

# ISE の BYOD に使用する Windows サーバ AD 2012 の SCEP RA 証明書を更新する

## 目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[問題](#)

[解決策](#)

1. [古い秘密キーの特定](#)
2. [古い秘密キーの削除](#)
3. [古い MSCEP-RA 証明書の削除](#)
4. [SCEP の新しい証明書の生成](#)
  - 4.1. [Exchange 登録証明書を生成する](#)
  - 4.2. [CEP 暗号化証明書を生成する](#)
5. [確認](#)
6. [IIS の再起動](#)
7. [新しい SCEP RA プロファイルの作成](#)
8. [証明書テンプレートの変更](#)

[参考資料](#)

## 概要

このドキュメントでは、Simple Certificate Enrollment Protocol ( SCEP ) で使用される 2 つの証明書 ( Microsoft Active Directory 2012 の Exchange 登録エージェント証明書と CEP 暗号化証明書 ) を更新する方法について説明します。

## 前提条件

### 要件

次の項目に関する知識が推奨されます。

- Microsoft Active Directory の設定に関する基本的な知識
- Public Key Infrastructure ( PKI ) に関する基本的な知識
- Identity Services Engine ( ISE ) の基礎知識

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco Identity Services Engine バージョン 2.0

- Microsoft Active Directory 2012 R2

## 問題

Cisco ISE では、SCEP プロトコルを使用して、個人用デバイス登録 ( BYOD オンボード ) をサポートしています。外部 SCEP CA を使用する場合、この CA は、ISE の SCEP RA プロファイルによって定義されます。SCEP RA のプロファイルが作成されると、次の 2 つの証明書が信頼できる証明書ストアに自動的に追加されます。

- CA ルート証明書
- CA によって署名される RA ( 登録局 ) 証明書

RA は、登録するデバイスからのリクエストを受信して検証し、クライアント証明書を発行する CA にそのリクエストを転送する必要があります。

RA 証明書が期限切れになると、CA 側 ( この例では Windows Server 2012 ) でその証明書が自動的に更新されません。Active Directory/CA 管理者が証明書を手動で更新する必要があります。

次の例では、Windows Server 2012 R2 で証明書を更新する方法を示しています。

ISE に表示されている初期 SCEP 証明書。

### 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>

MSCEP-RA 証明書が期限切れになっているため、この証明書を更新する必要があることを前提としています。

## 解決策

注意：Windows サーバへの変更については、最初に Windows サーバの管理者に問い合わせてください。

## 1. 古い秘密キーの特定

certutil ツールを使用して、RA に関連付けられている秘密キーを見つけます。次に、Key Container を見つけます。

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

初期 MSCEP-RA 証明書の名前が異なっている場合、その名前をこのリクエストで調整する必要がありますことに注意してください。ただし、名前には、デフォルトでコンピュータ名が含まれている必要があります。

```
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. 古い秘密キーの削除

次のフォルダから参照キーを手動で削除します。

```
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. 古い MSCEP-RA 証明書の削除

秘密キーを削除した後、MMC コンソールから MSCEP-RA 証明書を削除します。

[MMC] > [File] > [Add/Remove Snap-in...] > [Add "Certificates"] > [Computer account] > [Local computer]

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. SCEP の新しい証明書の生成

#### 4.1. Exchange 登録証明書を生成する

4.1.1. 以下のコンテンツを使用してファイル `cisco_ndes_sign.inf` を作成します。この情報は `certreq.exe` ツールによって後で使用され、証明書署名要求 (CSR) が生成されます。

```
[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
```

ヒント：このファイルテンプレートをコピーする場合は、要件に応じてテンプレートを調

整し、すべての文字（引用符を含む）が適切にコピーされていることを確認してください。

4.1.2. 次のコマンドを使用して、.INF ファイルに基づいて CSR を作成します。

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

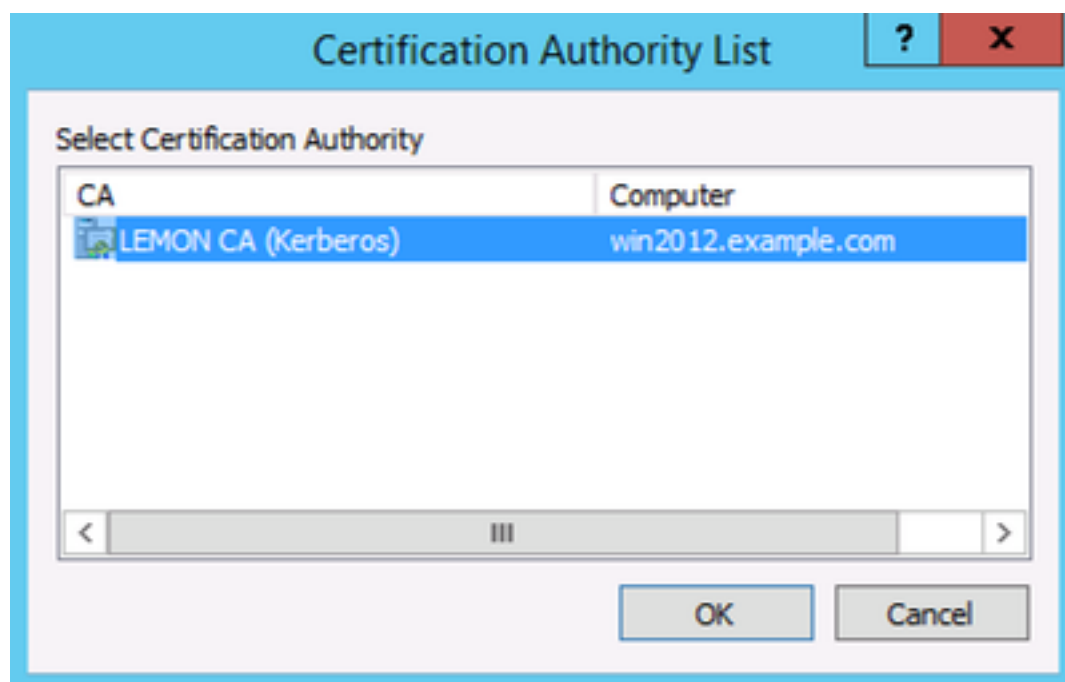
警告ダイアログ [User context template conflicts with machine context] がポップアップした場合は、[OK] をクリックします。この警告は無視できます。

```
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. 次のコマンドを使用して、CSR を送信します。

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

この手順の際にウィンドウがポップアップするので、適切な CA を選択する必要があります。



```
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. 前の手順で発行された証明書を受け入れます。このコマンドの結果、新しい証明書がインポートされて、ローカルコンピュータの個人用ストアに移されます。

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

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

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

## 4.2. CEP 暗号化証明書を生成する

### 4.2.1. 新しいファイル `cisco_ndes_xchg.inf` を作成します。

```
[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
```

### 4.1. で説明した同じ手順を実行します。

### 4.2.2. 新しい `.INF` ファイルに基づいて CSR を生成します。

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

### 4.2.3. リクエストを送信します。

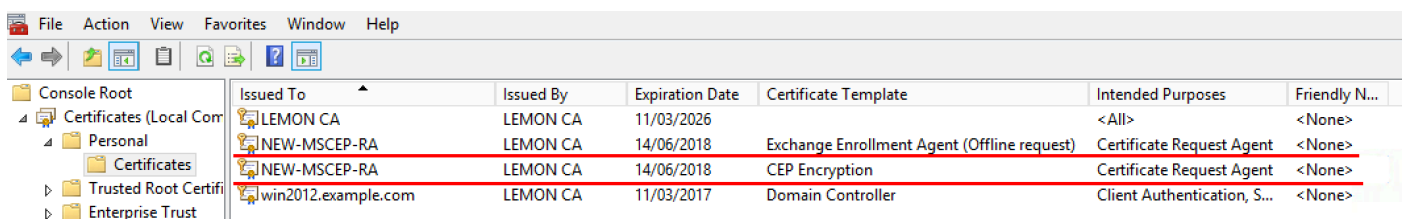
```
certreq -submit cisco_ndes_xchg.req cisco_ndes_xchg.cer
```

### 4.2.4. 新しい証明書をローカル コンピュータの個人用ストアに移動して、この証明書を受け入れます。

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

## 5. 確認

手順 4 が完了すると、ローカル コンピュータの個人用ストアに 2 つの新しい MSCEP-RA 証明書が表示されます。



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` ツールを使用して、証明書を確認することもできます (新しい証明書の正しい名前を使用する必要があります)。新しい共通名とシリアル番号が付いた MSCEP-RA 証明書が表示さ

れるはずですが。

```
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. IIS の再起動

変更を適用するために、インターネット インフォメーション サービス (IIS) サーバを再起動します。

```
iisreset.exe
```

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

## 7. 新しい SCEP RA プロファイルの作成

ISE で、新しい SCEP RA プロファイルを作成し (古いサーバ URL と同じ URL を使用して)、新しい証明書をダウンロードして信頼できる証明書ストアに追加します。

## 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. 証明書テンプレートの変更

BYOD が使用する証明書テンプレートで新しい SCEP RA プロファイルが指定されていることを確認します ( [Administration] > [System] > [Certificates] > [Certificate Authority] > [Certificates Templates] を選択して確認できます ) 。

The screenshot displays the 'Edit Certificate Template' configuration page in the Cisco ISE Administration console. The breadcrumb navigation is: Administration > System > Certificates > Certificate Authority > Certificate Templates. The left-hand navigation pane shows 'Certificate Management' expanded to 'Certificate Authority', with 'External CA Settings' selected. The main content area is titled 'Edit Certificate Template' and 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:** A dropdown menu is open, showing the following options: ISE Internal CA, New\_External\_Scep (highlighted), and External\_SCEP.

## 参考資料

1. [Microsoft Technet ゾーンの記事](#)
2. [Cisco ISE 設定ガイド](#)