

Rinnova certificato SCEP RA in Windows Server AD 2012 utilizzato per BYOD in ISE

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Problema](#)

[Soluzione](#)

- [1. Identificare le vecchie chiavi private](#)
 - [2. Eliminare le vecchie chiavi private](#)
 - [3. Eliminare i certificati MSCEP-RA precedenti](#)
 - [4. Generare nuovi certificati per SCEP](#)
 - [4.1. Generare il certificato di registrazione di Exchange](#)
 - [4.2. Generare il certificato di crittografia CEP](#)
 - [5. Verifica](#)
 - [6. Riavviare IIS](#)
 - [7. Creare un nuovo profilo SCEP RA](#)
 - [8. Modifica modello di certificato](#)
- [Riferimenti](#)

Introduzione

In questo documento viene descritto come rinnovare due certificati utilizzati per SCEP (Simple Certificate Enrollment Protocol): Agente di registrazione di Exchange e certificato di crittografia CEP in Microsoft Active Directory 2012.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base della configurazione di Microsoft Active Directory
- Conoscenze base di PKI (Public Key Infrastructure)
- Conoscenze base di Identity Services Engine (ISE)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Problema

Cisco ISE utilizza il protocollo SCEP per supportare la registrazione del dispositivo personale (onboarding BYOD). Quando si utilizza una CA SCEP esterna, questa CA è definita da un profilo RA SCEP su ISE. Quando si crea un profilo SCEP RA, vengono aggiunti automaticamente due certificati all'archivio dei certificati attendibili:

- certificato radice CA,
- Certificato RA (Registration Authority) firmato dalla CA.

L'Autorità registrazione è responsabile della ricezione e della convalida della richiesta dal dispositivo di registrazione e dell'inoltro alla CA che rilascia il certificato client.

Alla scadenza, il certificato di Autorità registrazione non viene rinnovato automaticamente dal lato CA (in questo esempio, Windows Server 2012). Questa operazione deve essere eseguita manualmente dall'amministratore di Active Directory/CA.

Di seguito è riportato l'esempio di come eseguire questa operazione in Windows Server 2012 R2.

Certificati SCEP iniziali visibili su 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

Si presume che il CERTIFICATO MSCEP-RA sia scaduto e debba essere rinnovato.

Soluzione

Attenzione: Qualsiasi modifica apportata a Windows Server deve essere prima consultata

con l'amministratore.

1. Identificare le vecchie chiavi private

Trovare le chiavi private associate ai certificati di Autorità registrazione in Active Directory utilizzando lo strumento **certutil**. Quindi individuare il **contenitore di chiavi**.

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

Se il nome del certificato MSCEP-RA iniziale è diverso, è necessario modificarlo nella richiesta. Per impostazione predefinita, tuttavia, deve contenere il nome del computer.

```
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. Eliminare le vecchie chiavi private

Eliminare manualmente le chiavi di riferimento dalla cartella seguente:

```
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. Eliminare i certificati MSCEP-RA precedenti

Dopo aver eliminato le chiavi private, rimuovere i certificati MSCEP-RA dalla console MMC.

MMC > File > Aggiungi/Rimuovi snap-in... > Aggiungi "Certificati" > Account computer > Computer locale

| 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. Generare nuovi certificati per SCEP

4.1. Generare il certificato di registrazione di Exchange

4.1.1. Creare un file `cisco_ndes_sign.inf` con il contenuto seguente. Queste informazioni vengono utilizzate in seguito dallo strumento `certreq.exe` per generare la richiesta di firma del certificato (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
```

Suggerimento: Se si copia il modello di file, adattarlo in base alle proprie esigenze e verificare che tutti i caratteri siano stati copiati correttamente, incluse le virgolette.

4.1.2. Creare CSR basato sul file INF con questo comando:

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

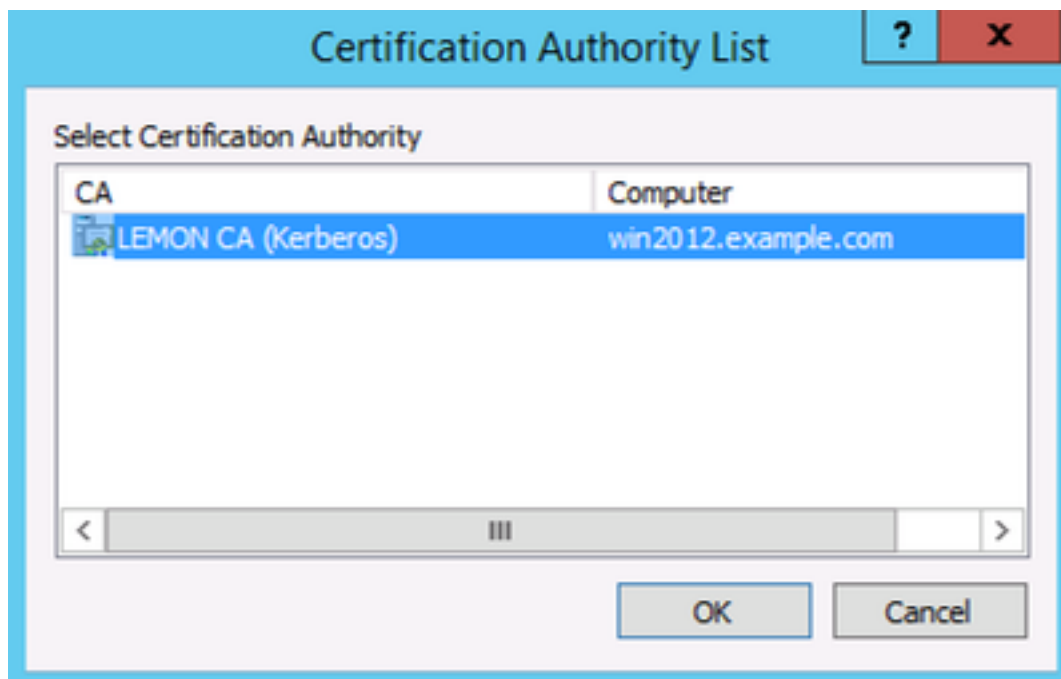
Se viene visualizzata la finestra di dialogo di avviso **Modello di contesto utente in conflitto con il contesto del computer**, fare clic su OK. Questo avviso può essere ignorato.

```
C:\Users\Administrator\Desktop>certreq -f -new cisco_ndes_sign.inf cisco_ndes_sign.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. Inviare il CSR con questo comando:

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

Durante questa procedura viene visualizzata una finestra ed è necessario scegliere la CA appropriata.



```
C:\Users\Administrator\Desktop>certreq -submit cisco_ndes_sign.req cisco_ndes_sign.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 Accettare il certificato rilasciato nella fase precedente. Come risultato di questo comando, il

nuovo certificato viene importato e spostato nell'archivio personale del computer locale:

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

4.2. Generare il certificato di crittografia CEP

4.2.1. Creare un nuovo file `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
```

Seguire la procedura descritta al punto 4.1.

4.2.2. Generare un CSR basato sul nuovo file INF:

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

4.2.3. Presentare la richiesta:

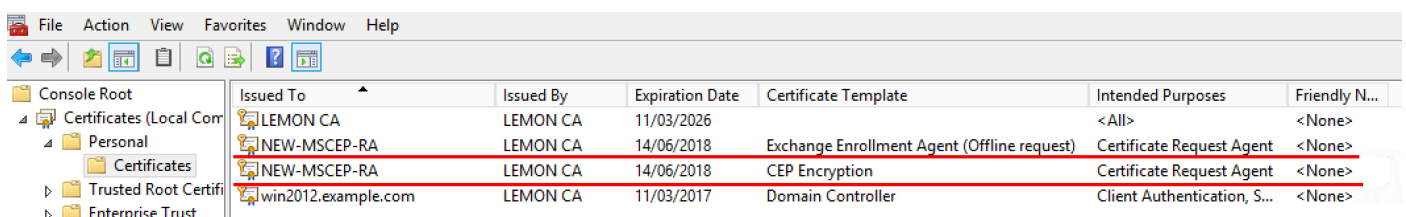
```
certreq -submit cisco_ndes_xchg.req cisco_ndes_xchg.cer
```

4.2.4 : Accettare il nuovo certificato spostandolo nell'archivio personale del computer locale:

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

5. Verifica

Dopo aver completato il passaggio 4, nell'archivio personale del computer locale verranno visualizzati due nuovi certificati MSCEP-RA:



| 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> |

È inoltre possibile verificare i certificati con lo strumento **certutil.exe** (assicurarsi di utilizzare il

nuovo nome del certificato corretto). I certificati MSCEP-RA con nuovi nomi comuni e nuovi numeri di serie devono essere visualizzati:

```
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. Riavviare IIS

Riavviare il server Internet Information Services (IIS) per applicare le modifiche:

```
iisreset.exe
```

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

7. Creare un nuovo profilo SCEP RA

Ad ISE creare un nuovo profilo SCEP RA (con lo stesso URL del server del precedente), in modo che i nuovi certificati vengano scaricati e aggiunti all'archivio dei certificati attendibili:

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. Modifica modello di certificato

Assicurarsi che il nuovo profilo SCEP RA sia specificato nel modello di certificato utilizzato da BYOD (è possibile selezionare *Amministrazione > Sistema > Certificati > Autorità di certificazione > Modelli di certificato*):

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 is part of the 'Certificates' section under 'Administration'. The left sidebar shows the navigation menu with 'Certificate Management' expanded to 'Certificate Authority' and 'External CA Settings' selected. 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 (dropdown menu is open, showing options: ISE Internal CA, New_External_Scep, External_SCEP)

Riferimenti

1. [Articolo su Microsoft Technet zone](#)
2. [Guide alla configurazione di Cisco ISE](#)