

使用數位證書的Windows 2000和VPN 3000集中器之間的L2TP Over IPsec配置示例

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[目標](#)

[慣例](#)

[獲取根證書](#)

[獲取客戶端的身分證書](#)

[使用網路連線嚮導建立與VPN 3000的連線](#)

[配置VPN 3000 Concentrator](#)

[獲取根證書](#)

[獲取VPN 3000集中器的身分證書](#)

[配置客戶端池](#)

[配置IKE方案](#)

[配置SA](#)

[配置組和使用者的](#)

[偵錯資訊](#)

[疑難排解資訊](#)

[相關資訊](#)

簡介

本文檔介紹使用L2TP/IPSec內建客戶端從Windows 2000客戶端連線到VPN 3000集中器的分步過程。假設您使用數位證書(無證書註冊協定(CEP)的獨立根證書頒發機構(CA)來驗證與VPN集中器的連線。本檔案使用Microsoft憑證服務作為說明。請參閱[Microsoft 網站](#)，獲取有關如何配置它的文檔。

注意：這只是一個示例，因為Windows 2000螢幕的外觀可以更改。

[必要條件](#)

[需求](#)

本文件沒有特定需求。

[採用元件](#)

本文檔中的資訊適用於Cisco VPN 3000 Concentrator系列。

目標

在此過程中，請完成以下步驟：

1. 獲取根證書。
2. 獲取客戶端的身份證書。
3. 使用「網路連線嚮導」建立與VPN 3000的連線。
4. 配置VPN 3000 Concentrator。

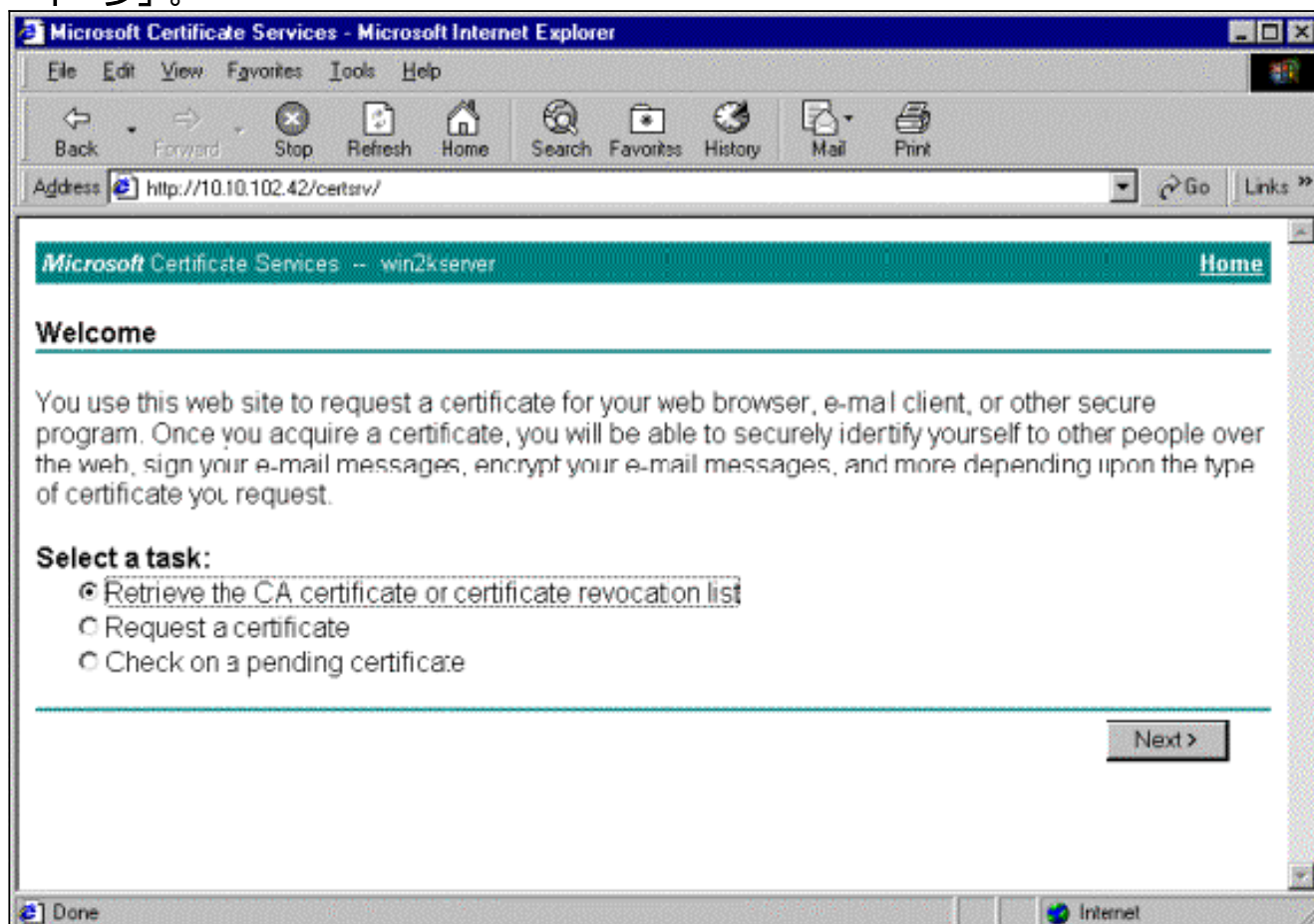
慣例

如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

獲取根證書

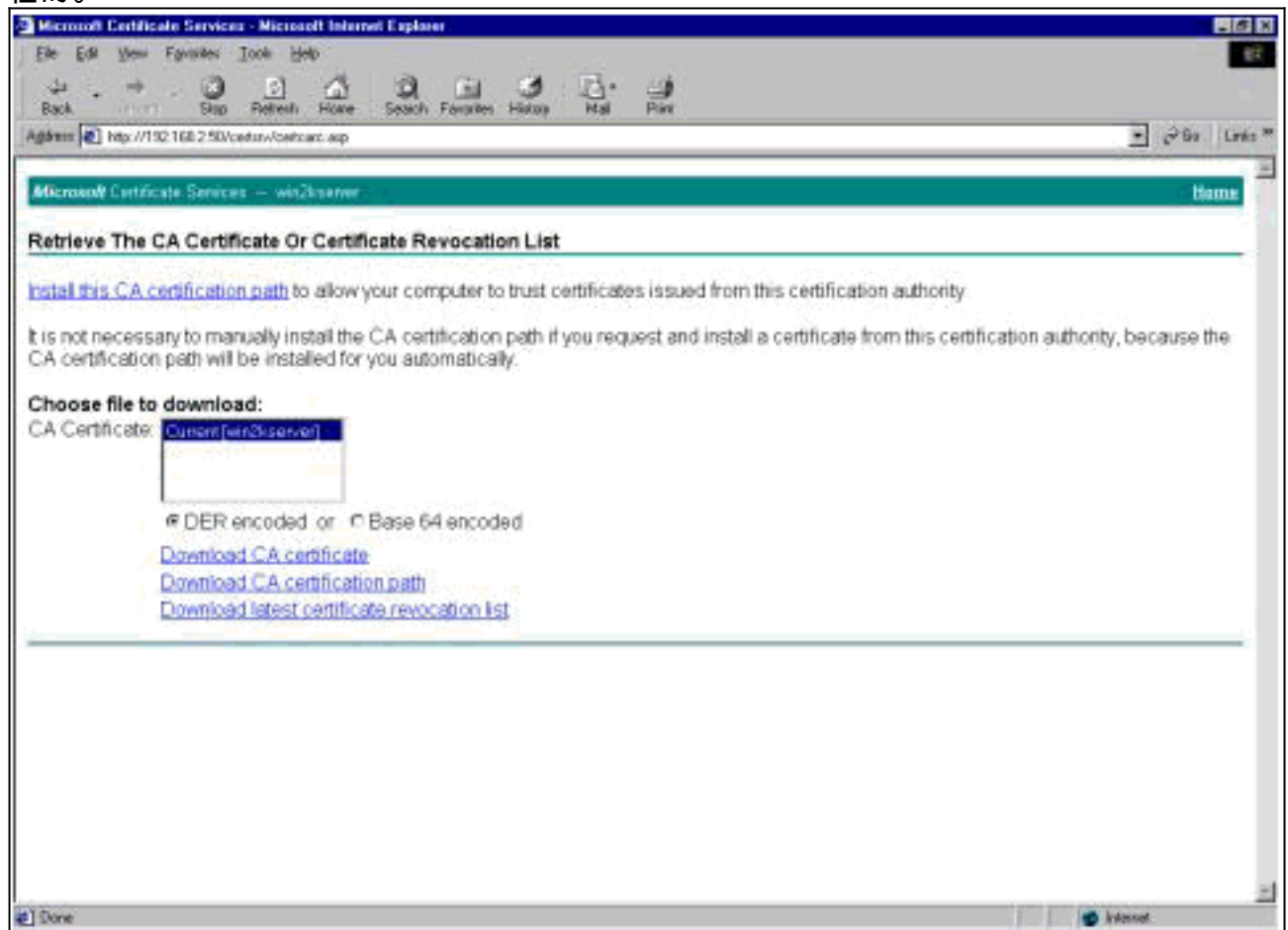
完成以下說明以取得根憑證：

1. 開啟瀏覽器視窗，輸入Microsoft證書頒發機構的URL(通常為http://servername或CA/certsrv的IP地址)。此時將顯示證書檢索和請求的歡迎視窗。
2. 在「歡迎使用」視窗的「選擇任務」下，選擇「**檢索CA證書或證書吊銷清單**」，然後按一下「**下一步**」。



3. 在「檢索CA證書或證書撤銷清單」視窗中，按一下左角的**安裝此CA證書路徑**。這會將CA證書新增到受信任的根證書頒發機構儲存中。這表示此CA頒發給此使用者端的所有憑證都是受信

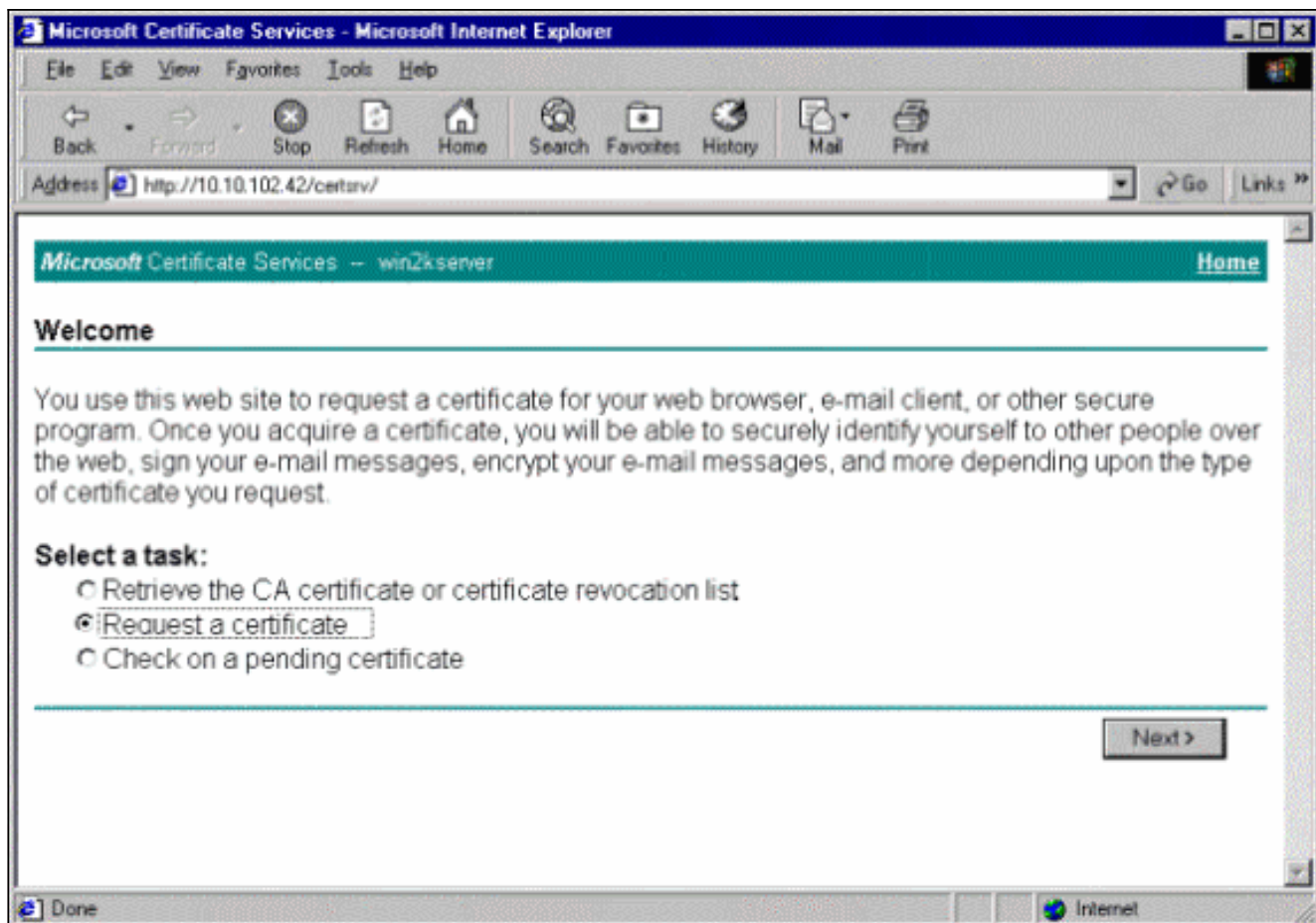
任的。



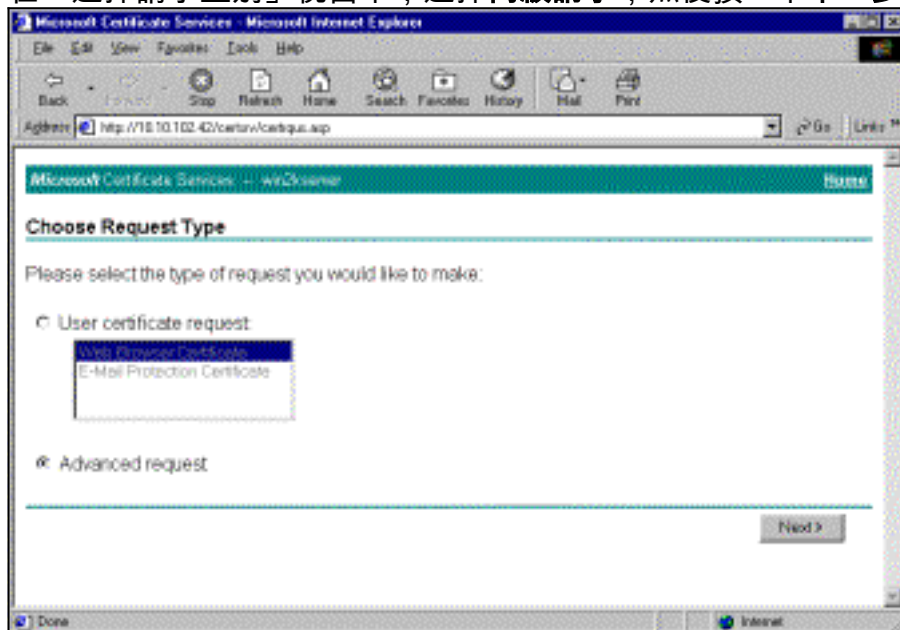
獲取客戶端的身分證書

完成以下步驟，即可取得使用者端的身分憑證：

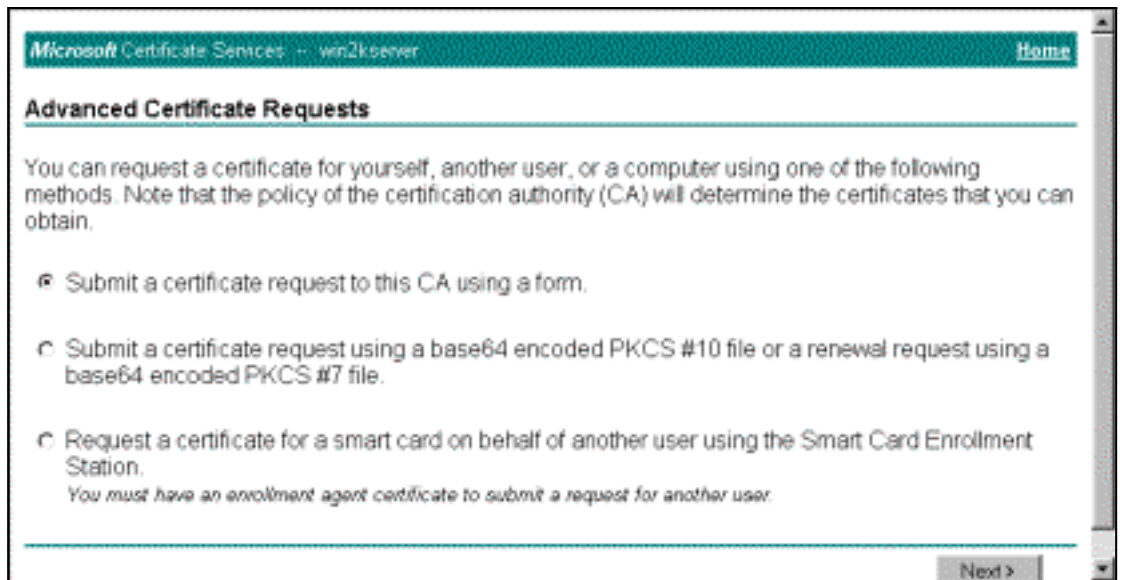
1. 開啟瀏覽器視窗，輸入Microsoft證書頒發機構的URL(通常為http://servername或CA/certsrv的IP地址)。此時將顯示證書檢索和請求的歡迎視窗。
2. 在「歡迎」視窗的「選擇任務」下，選擇「請求證書」，然後按一下下一步。



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。



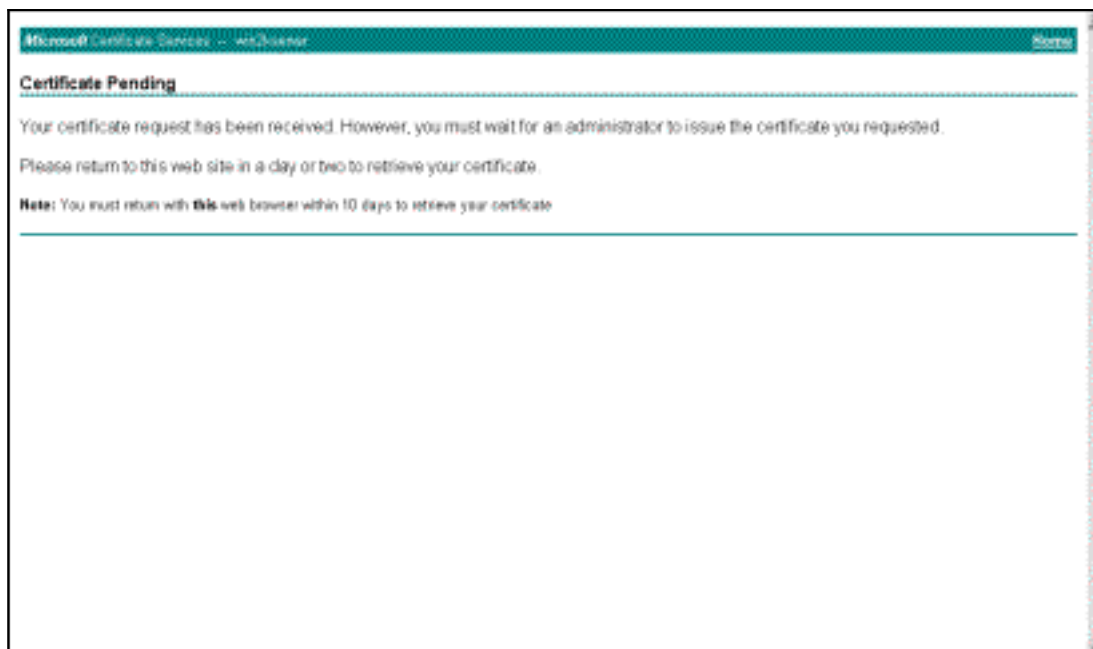
4. 在「Advanced Certificate Requests」視窗中，選擇**Submit a certificate request to this CA**



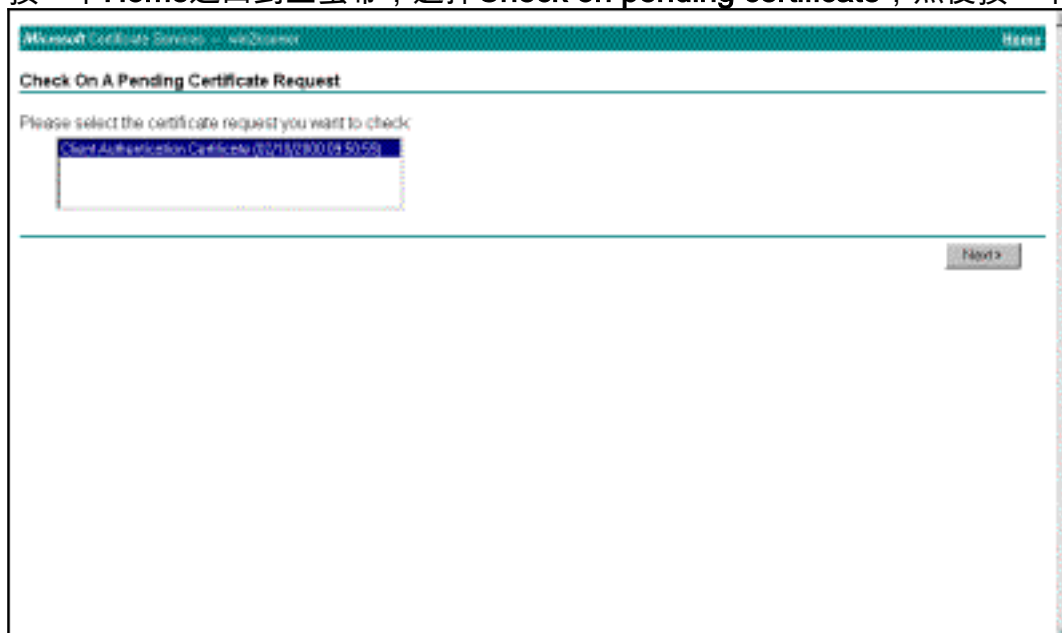
using a form.

5. 填寫欄位，如本例所示。部門（組織單位）的值需要與VPN集中器上配置的組匹配。請勿指定大於1024的金鑰大小。請務必選中**Use local machine store**覈取方塊。完成後，按一下下一步。

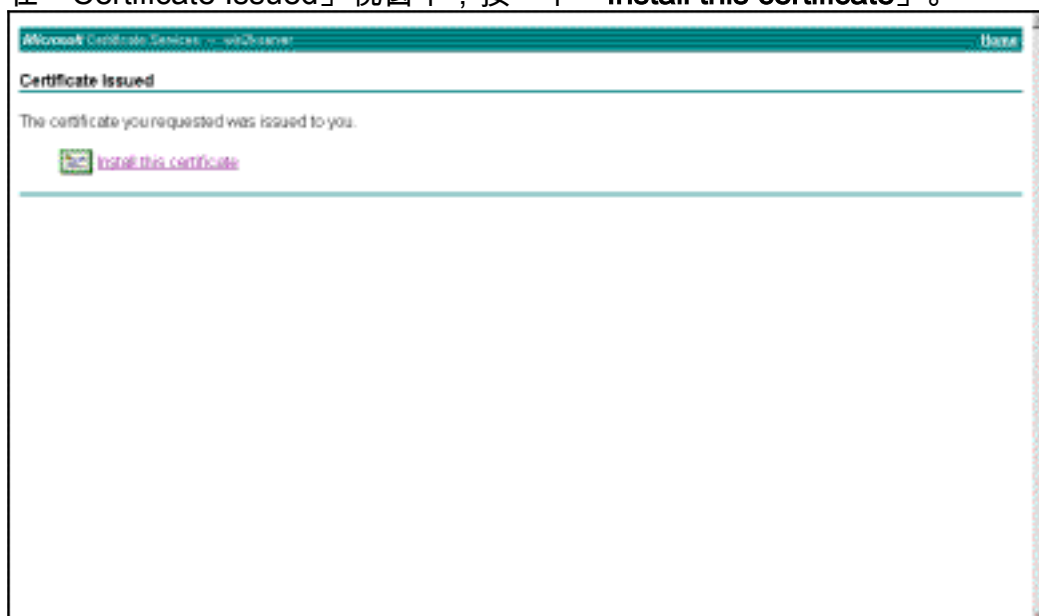
根據CA伺服器的配置，有時會出現此視窗。如果是，請聯絡CA管理員。



6. 按一下**Home**返回到主螢幕，選擇**Check on pending certificate**，然後按一下**Next**。

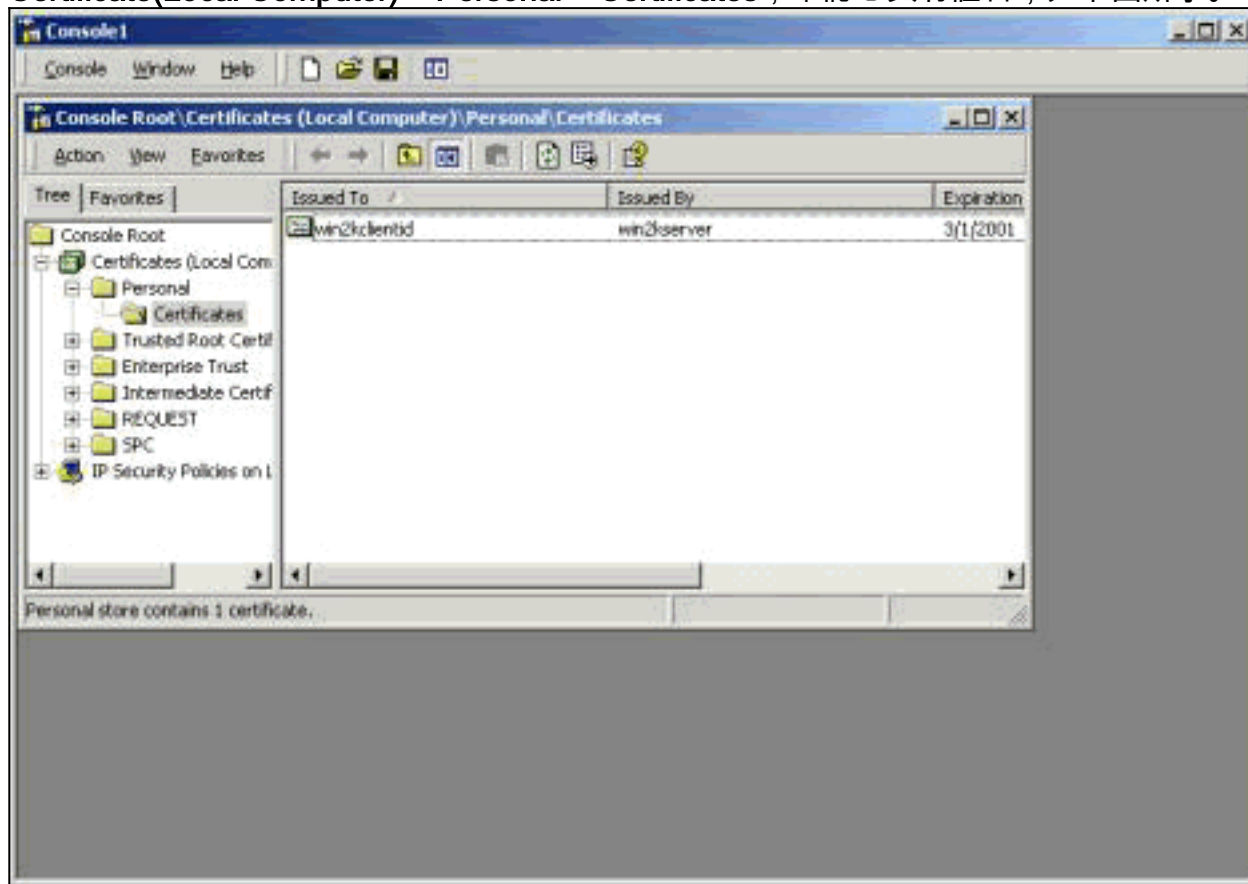


7. 在「Certificate Issued」視窗中，按一下「**Install this certificate**」。



8. 要檢視您的客戶端證書，請選擇**開始 > 運行**，然後執行Microsoft管理控制檯(MMC)。

9. 按一下**Console**，然後選擇**Add/Remove Snap-in**。
10. 按一下「**Add**」，然後從清單中選擇「**Certificate**」。
11. 當出現詢問證書範圍的視窗時，選擇**Computer Account**。
12. 驗證CA伺服器的證書是否位於受信任的根證書頒發機構下。此外，選擇**Console Root > Certificate(Local Computer) > Personal > Certificates**，確認您具有證書，如下圖所示。



使用網路連線嚮導建立與VPN 3000的連線

完成以下過程，以便藉助網路連線嚮導建立與VPN 3000的連線：

1. 按一下右鍵**My Network Places**，選擇**Properties**，然後按一下**Make New Connection**。
2. 在「**Network Connection Type (網路連線型別)**」視窗中，選擇「**Connect to a private network through the Internet (通過Internet連線到專用網路)**」，然後按一下「**Next (下一步)**」。

Network Connection Wizard

Network Connection Type

You can choose the type of network connection you want to create, based on your network configuration and your networking needs.



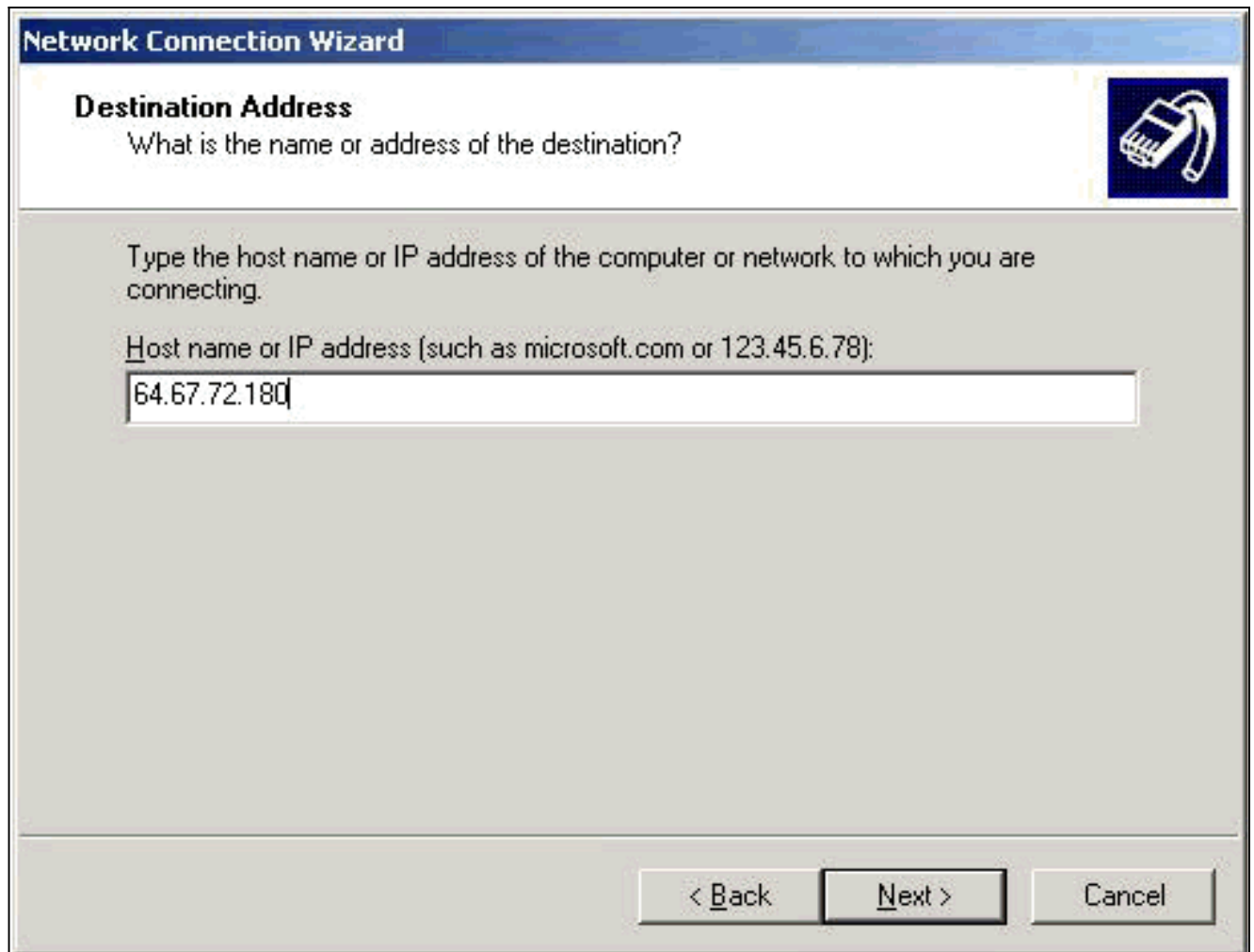
- Dial-up to private network**
Connect using my phone line (modem or ISDN).
- Dial-up to the Internet**
Connect to the Internet using my phone line (modem or ISDN).
- Connect to a private network through the Internet**
Create a Virtual Private Network (VPN) connection or 'tunnel' through the Internet.
- Accept incoming connections**
Let other computers connect to mine by phone line, the Internet, or direct cable.
- Connect directly to another computer**
Connect using my serial, parallel, or infrared port.

< Back

Next >

Cancel

3. 輸入VPN集中器的公共介面的主機名或IP地址，然後按一下下一步。



4. 在「連線可用性」視窗中，為我自己選擇Only，然後單擊Next。

Network Connection Wizard

Connection Availability

You may make the new connection available to all users, or just yourself.



You may make this connection available to all users, or keep it only for your own use. A connection stored in your profile will not be available unless you are logged on.

Create this connection:

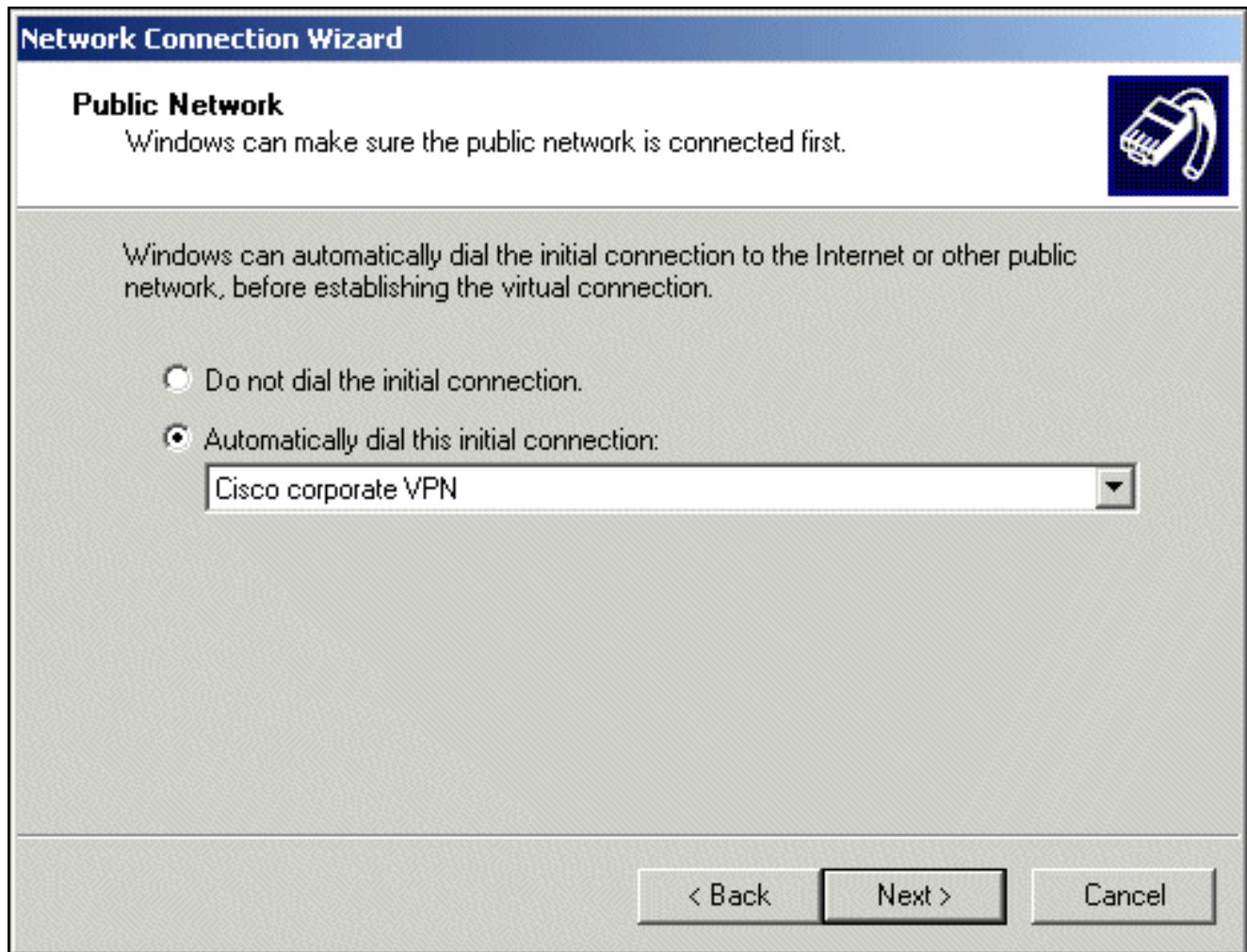
- For all users
- Only for myself

< Back

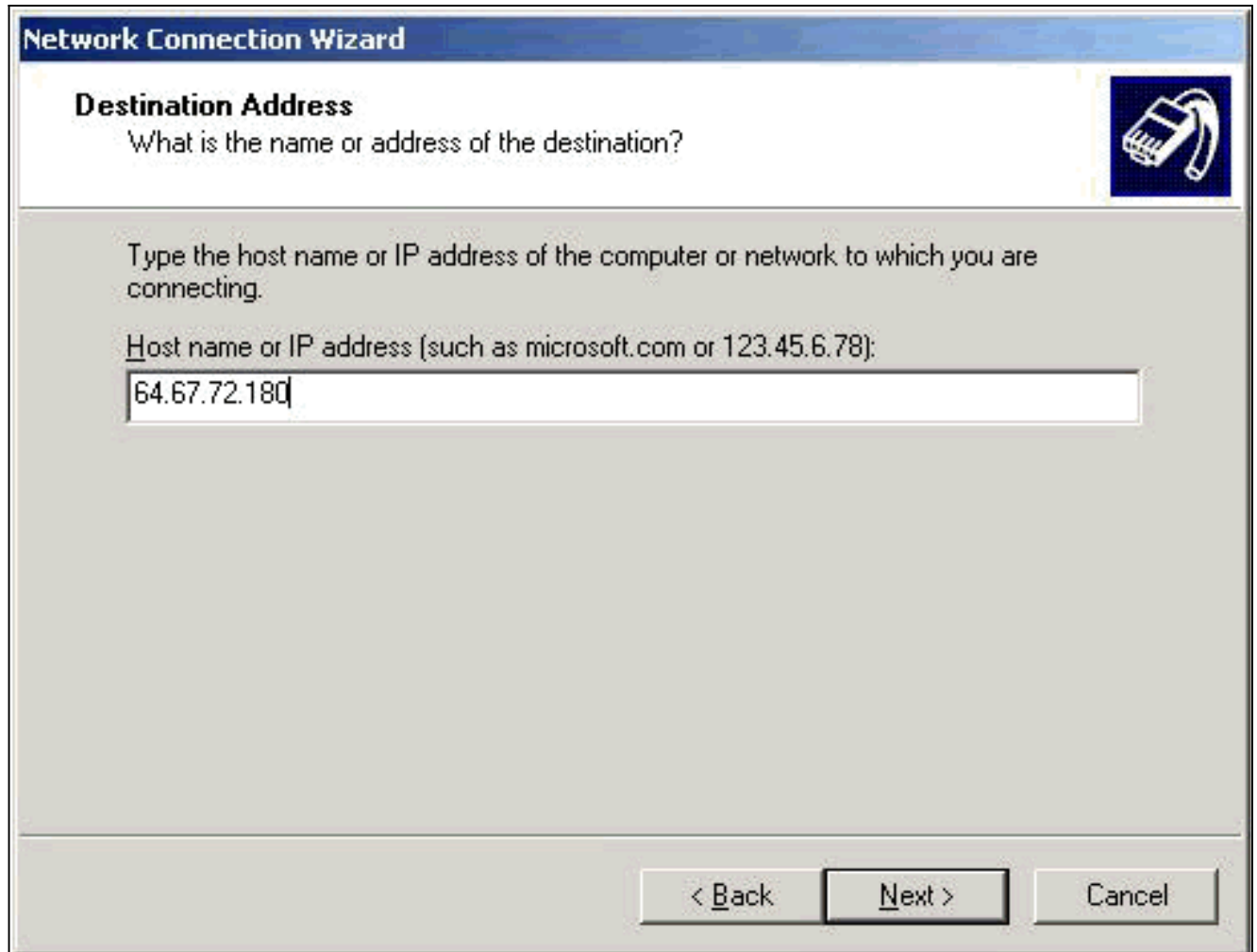
Next >

Cancel

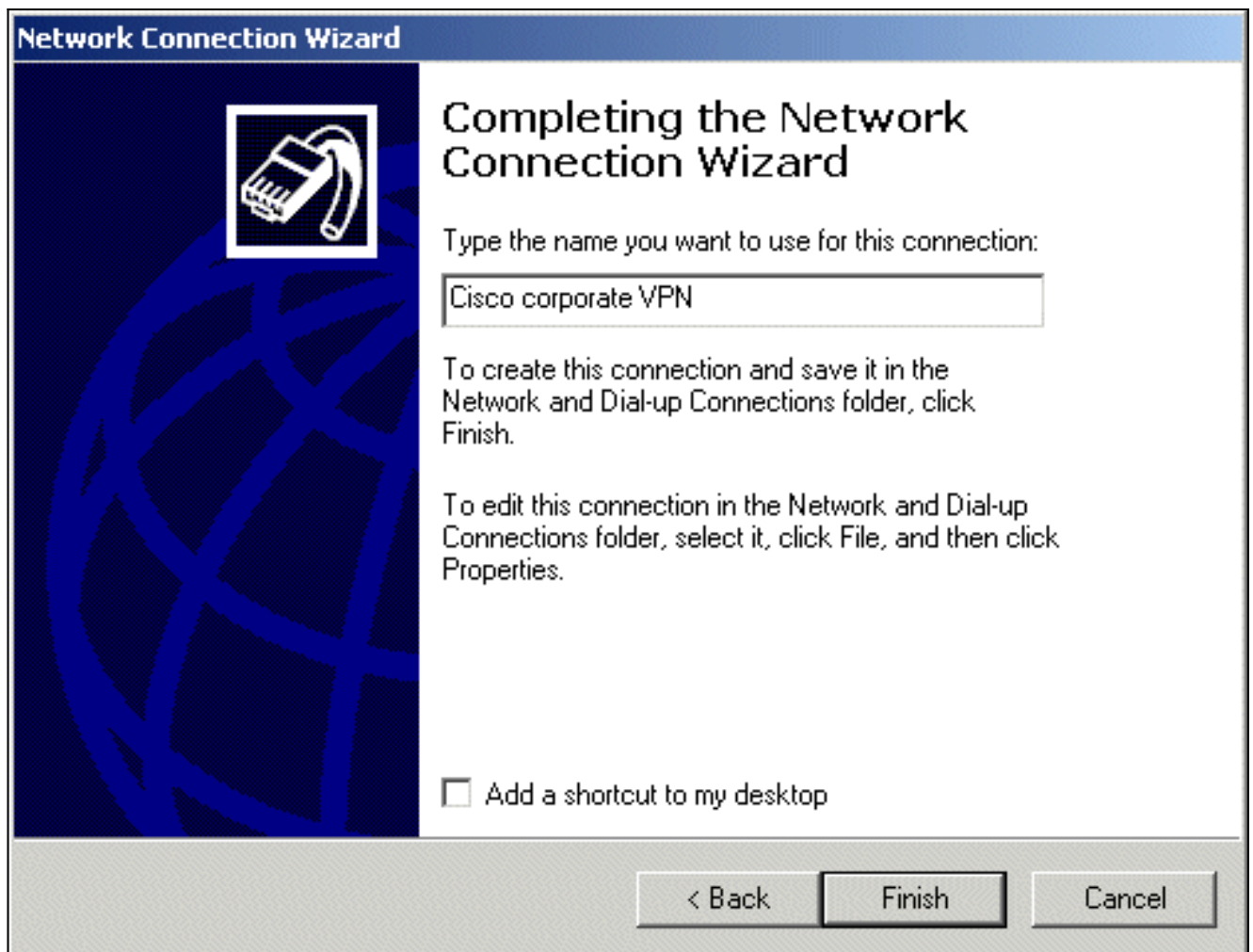
5. 在Public Network視窗中，選擇是否自動撥號初始連線（ISP帳戶）。



6. 在Destination Address螢幕上，輸入VPN 3000 Concentrator的主機名或IP地址，然後點選Next。



7. 在「網路連線嚮導」視窗中，輸入連線的名稱，然後按一下**完成**。在本示例中，連線命名為「Cisco corporate VPN」。

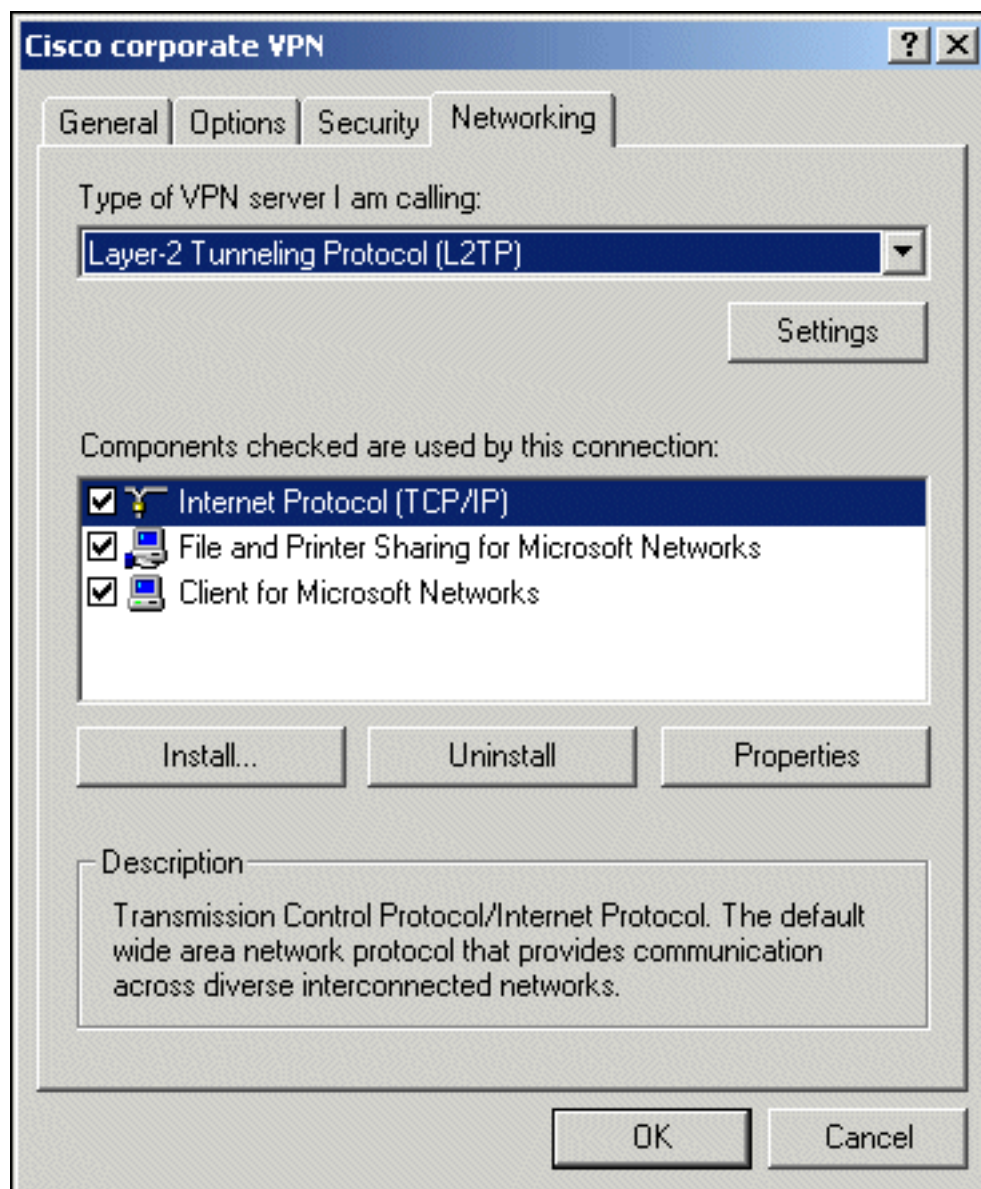


8. 在「虛擬專用連線」視窗中，按一下**屬性**。



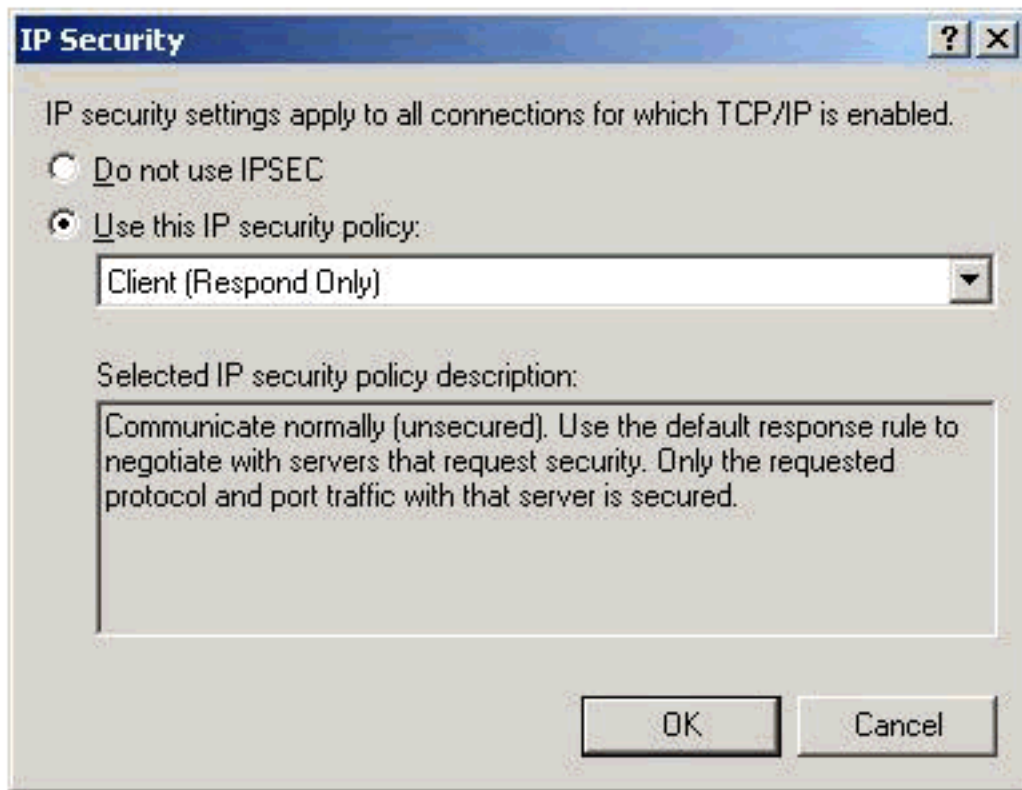
9. 在「屬性」視窗中，選擇「網路」頁籤。

10. 在Type of VPN server I am calling下，從下拉選單中選擇L2TP，選中Internet Protocol TCP/IP，然後按一下**Properties**。



11. 選擇 **Advanced > Options > Properties**。

12. 在 IP Security 視窗中，選擇 **Use this IP security policy**。



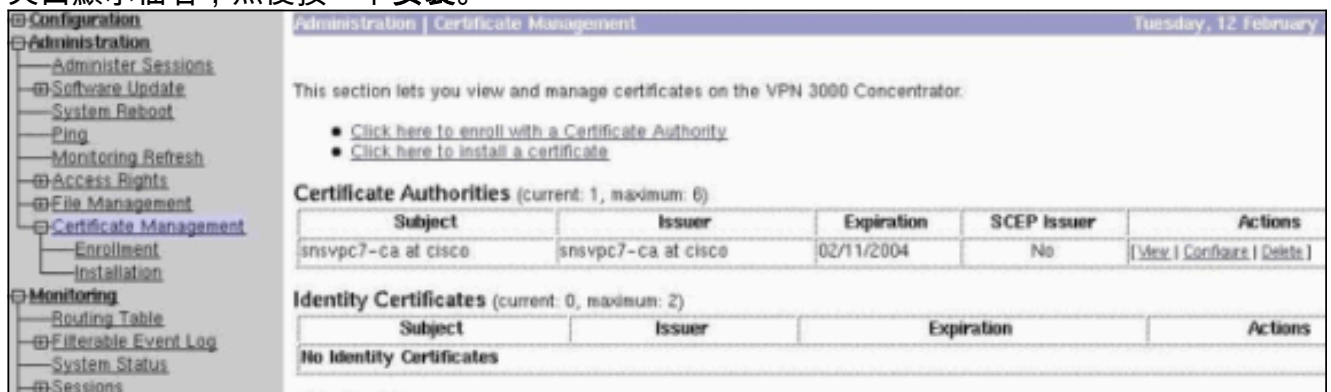
13. 從下拉選單中選擇**Client(Respond Only)**策略，然後多次按一下**OK**，直到返回Connect螢幕。
14. 若要啟動連線，請輸入您的使用者名稱和密碼，然後按一下**Connect**。

配置VPN 3000 Concentrator

獲取根證書

完成以下步驟，以便獲取VPN 3000集中器的根證書：

1. 將瀏覽器指向您的CA(通常例如http://ip_add_of_ca/certsrv/)，**檢索CA證書或證書撤銷清單**，然後按一下**下一步**。
2. 按一下「**Download CA certificate**」，將檔案儲存在本機磁碟上的某個位置。
3. 在VPN 3000 Concentrator上，選擇**Administration > Certificate Management**，然後按一下 **Click here to install a certificate**和**Install CA Certificate**。
4. 按一下「**Upload File from Workstation**」。
5. 按一下「**Browse**」，然後選擇您剛下載的CA憑證檔案。
6. 突出顯示檔名，然後按一下**安裝**。



獲取VPN 3000集中器的身份證書

完成以下步驟，以便獲取VPN 3000集中器的身份證書：

1. 選擇ConfAdministration > Certificate Management > Enroll > Identity Certificate，然後按一下 **Enroll via PKCS10 Request(Manual)**。填寫此處的表單，然後按一下註冊。

Administration | Certificate Management | Enroll | Identity Certificate | PKCS10

Enter the information to be included in the certificate request. The CA's certificate *must* be installed as a Certificate Authority before installing the certificate you requested. Please wait for the operation to finish.

Common Name (CN) Enter the common name for the VPN 3000 Concentrator to be used in this PKI.

Organizational Unit (OU) Enter the department.

Organization (O) Enter the Organization or company.

Locality (L) Enter the city or town.

State/Province (SP) Enter the State or Province.

Country (C) Enter the two-letter country abbreviation (e.g. United States = US).

Subject/AlternativeName (FQDN) Enter the Fully Qualified Domain Name for the VPN 3000 Concentrator to be used in this PKI.

Subject/AlternativeName (E-Mail Address) Enter the E-Mail Address for the VPN 3000 Concentrator to be used in this PKI.

Key Size Select the key size for the generated RSA/DSA key pair.

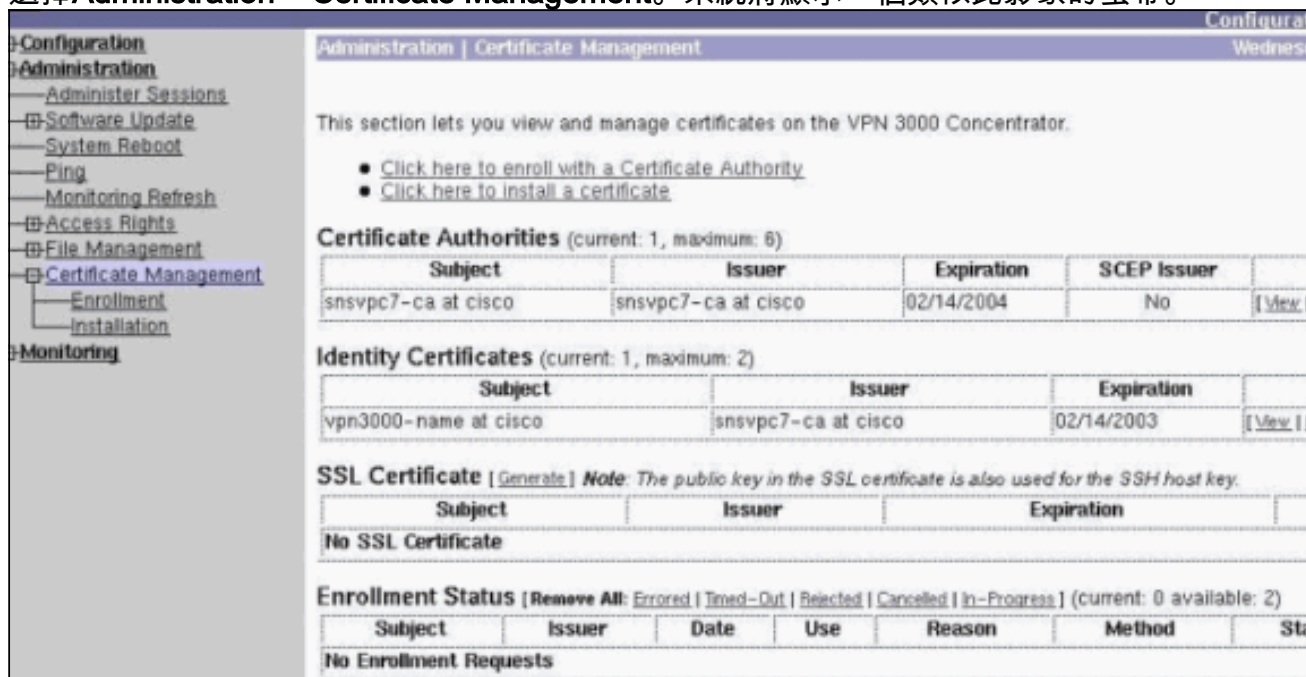
瀏覽器視窗隨證書請求彈出。它需要包含類似於以下輸出的文本：

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBPDCB5wIBADBQMRUwEwYDVQQDEwx2cG4zMdAwLW5hbWUxDDAKBgNVBAsTA3Nu
czEOMAwGA1UEChMFY2l2Y28xMDEwLW5hbWUxDDAKBgNVBACjA2J4bDELMakGA1UEBhMCYmUwWjAN
BgkqhkiG9w0BAQEFAANJADBGAkEAX7K+pve004qILNNw3kPVWXrdlqZV4yeOIPdh
C8/V5YUqq5tMWY3L1W6DC0p256bvGqzd5fhqSkOhBVnNJ1Y/KQIBA6A0MDIGCSqG
SIb3DQEJDDjE1MCMwIQYDVR0RBBAwGIIWdnBuMzAwMCl1uYW11LmNpc2NvLmNvbTAN
BgkqhkiG9w0BAQQFAANBAbzcG3IKaWnDLFtrNf1QDi+D7w8dxPu74b/BRHn9fsKI
X6+X0ed0EuEgm1/2nfj8Ux0nV5F/c5wukUfysMmJ/ak=
-----END NEW CERTIFICATE REQUEST-----
```

2. 將瀏覽器指向CA伺服器，選中Request a certificate，然後按一下Next。
3. 選中Advanced Request，按一下Next，然後選擇Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file。
4. 按「Next」（下一步）。剪下並貼上文本區域中之前顯示的證書請求的文本。按一下「Submit」。
5. 根據CA伺服器的配置方式，您可以按一下Download CA certificate。或者，CA核發憑證後，請返回您的CA伺服器，並勾選「Check on a pending certificate」。
6. 按一下下一步，選擇您的請求，然後再次按一下下一步。
7. 按一下「Download CA certificate」，將檔案儲存到本機磁碟上。
8. 在VPN 3000 Concentrator上，選擇Administration > Certificate Management > Install，然後點選Install certificate obtain via enrollment。然後您會看到狀態為「In Progress」的待處理請求，如下圖所示。



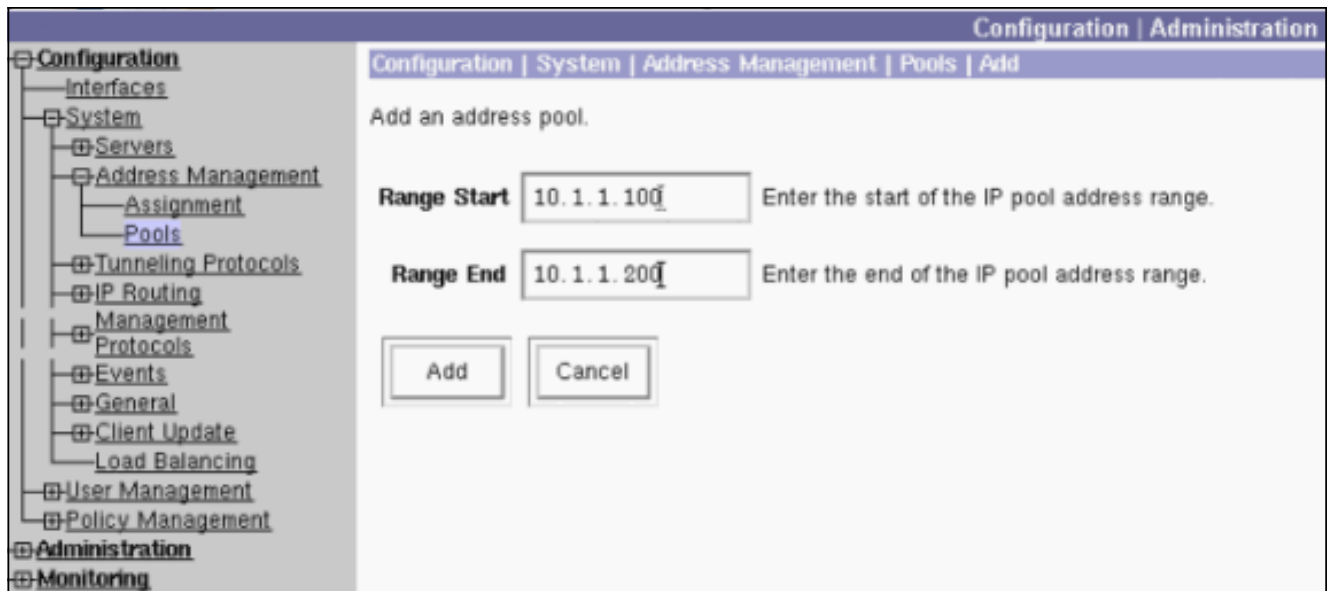
9. 按一下「Install」，然後「Upload File from Workstation」。
10. 按一下Browse，然後選擇包含CA頒發的證書的檔案。
11. 突出顯示檔名，然後按一下安裝。
12. 選擇Administration > Certificate Management。系統將顯示一個類似此影像的螢幕。



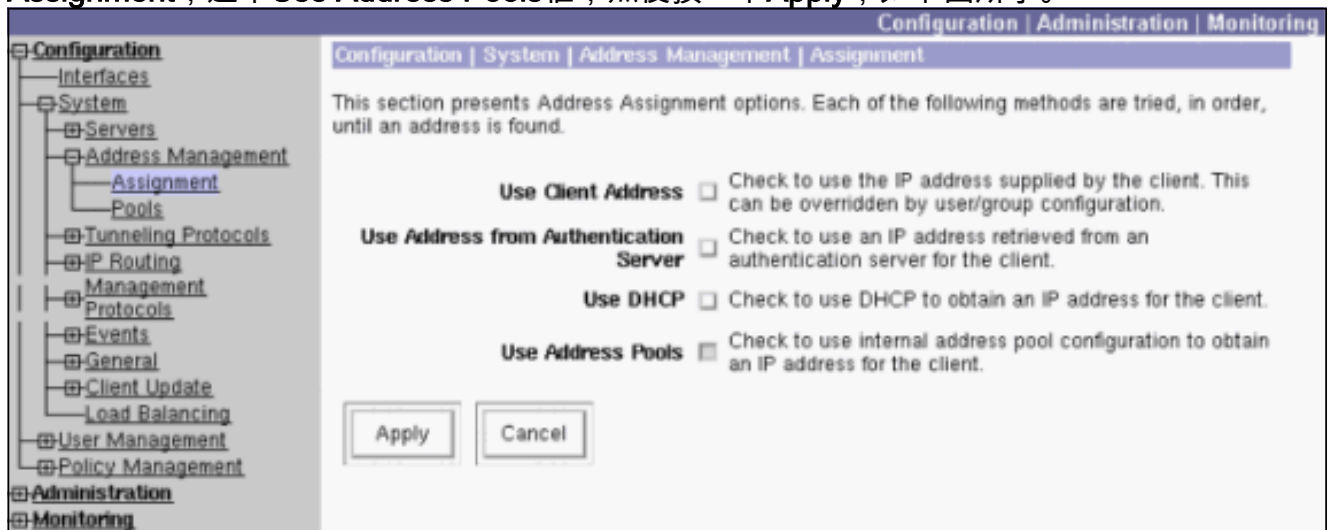
配置客戶端池

完成以下步驟即可為客戶端配置池：

1. 要分配可用的IP地址範圍，請將瀏覽器指向VPN 3000集中器的內部介面，然後選擇 **Configuration > System > Address Management > Pools > Add**。
2. 指定與內部網路上的任何其他裝置不衝突的IP地址範圍，然後按一下Add。



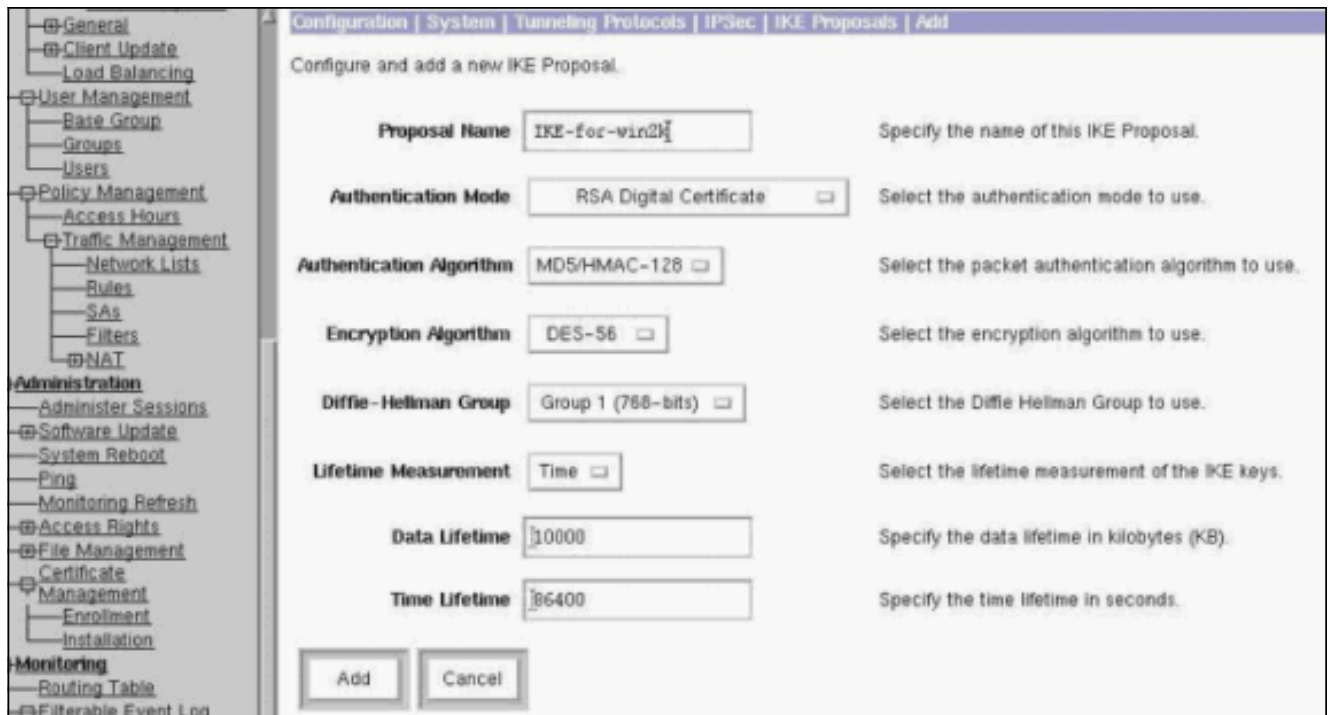
3. 要通知VPN 3000集中器使用池，請選擇Configuration > System > Address Management > Assignment，選中Use Address Pools框，然後按一下Apply，如下圖所示。



配置IKE方案

完成以下步驟以配置IKE提議：

1. 選擇Configuration > System > Tunneling Protocols > IPSec > IKE Proposals，按一下Add並選擇引數，如下圖所示。



2. 按一下**Add**，在右欄中突出顯示新建議，然後按一下**Activate**。

配置SA

完成以下步驟即可設定安全關聯(SA):

1. 選擇**Configuration > Policy Management > Traffic Management > SA**，然後按一下**ESP-L2TP-TRANSPORT**。如果此SA不可用，或者您將其用於其他用途，請建立一個類似此SA的新SA。可以接受不同的SA設定。根據您的安全策略更改此引數。
2. 在**Digital Certificate**下拉選單中選擇之前配置的數位證書。選擇**IKE-for-win2k** Internet Key Exchange(IKE)方案。**注意**：這不是強制的。當L2TP/IPSec客戶端連線到VPN集中器時，將依次嘗試在**Configuration > System > Tunneling Protocols > IPsec > IKE Proposals**頁的活動列下配置的所有IKE提議。此圖顯示SA所需的配置

:



配置組和使用者

完成以下步驟以配置組和使用者：

1. 選擇 **Configuration > User Management > Base Group**。
2. 在 General 頁籤下，確保 **L2TP over IPsec** 已選中。
3. 在 IPsec 頁籤下，選擇 **ESP-L2TP-TRANSPORT SA**。
4. 在 PPTP/L2TP 頁籤下，取消選中所有 **L2TP 加密** 選項。
5. 選擇 **Configuration > User Management > Users**，然後按一下 **Add**。
6. 輸入用於從 Windows 2000 客戶端連線的名稱和密碼。確保在「Group Selection」下選擇 **Base Group**。
7. 在 General 頁籤下，檢查 **L2TP over IPsec 通道** 協定。
8. 在 IPsec 頁籤下，選擇 **ESP-L2TP-TRANSPORT SA**。
9. 在 PPTP/L2TP 頁籤下，取消選中所有 **L2TP 加密** 選項，然後按一下 **Add**。現在您可以通過 L2TP/IPsec Windows 2000 客戶端進行連線。**注意**：您已選擇將基本組配置為接受遠端 L2TP/IPsec 連線。也可以配置與 SA 的 Organization Unit (OU) 欄位匹配的組來接受傳入連線。配置相同。

偵錯資訊

```
269 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3868 10.48.66.76
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 2
Cfg'd: Oakley Group 7
```

```
271 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3869 10.48.66.76
Phase 1 failure against global IKE proposal # 16:
```

Mismatched attr types for class DH Group:

Rcv'd: Oakley Group 2

Cfg'd: Oakley Group 1

274 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3870 10.48.66.76

Proposal # 1, Transform # 2, Type ISAKMP, Id IKE

Parsing received transform:

Phase 1 failure against global IKE proposal # 1:

Mismatched attr types for class Encryption Alg:

Rcv'd: DES-CBC

Cfg'd: Triple-DES

279 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3871 10.48.66.76

Phase 1 failure against global IKE proposal # 2:

Mismatched attr types for class Encryption Alg:

Rcv'd: DES-CBC

Cfg'd: Triple-DES

282 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3872 10.48.66.76

Phase 1 failure against global IKE proposal # 3:

Mismatched attr types for class Encryption Alg:

Rcv'd: DES-CBC

Cfg'd: Triple-DES

285 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3873 10.48.66.76

Phase 1 failure against global IKE proposal # 4:

Mismatched attr types for class DH Group:

Rcv'd: Oakley Group 2

Cfg'd: Oakley Group 1

288 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3874 10.48.66.76

Phase 1 failure against global IKE proposal # 5:

Mismatched attr types for class DH Group:

Rcv'd: Oakley Group 2

Cfg'd: Oakley Group 1

291 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3875 10.48.66.76

Phase 1 failure against global IKE proposal # 6:

Mismatched attr types for class Encryption Alg:

Rcv'd: DES-CBC

Cfg'd: Triple-DES

294 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3876 10.48.66.76

Phase 1 failure against global IKE proposal # 7:

Mismatched attr types for class Encryption Alg:

Rcv'd: DES-CBC

Cfg'd: Triple-DES

297 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3877 10.48.66.76

Phase 1 failure against global IKE proposal # 8:

Mismatched attr types for class Encryption Alg:

Rcv'd: DES-CBC

Cfg'd: Triple-DES

300 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3878 10.48.66.76

Phase 1 failure against global IKE proposal # 9:

Mismatched attr types for class Encryption Alg:

Rcv'd: DES-CBC

Cfg'd: Triple-DES

303 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3879 10.48.66.76

Phase 1 failure against global IKE proposal # 10:

Mismatched attr types for class DH Group:

Rcv'd: Oakley Group 2

Cfg'd: Oakley Group 1

306 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3880 10.48.66.76
Phase 1 failure against global IKE proposal # 11:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 2
Cfg'd: Oakley Group 1

309 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3881 10.48.66.76
Phase 1 failure against global IKE proposal # 12:
Mismatched attr types for class Encryption Alg:
Rcv'd: DES-CBC
Cfg'd: Triple-DES

312 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3882 10.48.66.76
Phase 1 failure against global IKE proposal # 13:
Mismatched attr types for class Encryption Alg:
Rcv'd: DES-CBC
Cfg'd: Triple-DES

315 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3883 10.48.66.76
Phase 1 failure against global IKE proposal # 14:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 2
Cfg'd: Oakley Group 1

318 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3884 10.48.66.76
Phase 1 failure against global IKE proposal # 15:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 2
Cfg'd: Oakley Group 7

321 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3885 10.48.66.76
Phase 1 failure against global IKE proposal # 16:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 2
Cfg'd: Oakley Group 1

324 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3886 10.48.66.76
Proposal # 1, Transform # 3, Type ISAKMP, Id IKE
Parsing received transform:
Phase 1 failure against global IKE proposal # 1:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 1
Cfg'd: Oakley Group 2

329 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3887 10.48.66.76
Phase 1 failure against global IKE proposal # 2:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 1
Cfg'd: Oakley Group 2

332 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3888 10.48.66.76
Phase 1 failure against global IKE proposal # 3:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 1
Cfg'd: Oakley Group 2

335 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3889 10.48.66.76
Phase 1 failure against global IKE proposal # 4:
Mismatched attr types for class Encryption Alg:
Rcv'd: DES-CBC
Cfg'd: Triple-DES

338 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3890 10.48.66.76
Phase 1 failure against global IKE proposal # 5:
Mismatched attr types for class Encryption Alg:
Rcv'd: DES-CBC
Cfg'd: Triple-DES

341 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3891 10.48.66.76
Phase 1 failure against global IKE proposal # 6:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 1
Cfg'd: Oakley Group 2

344 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3892 10.48.66.76
Phase 1 failure against global IKE proposal # 7:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 1
Cfg'd: Oakley Group 2

347 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3893 10.48.66.76
Phase 1 failure against global IKE proposal # 8:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 1
Cfg'd: Oakley Group 2

350 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3894 10.48.66.76
Phase 1 failure against global IKE proposal # 9:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 1
Cfg'd: Oakley Group 2

353 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3895 10.48.66.76
Phase 1 failure against global IKE proposal # 10:
Mismatched attr types for class Encryption Alg:
Rcv'd: DES-CBC
Cfg'd: Triple-DES

356 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3896 10.48.66.76
Phase 1 failure against global IKE proposal # 11:
Mismatched attr types for class Hash Alg:
Rcv'd: SHA
Cfg'd: MD5

358 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3897 10.48.66.76
Phase 1 failure against global IKE proposal # 12:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 1
Cfg'd: Oakley Group 2

361 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3898 10.48.66.76
Phase 1 failure against global IKE proposal # 13:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 1
Cfg'd: Oakley Group 2

364 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3899 10.48.66.76
Phase 1 failure against global IKE proposal # 14:
Mismatched attr types for class Encryption Alg:
Rcv'd: DES-CBC
Cfg'd: Triple-DES

367 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3900 10.48.66.76
Phase 1 failure against global IKE proposal # 15:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 1

Cfg'd: Oakley Group 7

370 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3901 10.48.66.76
Phase 1 failure against global IKE proposal # 16:
Mismatched attr types for class Hash Alg:
Rcv'd: SHA
Cfg'd: MD5

372 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3902 10.48.66.76
Proposal # 1, Transform # 4, Type ISAKMP, Id IKE
Parsing received transform:
Phase 1 failure against global IKE proposal # 1:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 1
Cfg'd: Oakley Group 2

377 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3903 10.48.66.76
Phase 1 failure against global IKE proposal # 2:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 1
Cfg'd: Oakley Group 2

380 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3904 10.48.66.76
Phase 1 failure against global IKE proposal # 3:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 1
Cfg'd: Oakley Group 2

383 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3905 10.48.66.76
Phase 1 failure against global IKE proposal # 4:
Mismatched attr types for class Encryption Alg:
Rcv'd: DES-CBC
Cfg'd: Triple-DES

386 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3906 10.48.66.76
Phase 1 failure against global IKE proposal # 5:
Mismatched attr types for class Encryption Alg:
Rcv'd: DES-CBC
Cfg'd: Triple-DES

389 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3907 10.48.66.76
Phase 1 failure against global IKE proposal # 6:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 1
Cfg'd: Oakley Group 2

392 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3908 10.48.66.76
Phase 1 failure against global IKE proposal # 7:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 1
Cfg'd: Oakley Group 2

395 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3909 10.48.66.76
Phase 1 failure against global IKE proposal # 8:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 1
Cfg'd: Oakley Group 2

398 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3910 10.48.66.76
Phase 1 failure against global IKE proposal # 9:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 1
Cfg'd: Oakley Group 2

401 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3911 10.48.66.76
Phase 1 failure against global IKE proposal # 10:
Mismatched attr types for class Encryption Alg:
Rcv'd: DES-CBC
Cfg'd: Triple-DES

404 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3912 10.48.66.76
Phase 1 failure against global IKE proposal # 11:
Mismatched attr types for class Auth Method:
Rcv'd: RSA signature with Certificates
Cfg'd: Preshared Key

407 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3913 10.48.66.76
Phase 1 failure against global IKE proposal # 12:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 1
Cfg'd: Oakley Group 2

410 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3914 10.48.66.76
Phase 1 failure against global IKE proposal # 13:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 1
Cfg'd: Oakley Group 2

413 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3915 10.48.66.76
Phase 1 failure against global IKE proposal # 14:
Mismatched attr types for class Encryption Alg:
Rcv'd: DES-CBC
Cfg'd: Triple-DES

416 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3916 10.48.66.76
Phase 1 failure against global IKE proposal # 15:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 1
Cfg'd: Oakley Group 7

419 02/15/2002 12:47:24.430 SEV=7 IKEDBG/28 RPT=20 10.48.66.76
IKE SA Proposal # 1, Transform # 4 acceptable
Matches global IKE entry # 16

420 02/15/2002 12:47:24.440 SEV=9 IKEDBG/0 RPT=3917 10.48.66.76
constructing ISA_SA for isakmp

421 02/15/2002 12:47:24.490 SEV=8 IKEDBG/0 RPT=3918 10.48.66.76
SENDING Message (msgid=0) with payloads :
HDR + SA (1) + NONE (0) ... total length : 80

423 02/15/2002 12:47:24.540 SEV=8 IKEDBG/0 RPT=3919 10.48.66.76
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152

425 02/15/2002 12:47:24.540 SEV=8 IKEDBG/0 RPT=3920 10.48.66.76
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152

427 02/15/2002 12:47:24.540 SEV=9 IKEDBG/0 RPT=3921 10.48.66.76
processing ke payload

428 02/15/2002 12:47:24.540 SEV=9 IKEDBG/0 RPT=3922 10.48.66.76
processing ISA_KE

429 02/15/2002 12:47:24.540 SEV=9 IKEDBG/1 RPT=104 10.48.66.76
processing nonce payload

430 02/15/2002 12:47:24.600 SEV=9 IKEDBG/0 RPT=3923 10.48.66.76
constructing ke payload

431 02/15/2002 12:47:24.600 SEV=9 IKEDBG/1 RPT=105 10.48.66.76
constructing nonce payload

432 02/15/2002 12:47:24.600 SEV=9 IKEDBG/0 RPT=3924 10.48.66.76
constructing certreq payload

433 02/15/2002 12:47:24.600 SEV=9 IKEDBG/0 RPT=3925 10.48.66.76
Using initiator's certreq payload data

434 02/15/2002 12:47:24.600 SEV=9 IKEDBG/46 RPT=61 10.48.66.76
constructing Cisco Unity VID payload

435 02/15/2002 12:47:24.600 SEV=9 IKEDBG/46 RPT=62 10.48.66.76
constructing xauth V6 VID payload

436 02/15/2002 12:47:24.600 SEV=9 IKEDBG/48 RPT=39 10.48.66.76
Send IOS VID

437 02/15/2002 12:47:24.600 SEV=9 IKEDBG/38 RPT=20 10.48.66.76
Constructing VPN 3000 spoofing IOS Vendor ID payload
(version: 1.0.0, capabilities: 20000001)

439 02/15/2002 12:47:24.600 SEV=9 IKEDBG/46 RPT=63 10.48.66.76
constructing VID payload

440 02/15/2002 12:47:24.600 SEV=9 IKEDBG/48 RPT=40 10.48.66.76
Send Altiga GW VID

441 02/15/2002 12:47:24.600 SEV=9 IKEDBG/0 RPT=3926 10.48.66.76
Generating keys for Responder...

442 02/15/2002 12:47:24.610 SEV=8 IKEDBG/0 RPT=3927 10.48.66.76
SENDING Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + CERT_REQ (7) + VENDOR (13) + VENDOR (13)
+ VENDOR (13) + VENDOR (13) + NONE (0) ... total length : 229

445 02/15/2002 12:47:24.640 SEV=8 IKEDBG/0 RPT=3928 10.48.66.76
RECEIVED Message (msgid=0) with payloads :
HDR + ID (5) + CERT (6) + SIG (9) + CERT_REQ (7) + NONE (0)
... total length : 1186

448 02/15/2002 12:47:24.640 SEV=9 IKEDBG/1 RPT=106 10.48.66.76
Processing ID

449 02/15/2002 12:47:24.640 SEV=9 IKEDBG/0 RPT=3929 10.48.66.76
processing cert payload

450 02/15/2002 12:47:24.640 SEV=9 IKEDBG/1 RPT=107 10.48.66.76
processing RSA signature

451 02/15/2002 12:47:24.640 SEV=9 IKEDBG/0 RPT=3930 10.48.66.76
computing hash

452 02/15/2002 12:47:24.650 SEV=9 IKEDBG/0 RPT=3931 10.48.66.76
processing cert request payload

453 02/15/2002 12:47:24.650 SEV=9 IKEDBG/0 RPT=3932 10.48.66.76
Storing cert request payload for use in MM msg 4

454 02/15/2002 12:47:24.650 SEV=9 IKEDBG/23 RPT=20 10.48.66.76
Starting group lookup for peer 10.48.66.76

455 02/15/2002 12:47:24.650 SEV=9 IKE/21 RPT=12 10.48.66.76
No Group found by matching IP Address of Cert peer 10.48.66.76

456 02/15/2002 12:47:24.650 SEV=9 IKE/20 RPT=12 10.48.66.76
No Group found by matching OU(s) from ID payload:
ou=sns,

457 02/15/2002 12:47:24.650 SEV=9 IKE/0 RPT=12 10.48.66.76
Group [VPNC_Base_Group]
No Group name for IKE Cert session, defaulting to BASE GROUP

459 02/15/2002 12:47:24.750 SEV=7 IKEDBG/0 RPT=3933 10.48.66.76
Group [VPNC_Base_Group]
Found Phase 1 Group (VPNC_Base_Group)

460 02/15/2002 12:47:24.750 SEV=7 IKEDBG/14 RPT=20 10.48.66.76
Group [VPNC_Base_Group]
Authentication configured for Internal

461 02/15/2002 12:47:24.750 SEV=9 IKEDBG/19 RPT=20 10.48.66.76
Group [VPNC_Base_Group]
IKEGetUserAttributes: default domain = fenetwork.com

462 02/15/2002 12:47:24.770 SEV=5 IKE/79 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
Validation of certificate successful
(CN=my_name, SN=6102861F000000000005)

464 02/15/2002 12:47:24.770 SEV=7 IKEDBG/0 RPT=3934 10.48.66.76
Group [VPNC_Base_Group]
peer ID type 9 received (DER_ASN1_DN)

465 02/15/2002 12:47:24.770 SEV=9 IKEDBG/1 RPT=108 10.48.66.76
Group [VPNC_Base_Group]
constructing ID

466 02/15/2002 12:47:24.770 SEV=9 IKEDBG/0 RPT=3935 10.48.66.76
Group [VPNC_Base_Group]
constructing cert payload

467 02/15/2002 12:47:24.770 SEV=9 IKEDBG/1 RPT=109 10.48.66.76
Group [VPNC_Base_Group]
constructing RSA signature

468 02/15/2002 12:47:24.770 SEV=9 IKEDBG/0 RPT=3936 10.48.66.76
Group [VPNC_Base_Group]
computing hash

469 02/15/2002 12:47:24.800 SEV=9 IKEDBG/46 RPT=64 10.48.66.76
Group [VPNC_Base_Group]
constructing dpd vid payload

470 02/15/2002 12:47:24.800 SEV=8 IKEDBG/0 RPT=3937 10.48.66.76
SENDING Message (msgid=0) with payloads :
HDR + ID (5) + CERT (6) + SIG (9) + VENDOR (13) + NONE (0)
... total length : 1112

473 02/15/2002 12:47:24.800 SEV=4 IKE/119 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
PHASE 1 COMPLETED

474 02/15/2002 12:47:24.800 SEV=6 IKE/121 RPT=4 10.48.66.76
Keep-alive type for this connection: None

475 02/15/2002 12:47:24.800 SEV=6 IKE/122 RPT=4 10.48.66.76
Keep-alives configured on but peer does not support keep-alives (type = None)

476 02/15/2002 12:47:24.800 SEV=7 IKEDBG/0 RPT=3938 10.48.66.76
Group [VPNC_Base_Group]
Starting phase 1 rekey timer: 21600000 (ms)

477 02/15/2002 12:47:24.810 SEV=8 IKEDBG/0 RPT=3939 10.48.66.76
RECEIVED Message (msgid=781ceadc) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0)
... total length : 1108

480 02/15/2002 12:47:24.810 SEV=9 IKEDBG/0 RPT=3940 10.48.66.76
Group [VPNC_Base_Group]
processing hash

481 02/15/2002 12:47:24.810 SEV=9 IKEDBG/0 RPT=3941 10.48.66.76
Group [VPNC_Base_Group]
processing SA payload

482 02/15/2002 12:47:24.810 SEV=9 IKEDBG/1 RPT=110 10.48.66.76
Group [VPNC_Base_Group]
processing nonce payload

483 02/15/2002 12:47:24.810 SEV=9 IKEDBG/1 RPT=111 10.48.66.76
Group [VPNC_Base_Group]
Processing ID

484 02/15/2002 12:47:24.810 SEV=5 IKE/25 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
Received remote Proxy Host data in ID Payload:
Address 10.48.66.76, Protocol 17, Port 1701

487 02/15/2002 12:47:24.810 SEV=9 IKEDBG/1 RPT=112 10.48.66.76
Group [VPNC_Base_Group]
Processing ID

488 02/15/2002 12:47:24.810 SEV=5 IKE/24 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
Received local Proxy Host data in ID Payload:
Address 10.48.66.109, Protocol 17, Port 0

491 02/15/2002 12:47:24.810 SEV=8 IKEDBG/0 RPT=3942
QM IsRekeyed old sa not found by addr

492 02/15/2002 12:47:24.810 SEV=5 IKE/66 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
IKE Remote Peer configured for SA: ESP-L2TP-TRANSPORT

493 02/15/2002 12:47:24.810 SEV=9 IKEDBG/0 RPT=3943 10.48.66.76
Group [VPNC_Base_Group]
processing IPSEC SA

494 02/15/2002 12:47:24.810 SEV=7 IKEDBG/27 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
IPSec SA Proposal # 1, Transform # 1 acceptable

495 02/15/2002 12:47:24.810 SEV=7 IKEDBG/0 RPT=3944 10.48.66.76
Group [VPNC_Base_Group]
IKE: requesting SPI!

496 02/15/2002 12:47:24.810 SEV=8 IKEDBG/6 RPT=4
IKE got SPI from key engine: SPI = 0x10d19e33

497 02/15/2002 12:47:24.810 SEV=9 IKEDBG/0 RPT=3945 10.48.66.76
Group [VPNC_Base_Group]
oakley constructing quick mode

498 02/15/2002 12:47:24.810 SEV=9 IKEDBG/0 RPT=3946 10.48.66.76
Group [VPNC_Base_Group]
constructing blank hash

499 02/15/2002 12:47:24.820 SEV=9 IKEDBG/0 RPT=3947 10.48.66.76
Group [VPNC_Base_Group]
constructing ISA_SA for ipsec

500 02/15/2002 12:47:24.820 SEV=9 IKEDBG/1 RPT=113 10.48.66.76
Group [VPNC_Base_Group]
constructing ipsec nonce payload

501 02/15/2002 12:47:24.820 SEV=9 IKEDBG/1 RPT=114 10.48.66.76
Group [VPNC_Base_Group]
constructing proxy ID

502 02/15/2002 12:47:24.820 SEV=7 IKEDBG/0 RPT=3948 10.48.66.76
Group [VPNC_Base_Group]
Transmitting Proxy Id:
Remote host: 10.48.66.76 Protocol 17 Port 1701
Local host: 10.48.66.109 Protocol 17 Port 0

506 02/15/2002 12:47:24.820 SEV=9 IKEDBG/0 RPT=3949 10.48.66.76
Group [VPNC_Base_Group]
constructing qm hash

507 02/15/2002 12:47:24.820 SEV=8 IKEDBG/0 RPT=3950 10.48.66.76
SENDING Message (msgid=781ceadc) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0)
... total length : 156

510 02/15/2002 12:47:24.820 SEV=8 IKEDBG/0 RPT=3951 10.48.66.76
RECEIVED Message (msgid=781ceadc) with payloads :
HDR + HASH (8) + NONE (0) ... total length : 48

512 02/15/2002 12:47:24.830 SEV=9 IKEDBG/0 RPT=3952 10.48.66.76
Group [VPNC_Base_Group]
processing hash

513 02/15/2002 12:47:24.830 SEV=9 IKEDBG/0 RPT=3953 10.48.66.76
Group [VPNC_Base_Group]
loading all IPSEC SAs

514 02/15/2002 12:47:24.830 SEV=9 IKEDBG/1 RPT=115 10.48.66.76
Group [VPNC_Base_Group]
Generating Quick Mode Key!

515 02/15/2002 12:47:24.830 SEV=9 IKEDBG/1 RPT=116 10.48.66.76
Group [VPNC_Base_Group]
Generating Quick Mode Key!

516 02/15/2002 12:47:24.830 SEV=7 IKEDBG/0 RPT=3954 10.48.66.76
Group [VPNC_Base_Group]
Loading host:
Dst: 10.48.66.109
Src: 10.48.66.76

517 02/15/2002 12:47:24.830 SEV=4 IKE/49 RPT=4 10.48.66.76
Group [VPNC_Base_Group]

```
Security negotiation complete for User ()
Responder, Inbound SPI = 0x10d19e33, Outbound SPI = 0x15895ab9

520 02/15/2002 12:47:24.830 SEV=8 IKEDBG/7 RPT=4
IKE got a KEY_ADD msg for SA: SPI = 0x15895ab9

521 02/15/2002 12:47:24.830 SEV=8 IKEDBG/0 RPT=3955
pitcher: rcv KEY_UPDATE, spi 0x10d19e33

522 02/15/2002 12:47:24.830 SEV=4 IKE/120 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
PHASE 2 COMPLETED (msgid=781ceadc)

523 02/15/2002 12:47:24.840 SEV=8 IKEDBG/0 RPT=3956
pitcher: rcv KEY_SA_ACTIVE spi 0x10d19e33

524 02/15/2002 12:47:24.840 SEV=8 IKEDBG/0 RPT=3957
KEY_SA_ACTIVE no old rekey centry found with new spi 0x10d19e33, mess_id 0x0
```

疑難排解資訊

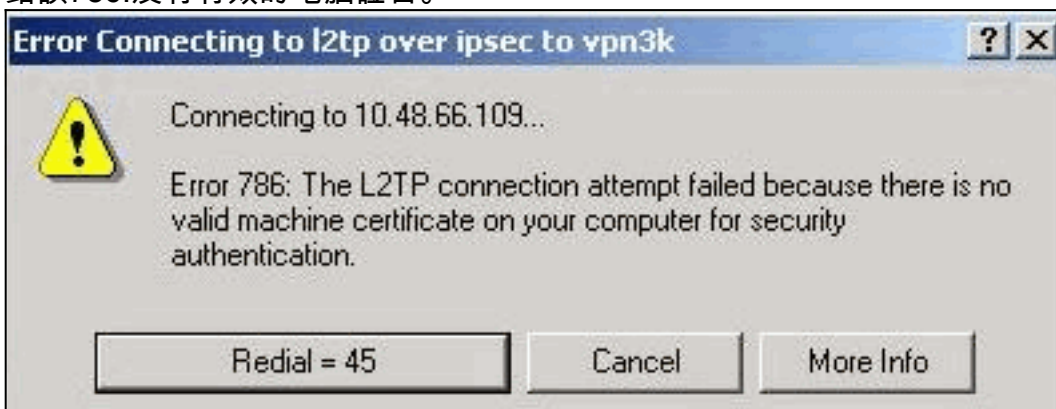
本節介紹一些常見問題以及每種問題的故障排除方法。

- 無法啟動伺服器。

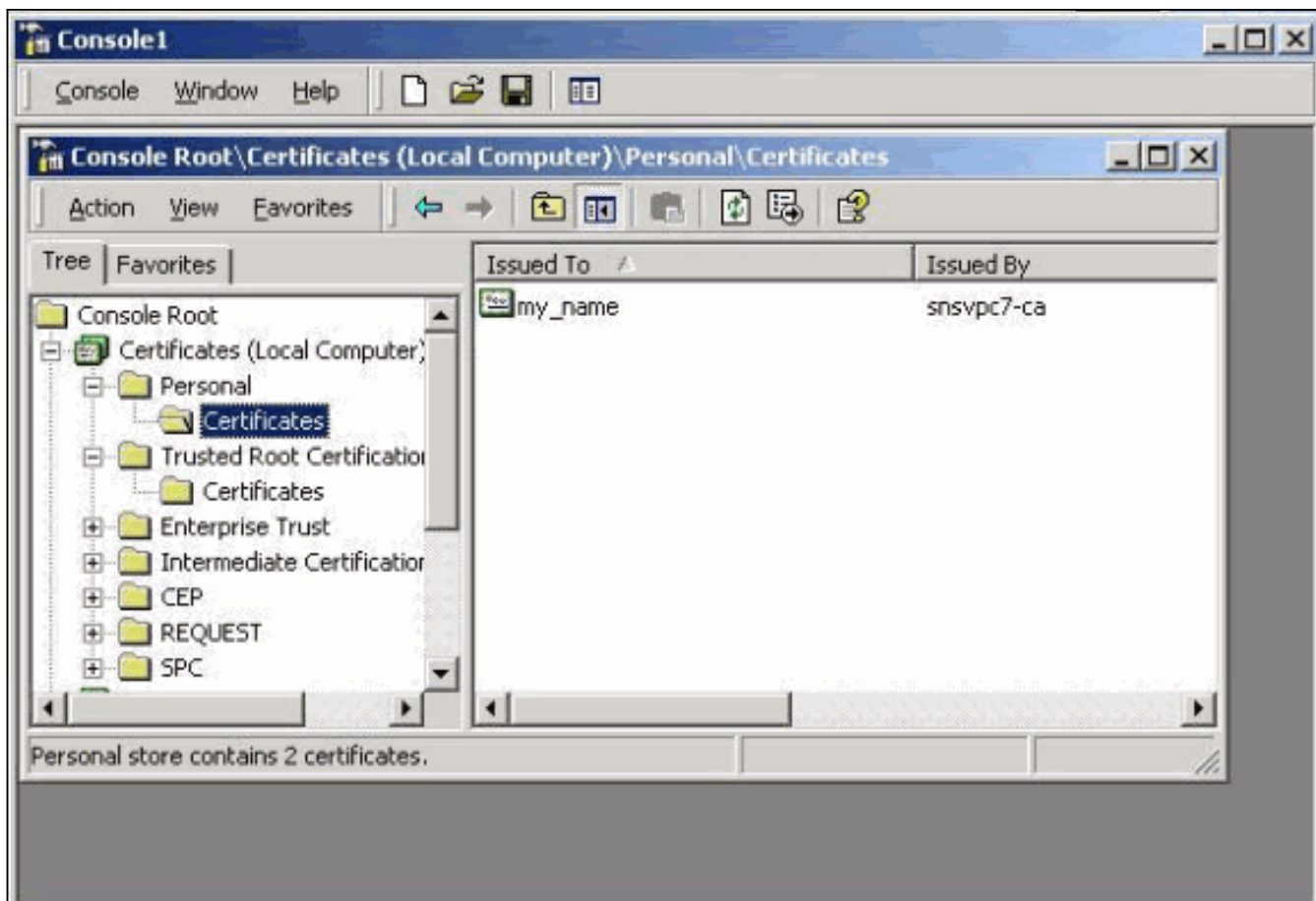


很可能未啟動IPSec服務。選擇**Start > Programs > Administrative tools > Service**，然後確保IPSec服務已啟用。

- 錯誤786:沒有有效的電腦證書。



此錯誤表示本地電腦上的證書有問題。若要輕鬆檢視您的證書，請選擇**開始>運行**，然後執行MMC。按一下**Console**，然後選擇**Add/Remove Snap-in**。按一下「**Add**」，然後從清單中選擇「**Certificate**」。當出現詢問證書範圍的視窗時，選擇**Computer Account**。現在，您可以驗證CA伺服器的證書是否位於受信任的根證書頒發機構下。您還可以通過選擇**Console Root > Certificate(Local Computer)> Personal > Certificates**來驗證您是否有證書，如下圖所示。



按一下**certificate**。驗證所有內容是否正確。在此範例中，有一個私鑰與該憑證相關聯。但是，此證書已過期。這就是問題的原因。



- 錯誤792:安全協商超時。此消息在經過較長時間後顯示。



按照[Cisco VPN](#)

[3000 Concentrator FAQ](#)中的說明開啟相關的調試。仔細讀讀。您需要看到類似以下輸出的內容

:

```
9337 02/15/2002 15:06:13.500 SEV=8 IKEDBG/0 RPT=7002 10.48.66.76
Phase 1 failure against global IKE proposal # 6:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 1
Cfg'd: Oakley Group 2
```

```
9340 02/15/2002 15:06:13.510 SEV=8 IKEDBG/0 RPT=7003 10.48.66.76
Phase 1 failure against global IKE proposal # 7:
```


Mismatched attr types for class Auth Method:

Rcv'd: RSA signature with Certificates

Cfg'd: Preshared Key

9343 02/15/2002 15:06:13.510 SEV=8 IKEDBG/0 RPT=7004 10.48.66.76

Phase 1 failure against global IKE proposal # 8:

Mismatched attr types for class DH Group:

Rcv'd: Oakley Group 1

Cfg'd: Oakley Group 7

9346 02/15/2002 15:06:13.510 SEV=7 IKEDBG/0 RPT=7005 10.48.66.76

All SA proposals found unacceptable

9347 02/15/2002 15:06:13.510 SEV=4 IKE/48 RPT=37 10.48.66.76

Error processing payload: Payload ID: 1

9348 02/15/2002 15:06:13.510 SEV=9 IKEDBG/0 RPT=7006 10.48.66.76

IKE SA MM:261e40dd terminating:

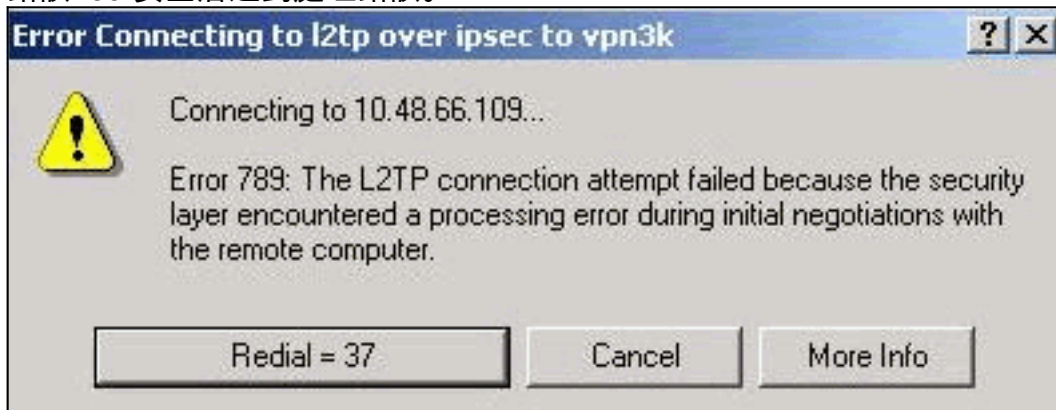
flags 0x01000002, refcnt 0, tuncnt 0

9349 02/15/2002 15:06:13.510 SEV=9 IKEDBG/0 RPT=7007

sending delete message

這表示尚未正確配置IKE提議。驗證本文檔的[配置IKE建議](#)部分中的資訊。

- 錯誤789:安全層遇到處理錯誤。



按照[Cisco VPN](#)

[3000 Concentrator FAQ](#)中的說明開啟相關的調試。仔細讀讀。您需要看到類似以下輸出的內容

:

11315 02/15/2002 15:36:32.030 SEV=8 IKEDBG/0 RPT=7686

Proposal # 1, Transform # 2, Type ESP, Id DES-CBC

Parsing received transform:

Phase 2 failure:

Mismatched attr types for class Encapsulation:

Rcv'd: Transport

Cfg'd: Tunnel

11320 02/15/2002 15:36:32.030 SEV=5 IKEDBG/0 RPT=7687

AH proposal not supported

11321 02/15/2002 15:36:32.030 SEV=4 IKE/0 RPT=27 10.48.66.76

Group [VPNC_Base_Group]

All IPSec SA proposals found unacceptable!

- 使用的版本選擇Monitoring > System Status以檢視此輸出 :

VPN Concentrator Type: 3005

Bootcode Rev: Altiga Networks/VPN Concentrator Version 2.2.int_9 Jan 19 2000 05:36:41

Software Rev: Cisco Systems, Inc./VPN 3000 Concentrator Version 3.5.Rel Nov 27 2001 13:35:16

Up For: 44:39:48

Up Since: 02/13/2002 15:49:59

RAM Size: 32 MB

相關資訊

- [IPSec協商/IKE通訊協定產品支援](#)
- [技術支援 - Cisco Systems](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。