Renove o certificado SCEP RA em Windows Server AD 2012 usado para BYOD no ISE

Índice

Introdução

Este documento descreve como renovar dois Certificados que são usados para o protocolo simple certificate enrollment (SCEP): Troque o certificado do agente do registro e da criptografia CEP no microsoft ative directory 2012.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico da configuração do microsoft ative directory
- Conhecimento básico da chave pública Infrastracture (PKI)
- Conhecimento básico do Identity Services Engine (ISE)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Versão 2.0 do Cisco Identity Services Engine

- Microsoft ative directory 2012 R2

Problema

Cisco ISE usa o protocolo scep para apoiar o registro pessoal do dispositivo (BYOD que onboarding). Ao usar um SCEP externo CA, este CA é definido por um perfil SCEP RA no ISE. Quando um perfil SCEP RA é criado, dois Certificados estão adicionados automaticamente à loja dos certificados confiáveis:

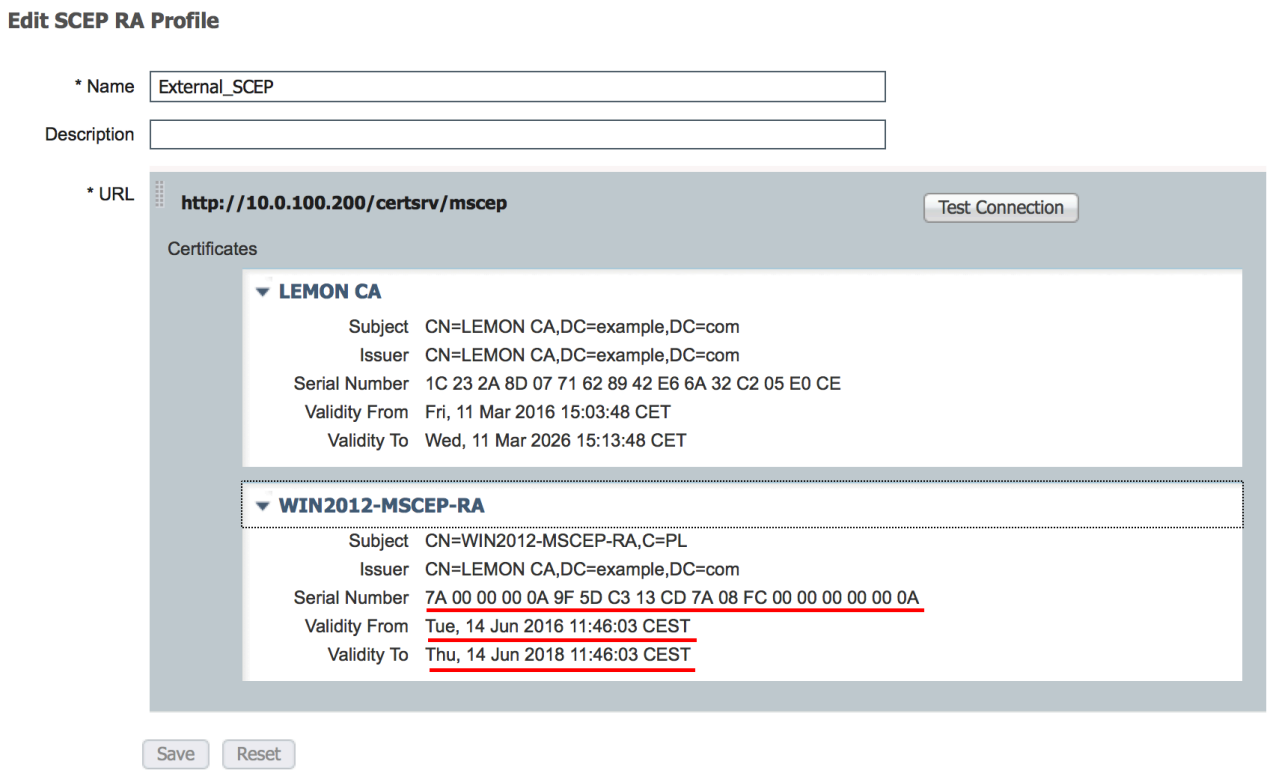
- Certificado de raiz de CA,
- Certificado RA (autoridade de registro) que é assinado por CA.

O RA é responsável para receber e validar o pedido do dispositivo registrando-se, e enviá-lo a CA que emite o certificado de cliente.

Quando o certificado RA expira, não está renovado automaticamente no lado de CA (Windows Server 2012 neste exemplo). Isso deve manualmente ser feito pelo administartor ativo Directory/CA.

Está aqui o exemplo como conseguir isso em Windows Server 2012 R2.

Certificados iniciais SCEP visíveis no ISE:



A suposição é que o CERTIFICADO MSCEP-RA está expirado e tem que ser renovado.

Solução

> Cuidado: Todas as mudanças em Windows Server devem ser consultadas com seu administrador primeiramente.

1. Identifique chaves privadas velhas

Encontre chaves do privite associadas com os Certificados RA no diretório ativo usando a ferramenta do **certutil**. Em seguida isso encontra o **recipiente chave.**

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

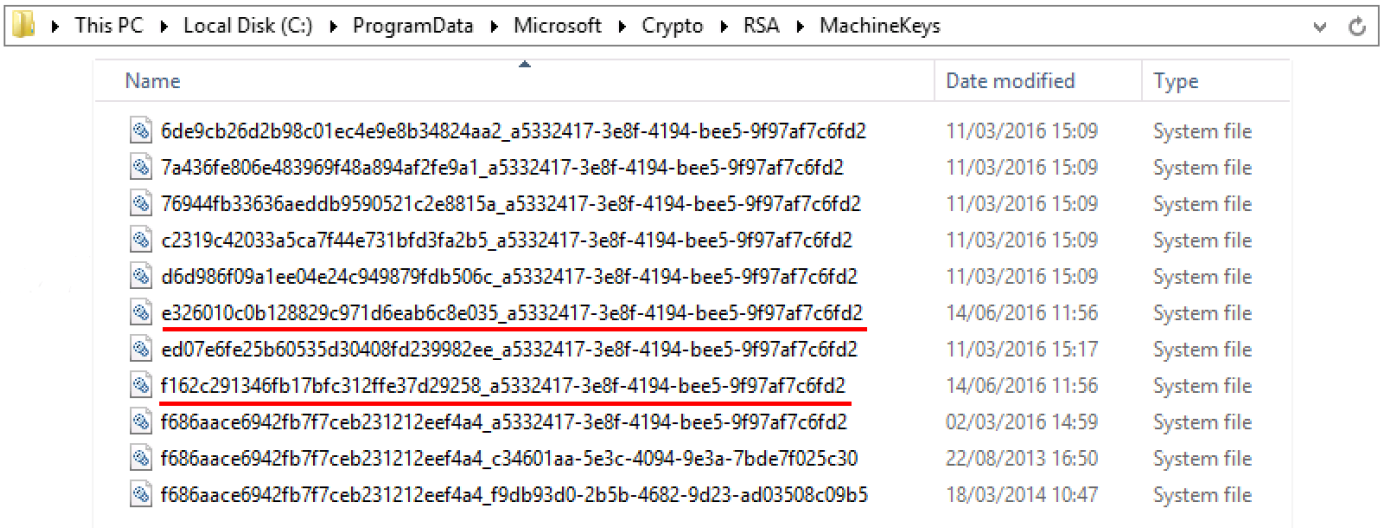
Note por favor que se o nome de seu certificado inicial MSCEP-RA é diferente então deve ser ajustado neste pedido. Contudo, à revelia deve conter o nome de computador.

```
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: 7a0000000a9f5dc313cd7a08fc00000000000a
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. Chaves privadas velhas da supressão

Suprima de consultar chaves manualmente do dobrador abaixo:

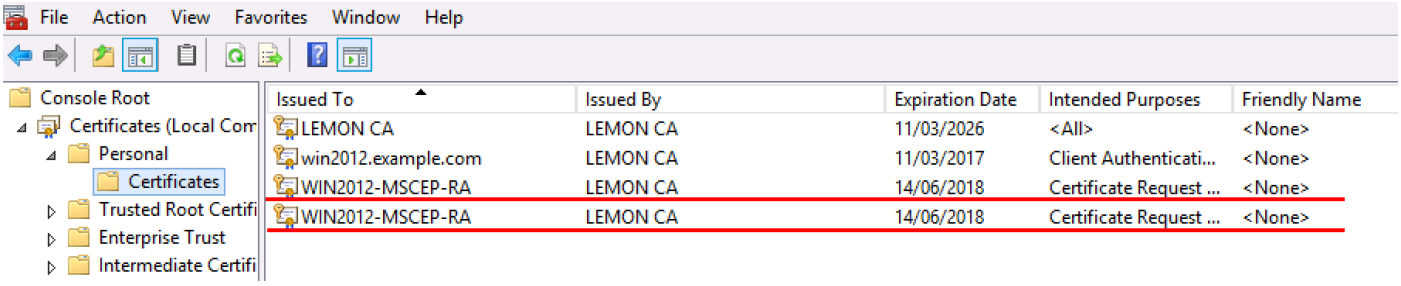
```
C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys
```



3. Suprima de ceritificates velhos MSCEP-RA

Após ter suprimido das chaves privadas, remova os ceritificates MSCEP-RA do console MMC.

O > Add MMC > de arquivo/remove Pressão-em… > Add "Ceritificates" > conta > computador local do computador



4. Gerencia Certificados novos para o SCEP

4.1. Gerencia o certificado do registro da troca

4.1.1. Crie um arquivo **cisco_ndes_sign.inf com o** índice abaixo. Esta informação é usada mais tarde pelo certreq.exetool a fim gerar a solicitação de assinatura 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
```

> Dica: Se você copia este molde do arquivo, certifique-se ajustá-lo conforme suas exigências e verificar se todos os caráteres são copiados corretamente (incluindo a cotação - marcas).

4.1.2. Crie o CSR baseado no arquivo do .INF com este comando:

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

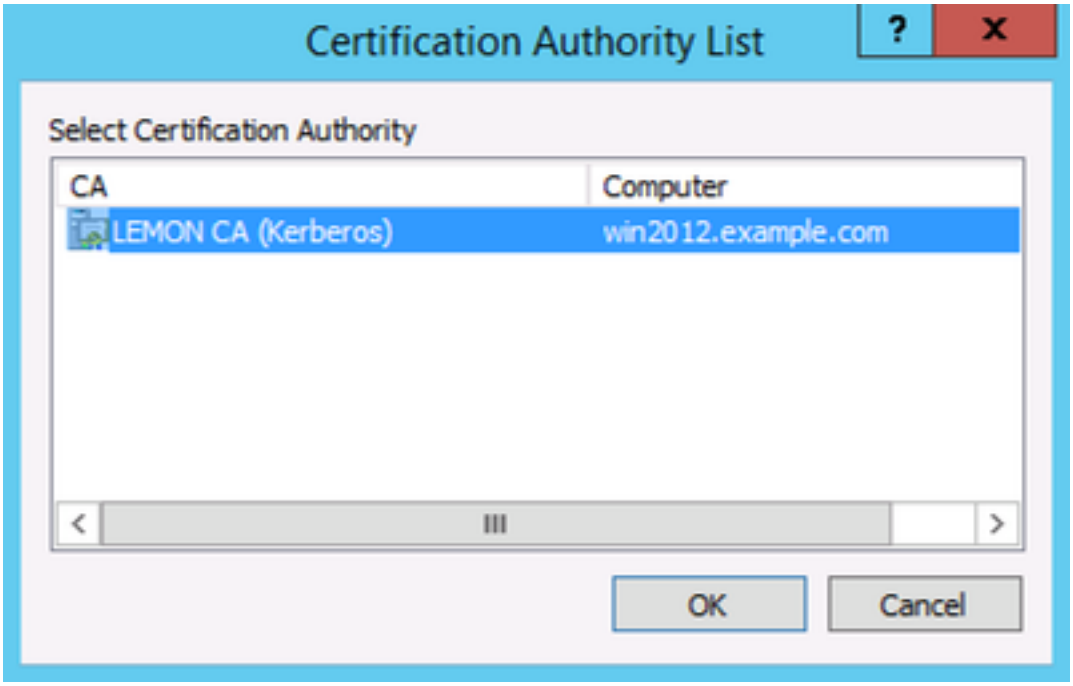
Se o **usuário** de advertência do diálogo **molde do contexto que opõe ao contexto da máquina** estala acima, clica a APROVAÇÃO. Este aviso pode ser ignorado.

```
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. Submeta o CSR com este comando:

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

Durante este procedimento um indicador estala acima e CA apropriado tem que ser escolhido.




```
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 Aceite o certificado emitido na etapa precedente. Em consequência deste comando, o certificado novo é importado e movido para a loja pessoal do computador local:

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

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

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

4.2. Gerencia o certificado da criptografia CEP

4.2.1. Crie um arquivo novo **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 as mesmas etapas como descrito em 4.1.

4.2.2. Gerencia um CSR baseado no arquivo novo do .INF:

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

4.2.3. Submeta o pedido:

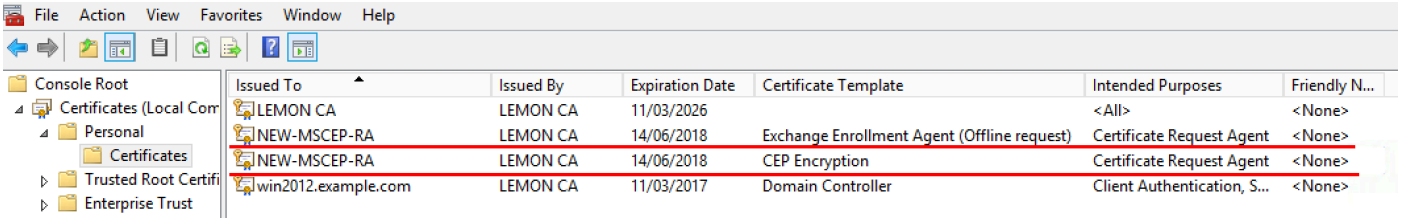
```
certreq -submit cisco_ndes_xchg.req cisco_ndes_xchg.cer
```

4.2.4: Aceite o certificado novo movendo o na loja pessoal do computador local:

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

5. Verificar

Após ter terminado etapa 4, dois Certificados novos MSCEP-RA aparecerão na loja pessoal do computador local:



Igualmente você pode verificar os Certificados com **ferramenta certutil.exe** (se certifique que você usa o nome novo correto do certificado). Os Certificados MSCEP-RA com nomes comuns novos e números de série novos devem ser indicados:

```
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. Reinício IIS

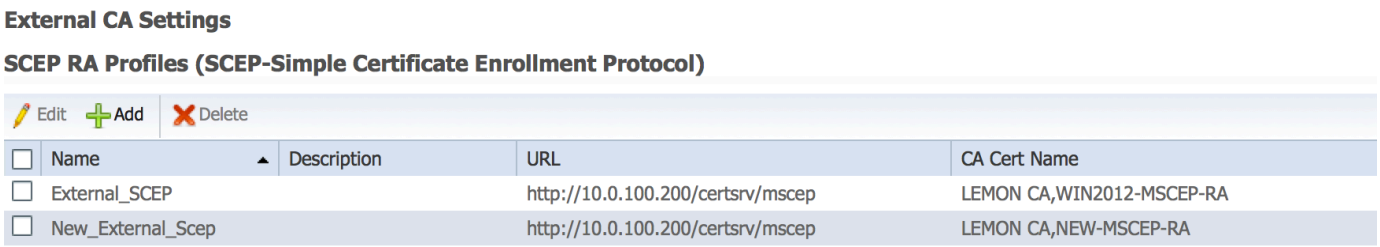
Server do Internet Information Services do reinício (IIS) a fim aplicar as mudanças:

```
iisreset.exe
```

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

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

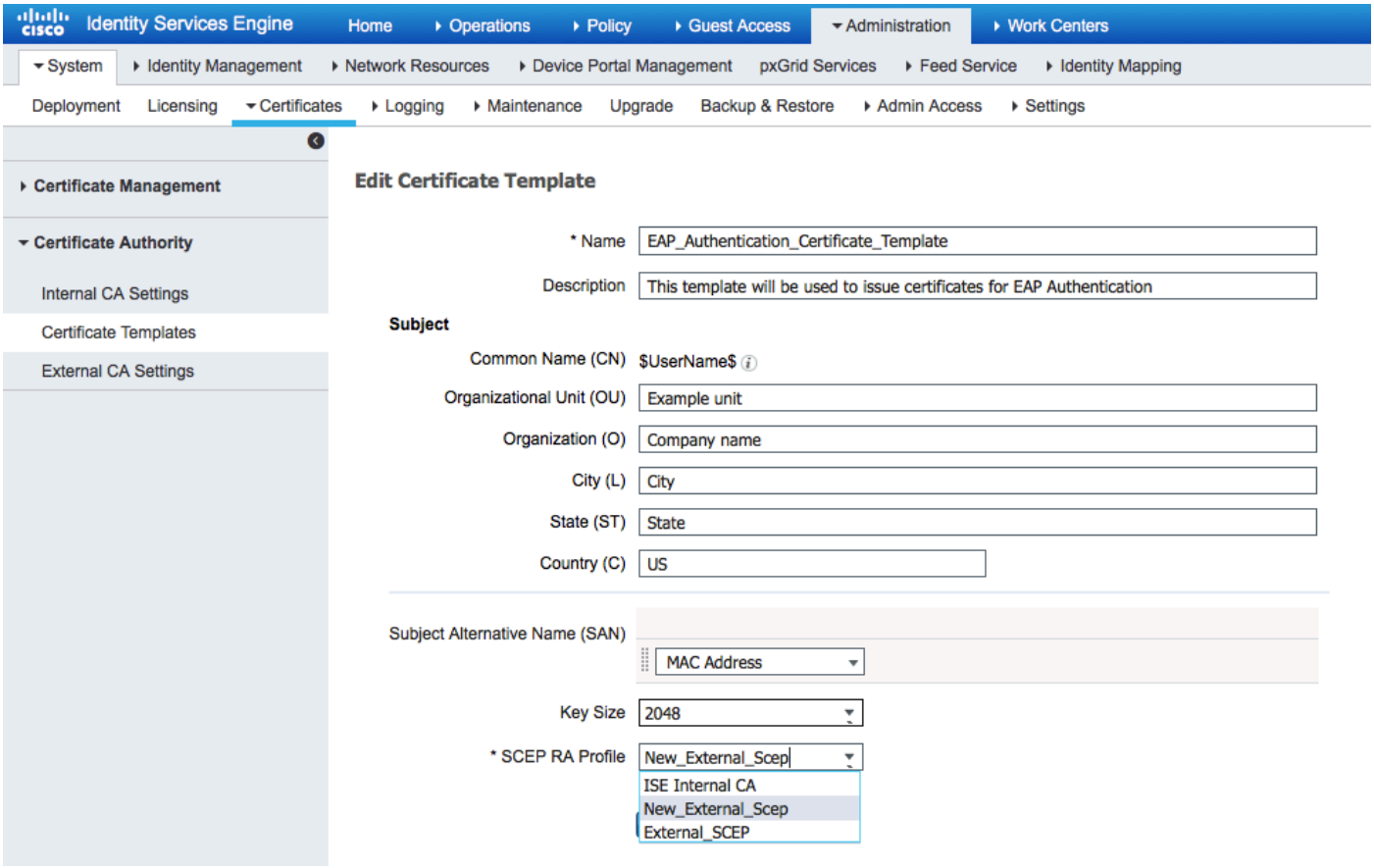
7. Crie o perfil novo SCEP RA

No ISE crie um perfil novo SCEP RA (com o mesmo server URL que velha), assim que os Certificados novos são transferidos e adicionados aos certificados confiáveis a loja:



8. Altere o molde de certificado

Certifique-se que o perfil novo SCEP RA está especificado no molde de certificado usado por BYOD (você pode o verificar na *administração > no sistema > nos Certificados > no Certificate Authority > nos moldes dos Certificados*):



Referências

1. Artigo da zona de Microsoft Technet
2. Manuais de configuração de Cisco ISE