

Windows Server 2012 AD ىل ع SCEP RA ةداهش دي دجت ISE ىل ع BYOD ل ةمدختس مل AD 2012

تاىوت حمل

[ةمدقملا](#)

[ةيساسأل تابلطت مل](#)

[تابلطت مل](#)

[ةمدختس مل تانوك مل](#)

[ةلكش مل](#)

[لحل](#)

[1. ةميدقلا ةصاخلا حيتاف مل دي دجت](#)

[2. ةميدقلا ةصاخلا حيتاف مل فذح](#)

[3. ةميدقلا MSCEP-RA تاناي ب فذح](#)

[4. SCEP ل ةدي دجت تاداهش عاشنا](#)

[4.1. Exchange ليجست ةداهش عاشنا](#)

[4.2. CEP ريفشت ةداهش عاشنا](#)

[5. ةحصللا نم ققحتلا](#)

[6. IIS ليجشت ةداعا](#)

[7. دي دجت SCEP RA فيرعت فلم عاشنا](#)

[8. ةداهشلا بلاق ليدعت](#)

[عجار مل](#)

ةمدقملا

ةداهشلا ليجست لوكوتور بل امه مادختسإ متي ني تدهاش دي دجت ةيفيك دن تس مل اذه حضوي
Microsoft Active Directory 2012 ىل ع CEP ريفشت ةداهش و Exchange ليجست ليمع (SCEP) طيس بل
Directory 2012.

ةيساسأل تابلطت مل

تابلطت مل

ةيلاتل عيضاوملاب ةفرعم كي دل نوكت نأ Cisco ىصوت

- Microsoft Active Directory نيوكت ب ةيساسأل ةفرعم
- (PKI) ماعلا حاتف مل ةيساسأل ةينبلاب ةيساسأل ةفرعم
- (ISE) ةيوهلا تامدخ كرحمل ةيساسأل ةفرعم

ةمدختس مل تانوك مل

ةيلاتل ةيدامل تانوك مل او جمار بل تارادصلإ ل دن تس مل اذه في ةدراول تامولعمل دن تس

- Cisco Identity Services Engine، 2.0 رادصلإ

- Microsoft Active Directory 2012 R2

ةل كشملا

دنع (BYOD مض) يصخشلا زاهلا ليجست معدل SCEP لوكوتورب Cisco ISE مدختسي فيرعت فلم ةطساوب قدصملا عجرملا اذه فيرعت متي، يجراخ SCEP قدصم عجرم مادختسا نزم يلا ائاقولت ني تدهاش ةفاضلا متت، SCEP RA في صوت ءاشن دنع. ISE يلع SCEP RA اهاب قوثلما تادهاشلا:

- قدصملا عجرملا رذج ةدهاش،
- ليجستلا حلصم لبق نم هعقوملا (ليجستلا حلصم) هدهاش.

ههيجوت ةداعاو، ليجستلا زاه نم هتحص نم ققحتلاو بلطلا مالتسا نع ال وئسم RA نوكي لي عمل ةدهاش ردصي يذلا CA يلا.

CA (Windows Server 2012) بناج يلع ائاقولت اهديجت متي ال، RA ةدهاش ةيحلصم ءاهتنا دنع Active Directory/CA لوؤسم ةطساوب ايودي كلذ متي نا بجي. (لاثلما اذه في

Windows Server 2012 R2 ليغشلتا ماظن يلع كلذ قيقحت ةيفيكي يلاتلا لاثملا كيلا.

ISE يلع ةيئرمل ةيولوال SCEP تادهاش:

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 0A

Validity From Tue, 14 Jun 2016 11:46:03 CEST

Validity To Thu, 14 Jun 2018 11:46:03 CEST

اهديجت بجيو ةيحلصملا ةيهرنم MSCEP-RA ةدهاش نا ضررت في.

لحللا

Windows Server يلع ارطت تاريخيغت ي لول الو لوؤسملا ةراشتسا بجي: ريذحت

1. عميدقلا ؤصاخلا حيتافملا ديحت

دعب certutil. اءا مءءءسءاب Active Directory على RA ءاءاءشءب ؤنرءقم ؤصاخ حيتافم نع ءءءبلا حيتافملا ؤيواء ؤقوم دءء كلء

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

اذه يف اهليءءء بءءي فء، افءءءم ؤيولوالا MSCEP-RA ؤءاءش مءسا ناءا اءءا هنأ ؤءءءالم يءءري رءوي بمكل مءسا على يءءارءءا لءكشءب يوءءءي نأ بءءي ءءء عم وبللءا

```
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. عميدقلا ؤصاخلا حيتافملا فءء

هانءا ءءءءالم نم ايوي ؤءءءءا حيتافم فءء:

```
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. عمى دقل ال MSCEP-RA تاناىب فذح

MMC م كحت ةدحو نم MSCEP-RA تاناىب ةلازاب مق ،ةصاخلا حىتافملا فذح دعب

MMC > رتوىبمكل باسح > "رداصم" ةفاضا | > ...ةفاضا ةاذا ةلازا/ةفاضا | > فلم > رتوىبمكل باسح

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

4. ل SCEP ةديدج تاداهش عاشن |

4.1. Exchange لىجست ةداهش عاشن |

تامولعمل هذه مادختسا متي .هاندا يوتحمل اب Cisco_ndes_sign.inf فلم عاشن اب مق . 4.1.1. (CSR) ةداهشال عىقوت بلط عاشن ال certreq.exe ةادا ةطساوب اقحال

```
[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
```

نم ققحتو كتابلطتم بسح هطبض نم دكات ،اذه فلملا بلاق خسنب تمق اذا: حىملت

(سابتقالا تامالع كلذيف امب) حيحص لكش ب فورحلال لك حسن.

4.1.2. رمألا اذه مادختساب .inf فلم ىل اذانتسا CSR عاشناب مق:

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

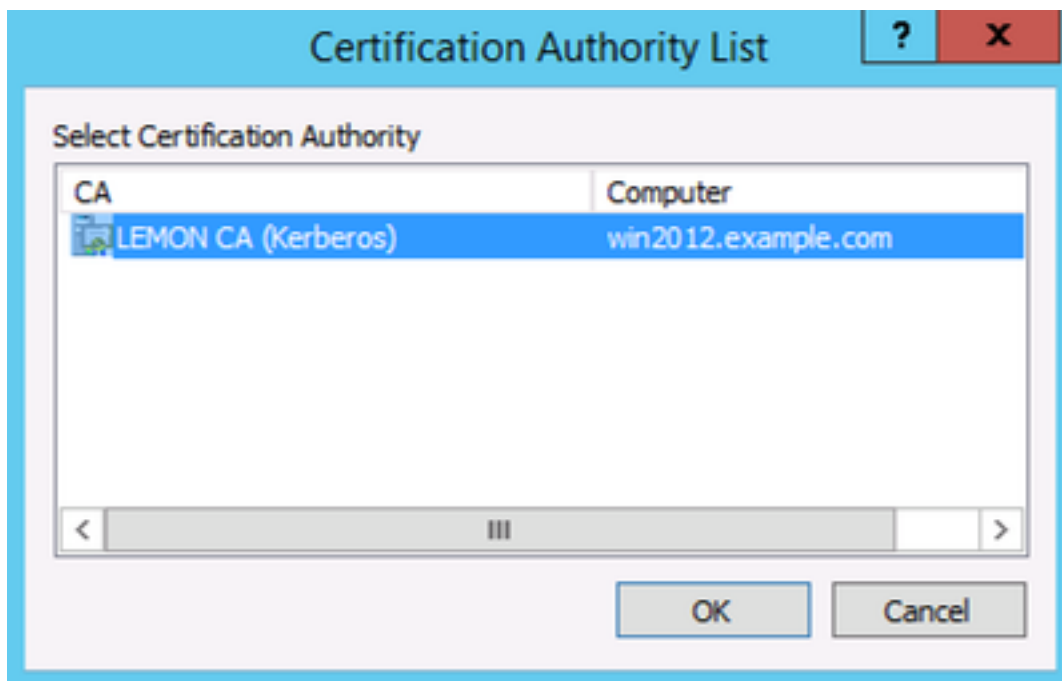
قوف رقنا، ريذحتلا راوح عبرم يف زاهجلا قايس ليغشت عم مدختسملا قايس بللق ضراعت اذ ا ريذحتلا اذه لهاجت نكمي. قفاوم.

```
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. رمألا اذه مادختساب CSR لاسرا:

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

بسانملا قدصملا عجرملا رايتخا بجوتيو ةذفان رهظت، عارجلا اذه لالخ.



```
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>
```

ءءاهشلا ءاريتسا متي، رمألا اذهل ءجيتن. ءق باسلا ءوطخل يف ءرداصل ءءاهشلا لوبق 4-1-4
يف لحمل رتوي بمكلل يصخشلا نزلحمل ىل اهللقنو ءءءءل

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

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

4.2. ريفشت ةداهش عاشن | CEP

4.2.1. Cisco_ndes_xchg.inf دي دج فلم عاشن اب مق

```
[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. ف ة حضوم ال اهسفن تاوطلخ ال عبتا

4.2.2. دي دج ال .inf فلم ال ادان ت سا CSR عاشن اب مق

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

4-2-3- ب لطل م يدقت:

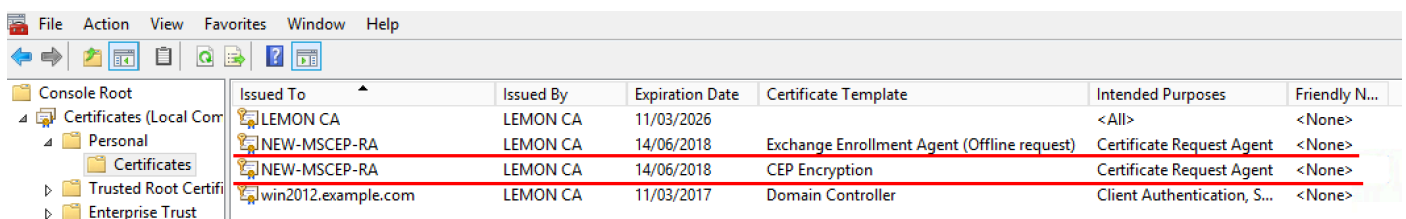
```
certreq -submit cisco_ndes_xchg.req cisco_ndes_xchg.cer
```

4-2-4: ي ل حمل ال رت وي ب م كل ال نزخم ال ال اهل قنب ة دي دج ال ةداهش ال لوبق:

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

5. ة حصل ال نم ق قحت ال

ي صخش ال رت وي ب م كل ال نزخم " ف ن ا ت دي دج MSCEP-RA ت داهش رهظت س ، 4 ة وطلخ ال ل امك دع ب "ي ل حمل ال":



| 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> |

ةداهش ال م سا م ادخت سا (نم دكأت) **certutil.exe** ةادأ م ادخت سا ب ت اداهش ال نم ق قحت ال اضيأ كنك مي م ا ق ر أو ة دي دج ة ماع عام س ال ل ع ي وحت ي ت ال MSCEP-RA ت اداهش ضرع ب جي . (ح ي حصل ال دي دج ال ة دي دج ة ي ل س ل س ت

```
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. ليغشت ةداع | IIS

تاريغيغتل قيبطتل (IIS) تترت نإلا تامولعم تامدخ مداخ ليغشت ةداع اب مق

```
iisreset.exe
```

```
C:\Users\Administrator\Desktop>iisreset.exe
```

```
Attempting stop...
```

```
Internet services successfully stopped
```

```
Attempting start...
```

```
Internet services successfully restarted
```

7. ديچ SCEP RA فيرعت فلم عاشن |

ثيحب، (ميدقلا لثم مداخللا طبر ناووع سفن عم) ديچ SCEP RA فيصوت ءيشنأ ISE ىل ع
اهب قوئوملا تاداهشلا نزم ىل اهتفاض او ةديجل تاداهشلا ليزنت متي

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. ةداهشلا بلق ليدعت

BYOD لبق نم مدختسملا ةداهشلا بلق يف ديدجل SCEP RA فيرت فلم ديدحت نم دكأت (تاداهشلا بلق > قدصملا عجرملا > تاداهشلا > ماظنلا > ةرادلا يف هت عجرم كنكمي):

Edit Certificate Template

* 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, ISE Internal CA, New_External_Scep, External_SCEP

عجرملا

1. [Microsoft TechNet Zone](#) ةلاقم

2. [Cisco ISE](#) نيوكت ةلدا

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا ذه Cisco ت مچرت
م ل ا ل اء ان ا ع مچ ي ف ن م دخت س م ل ل م عد و ت م م م دقت ل ة يرش ب ل و
امك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ال م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت م م مچرت م ا م د ق ي ي ت ل ا ة ي ف ا ر ت ح ال ا ة مچرت ل ا م ل ا ح ل ا و ه
ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا هذه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا