

مادخات ساب Cisco VPN Client و PIX ني ب IPsec Smartcard تاداهش ني وكت لاثم

المحتويات

[المقدمة](#)

[المتطلبات الأساسية](#)

[المتطلبات](#)

[المكونات المستخدمة](#)

[الاصطلاحات](#)

[تسجيل PIX وتكوينه](#)

[التكوينات](#)

[تسجيل شهادات عميل شبكة VPN من Cisco](#)

[تكوين عميل Cisco VPN لاستخدام الشهادة للاتصال ب PIX](#)

[تثبيت برامج تشغيل البطاقة الذكية من eToken](#)

[التحقق من الصحة](#)

[استكشاف الأخطاء وإصلاحها](#)

[معلومات ذات صلة](#)

المقدمة

يوضح هذا المستند كيفية تكوين نفق IPsec VPN بين جدار حماية PIX وعميل Cisco VPN 4.0.x. كما يسلط مثال التكوين في هذا المستند الضوء على إجراء تسجيل مرجع التصديق (CA) لكل من موجه Cisco IOS و عميل Cisco VPN، بالإضافة إلى استخدام البطاقة الذكية كتخزين شهادات.

ارجع إلى تكوين IPsec بين موجهات Cisco IOS وعميل Cisco VPN باستخدام شهادات Entrust لمعرفة المزيد حول تكوين IPsec بين موجهات Cisco IOS وعميل Cisco VPN باستخدام شهادات Entrust.

ارجع إلى تكوين هيئات شهادات الهوية المتعددة على موجهات Cisco IOS لمعرفة المزيد حول تكوين هيئات شهادات الهوية المتعددة على موجهات Cisco IOS.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- جدار حماية Cisco PIX الذي يشغل البرنامج الإصدار 6.3(3)

- Cisco VPN Client 4.0.3 على كمبيوتر يعمل بنظام التشغيل Windows XP
 - يستخدم خادم Microsoft Windows 2000 CA في هذا المستند كخادم CA.
 - يتم تخزين الشهادات الموجودة على عميل Cisco VPN باستخدام البطاقة الذكية e-Token [Aladdin](#).
- تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، ارجع إلى [اصطلاحات تلميحات Cisco التقنية](#).

تسجيل PIX وتكوينه

في هذا القسم، تقدم لك المعلومات لتكوين الميزات الموضحة في هذا المستند.

ملاحظة: للعثور على معلومات إضافية حول الأوامر المستخدمة في هذا المستند، استخدم [أداة بحث الأوامر \(للمعلماء المسجلين فقط\)](#).

التكوينات

يستخدم هذا المستند هذه التكوينات.

- [تسجيل الشهادة على جدار حماية PIX](#)
- [تكوين جدار حماية PIX](#)

تسجيل الشهادة على جدار حماية PIX

```

Define a hostname and domain name for the router. ---!
!--- The fully qualified domain name (FQDN) is used !---
      as the identity of the router during certificate
      enrollment. pix(config)#hostname sv2-11
      sv2-11(config)#domain-name cisco.com
Confirm that you have the correct time set on the ---!
      PIX. show clock
      clock set

This command clears the PIX RSA keys. ca zeroize ---!
      rsa
Generate RSA (encryption and authentication) keys. ---!
      ca gen rsa key
Select the modulus size (512 or 1024). !--- Confirm ---!
      the keys generated. show ca mypub rsa
Define the CA identity. ca ident kobe ---!
      10.1.1.2:/certsrv/mscep/mscep.dll
      ca conf kobe ra 1 20 crlopt
      ca auth kobe
[ca enroll kobe [ipaddress
Confirm the certificate and validity. show ca cert ---!

```

تكوين جدار حماية PIX

```

(PIX Version 6.3(3
    interface ethernet0 auto
    interface ethernet1 auto
    interface ethernet2 auto shutdown
    interface ethernet3 auto shutdown
    interface ethernet4 auto shutdown
    interface ethernet5 auto shutdown
    nameif ethernet0 outside security0
    nameif ethernet1 inside security100
    nameif ethernet2 intf2 security4
    nameif ethernet3 intf3 security6
    nameif ethernet4 intf4 security8
    nameif ethernet5 intf5 security10
    enable password 8Ry2YjIyt7RRXU24 encrypted
    passwd 2KFQnbNIdI.2KYOU encrypted
    hostname sv2-11
    domain-name cisco.com
    fixup protocol dns maximum-length 512
    fixup protocol ftp 21
    fixup protocol h323 h225 1720
    fixup protocol h323 ras 1718-1719
    fixup protocol http 80
    fixup protocol rsh 514
    fixup protocol rtsp 554
    fixup protocol sip 5060
    fixup protocol sip udp 5060
    fixup protocol skinny 2000
    fixup protocol smtp 25
    fixup protocol sqlnet 1521
    fixup protocol tftp 69
    names
    access-list 101 permit tcp any host 209.165.201.21 eq
    www
    access-list 120 permit ip 10.1.1.0 255.255.255.0
    10.0.0.0 255.255.255.0
    pager lines 24
    mtu outside 1500
    mtu inside 1500
    mtu intf2 1500
    mtu intf3 1500
    mtu intf4 1500
    mtu intf5 1500
    ip address outside 209.165.201.20 255.255.255.224
    ip address inside 10.1.1.10 255.255.255.0
    ip address intf2 127.0.0.1 255.255.255.255
    no ip address intf3
    no ip address intf4
    no ip address intf5
    ip audit info action alarm
    ip audit attack action alarm
    ip local pool vpnpool 10.0.0.10-10.0.0.100
    no failover
    failover timeout 0:00:00
    failover poll 15
    no failover ip address outside
    no failover ip address inside
    no failover ip address intf2
    no failover ip address intf3
    no failover ip address intf4
    no failover ip address intf5
    pdm history enable

```

```

arp timeout 14400
nat (inside) 0 access-list 120
static (inside,outside) 209.165.201.21 10.1.1.2 netmask
255.255.255.255 0 0
access-group 101 in interface outside
route outside 0.0.0.0 0.0.0.0 209.165.201.30 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media
0:02:00
timeout uauth 0:05:00 absolute
+aaa-server TACACS+ protocol tacacs
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
crypto ipsec transform-set myset esp-3des esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap
crypto map mymap interface outside
isakmp enable outside
isakmp policy 10 authentication rsa-sig
isakmp policy 10 encryption 3des
isakmp policy 10 hash md5
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
vpngroup vpncert address-pool vpnpool
vpngroup vpncert idle-time 1800
***** vpngroup vpncert password
ca identity kobe 10.1.1.2:/certsrv/mscep/mscep.dll
ca configure kobe ra 1 20 crloptional
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:2ae252ac69e5218d13d35acdf1f30e55
end :
[OK]
#(sv2-11(config)



```

تسجيل شهادات عميل شبكة VPN من Cisco

تذكر تثبيت جميع برامج التشغيل والأدوات المساعدة اللازمة الواردة مع جهاز البطاقة الذكية على الكمبيوتر الشخصي المراد استخدامه مع عميل شبكة VPN من Cisco.

توضح هذه الخطوات الإجراءات المستخدمة لتسجيل عميل Cisco VPN لشهادات MS. يتم تخزين الشهادة على مخزن Aladdin e-Token Smartcard.

1. قم بتشغيل متصفح وانتقل إلى صفحة خادم الشهادات (<http://CAServeraddress/certsrv/>), في هذا المثال).
2. حدد طلب شهادة وانقر التالي.

Address  http://209.165.201.21/certsrv/  Go Lin

Microsoft Certificate Services -- kobe [Home](#)

Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

Select a task:

- Retrieve the CA certificate or certificate revocation list
- Request a certificate
- Check on a pending certificate

[Next >](#)

3. في نافذة إختيار نوع الطلب ، حدد طلب متقدم وانقر بعد ذلك.

Microsoft Certificate Services -- kobe [Home](#)

Choose Request Type

Please select the type of request you would like to make:

User certificate request:

Web Browser Certificate

E-Mail Protection Certificate

Advanced request

[Next >](#)

4. حدد إرسال طلب شهادة إلى المرجع المصدق هذا باستخدام نموذج وانقر بعد ذلك.

Advanced Certificate Requests

You can request a certificate for yourself, another user, or a computer using one of the following methods. Note that the policy of the certification authority (CA) will determine the certificates that you can obtain.

- Submit a certificate request to this CA using a form.
- Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file.
- Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station.
You must have an enrollment agent certificate to submit a request for another user.

[Next >](#)

5. املأ كل العناصر في نموذج طلب الشهادة المتقدمة. تأكد من أن القسم أو الوحدة التنظيمية (OU) تتوافق مع اسم مجموعة عملاء شبكة VPN من Cisco، كما تم تكوينها في اسم مجموعة PIX vpn. حدد موفر خدمة الشهادات الصحيح (CSP) المناسب للإعداد الخاص بك.

Advanced Certificate Request

Identifying Information:

Name:

E-Mail:

Company:

Department:

City:

State:

Country/Region:

Intended Purpose:

Key Options:

CSP:

Key Usage: Exchange Signature Both

Key Size: Min: 384 Max: 1024 (common key sizes: [512](#) [1024](#))

Create new key set

Set the container name

Use existing key set

Enable strong private key protection

Mark keys as exportable

Use local machine store

You must be an administrator to generate

Additional Options:

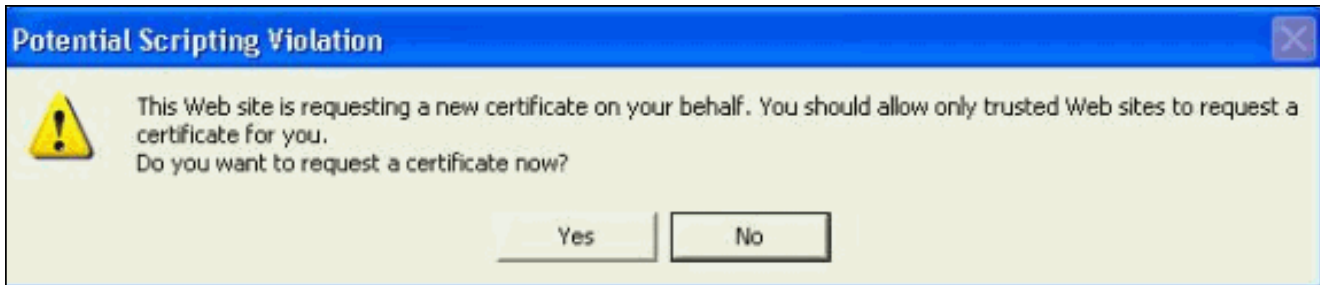
Hash Algorithm:

Only used to sign request.

Save request to a PKCS #10 file

Attributes:

6. حدد نعم لمتابعة التثبيت عند الحصول على تحذير التحقق من صحة البرامج النصية المحتملة.

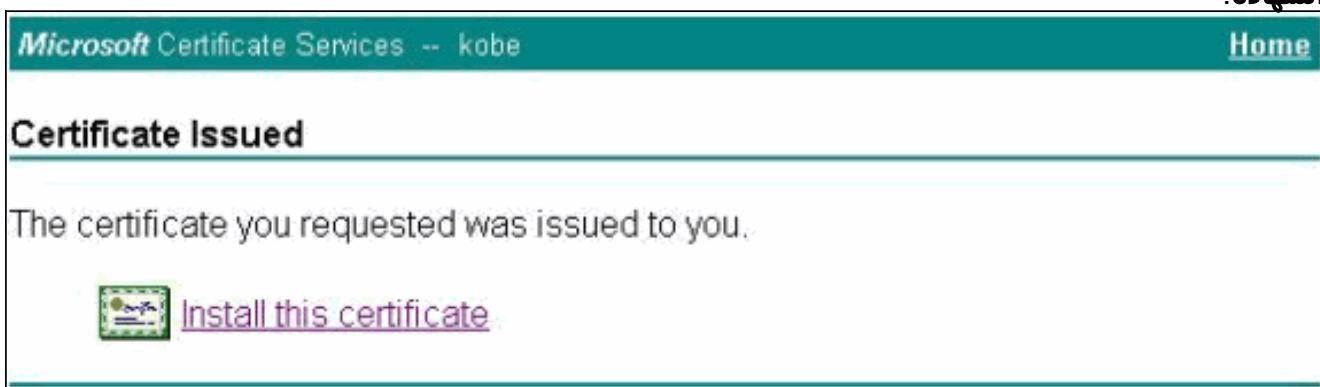


7. يقوم تسجيل الشهادة باستدعاء مخزن eToken. أدخل كلمة المرور وانقر فوق



موافق.

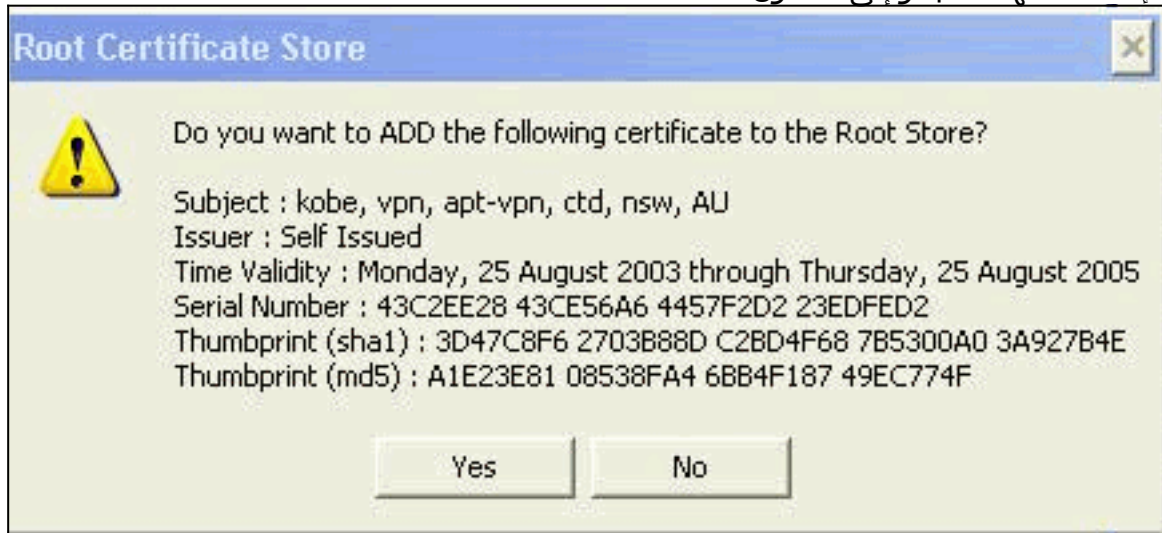
8. انقر على تثبيت هذه الشهادة.



9. حدد نعم لمتابعة التثبيت عند الحصول على تحذير التحقق من صحة البرامج النصية المحتملة.

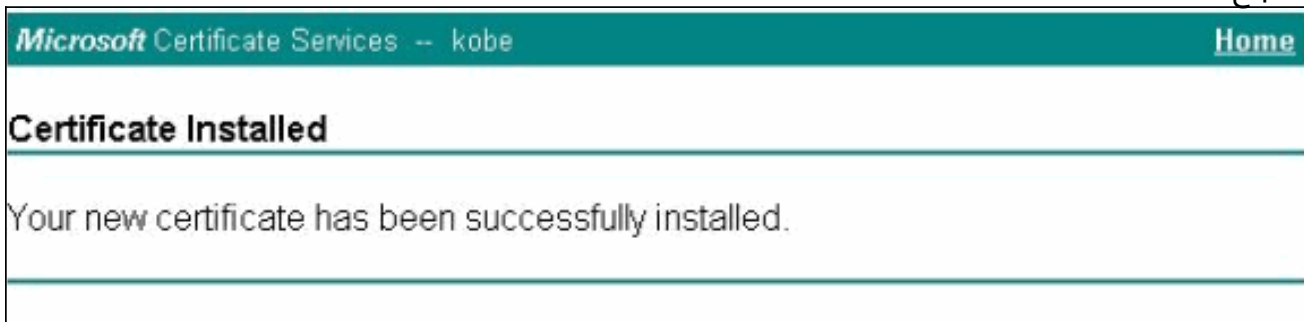


10. حدد نعم لإضافة الشهادة الجذر إلى المخزن

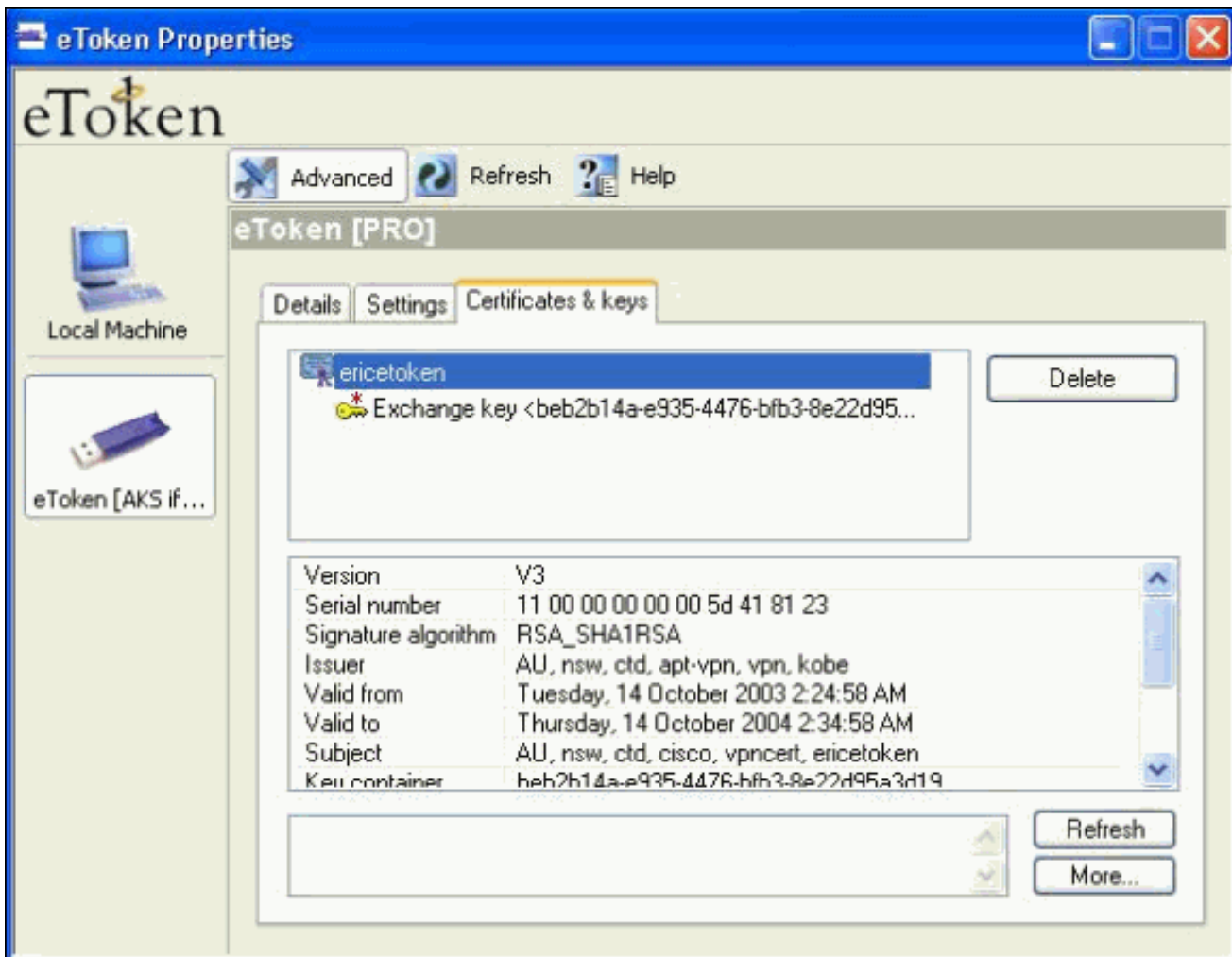


الجذري.

11. يظهر إطار الشهادة المثبتة ويؤكد التثبيت الناجح.



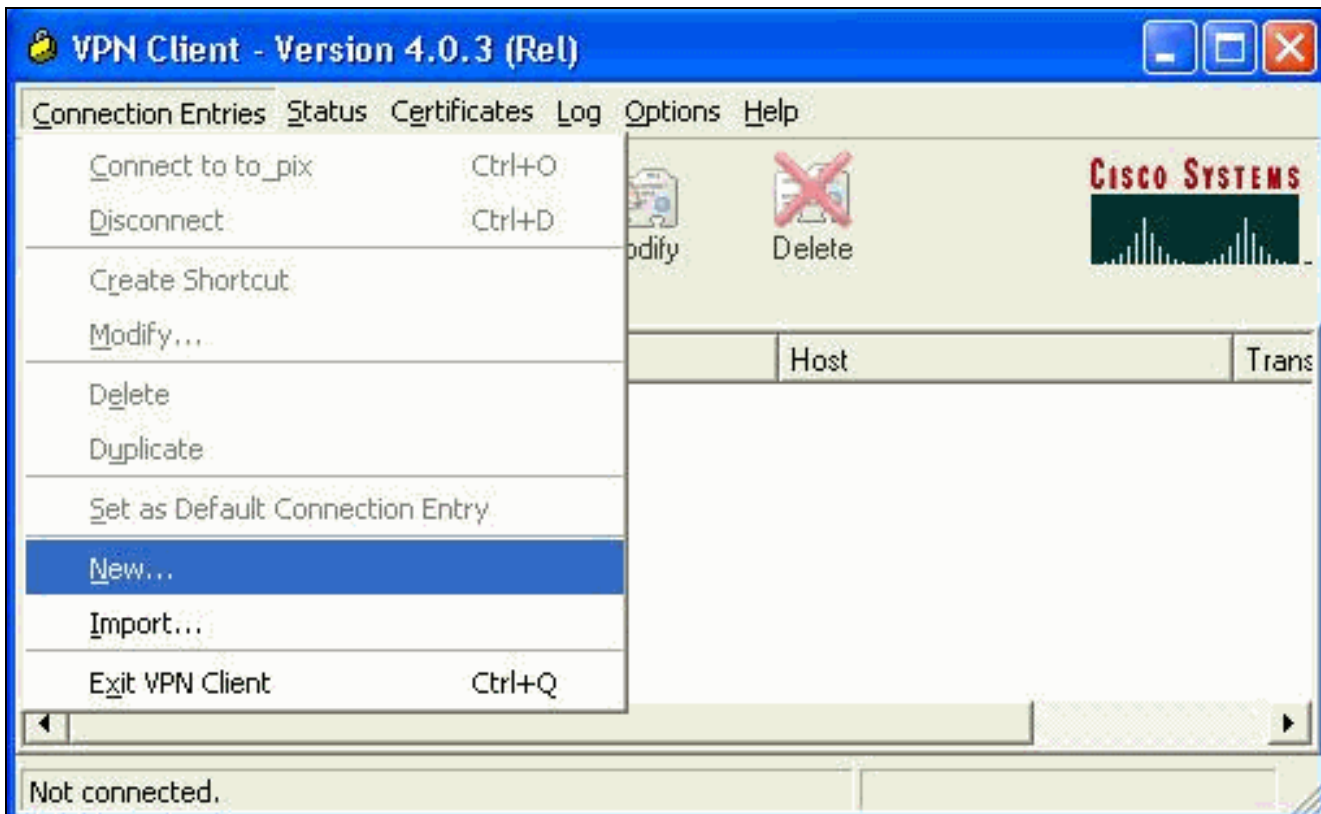
12. أستخدم عارض تطبيق الرمز المميز لعرض الشهادة المخزنة على البطاقة الذكية.



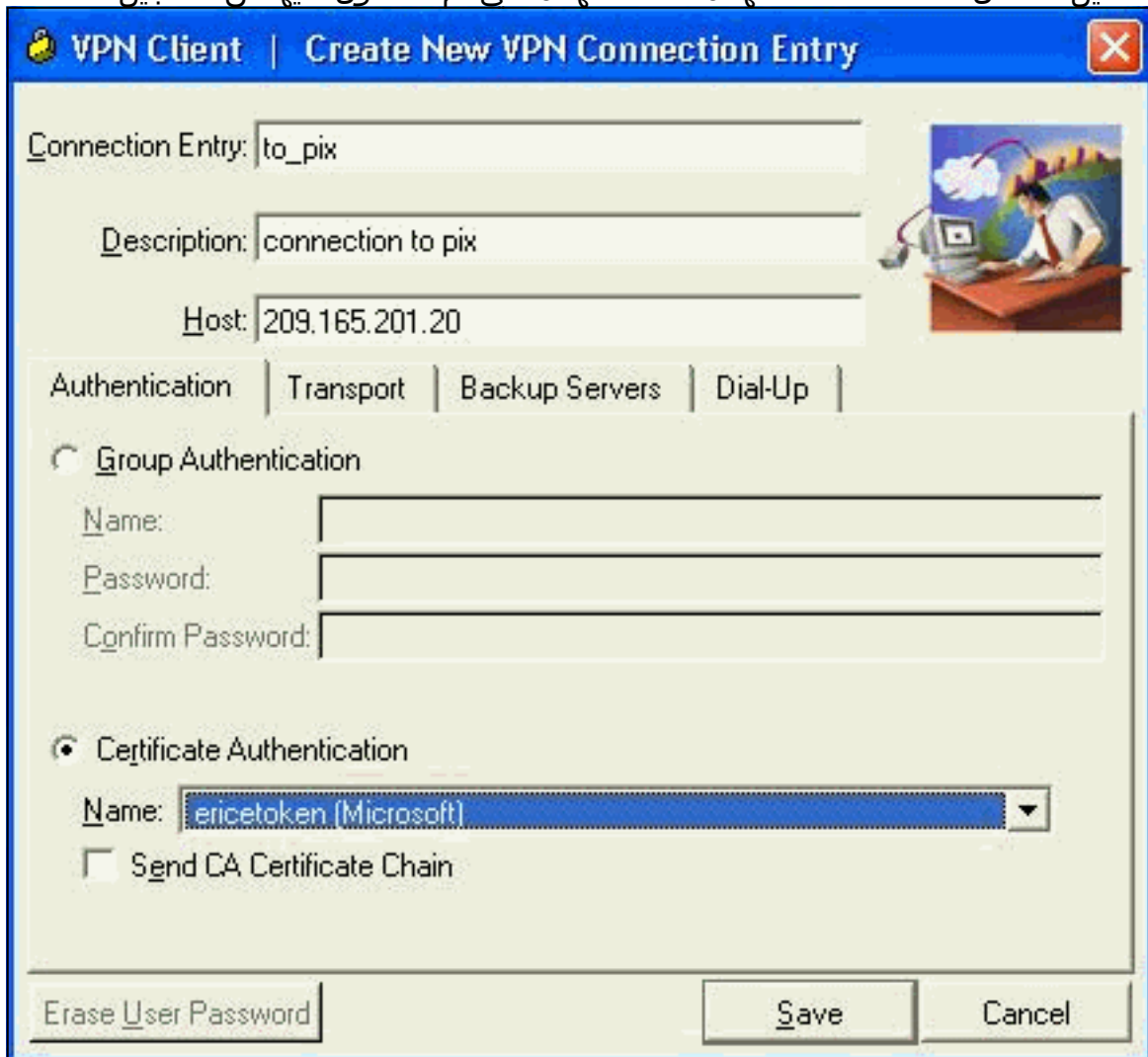
تكوين عميل Cisco VPN لاستخدام الشهادة للاتصال ب PIX

توضح هذه الخطوات الإجراءات المستخدمة لتكوين عميل Cisco VPN لاستخدام الشهادة لاتصالات PIX.

1. قم بتشغيل عميل Cisco VPN. تحت "إدخالات الاتصال" انقر فوق جديد لإنشاء اتصال جديد.

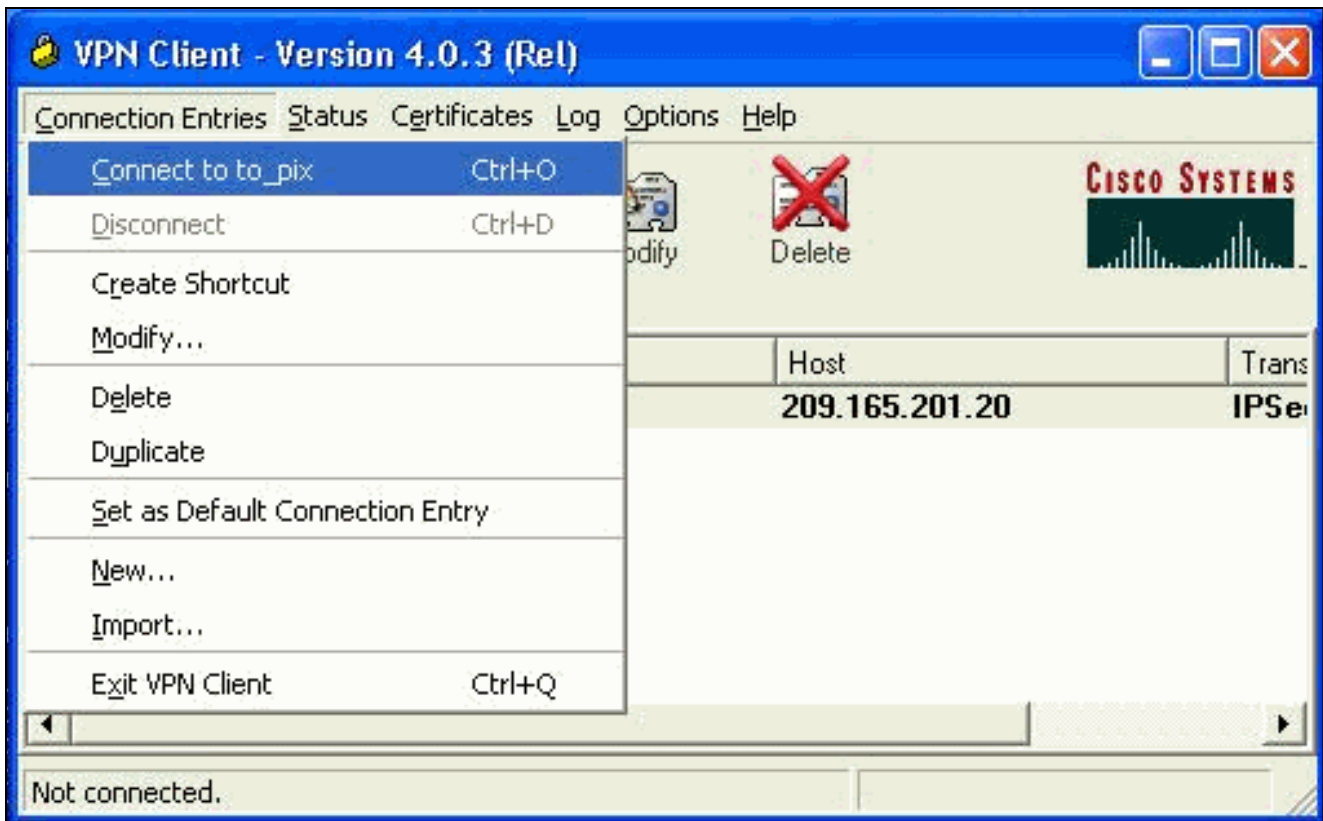


2. أكمل تفاصيل الاتصال، حدد مصادقة الشهادة، حدد الشهادة التي تم الحصول عليها من التسجيل. قطعة



حفظ

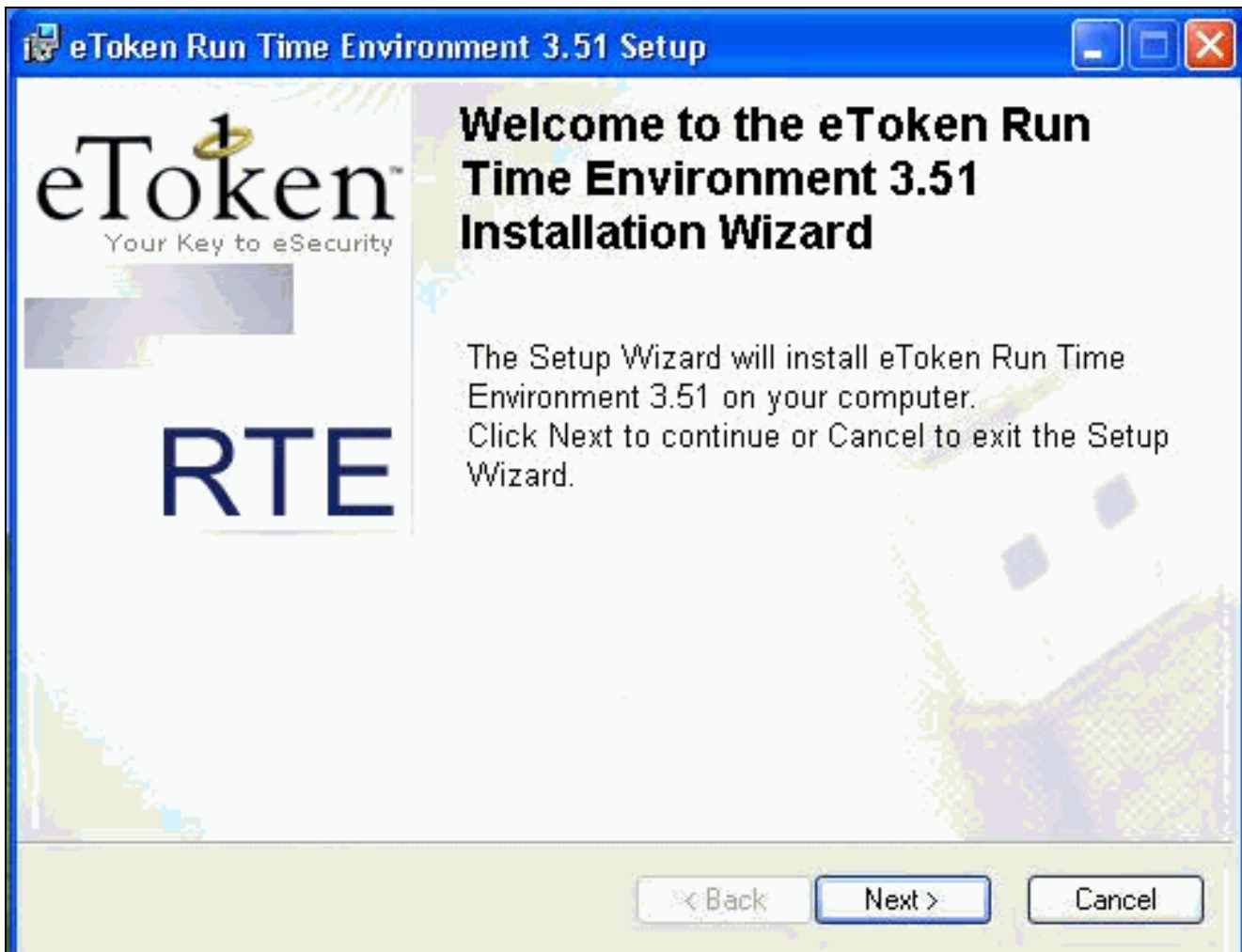
3. أخترت in order to بدأت ال cisco VPN زبون توصيل إلى ال PIX، ال مرغوب توصيل مدخل و قطعة توصيل.



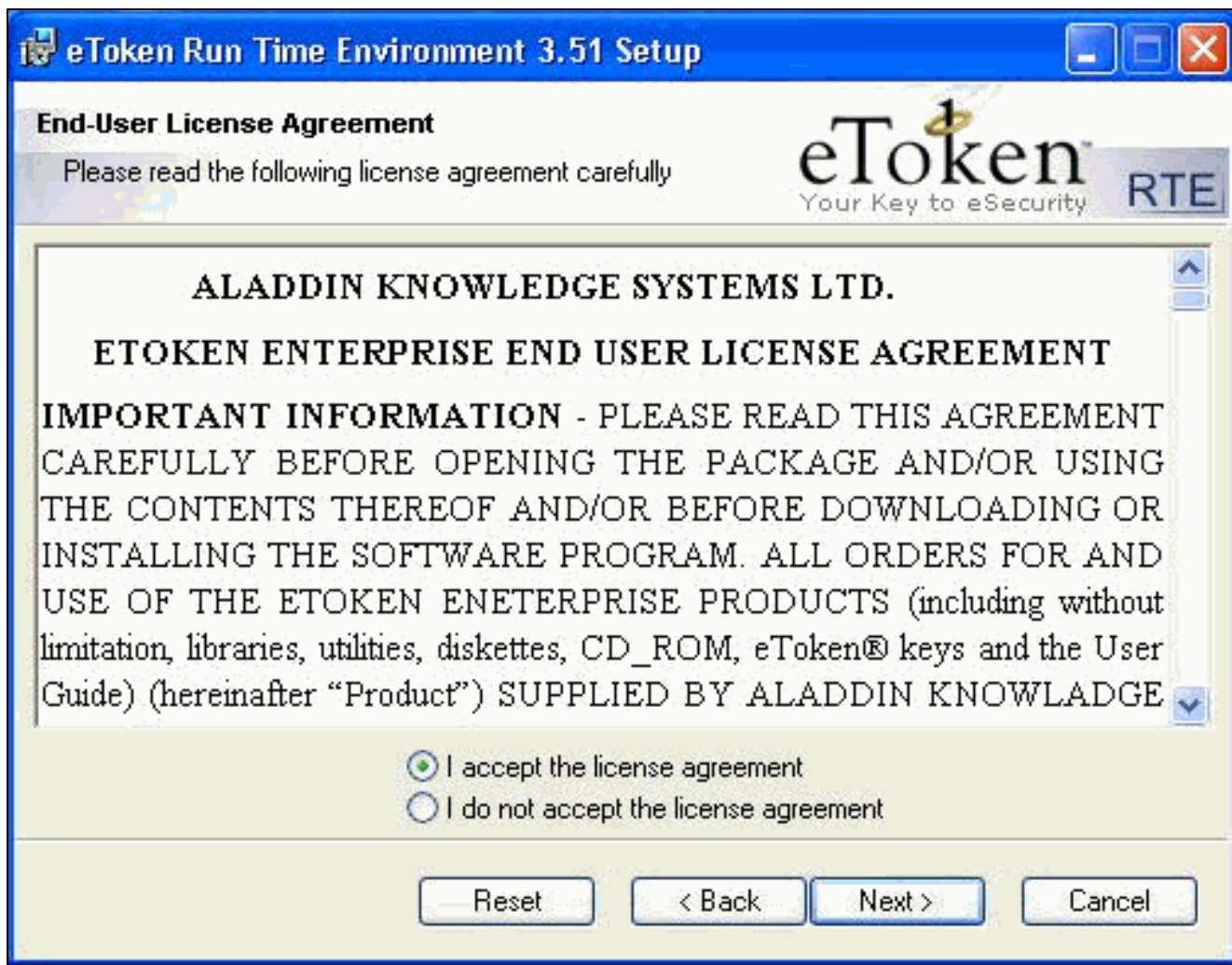
تثبيت برامج تشغيل البطاقة الذكية من eToken

توضح هذه الخطوات تثبيت برامج تشغيل eToken Smartcard [Aladdin](#).

1. افتح معالج إعداد بيئة وقت تشغيل eToken
3.51



2. اقبل شروط إتفاقية الترخيص وانقر فوق التالي.



3. انقر على
تثبيت.



4. تم تثبيت برامج تشغيل البطاقة الذكية من eToken الآن. انقر فوق إنهاء" للخروج من معالج الإعداد.



التحقق من الصحة

يوفر هذا القسم معلومات يمكنك إستخدامها للتأكد من أن التكوين يعمل بشكل صحيح.

يتم دعم بعض أوامر العرض بواسطة [أداة مترجم الإخراج \(العملاء المسجلون فقط\)](#)، والتي تتيح لك عرض تحليل [إخراج أمر العرض](#).

• **show crypto isakmp sa** — يعرض جميع اقترانات أمان تبادل مفتاح الإنترنت (IKE) الحالية (SAs) في نظير.

```
SV2-11(config)#show crypto isa sa
Total      : 1
Embryonic  : 0
```

dst	src	state	pending	created
QM_IDLE	0	1	209.165.201.19	209.165.201.20

• **show crypto ipsec** — يعرض الإعدادات المستخدمة من قبل اقترانات الأمان الحالية.

```
SV1-11(config)#show crypto ipsec sa
interface: outside
Crypto map tag: mymap, local addr. 209.165.201.20
(local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
(remote ident (addr/mask/prot/port): (10.0.0.10/255.255.255.255/0/0)
current_peer: 209.165.201.19:500
dynamic allocated peer ip: 10.0.0.10
{ }=PERMIT, flags
```

```
pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4#
pkts decaps: 7, #pkts decrypt: 7, #pkts verify 7#
```

```
pkts compressed: 0, #pkts decompressed: 0#
```

```
pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0#
```

```
send errors 0, #recv errors 0#
```

```
local crypto endpt.: 209.165.201.20, remote crypto endpt.: 209.165.201.19
```



```
path mtu 1500, ipsec overhead 56, media mtu 1500
current outbound spi: c9a9220e
      :inbound esp sas
      (spi: 0xa9857984(2844096900
      , transform: esp-3des esp-md5-hmac
      { ,in use settings ={Tunnel
slot: 0, conn id: 1, crypto map: mymap
(sa timing: remaining key lifetime (k/sec): (4607996/28746
      IV size: 8 bytes
      replay detection support: Y
      :inbound ah sas
      :inbound pcp sas
      :outbound esp sas
      (spi: 0xc9a9220e(3383304718
      , transform: esp-3des esp-md5-hmac
      { ,in use settings ={Tunnel
slot: 0, conn id: 2, crypto map: mymap
(sa timing: remaining key lifetime (k/sec): (4608000/28748
      IV size: 8 bytes
      replay detection support: Y
      :outbound ah sas
      :outbound pcp sas
```

استكشاف الأخطاء وإصلاحها

ارجع إلى [استكشاف أخطاء PIX وإصلاحها](#) لتمرير حركة مرور البيانات على نفق IPsec المنشأ للحصول على مزيد من المعلومات حول استكشاف أخطاء هذا التكوين وإصلاحها.

معلومات ذات صلة

- [مراجع أوامر جدار حماية PIX الآمن من Cisco](#)
- [طلبات التعليقات \(RFCs\)](#)
- [صفحة دعم IPsec \(بروتوكول أمان IP\)](#)
- [صفحة دعم عميل شبكة VPN من Cisco](#)
- [صفحة دعم جدران الحماية من السلسلة PIX 500](#)
- [الدعم الفني - Cisco Systems](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا اذ ه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ م ف ن م دخت س م ل م عد و ت م م م دقت ل ة م ش ب ل و
م ك 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 ا ل م م چ ر ي . ة ص ا خ ل م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت م م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا م ل ا ح ل ا و ه
ل ا ا م ا د ا د ع و چ ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه 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 چ ن ا ل ا دن ت س م ل ا