

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

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Problema](#)

[Solução](#)

1. [Identifique chaves privadas velhas](#)
2. [Suprima de chaves privadas velhas](#)
3. [Suprima de certificados velhos MSCEP-RA](#)
4. [Gerencia Certificados novos para o SCEP](#)
  - 4.1. [Gerencia o certificado do registro da troca](#)
  - 4.2. [Gerencia o certificado da criptografia CEP](#)
5. [Verificar](#)
6. [Reinicie o IIS](#)
7. [Crie o perfil novo SCEP RA](#)
8. [Altere o molde de certificado](#)

[Referências](#)

## 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 active directory 2012.

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico da configuração do microsoft active directory
- Conhecimento básico da chave pública Infrastructure (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 active 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 administrador ativo Directory/CA.

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

Certificados iniciais SCEP visíveis no 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 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

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

## Solução

**Caution:** Todas as mudanças em Windows Server devem ser consultadas com seu administrador primeiramente.

## 1. Identifique chaves privadas velhas

Encontre chaves do private 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
```

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. Suprima de certificados velhos MSCEP-RA

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

*O > Add MMC > de arquivo/remove Pressão-em... > Add "Certificates" > conta > computador local do computador*

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. 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
```

**Tip:** Se você copia este molde do arquivo, certifique-se ajustá-lo conforme suas exigências e

verificar se todos os caracteres 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
```

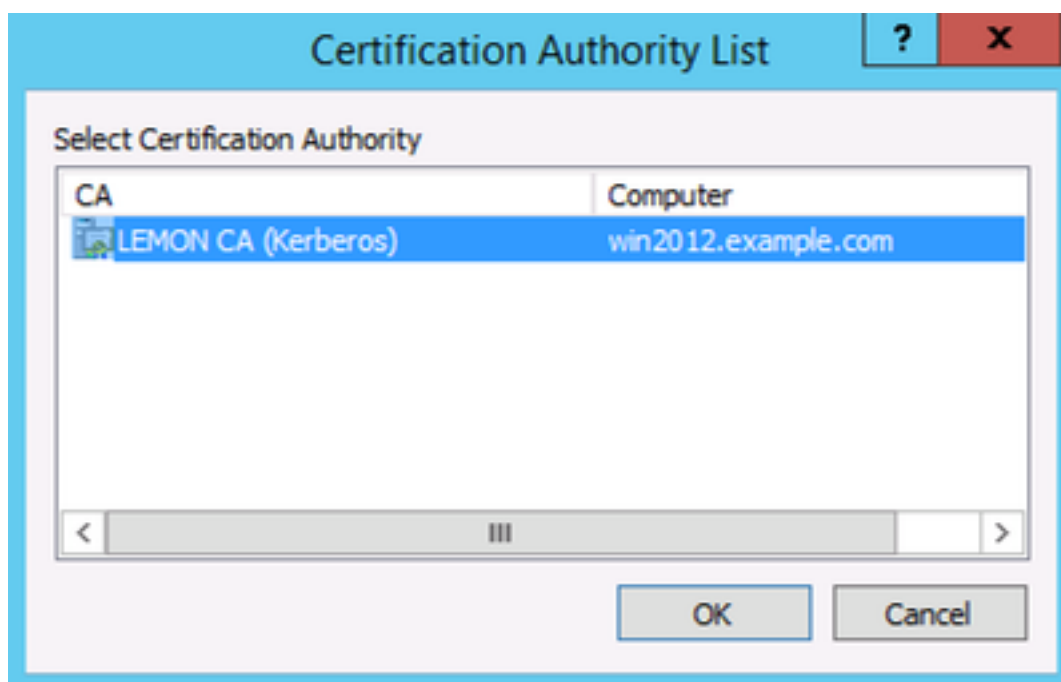
Se o usuário de advertência do diálogo **molde do contexto** que opõe ao contexto da máquina estala acima, clica a APROVAÇÃO. Este aviso pode ser ignorado.

```
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:

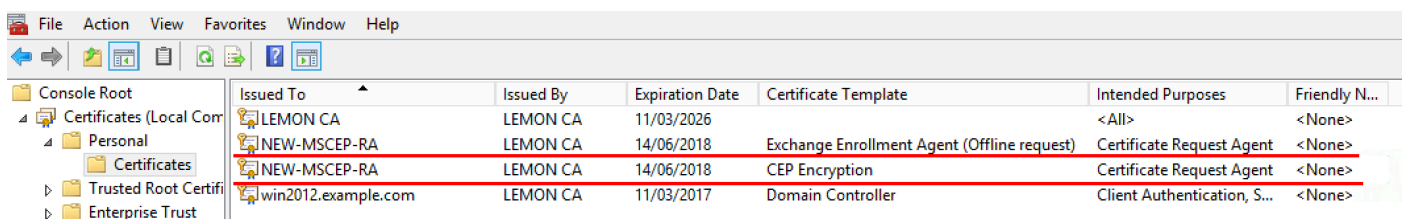
```
certreq -submit cisco_ndes_xchg.req cisco_ndes_xchg.cer
```

### 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:



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>

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:

## 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. 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*):

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)

The SCEP RA Profile dropdown menu is open, showing the following options: ISE Internal CA, New\_External\_Scep, and External\_SCEP.

## Referências

1. [Artigo da zona de Microsoft Technet](#)
2. [Manuais de configuração de Cisco ISE](#)