

# Verlängern Sie das SCEP RA-Zertifikat für Windows Server AD 2012, das für BYOD auf der ISE verwendet wird.

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Problem](#)

[Lösung](#)

[1. Identifizieren alter privater Schlüssel](#)

[2. Alte private Schlüssel löschen](#)

[3. Alte MSCEP-RA-Zertifikate löschen](#)

[4. Erstellen neuer Zertifikate für SCEP](#)

[4.1 Erstellen des Exchange-Anmeldezertifikats](#)

[4.2 Generieren des CEP-Verschlüsselungszertifikats](#)

[5. Überprüfen](#)

[6. IIS neu starten](#)

[7. Neues SCEP-RA-Profil erstellen](#)

[8. Zertifikatsvorlage ändern](#)

[Referenzen](#)

## Einführung

In diesem Dokument wird beschrieben, wie Sie zwei Zertifikate erneuern, die für das Simple Certificate Enrollment Protocol (SCEP) verwendet werden: Exchange Enrollment Agent und CEP Encryption-Zertifikat auf Microsoft Active Directory 2012.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Grundkenntnisse der Microsoft Active Directory-Konfiguration
- Grundkenntnisse der Public Key Infrastructure (PKI)
- Grundkenntnisse der Identity Services Engine (ISE)

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und

Hardwareversionen:

- Cisco Identity Services Engine Version 2.0
- Microsoft Active Directory 2012 R2

## Problem

Die Cisco ISE verwendet das SCEP-Protokoll, um die Registrierung von privaten Geräten (BYOD Onboarding) zu unterstützen. Bei Verwendung einer externen SCEP-CA wird diese CA durch ein SCEP-RA-Profil auf der ISE definiert. Wenn ein SCEP-RA-Profil erstellt wird, werden dem Trusted Certificates Store automatisch zwei Zertifikate hinzugefügt:

- CA-Stammzertifikat,
- RA (Registration Authority)-Zertifikat, das von der Zertifizierungsstelle signiert wird.

RA ist dafür verantwortlich, die Anforderung vom registrierenden Gerät zu empfangen und zu validieren und an die Zertifizierungsstelle weiterzuleiten, die das Client-Zertifikat ausstellt.

Wenn das RA-Zertifikat abläuft, wird es auf CA-Seite nicht automatisch verlängert (in diesem Beispiel Windows Server 2012). Dies sollte manuell vom Active Directory/CA-Administrator durchgeführt werden.

Dies ist ein Beispiel dafür, wie Sie dies auf Windows Server 2012 R2 erreichen.

Die ersten SCEP-Zertifikate sind auf der ISE sichtbar:

### 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 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>

Es wird davon ausgegangen, dass das MSCEP-RA-ZERTIFIKAT abgelaufen ist und verlängert werden muss.

## Lösung

**Vorsicht:** Alle Änderungen an Windows Server sollten zuerst mit dem Administrator abgefragt werden.

## 1. Identifizieren alter privater Schlüssel

Suchen Sie mithilfe des **certutil**-Tools nach privaten Schlüsseln, die den RA-Zertifikaten im Active Directory zugeordnet sind. Suchen Sie anschließend nach **Schlüsselcontainern**.

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

Wenn der Name Ihres ursprünglichen MSCEP-RA-Zertifikats nicht identisch ist, sollte er in dieser Anforderung angepasst werden. Standardmäßig sollte er jedoch den Computernamen enthalten.

```
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. Alte private Schlüssel löschen

Löschen Sie die verweisenden Tasten manuell aus dem Ordner unten:

```
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. Alte MSCEP-RA-Zertifikate löschen

Entfernen Sie nach dem Löschen der privaten Schlüssel die MSCEP-RA-Zertifikate aus der MMC-Konsole.

MMC > Datei > Snap-In hinzufügen/entfernen... > "Zertifikate" > Computerkonto > Lokaler Computer hinzufügen

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. Erstellen neuer Zertifikate für SCEP

#### 4.1 Erstellen des Exchange-Anmeldezertifikats

4.1.1 Erstellen Sie eine Datei `cisco_ndes_sign.inf` mit dem folgenden Inhalt. Diese Informationen werden später vom Tool `certreq.exe` verwendet, um die Zertifikatssignierungsanforderung (Certificate Signing Request, CSR) zu generieren:

```
[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

**Tipp:** Wenn Sie diese Dateivorlage kopieren, stellen Sie sicher, dass Sie sie an Ihre Anforderungen anpassen und überprüfen, ob alle Zeichen ordnungsgemäß kopiert wurden (einschließlich Anführungszeichen).

4.1.2 Erstellen Sie mit dem folgenden Befehl CSR auf der Grundlage der INF-Datei:

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

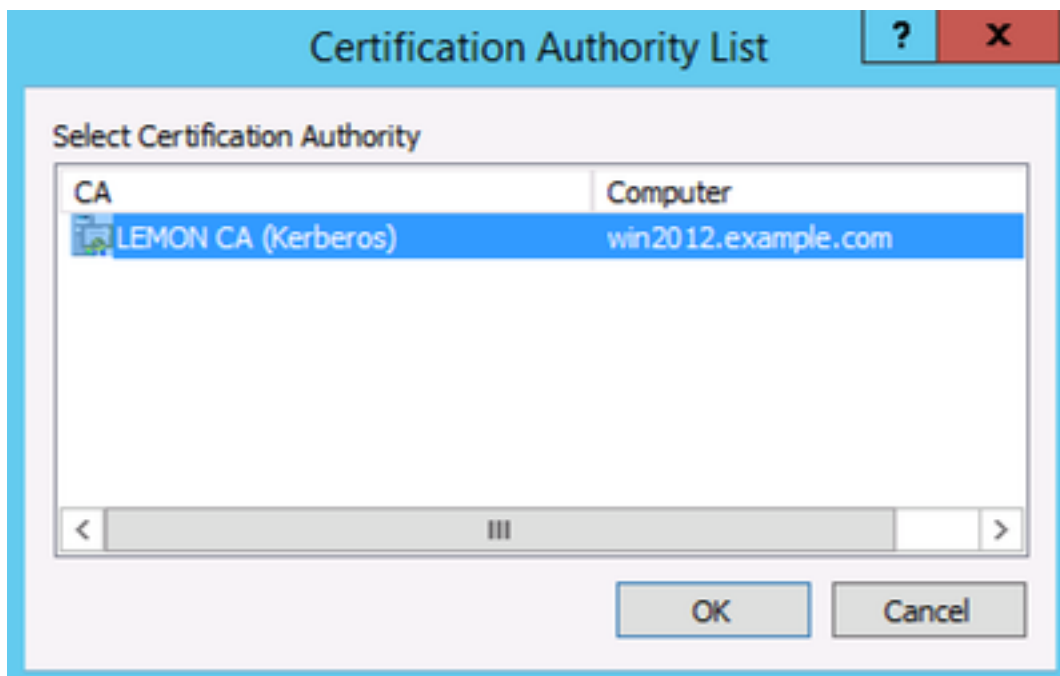
Wenn das Warndialogfeld **Benutzerkontextregelungen mit Maschinenkontexten in Konflikt** steht, klicken Sie auf OK. Diese Warnung kann ignoriert werden.

```
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 Senden Sie die CSR-Anfrage mit dem folgenden Befehl:

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

Während dieses Vorgangs wird ein Fenster geöffnet, und die richtige CA muss ausgewählt werden.



```
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 Das im vorherigen Schritt ausgestellte Zertifikat akzeptieren. Durch diesen Befehl wird das neue Zertifikat importiert und in den lokalen Computer Personal Store verschoben:

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

## 4.2 Generieren des CEP-Verschlüsselungszertifikats

### 4.2.1 Erstellen Sie eine neue Datei 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
```

Befolgen Sie die gleichen Schritte wie in 4.1 beschrieben.

### 4.2.2 Erstellen Sie einen CSR auf der Grundlage der neuen INF-Datei:

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

### 4.2.3 Senden Sie die Anfrage:

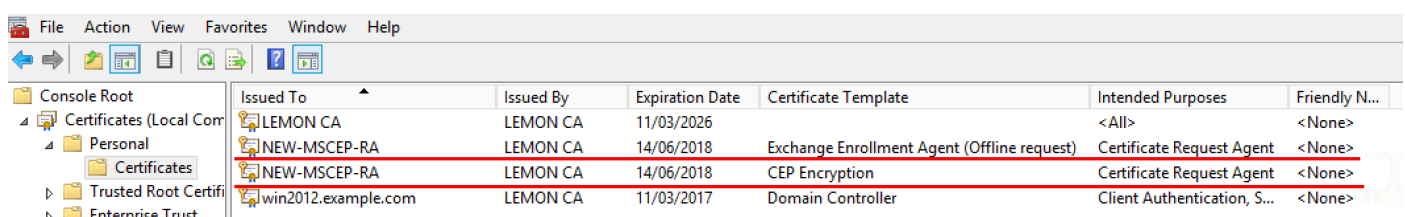
```
certreq -submit cisco_ndes_xchg.req cisco_ndes_xchg.cer
```

4.2.4 Akzeptieren Sie das neue Zertifikat, indem Sie es in den lokalen Computer Personal Store verschieben:

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

## 5. Überprüfen

Nach Abschluss von Schritt 4 werden zwei neue MSCEP-RA-Zertifikate im lokalen Computer Personal Store angezeigt:



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>

Sie können die Zertifikate auch mit dem Tool `certutil.exe` überprüfen (verwenden Sie den richtigen neuen Zertifikatsnamen). MSCEP-RA-Zertifikate mit neuen gemeinsamen Namen und neuen Seriennummern müssen angezeigt werden:

```
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. IIS neu starten

Starten Sie den IIS-Server (Internetinformationsdienste) neu, um die Änderungen anzuwenden:

```
iisreset.exe
```

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

## 7. Neues SCEP-RA-Profil erstellen

Erstellen Sie auf der ISE ein neues SCEP RA-Profil (mit derselben Server-URL wie der alte), sodass neue Zertifikate heruntergeladen und dem Trusted Certificates Store hinzugefügt werden:

## 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. Zertifikatsvorlage ändern

Vergewissern Sie sich, dass das neue SCEP-RA-Profil in der vom BYOD verwendeten Zertifikatsvorlage festgelegt ist (Sie können es unter *Administration > System > Certificates > Certificate Authority > Certificates Templates (Administration > System > Zertifikate > Zertifizierungsstelle > Zertifikatsvorlagen)* überprüfen:

The screenshot displays the 'Edit Certificate Template' configuration page in the Cisco Identity Services Engine (ISE) web interface. The breadcrumb navigation path is: Administration > System > Certificates > Certificate Authority > Certificates Templates. The left sidebar shows the navigation menu with 'External CA Settings' selected. The main configuration area includes 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, External\_SCEP

## Referenzen

1. [Microsoft TechNet-Zonenartikel](#)
2. [Cisco ISE-Konfigurationsleitfäden](#)