

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

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[문제](#)

[솔루션](#)

[1. 이전 개인 키 식별](#)

[2. 이전 개인 키 삭제](#)

[3. 이전 MSCEP-RA 인증서 삭제](#)

[4. SCEP에 대한 새 인증서를 생성합니다.](#)

[4.1. Exchange 등록 인증서 생성](#)

[4.2. CEP 암호화 인증서 생성](#)

[5. 확인](#)

[6. IIS를 다시 시작합니다.](#)

[7. 새 SCEP RA 프로파일 생성](#)

[8. 인증서 템플릿 수정](#)

[참조](#)

## 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:

### Edit SCEP RA Profile

\* Name

Description

\* URL

Certificates

- LEMOM CA**
  - Subject CN=LEMOM CA,DC=example,DC=com
  - Issuer CN=LEMOM CA,DC=example,DC=com
  - Serial Number 1C 23 2A 8D 07 71 62 89 42 E6 6A 32 C2 05 E0 CE
  - Validity From Fri, 11 Mar 2016 15:03:48 CET
  - Validity To Wed, 11 Mar 2026 15:13:48 CET
- WIN2012-MSCEP-RA**
  - Subject CN=WIN2012-MSCEP-RA,C=PL
  - Issuer CN=LEMOM CA,DC=example,DC=com
  - Serial Number 7A 00 00 00 0A 9F 5D C3 13 CD 7A 08 FC 00 00 00 00 0A
  - Validity From Tue, 14 Jun 2016 11:46:03 CEST
  - Validity To Thu, 14 Jun 2018 11:46:03 CEST

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
```

This PC > Local Disk (C:) > ProgramData > Microsoft > Crypto > RSA > MachineKeys

Name	Date modified	Type
6de9cb26d2b98c01ec4e9e8b34824aa2_a5332417-3e8f-4194-bee5-9f97af7c6fd2	11/03/2016 15:09	System file
7a436fe806e483969f48a894af2fe9a1_a5332417-3e8f-4194-bee5-9f97af7c6fd2	11/03/2016 15:09	System file
76944fb33636aeddb9590521c2e8815a_a5332417-3e8f-4194-bee5-9f97af7c6fd2	11/03/2016 15:09	System file
c2319c42033a5ca7f44e731bfd3fa2b5_a5332417-3e8f-4194-bee5-9f97af7c6fd2	11/03/2016 15:09	System file
d6d986f09a1ee04e24c949879fdb506c_a5332417-3e8f-4194-bee5-9f97af7c6fd2	11/03/2016 15:09	System file
<u>e326010c0b128829c971d6eab6c8e035_a5332417-3e8f-4194-bee5-9f97af7c6fd2</u>	14/06/2016 11:56	System file
ed07e6fe25b60535d30408fd239982ee_a5332417-3e8f-4194-bee5-9f97af7c6fd2	11/03/2016 15:17	System file
<u>f162c291346fb17bfc312ffe37d29258_a5332417-3e8f-4194-bee5-9f97af7c6fd2</u>	14/06/2016 11:56	System file
f686aace6942fb7f7ceb231212eef4a4_a5332417-3e8f-4194-bee5-9f97af7c6fd2	02/03/2016 14:59	System file
f686aace6942fb7f7ceb231212eef4a4_c34601aa-5e3c-4094-9e3a-7bde7f025c30	22/08/2013 16:50	System file
f686aace6942fb7f7ceb231212eef4a4_f9db93d0-2b5b-4682-9d23-ad03508c09b5	18/03/2014 10:47	System file

### 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

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
LEMON CA	LEMON CA	11/03/2026	<All>	<None>
win2012.example.com	LEMON CA	11/03/2017	Client Authenticati...	<None>
<u>WIN2012-MSCEP-RA</u>	<u>LEMON CA</u>	<u>14/06/2018</u>	<u>Certificate Request ...</u>	<u>&lt;None&gt;</u>
<u>WIN2012-MSCEP-RA</u>	<u>LEMON CA</u>	<u>14/06/2018</u>	<u>Certificate Request ...</u>	<u>&lt;None&gt;</u>

### 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(다음표 포함) 확인하십시오.

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

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

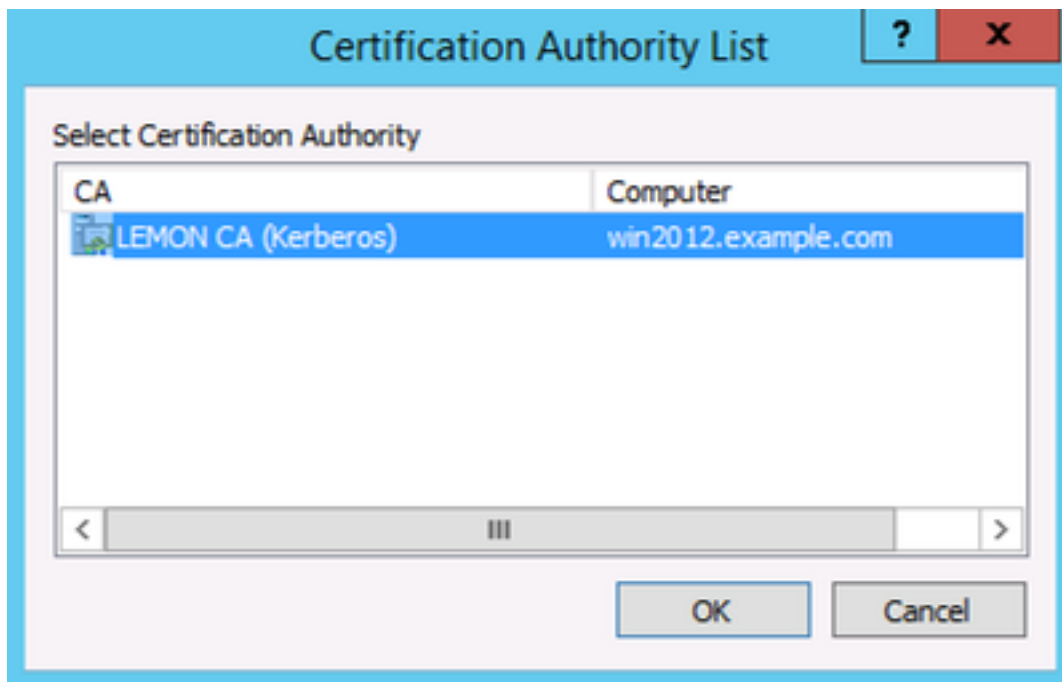
경고 대화 상자 사용자 컨텍스트 템플릿이 시스템 컨텍스트와 충돌하는 경우 확인을 클릭합니다.이 경고는 무시될 수 있습니다.

```
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.

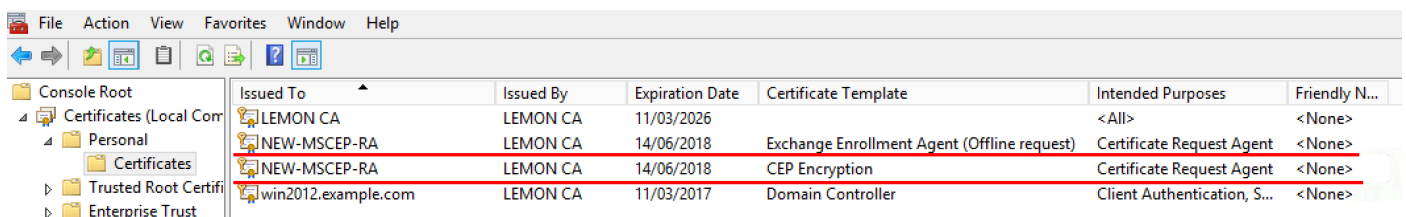
```
certreq -submit cisco_ndes_xchg.req cisco_ndes_xchg.cer
```

### 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.



Issued To	Issued By	Expiration Date	Certificate Template	Intended Purposes	Friendly N...
LEMON CA	LEMON CA	11/03/2026		<All>	<None>
NEW-MSCEP-RA	LEMON CA	14/06/2018	Exchange Enrollment Agent (Offline request)	Certificate Request Agent	<None>
NEW-MSCEP-RA	LEMON CA	14/06/2018	CEP Encryption	Certificate Request Agent	<None>
win2012.example.com	LEMON CA	11/03/2017	Domain Controller	Client Authentication, S...	<None>

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: 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. 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 프로파일(이전 URL과 동일한 서버 URL)을 생성하므로 새 인증서가 다운로드 되고 신뢰할 수 있는 인증서 저장소에 추가됩니다.

## External CA Settings

### SCEP RA Profiles (SCEP-Simple Certificate Enrollment Protocol)

<input type="checkbox"/>	Name	Description	URL	CA Cert Name
<input type="checkbox"/>	External_SCEP		http://10.0.100.200/certsrv/mscep	LEMON CA,WIN2012-MSCEP-RA
<input type="checkbox"/>	New_External_Scep		http://10.0.100.200/certsrv/mscep	LEMON CA,NEW-MSCEP-RA

## 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).

The screenshot displays the 'Edit Certificate Template' configuration page in the Cisco ISE Administration console. The left sidebar shows the navigation menu with 'Certificate Management' expanded. The main content area contains the following fields:

- Name:** EAP\_Authentication\_Certificate\_Template
- Description:** This template will be used to issue certificates for EAP Authentication
- Subject:**
  - Common Name (CN): \$UserName\$
  - Organizational Unit (OU): Example unit
  - Organization (O): Company name
  - City (L): City
  - State (ST): State
  - Country (C): US
- Subject Alternative Name (SAN):** MAC Address
- Key Size:** 2048
- \* SCEP RA Profile:** New\_External\_Scep (selected), ISE Internal CA, New\_External\_Scep, External\_SCEP

## 참조

- [microsoft 기술권역 문서](#)
- [Cisco ISE 컨피그레이션 가이드](#)