

Verleng SCEP RA-certificaat op Windows Server AD 2012, gebruikt voor BYOD op ISE

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Probleem](#)

[Oplossing](#)

[1. Identificeer oude privé-sleutels](#)

[2. Verwijder oude privé-toetsen](#)

[3. Verwijder oude MSCEP-RA-certificaten](#)

[4. Nieuwe certificaten genereren voor SCEP](#)

[4.1. Het inlogcertificaat genereren](#)

[4.2. Het CEP-versleutelcertificaat genereren](#)

[5. Controleer](#)

[6. Herstart IS](#)

[7. Een nieuw SCEP RA-profiel maken](#)

[8. certificaatsjabloon wijzigen](#)

[Referenties](#)

Inleiding

Dit document beschrijft hoe u twee certificaten kunt vernieuwen die worden gebruikt voor Eenvoudig protocol voor certificaatinschrijving (SCEP): Exchange Encapsulation Agent en CEP Encryption certificate in Microsoft Active Directory 2012.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van Microsoft Active Directory-configuratie
- Basiskennis van de openbare sleutelinfrastructuur (PKI)
- Basiskennis van Identity Services Engine (ISE)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Identity Services Engine versie 2.0

- Microsoft Active Directory 2012 R2

Probleem

Cisco ISE gebruikt SCEP-protocol ter ondersteuning van de registratie van persoonlijk apparaat (BYOD-on-boarding). Wanneer een extern SCEP CA wordt gebruikt, wordt dit CA gedefinieerd door een SCEP RA profiel op ISE. Wanneer een SCEP RA-profiel wordt gecreëerd, worden automatisch twee certificaten toegevoegd aan de Trusted Certificates-winkel:

- CA-basiscertificaat,
- RA (Registratieautoriteit)-certificaat dat door de CA is ondertekend.

RA is verantwoordelijk voor het ontvangen en valideren van het verzoek van het registrerende apparaat en het doorsturen ervan naar de CA die het client-certificaat afgeeft.

Als het RA-certificaat afloopt, wordt het niet automatisch verlengd aan de CA-kant (in dit voorbeeld Windows Server 2012). Dit moet handmatig worden gedaan door de beheerder Active Directory/CA.

Hier is het voorbeeld hoe je dat kunt bereiken op Windows Server 2012 R2.

Oorspronkelijke SCEP-certificaten zichtbaar op ISE:

Edit SCEP RA Profile

* Name

Description

* URL

Certificates

▼ **LEMON CA**

Subject	CN=LEMON CA,DC=example,DC=com
Issuer	CN=LEMON 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=LEMON CA,DC=example,DC=com
Serial Number	<u>7A 00 00 00 0A 9F 5D C3 13 CD 7A 08 FC 00 00 00 00 0A</u>
Validity From	<u>Tue, 14 Jun 2016 11:46:03 CEST</u>
Validity To	<u>Thu, 14 Jun 2018 11:46:03 CEST</u>

Aangenomen wordt dat het MSCEP-RA-CERTIFICAAT is verlopen en moet worden verlengd.

Oplossing

Voorzichtig: Alle wijzigingen op Windows Server moeten eerst met de beheerder worden geraadpleegd.

1. Identificeer oude privé-sleutels

Zoek privétoetsen geassocieerd met de RA certificaten op de Actieve Map met behulp van certutil tool. Plaats daarna Key container.

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

Als de naam van uw oorspronkelijke MSCEP-RA-certificaat anders is, dient deze in dit verzoek te worden aangepast. De standaardinstelling is echter dat deze de computernaam bevat.

```
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 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. Verwijder oude privé-toetsen

Verwijdert de verwijzingstoetsen handmatig uit de onderstaande map:

```
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. Verwijder oude MSCEP-RA-certificaten

Nadat u de privé toetsen hebt verwijderd, verwijdert u de MSCEP-RA certificaten uit de MMC-console.

MMC > Bestand > Magnetisch toevoegen/verwijderen... > Bijvoegen "Certificaten" > Computer-account > Lokale computer

File Action View Favorites Window Help

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><None></u>
<u>WIN2012-MSCEP-RA</u>	<u>LEMON CA</u>	<u>14/06/2018</u>	<u>Certificate Request ...</u>	<u><None></u>

4. Nieuwe certificaten genereren voor SCEP

4.1. Het inlogcertificaat genereren

4.1.1. Maak een bestand van **cisco_ndes_sign.inf** met de onderstaande inhoud. Deze informatie wordt later door het gereedschap **certreq.exe** gebruikt om de certificaataanvraag (CSR) te genereren:

```
[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

Tip: Als u deze bestandsjabloon kopieert, moet u deze volgens uw vereisten aanpassen en controleren of alle tekens correct zijn gekopieerd (inclusief aanhalingstekens).

4.1.2. Maak CSR op basis van het .INF-bestand met deze opdracht:

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

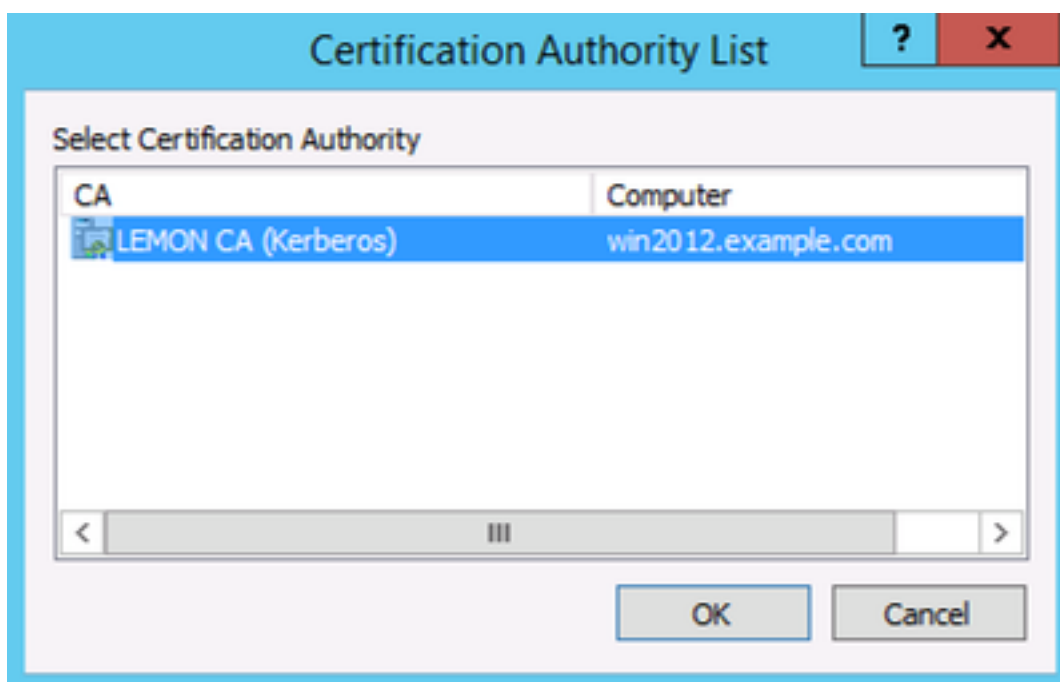
Als er een **conflict ontstaat tussen de** waarschuwingscontext van de **gebruikerscontext en de** context van de **machine**, klikt u op OK. Deze waarschuwing kan worden genegeerd.

```
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. Vermeld de CSR met deze opdracht:

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

Tijdens deze procedure verschijnt een venster en wordt een juiste CA gekozen.



```
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 Aanvaard het in de vorige stap afgegeven certificaat. Als resultaat van deze opdracht, wordt

het nieuwe certificaat geïmporteerd en overgebracht naar de lokale PC Persoonlijke winkel:

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

4.2. Het CEP-versleutelcertificaat genereren

4.2.1. Maak een nieuw bestand `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
```

Volg dezelfde stappen als in punt 4.1.

4.2.2. Generate a CSR op basis van het nieuwe .INF-bestand:

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

4.2.3. Vermeld het verzoek:

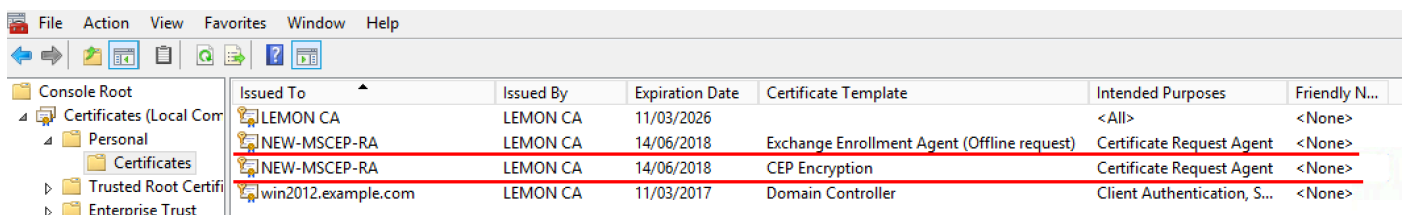
```
certreq -submit cisco_ndes_xchg.req cisco_ndes_xchg.cer
```

4.2.4: Accepteer het nieuwe certificaat door het naar de persoonlijke winkel van de lokale computer te verplaatsen:

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

5. Controleer

Na voltooiing van stap 4 worden twee nieuwe MSCEP-RA-certificaten in de Local Computer Mobile Store aangebracht:



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>

U kunt de certificaten ook controleren met het gereedschap **certutil.exe** (controleer of u de juiste nieuwe certificaatnaam gebruikt). MSCEP-RA-certificaten met nieuwe gemeenschappelijke namen en nieuwe serienummers moeten worden weergegeven:

```
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 = 320e64806hd159eca7b12283f3f67ee6_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. Herstart IS

Start Internet Information Services (IS)-server opnieuw om de wijzigingen toe te passen:

iisreset.exe

```
C:\Users\Administrator\Desktop>iisreset.exe
Attempting stop...
Internet services successfully stopped
Attempting start...
Internet services successfully restarted
```

7. Een nieuw SCEP RA-profiel maken

Op ISE om een nieuw SCEP RA profiel te maken (met dezelfde server-URL als de oude), zodat nieuwe certificaten worden gedownload en toegevoegd aan de Trusted Certificates Store:

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. certificaatsjabloon wijzigen

Zorg ervoor dat het nieuwe SCEP RA-profiel is gespecificeerd in de certificaatsjabloon die door BYOD wordt gebruikt (u kunt dit controleren in *Beheer > Systeem > Certificaten > certificaatinstantie > Certificaatsjablonen*):

The screenshot displays the 'Edit Certificate Template' configuration page in the Cisco Identity Services Engine (ISE) interface. The page is titled 'Edit Certificate Template' and shows the following configuration details:

- 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 from a dropdown menu that also includes ISE Internal CA and External_SCEP)

Referenties

1. [Artikel over Microsoft technische zone](#)
2. [Cisco ISE-configuratiehandleidingen](#)