ISE의 BYOD에 사용되는 Windows Server AD 2012에서 SCEP RA 인증서 갱신

목차

소개

이 문서에서는 SCEP(Simple Certificate Enrollment Protocol)에 사용되는 두 인증서를 갱신하는 방법에 대해 설명합니다.Microsoft Active Directory 2012의 Exchange 등록 에이전트 및 CEP 암호화 인증서

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Microsoft Active Directory 구성에 대한 기본 지식
- PKI(Public Key Infrastructure)에 대한 기본 지식
- ISE(Identity Services Engine)에 대한 기본 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Identity Services Engine 버전 2.0

- Microsoft Active Directory 2012 R2

문제

Cisco ISE는 SCEP 프로토콜을 사용하여 개인 장치 등록(BYOD 온보딩)을 지원합니다. 외부 SCEP CA를 사용할 때 이 CA는 ISE의 SCEP RA 프로필에 의해 정의됩니다.SCEP RA 프로파일이 생성되면 두 인증서가 신뢰할 수 있는 인증서 저장소에 자동으로 추가됩니다.

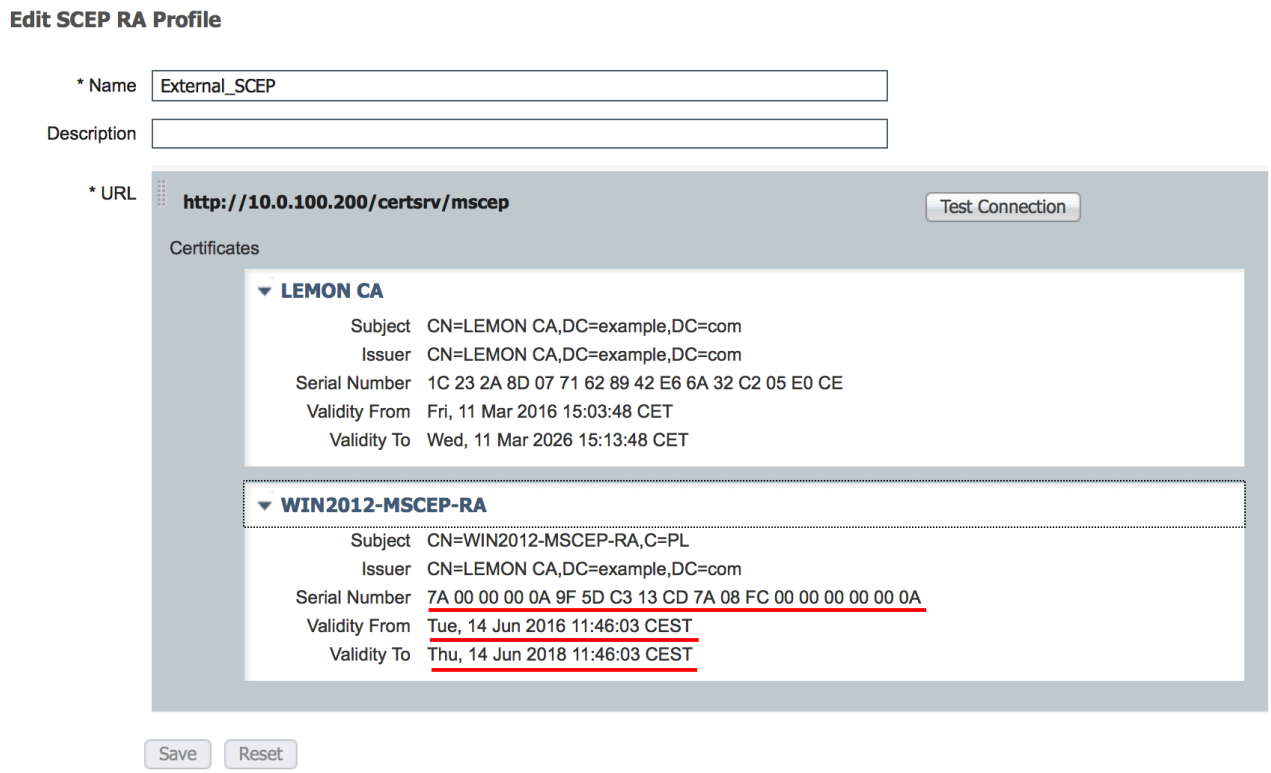
- CA 루트 인증서,
- CA에서 서명한 RA(등록 기관) 인증서

RA는 등록 디바이스에서 요청을 수신 및 검증하고, 클라이언트 인증서를 발급하는 CA에 요청을 전달하는 업무를 담당합니다.

RA 인증서가 만료되면 CA 측(이 예에서는 Windows Server 2012)에서 자동으로 갱신되지 않습니다. 이는 Active Directory/CA 관리자가 수동으로 수행해야 합니다.

다음은 Windows Server 2012 R2에서 이를 달성하는 방법의 예입니다.

ISE에 표시되는 초기 SCEP 인증서:



MSCEP-RA 인증서가 만료되어 갱신되어야 한다고 가정합니다.

솔루션

주의: Windows Server의 모든 변경 사항은 먼저 해당 관리자에게 문의하십시오.

1. 이전 개인 키 식별

certutil 툴을 사용하여 Active Directory에서 RA 인증서와 연결된 개인 키를 찾습니다.그런 다음 **키 컨테이너를 찾습니다.**

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

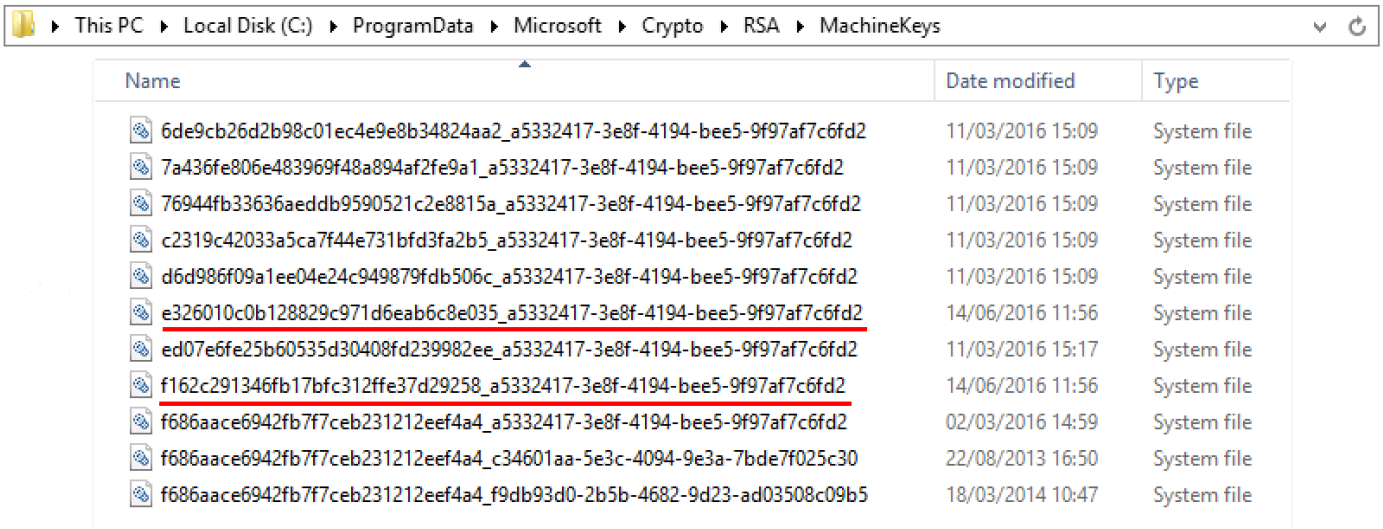
초기 MSCEP-RA 인증서의 이름이 다른 경우 이 요청에서 조정되어야 합니다.그러나 기본적으로 컴퓨터 이름이 포함되어야 합니다.

```
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. 이전 개인 키 삭제

아래 폴더에서 참조 키를 수동으로 삭제합니다.

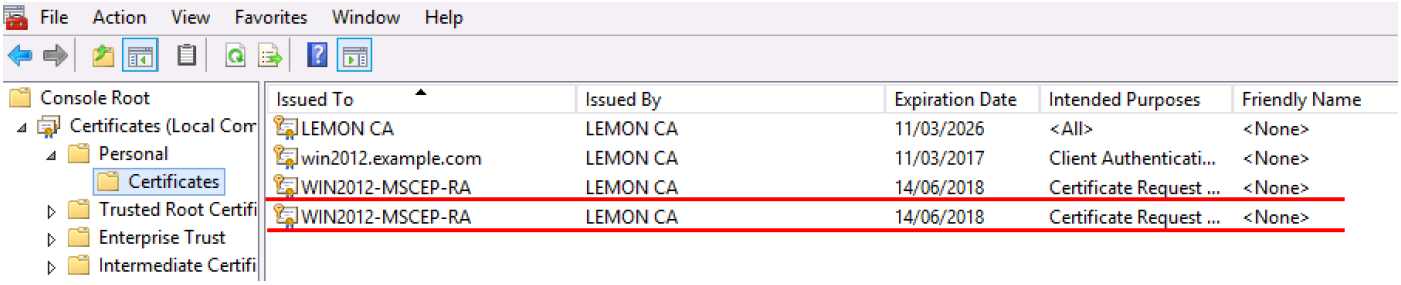
```
C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys
```



3. 이전 MSCEP-RA 인증서 삭제

개인 키를 삭제한 후 MMC 콘솔에서 MSCEP-RA 인증서를 제거합니다.

MMC > 파일 > 스냅인 추가/제거... > "인증서 추가" > 컴퓨터 계정 > 로컬 컴퓨터



4. SCEP에 대한 새 인증서를 생성합니다.

4.1. Exchange 등록 인증서 생성

4.1.1. 아래의 내용을 사용하여 **cisco_ndes_sign.inf** 파일을 생성합니다.이 정보는 나중에 CSR(Certificate Signing Request)을 생성하기 위해 certreq.**exe** 도구에서 사용합니다.

```
[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
```

팁:이 파일 템플릿을 복사할 경우 요구 사항에 따라 파일을 조정하고 모든 문자가 올바르게 복사되었는지(따옴표 포함) 확인하십시오.

4.1.2. 다음 명령을 사용하여 .INF 파일을 기반으로 CSR을 만듭니다.

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

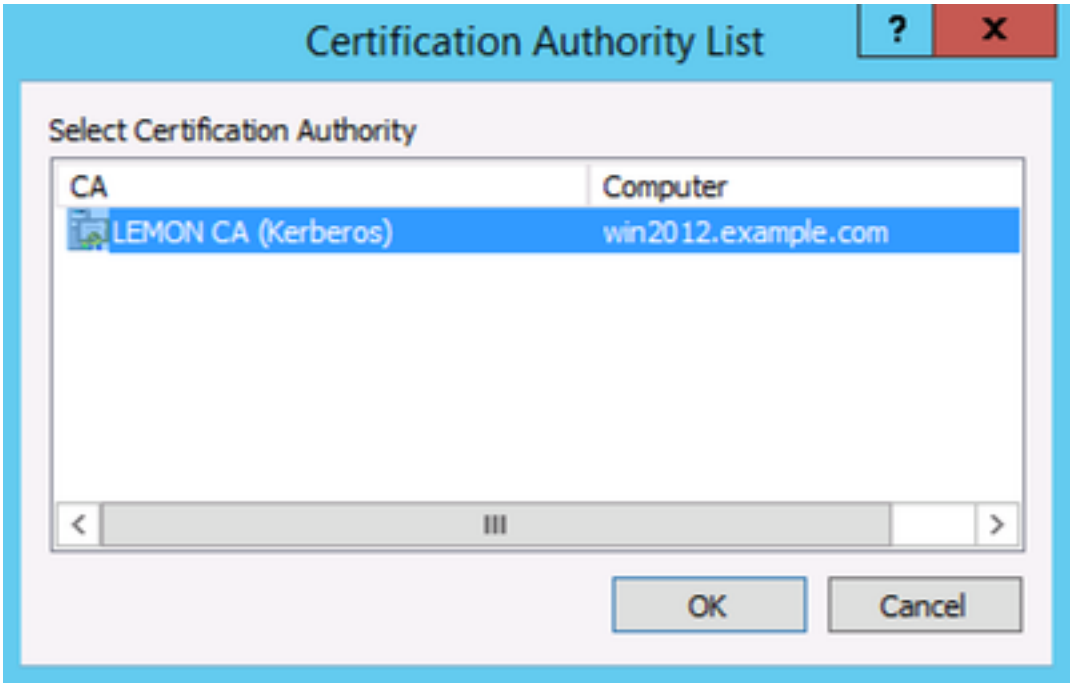
경고 대화 상자 **사용자 컨텍스트 템플릿이 시스템 컨텍스트와 충돌하는 경우** 확인을 클릭합니다.이 경고는 무시될 수 있습니다.

```
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. 다음 명령을 사용하여 CSR을 제출합니다.

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

이 절차를 진행하는 동안 창이 열리고 적절한 CA를 선택해야 합니다.




```
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 이전 단계에서 발급된 인증서를 수락합니다.이 명령의 결과로 새 인증서를 가져오고 로컬 컴퓨터 개인 저장소로 이동합니다.

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

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

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

4.2. CEP 암호화 인증서 생성

4.2.1. 새 파일 cisco_ndes_xchg.inf를 생성합니다.

```
[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
```

4.1에 설명된 것과 동일한 단계를 수행합니다.

4.2.2. 새 .INF 파일을 기반으로 CSR을 생성합니다.

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

4.2.3. 요청을 실행합니다.

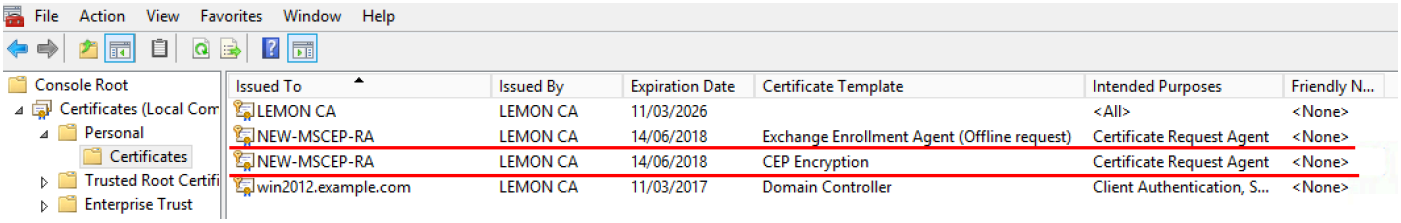
```
certreq -submit cisco_ndes_xchg.req cisco_ndes_xchg.cer
```

4.2.4:로컬 컴퓨터 개인 저장소로 이동하여 새 인증서를 수락합니다.

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

5. 확인

4단계를 마치면 2개의 새 MSCEP-RA 인증서가 로컬 컴퓨터 개인 저장소에 나타납니다.



certutil.exe 도구를 사용하여 인증서를 확인할 수도 있습니다(올바른 새 인증서 이름을 사용하는지 확인).새 공통 이름 및 새 일련 번호가 포함된 MSCEP-RA 인증서가 표시되어야 합니다.

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

```
C:\Users\Administrator\Desktop>certutil -store MY NEW-MSCEP-RA
MY "Personal"
================ Certificate 2 ================
Serial Number: 7a0000000cb250f5a9d6c1135000000000000c
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. IIS를 다시 시작합니다.

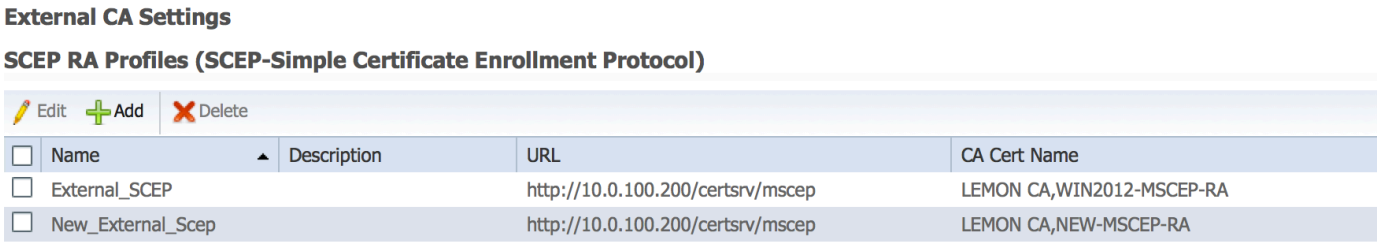
변경 내용을 적용하려면 IIS(인터넷 정보 서비스) 서버를 다시 시작하십시오.

```
iisreset.exe
```

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

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

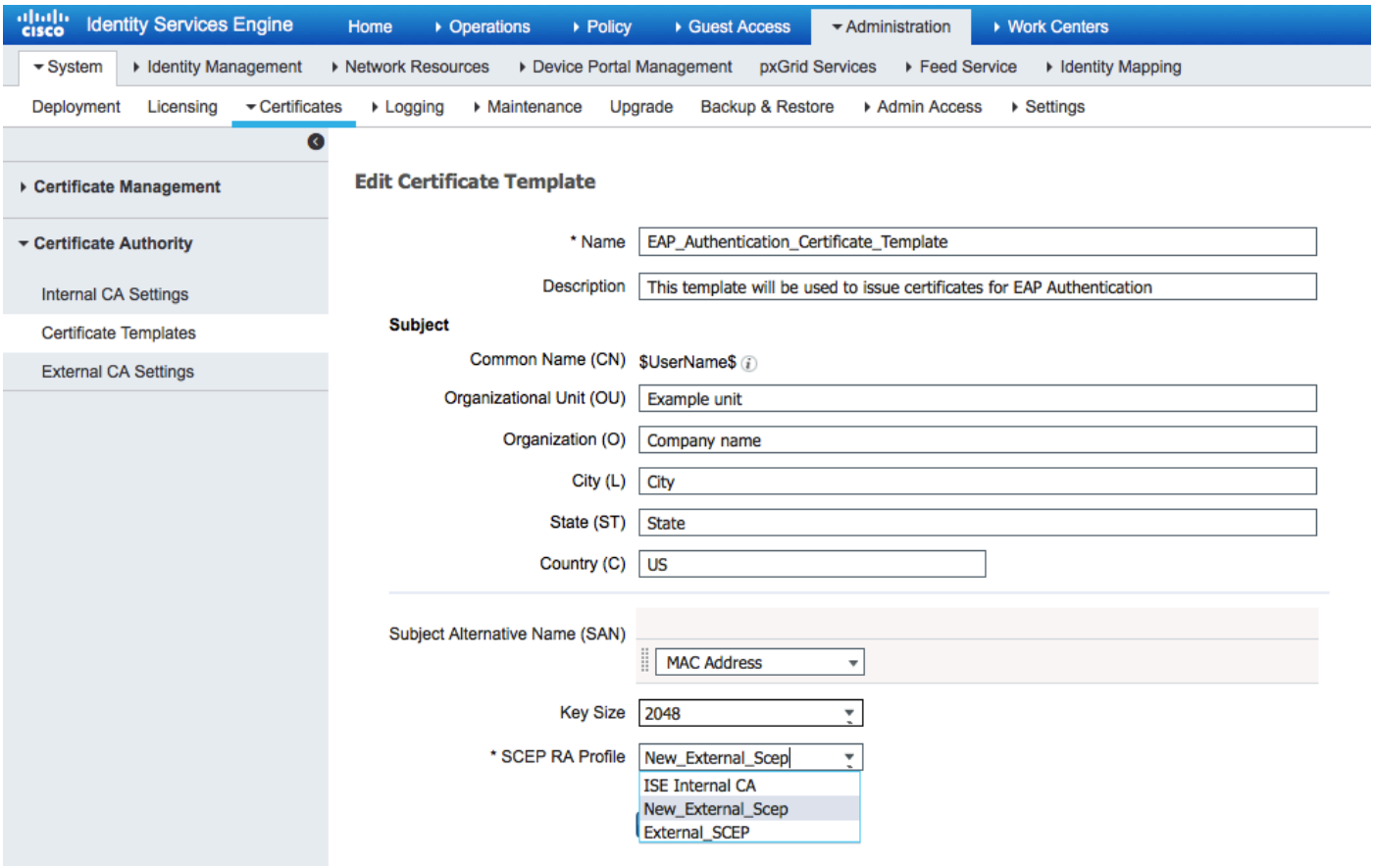
7. 새 SCEP RA 프로파일 생성

ISE에서 새 SCEP RA 프로필(이전 URL과 동일한 서버 URL)을 생성하므로 새 인증서가 다운로드되고 신뢰할 수 있는 인증서 저장소에 추가됩니다.



8. 인증서 템플릿 수정

새 SCEP RA 프로파일이 BYOD에서 사용하는 인증서 템플릿에 지정되었는지 확인합니다(*관리 > 시스템 > 인증서 > 인증 기관 > 인증서 템플릿*에서 확인할 수 있음).



참조

1. [microsoft 기술권역 문서]
2. [Cisco ISE 컨피그레이션 가이드]