, aseegurese ajustarla según sus requisitos y marcar si todos los caracteres se copian correctamente (comillas incluyendo).

4.1.2. Cree el CSR basado en el archivo del .INF con este comando:

```
certreq -f -new cisco_ndes_sign.inf cisco_ndes_sign.req
```

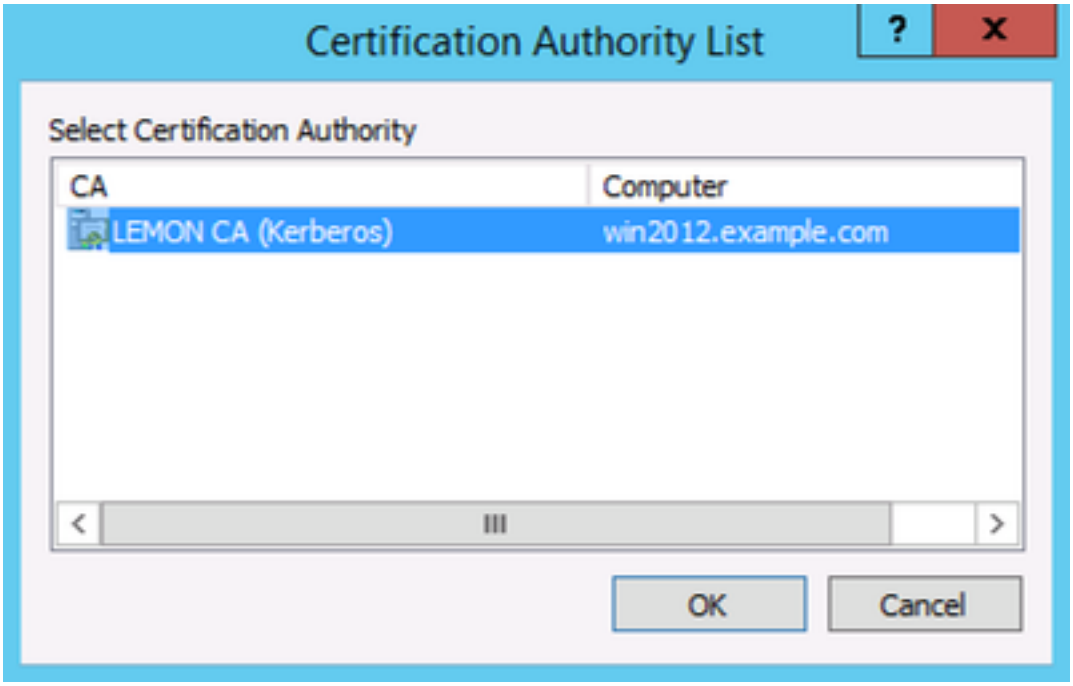
Si el **usuario** amonestador del diálogo que **plantilla del contexto está en conflicto con el contexto de la máquina** surge, hace clic la AUTORIZACIÓN. Esta advertencia puede ser ignorada.

```
C:\Users\Administrator\Desktop>certreq -f -new cisco_ndes_sign.inf cisco_ndes_si
gn.req
Active Directory Enrollment Policy
  {55845063-8765-4C03-84BB-E141A1DFD840}
  ldap:
User context template conflicts with machine context.

CertReq: Request Created

C:\Users\Administrator\Desktop>_
```

4.1.3. Someta el CSR con este comando:

```
certreq -submit cisco_ndes_sign.req cisco_ndes_sign.cer
```

Durante este procedimiento una ventana surge y CA apropiado tiene que ser elegido.




```
C:\Users\Administrator\Desktop>certreq -submit cisco_ndes_sign.req cisco_ndes_si
gn.cer
Active Directory Enrollment Policy
  {55845063-8765-4C03-84BB-E141A1DFD840}
  ldap:
RequestId: 11
RequestId: "11"
Certificate retrieved(Issued) Issued

C:\Users\Administrator\Desktop>_
```

4.1.4 Valide el certificado publicado en el paso anterior. Como resultado de este comando, el nuevo certificado se importa y se mueve al almacén personal de la computadora local:

```
certreq -accept cisco_ndes_sign.cer
```

```
C:\Users\Administrator\Desktop>certreq -accept cisco_ndes_sign.cer

C:\Users\Administrator\Desktop>_
```

4.2. Genere el certificado del cifrado CEP

4.2.1. Cree un nuevo archivo **cisco_ndes_xchg.inf:**

```
[NewRequest]
Subject = "CN=NEW-MSCEP-RA,OU=Cisco,O=Systems,L=Krakow,S=Malopolskie,C=PL"

Exportable = TRUE
KeyLength = 2048
KeySpec = 1
KeyUsage = 0x20
MachineKeySet = TRUE
ProviderName = “Microsoft RSA Schannel Cryptographic Provider”
ProviderType = 12

[EnhancedKeyUsageExtension]
OID = 1.3.6.1.4.1.311.20.2.1

[RequestAttributes]
CertificateTemplate = CEPEncryption
```

Siga los mismos pasos según lo descrito en 4.1.

4.2.2. Genere un CSR basado en el nuevo archivo del .INF:

```
certreq -f -new cisco_ndes_xchg.inf cisco_ndes_xchg.req
```

4.2.3. Someta la petición:

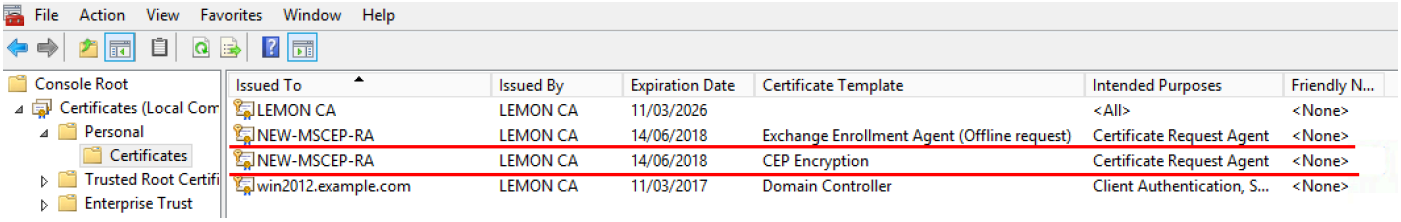
```
certreq -submit cisco_ndes_xchg.req cisco_ndes_xchg.cer
```

4.2.4: Valide el nuevo certificado trasladándose lo al almacén personal de la computadora local:

```
certreq -accept cisco_ndes_xchg.cer
```

5. Verificación

Después de completar el paso 4, dos nuevos Certificados MSCEP-RA aparecerán en el almacén personal de la computadora local:



También usted puede verificar los Certificados con la **herramienta certutil.exe** (aseegurese le utilizar el nuevo nombre correcto del certificado). Los Certificados MSCEP-RA con los nuevos nombres comunes y los nuevos números de serie deben ser visualizados:

```
certutil -store MY NEW-MSCEP-RA
```

```
C:\Users\Administrator\Desktop>certutil -store MY NEW-MSCEP-RA
MY "Personal"
================ Certificate 2 ================
Serial Number: 7a0000000cb250f5a9d6c1113500000000000c
Issuer: CN=LEMON CA, DC=example, DC=com
 NotBefore: 14/06/2016 13:40
 NotAfter: 14/06/2018 13:40
Subject: CN=NEW-MSCEP-RA, OU=Cisco, O=Systems, L=Krakow, S=Malopolskie, C=PL
Certificate Template Name (Certificate Type): CEPEncryption
Non-root Certificate
Template: CEPEncryption, CEP Encryption
Cert Hash(sha1): 31 4e 83 08 57 14 95 e9 0b b6 9a e0 4f c6 f2 cf 61 0b e8 99
  Key Container = 1ba225d16a794c70c6159e78b356342c_a5332417-3e8f-4194-bee5-9f97a
f7c6fd2
  Simple container name: CertReq-CEPEncryption-f42ec236-077a-40a9-b83a-47ad6cc8d
a0e
  Provider = Microsoft RSA SChannel Cryptographic Provider
Encryption test passed

================ Certificate 3 ================
Serial Number: 7a0000000b2813070a2b3616f000000000000b
Issuer: CN=LEMON CA, DC=example, DC=com
 NotBefore: 14/06/2016 13:35
 NotAfter: 14/06/2018 13:35
Subject: CN=NEW-MSCEP-RA, OU=Cisco, O=Systems, L=Krakow, S=Malopolskie, C=PL
Certificate Template Name (Certificate Type): EnrollmentAgentOffline
Non-root Certificate
Template: EnrollmentAgentOffline, Exchange Enrollment Agent (Offline request)
Cert Hash(sha1): 12 44 ba e6 4c 4e f8 78 7a a6 ae 60 9b b0 b2 ad e7 ba 62 9a
  Key Container = 320e64806bd159eca7b12283f3f67ee6_a5332417-3e8f-4194-bee5-9f97a
f7c6fd2
  Simple container name: CertReq-EnrollmentAgentOffline-0ec8b0c4-8828-4f09-927b-
c2f869589cab
  Provider = Microsoft Enhanced Cryptographic Provider v1.0
Signature test passed
CertUtil: -store command completed successfully.

C:\Users\Administrator\Desktop>_
```

6. Reiniciar IIS

Servidor de los Servicios de Internet Information Server del reinicio (IIS) para aplicar los cambios:

```
iisreset.exe
```

```
C:\Users\Administrator\Desktop>iisreset.exe

Attempting stop...
Internet services successfully stopped
Attempting start...
Internet services successfully restarted
```

7. Cree el nuevo perfil SCEP RA

En el ISE cree un nuevo perfil SCEP RA (con el mismo servidor URL que el viejo), así que los nuevos Certificados se descargan y se agregan a los certificados confiables el almacén:

External CA Settings

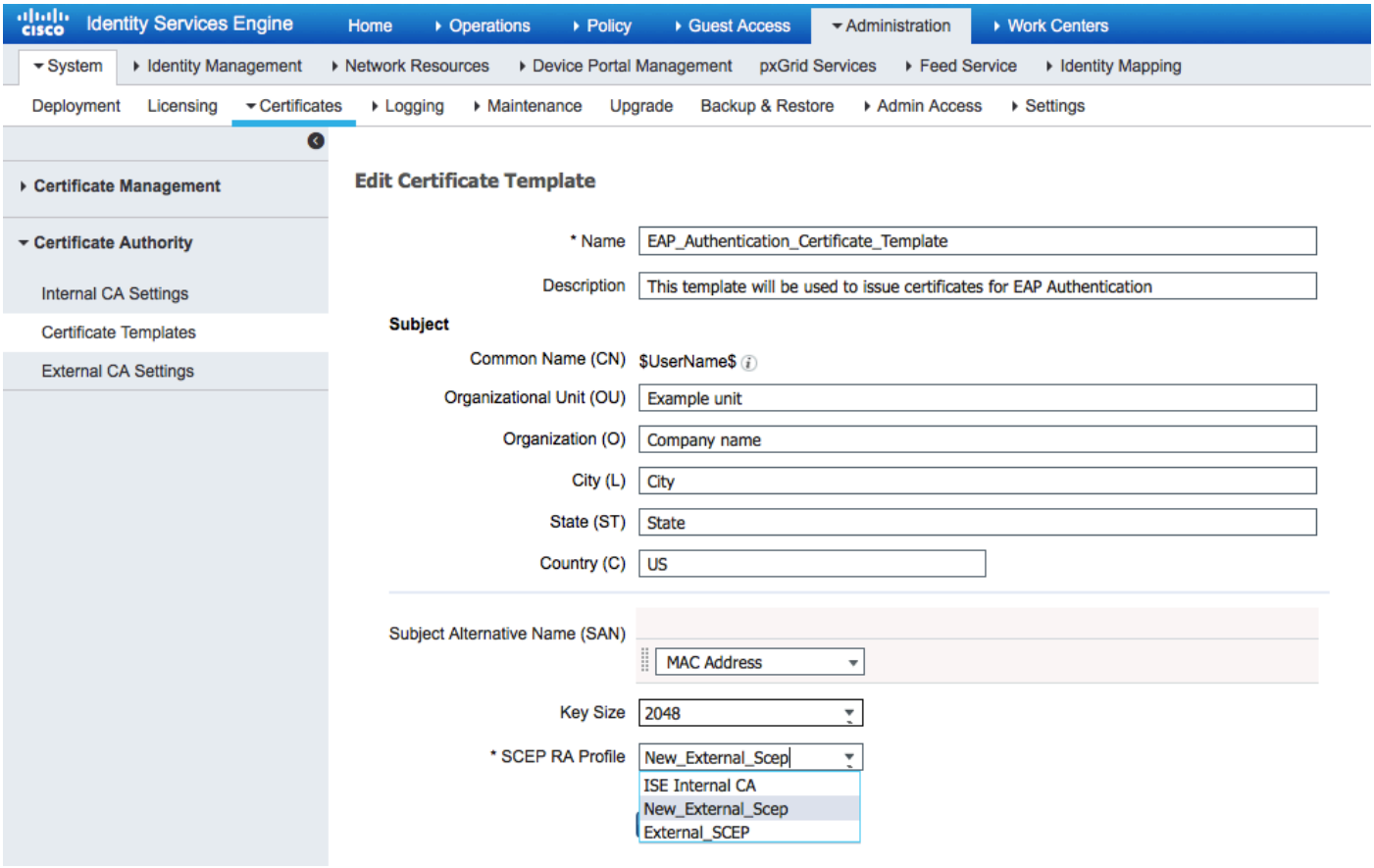
SCEP RA Profiles (SCEP-Simple Certificate Enrollment Protocol)

Edit | Add | Delete

Name	Description	URL	CA Cert Name
External_SCEP		http://10.0.100.200/certsrv/mscep	LEMON CA,WIN2012-MSCEP-RA
New_External_Scep		http://10.0.100.200/certsrv/mscep	LEMON CA,NEW-MSCEP-RA

8. Modifique el Certificate Template plantilla de certificado

Aseegurese el nuevo perfil SCEP RA se especifica en el Certificate Template plantilla de certificado usado por BYOD (usted puede marcarlo en la *administración > el sistema > los Certificados > el Certificate Authority > las plantillas de los Certificados*):



Referencias

1. Artículo de la zona de Microsoft Technet
2. Guías de configuración de Cisco ISE