

使用智慧卡證書的PIX和Cisco VPN客戶端之間的IPSec配置示例

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[註冊並配置PIX](#)

[組態](#)

[註冊Cisco VPN客戶端證書](#)

[配置Cisco VPN客戶端以使用證書連線到PIX](#)

[安裝eToken智慧卡驅動程式](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本文檔演示如何在PIX防火牆和Cisco VPN客戶端4.0.x之間配置IPSec VPN隧道。本文檔中的配置示例還重點介紹了Cisco IOS®路由器和Cisco VPN客戶端的證書頒發機構(CA)註冊過程，以及智慧卡用作證書儲存的方法。

請參閱[使用委託證書在Cisco IOS路由器和Cisco VPN客戶端之間配置IPSec](#)，以瞭解有關使用委託證書在Cisco IOS路由器和Cisco VPN客戶端之間配置IPSec的詳細資訊。

請參閱[在Cisco IOS路由器上配置多身份證書頒發機構](#)，瞭解有關在Cisco IOS路由器上配置多身份證書頒發機構的詳細資訊。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 運行軟體版本6.3(3)的Cisco PIX防火牆

- 運行Windows XP的PC上的Cisco VPN客戶端4.0.3
- 在本文檔中，Microsoft Windows 2000 CA伺服器用作CA伺服器。
- Cisco VPN使用者端上的憑證是使用[Aladdin e-Token](#)智慧卡儲存的。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

註冊並配置PIX

本節提供用於設定本檔案中所述功能的資訊。

注意：若要查詢有關本文檔中使用的命令的其他資訊，請使用[命令查詢工具](#)（僅限註冊客戶）。

組態

本檔案會使用這些設定。

- [PIX防火牆上的證書註冊](#)
- [PIX防火牆配置](#)

PIX防火牆上的證書註冊

```
!--- 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
```

PIX防火牆配置

```
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)#

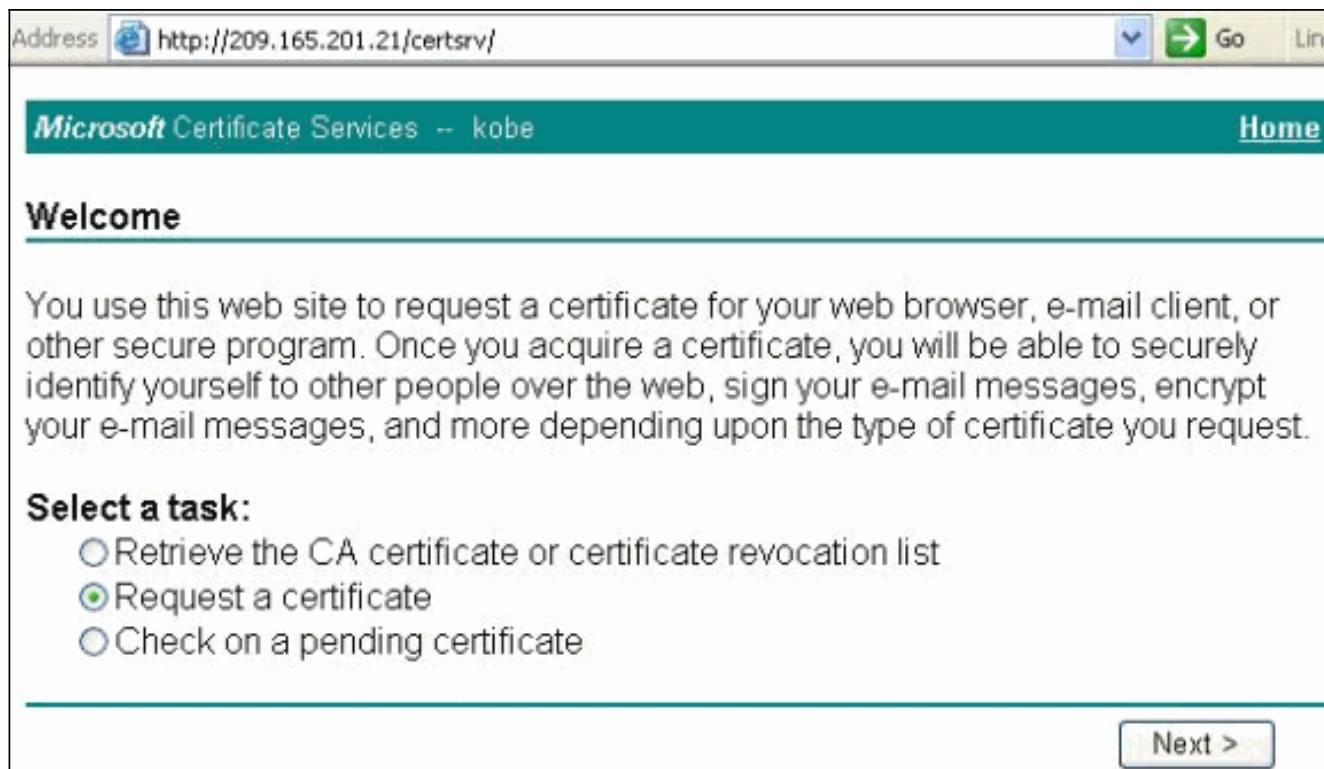
```

註冊Cisco VPN客戶端證書

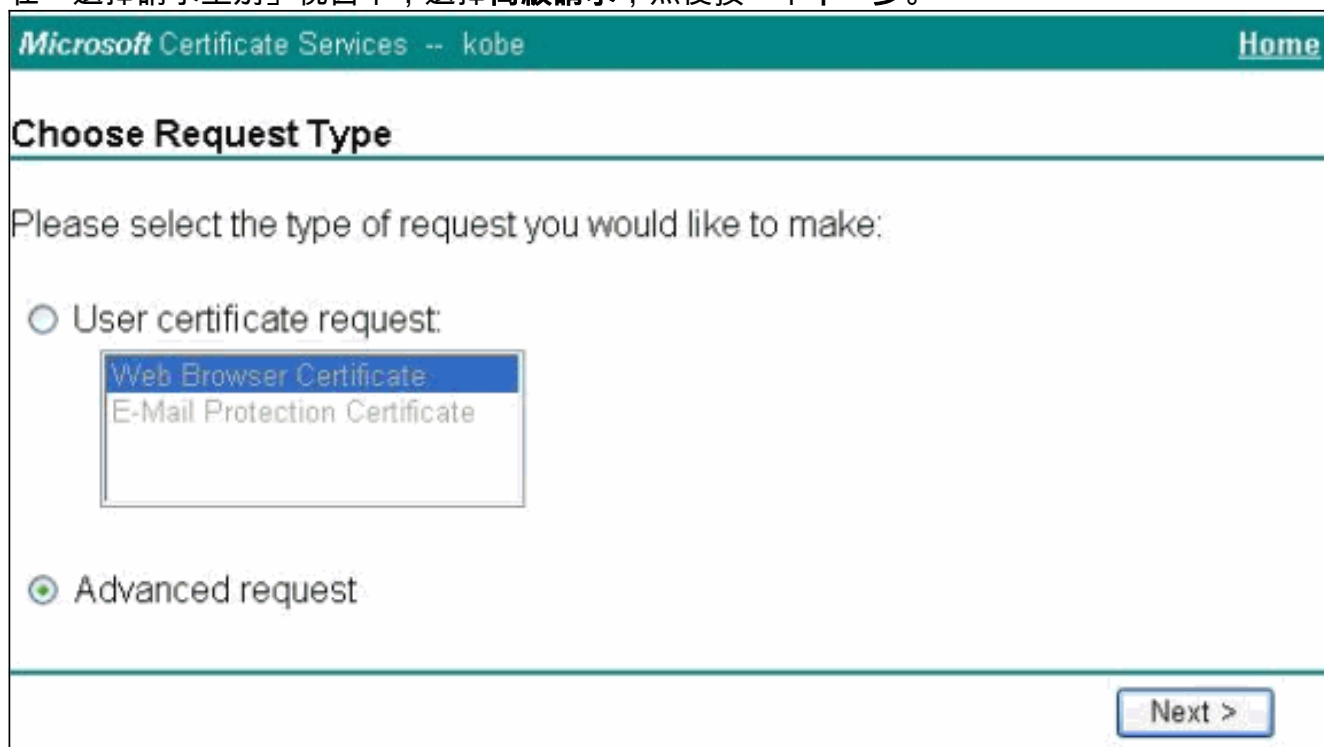
請記得在PC上安裝智慧卡裝置隨附的所有必要的驅動程式和實用程式，以便與Cisco VPN客戶端配合使用。

以下步驟演示用於註冊Cisco VPN Client for MS證書的過程。憑證儲存在[Aladdin](#) e-Token Smartcard儲存區上。

1. 啟動瀏覽器並前往憑證伺服器頁面(在本範例中為http://CAServeraddress/certsrv/)。
2. 選擇**Request a certificate**，然後按一下**Next**。



3. 在「選擇請求型別」視窗中，選擇**高級請求**，然後按一下下一步。



4. 選擇Submit a certificate request to this CA using a form，然後按一下Next。

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. 填寫「高級證書請求」表單中的所有專案。確保部門或組織單位(OU)對應於Cisco VPN客戶端組名稱，如PIX vpngroup名稱中所配置。選擇適用於您的設定的正確證書服務提供商(CSP)。

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:

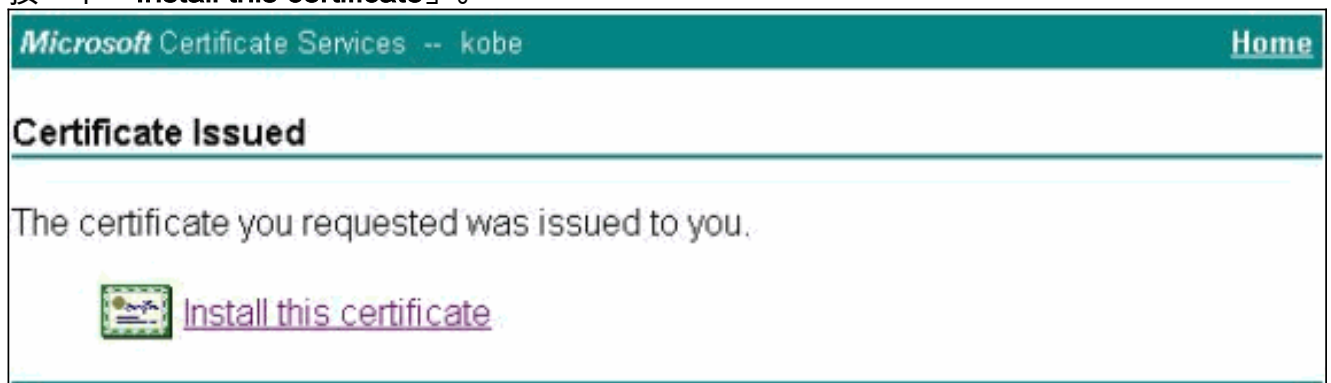
6. 選擇Yes可在收到潛在指令碼驗證警告時繼續安裝。



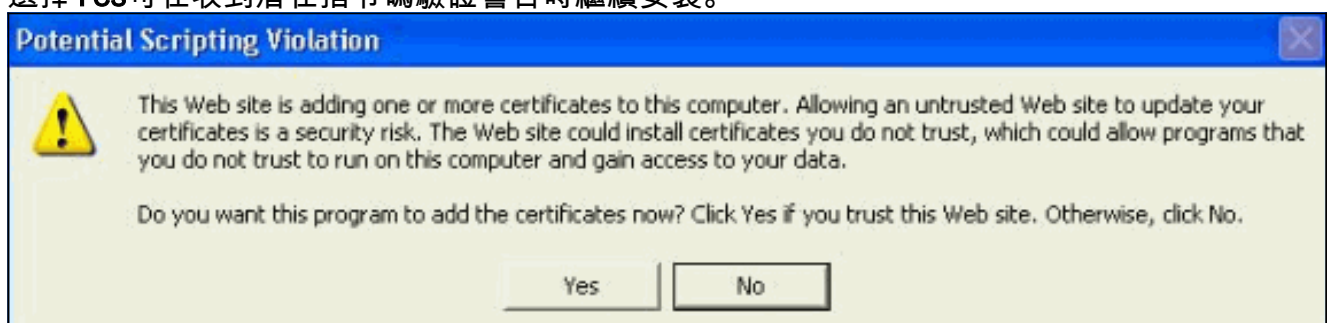
7. 證書註冊將呼叫eToken儲存。輸入密碼並按一下OK。



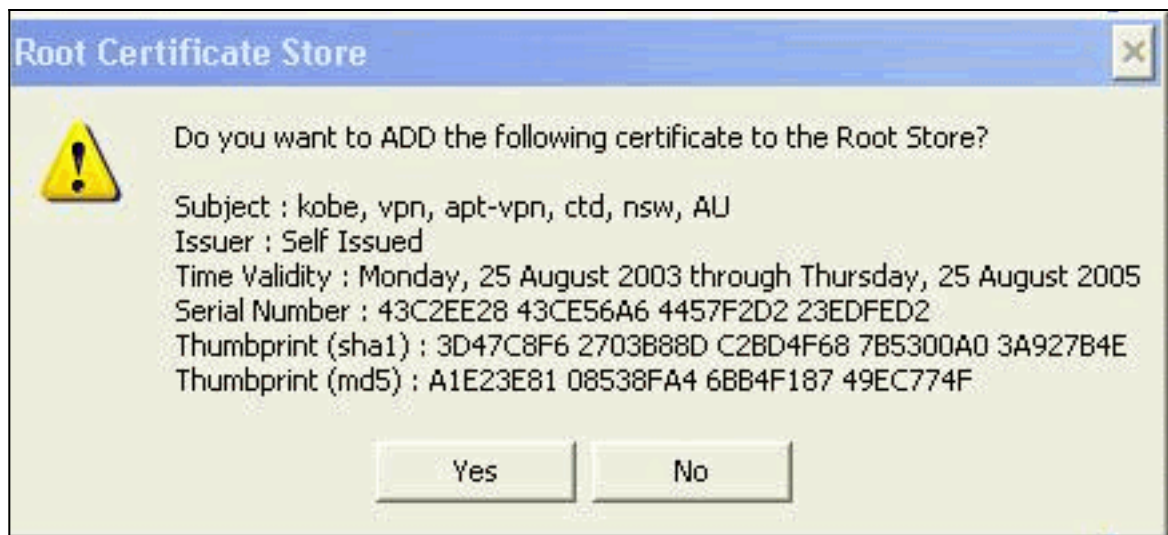
8. 按一下「Install this certificate」。



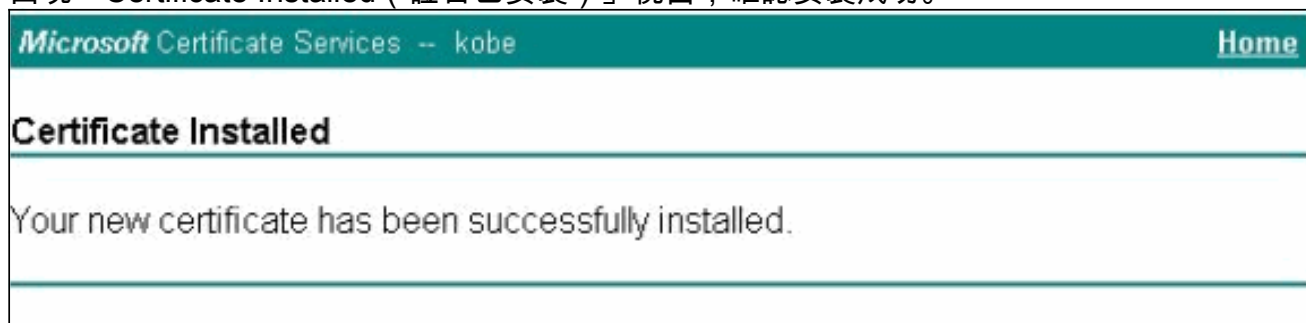
9. 選擇Yes可在收到潛在指令碼驗證警告時繼續安裝。



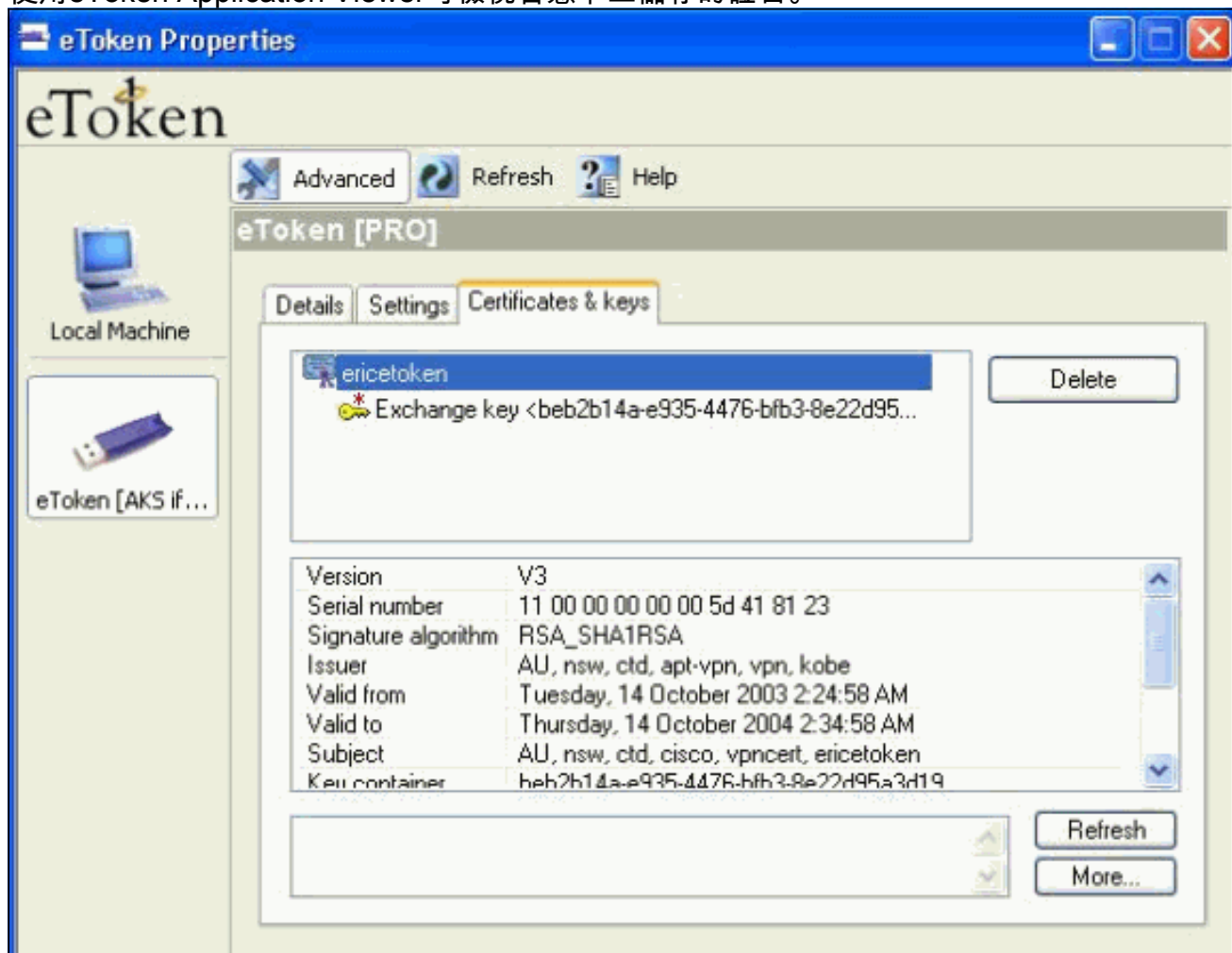
10. 選擇Yes以將根證書新增到根儲存區。



11. 出現「Certificate Installed (證書已安裝)」視窗，確認安裝成功。



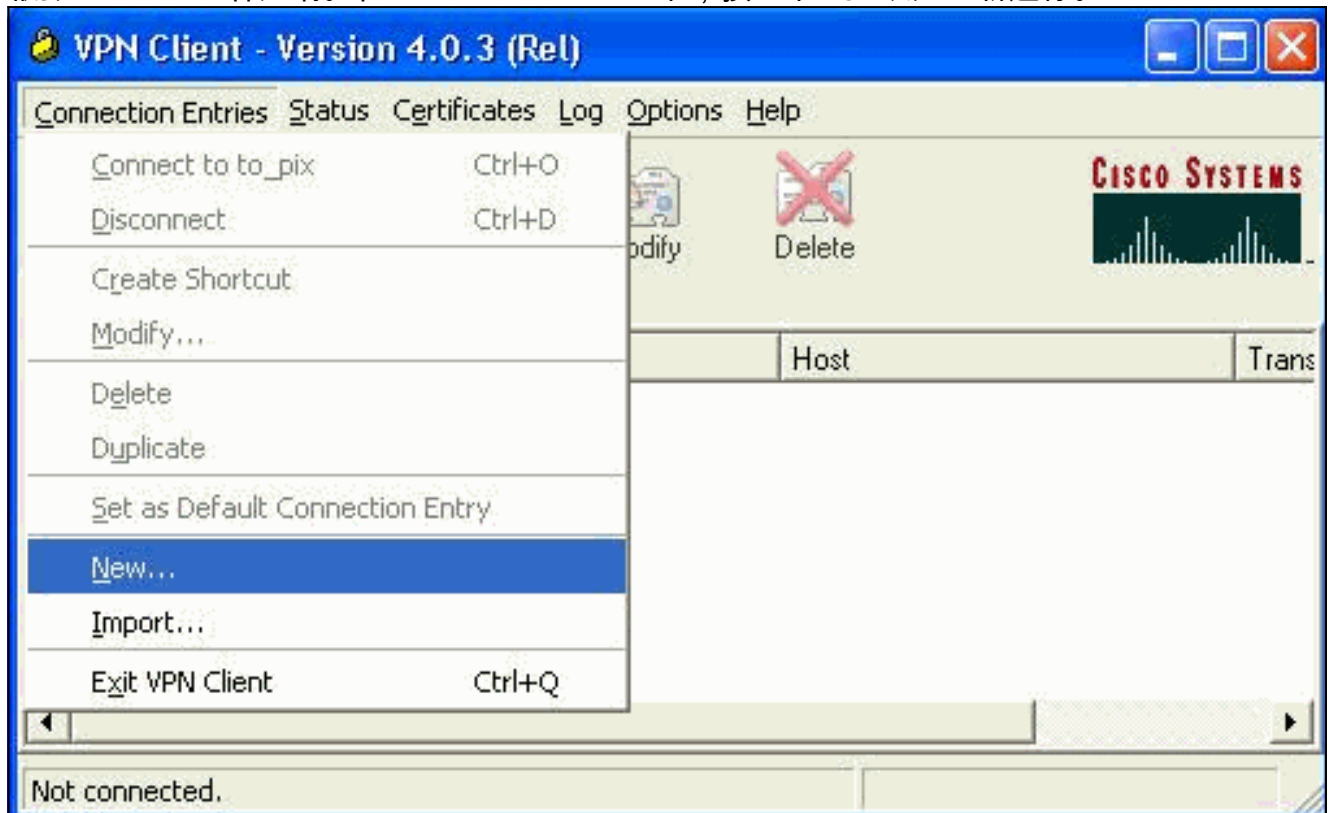
12. 使用eToken Application Viewer可檢視智慧卡上儲存的證書。



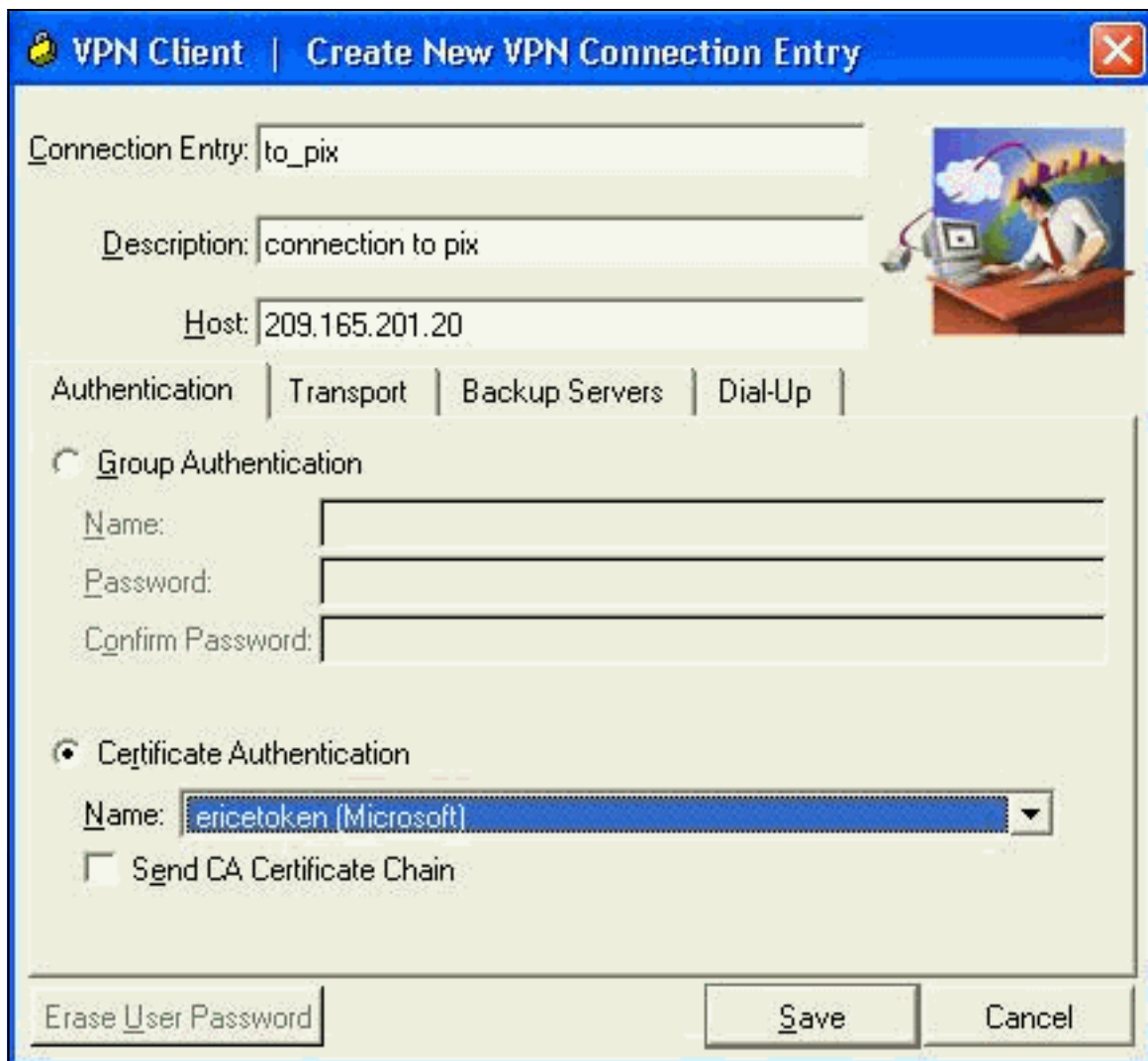
配置Cisco VPN客戶端以使用證書連線到PIX

這些步驟演示了將Cisco VPN客戶端配置為使用證書進行PIX連線的過程。

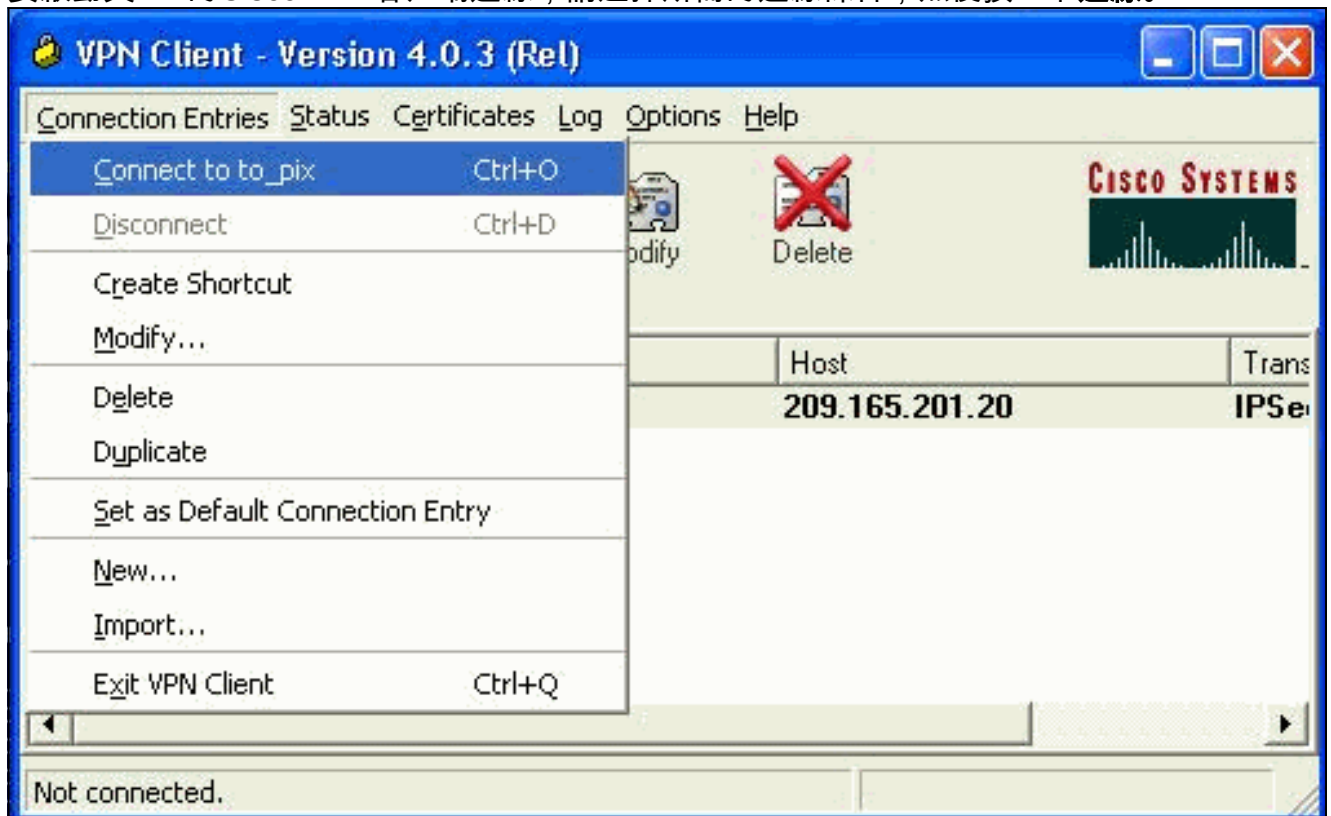
1. 啟動Cisco VPN客戶端。在Connection Entries下，按一下**New**以建立新連線。



2. 完成連線詳細資訊，指定證書身份驗證，選擇從註冊中獲取的證書。按一下「Save」。



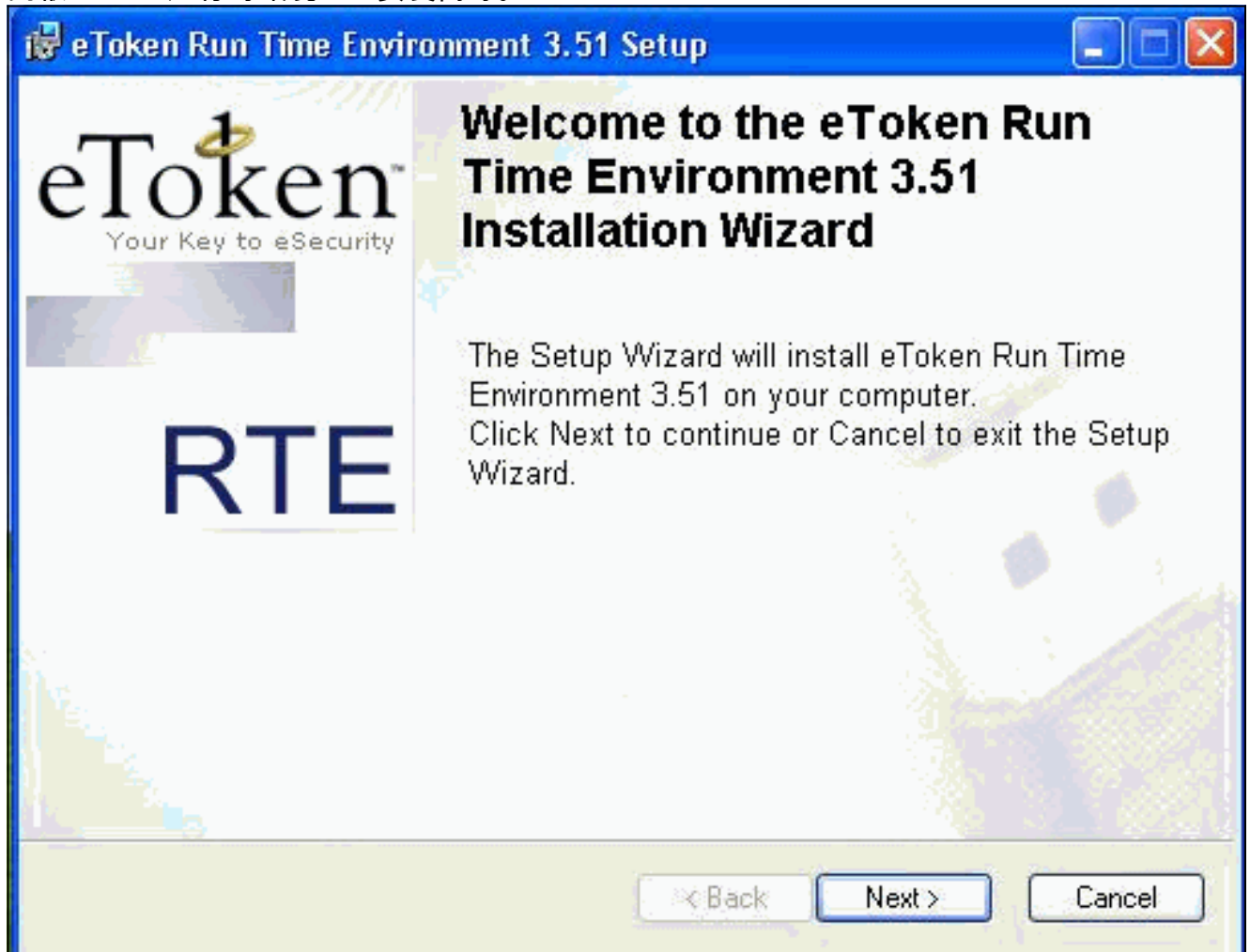
3. 要啟動與PIX的Cisco VPN客戶端連線，請選擇所需的連線條目，然後按一下**連線**。



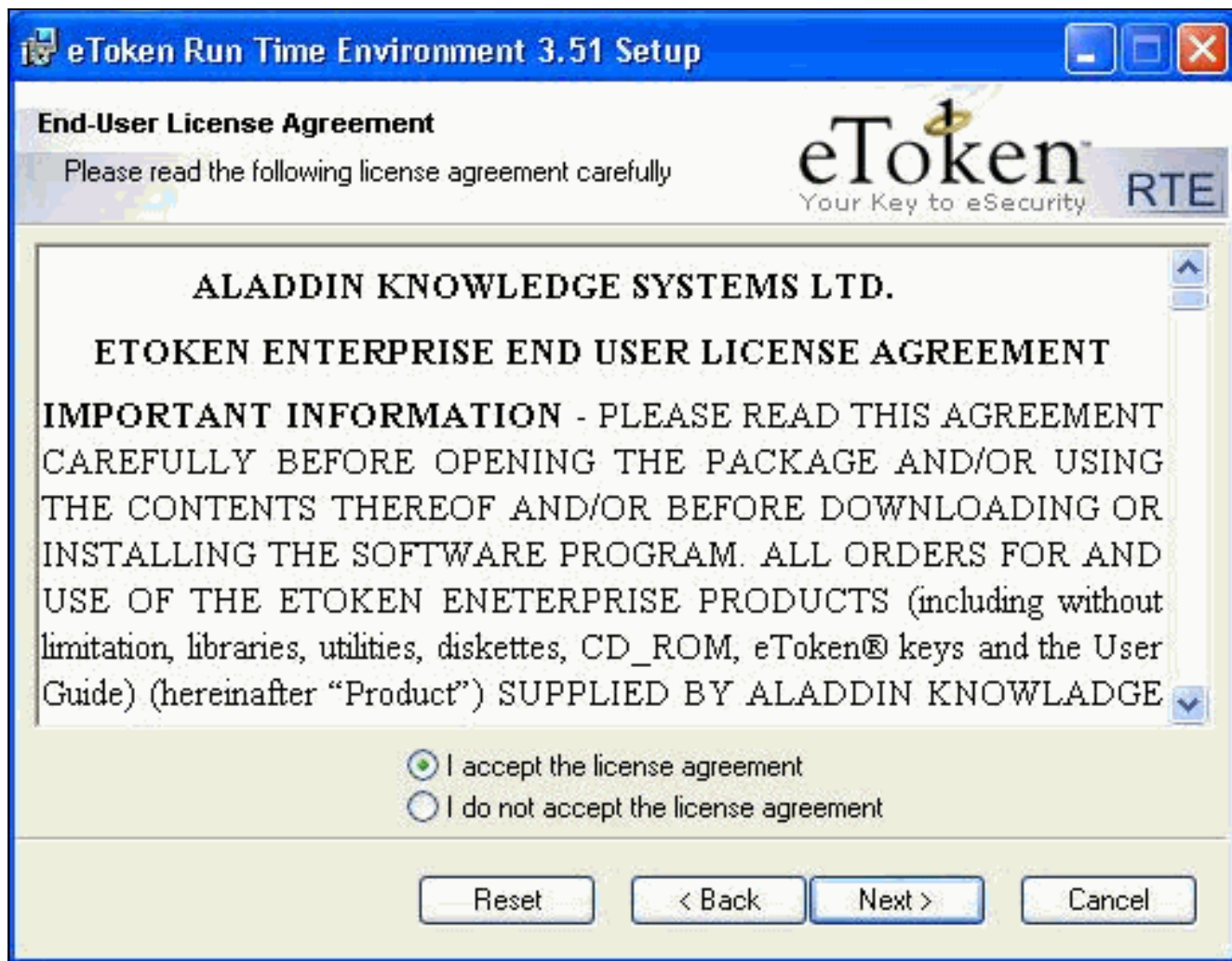
[安裝eToken智慧卡驅動程式](#)

以下步驟演示如何安裝Aladdin eToken智慧卡驅動程式。

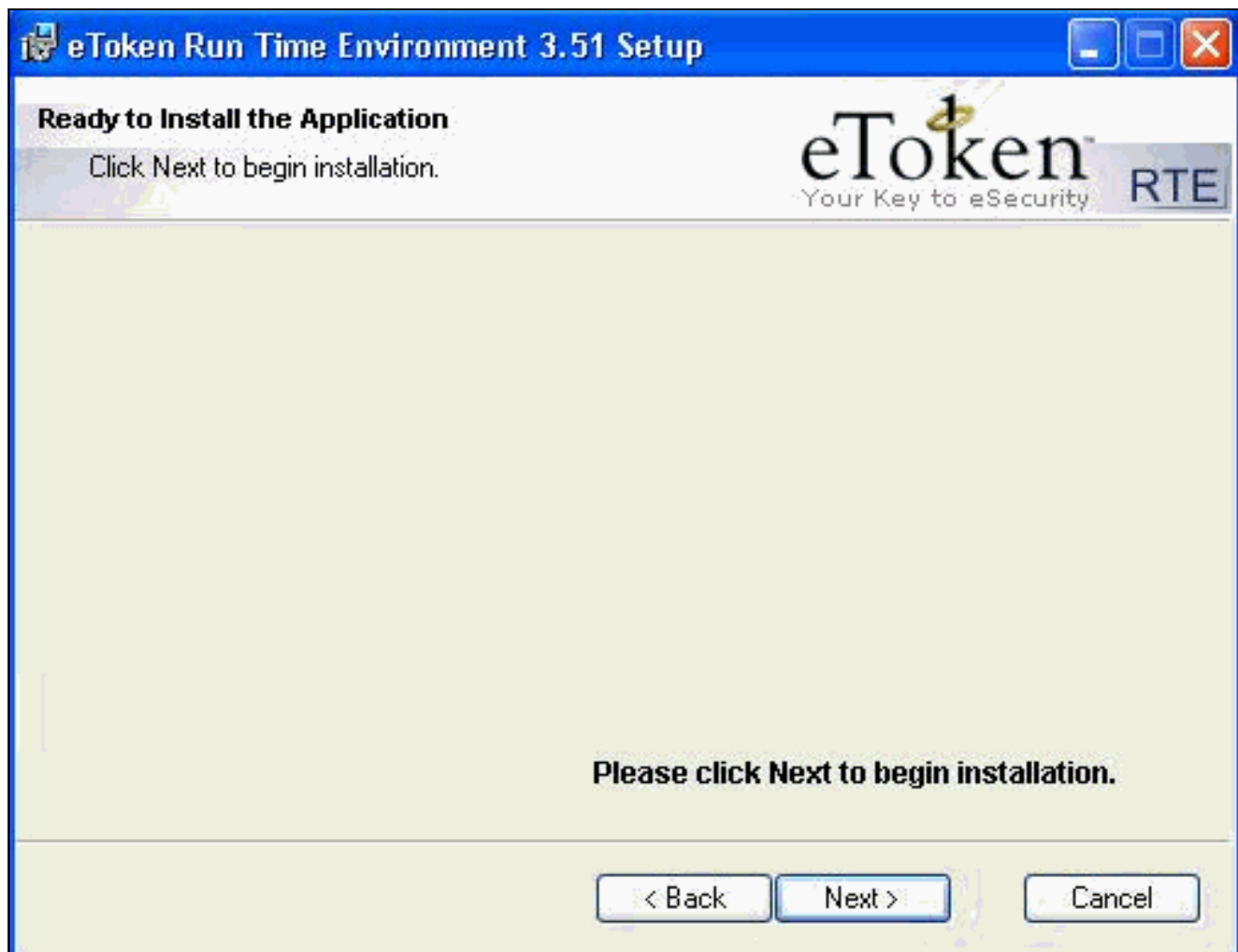
1. 開啟eToken運行時環境3.51安裝嚮導。



2. 接受許可協定條款，然後點選下一步。



3. 按一下「Install」。



4. 現在已安裝eToken智慧卡驅動程式。按一下**完成**以退出安裝嚮導。



驗證

本節提供的資訊可用於確認您的組態是否正常運作。

[輸出直譯器工具](#)(僅供註冊客戶使用)支援某些show命令，此工具可讓您檢視show命令輸出的分析。

- **show crypto isakmp sa** — 顯示對等體上的所有當前網際網路金鑰交換(IKE)安全關聯(SA)。

```
SV2-11(config)#show crypto isa sa
Total      : 1
Embryonic  : 0
      dst                src          state      pending   created
209.165.201.20  209.165.201.19  QM_IDLE    0         1
```

- **show crypto ipsec sa** — 顯示當前安全關聯使用的設定。

```
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:
```

[疑難排解](#)

如需此配置故障排除的詳細資訊，請參閱[排除PIX故障以在已建立的IPSec隧道上傳遞資料流量](#)。

[相關資訊](#)

- [Cisco Secure PIX防火牆命令參考](#)
- [要求建議 \(RFC\)](#)
- [IPSec \(IP 安全通訊協定 \) 支援頁面](#)
- [Cisco VPN使用者端支援頁面](#)
- [PIX 500系列防火牆支援頁面](#)
- [技術支援 - Cisco Systems](#)