

# ASA 8.X:通過隧道預設網關路由SSL VPN流量配置示例

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[背景資訊](#)

[設定](#)

[網路圖表](#)

[使用ASDM 6.1\(5\)的ASA配置](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

## 簡介

本文檔介紹如何配置自適應安全裝置(ASA)以通過隧道預設網關(TDG)路由SSL VPN流量。當您使用隧道選項建立預設路由時，所有來自在ASA上終止且無法使用已獲取或靜態路由進行路由的隧道的流量都會傳送到此路由。對於從隧道中湧現的流量，此路由會覆蓋任何其他已配置或已獲知的預設路由。

## 必要條件

### 需求

嘗試此組態之前，請確保符合以下要求：

- 運行在8.x版上的ASA
- Cisco SSL VPN使用者端(SVC)1.x注意：從[Cisco Software Download](#)（僅限註冊客戶）下載SSL VPN客戶端包([sslclient-win\\*.pkg](#))。將SVC複製到ASA上的快閃記憶體。需要將SVC下載到遠端使用者電腦，以便與ASA建立SSL VPN連線。

### 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8.x的Cisco 5500系列ASA

- 適用於Windows 1.1.4.179的Cisco SSL VPN客戶端版本
- 運行Windows 2000 Professional或Windows XP的PC
- 思科調適型安全裝置管理員(ASDM)版本6.1(5)

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

請參閱[思科技術提示慣例](#)以瞭解更多有關文件慣例的資訊。

## 背景資訊

SSL VPN客戶端(SVC)是一種VPN隧道技術，使遠端使用者能夠享受IPSec VPN客戶端的好處，而無需網路管理員在遠端電腦上安裝和配置IPSec VPN客戶端。SVC使用遠端電腦上已有的SSL加密以及安全裝置的WebVPN登入和身份驗證。

在當前場景中，有一個SSL VPN客戶端通過SSL VPN隧道連線到ASA後面的內部資源。未啟用拆分隧道。當SSL VPN客戶端連線到ASA時，所有資料都將通過隧道傳輸。除了訪問內部資源外，主要標準是通過預設隧道網關(DTG)路由此隧道流量。

您可以為隧道流量定義單獨的預設路由以及標準預設路由。ASA接收的未加密流量沒有靜態路由或學習路由，通過標準預設路由進行路由。ASA接收的加密流量 ( 對於該流量沒有靜態路由或已學習路由 ) 將傳遞到通過隧道預設路由定義的DTG。

要定義隧道化預設路由，請使用以下命令：

```
route <if_name> 0.0.0.0 0.0.0.0 <gateway_ip> tunneled
```

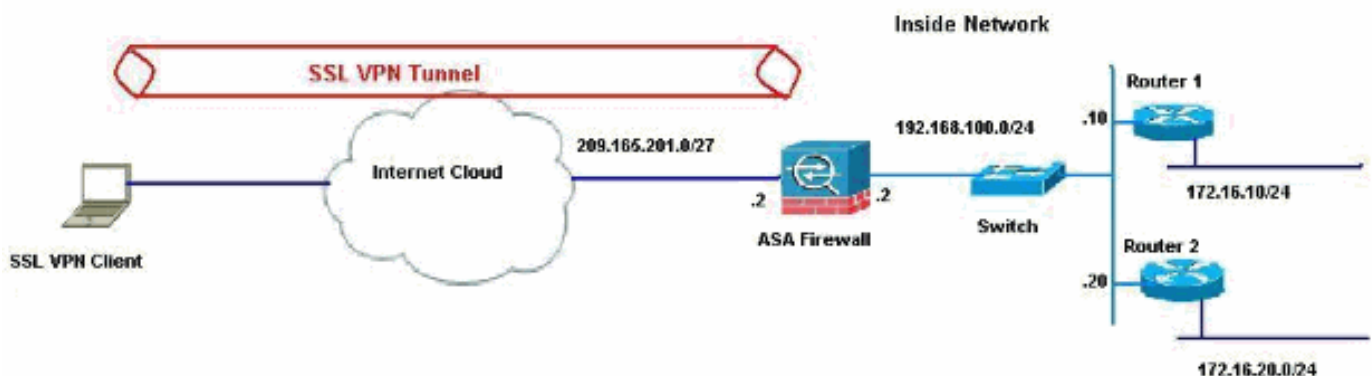
## 設定

本節提供用於設定本文件中所述功能的資訊。

**註：**使用[Command Lookup Tool](#)([僅供已註冊客戶使用](#))可獲取本節中使用的命令的詳細資訊。

## 網路圖表

本檔案會使用以下網路設定：



在本示例中，SSL VPN客戶端通過隧道訪問ASA的內部網路。用於內部網路以外目的地的流量也通過隧道傳輸，因為沒有配置拆分隧道，因此通過TDG(192.168.100.20)進行路由。

將封包路由到TDG後（在本案例中為Router 2），它會執行位址轉譯，以便將那些封包路由到網際網路。有關將路由器配置為網際網路網關的詳細資訊，請參閱[如何在非Cisco電纜數據機後面配置Cisco路由器](#)。

## 使用ASDM 6.1(5)的ASA配置

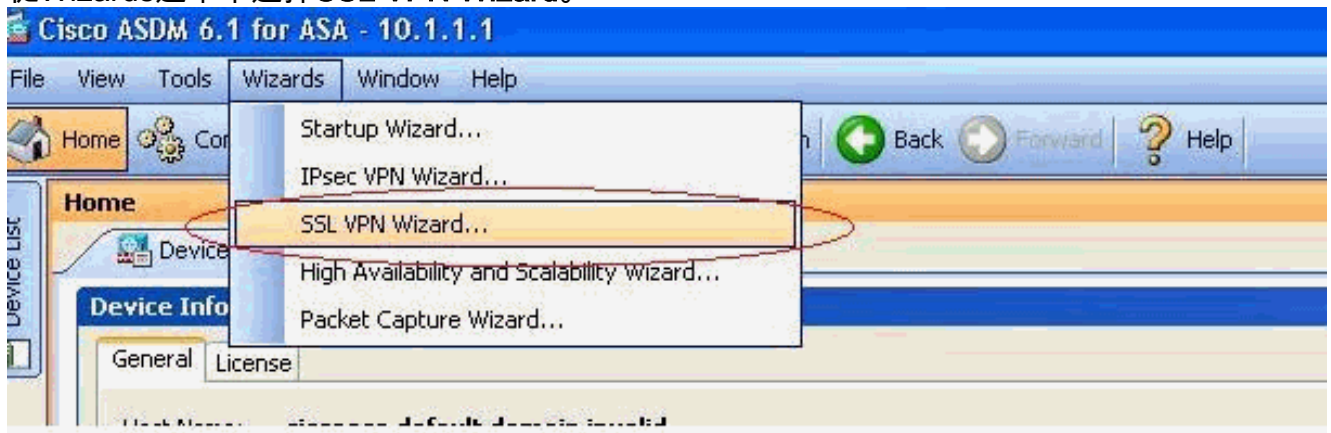
本檔案假設基本設定（例如介面組態）已完整且運作正常。

**注意：**有關如何允許ASDM配置ASA的資訊，請參閱[允許ASDM進行HTTPS訪問](#)。

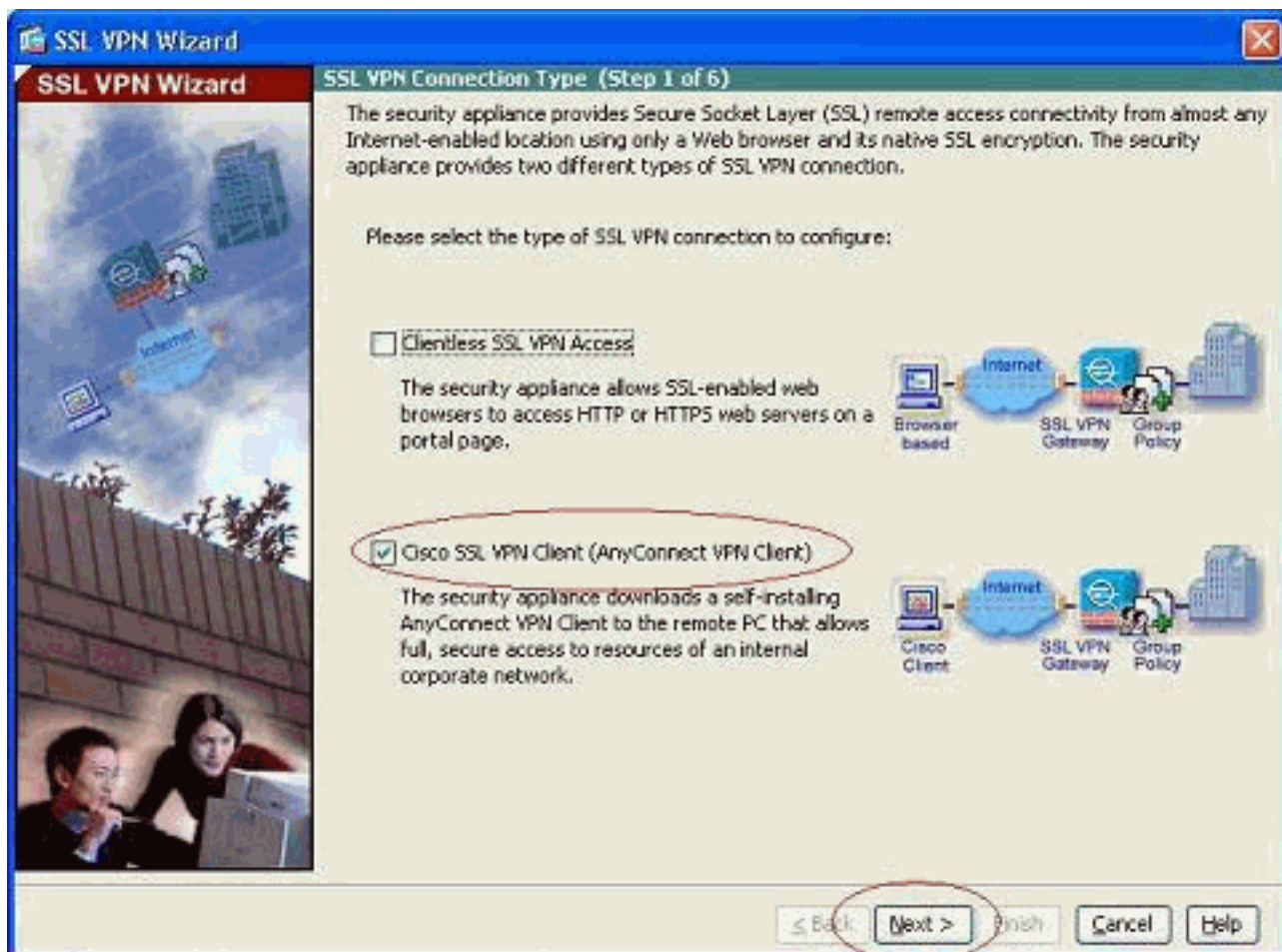
**注意：**除非更改埠號，否則不能在同一個ASA介面上啟用WebVPN和ASDM。有關詳細資訊，請參閱[在同一介面ASA上啟用ASDM和WebVPN](#)。

完成這些步驟，以便使用SSL VPN嚮導配置SSL VPN。

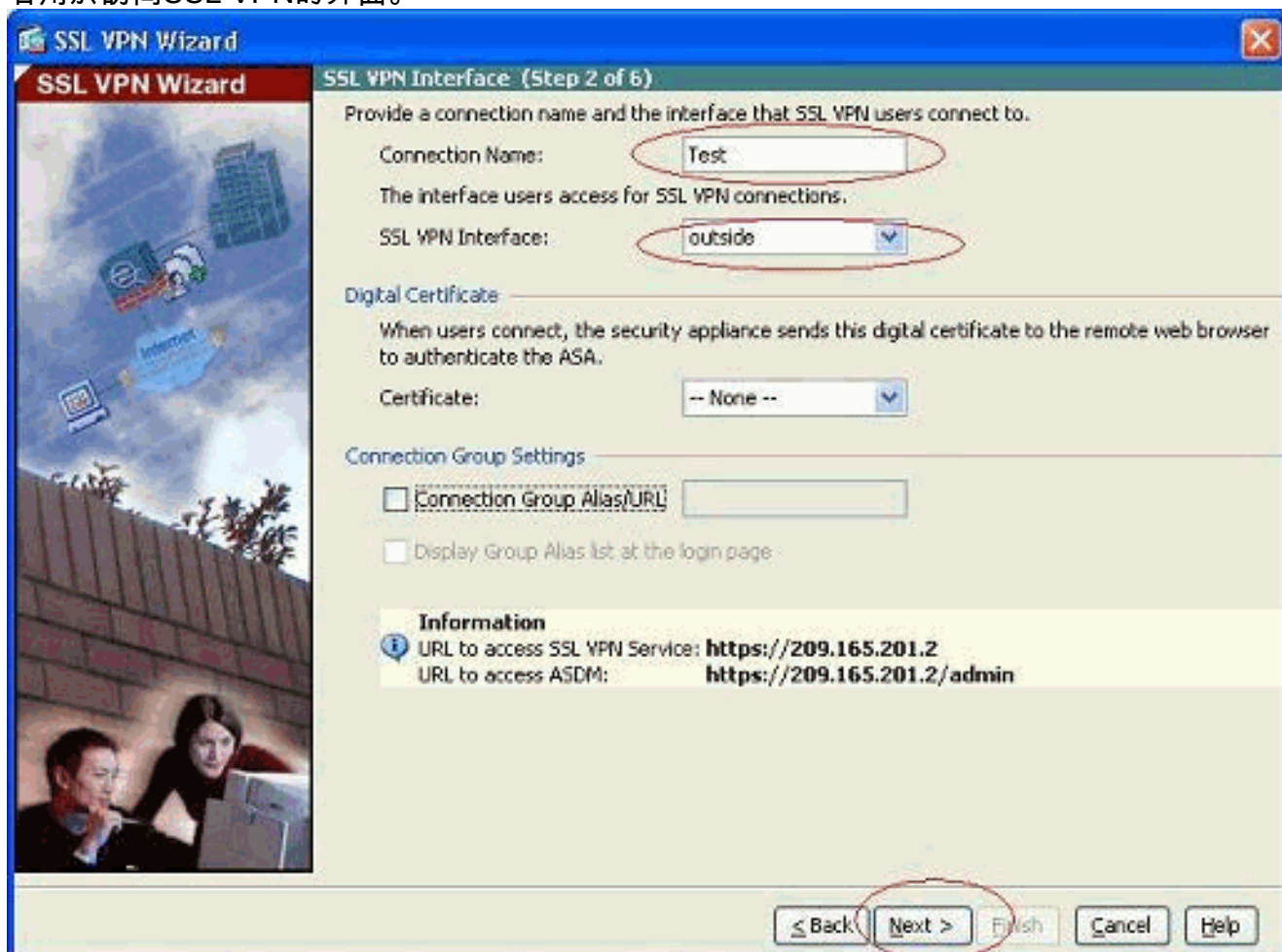
1. 從Wizards選單中選擇**SSL VPN Wizard**。



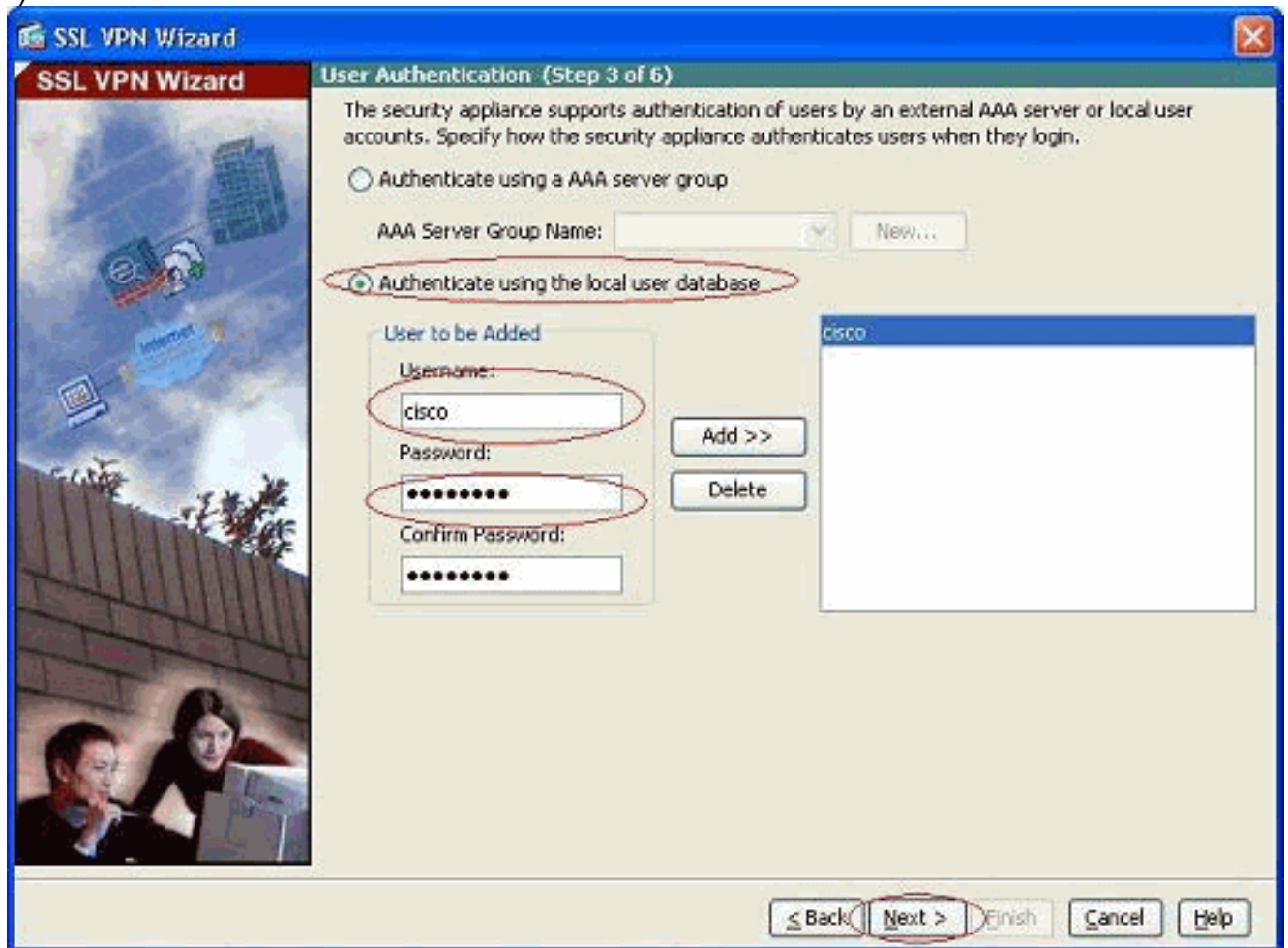
2. 按一下**Cisco SSL VPN Client**覈取方塊，然後按一下**Next**。



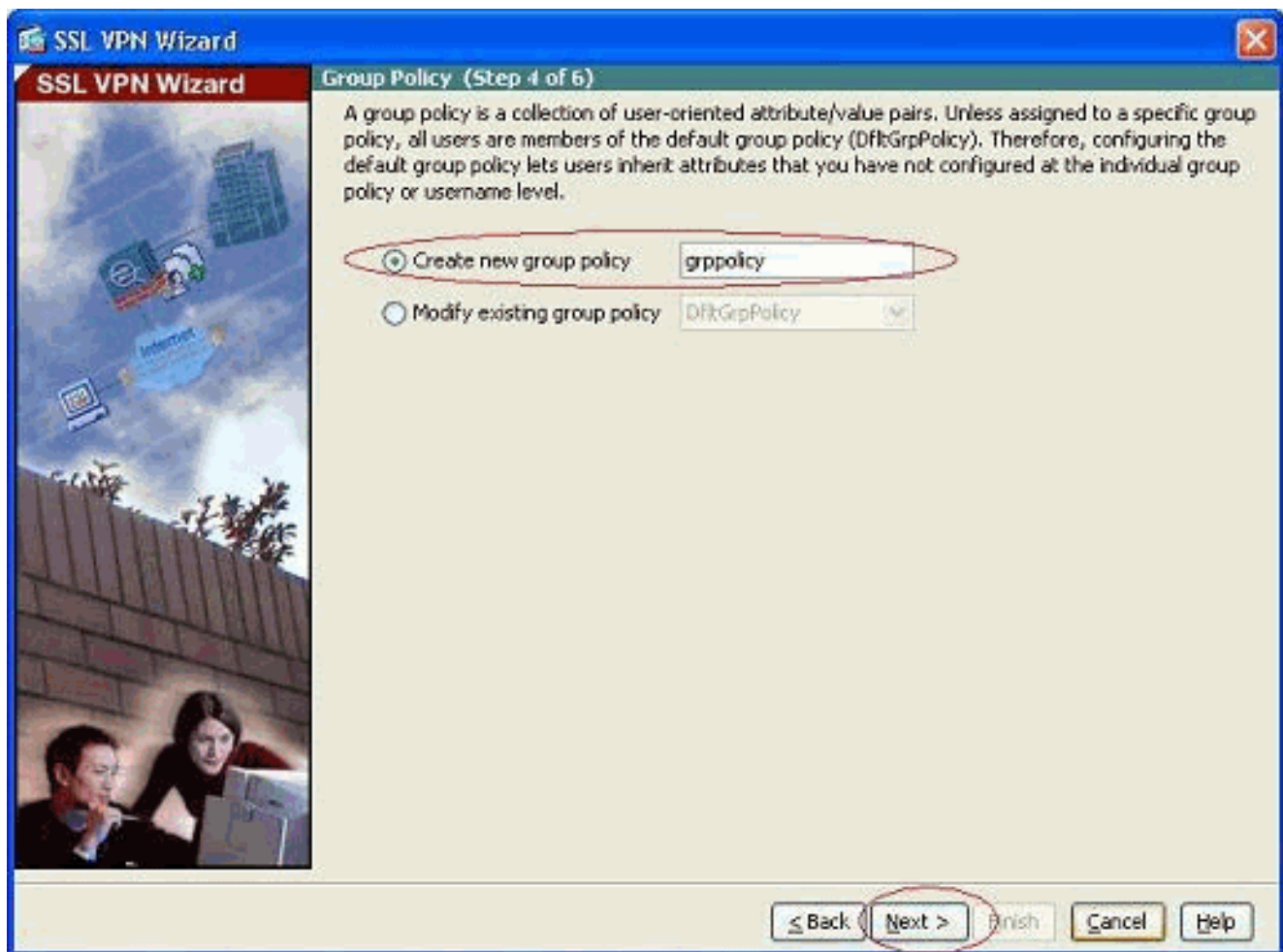
3. 在Connection Name欄位中輸入連線的名稱，然後從SSL VPN Interface下拉選單中選擇使用者用於訪問SSL VPN的介面。



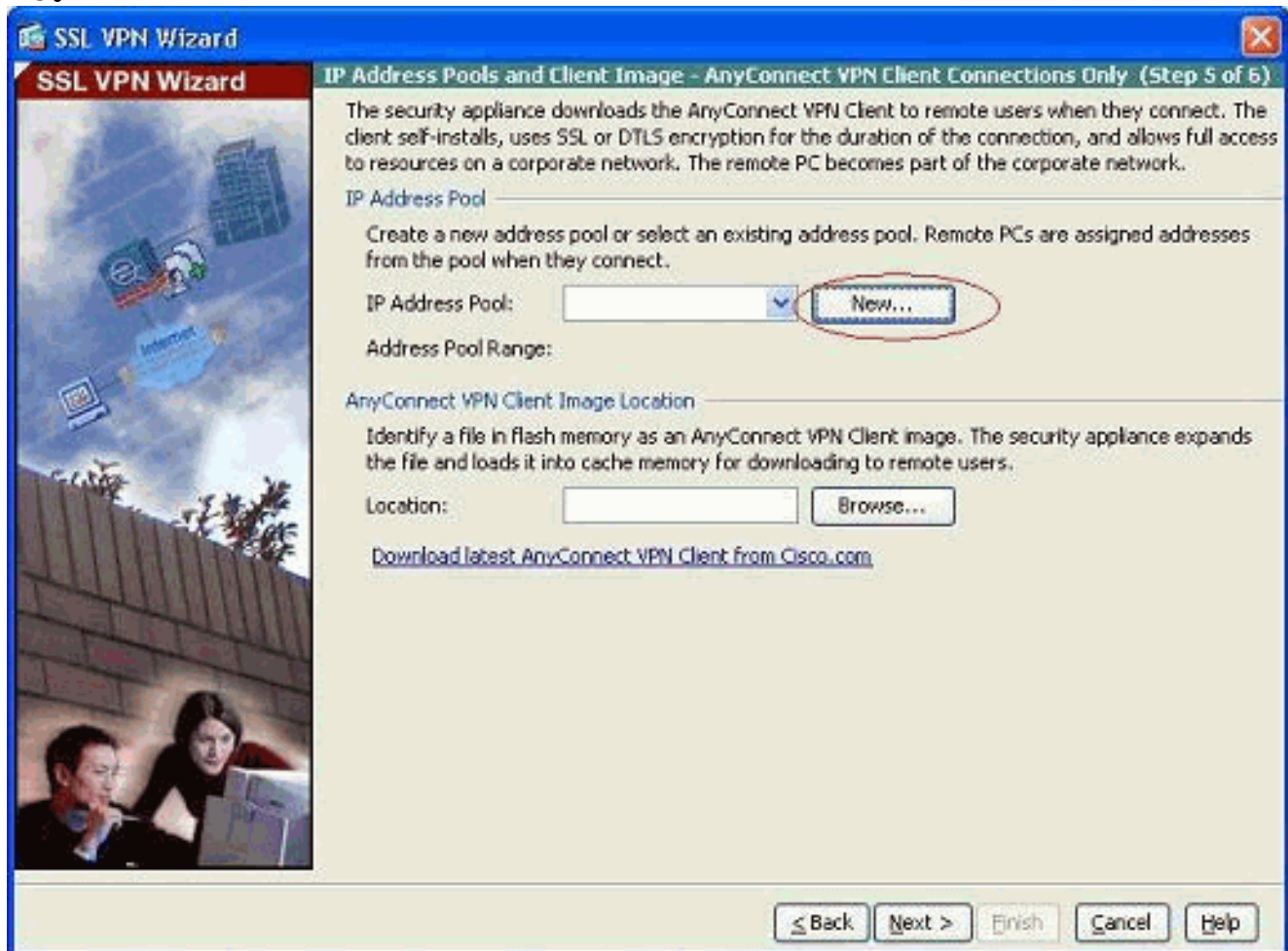
- 按「Next」（下一步）。
- 選擇身份驗證模式，然後按一下Next。（此示例使用本地身份驗證。



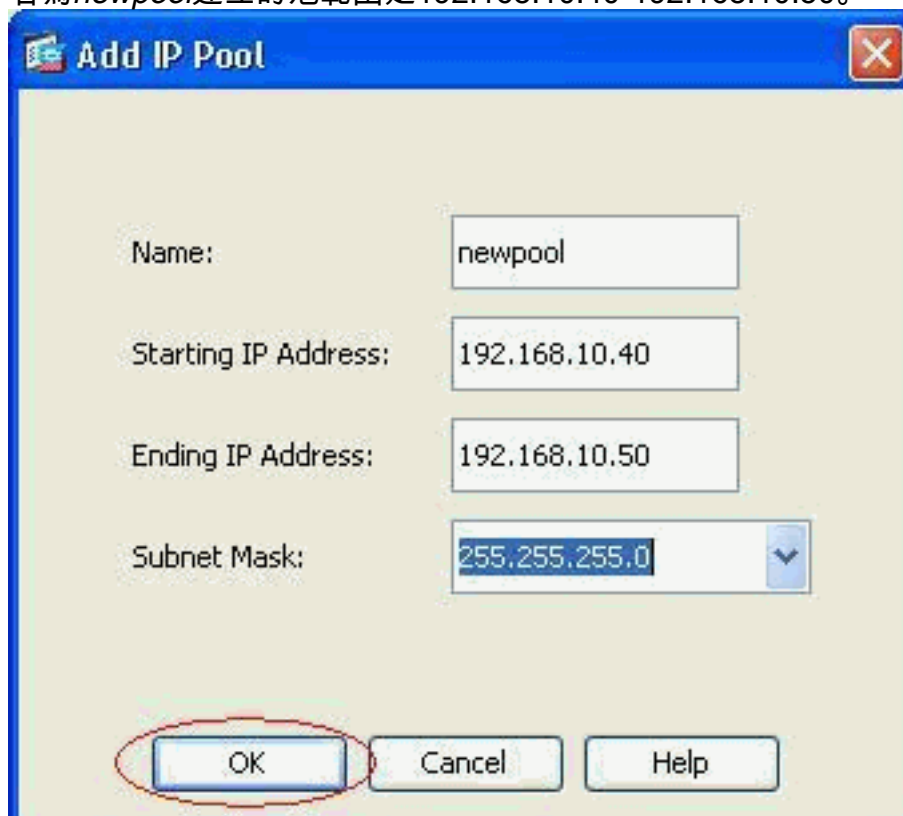
- 建立新的組策略，而不是現有的預設組策略。



7. 建立一個新的地址池，一旦連線到SSL VPN客戶端PC，該地址池將被分配給SSL VPN客戶端PC。



名為newpool建立的池範圍是192.168.10.40-192.168.10.50。



**Add IP Pool**

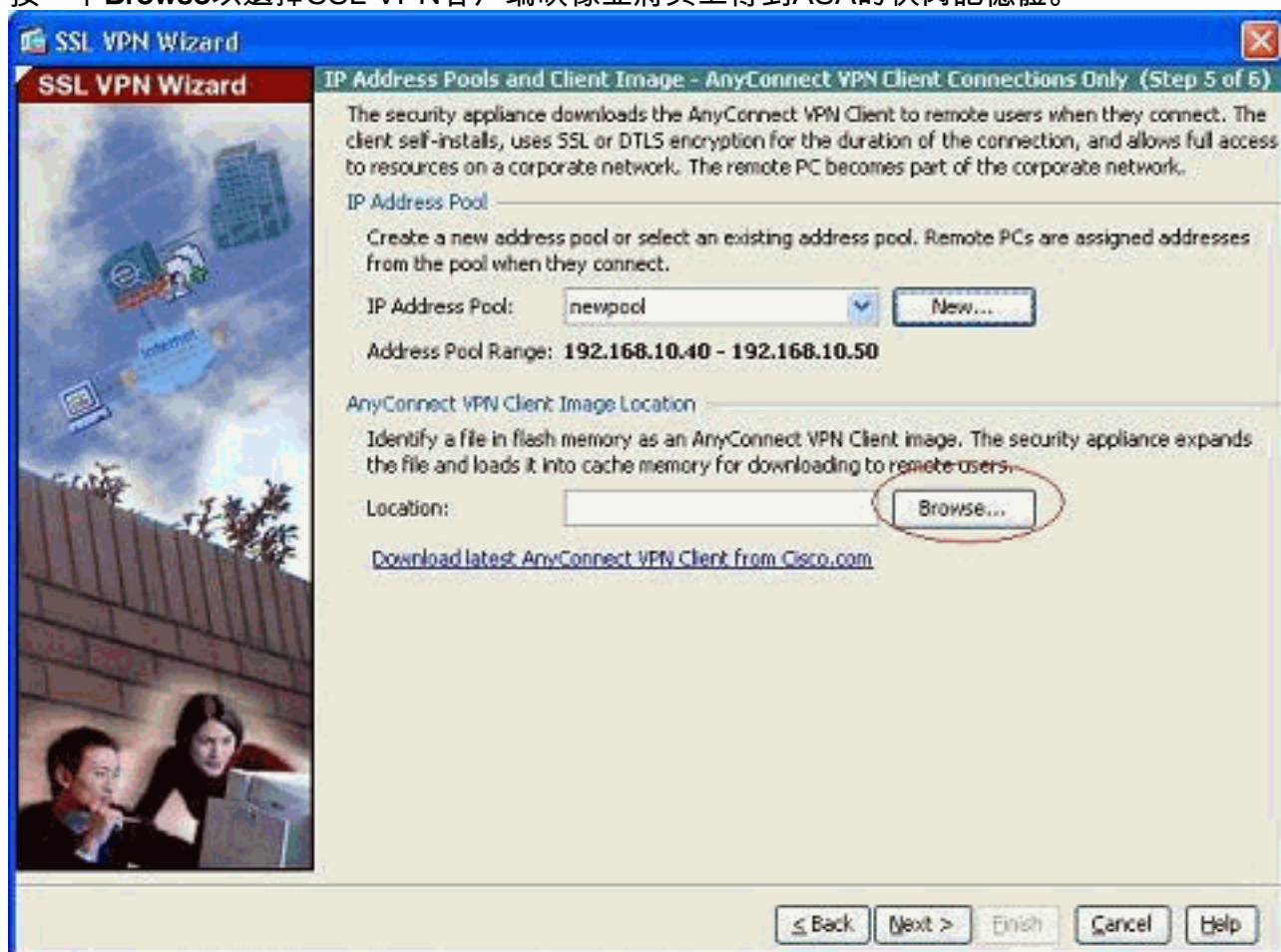
Name:

Starting IP Address:

Ending IP Address:

Subnet Mask:

8. 按一下**Browse**以選擇SSL VPN客戶端映像並將其上傳到ASA的快閃記憶體。



**SSL VPN Wizard**

**IP Address Pools and Client Image - AnyConnect VPN Client Connections Only (Step 5 of 6)**

The security appliance downloads the AnyConnect VPN Client to remote users when they connect. The client self-installs, uses SSL or DTLS encryption for the duration of the connection, and allows full access to resources on a corporate network. The remote PC becomes part of the corporate network.

IP Address Pool

Create a new address pool or select an existing address pool. Remote PCs are assigned addresses from the pool when they connect.

IP Address Pool:

Address Pool Range: **192.168.10.40 - 192.168.10.50**

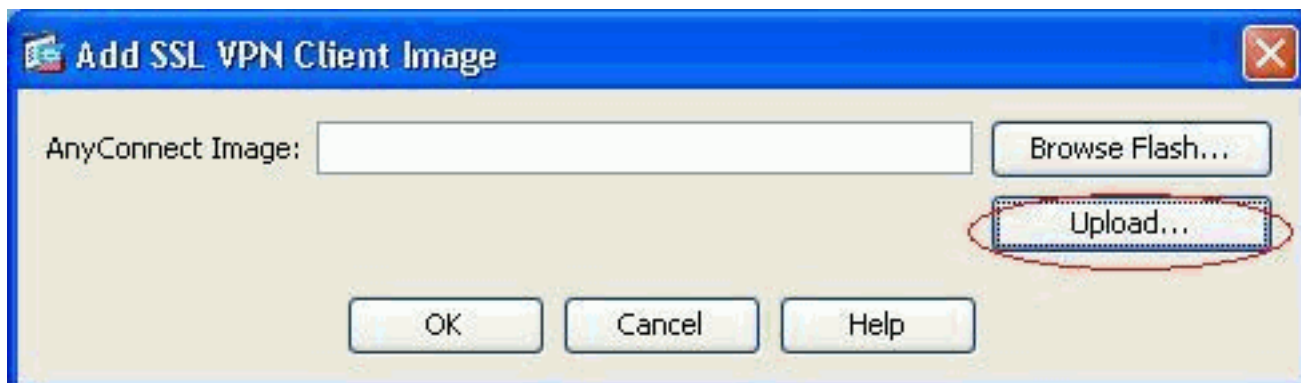
AnyConnect VPN Client Image Location

Identify a file in flash memory as an AnyConnect VPN Client image. The security appliance expands the file and loads it into cache memory for downloading to remote users.

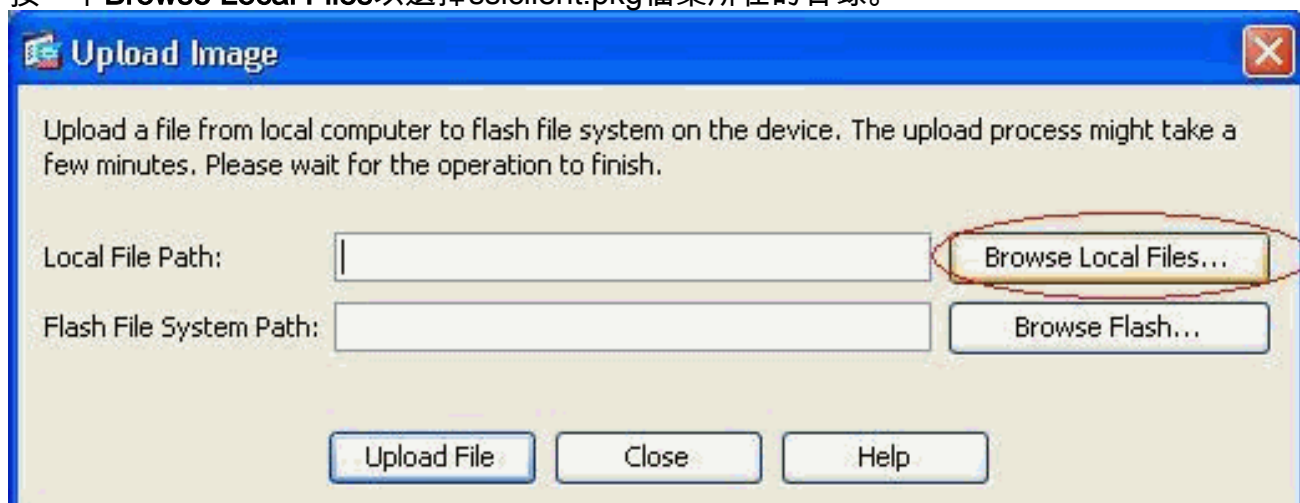
Location:

[Download latest AnyConnect VPN Client from Cisco.com](#)

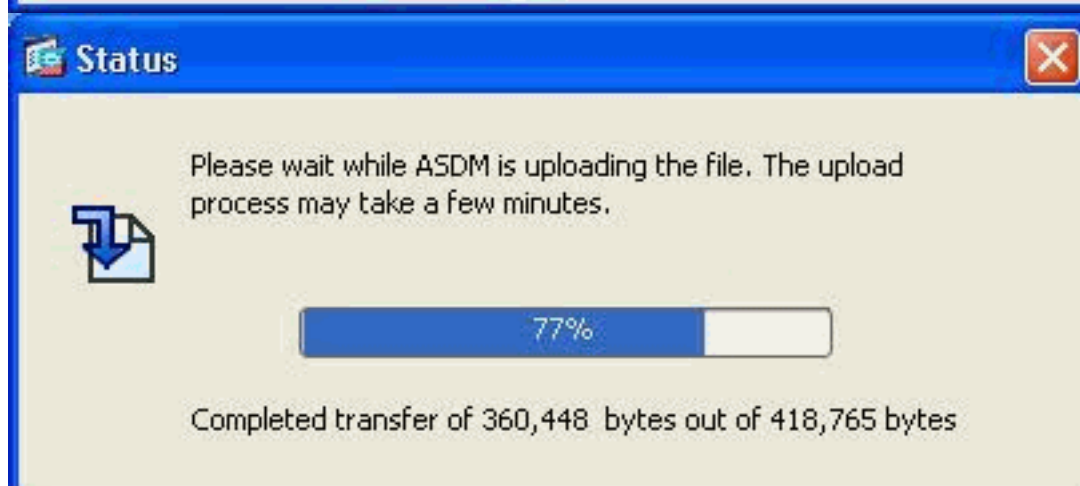
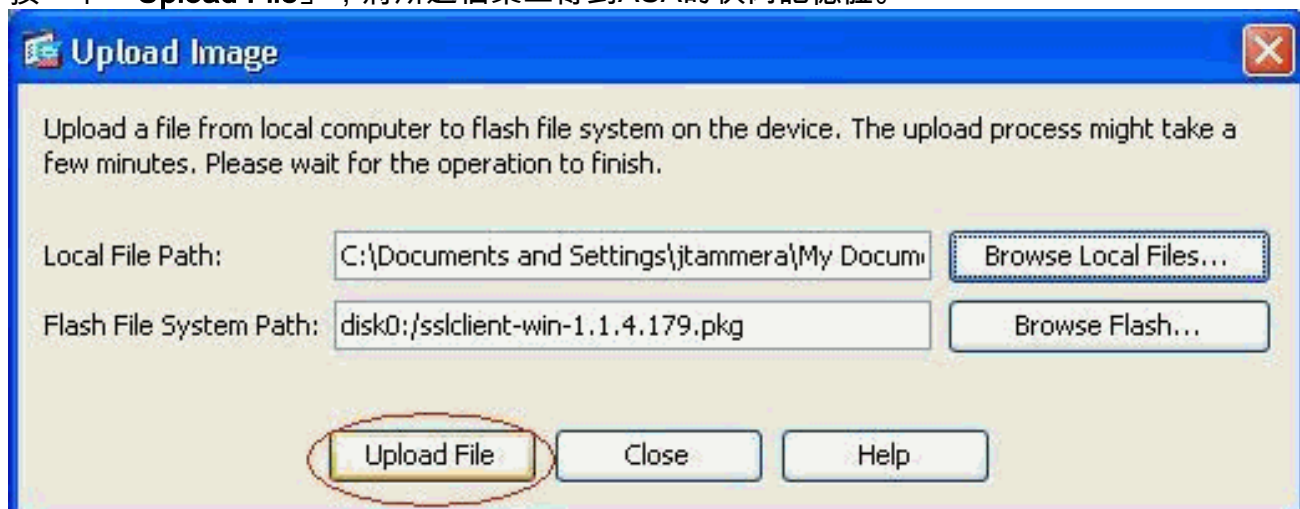
9. 按一下「**Upload**」以設定從機器本地目錄到檔案的路徑。



10. 按一下 **Browse Local Files** 以選擇 sslclient.pkg 檔案所在的目錄。



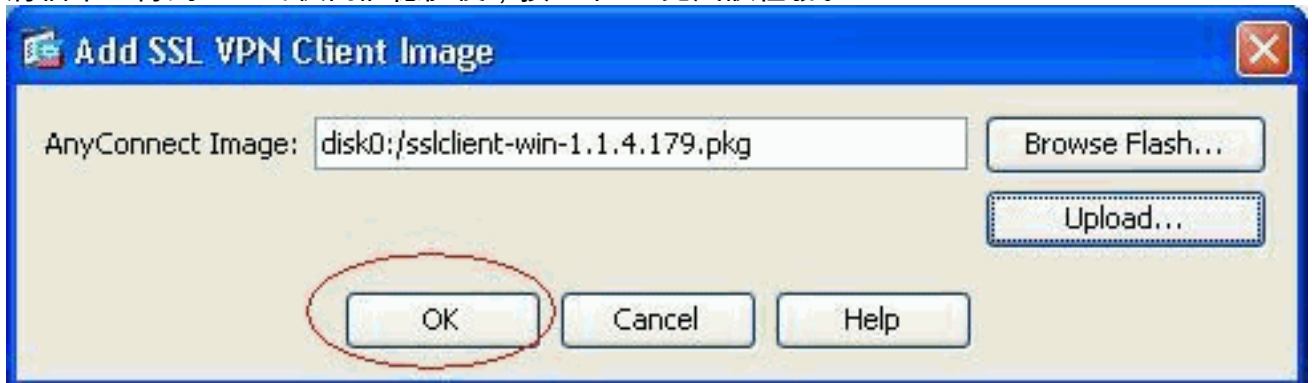
11. 按一下「**Upload File**」，將所選檔案上傳到ASA的快閃記憶體。



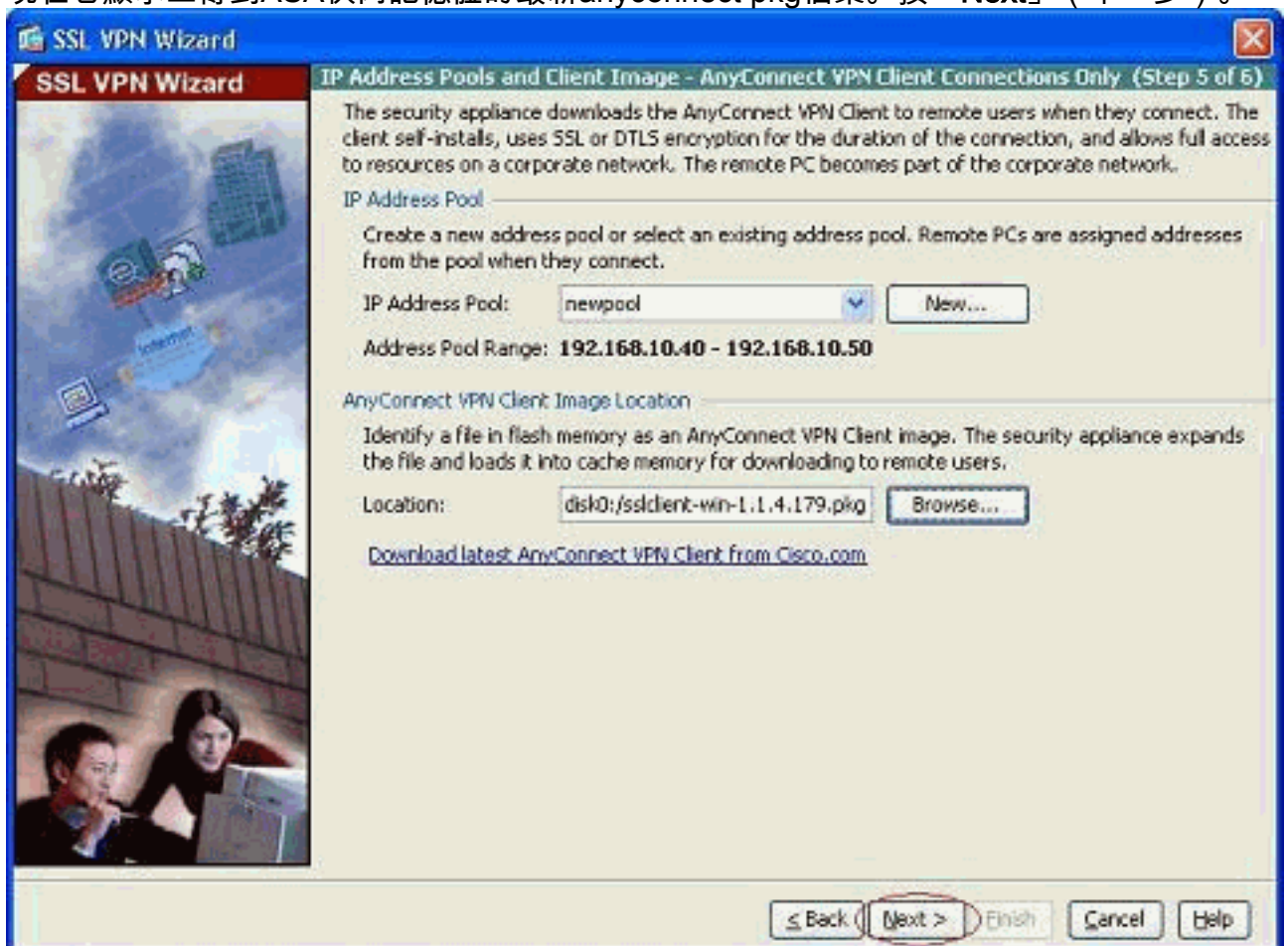




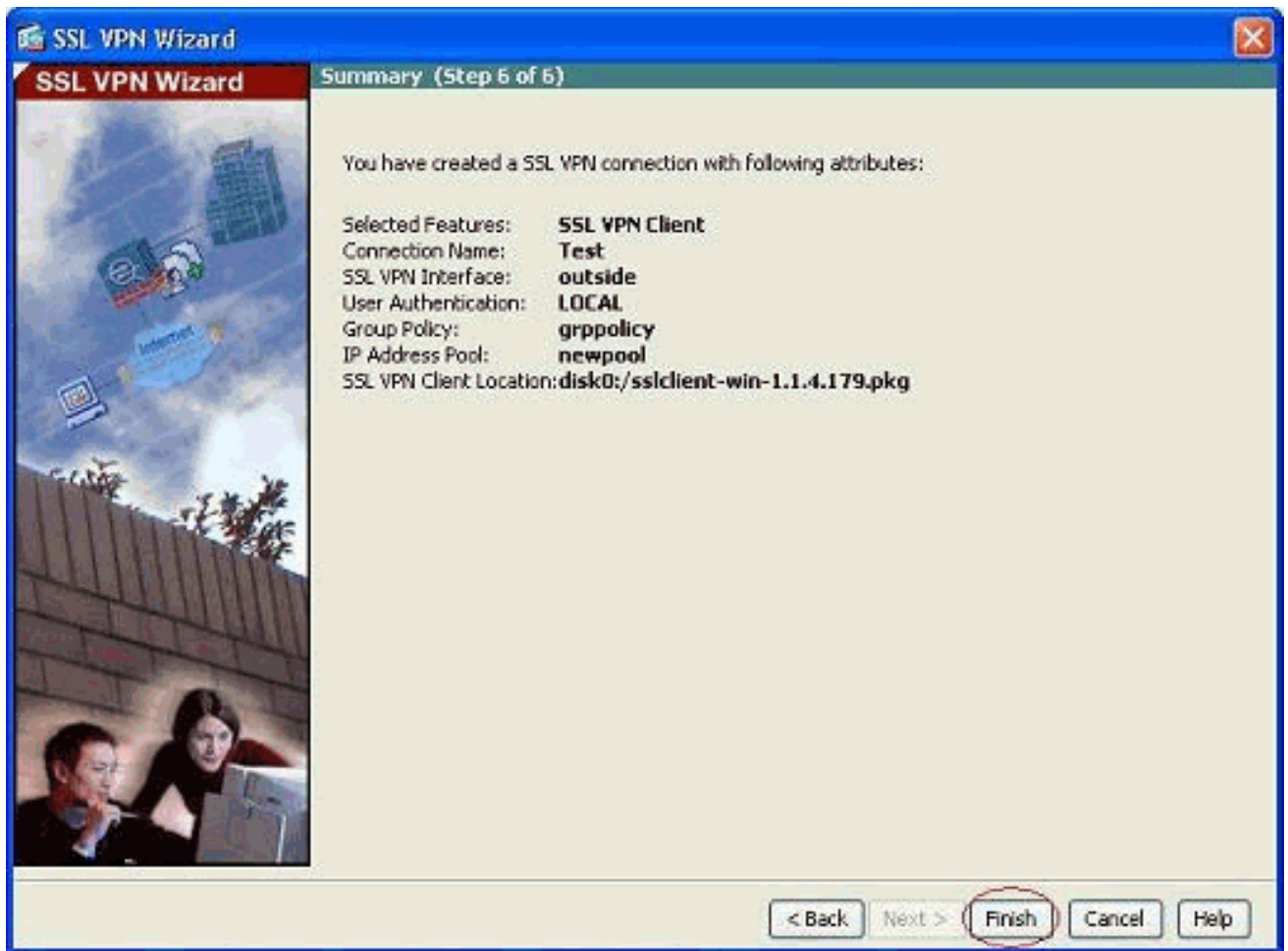
12. 將檔案上傳到ASA的快閃記憶體後，按一下OK完成該任務。



13. 現在它顯示上傳到ASA快閃記憶體的最新anyconnect pkg檔案。按「Next」（下一步）。



14. 顯示SSL VPN客戶端配置的摘要。按一下完成完成嚮導。



ASDM中顯示的配置主要與SSL VPN客戶端嚮導配置有關。

在CLI中，您可以觀察某些其他組態。下面顯示了完整的CLI配置，並突出顯示了一些重要命令。

```
ciscoasa  
  
ciscoasa#show running-config  
: Saved  
:  
ASA Version 8.0(4)  
!  
hostname ciscoasa  
enable password 8Ry2YjIyt7RRXU24 encrypted  
names  
!  
interface Ethernet0/0  
  nameif outside  
  security-level 0  
  ip address 209.165.201.2 255.255.255.224  
!  
interface Ethernet0/1  
  nameif inside  
  security-level 100  
  ip address 192.168.100.2 255.255.255.0  
!  
interface Ethernet0/2  
  nameif manage  
  security-level 0  
  ip address 10.1.1.1 255.255.255.0  
!  
interface Ethernet0/3  
  shutdown
```

```

no nameif
no security-level
no ip address
!
interface Ethernet0/4
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet0/5
shutdown
no nameif
no security-level
no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
access-list nonat extended permit ip 192.168.100.0
255.255.255.0 192.168.10.0 255.255.255.0
access-list nonat extended permit ip 192.168.10.0
255.255.255.0 192.168.100.0 255.255.255.0
!--- ACL to define the traffic to be exempted from NAT.
no pager logging enable logging asdm informational mtu
outside 1500 mtu inside 1500 mtu manage 1500 !---
Creating IP address block to be assigned for the VPN
clients ip local pool newpool 192.168.10.40-
192.168.10.50 mask 255.255.255.0
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-615.bin
no asdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 0 access-list nonat
!--- The traffic permitted in "nonat" ACL is exempted
from NAT. nat (inside) 1 192.168.100.0 255.255.255.0
route outside 0.0.0.0 0.0.0.0 209.165.201.1 1
!--- Default route is configured through "inside"
interface for normal traffic. route inside 0.0.0.0
0.0.0.0 192.168.100.20 tunneled
!--- Tunneled Default route is configured through
"inside" interface for encrypted traffic ! timeout xlate
3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00
h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip
0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-
disconnect 0:02:00 timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy http
server enable
!--- Configuring the ASA as HTTP server. http 10.1.1.0
255.255.255.0 manage
!--- Configuring the network to be allowed for ASDM
access. ! !--- Output is suppressed ! telnet timeout 5
ssh timeout 5 console timeout 0 threat-detection basic-
threat threat-detection statistics access-list ! class-
map inspection_default match default-inspection-traffic
! ! policy-map type inspect dns preset_dns_map
parameters message-length maximum 512 policy-map
global_policy class inspection_default inspect dns
preset_dns_map inspect ftp inspect h323 h225 inspect
h323 ras inspect netbios inspect rsh inspect rtsp
inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp ! service-

```

```
policy global_policy global ! !--- Output suppressed !
webvpn
  enable outside
  !--- Enable WebVPN on the outside interface svc image
  disk0:/sslclient-win-1.1.4.179.pkg 1
  !--- Assign the AnyConnect SSL VPN Client image to be
  used svc enable
  !--- Enable the ASA to download SVC images to remote
  computers group-policy grppolicy internal
  !--- Create an internal group policy "grppolicy" group-
  policy grppolicy attributes
  VPN-tunnel-protocol svc
  !--- Specify SSL as a permitted VPN tunneling protocol !
  username cisco password ffIRPGpDSOJh9YLq encrypted
  privilege 15
  !--- Create a user account "cisco" tunnel-group Test
  type remote-access
  !--- Create a tunnel group "Test" with type as remote
  access tunnel-group Test general-attributes
  address-pool newpool
  !--- Associate the address pool vpnpool created default-
  group-policy grppolicy
  !--- Associate the group policy "clientgroup" created
  prompt hostname context
  Cryptochecksum:1b247197c8ff70ee4432c13fb037854e : end
  ciscoasa#
```

## 驗證

本節給出的命令可用於驗證此配置。

[輸出直譯器工具](#)(僅供[已註冊](#)客戶使用)(OIT)支援某些show命令。使用OIT檢視show命令輸出的分析

。

- `show webvpn svc` — 顯示儲存在ASA快閃記憶體中的SVC映像。
- `show VPN-sessiondb svc` — 顯示有關當前SSL連線的資訊。

## 疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

## 相關資訊

- [Cisco 5500系列調適型安全裝置支援](#)
- [單臂公共網際網路VPN的PIX/ASA和VPN客戶端配置示例](#)
- [帶ASDM的ASA上的SSL VPN客戶端\(SVC\)配置示例](#)
- [技術支援與文件 - Cisco Systems](#)