ASA 8.x：適用於Windows的AnyConnect SSL VPN CAC智慧卡配置

目錄

簡介

本文檔提供在思科自適應安全裝置(ASA)上使用通用訪問卡(CAC)進行身份驗證的適用於Windows的AnyConnect VPN遠端訪問配置示例。

本文檔的範圍包括使用自適應安全裝置管理器(ASDM)、Cisco AnyConnect VPN客戶端和Microsoft Active Directory (AD)/輕量級目錄訪問協定(LDAP)配置Cisco ASA。

本指南中的配置使用Microsoft AD/LDAP伺服器。本文檔還介紹了OCSP、LDAP屬性對映和動態訪問策略(DAP)等高級功能。

必要條件

需求

對Cisco ASA、Cisco AnyConnect客戶端、Microsoft AD/LDAP和公鑰基礎設施(PKI)的基本瞭解有助於理解整個設定。熟悉AD組成員資格、使用者屬性以及LDAP對象有助於在證書屬性和AD/LDAP對象之間關聯授權過程。

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8.0(x)及更高版本的Cisco 5500系列自適應安全裝置(ASA)
- 適用於ASA 8.x的Cisco調適型安全裝置管理器(ASDM)版本6.x
- 適用於Windows的Cisco AnyConnect VPN客戶端

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。

Cisco ASA配置

本節介紹透過ASDM配置Cisco ASA。它介紹了透過SSL AnyConnect連線部署VPN遠端訪問隧道所需的步驟。CAC證書用於身份驗證，並且證書中的使用者主體名稱(UPN)屬性填充到active directory中以進行授權。

部署注意事項

- 本指南不包括基本配置，例如介面、DNS、NTP、路由、裝置訪問、ASDM訪問等。假設網路操作員熟悉這些配置。

  有關詳細資訊，請參閱多功能安全裝置。
- 以紅色突出顯示的部分是基本VPN訪問所需的必要配置。例如，可以使用CAC卡設定VPN隧道，而無需執行OCSP檢查、LDAP對映和動態訪問策略(DAP)檢查。DoD要求OCSP檢查，但隧道在沒有配置OCSP的情況下工作。
- 以藍色突出顯示的部分是高級功能，可以增加更多安全性到設計中。
- ASDM和AnyConnect/SSL VPN不能在同一介面上使用相同的埠。建議更改其中一個埠或另一個埠以獲得訪問許可權。例如，對ASDM使用埠445，對AC/SSL VPN使用埠443。在8.x中更改了ASDM URL訪問。使用`https://<ip_address>`：<port>/admin.html。
- 所需的ASA映像至少為8.0.2.19和ASDM 6.0.2。
- Vista支援AnyConnect/CAC。
- 有關更多策略實施的LDAP和動態訪問策略對映示例，請參閱附錄A。
- 有關如何在MS中檢查LDAP對象，請參閱附錄D。
- 有關防火牆配置的應用程式埠清單，請參閱相關資訊。

身份驗證、授權、記帳(AAA)配置

您會透過憑證授權單位(CA)伺服器或其所屬組織的CA伺服器，在其通用存取卡(CAC)中使用憑證進行驗證。憑證必須有效才能遠端存取網路。除了驗證之外，您還必須獲得使用Microsoft Active Directory或輕量型目錄存取通訊協定(LDAP)物件的授權。國防部(DoD)需要使用使用者主體名稱(UPN)屬性進行授權，這是憑證主體替代名稱(SAN)部分的一部分。UPN或EDI/PI必須採用以下格式：1234567890@mil。這些配置顯示了如何使用LDAP伺服器在ASA中配置AAA伺服器以進行授權。有關更多透過LDAP對象對映進行的配置，請參閱附錄A。

設定LDAP伺服器

請完成以下步驟：

1. 選擇Remote Access VPN > AAA Setup > AAA Server Group。

2. 在AAA伺服器組表中，按一下Add 3。

3. 輸入伺服器組名稱，並選擇LDAP協定單選按鈕。請參閱圖1。

4. 在所選組表的Servers中，按一下Add。請確定您建立的伺服器已在上一個表格中反白。

5. 在「編輯AAA伺服器」窗口中，完成以下步驟。請參閱圖2。

> 注意：如果您的LDAP/AD已針對此類連線進行配置，請選擇Enable LDAP over SSL選項。

a. 選擇LDAP所在的介面。本指南顯示介面內部。

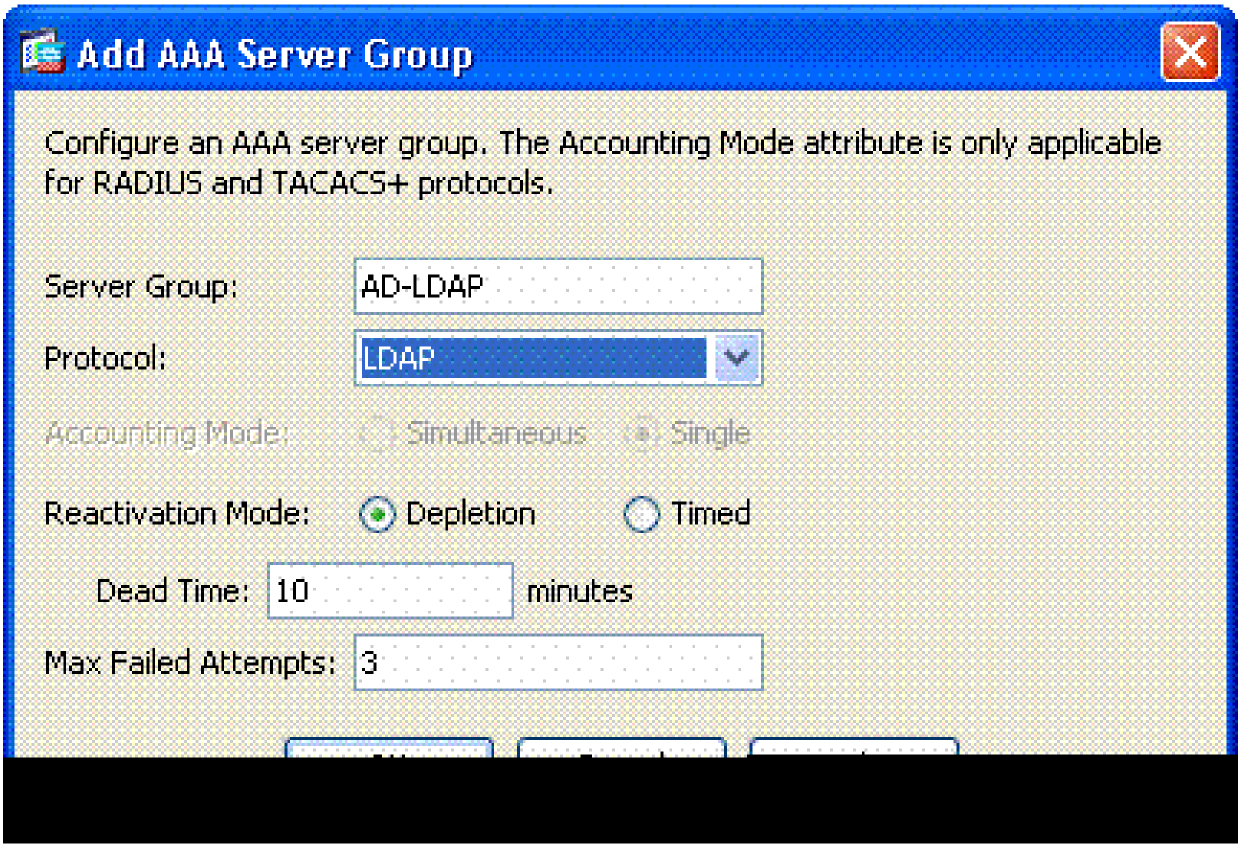
b. 輸入伺服器的IP地址。

c. 輸入server port。預設LDAP埠為389。

d. 選擇Server Type。

e. 輸入Base DN。請向您的AD/LDAP管理員詢問這些值。

圖1



Add AAA Server Group

Configure an AAA server group. The Accounting Mode attribute is only applicable for RADIUS and TACACS+ protocols.

Server Group: AD-LDAP

Protocol: LDAP

Accounting Mode: ○ Simultaneous ● Single

Reactivation Mode: ● Depletion ○ Timed

Dead Time: 10 minutes

Max Failed Attempts: 3

[redacted]

f. 在「範圍」選項下，選擇適當的答案。這取決於基本DN。請向您的AD/LDAP管理員尋求幫助。

g. 在Naming Attribute中，輸入userPrincipalName。此屬性用於AD/LDAP伺服器中的使用

者授權。

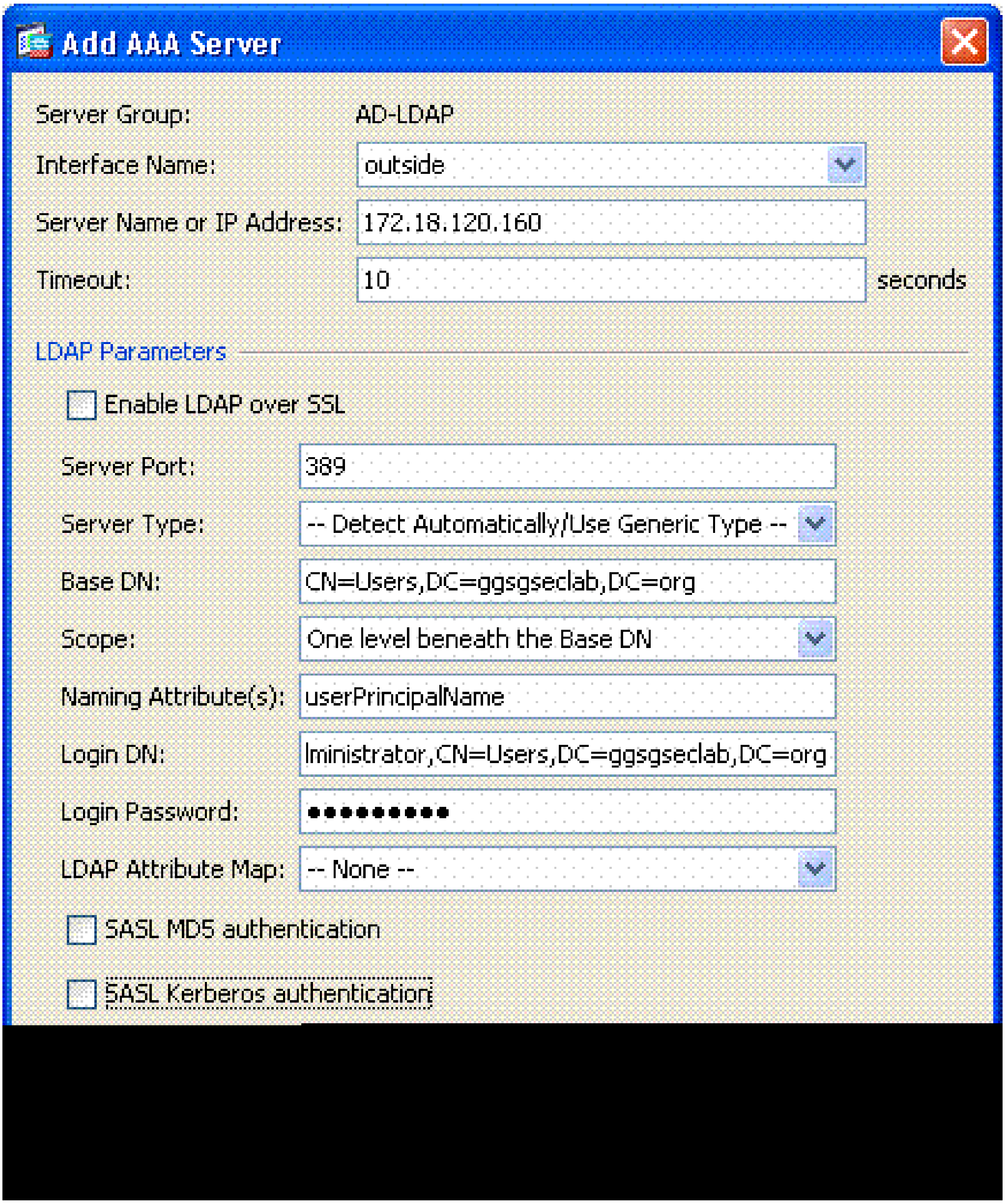
h. 在Login DN中，輸入管理員DN。

> 注意：您擁有檢視/搜尋包含使用者物件和群組成員資格之LDAP結構的管理許可權或許可權。

i. 在登入密碼中，輸入管理員的密碼。

j. 保留LDAP屬性的預設設定none。

圖2



Server Group: AD-LDAP

Interface Name: outside

Server Name or IP Address: 172.18.120.160

Timeout: 10 seconds

LDAP Parameters

☐ Enable LDAP over SSL

Server Port: 389

Server Type: -- Detect Automatically/Use Generic Type --

Base DN: CN=Users,DC=ggsgseclab,DC=org

Scope: One level beneath the Base DN

Naming Attribute(s): userPrincipalName

Login DN: lministrator,CN=Users,DC=ggsgseclab,DC=org

Login Password: ●●●●●●●●●●

LDAP Attribute Map: -- None --

☐ SASL MD5 authentication

☐ SASL Kerberos authentication

注意：以後在配置中使用此選項可以增加其他AD/LDAP對象以進行授權。

k. 選擇OK。

6. 選擇OK。

管理憑證

在ASA上安裝證書需要兩個步驟。首先，安裝所需的CA證書（根和從屬證書頒發機構）。其次，將ASA註冊到特定CA並獲得身份證書。DoD PKI使用以下證書：根CA2、類3根、CA##

INTERMEDIATE（ASA註冊時使用）、ASA ID證書和OCSP證書。但是，如果選擇不使用OCSP，則不需要安裝OCSP證書。

注意：請與您的安全POC聯絡以獲得根證書以及如何註冊裝置的身份證書的說明。SSL證書應足夠ASA進行遠端訪問。不需要雙SAN證書。

注意：本地電腦還必須安裝DoD CA鏈。憑證可以在Microsoft憑證存放區中使用Internet Explorer檢視。DoD已生成一個批處理檔案，該檔案會自動將所有CA增加到電腦。有關更多資訊，請諮詢您的PKI POC。

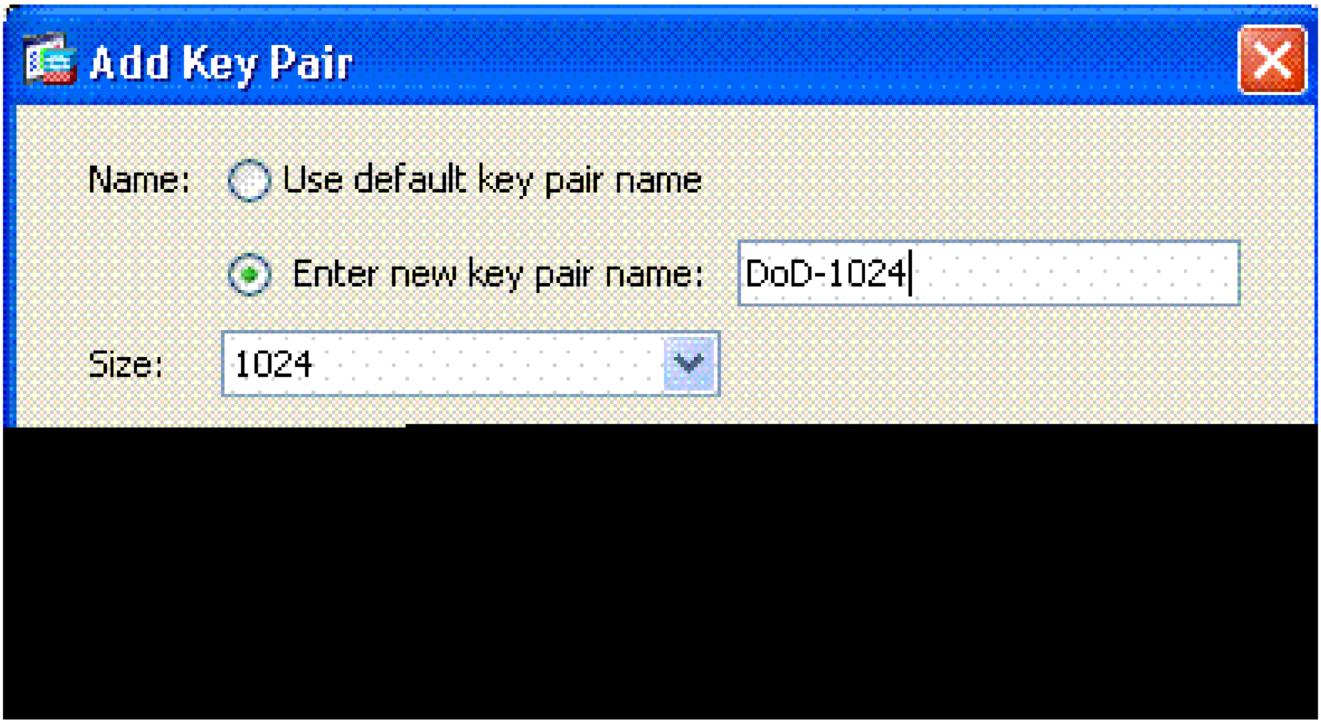
註：DoD CA2和3類根以及發出ASA證書的ASA ID和CA中間裝置應該是使用者身份驗證所需的唯一CA。所有當前的CA中間體都屬於CA2和3類根鏈，只要增加了CA2和3類根，這些中間體就受信任。

產生金鑰

請完成以下步驟：

1. 選擇Remote Access VPN > Certificate Management > Identity Certificate > Add。
2. 選擇Add a new id certificate，然後選擇金鑰對選項旁邊的New。
3. 在Add Key Pair窗口中，輸入金鑰名稱DoD-1024。按一下無線電以新增金鑰。請參閱圖3。

圖3



Add Key Pair

Name: ○ Use default key pair name

● Enter new key pair name: DoD-1024

Size: 1024

[redacted]

4. 選擇金鑰的大小。

5. 保留Usage的預設設定General Purpose。

6. 按一下Generate Now。

> 註： DoD Root CA 2使用2048位金鑰。應生成使用2048位金鑰對的第二個金鑰，以便能夠使用此CA。完成上述步驟以增加第二個鍵。

安裝根CA證書

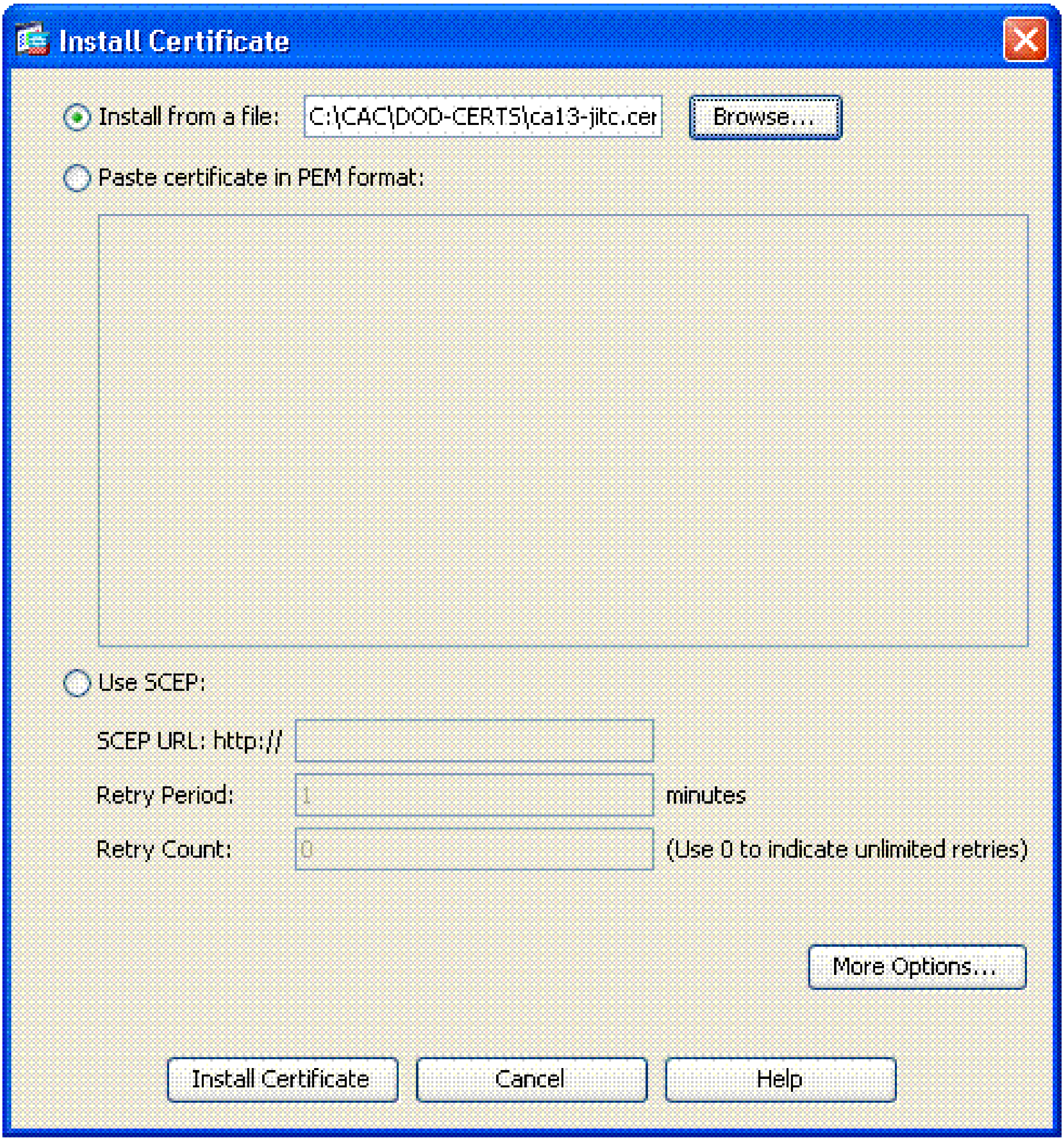
請完成以下步驟：

1. 選擇Remote Access VPN > Certificate Management > CA Certificate > Add。

2. 選擇Install from File，並瀏覽到相應證書。

3. 選擇Install Certificate。

   圖4：安裝根證書



● Install from a file: C:\CAC\DOD-CERTS\ca13-jitc.cer

○ Paste certificate in PEM format:

○ Use SCEP:

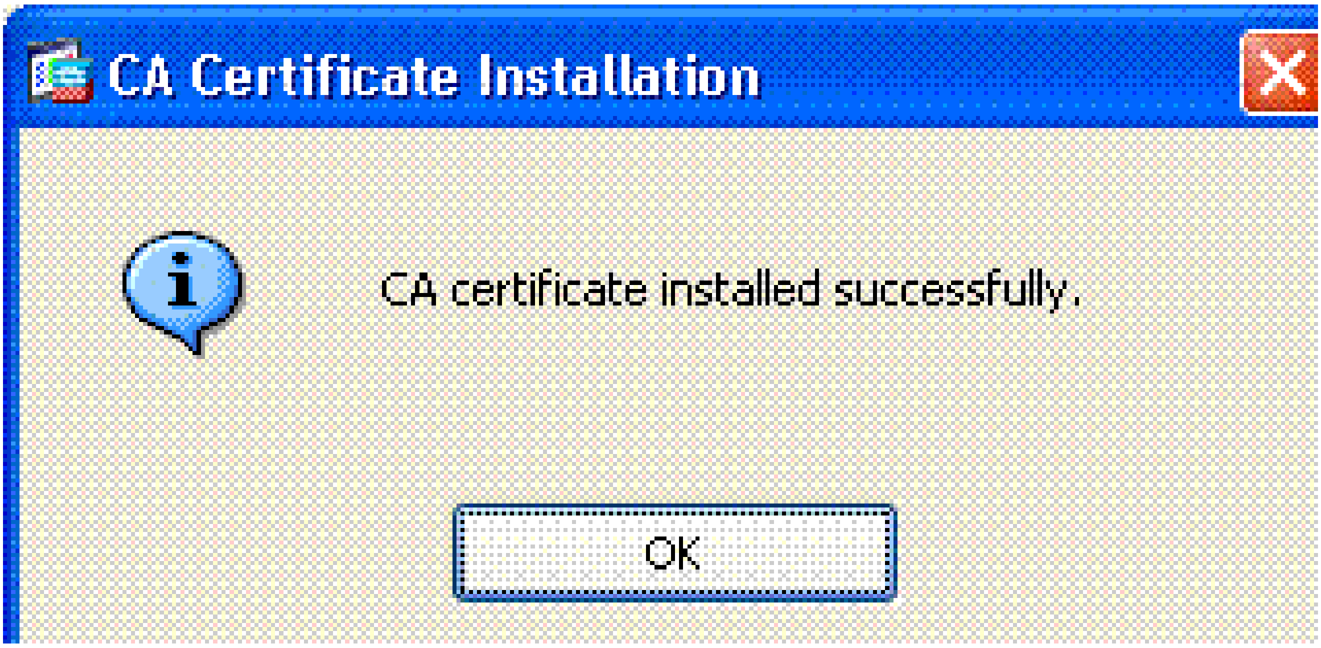
SCEP URL: http://

Retry Period: 1 minutes

Retry Count: 0 (Use 0 to indicate unlimited retries)

4. 此視窗應該會出現。請參閱圖5。

圖5

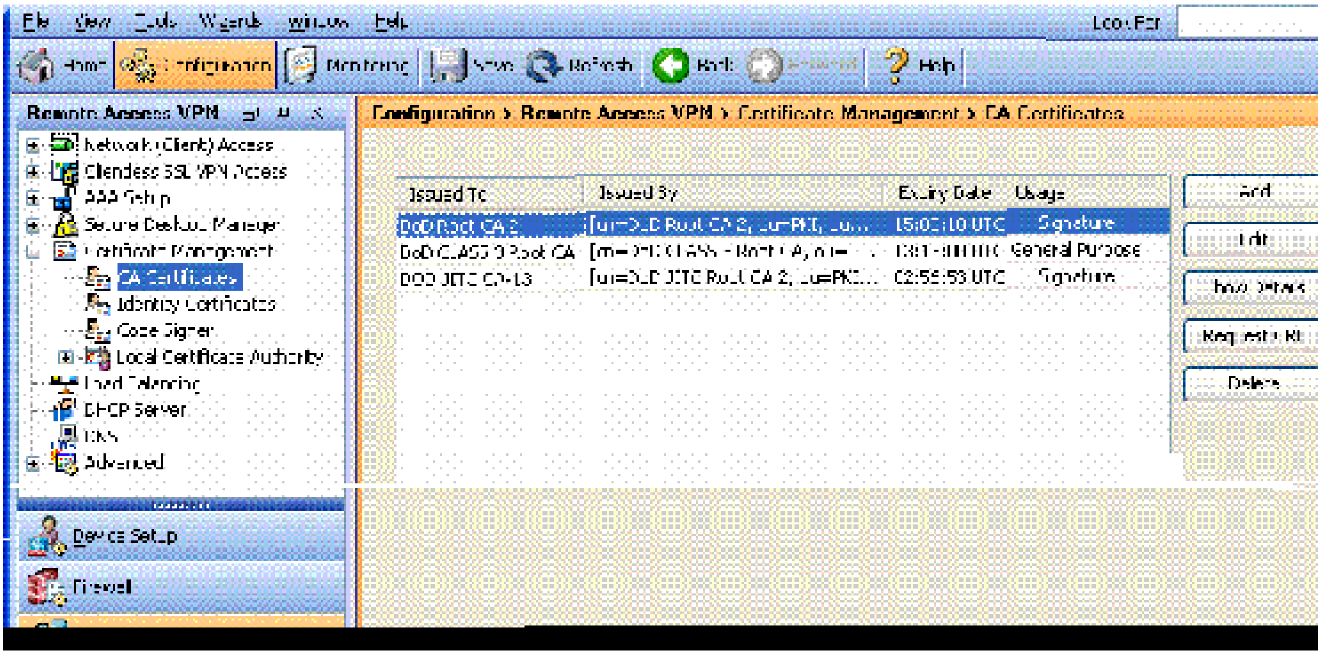


CA Certificate Installation

CA certificate installed successfully.

注意：對要安裝的每個證書重複步驟1到3。DoD PKI需要以下每個項的證書：根CA 2、類3根、CA##中間、ASA ID和OCSP伺服器。如果不使用OCSP，則不需要OCSP證書。

圖6：安裝根證書



Configuration > Remote Access VPN > Certificate Management > CA Certificates

Issued To	Issued By	Expiry Date	Usage
DoD Root CA 2	[cn=DoD Root CA 2, ou=PKI, ou=...	15:03:10 UTC	Signature
DoD CLASS 3 Root CA	[cn=DOD CLASS 3 Root CA, ou=...	[illegible] UTC	General Purpose
DOD JITC CA-13	[cn=DoD JITC Root CA 2, ou=PKI...	02:55:53 UTC	Signature

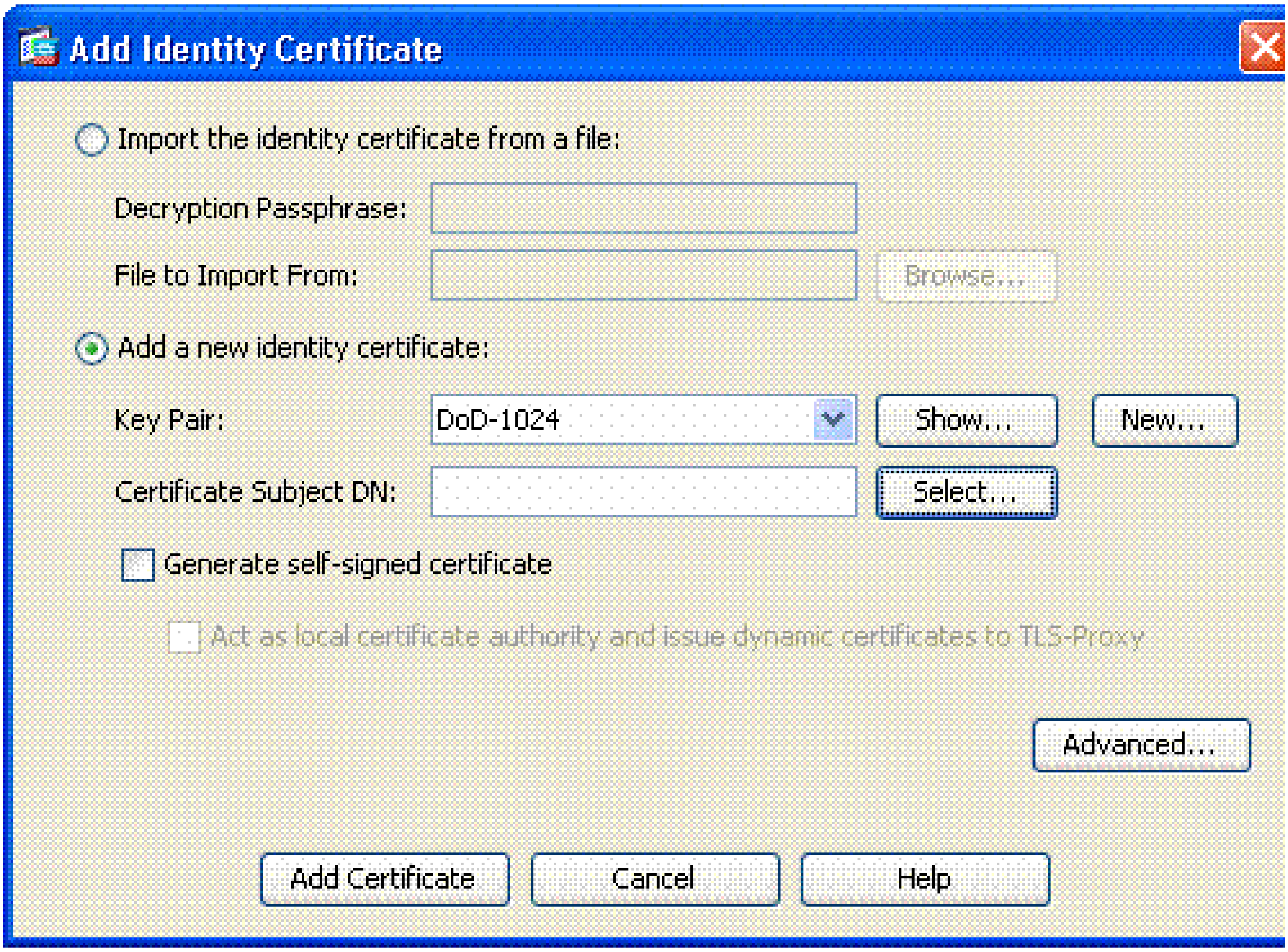
註冊ASA並安裝身份證書

1. 選擇Remote Access VPN > Certificate Management > Identity Certificate > Add。

2. 選擇Add a new id certificate。

3. 選擇DoD-1024金鑰對。請參閱圖7

圖7：身份證書引數



○ Import the identity certificate from a file:

Decryption Passphrase:

File to Import From:

● Add a new identity certificate:

Key Pair: DoD-1024

Certificate Subject DN:

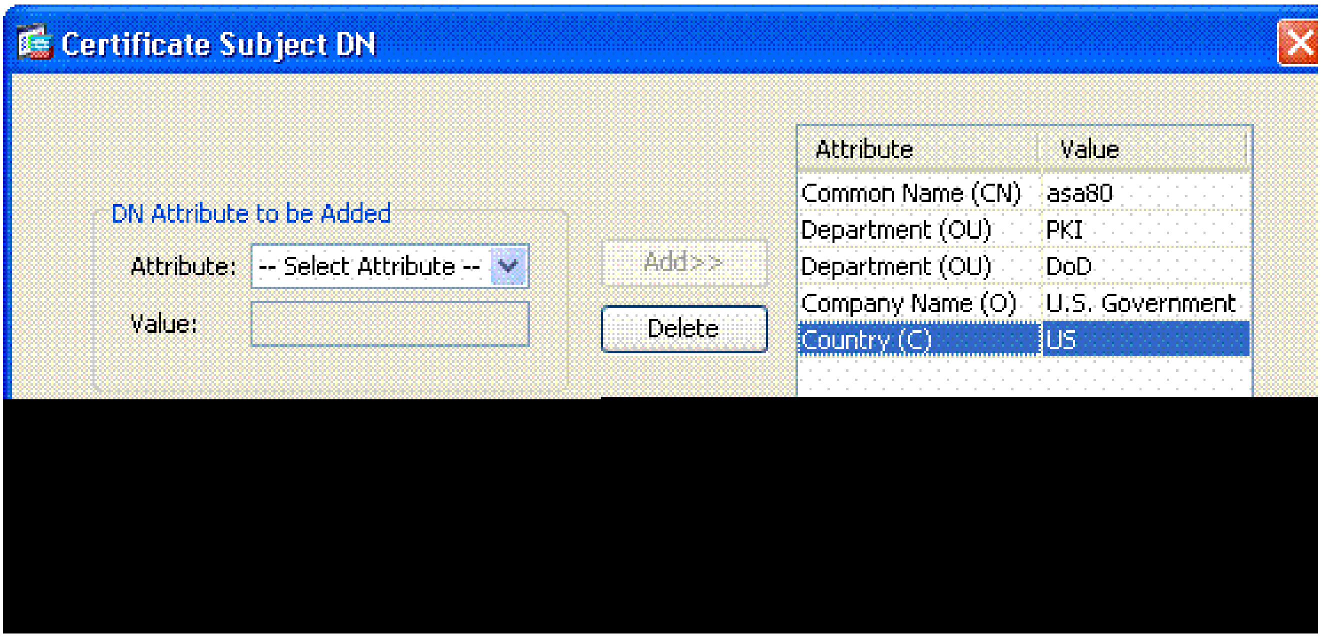
□ Generate self-signed certificate

□ Act as local certificate authority and issue dynamic certificates to TLS-Proxy

4. 轉到Certificate subject DN框，並按一下Select。

5. 在Certificate Subject DN窗口中，輸入裝置的資訊。有關示例，請參見圖8。

圖8：編輯DN



Attribute: -- Select Attribute --

Value:

Attribute	Value
Common Name (CN)	asa80
Department (OU)	PKI
Department (OU)	DoD
Company Name (O)	U.S. Government
Country (C)	US

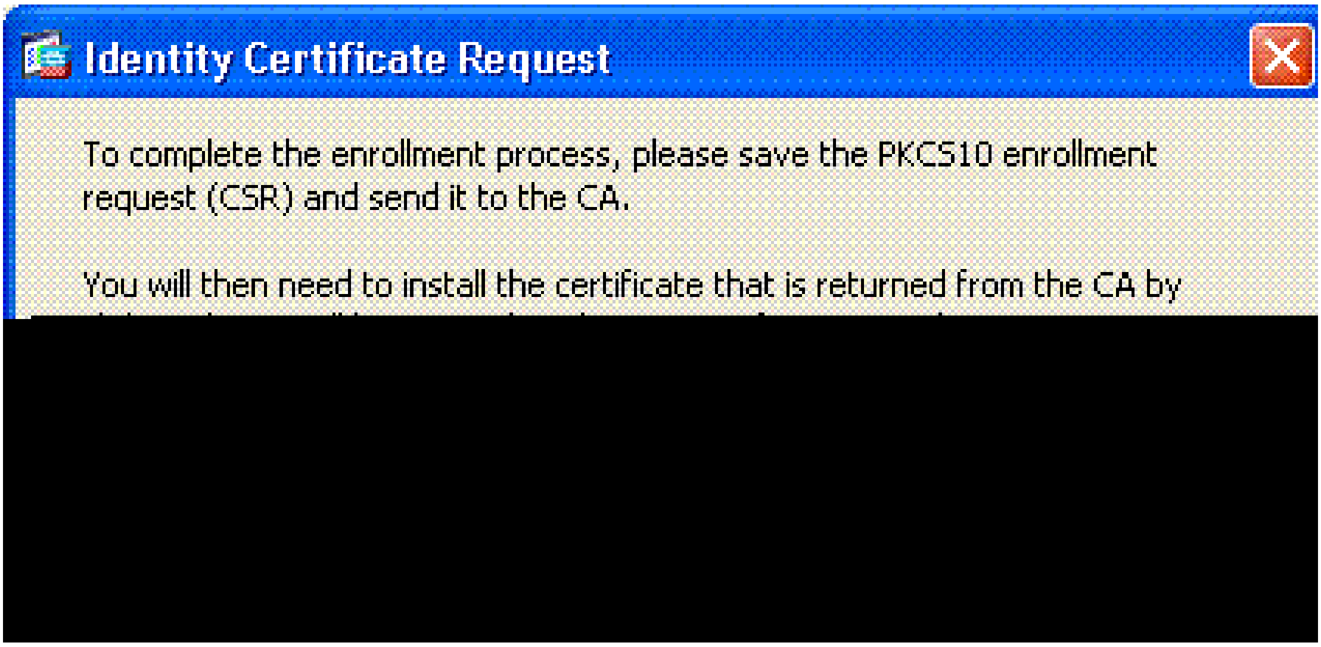
6. 選擇OK。

注意：增加主題DN時，請確保使用系統中配置的裝置主機名。PKI POC可以告訴您必填欄位。

7. 選擇Add certificate。

8. 按一下Browse，以選擇要儲存請求的目錄位置。請參閱圖9。

圖9：證書請求



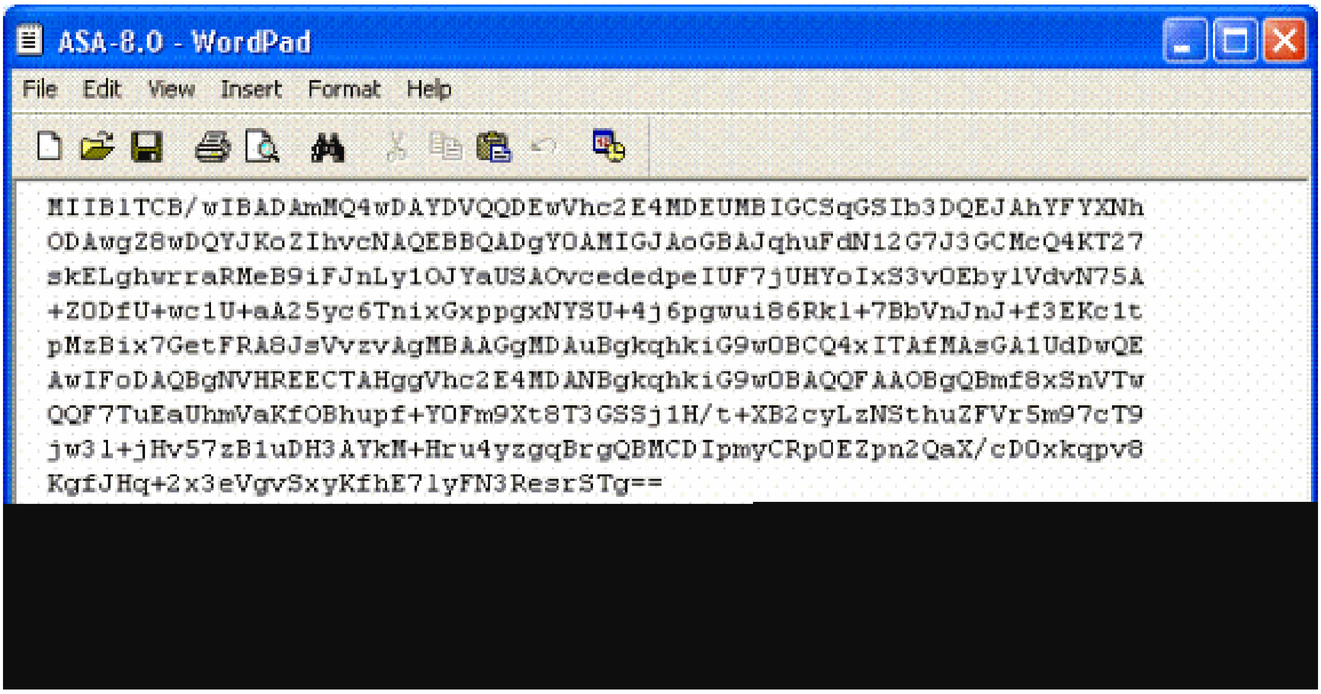
To complete the enrollment process, please save the PKCS10 enrollment request (CSR) and send it to the CA.

You will then need to install the certificate that is returned from the CA by

[redacted]

9. 使用寫字板打開檔案，將請求複製到相應的文檔，然後傳送到您的PKI POC。請參閱圖10。

圖10：註冊請求

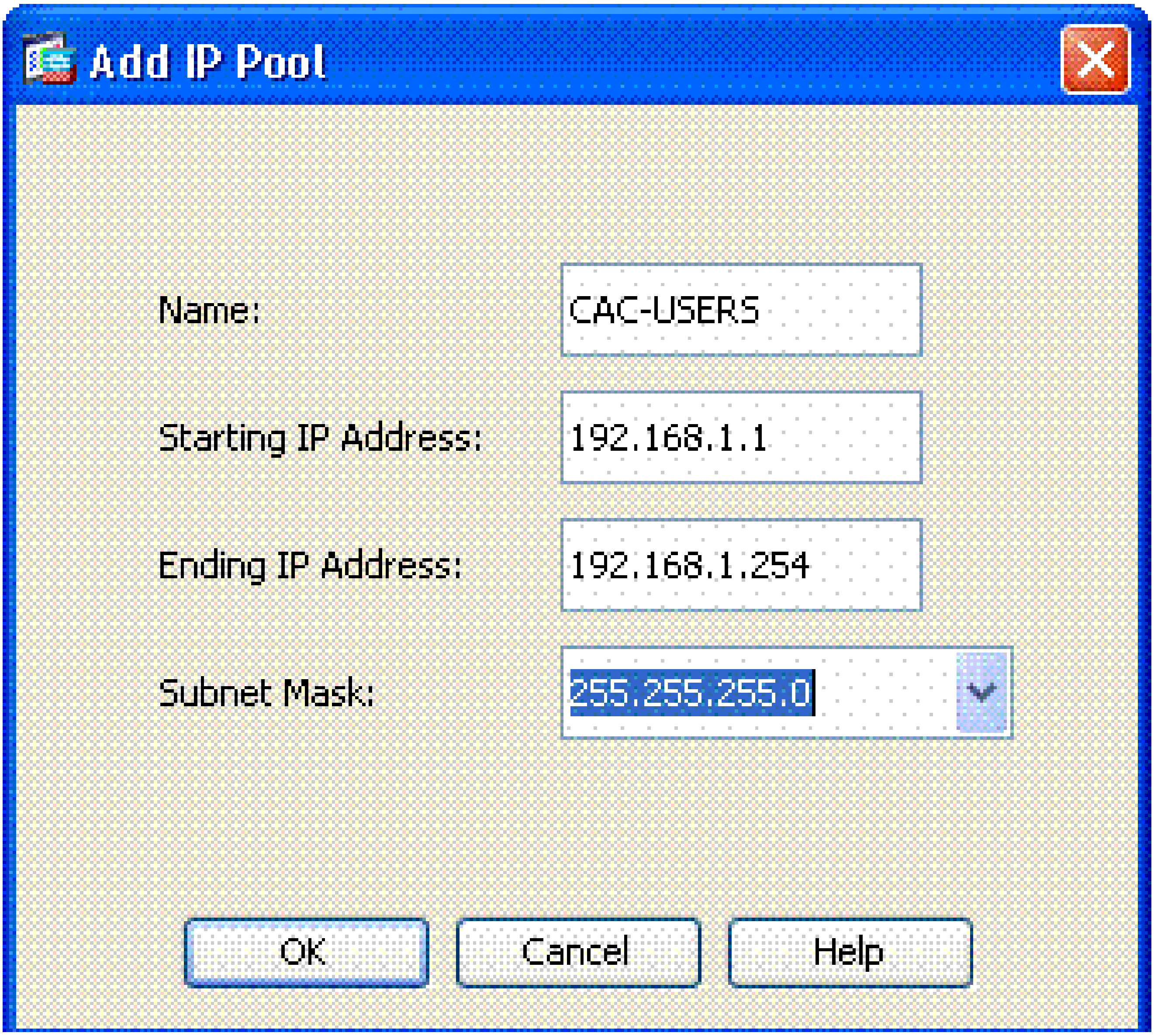


```
MIIB1TCB/wIBADAmMQ4wDAYDVQQDEwVhc2E4MDEUMBIGCSqGSIb3DQEJAhYFYXNh
ODAwgZ8wDQYJKoZIhvcNAQEBBQADgYOAMIGJAoGBAJqhuFdN12G7J3GCMcQ4KT27
skELghwrraRMeB9iFJnLy1OJYaUSAOvcededpeIUF7jUHYoIxS3vOEbylVdvN75A
+ZODfU+wc1U+aA25yc6TnixGxppgxNYSU+4j6pgwui86Rkl+7BbVnJnJ+f3EKc1t
pMzBix7GetFRA8JsVvzvAgMBAAGgMDAuBgkqhkiG9w0BCQ4xITAfMAsGA1UdDwQE
AwIFoDAQBgNVHREECTAHggVhc2E4MDANBgkqhkiG9w0BAQQFAAOBgQBmf8xSnVTw
QQF7TuEaUhmVaKfOBhupf+YOFm9Xt8T3GSSj1H/t+XB2cyLzNSthuZFVr5m97cT9
jw3l+jHv57zB1uDH3AYkM+Hru4yzgqBrgQBMCDIpmyCRpOEZpn2QaX/cDOxkqpv8
KgfJHq+2x3eVgvSxyKfhE7lyFN3ResrSTg==
```

[redacted]

10. 從CA管理員處收到證書後，請選擇Remote Access VPN > Certificate Management > ID Certificate > Install。請參閱圖11。

圖11：導入身份證書



Add IP Pool

Name: CAC-USERS

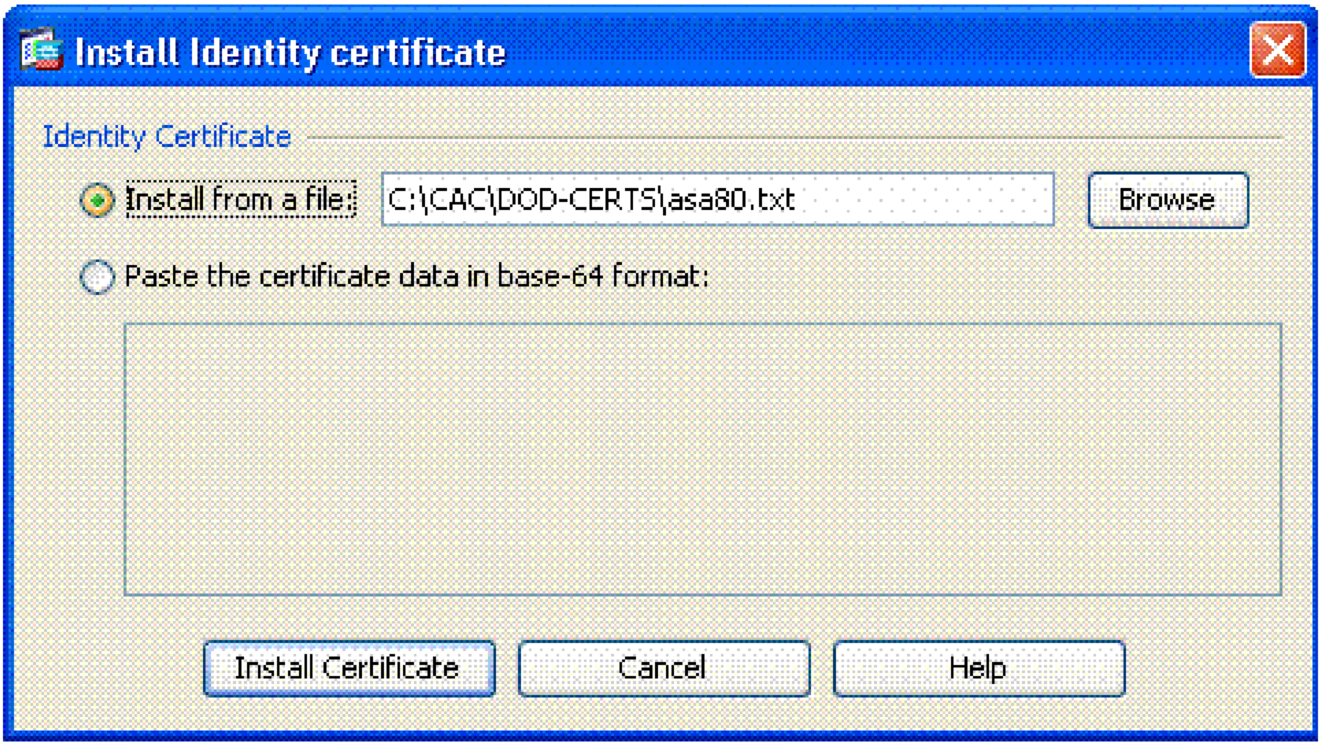
Starting IP Address: 192.168.1.1

Ending IP Address: 192.168.1.254

Subnet Mask: 255.255.255.0

11. 在Install certificate窗口中，瀏覽到該ID證書，並選擇Install Certificate。有關示例，請參見圖12。

圖12：安裝身份證書



C:\CAC\DOD-CERTS\asa80.txt

注意：建議導出ID證書信任點以儲存頒發的證書和金鑰對。這允許ASA管理員將證書和金鑰對導入到新的ASA，以防RMA或硬體故障。有關詳細資訊，請參閱導出和導入信任點。

注意：按一下SAVE，以將配置儲存在快閃記憶體中。

AnyConnect VPN配置

在ASDM中配置VPN引數有兩個選項。第一個選項是使用SSL VPN嚮導。對於不熟悉VPN配置的使用者來說，這是一個易於使用的工具。第二個選項是手動執行並逐一檢查每個選項。本配置指南使用手動方法。

註：有兩種方法可將AC客戶端提供給使用者：

1. 您可以從思科網站下載使用者端，然後將其安裝至其電腦上。
2. 使用者可透過Web瀏覽器訪問ASA，並且可以下載客戶端。

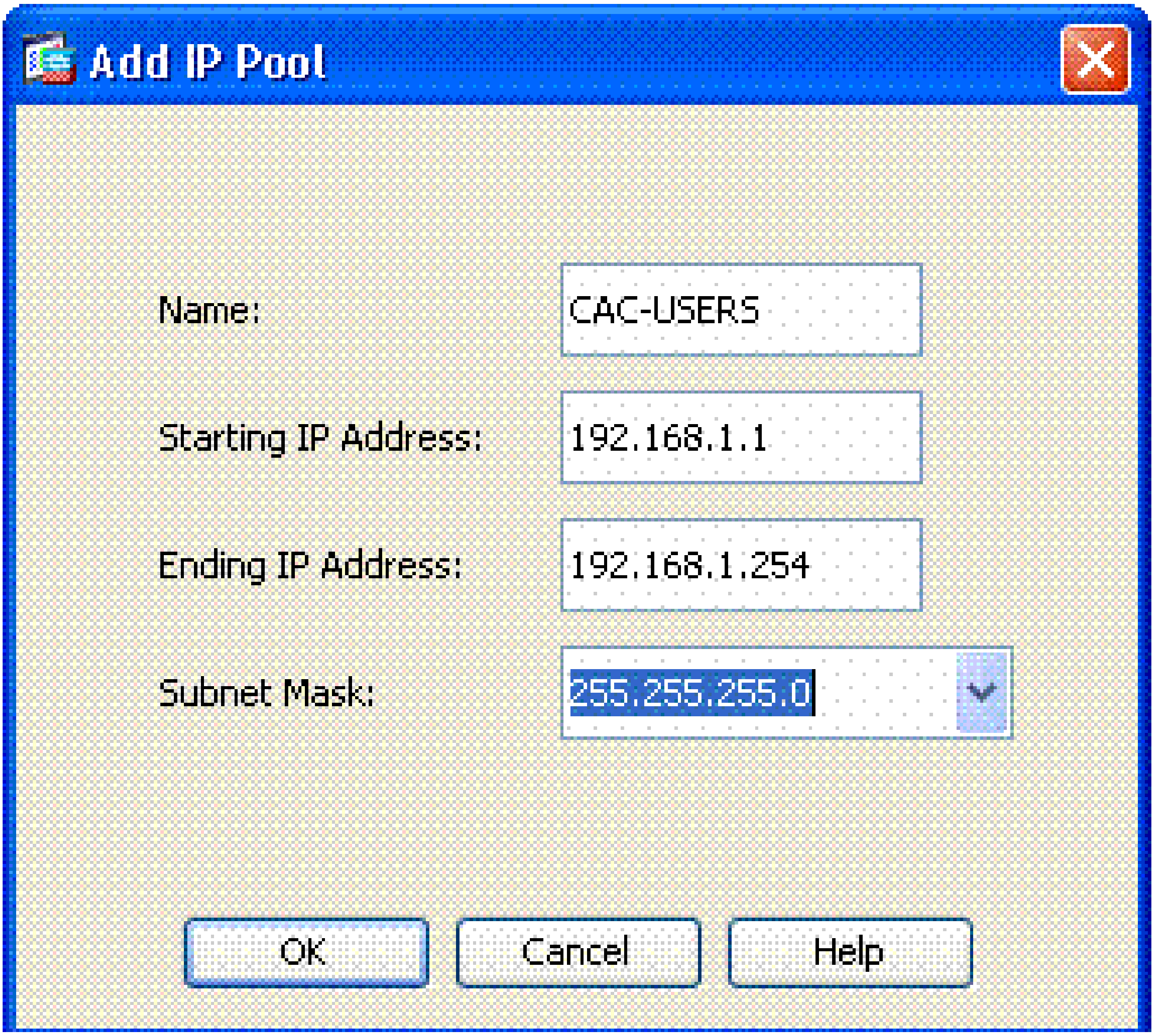
附註：例如https://asa.test.com。本指南使用第二種方法。將AC客戶端永久安裝到客戶端電腦上後，您只需從應用程式啟動AC客戶端。

建立IP地址池

如果使用其他方法（如DHCP），則這是可選的。

1. 選擇Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools。
2. 按一下Add。
3. 在Add IP Pool窗口中，輸入IP池的名稱、起始IP地址和結束IP地址，然後選擇子網掩碼。請參閱圖13。

圖13：增加IP池



Add IP Pool

Name: CAC-USERS

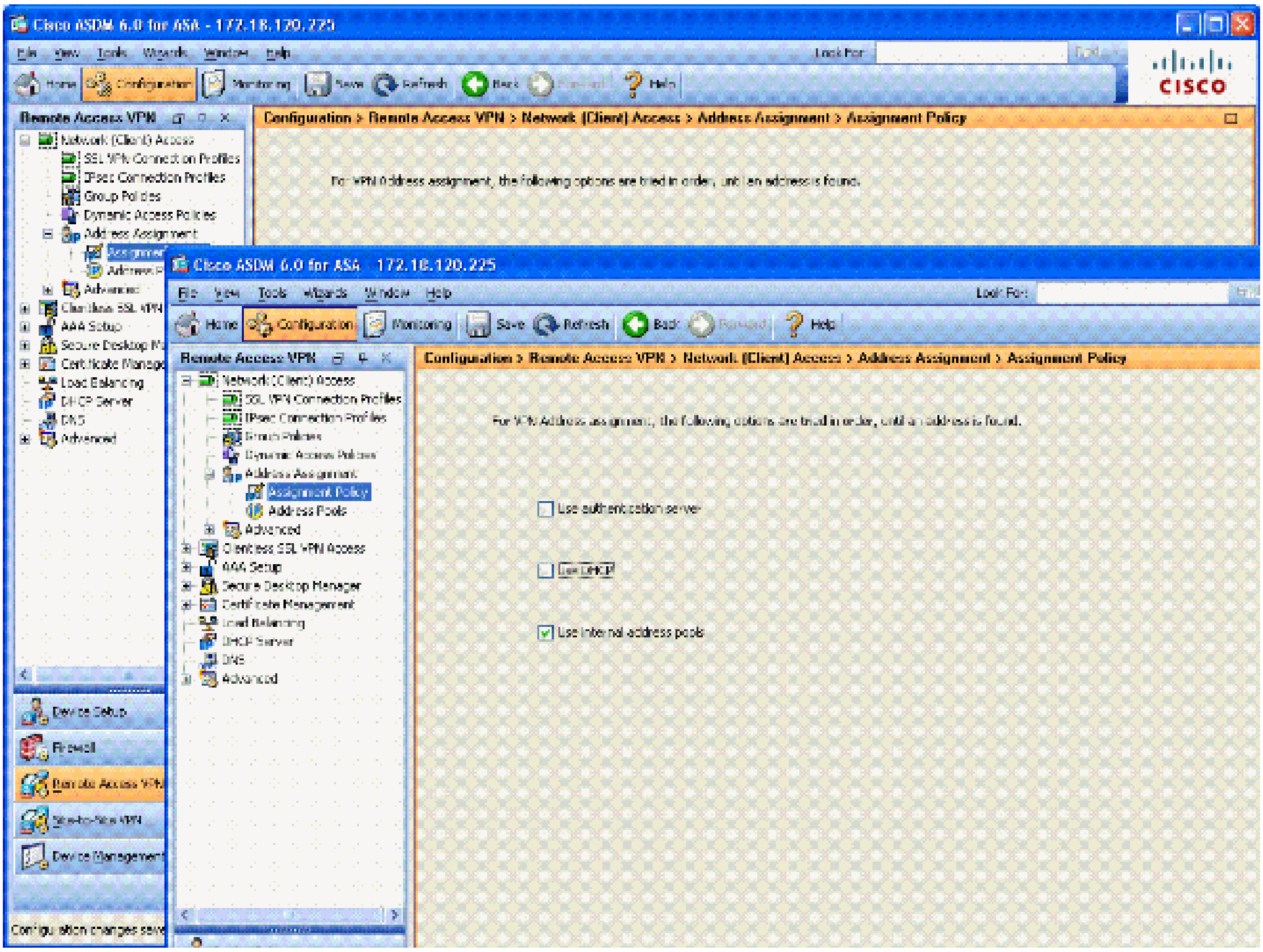
Starting IP Address: 192.168.1.1

Ending IP Address: 192.168.1.254

Subnet Mask: 255.255.255.0

4. 選擇Ok。
5. 選擇Remote Access VPN > Network (Client) Access > Address Assignment > Assignment Policy。
6. 選擇適當的IP地址分配方法。本指南使用內部地址池。請參閱圖14。

圖14：IP地址分配方法



For VPN Address assignment, the following options are tried in order, until an address is found.

□ Use authentication server

□ Use DHCP

☑ Use internal address pools

7. 按一下「Apply」。

建立隧道組和組策略

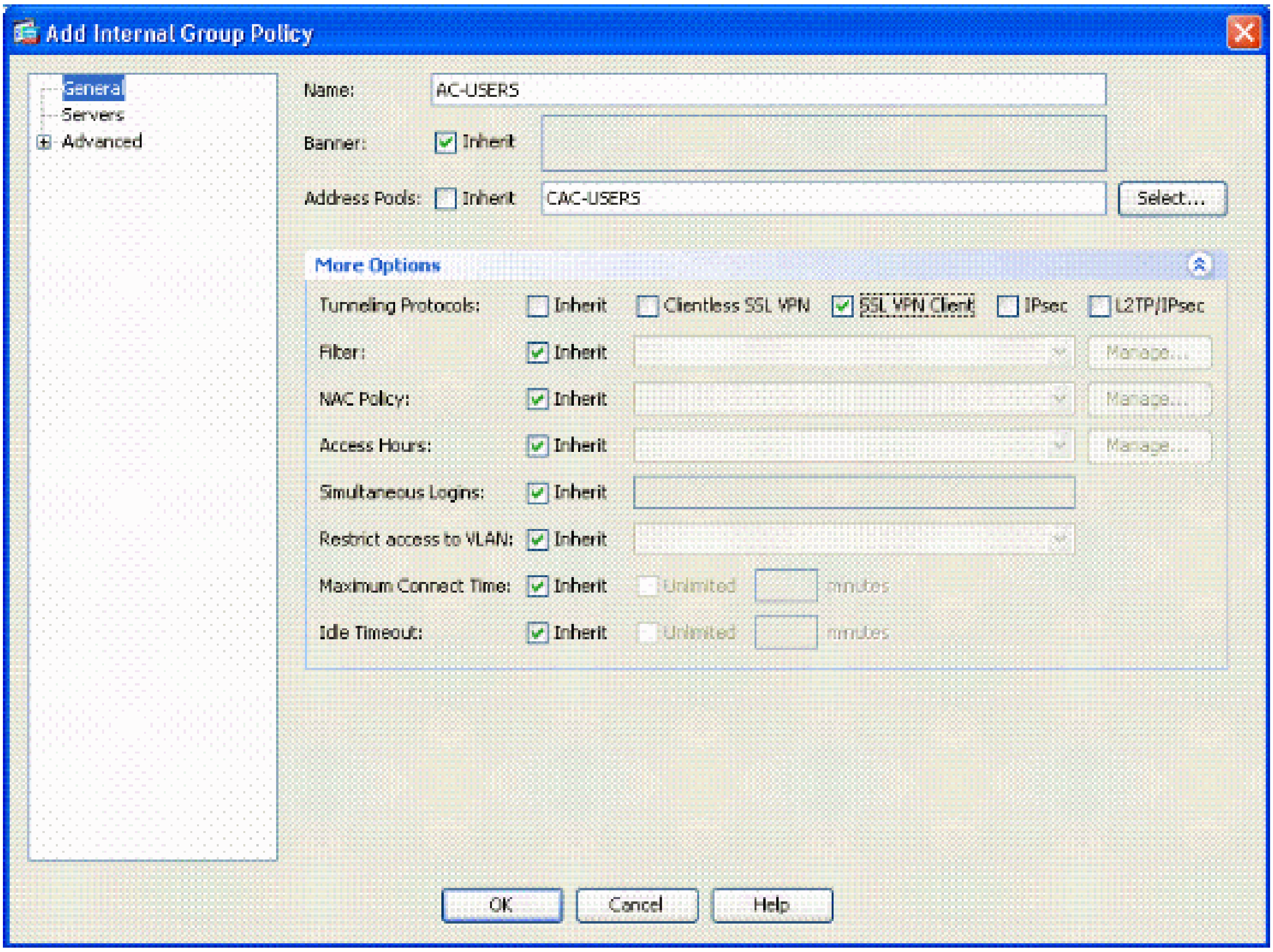
群組原則

注意：如果不想建立新策略，則可以使用預設的內建組策略。

---

1. 選擇Remote Access VPN -> Network (Client) Access -> Group Policies。
2. 按一下Add並選擇Internal Group Policy。
3. 在Add Internal Group Policy窗口中，在Name文本框中輸入組策略的名稱。請參閱圖15。

圖15：增加內部組策略



Add Internal Group Policy

- General
- Servers
- ⊞ Advanced

Name: AC-USERS

Banner: ☑ Inherit

Address Pools: □ Inherit CAC-USERS Select...

More Options

Tunneling Protocols: □ Inherit □ Clientless SSL VPN ☑ SSL VPN Client □ IPsec □ L2TP/IPsec

Filter: ☑ Inherit Manage...

NAC Policy: ☑ Inherit Manage...

Access Hours: ☑ Inherit Manage...

Simultaneous Logins: ☑ Inherit

Restrict access to VLAN: ☑ Inherit

Maximum Connect Time: ☑ Inherit □ Unlimited minutes

Idle Timeout: ☑ Inherit □ Unlimited minutes

OK Cancel Help

a. 在General頁籤上，選擇SSL VPN Client in the Tunneling Protocols 選項，除非您使用其他協定（如Clientless SSL）。

b. 在Servers部分中，取消選中inherit覈取方塊，並輸入DNS和WINS伺服器的IP地址。輸入DHCP作用域（如果適用）。

c. 在Servers部分中，取消選中Default Domain中的inherit覈取方塊，並輸入適當的域名。

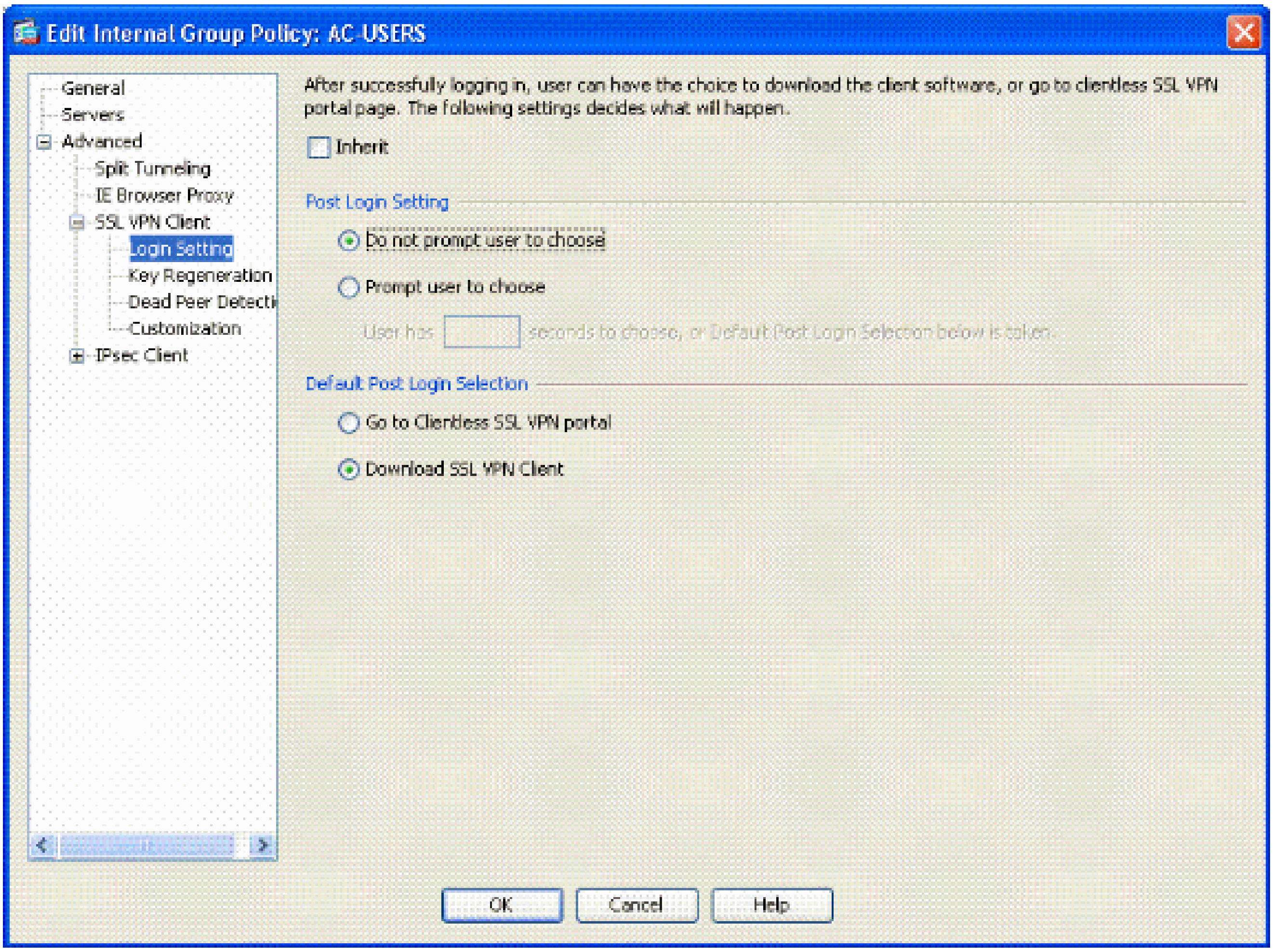
d. 在General頁籤上，取消選中Address Pool部分中的Inherit覈取方塊，並增加在上一步建立的地址池。如果您使用其他IP地址分配方法，請保留此方法以繼承並進行適當的更改。

e. 所有其他配置頁籤都保留為預設設定。

> 註：有兩種方法可將AC客戶端提供給終端使用者。一種方法是訪問Cisco.com並下載AC客戶端。第二種方法是在使用者嘗試連線時，讓ASA將客戶端下載給使用者。此範例顯示後一種方法。

4. 然後，選擇Advanced > SSL VPN Client > Login Settings。請參閱圖16。

圖16：增加內部組策略



After successfully logging in, user can have the choice to download the client software, or go to clientless SSL VPN portal page. The following settings decides what will happen.

□ Inherit

Post Login Setting

● Do not prompt user to choose

○ Prompt user to choose

User has [ ] seconds to choose, or Default Post Login Selection below is taken

Default Post Login Selection

○ Go to Clientless SSL VPN portal

● Download SSL VPN Client

a. 取消選中Inherit覈取方塊。

b. 選擇適合您環境的適當登入後設定。

c. 選擇適合您環境的適當「預設登入後選擇」。

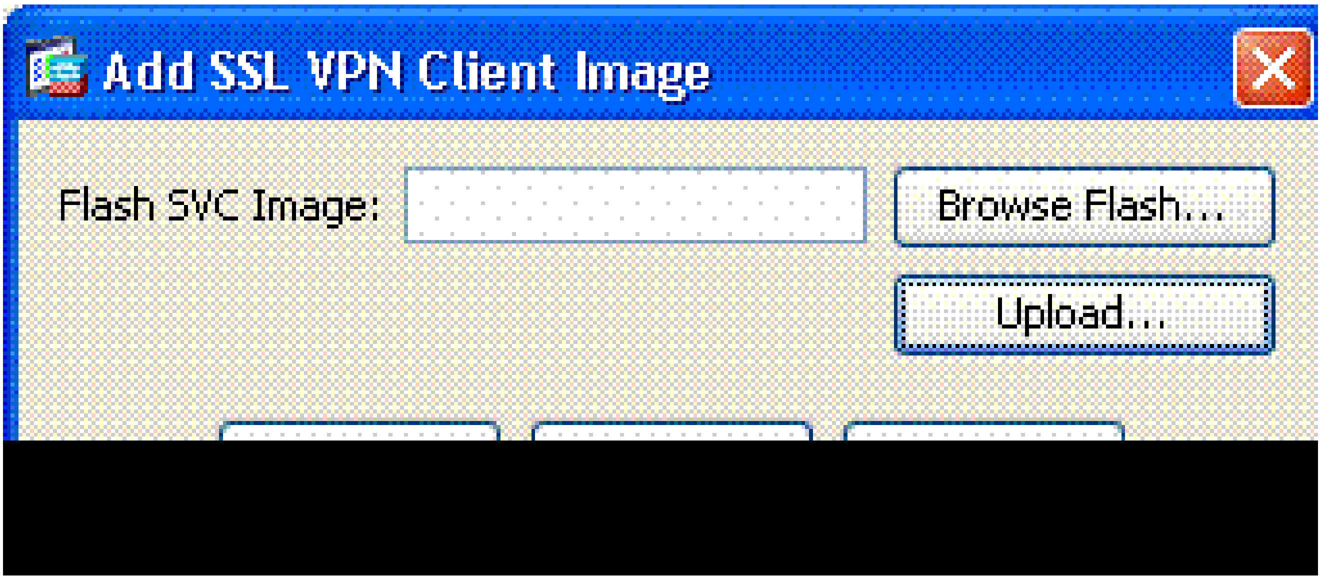
d. 選擇OK。

隧道組介面和映像設定

附註：如果您不想建立新群組，可以使用預設的內建群組。

1. 選擇Remote Access VPN > Network (Client) Access > SSL VPN Connection Profile。
2. 選擇Enable Cisco AnyConnect Client...。
3. 將顯示一個對話方塊，詢問您`Would you like to designate an SVC image`？
4. 選擇Yes。
5. 如果已經存在映像，請選擇要與Browse Flash一起使用的映像。如果不存在映像，請選擇Upload，並瀏覽到本地電腦上的檔案。請參閱圖17。檔案可以從Cisco.com下載，其中包含Windows、MAC和Linux檔案。

圖17：增加SSL VPN客戶端映像

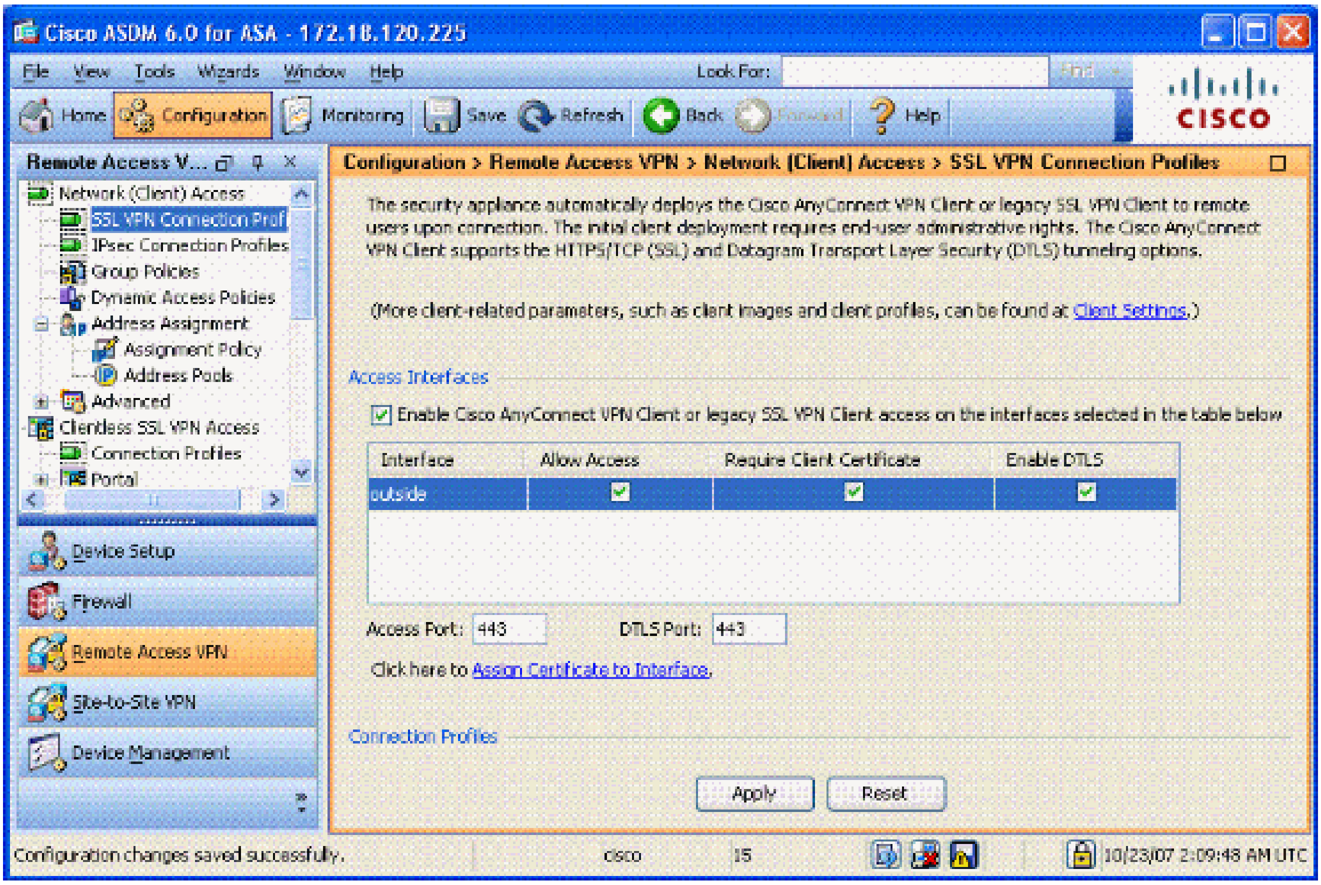


Add SSL VPN Client Image

Flash SVC Image:

6. 然後啟用Allow Access、Require Client Cert，並根據需要啟用Enable DTLS。請參閱圖18。

圖18：啟用存取



Cisco ASDM 6.0 for ASA - 172.18.120.225

Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles

The security appliance automatically deploys the Cisco AnyConnect VPN Client or legacy SSL VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports the HTTPS/TCP (SSL) and Datagram Transport Layer Security (DTLS) tunneling options.

(More client-related parameters, such as client images and client profiles, can be found at Client Settings.)

Access Interfaces

☑ Enable Cisco AnyConnect VPN Client or legacy SSL VPN Client access on the interfaces selected in the table below

Interface	Allow Access	Require Client Certificate	Enable DTLS
outside	☑	☑	☑

Access Port: 443 DTLS Port: 443

Click here to Assign Certificate to Interface.

Connection Profiles

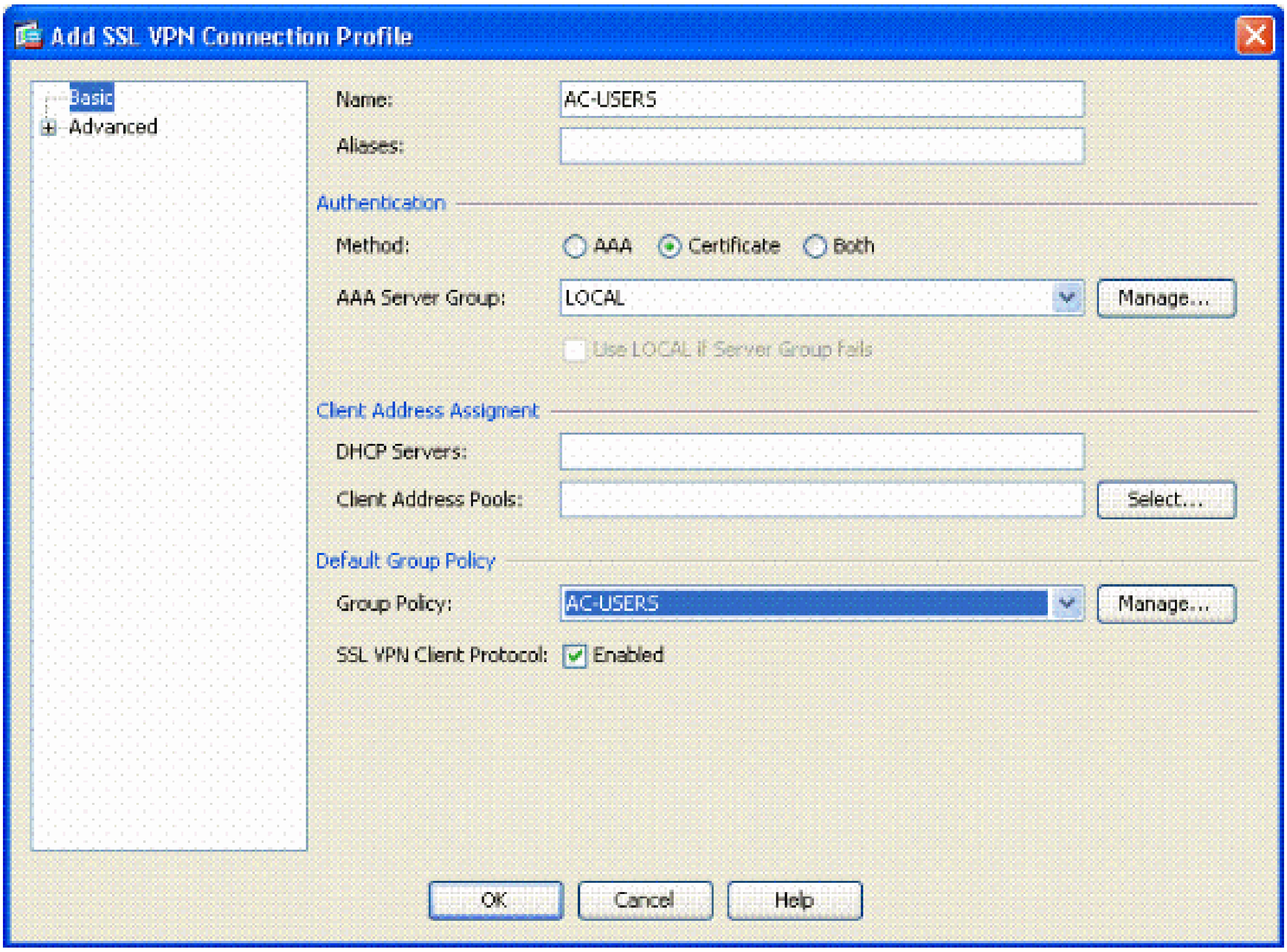
Configuration changes saved successfully. cisco 15 10/23/07 2:09:48 AM UTC

7. 按一下「Apply」。

8. 接下來，建立連線配置檔案/隧道組。選擇Remote Access VPN > Network (Client) Access > SSL VPN Connection Profile。

9. 在Connection Profiles部分中，按一下 Add。

圖19：增加連線配置檔案



Name: AC-USERS

Aliases:

Authentication

Method: ○ AAA ● Certificate ○ Both

AAA Server Group: LOCAL

□ Use LOCAL if Server Group fails

Client Address Assigment

DHCP Servers:

Client Address Pools:

Default Group Policy

Group Policy: AC-USERS

SSL VPN Client Protocol: ☑ Enabled

a. 命名群組。

b. 在身份驗證方法中選擇Certificate。

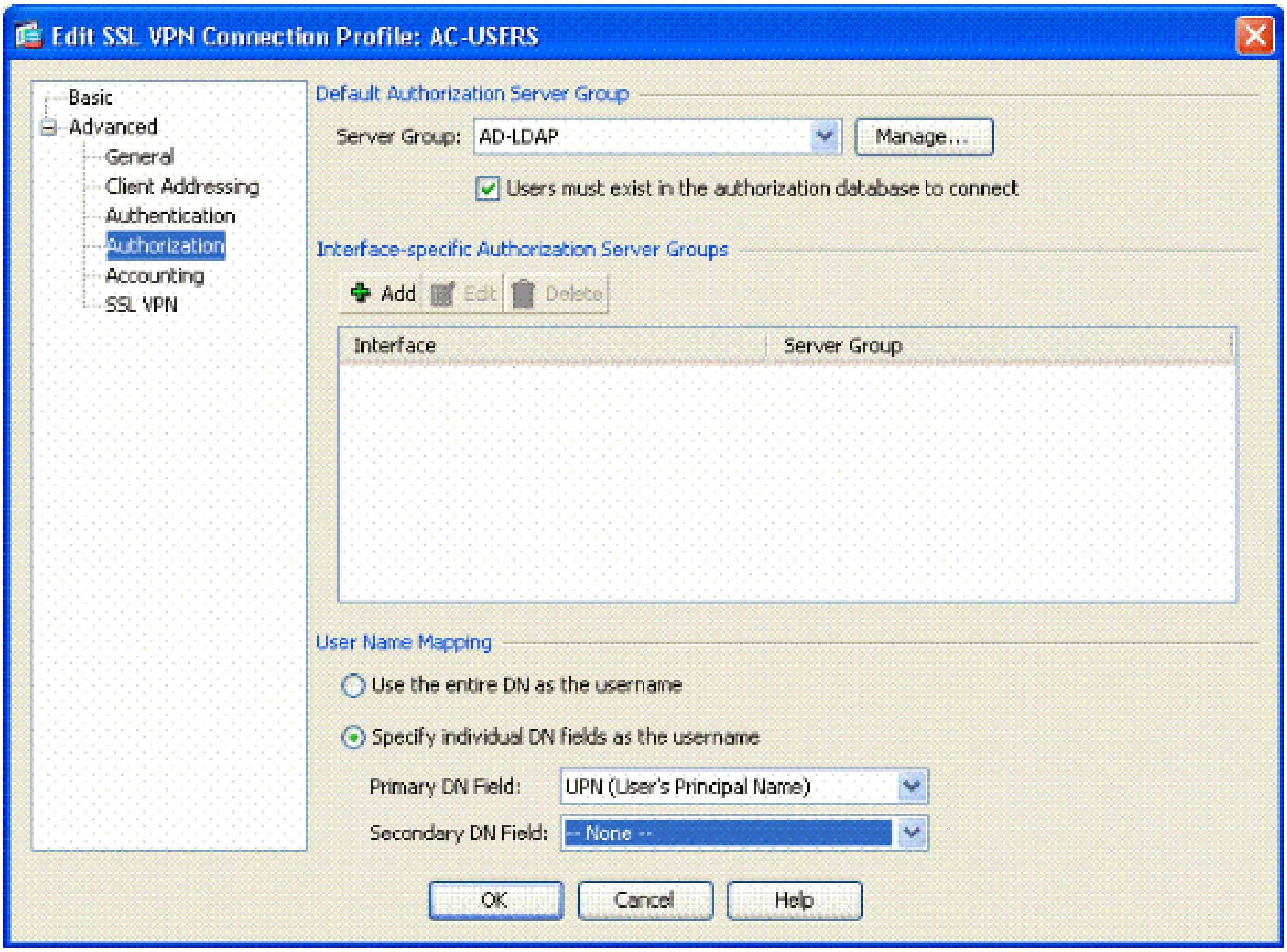
c. 選擇之前建立的組策略。

d. 確保啟用SSL VPN Client。

e. 保留其他選項為預設值。

10. 然後，選擇Advanced > Authorization。請參閱圖20

圖20：授權



Edit SSL VPN Connection Profile: AC-USERS

Default Authorization Server Group

Server Group: AD-LDAP

☑ Users must exist in the authorization database to connect

Interface-specific Authorization Server Groups

Interface	Server Group

User Name Mapping

○ Use the entire DN as the username

● Specify individual DN fields as the username

Primary DN Field: UPN (User's Principal Name)

Secondary DN Field: -- None --

a. 選擇之前建立的AD-LDAP組。

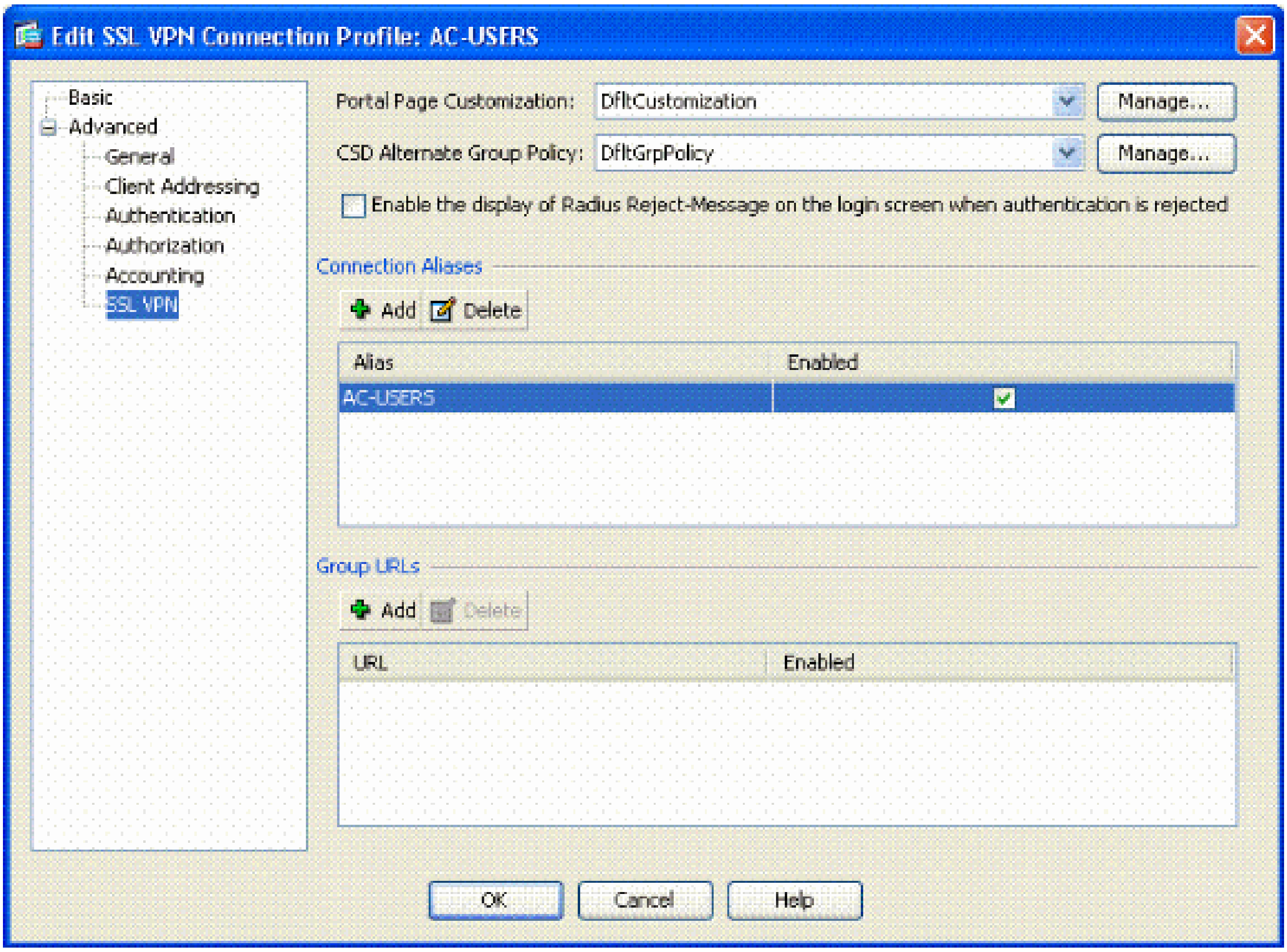
b. 選中Users must exist...to connect。

c. 在對映欄位中，分別為主欄位和輔欄位選擇UPN和none。

11. 選擇選單項SSL VPN。

12. 在Connection Aliases部分中，完成以下步驟：

圖21：連線別名


Edit SSL VPN Connection Profile: AC-USERS

Portal Page Customization: DfltCustomization

CSD Alternate Group Policy: DfltGrpPolicy

□ Enable the display of Radius Reject-Message on the login screen when authentication is rejected

Connection Aliases

Alias	Enabled
AC-USERS	☑

Group URLs

URL	Enabled

a. 選擇Add。

b. 輸入要使用的群組別名。

c. 確保選中Enabled。請參閱圖21。

13. 按一下「OK」（確定）。

注意：按一下Save，以將配置儲存在快閃記憶體中。

證書匹配規則（如果使用OCSP）

1. 選擇Remote Access VPN > Advanced > Certificate to SSL VPN Connection Profile Maps。請參閱圖22。

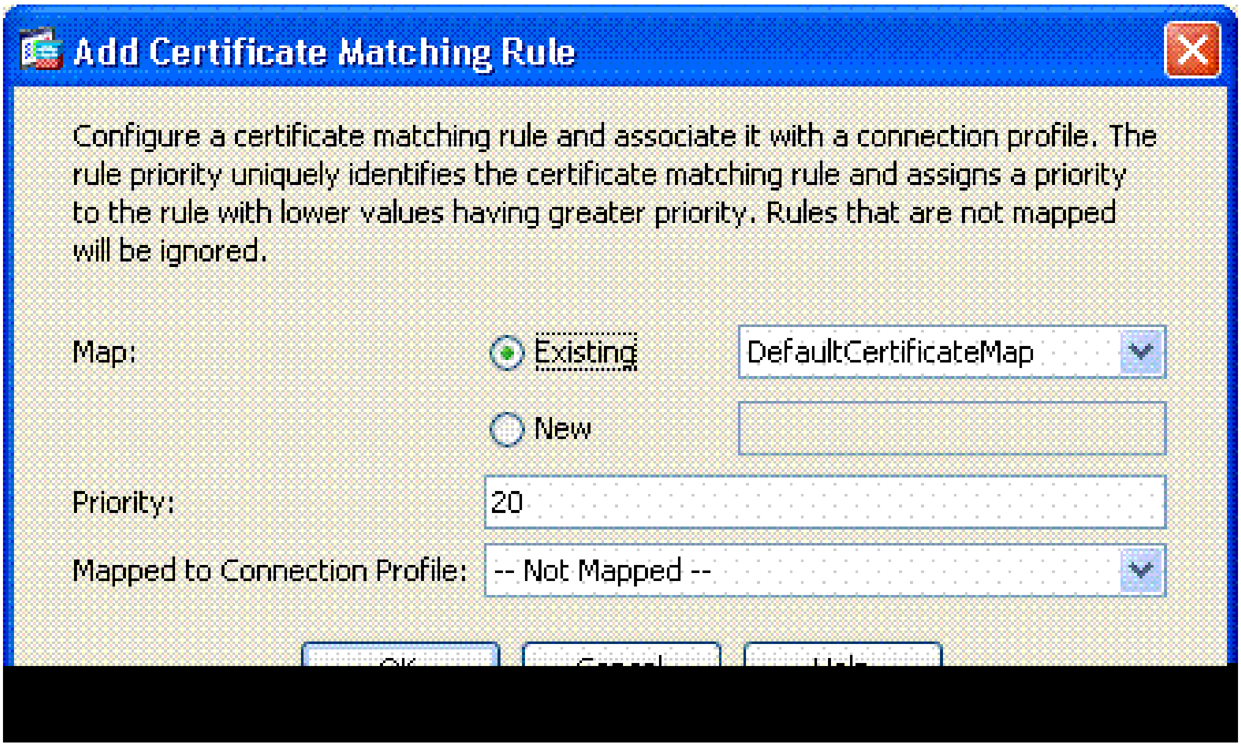
    a. 在Certificate to Connection Profile Maps部分中，選擇Add。

    b. 您可以在對映部分將現有對映保留為DefaultCertificateMap，如果已經為IPsec使用證書對映，則可以建立新對映。

    c. 保留規則優先順序。

    d. 在對映組下，保留為- Not Mapped —。請參閱圖22。

圖22：增加證書匹配規則



Add Certificate Matching Rule

Configure a certificate matching rule and associate it with a connection profile. The rule priority uniquely identifies the certificate matching rule and assigns a priority to the rule with lower values having greater priority. Rules that are not mapped will be ignored.

Map: ● Existing DefaultCertificateMap

○ New

Priority: 20

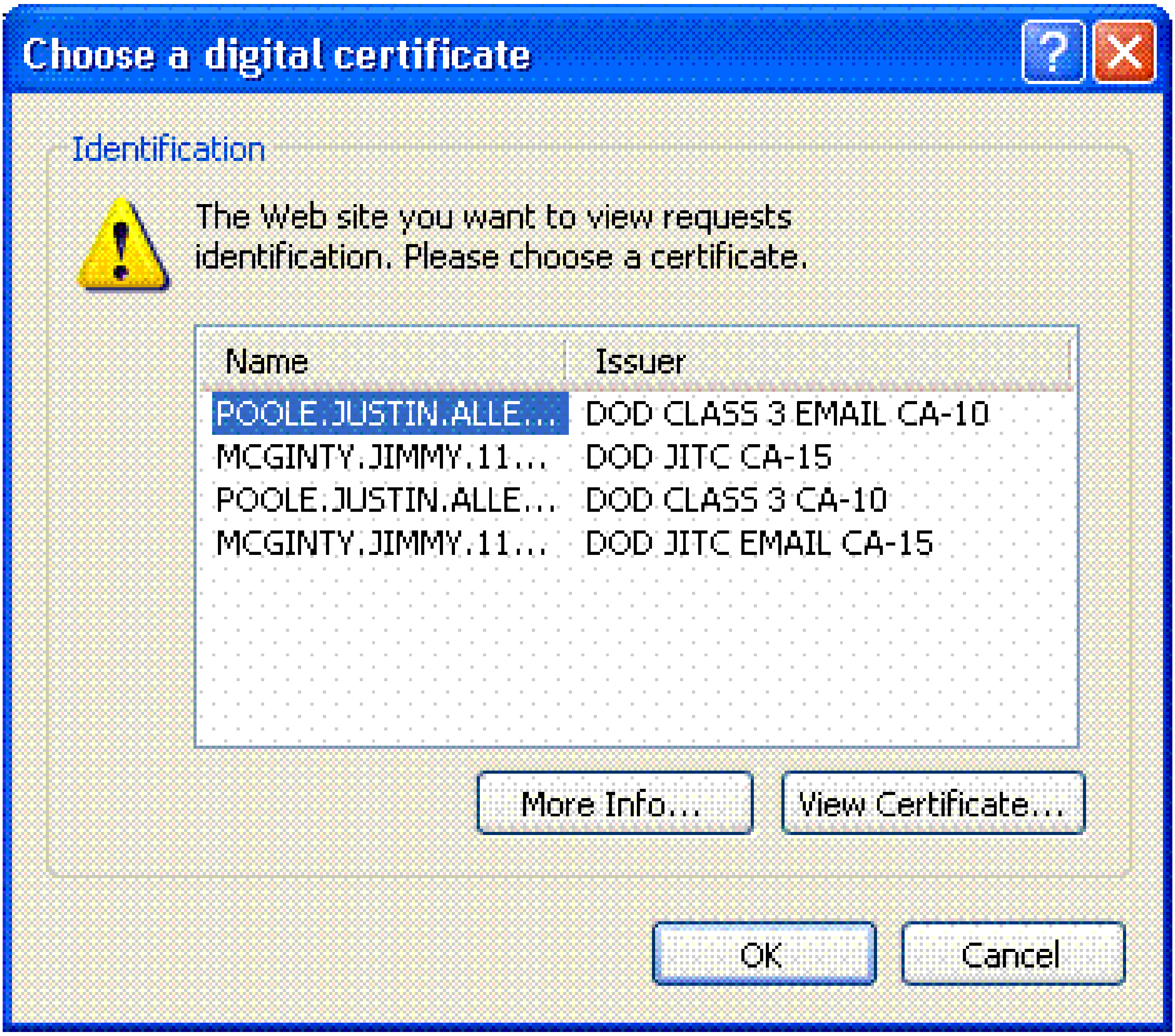
Mapped to Connection Profile: -- Not Mapped --

e. 按一下「OK」（確定）。

2. 在底部表上按一下Add。

3. 在Add certificate Matching Rule Criterion窗口中，完成以下步驟：

圖23：證書匹配規則條件



The Web site you want to view requests identification. Please choose a certificate.

Name	Issuer
POOLE.JUSTIN.ALLE...	DOD CLASS 3 EMAIL CA-10
MCGINTY.JIMMY.11...	DOD JITC CA-15
POOLE.JUSTIN.ALLE...	DOD CLASS 3 CA-10
MCGINTY.JIMMY.11...	DOD JITC EMAIL CA-15

a. 保留Field列的預設值Subject。

b. 保留Component列的預設值Whole Field。

c. 將Operator列更改為Does Not Equal。

d. 在Value列中，輸入兩個雙引號「」。

e. 按一下Ok和Apply。例如，請參見圖23。

配置OCSP

OCSP的配置可能有所不同，具體取決於OCSP響應方供應商。有關詳細資訊，請閱讀供應商手冊。

配置OCSP響應方證書

1. 從OCSP響應方獲取自行生成的證書。

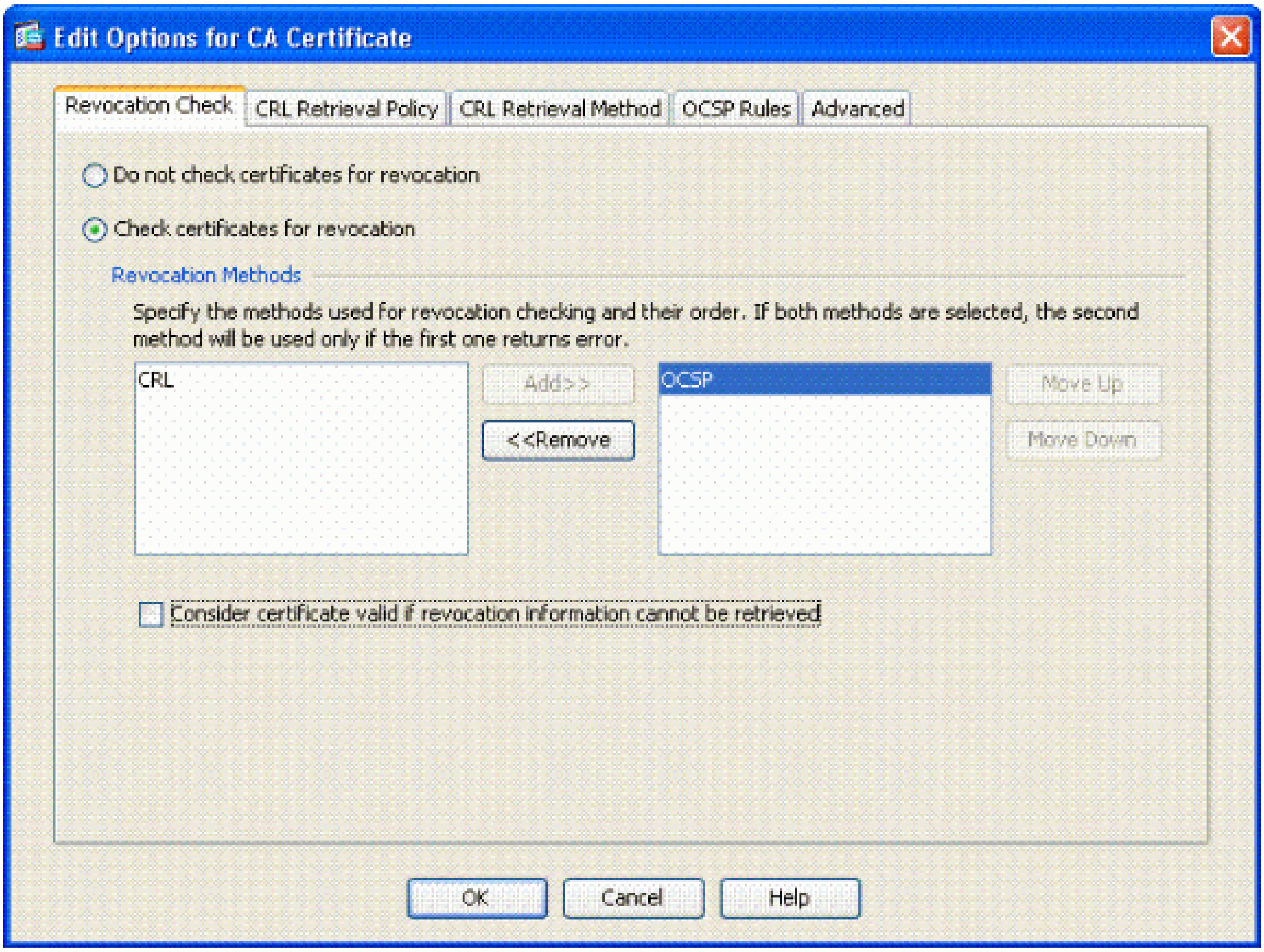
2. 完成前面提到的步驟，並為OSCP伺服器安裝證書。

注意：確保為OCSP證書信任點選中Do not check certificates for revocation。

配置CA以使用OCSP

1. 選擇Remote Access VPN> Certificate Management > CA Certificates。
2. 突出顯示OCSP，以選擇要配置為使用OCSP的CA。
3. 按一下Edit。
4. 確保選中Check certificate for revocation。
5. 在Revocation Methods部分中，增加OCSP。請參閱圖24。

   OCSP撤銷檢查



Edit Options for CA Certificate

Revocation Check | CRL Retrieval Policy | CRL Retrieval Method | OCSP Rules | Advanced

○ Do not check certificates for revocation

● Check certificates for revocation

Revocation Methods

Specify the methods used for revocation checking and their order. If both methods are selected, the second method will be used only if the first one returns error.

CRL

OCSP

□ Consider certificate valid if revocation information cannot be retrieved

6. 如果要遵循嚴格的OCSP檢查，請確保取消選中Consider Certificate valid...cannot be retrieved。

注意：配置/編輯使用OCSP進行吊銷的所有CA伺服器。

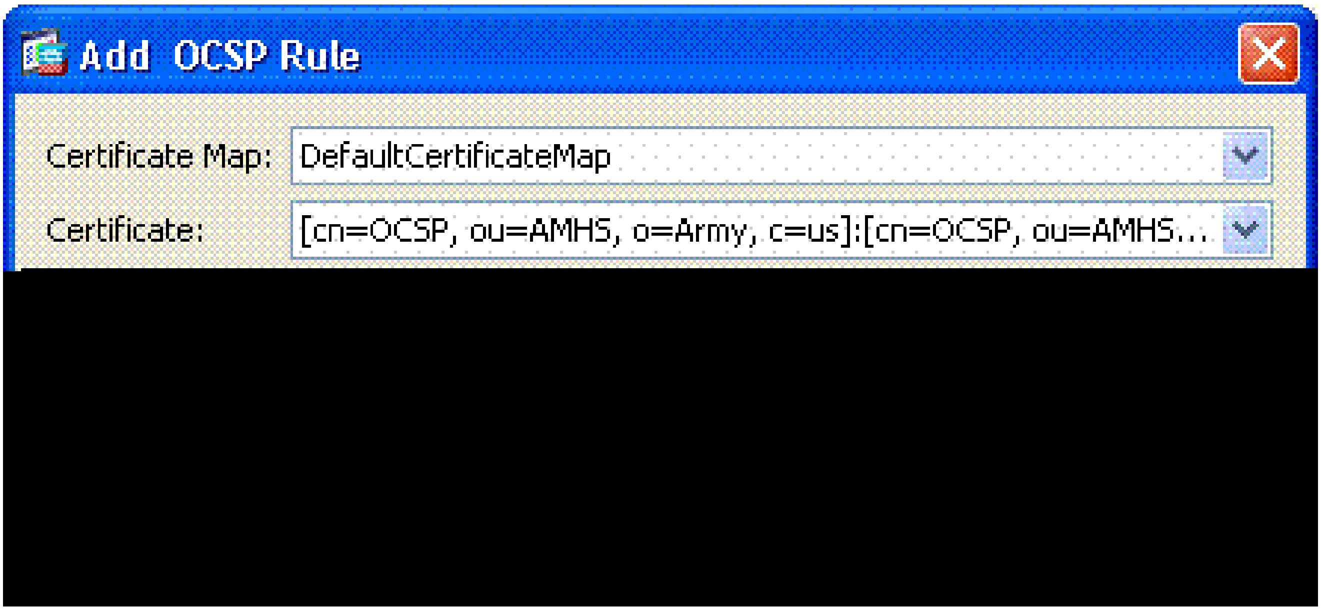
配置OCSP規則

注意：完成以下步驟之前，請驗證是否已建立證書組匹配策略以及是否配置了OCSP響應程式
。

注意：在某些OCSP實施中，ASA可能需要DNS A和PTR記錄。此檢查是為了驗證ASA是否來自.mil站點。

1. 選擇Remote Access VPN> Certificate Management > CA Certificates 2。
2. 突出顯示OCSP，以選擇要配置為使用OCSP的CA。
3. 選擇Edit。
4. 按一下OCSP Rule頁籤。
5. 按一下Add。
6. 在「增加OCSP規則」窗口中，完成以下步驟。請參閱圖25。

圖25：增加OCSP規則



Certificate Map: DefaultCertificateMap

Certificate: [cn=OCSP, ou=AMHS, o=Army, c=us]:[cn=OCSP, ou=AMHS...

[redacted]

   a. 在Certificate Map選項中，選擇DefaultCertificateMap或之前建立的對映。
   b. 在Certificate選項中，選擇OCSP responder。
   c. 在index選項中，輸入10。
   d. 在URL選項中，輸入OCSP響應方的IP地址或主機名。如果使用主機名，請確保在ASA上配置了DNS伺服器。
   e. 按一下「OK」（確定）。

f. 按一下「Apply」。

Cisco AnyConnect客戶端配置

本節介紹Cisco AnyConnect VPN客戶端的配置。

假設 -已在主機PC上安裝Cisco AnyConnect VPN客戶端和中介軟體應用程式。已測試ActivCard Gold和ActivClient。

> 注意：本指南僅將group-url方法用於初始AC客戶端安裝。安裝AC客戶端後，您就可以像IPSec客戶端一樣啟動AC應用程式。

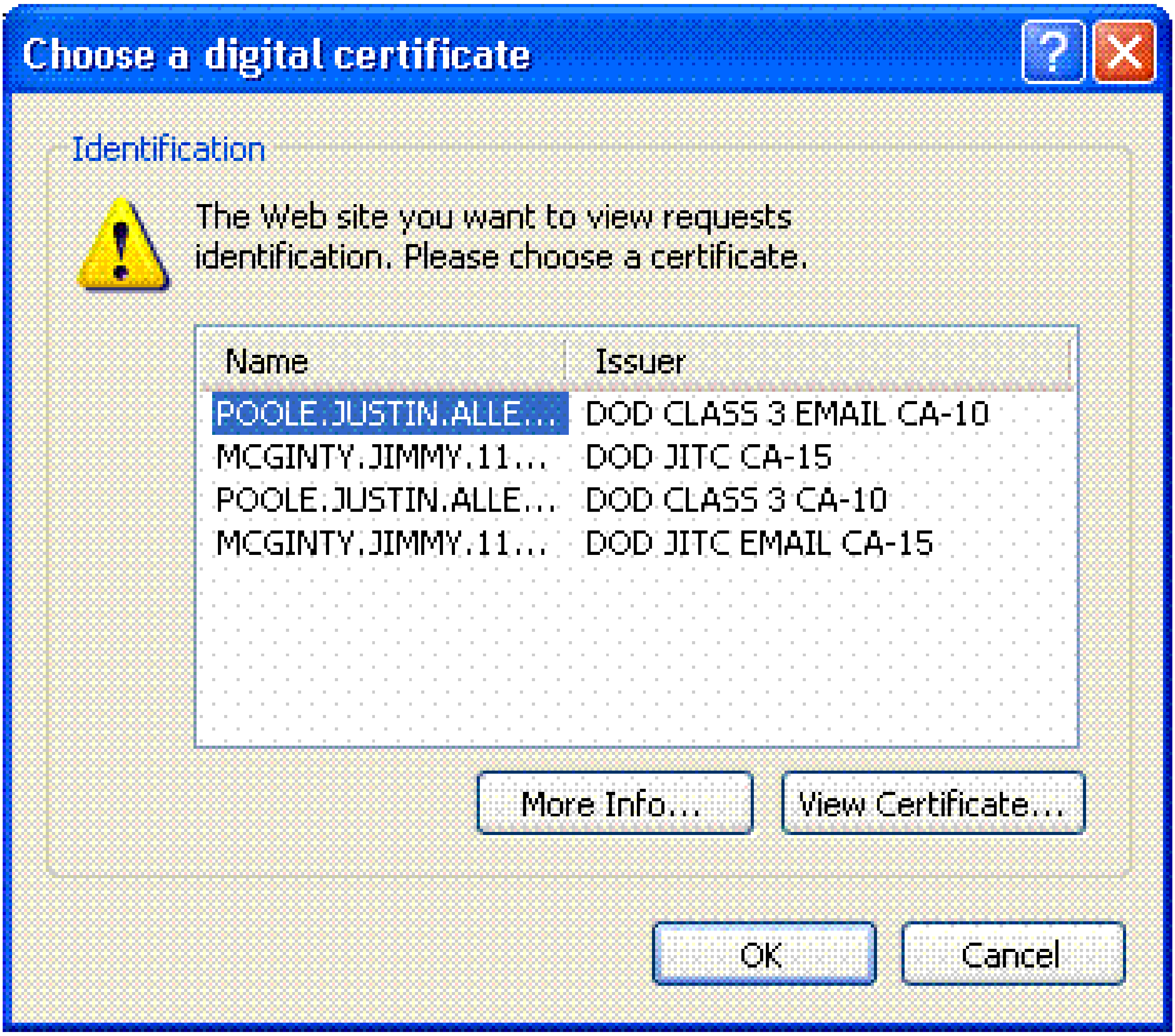
> 注意：需要在本地電腦上安裝DoD證書鏈。請向PKI POC檢查以獲得證書/批處理檔案。

下載Cisco Anyconnect VPN客戶端- Windows

1. 透過Internet Explorer啟動到ASA的Web會話。地址的格式應為https://Outside-Interface。例如，https://172.18.120.225。

2. 選擇要用於訪問的簽名證書。請參閱圖26。

   圖26：選擇正確的證書



Choose a digital certificate

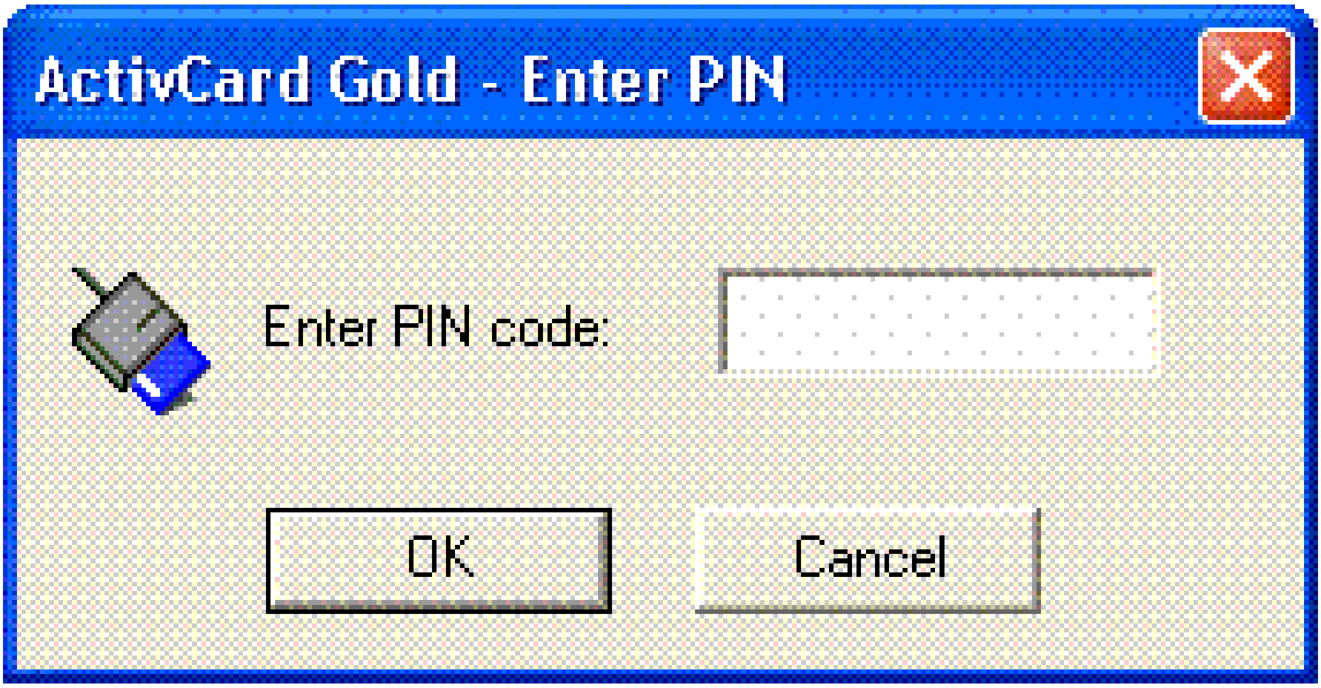
Identification

The Web site you want to view requests identification. Please choose a certificate.

Name	Issuer
POOLE.JUSTIN.ALLE...	DOD CLASS 3 EMAIL CA-10
MCGINTY.JIMMY.11...	DOD JITC CA-15
POOLE.JUSTIN.ALLE...	DOD CLASS 3 CA-10
MCGINTY.JIMMY.11...	DOD JITC EMAIL CA-15

3. 出現提示時，輸入您的PIN。

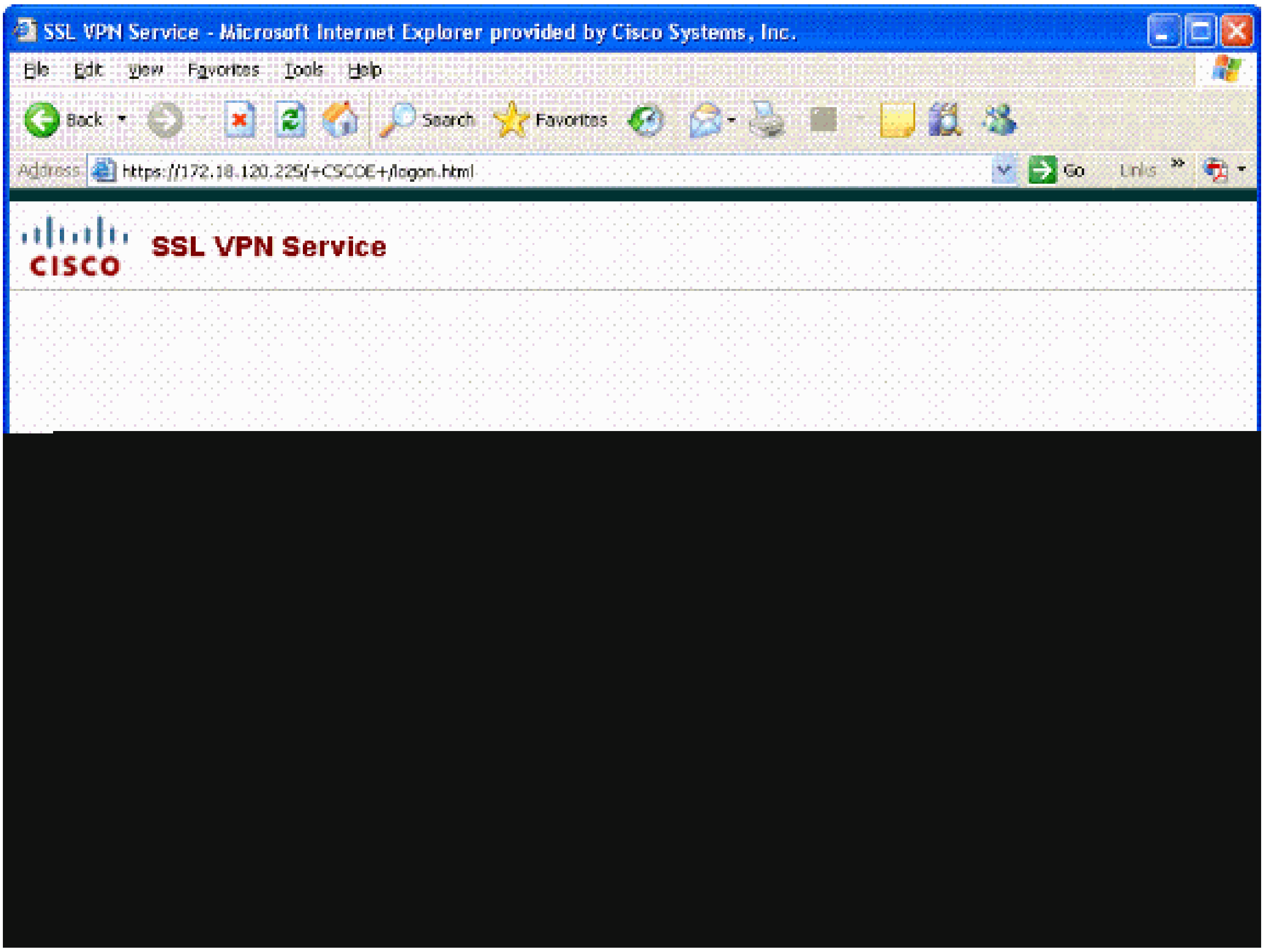
圖27：輸入PIN



4. 選擇Yes以接受安全警報。

5. 出現SSL Login頁面後，選擇Login。使用者端憑證用於登入。請參閱圖28。

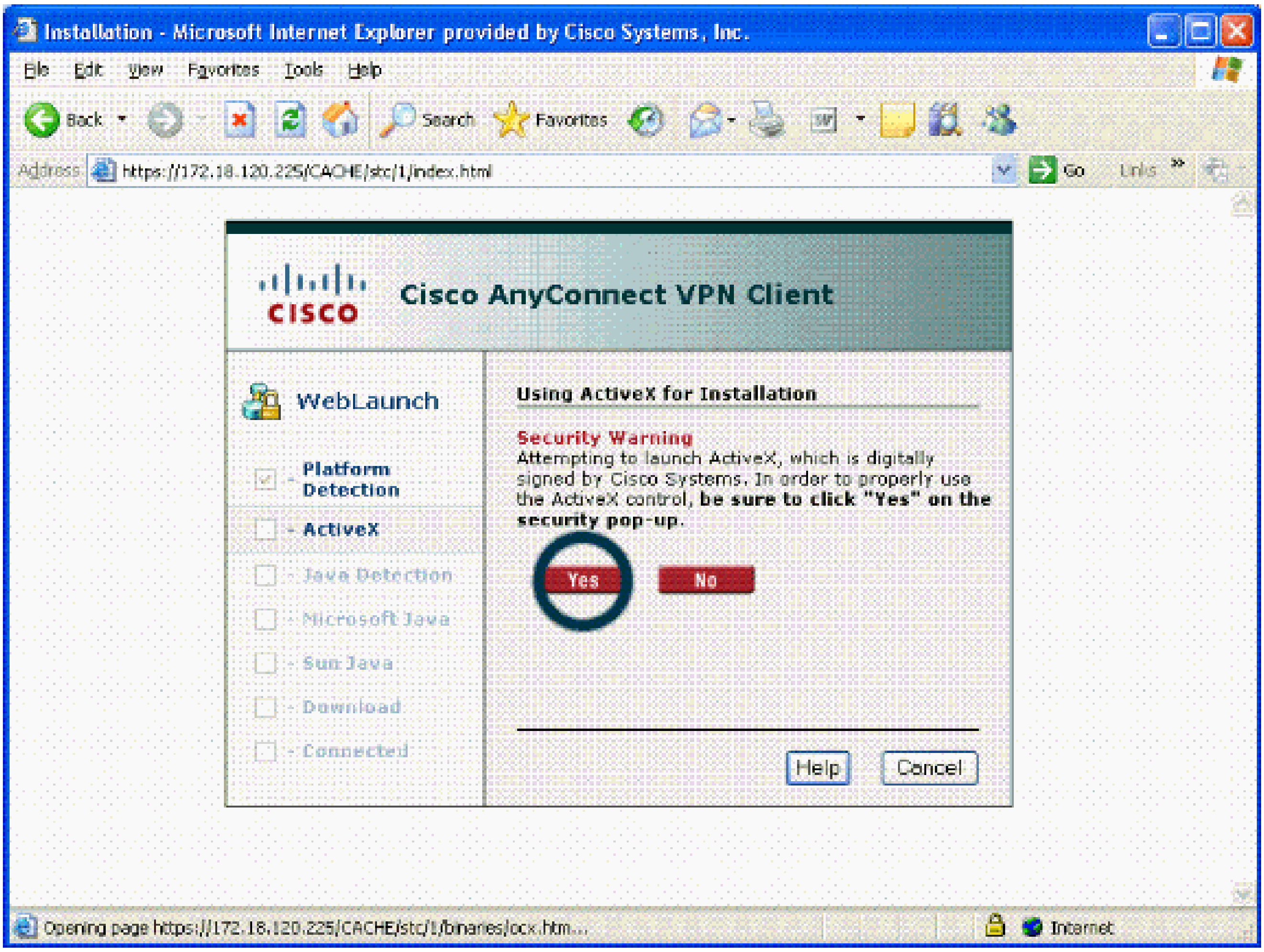
圖28： SSL登入



https://172.18.120.225/+CSCOE+/logon.html

6. AnyConnect開始下載客戶端。請參閱圖29。

圖29：安裝AnyConnect



Installation - Microsoft Internet Explorer provided by Cisco Systems, Inc.

https://172.18.120.225/CACHE/stc/1/index.html

Cisco AnyConnect VPN Client

Using ActiveX for Installation

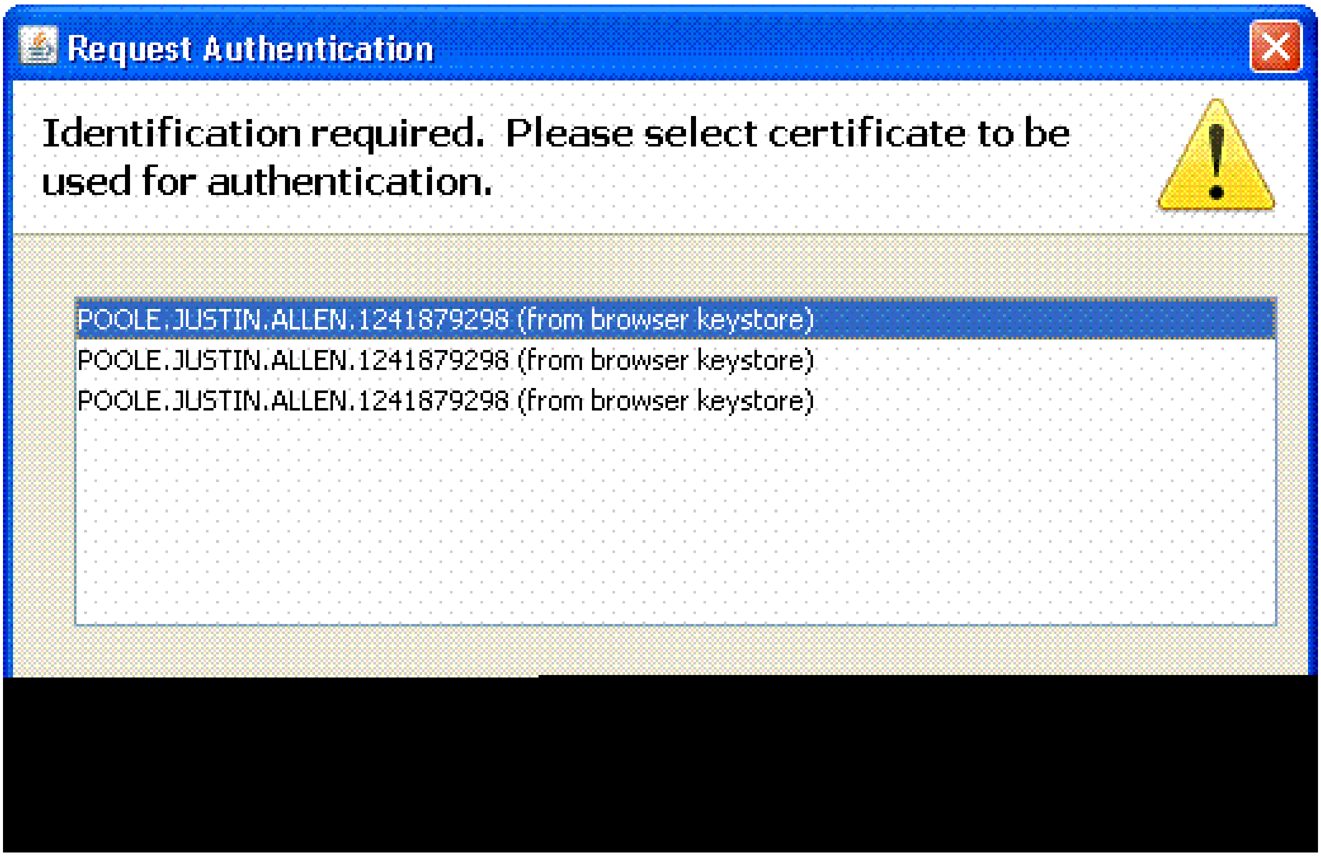
Security Warning

Attempting to launch ActiveX, which is digitally signed by Cisco Systems. In order to properly use the ActiveX control, **be sure to click "Yes" on the security pop-up.**

Opening page https://172.18.120.225/CACHE/stc/1/binaries/ocx.htm...

7. 選擇要使用的相應證書。請參閱圖30。AnyConnect繼續安裝。ASA管理員可允許客戶端在每個ASA連線上永久安裝或安裝。

圖30：證書



Identification required. Please select certificate to be used for authentication.

POOLE.JUSTIN.ALLEN.1241879298 (from browser keystore)
POOLE.JUSTIN.ALLEN.1241879298 (from browser keystore)
POOLE.JUSTIN.ALLEN.1241879298 (from browser keystore)

[redacted]

啟動Cisco AnyConnect VPN客戶端- Windows

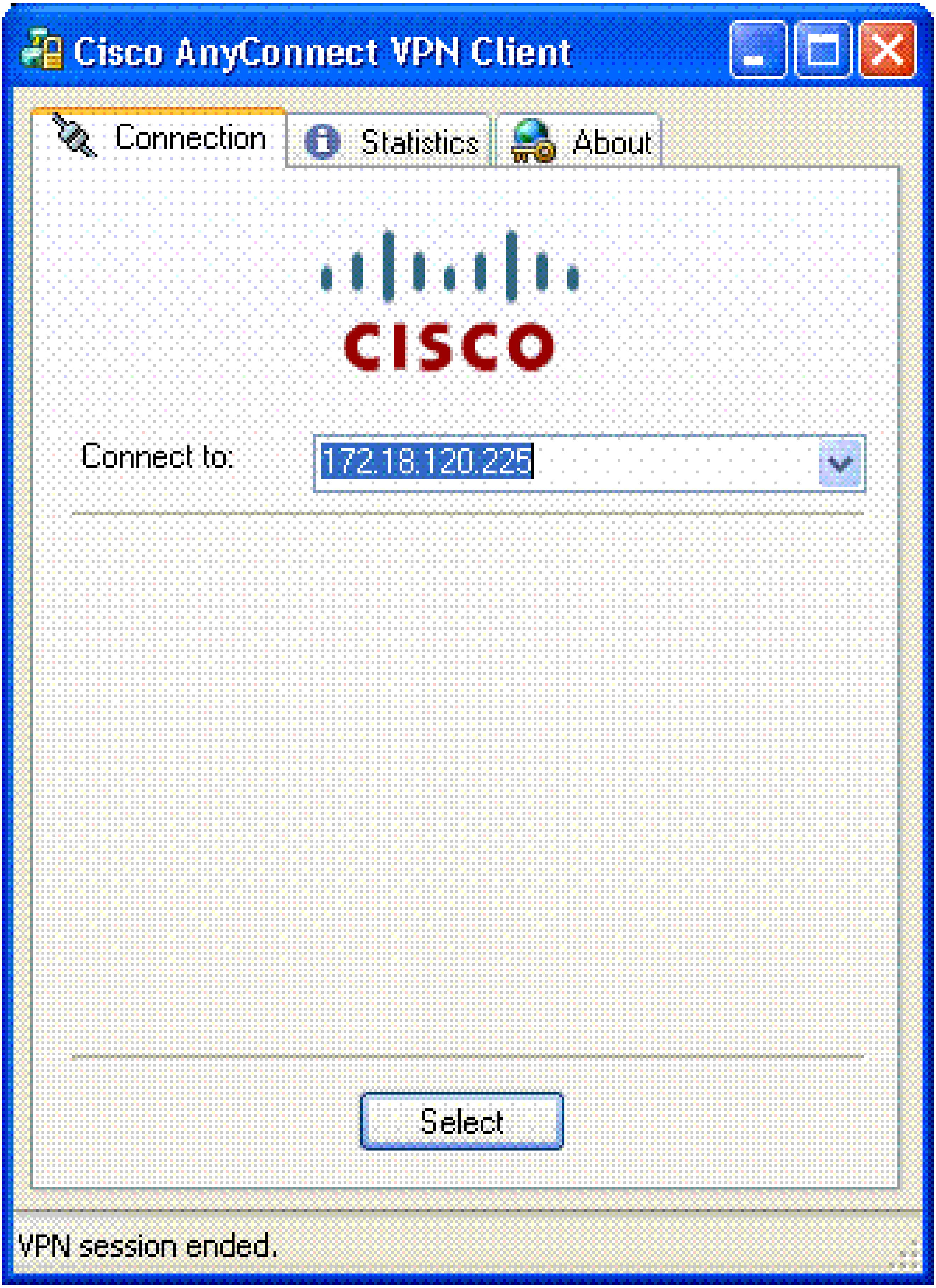
從主機PC上，選擇「開始」>「所有程式」>「Cisco」>「AnyConnect VPN客戶端」。

註：有關可選AnyConnect客戶端配置檔案配置，請參閱附錄E。

新建連線

1. 出現AC窗口。請參閱圖34。

   圖34：新VPN連線



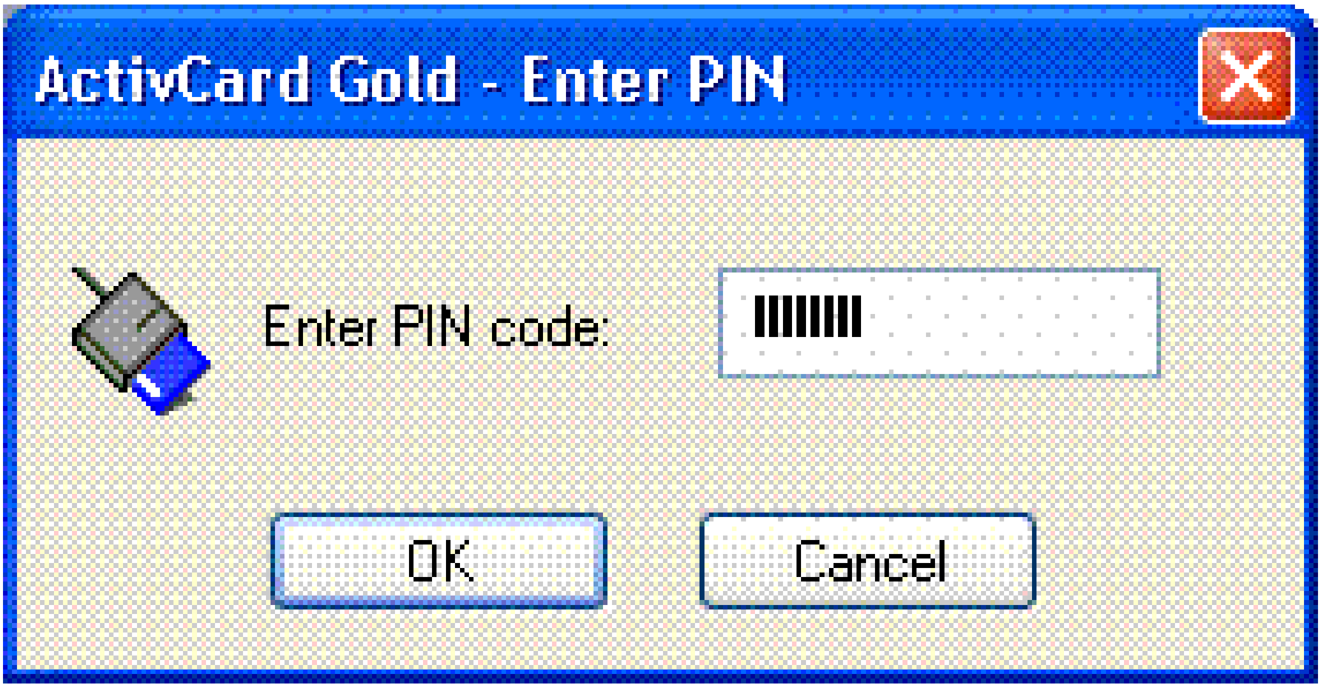
Connect to: 172.18.120.225

VPN session ended.

2. 如果AC沒有自動嘗試連線，請選擇適當的主機。

3. 出現提示時，輸入您的PIN。請參閱圖35。

圖35：輸入PIN

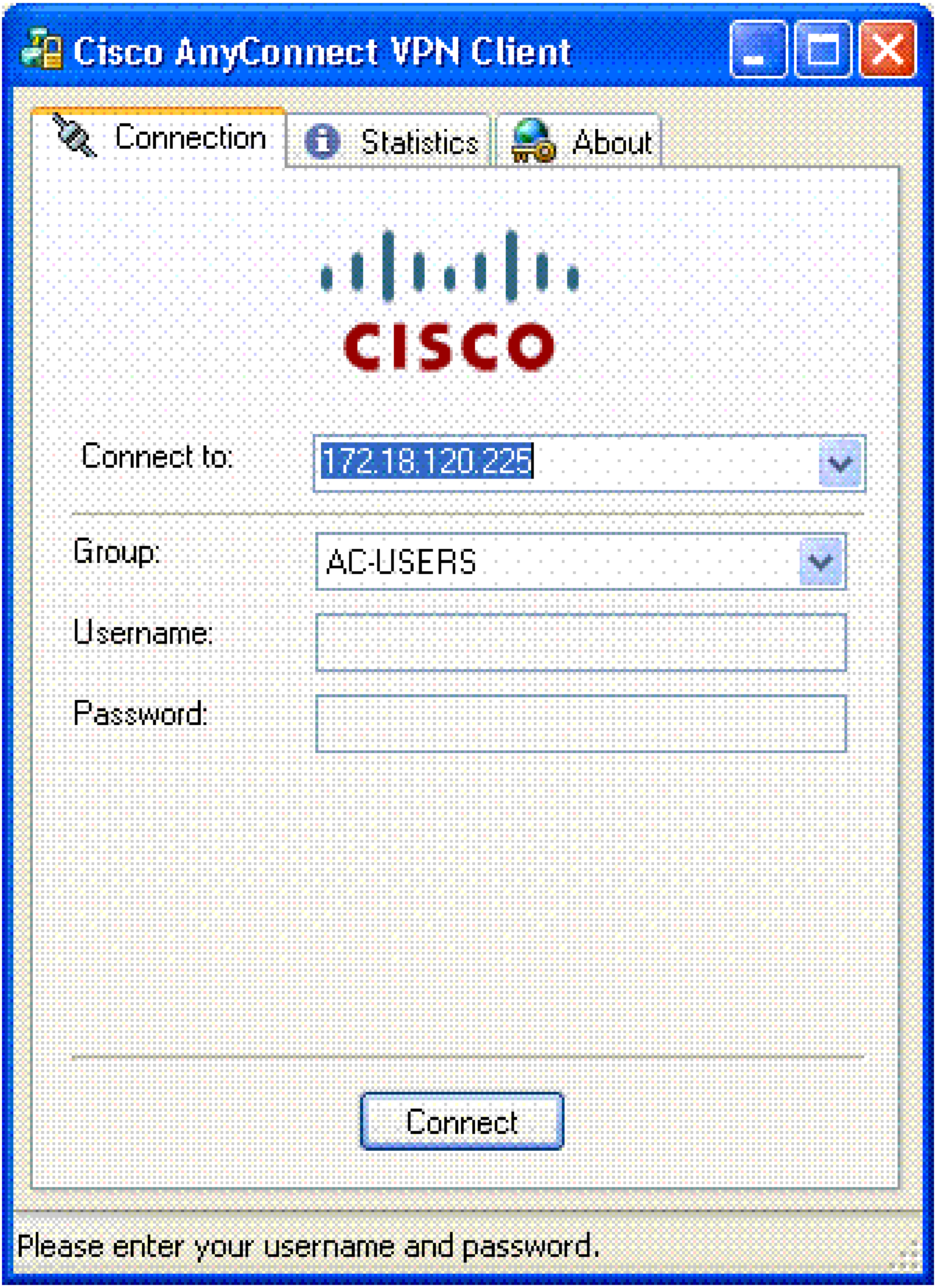


啟動遠端存取

選擇要連線的組和主機。

因為使用證書，請選擇Connect 以建立VPN。請參閱圖36。

圖36：連線



Connect to: 172.18.120.225

Group: AC-USERS

Username:

Password:

Please enter your username and password.

注意：由於連線使用證書，因此不需要輸入使用者名稱和密碼。

註：有關可選AnyConnect客戶端配置檔案配置，請參閱附錄E。

附錄A - LDAP對映和DAP

在ASA/PIX版本7.1(x)及更高版本中，引入了稱為LDAP對映的功能。這是一項強大的功能，可提供Cisco屬性與LDAP對象/屬性之間的對映，從而無需更改LDAP架構。對於CAC身份驗證實施，這可以支援遠端訪問連線上的其他策略實施。以下是LDAP對映的示例。請注意，您需要具有管理員許可權才能在AD/LDAP伺服器中進行變更。在ASA 8.x軟體中，引入了動態訪問策略(DAP)功能。DAP可以與CAC結合使用，檢視多個AD組以及推送策略、ACL等。

方案1：使用遠端訪問許可權撥入實施Active Directory -允許/拒絕訪問

此示例將AD屬性msNPAllowDailin對映到Cisco屬性cVPN3000-Tunneling-Protocol。

- AD屬性值：TRUE =允許；FALSE =拒絕
- Cisco屬性值：1 = FALSE、4 (IPSec)或20 (4 IPSEC + 16 WebVPN) = TRUE、

對於ALLOW條件，進行以下對映：

- 真= 20

對於DENY撥入條件，進行以下對映：

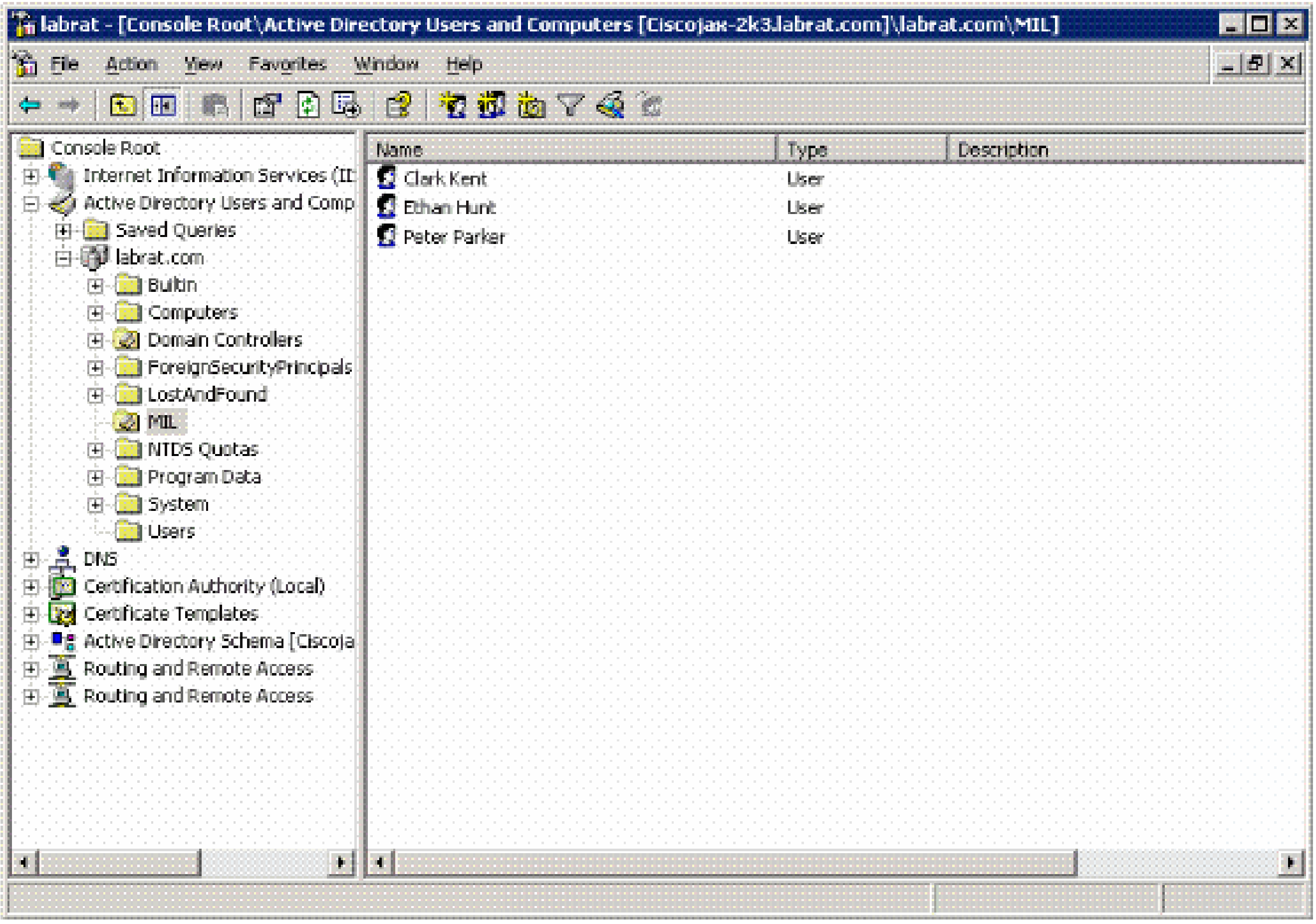
- FALSE = 1

注意：確保TRUE和FALSE全部大寫。有關詳細資訊，請參閱配置外部伺服器以便進行安全裝置使用者授權。

Active Directory安裝

1. 在Active Directory伺服器中，按一下Start > Run。
2. 在Open文本框中，鍵入dsa.msc，然後按一下Ok。這會啟動Active Directory管理主控台。
3. 在Active Directory管理控制檯中，按一下加號以展開「Active Directory使用者和電腦」。
4. 按一下加號以展開域名。
5. 如果您已為使用者建立OU，請展開OU以檢視所有使用者；如果您在「使用者」資料夾中指定所有使用者，請展開該資料夾以檢視使用者。請參閱圖A1。

   圖A1： Active Directory管理控制檯

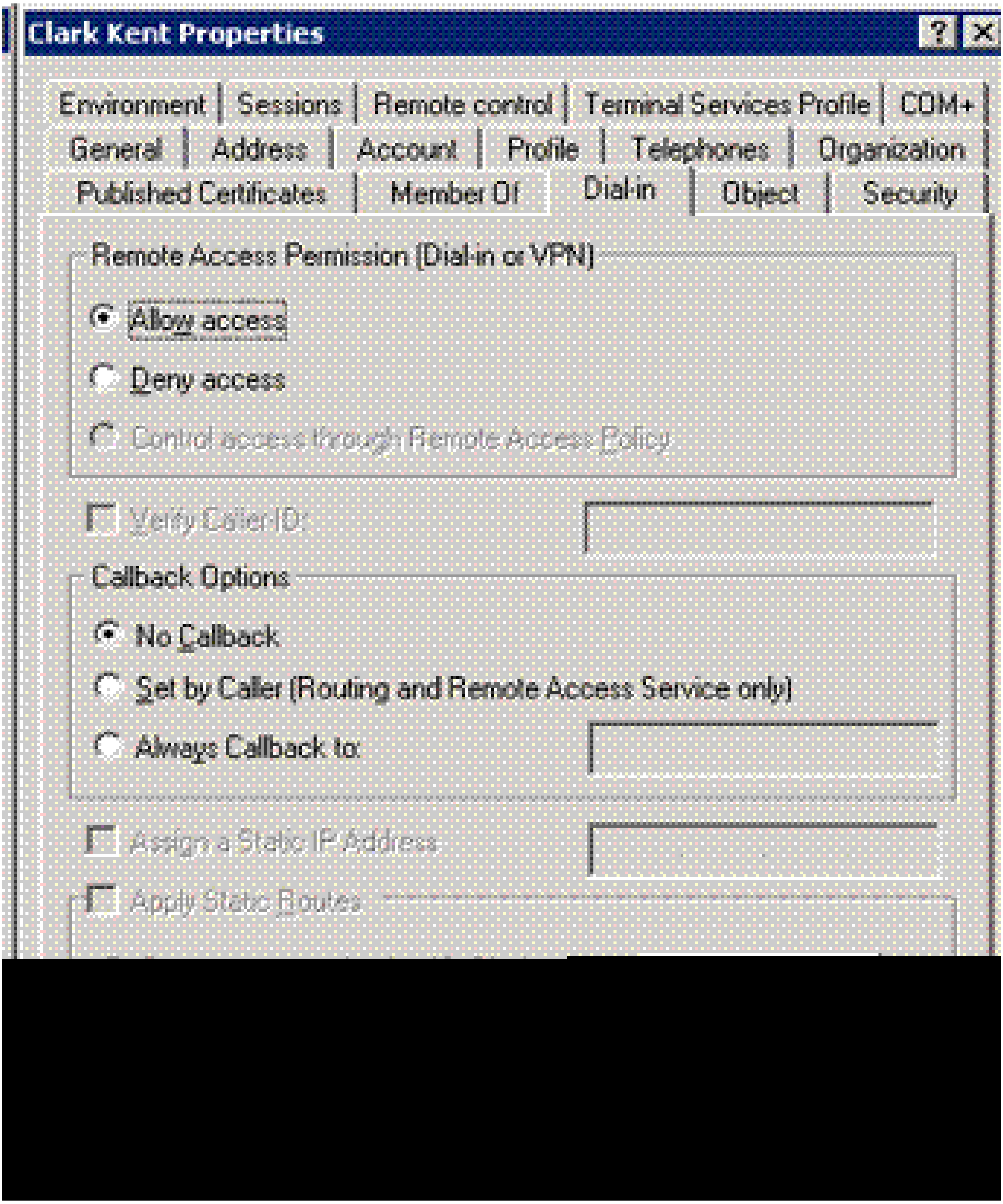

labrat - [Console Root\Active Directory Users and Computers [Ciscojax-2k3.labrat.com]\labrat.com\MIL]
File
Action
View
Favorites
Window
Help
Console Root
Internet Information Services (II
Active Directory Users and Comp
Saved Queries
labrat.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
LostAndFound
MIL
NTDS Quotas
Program Data
System
Users
DNS
Certification Authority (Local)
Certificate Templates
Active Directory Schema [Ciscoja
Routing and Remote Access
Routing and Remote Access

Name	Type	Description
Clark Kent	User	
Ethan Hunt	User	
Peter Parker	User	

6. 按兩下要編輯的使用者。

按一下使用者屬性頁中的Dial-in頁籤，並按一下Allow或deny。請參閱圖A2。

圖A2：使用者屬性



Clark Kent Properties

Environment | Sessions | Remote control | Terminal Services Profile | COM+
General | Address | Account | Profile | Telephones | Organization
Published Certificates | Member Of | Dial-in | Object | Security

Remote Access Permission (Dial-in or VPN)

● Allow access

○ Deny access

○ Control access through Remote Access Policy

□ Verify Caller-ID:

Callback Options

● No Callback

○ Set by Caller (Routing and Remote Access Service only)

○ Always Callback to:

□ Assign a Static IP Address

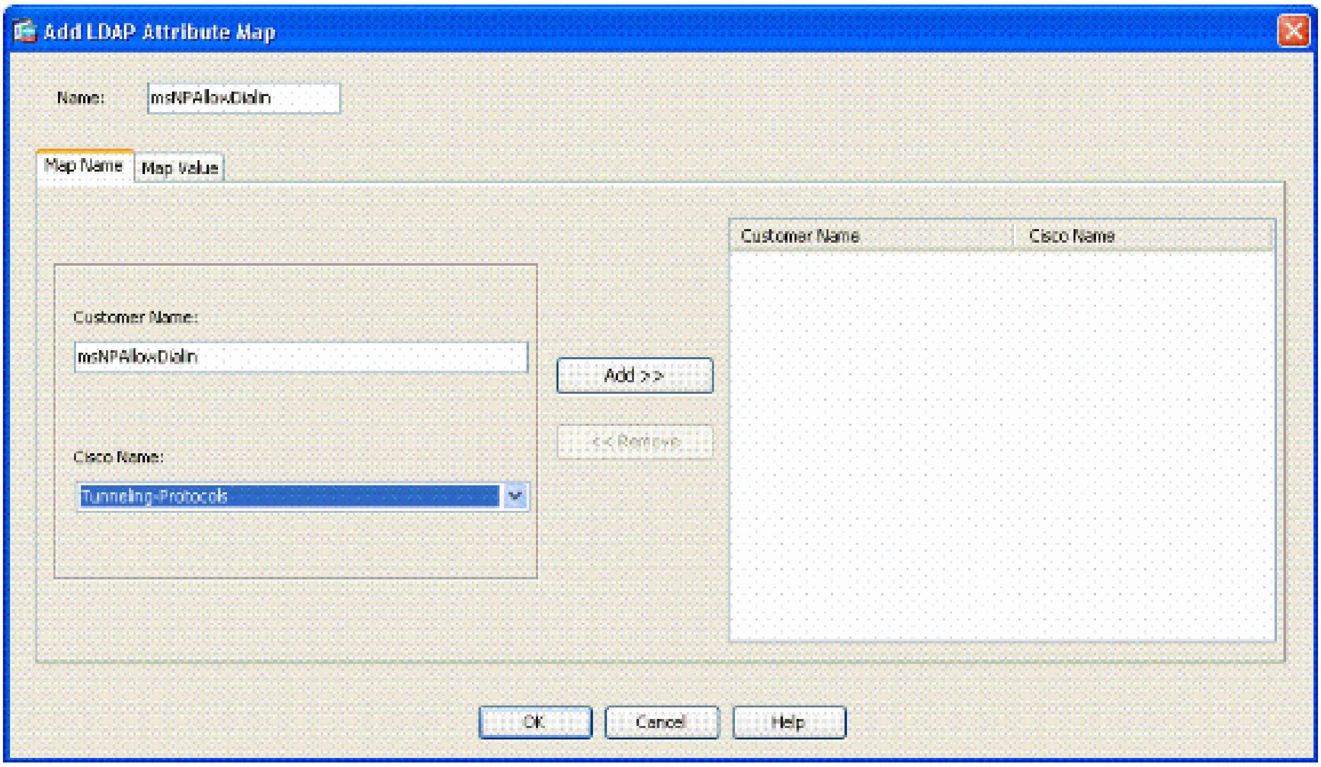
□ Apply Static Routes

7. 然後按一下Ok。

ASA配置

1. 在ASDM中，選擇Remote Access VPN> AAA Setup > LDAP Attribute Map。
2. 按一下Add。
3. 在Add LDAP Attribute Map窗口中，完成以下步驟。請參閱圖A3。

圖A3：增加LDAP屬性對映



Name: msNPAllowDialin

Customer Name: msNPAllowDialin

Cisco Name: Tunneling-Protocols

a. 在「名稱」文字方塊中輸入名稱。

b. 在Map Name頁籤中，在Customer Name文本框中鍵入msNPAllowDialin。

c. 在Map Name頁籤中，從Cisco Name的下拉選項中選擇Tunneling-Protocols。

d. 按一下Add。

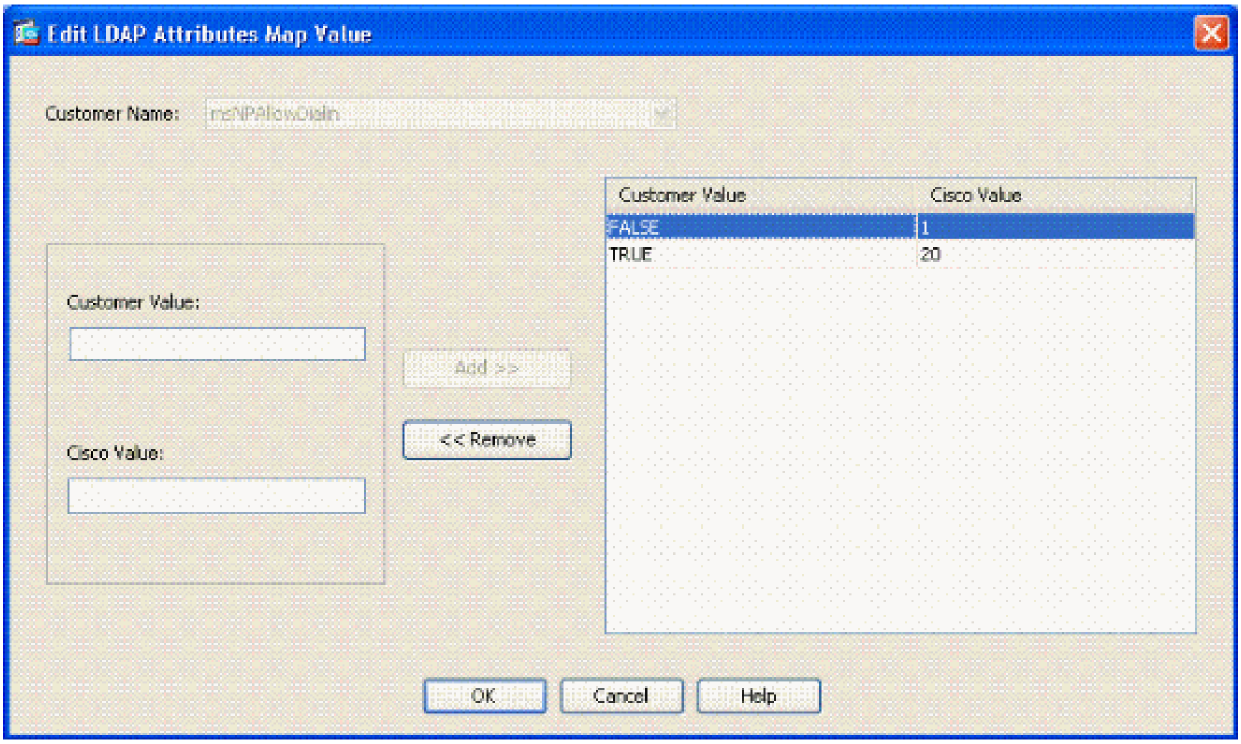
e. 選擇Map Value頁籤。

f. 按一下Add。

g. 在Add Attribute LDAP Map Value窗口中，在Customer Name文本框中鍵入TRUE，並在Cisco Value文本框中鍵入20。

h. 按一下Add。

i. 在Customer Name文本框中鍵入FALSE，並在Cisco Value文本框中鍵入1。請參閱圖A4。



Edit LDAP Attributes Map Value

Customer Name: msNPAllowDialin

Customer Value	Cisco Value
FALSE	1
TRUE	20

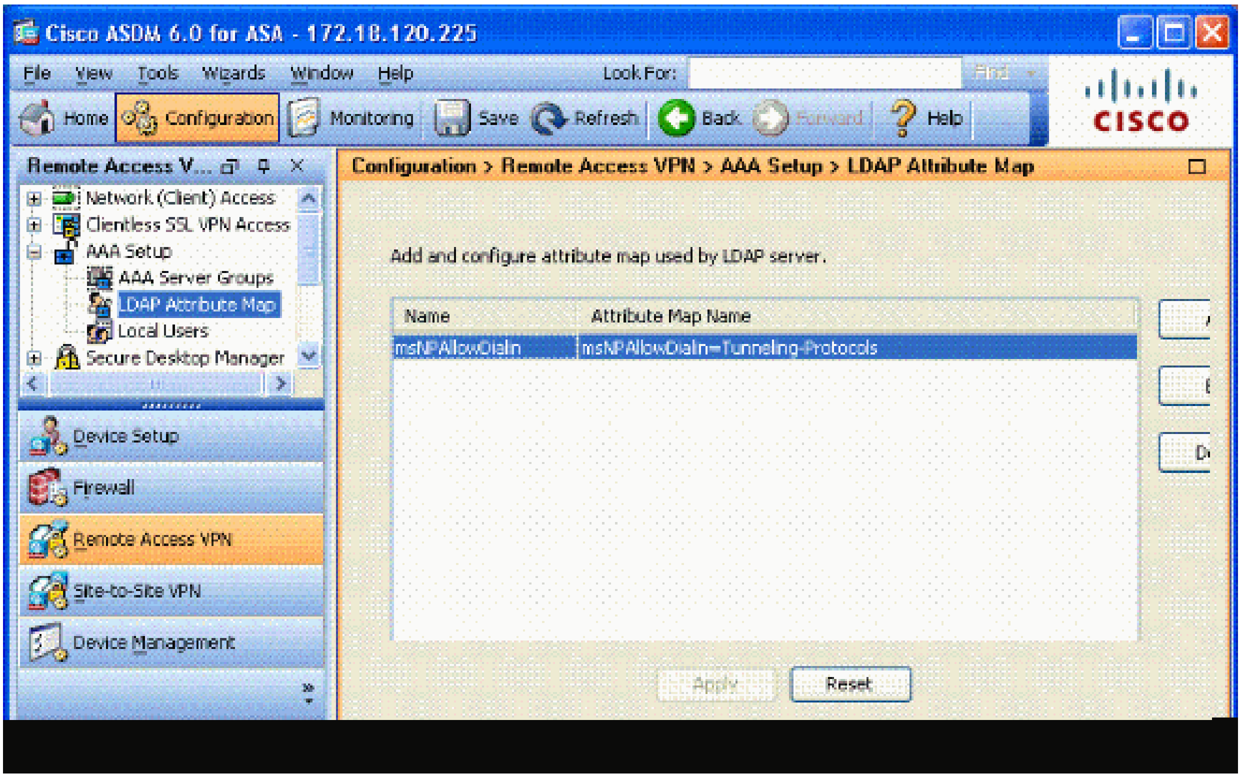
j. 按一下「OK」（確定）。

k. 按一下「OK」（確定）。

l. 按一下「Apply」。

m. 配置應如圖A5所示。

圖A5：LDAP屬性對映配置



Cisco ASDM 6.0 for ASA - 172.18.120.225

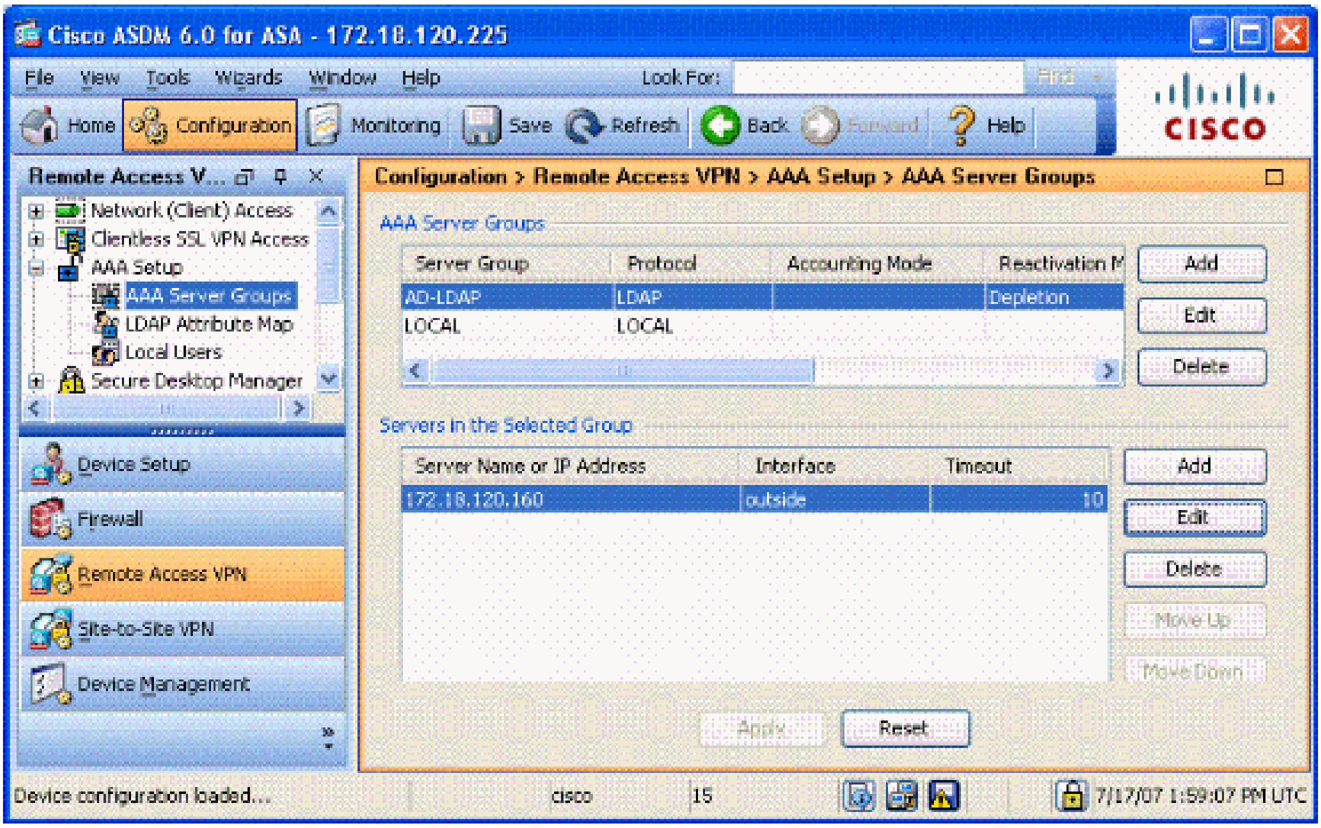
Configuration > Remote Access VPN > AAA Setup > LDAP Attribute Map

Add and configure attribute map used by LDAP server.

Name	Attribute Map Name
msNPAllowDialin	msNPAllowDialin=Tunneling-Protocols

4. 選擇Remote Access VPN> AAA Setup > AAA Server Groups。請參閱圖A6。

圖A6：AAA伺服器組



AAA Server Groups

Server Group	Protocol	Accounting Mode	Reactivation M
AD-LDAP	LDAP		Depletion
LOCAL	LOCAL		

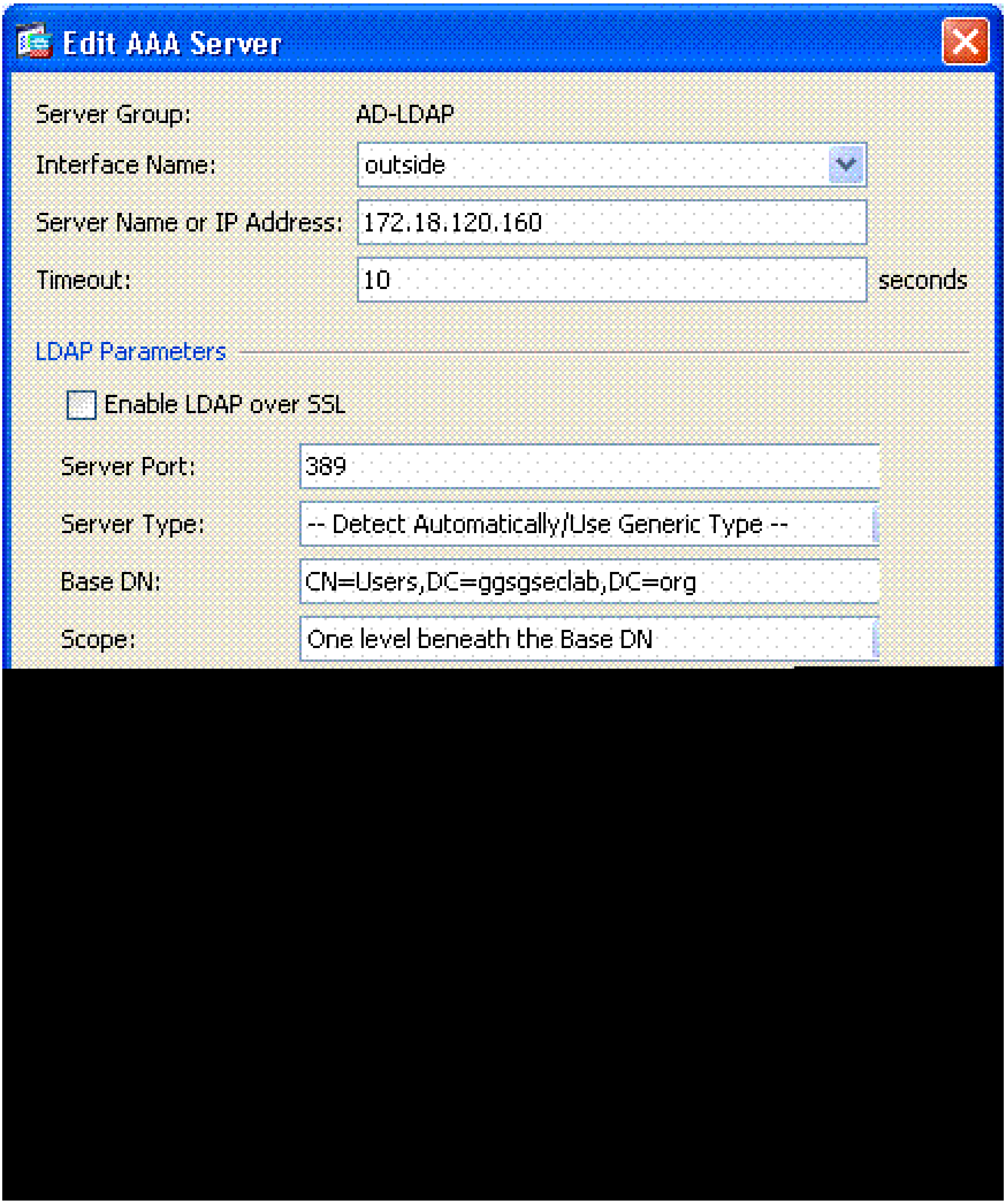
Servers in the Selected Group

Server Name or IP Address	Interface	Timeout
172.18.120.160	outside	10

5. 按一下要編輯的伺服器組。在Selected Group部分的Servers中，選擇伺服器IP地址或主機名，然後按一下Edit。

6. 在Edit AAA Server窗口的LDAP Attribute Map文本框中，選擇下拉選單中建立的LDAP屬性對映。請參閱圖A7

圖A7：增加LDAP屬性對映



Edit AAA Server

Server Group: AD-LDAP

Interface Name: outside

Server Name or IP Address: 172.18.120.160

Timeout: 10 seconds

LDAP Parameters

□ Enable LDAP over SSL

Server Port: 389

Server Type: -- Detect Automatically/Use Generic Type --

Base DN: CN=Users,DC=ggsgseclab,DC=org

Scope: One level beneath the Base DN

[redacted]

7. 按一下「OK」（確定）。

注意：在測試時打開LDAP調試，以驗證LDAP繫結和屬性對映是否正常工作。有關故障排除命令，請參閱附錄C。

方案2：使用組成員身份實施Active Directory以允許/拒絕訪問

本示例使用LDAP屬性memberOf對映到Tunneling Protocol屬性，以便建立組成員資格作為條件。

若要使用此原則，您必須具備以下條件：

- 使用已存在的組或為ASA VPN使用者建立新組作為ALLOW條件的成員。
- 使用已存在的組或為非ASA使用者建立新組作為DENY條件的成員。
- 確保在LDAP檢視器中檢查您擁有該組的正確DN。見附錄D 。如果DN錯誤，則對映無法正常工作。

注意：請注意，在此版本中ASA只能讀取memberOf屬性的第一個字串。確定建立的新群組位於清單頂端。另一個選項是在名稱前加上特殊字元，因為AD會先檢視特殊字元。要解決此警告，請使用8.x軟體中的DAP檢視多個組。

注意：確保使用者是deny組的一部分或至少另一個組的一部分，以便memberOf始終傳送回ASA。您不必指定FALSE拒絕條件，但最佳做法是指定。如果現有群組名稱或群組名稱包含空格，請以下列方式輸入屬性：

```
CN=Backup Operators，CN=Builtin，DC=ggsgseclab，DC=org
```

注意：DAP允許ASA檢視memberOf屬性中的多個組以及組的基本授權。請參閱DAP部分。

對應

- AD屬性值：
  - memberOf CN=ASAUsers，CN=Users，DC=ggsgseclab，DC=org
  - memberOf CN=TelnetClients，CN=Users，DC=labrat，DC=com
- Cisco屬性值：1 = FALSE、20 = TRUE、

對於ALLOW情況，進行以下對映：

- memberOf CN=ASAUsers，CN=Users，DC=ggsgseclab，DC=org= 20

對於DENY情況，進行以下對映：

- memberOf CN=TelnetClients，CN=Users，DC=ggsgseclab，DC=org = 1

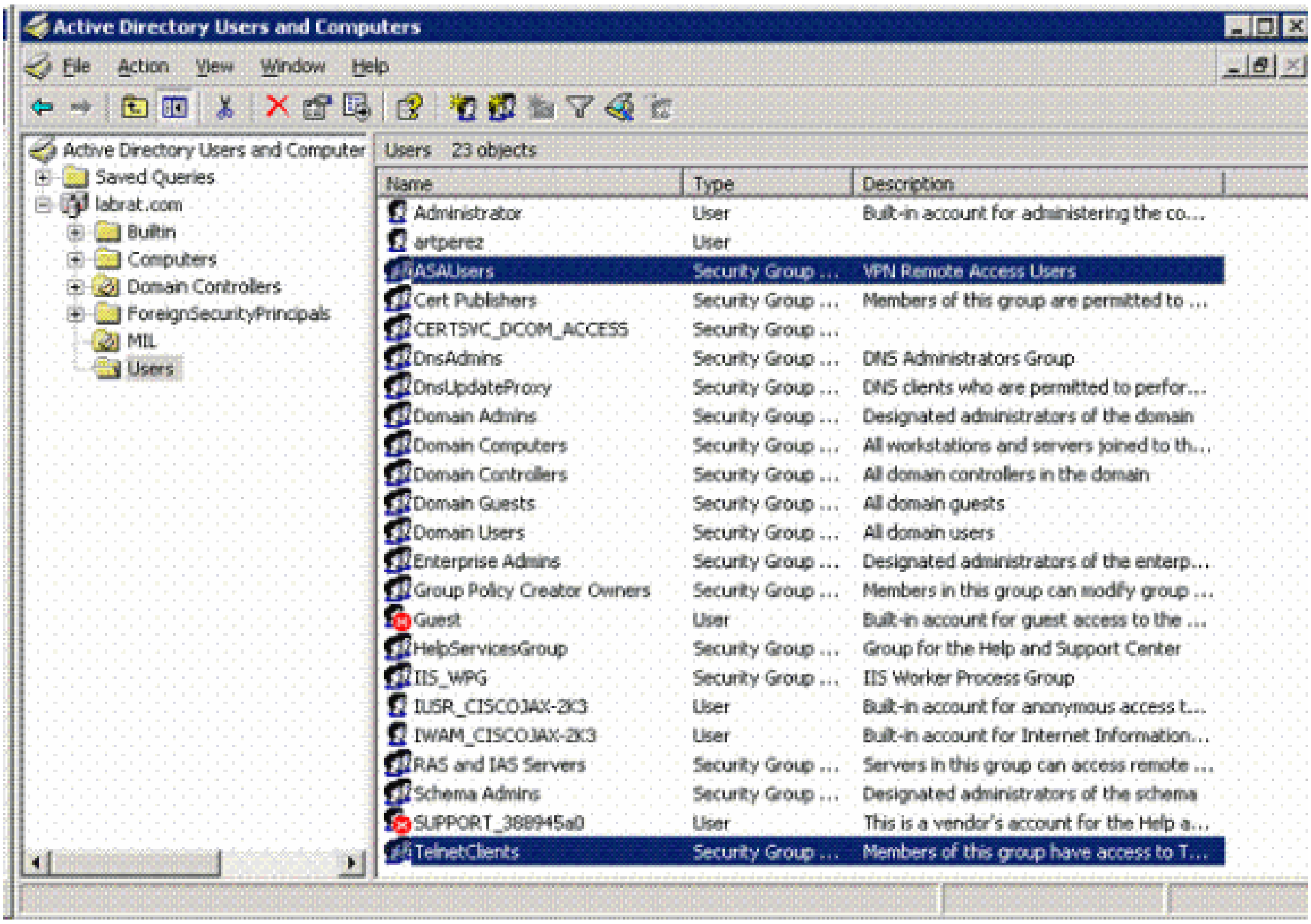
注意：在將來的版本中，有一個思科屬性用於允許和拒絕連線。有關Cisco屬性的詳細資訊，請參閱配置外部伺服器以便進行安全裝置使用者授權。

Active Directory安裝

1. 在Active Directory伺服器中，選擇Start > Run。
2. 在Open文本框中，鍵入dsa.msc，然後按一下Ok。這會啟動Active Directory管理主控台。

3. 在Active Directory管理控制檯中，按一下加號以展開「Active Directory使用者和電腦」。請參閱圖A8

圖A8： Active Directory組


Active Directory Users and Computers
File
Action
View
Window
Help
Active Directory Users and Computer
Saved Queries
labrat.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
MIL
Users

Users 23 objects

Name	Type	Description
Administrator	User	Built-in account for administering the co...
artperez	User	
ASAUsers	Security Group ...	VPN Remote Access Users
Cert Publishers	Security Group ...	Members of this group are permitted to ...
CERTSVC_DCOM_ACCESS	Security Group ...	
DnsAdmins	Security Group ...	DNS Administrators Group
DnsUpdateProxy	Security Group ...	DNS clients who are permitted to perfor...
Domain Admins	Security Group ...	Designated administrators of the domain
Domain Computers	Security Group ...	All workstations and servers joined to th...
Domain Controllers	Security Group ...	All domain controllers in the domain
Domain Guests	Security Group ...	All domain guests
Domain Users	Security Group ...	All domain users
Enterprise Admins	Security Group ...	Designated administrators of the enterp...
Group Policy Creator Owners	Security Group ...	Members in this group can modify group ...
Guest	User	Built-in account for guest access to the ...
HelpServicesGroup	Security Group ...	Group for the Help and Support Center
IIS_WPG	Security Group ...	IIS Worker Process Group
IUSR_CISCOJAX-2K3	User	Built-in account for anonymous access t...
IWAM_CISCOJAX-2K3	User	Built-in account for Internet Information...
RAS and IAS Servers	Security Group ...	Servers in this group can access remote ...
Schema Admins	Security Group ...	Designated administrators of the schema
SUPPORT_388945a0	User	This is a vendor's account for the Help a...
TelnetClients	Security Group ...	Members of this group have access to T...

4. 按一下加號以展開域名。

5. 按一下右鍵Users資料夾並選擇New > Group。

6. 輸入「群組名稱」。例如：ASAUsers。

7. 按一下「OK」（確定）。

8. 按一下Users資料夾，然後按兩下剛建立的組。

9. 選擇Members頁籤，然後按一下Add。

10. 鍵入要增加的使用者的Name，然後按一下Ok。

ASA配置

1. 在ASDM中，選擇Remote Access VPN > AAA Setup > LDAP Attribute Map。

2. 按一下Add。

3. 在Add LDAP Attribute Map窗口中，完成以下步驟。請參閱圖A3。

a. 在「名稱」文字方塊中輸入名稱。

b. 在Map Name頁籤中，在Customer Name文本框c中鍵入memberOf。

c. 在Map Name頁籤中，從Cisco Name的下拉選項中選擇Tunneling-Protocols。

d. 選擇Add。

e. 按一下Map Value頁籤。

f. 選擇Add。

g. 在Add Attribute LDAP Map Value窗口中，在Customer Name文本框中鍵入CN=ASAUsers，CN=Users，DC=ggsgseclab，DC=org，並在Cisco Value文本框中鍵入20。

h. 按一下Add。

i. 在Customer Name文本框中鍵入CN=TelnetClients，CN=Users，DC=ggsgseclab，DC=org，並在Cisco Value文本框中鍵入1。請參閱圖A4。

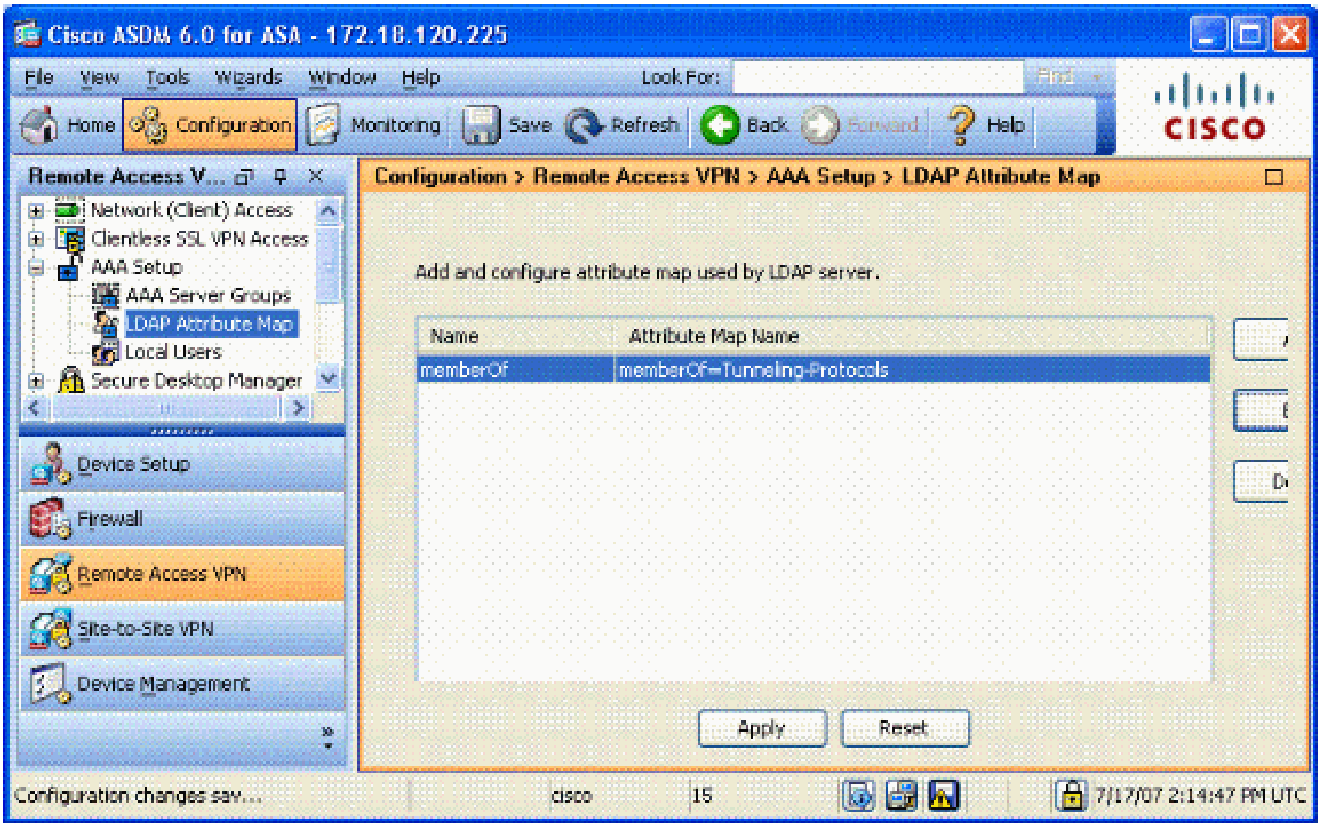
j. 按一下「OK」（確定）。

k. 按一下「OK」（確定）。

l. 按一下「Apply」。

m. 配置應如圖A9所示。

圖A9 LDAP屬性對映



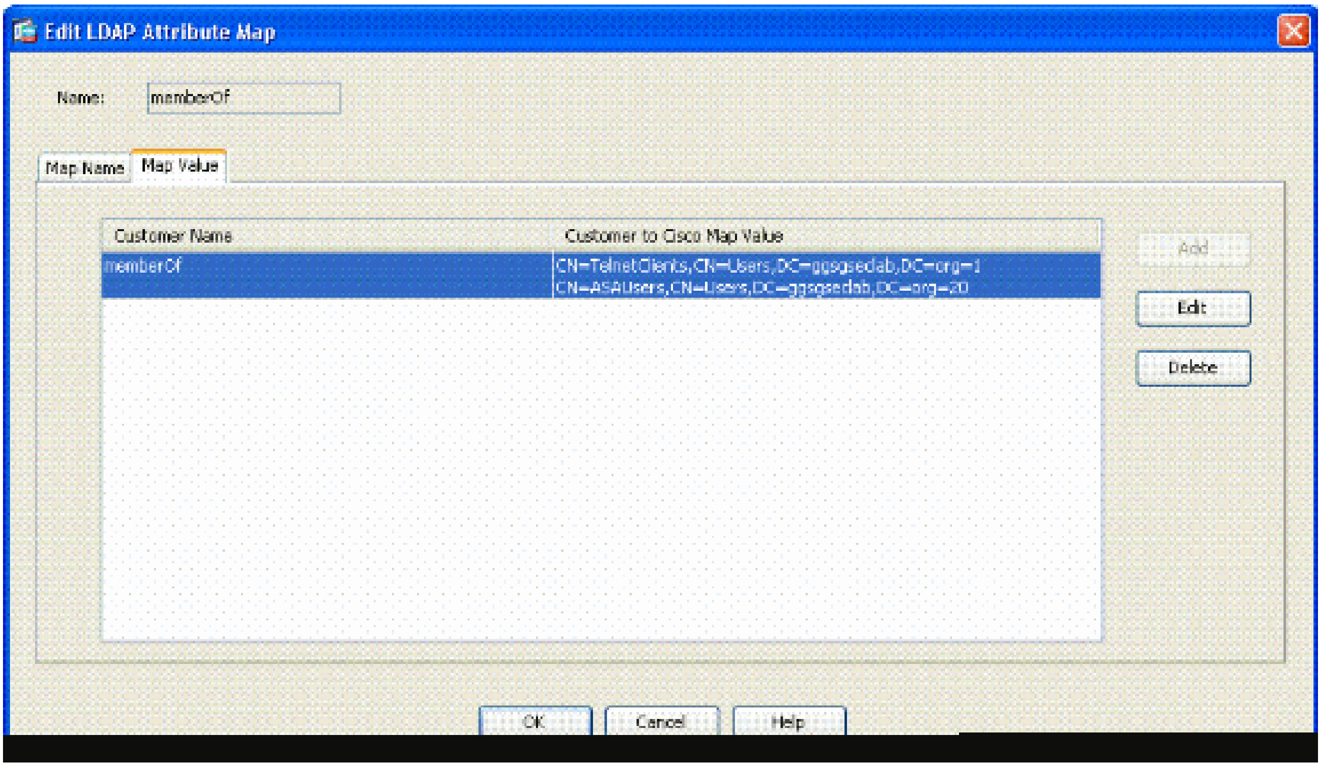
Configuration > Remote Access VPN > AAA Setup > LDAP Attribute Map

Add and configure attribute map used by LDAP server.

Name	Attribute Map Name
memberOf	memberOf=Tunneling-Protocols

4. 選擇Remote Access VPN> AAA Setup > AAA Server Groups。

5. 按一下要編輯的伺服器組。在Selected Group部分的Servers中，選擇伺服器IP地址或主機名，然後按一下Edit。



Name: memberOf

Customer Name	Customer to Cisco Map Value

memberOf	CN=TelnetClients,CN=Users,DC=ggsgsedab,DC=org=1
	CN=ASAUsers,CN=Users,DC=ggsgsedab,DC=org=20

6. 在Edit AAA Server窗口的LDAP Attribute Map文本框中，選擇下拉選單中建立的LDAP屬性對映。

7. 按一下「OK」（確定）。

注意：請在測試時打開LDAP調試，以驗證LDAP繫結和屬性對映是否正常工作。有關故障排除命令，請參閱附錄C。

案例3：多個屬性成員的動態存取原則

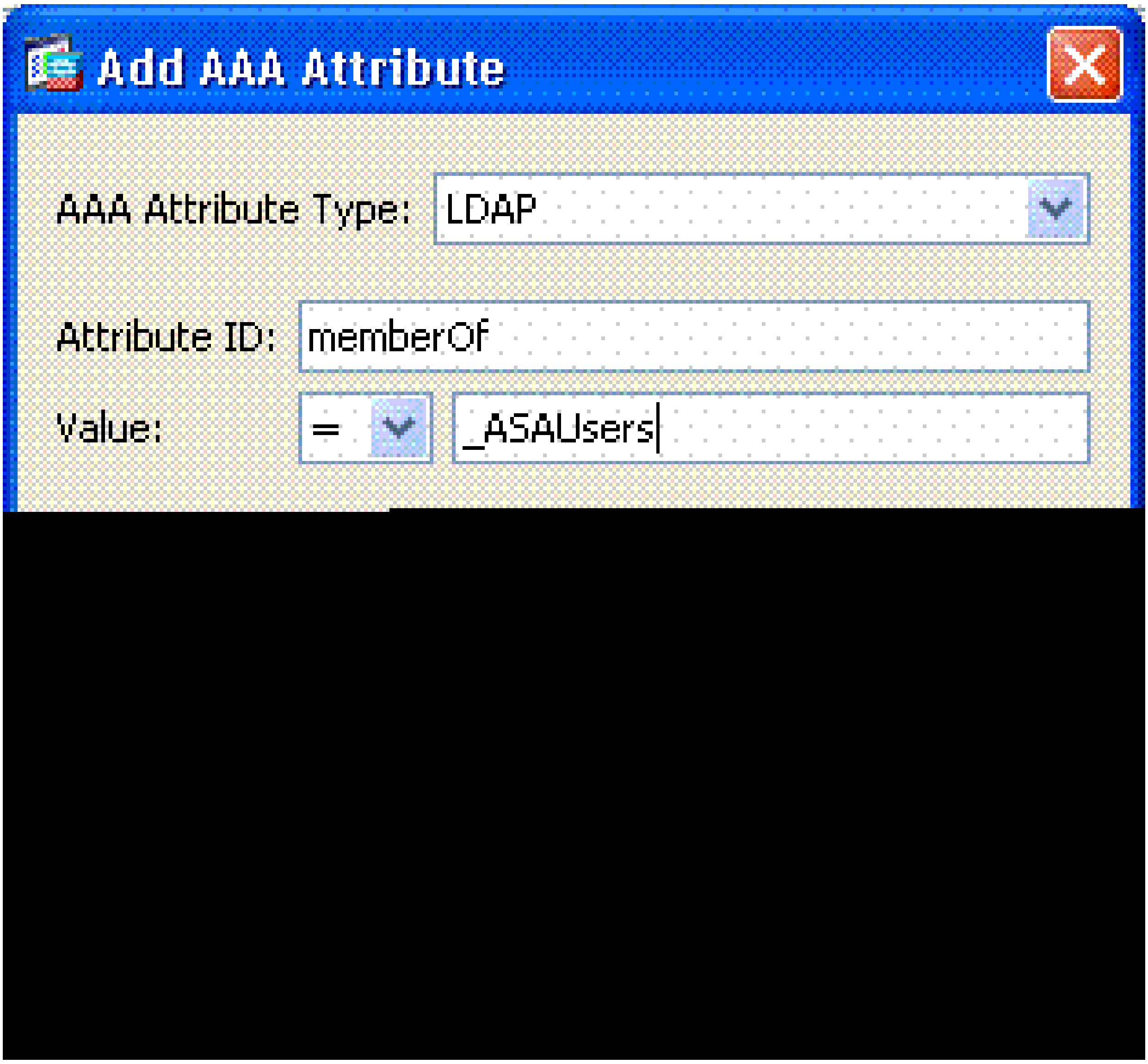
本示例使用DAP檢視多個memberOf屬性，以允許根據Active Directory組成員身份進行訪問。在8.x之前，ASA僅讀取第一個memberOf屬性。使用8.x及更高版本，ASA可以檢視所有memberOf屬性。

- 使用已存在的組或為ASA VPN使用者建立新組（或多個組），使其成為ALLOW條件的成員。
- 使用已存在的組或為非ASA使用者建立新組作為DENY條件的成員。
- 確保在LDAP檢視器中檢查您擁有該組的正確DN。見附錄D 。如果DN錯誤，則對映無法正常工作。

ASA配置

1. 在ASDM中，選擇Remote Access VPN> Network (Client) Access > Dynamic Access Policies。
2. 按一下Add。
3. 在增加動態訪問策略中，完成以下步驟：
   a. 在「名稱」文字方塊b中輸入名稱。
   b. 在Priority部分，輸入1或者大於0的其他數字。
   c. 在Selection Criteria中，按一下Add。
   d. 在Add AAA Attribute中，選擇LDAP。
   e. 在attribute ID部分中，輸入memberOf。
   f. 在value部分中，選擇=並輸入AD組名。針對要參照的每個群組重複此步驟。請參閱圖A10。

   圖A10 AAA屬性對映



AAA Attribute Type: LDAP

Attribute ID: memberOf

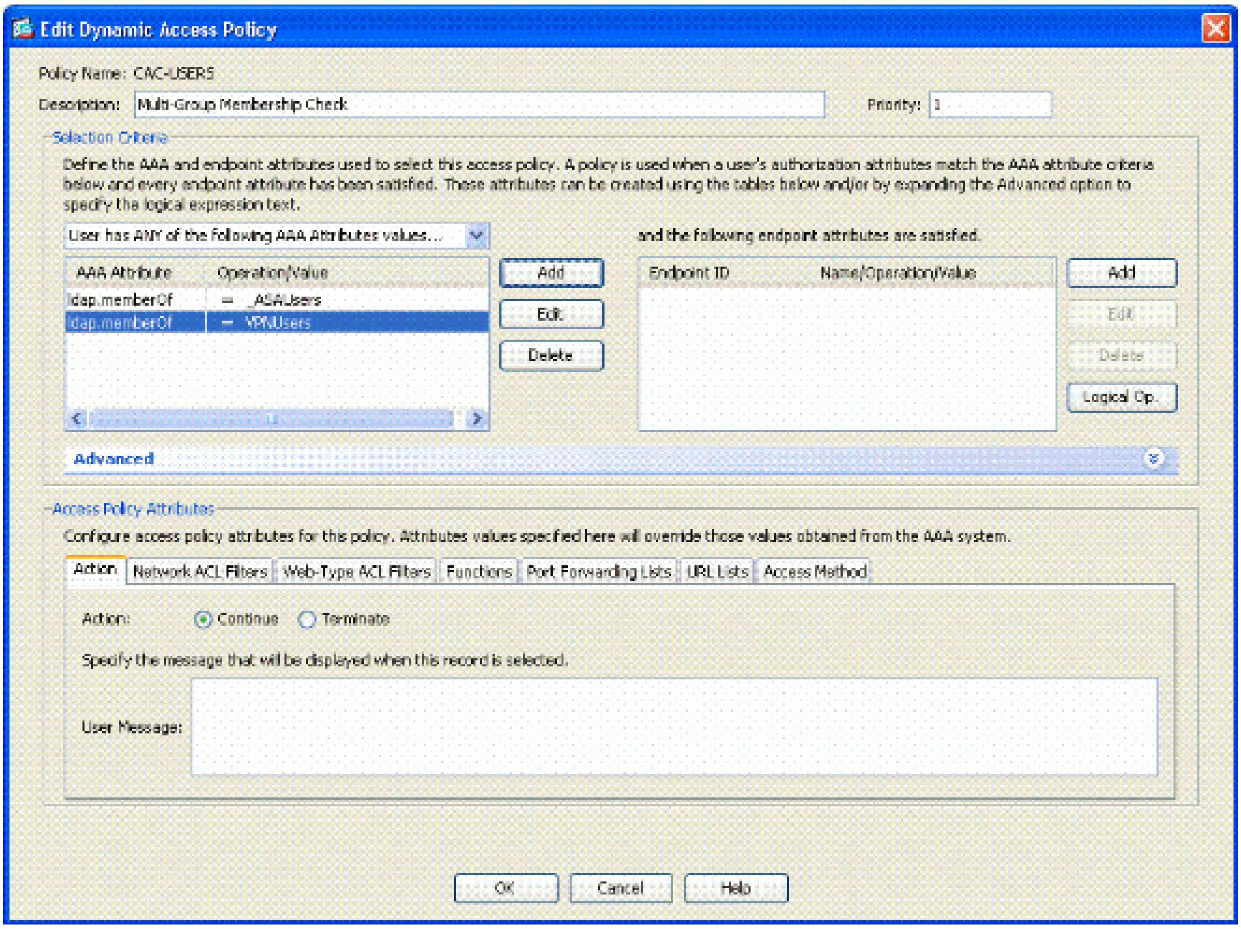
Value: = _ASAUsers

[redacted]

g. 按一下「OK」（確定）。

h. 在Access Policy Attributes部分中，選擇Continue。請參閱圖A11。

圖A11增加動態策略



Policy Name: CAC-USERS

Description: Multi-Group Membership Check

Priority: 1

Selection Criteria

Define the AAA and endpoint attributes used to select this access policy. A policy is used when a user's authorization attributes match the AAA attribute criteria below and every endpoint attribute has been satisfied. These attributes can be created using the tables below and/or by expanding the Advanced option to specify the logical expression text.

User has ANY of the following AAA Attributes values...

AAA Attribute	Operation/Value
ldap.memberOf	= _ASAUsers
ldap.memberOf	= VPNUsers

and the following endpoint attributes are satisfied.

Endpoint ID	Name/Operation/Value

Access Policy Attributes

Configure access policy attributes for this policy. Attributes values specified here will override those values obtained from the AAA system.

Action | Network ACL Filters | Web-Type ACL Filters | Functions | Port Forwarding Lists | URL Lists | Access Method

Action: ● Continue ○ Terminate

Specify the message that will be displayed when this record is selected.

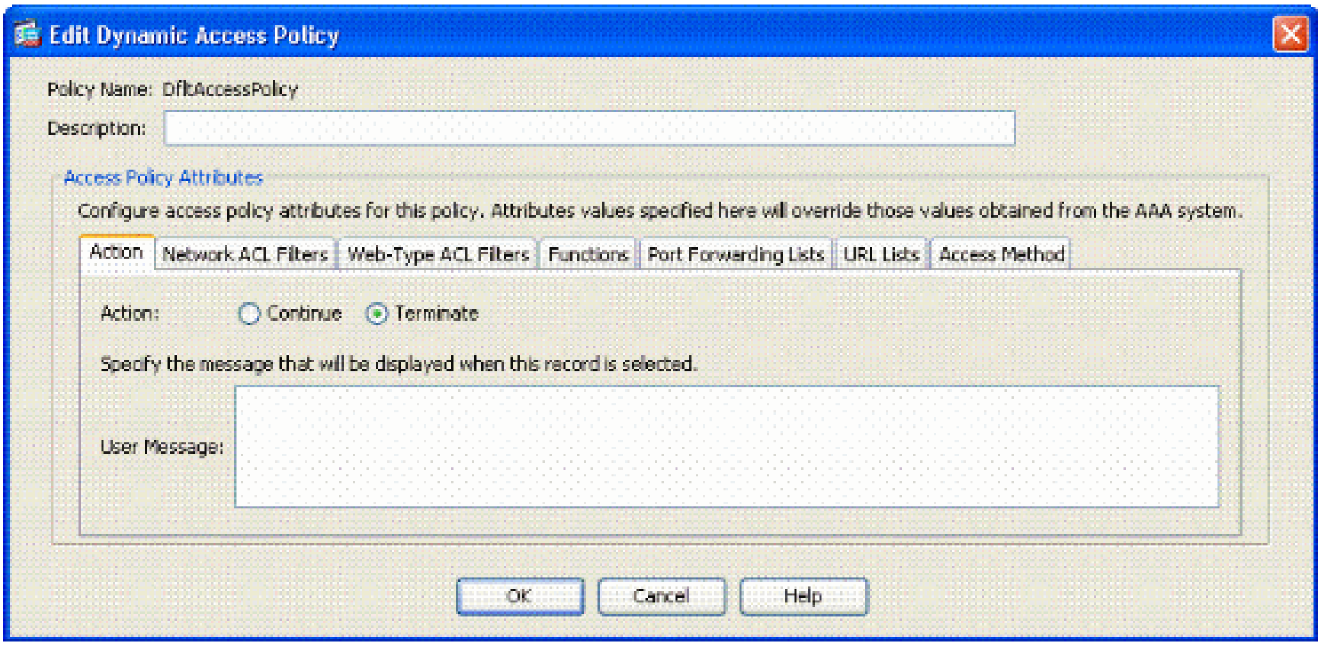
User Message:

4. 在ASDM中，選擇Remote Access VPN> Network (Client) Access > Dynamic Access Policies。

5. 選擇Default Access Policy，並選擇Edit。

6. 預設操作應設定為Terminate。請參閱圖A12。

圖A12編輯動態策略



Policy Name: DfltAccessPolicy

Description:

Access Policy Attributes

Configure access policy attributes for this policy. Attributes values specified here will override those values obtained from the AAA system.

Action | Network ACL Filters | Web-Type ACL Filters | Functions | Port Forwarding Lists | URL Lists | Access Method

Action: ○ Continue ● Terminate

Specify the message that will be displayed when this record is selected.

User Message:

7. 按一下「OK」（確定）。

註：如果未選擇Terminate，您將無法進入任何組，因為預設值為Continue。

附錄B - ASA CLI配置

ASA 5510

<#root>

```
ciscoasa#

show running-config

: Saved
:
ASA Version 8.0(2)
!
hostname asa80
domain-name army.mil
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address x.x.x.x 255.255.255.128
!
interface GigabitEthernet0/1
nameif inside
security-level 100
no ip address
!
boot system disk0:/asa802-k8.bin
ftp mode passive
dns server-group DefaultDNS
domain-name army.mil
!
--------------ACL's-------------------------------------------------
access-list out extended permit ip any any
--------------------------------------------------------------------
pager lines 24
logging console debugging
mtu outside 1500
!
---------------VPN Pool---------------------------------------------
ip local pool CAC-USERS 192.168.1.1-192.168.1.254 mask 255.255.255.0
--------------------------------------------------------------------
!
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-602.bin
no asdm history enable
arp timeout 14400
access-group out in interface outside
route outside 0.0.0.0 0.0.0.0 172.18.120.129 1
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
!
--------------------------LDAP Maps & DAP----------------------------
ldap attribute-map memberOf
map-name memberOf Tunneling-Protocols
```

```
map-value memberOf CN=_ASAUsers,CN=Users,DC=ggsgseclab,DC=org 20
ldap attribute-map msNPAllowDialin
map-name msNPAllowDialin Tunneling-Protocols
map-value msNPAllowDialin FALSE 1
map-value msNPAllowDialin TRUE 20
dynamic-access-policy-record CAC-USERS
description "Multi-Group Membership Check"
priority 1
dynamic-access-policy-record DfltAccessPolicy
action terminate
---------------------------------------------------------------------
!
--------------------LDAP Server--------------------------------------
aaa-server AD-LDAP protocol ldap
aaa-server AD-LDAP (outside) host 172.18.120.160
ldap-base-dn CN=Users,DC=ggsgseclab,DC=org
ldap-scope onelevel
ldap-naming-attribute userPrincipalName
ldap-login-password *
ldap-login-dn CN=Administrator,CN=Users,DC=ggsgseclab,DC=org
---------------------------------------------------------------------
!
aaa authentication http console LOCAL
http server enable 445
http 0.0.0.0 0.0.0.0 outside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
!
----------------CA Trustpoints---------------------------------------
crypto ca trustpoint ASDM_TrustPoint0
revocation-check ocsp
enrollment terminal
keypair DoD-1024
match certificate DefaultCertificateMap override ocsp trustpoint
ASDM_TrustPoint5 10 url http://ocsp.disa.mil
crl configure
crypto ca trustpoint ASDM_TrustPoint1
revocation-check ocsp
enrollment terminal
fqdn asa80
subject-name CN=asa80,OU=PKI,OU=DoD,O=U.S. Government,C=US
keypair DoD-1024
match certificate DefaultCertificateMap override ocsp trustpoint
ASDM_TrustPoint5 10 url http://ocsp.disa.mil
no client-types
crl configure
crypto ca trustpoint ASDM_TrustPoint2
revocation-check ocsp
```

```
enrollment terminal
keypair DoD-2048
match certificate DefaultCertificateMap override ocsp trustpoint
ASDM_TrustPoint5 10 url http://ocsp.disa.mil
no client-types
crl configure
crypto ca trustpoint ASDM_TrustPoint3
revocation-check ocsp none
enrollment terminal
crl configure
!
-------------------Certificate Map-------------------------------
crypto ca certificate map DefaultCertificateMap 10
subject-name ne ""
--------------------CA Certificates (Partial Cert is Shown)------------
crypto ca certificate chain ASDM_TrustPoint0
certificate ca 37
3082044c 30820334 a0030201 02020137 300d0609 2a864886 f70d0101
05050030
60310b30 09060355 04061302 55533118 30160603 55040a13 0f552e53
2e20476f
7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c 300a0603
55040b13
03504b49 311b3019 06035504 03131244 6f44204a 49544320 526f6f74
crypto ca certificate chain ASDM_TrustPoint1
certificate 319e
30820411 3082037a a0030201 02020231 9e300d06 092a8648 86f70d01
01050500
305c310b 30090603 55040613 02555331 18301606 0355040a 130f552e
532e2047
6f766572 6e6d656e 74310c30 0a060355 040b1303 446f4431 0c300a06
0355040b
crypto ca certificate chain ASDM_TrustPoint2
certificate ca 37
3082044c 30820334 a0030201 02020137 300d0609 2a864886 f70d0101
05050030
60310b30 09060355 04061302 55533118 30160603 55040a13 0f552e53
2e20476f
7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c 300a0603
55040b13
f766e045 f15ddb43 9549d1e9 a0ea6814 b64bcece 089e1b6e 1be959a5
6fc20a76
crypto ca certificate chain ASDM_TrustPoint3
certificate ca 05
30820370 30820258 a0030201 02020105 300d0609 2a864886 f70d0101
05050030
5b310b30 09060355 04061302 55533118 30160603 55040a13 0f552e53
2e20476f
7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c 300a0603
55040b13
03504b49 31163014 06035504 03130d44 6f442052 6f6f7420 43412032
301e170d
30343132 31333135 30303130 5a170d32 39313230 35313530 3031305a
305b310b
30090603 55040613 02555331 18301606 0355040a 130f552e 532e2047
6f766572
6e6d656e 74310c30 0a060355 040b1303 446f4431 0c300a06 0355040b
1303504b
49311630 14060355 0403130d 446f4420 526f6f74 20434120 32308201
crypto ca certificate chain ASDM_TrustPoint4
certificate ca 04
30820267 308201d0 a0030201 02020104 300d0609 2a864886 f70d0101
```

```
05050030
61310b30 09060355 04061302 55533118 30160603 55040a13 0f552e53
2e20476f
7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c 300a0603
55040b13
03504b49 311c301a 06035504 03131344 6f442043 4c415353 20332052
6f6f7420
!
!
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
!
-------------------------SSL/WEBvpn-windows------------------------------------
ssl certificate-authentication interface outside port 443
webvpn
enable outside
svc image disk0:/anyconnect-win-2.0.0343-k9.pkg 1
svc enable
tunnel-group-list enable
--------------------------------------------------------------------
----------------------VPN Group/Tunnel Policy--------------------
group-policy CAC-USERS internal
ggroup-policy AC-USERS internal
group-policy AC-USERS attributes
vpn-windows-tunnel-protocol svc
address-pools value CAC-USERS
webvpn
svc ask none default svc
tunnel-group AC-USERS type remote-access
tunnel-group AC-USERS general-attributes
authorization-server-group AD-LDAP
default-group-policy AC-USERS
authorization-required
authorization-dn-attributes UPN
tunnel-group AC-USERS webvpn-windows-attributes
authentication certificate
group-alias AC-USERS enable
tunnel-group-map enable rules
no tunnel-group-map enable ou
no tunnel-group-map enable ike-id
no tunnel-group-map enable peer-ip
--------------------------------------------------------------------
prompt hostname context
```

附錄C-故障排除

AAA和LDAP故障排除

- debug ldap 255 —顯示LDAP交換
- debug aaa common 10 —顯示AAA交換

範例1：允許具有正確屬性對應的連線

本示例顯示在與附錄A中場景2的成功連線期間debug ldap和debug aaa common的輸出。

圖C1：debug LDAP和debug aaa common output -正確對映

```
AAA API: In aaa_open
AAA session opened: handle = 39
AAA API: In aaa_process_async
aaa_process_async: sending AAA_MSG_PROCESS
AAA task: aaa_process_msg(1a87a64) received message type 0
AAA FSM: In AAA_StartAAATransaction
AAA FSM: In AAA_InitTransaction
Initiating authorization query (Svr Grp: AD-LDAP)
------------------------------------------------
AAA FSM: In AAA_BindServer
AAA_BindServer: Using server: 172.18.120.160
AAA FSM: In AAA_SendMsg
User: 1234567890@mil
Pasw: 1234567890@mil
Resp:
[78] Session Start
[78] New request Session, context 0x26f1c44, reqType = 0
[78] Fiber started
[78] Creating LDAP context with uri=ldap:// 172.18.120.160:389
[78] Binding as administrator
[78] Performing Simple authentication for Administrator to
172.18.120.160
[78] Connect to LDAP server: ldap:// 172.18.120.160, status =
Successful
[78] LDAP Search:
Base DN = [CN=Users,DC=ggsgseclab,DC=org]
Filter = [userPrincipalName=1234567890@mil]
Scope = [SUBTREE]
[78] Retrieved Attributes:
[78] objectClass: value = top
[78] objectClass: value = person
[78] objectClass: value = organizationalPerson
[78] objectClass: value = user
[78] cn: value = Ethan Hunt
```

```
[78] sn: value = Hunt
[78] userCertificate: value =
0..50........./.......60...*.H.......0@1.0.....&...,d....com1.0.....
&...,d...
[78] userCertificate: value =
0..'0........./..t....50...*.H.......0@1.0.....&...,d....com1.0.....
&...,d...
[78] givenName: value = Ethan
[78] distinguishedName: value = CN=Ethan
Hunt,OU=MIL,DC=labrat,DC=com
[78] instanceType: value = 4
[78] whenCreated: value = 20060613151033.0Z
[78] whenChanged: value = 20060622185924.0Z
[78] displayName: value = Ethan Hunt
[78] uSNCreated: value = 14050
[78] memberOf: value = CN=ASAUsers,CN=Users,DC=ggsgseclab,DC=org
[78] mapped to cVPN3000-Tunneling-Protocols: value = 20
[78] uSNChanged: value = 14855
[78] name: value = Ethan Hunt
[78] objectGUID: value = ..9...NJ..GU..z.
[78] userAccountControl: value = 66048
[78] badPwdCount: value = 0
[78] codePage: value = 0
[78] countryCode: value = 0
[78] badPasswordTime: value = 127954717631875000
[78] lastLogoff: value = 0
[78] lastLogon: value = 127954849209218750
[78] pwdLastSet: value = 127946850340781250
[78] primaryGroupID: value = 513
[78] objectSid: value = ................q......mY...
[78] accountExpires: value = 9223372036854775807
[78] logonCount: value = 25
[78] sAMAccountName: value = 1234567890
[78] sAMAccountType: value = 805306368
[78] userPrincipalName: value = 1234567890@mil
[78] objectCategory: value =
[78] mail: value = Ethan.Hunt@labrat.com
callback_aaa_task: status = 1, msg =
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 39, pAcb = 2ae115c
[78] Fiber exit Tx=147 bytes Rx=4821 bytes, status=1
[78] Session End
AAA task: aaa_process_msg(1a87a64) received message type 1
AAA FSM: In AAA_ProcSvrResp
Back End response:
------------------
Authorization Status: 1 (ACCEPT)
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_AUTHORIZE, auth_status = ACCEPT
AAA_NextFunction: authen svr = <none>, author svr = AD-LDAP, user pol =
, tunn pol = CAC-USERS
AAA_NextFunction: New i_fsm_state = IFSM_TUNN_GRP_POLICY,
AAA FSM: In AAA_InitTransaction
aaai_policy_name_to_server_id(CAC-USERS)
Got server ID 0 for group policy DB
Initiating tunnel group policy lookup (Svr Grp: GROUP_POLICY_DB)
------------------------------------------------
AAA FSM: In AAA_BindServer
AAA_BindServer: Using server: <Internal Server>
AAA FSM: In AAA_SendMsg
User: CAC-USER
Pasw:
```

```
Resp:
grp_policy_ioctl(12f1b20, 114698, 1a870b4)
grp_policy_ioctl: Looking up CAC-USERS
callback_aaa_task: status = 1, msg =
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 39, pAcb = 2ae115c
AAA task: aaa_process_msg(1a87a64) received message type 1
AAA FSM: In AAA_ProcSvrResp
Back End response:
------------------
Tunnel Group Policy Status: 1 (ACCEPT)
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_TUNN_GRP_POLICY, auth_status =
ACCEPT
AAA_NextFunction: authen svr = <none>, author svr = AD-LDAP, user pol =
, tunn pol = CAC-USERS
AAA_NextFunction: New i_fsm_state = IFSM_DONE,
AAA FSM: In AAA_ProcessFinal
Checking time simultaneous login restriction for user 1234567890@mil
AAA FSM: In AAA_Callback
user attributes:
1 Tunnelling-Protocol(4107) 20 20
user policy attributes:
None
tunnel policy attributes:
1 Primary-DNS(4101) 4 IP: 10.0.10.100
2 Secondary-DNS(4102) 4 IP: 0.0.0.0
3 Tunnelling-Protocol(4107) 4 4
4 Default-Domain-Name(4124) 10 "ggsgseclab.org"
5 List of address pools to assign addresses from(4313) 10
"CAC-USERS"
Auth Status = ACCEPT
AAA API: In aaa_close
AAA task: aaa_process_msg(1a87a64) received message type 3
In aaai_close_session (39)
AAA API: In aaa_send_acct_start
AAA API: In aaa_send_acct_stop
CAC-Test#
```

示例2：允許使用配置錯誤的Cisco屬性對映的連線

本示例顯示在與附錄A中場景2的允許連線期間debug ldap和debug aaa common的輸出。

圖C2：debug LDAP和debug aaa common output -不正確的對映

```
AAA API: In aaa_open
AAA session opened: handle = 41
AAA API: In aaa_process_async
aaa_process_async: sending AAA_MSG_PROCESS
AAA task: aaa_process_msg(1a87a64) received message type 0
AAA FSM: In AAA_StartAAATransaction
AAA FSM: In AAA_InitTransaction
Initiating authorization query (Svr Grp: AD-LDAP)
------------------------------------------------
AAA FSM: In AAA_BindServer
AAA_BindServer: Using server: 172.18.120.160
```

```
AAA FSM: In AAA_SendMsg
User: 1234567890@mil
Pasw: 1234567890@mil
Resp:
[82] Session Start
[82] New request Session, context 0x26f1c44, reqType = 0
[82] Fiber started
[82] Creating LDAP context with uri=ldap://172.18.120.160:389
[82] Binding as administrator
[82] Performing Simple authentication for Administrator to
172.18.120.160
[82] Connect to LDAP server: ldap:// 172.18.120.160:389, status =
Successful
[82] LDAP Search:
Base DN = [CN=Users,DC=ggsgseclab,DC=org]
Filter = [userPrincipalName=1234567890@mil]
Scope = [SUBTREE]
[82] Retrieved Attributes:
[82] objectClass: value = top
[82] objectClass: value = person
[82] objectClass: value = organizationalPerson
[82] objectClass: value = user
[82] cn: value = Ethan Hunt
[82] sn: value = Hunt
[82] userCertificate: value =
0..50........../........60...*.H........0@1.0.....&...,d....com1.0.....
&...,d...
[82] userCertificate: value =
0..'0........../..t.....50...*.H........0@1.0.....&...,d....com1.0.....
&...,d...
[82] givenName: value = Ethan
[82] distinguishedName: value = CN=Ethan
Hunt,OU=MIL,DC=labrat,DC=com
[82] instanceType: value = 4
[82] whenCreated: value = 20060613151033.0Z
[82] whenChanged: value = 20060622185924.0Z
[82] displayName: value = Ethan Hunt
[82] uSNCreated: value = 14050
[82] memberOf: value = CN=ASAUsers,CN=Users,DC=ggsgseclab,DC=org
[82] mapped to cVPN3000-Tunneling-Protocols: value =
CN=ASAUsers,CN=Users,DC=ggsgseclab,DC=org
[82] uSNChanged: value = 14855
[82] name: value = Ethan Hunt
[82] objectGUID: value = ..9...NJ..GU..z.
[82] userAccountControl: value = 66048
[82] badPwdCount: value = 0
[82] codePage: value = 0
[82] countryCode: value = 0
[82] badPasswordTime: value = 127954717631875000
[82] lastLogoff: value = 0
[82] lastLogon: value = 127954849209218750
[82] pwdLastSet: value = 127946850340781250
[82] primaryGroupID: value = 513
[82] objectSid: value = ................q......mY...
[82] accountExpires: value = 9223372036854775807
[82] logonCount: value = 25
[82] sAMAccountName: value = 1234567890
[82] sAMAccountType: value = 805306368
[82] userPrincipalName: value = 1234567890@mil
[82] objectCategory: value =
CN=Person,CN=Schema,CN=Configuration,DC=ggsgseclab,DC=org
[82] mail: value = Ethan.Hunt@labrat.com
```

```
callback_aaa_task: status = 1, msg =
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 41, pAcb = 2ae115c
[82] Fiber exit Tx=147 bytes Rx=4821 bytes, status=1
[82] Session End
AAA task: aaa_process_msg(1a87a64) received message type 1
AAA FSM: In AAA_ProcSvrResp
Back End response:
------------------
Authorization Status: 1 (ACCEPT)
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_AUTHORIZE, auth_status = ACCEPT
AAA_NextFunction: authen svr = <none>, author svr = AD-LDAP, user pol =
, tunn pol = CAC-USERS
AAA_NextFunction: New i_fsm_state = IFSM_TUNN_GRP_POLICY,
AAA FSM: In AAA_InitTransaction
aaai_policy_name_to_server_id(USAFE)
Got server ID 0 for group policy DB
Initiating tunnel group policy lookup (Svr Grp: GROUP_POLICY_DB)
------------------------------------------------
AAA FSM: In AAA_BindServer
AAA_BindServer: Using server: <Internal Server>
AAA FSM: In AAA_SendMsg
User: CAC-USERS
Pasw:
Resp:
grp_policy_ioctl(12f1b20, 114698, 1a870b4)
grp_policy_ioctl: Looking up CAC-USERS
callback_aaa_task: status = 1, msg =
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 41, pAcb = 2ae115c
AAA task: aaa_process_msg(1a87a64) received message type 1
AAA FSM: In AAA_ProcSvrResp
Back End response:
------------------
Tunnel Group Policy Status: 1 (ACCEPT)
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_TUNN_GRP_POLICY, auth_status =
ACCEPT
AAA_NextFunction: authen svr = <none>, author svr = AD-LDAP, user pol =
, tunn pol = CAC-USERS
AAA_NextFunction: New i_fsm_state = IFSM_DONE,
AAA FSM: In AAA_ProcessFinal
Checking time simultaneous login restriction for user 1234567890@mil
AAA FSM: In AAA_Callback
user attributes:
1 Tunnelling-Protocol(4107) 20 0
user policy attributes:
None
tunnel policy attributes:
1 Primary-DNS(4101) 4 IP: 10.0.10.100
2 Secondary-DNS(4102) 4 IP: 0.0.0.0
3 Tunnelling-Protocol(4107) 4 4
4 Default-Domain-Name(4124) 10 "ggsgseclab.org"
5 List of address pools to assign addresses from(4313) 10
"CAC-USERS"
Auth Status = ACCEPT
AAA API: In aaa_close
AAA task: aaa_process_msg(1a87a64) received message type 3
In aaai_close_session (41)
AAA API: In aaa_send_acct_start
AAA API: In aaa_send_acct_stop
```

DAP故障排除

- debug dap errors —顯示DAP錯誤
- debug dap trace -顯示DAP功能跟蹤

示例1：允許與DAP的連線

本示例顯示在與附錄A中所示場景3的成功連線期間debug dap errors和debug dap trace的輸出。請注意multiple memberOf attributes。您可以同時屬於_ASAUsers和VPNUsers或屬於任一組，這取決於ASA配置。

圖C3：調試DAP

```
<#root>

#

debug dap errors

debug dap errors enabled at level 1
#

debug dap trace

debug dap trace enabled at level 1
#
The DAP policy contains the following attributes for user:
1241879298@mil
-----------------------------------------------------------------------
---
1: action = continue
DAP_TRACE: DAP_open: C8EEFA10
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.1 = top
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.2 = person
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.3 =
organizationalPerson
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.4 = user
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.cn = 1241879298
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.physicalDeliveryOfficeName = NETADMIN
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.givenName = 1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.distinguishedName =
CN=1241879298,CN=Users,DC=ggsgseclab,DC=org
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.instanceType = 4
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.whenCreated =
20070626163734.0Z
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.whenChanged =
20070718151143.0Z
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.displayName = 1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.uSNCreated = 33691
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.memberOf.1 = VPNUsers
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.memberOf.2 = _ASAUsers
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.uSNChanged = 53274
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.department = NETADMIN
```

```
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.name = 1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectGUID =
....+..F.."5....
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.userAccountControl =
328192
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.badPwdCount = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.codePage = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.countryCode = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.badPasswordTime = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.lastLogoff = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.lastLogon = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.pwdLastSet =
128273494546718750
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.primaryGroupID = 513
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.userParameters = m:
d.
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectSid = ..
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.accountExpires =
9223372036854775807
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.logonCount = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.sAMAccountName =
1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.sAMAccountType =
805306368
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.userPrincipalName =
1241879298@mil
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectCategory =
CN=Person,CN=Schema,CN=Configuration,DC=ggsgseclab,DC=org
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.msNPAllowDialin = TRUE
DAP_TRACE: Username: 1241879298@mil, aaa.cisco.username =
1241879298@mil
DAP_TRACE: Username: 1241879298@mil, aaa.cisco.tunnelgroup = CAC-USERS
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["1"] = "top";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["2"] =
"person";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["3"] =
"organizationalPerson";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["4"] =
"user";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["cn"] = "1241879298";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["physicalDeliveryOfficeName"] =
"NETADMIN";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["givenName"] = "1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["distinguishedName"] =
"CN=1241879298,CN=Users,DC=ggsgseclab,DC=org";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["instanceType"] = "4";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["whenCreated"] =
"20070626163734.0Z";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["whenChanged"] =
"20070718151143.0Z";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["displayName"] =
"1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["uSNCreated"] = "33691";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["memberOf"]["1"] =
"VPNUsers";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["memberOf"]["2"] =
"_ASAUsers";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["uSNChanged"] = "53274";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["department"] = "NETADMIN";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["name"] = "1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectGUID"] contains
```

```
binary data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["userAccountControl"] =
"328192";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["badPwdCount"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["codePage"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["countryCode"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["badPasswordTime"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogoff"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogon"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["pwdLastSet"] =
"128273494546718750";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["primaryGroupID"] = "513";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["userParameters"] contains
binary data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectSid"] contains binary
data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["accountExpires"] =
"9223372036854775807";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["logonCount"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["sAMAccountName"] =
"1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["sAMAccountType"] =
"805306368";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["userPrincipalName"] =
"1241879298@mil";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectCategory"] =
"CN=Person,CN=Schema,CN=Configuration,DC=ggsgseclab,DC=org";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["msNPAllowDialin"] = "TRUE";
DAP_TRACE: dap_add_to_lua_tree:aaa["cisco"]["username"] =
"1241879298@mil";
DAP_TRACE: dap_add_to_lua_tree:aaa["cisco"]["tunnelgroup"] = "CACUSERS";
DAP_TRACE: dap_add_to_lua_tree:endpoint["application"]["clienttype"] =
"IPSec";
DAP_TRACE: Username: 1241879298@mil, Selected DAPs: CAC-USERS
DAP_TRACE: dap_request: memory usage = 33%
DAP_TRACE: dap_process_selected_daps: selected 1 records
DAP_TRACE: Username: 1241879298@mil, dap_aggregate_attr: rec_count = 1
DAP_TRACE: Username: 1241879298@mil, DAP_close: C8EEFA10
d.
```

示例2：與DAP的連線被拒絕

本示例顯示在與附錄A中所示場景3的未成功連線期間debug dap errors和debug dap trace的輸出。

圖C4：調試DAP

```
<#root>

#

debug dap errors

debug dap errors enabled at level 1
#

debug dap trace

debug dap trace enabled at level 1
```

```
#
The DAP policy contains the following attributes for user:
1241879298@mil
-----------------------------------------------------------------------
---
1: action = terminate
DAP_TRACE: DAP_open: C91154E8
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.1 = top
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.2 = person
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.3 =
organizationalPerson
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.4 = user
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.cn = 1241879298
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.physicalDeliveryOfficeName = NETADMIN
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.givenName = 1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.distinguishedName =
CN=1241879298,CN=Users,DC=ggsgseclab,DC=org
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.instanceType = 4
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.whenCreated =
20070626163734.0Z
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.whenChanged =
20070718151143.0Z
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.displayName = 1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.uSNCreated = 33691
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.memberOf = DnsAdmins
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.uSNChanged = 53274
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.department = NETADMIN
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.name = 1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectGUID =
....+..F.."5....
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.userAccountControl =
328192
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.badPwdCount = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.codePage = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.countryCode = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.badPasswordTime = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.lastLogoff = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.lastLogon = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.pwdLastSet =
128273494546718750
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.primaryGroupID = 513
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.userParameters = m:
d.
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectSid = ..
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.accountExpires =
9223372036854775807
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.logonCount = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.sAMAccountName =
1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.sAMAccountType =
805306368
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.userPrincipalName =
1241879298@mil
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectCategory =
CN=Person,CN=Schema,CN=Configuration,DC=ggsgseclab,DC=org
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.msNPAllowDialin = TRUE
DAP_TRACE: Username: 1241879298@mil, aaa.cisco.username =
1241879298@mil
DAP_TRACE: Username: 1241879298@mil, aaa.cisco.tunnelgroup = CAC-USERS
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["1"] = "top";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["2"] =
"person";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["3"] =
"organizationalPerson";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["4"] =
"user";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["cn"] = "1241879298";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["physicalDeliveryOfficeName"] =
"NETADMIN";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["givenName"] = "1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["distinguishedName"] =
"CN=1241879298,CN=Users,DC=ggsgseclab,DC=org";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["instanceType"] = "4";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["whenCreated"] =
"20070626163734.0Z";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["whenChanged"] =
"20070718151143.0Z";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["displayName"] =
"1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["uSNCreated"] = "33691";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["memberOf"] = "DnsAdmins";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["uSNChanged"] = "53274";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["department"] = "NETADMIN";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["name"] = "1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectGUID"] contains
binary data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["userAccountControl"] =
"328192";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["badPwdCount"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["codePage"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["countryCode"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["badPasswordTime"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogoff"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogon"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["pwdLastSet"] =
"128273494546718750";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["primaryGroupID"] = "513";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["userParameters"] contains
binary data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectSid"] contains binary
data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["accountExpires"] =
"9223372036854775807";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["logonCount"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["sAMAccountName"] =
"1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["sAMAccountType"] =
"805306368";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["userPrincipalName"] =
"1241879298@mil";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectCategory"] =
"CN=Person,CN=Schema,CN=Configuration,DC=ggsgseclab,DC=org";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["msNPAllowDialin"] = "TRUE";
DAP_TRACE: dap_add_to_lua_tree:aaa["cisco"]["username"] =
"1241879298@mil";
DAP_TRACE: Username: 1241879298@mil, Selected DAPs:
DAP_TRACE: dap_request: memory usage = 33%
DAP_TRACE: dap_process_selected_daps: selected 0 records
DAP_TRACE: Username: 1241879298@mil, dap_aggregate_attr: rec_count = 1
```

憑證授權單位/OCSP疑難排解

- debug crypto ca 3
- 在配置模式下— logging class ca console(or buffer) debugging

以下示例顯示了使用OCSP響應方和失敗的證書組匹配策略的證書驗證成功。

圖C3顯示了具有已驗證證書和工作證書組匹配策略的調試輸出。

圖C4顯示了配置錯誤的證書組匹配策略的調試輸出。

圖C5顯示了證書已撤銷的使用者的調試輸出。

圖C5： OCSP調試-證書驗證成功

```
CRYPTO_PKI: Found a suitable authenticated trustpoint
ASDM_TrustPoint11.
CRYPTO_PKI: Allocated OCSP data handle 0xca2d27b8
CRYPTO_PKI: Certificate validation: Successful, status: 0. Attempting
to retrieve revocation status if necessary
CRYPTO_PKI: status = 0: poll revocation status
CRYPTO_PKI: Attempting to find OCSP override for peer cert: serial
number: 0F192B, subject name:
cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, issuer_name: cn=DOD JITC EMAIL CA-
15,ou=PKI,ou=DoD,o=U.S. Government,c=US.
CRYPTO_PKI: Processing map rules for SSL.
CRYPTO_PKI: Processing map SSL sequence 20...
CRYPTO_PKI: Match of subject-name field to map PASSED. Peer cert field:
= cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, map rule: subject-name ne "".
CRYPTO_PKI: Peer cert has been authorized by map: SSL sequence: 20.
CRYPTO_PKI: Found OCSP override match. Override URL:
http://198.154.68.90, Override trustpoint: ASDM_TrustPoint12
CRYPTO_PKI: crypto_pki_get_cert_record_by_subject()
CRYPTO_PKI: Destroying OCSP data handle 0xca2d27b8
Crypto CA thread sleeps!
CRYPTO_PKI: Attempting to find tunnel group for cert with serial
number: 0F192B, subject name:
cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, issuer_name: cn=DOD JITC EMAIL CA-
15,ou=PKI,ou=DoD,o=U.S. Government,c=US.
CRYPTO_PKI: Processing map rules for DefaultCertificateMap.
CRYPTO_PKI: Processing map DefaultCertificateMap sequence 10...
CRYPTO_PKI: Match of subject-name field to map PASSED. Peer cert field:
= cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, map rule: subject-name ne "".
CRYPTO_PKI: Peer cert has been authorized by map: DefaultCertificateMap
sequence: 10.
CRYPTO_PKI: Ignoring match on map DefaultCertificateMap, index 10 for
WebVPN group map processing. No tunnel group is configured.
CRYPTO_PKI: Peer cert could not be authorized with map:
DefaultCertificateMap.
CRYPTO_PKI: Processing map rules for SSL.
CRYPTO_PKI: Processing map SSL sequence 20...
```

```
CRYPTO_PKI: Match of subject-name field to map PASSED. Peer cert field:
= cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, map rule: subject-name ne "".
CRYPTO_PKI: Peer cert has been authorized by map: SSL sequence: 20.
CRYPTO_PKI: Ignoring match on map SSL, index 20 for WebVPN group map
```

圖C5：失敗證書組匹配策略的輸出

圖C5：吊銷證書的輸出

```
n %PI=X-3-7E17t02h7a Certinf icaHtue cnhta,in faioled uvalidation=.
CMertifiIcLa,ted ccha=inl ais eibtrhaer tin,valdid cor =noct
oamuthori,zed.
map rule: subject-name ne "".
CRYPTO_PKI: Peer cert has been authorized by map: DefaultCertificateMap
sequence: 10.
Tunnel Group Match on map DefaultCertificateMap sequence # 10.
Group name is CAC-USERS
CRYPTO_PKI: Checking to see if an identical cert is
already in the database...
CRYPTO_PKI: looking for cert in handle=2467668, digest=
CRYPTO_PKI: Cert record not found, returning E_NOT_FOUND
CRYPTO_PKI: Cert not found in database.
CRYPTO_PKI: Looking for suitable trustpoints...
CRYPTO_PKI: Found a suitable authenticated trustpoint trustpoint0.
CRYPTO_PKI: Certificate validation: Successful, status: 0. Attempting
to retrieve revocation status if necessary
CRYPTO_PKI: Attempting to find OCSP override for peer cert: serial
number: 2FB5FC74000000000035, subject name: cn=Ethan
Hunt,ou=MIL,dc=ggsgseclab,dc=org, issuer_name:
cn=ggsgseclab,dc=ggsgseclab,dc=org.
CRYPTO_PKI: Processing map rules for DefaultCertificateMap.
CRYPTO_PKI: Processing map DefaultCertificateMap sequence 10...
CRYPTO_PKI: Match of subject-name field to map PASSED. Peer cert field:
= cn=Ethan Hunt,ou=MIL,dc=ggsgseclab,dc=org, map rule: subject-name
ne "".
CRYPTO_PKI: Peer cert has been authorized by map: DefaultCertificateMap
sequence: 10.
CRYPTO_PKI: Found OCSP override match. Override URL:
http://ocsp.disa.mil, Override trustpoint: OCSP
CRYPTO_PKI: crypto_pki_get_cert_record_by_subject()
CRYPTO_PKI: Found a subject match
ERROR: Certificate validation failed, Certificate is revoked, serial
number: 2FB5FC74000000000035, subject name: cn=Ethan
Hunt,ou=MIL,dc=ggsgseclab,dc=org
CRYPTO_PKI: Certificate not validated
```

附錄D -在MS中驗證LDAP對象

在Microsoft server 2003 CD中，可以安裝其他工具來檢視LDAP結構以及LDAP對象/屬性。要安裝這些工具，請選擇CD中的Support目錄，然後選擇Tools。安裝SUPTOOLS.MSI。

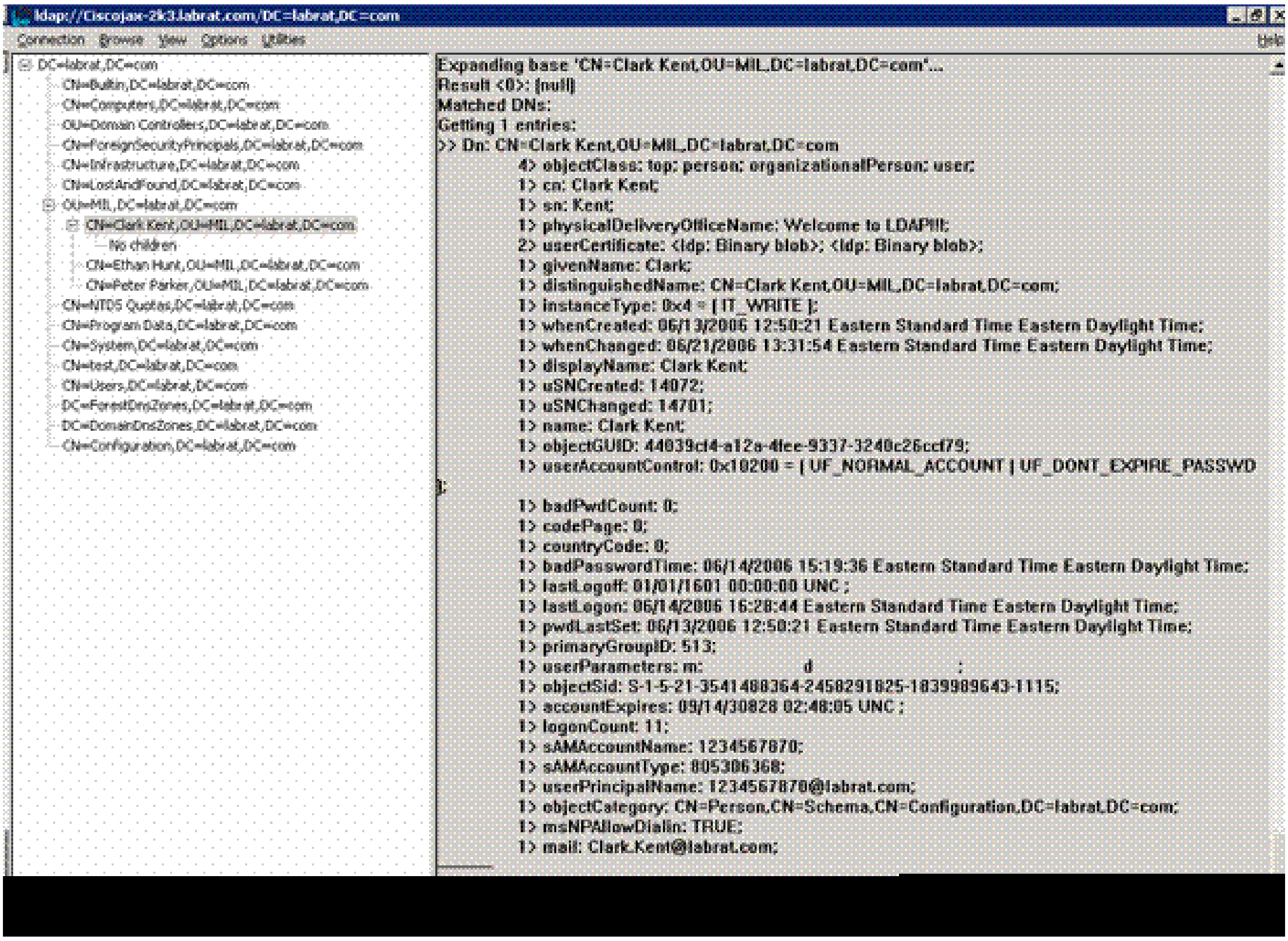
LDAP檢視器

1. 安裝完成後，選擇Start > Run。
2. 鍵入ldp，然後按一下Ok。這會啟動LDAP檢視器。
3. 選擇Connection > Connect。
4. 輸入伺服器名稱，然後按一下Ok。
5. 選擇Connection > Bind。
6. 輸入使用者名稱和密碼。

   附註：您需要管理員許可權。

7. 按一下「OK」（確定）。
8. 檢視LDAP對象。請參閱圖D1。

圖D1： LDAP檢視器



```
DC=labrat,DC=com
    CN=Builtin,DC=labrat,DC=com
    CN=Computers,DC=labrat,DC=com
    OU=Domain Controllers,DC=labrat,DC=com
    CN=ForeignSecurityPrincipals,DC=labrat,DC=com
    CN=Infrastructure,DC=labrat,DC=com
    CN=LostAndFound,DC=labrat,DC=com
    OU=MIL,DC=labrat,DC=com
        CN=Clark Kent,OU=MIL,DC=labrat,DC=com
            No children
        CN=Ethan Hunt,OU=MIL,DC=labrat,DC=com
        CN=Peter Parker,OU=MIL,DC=labrat,DC=com
    CN=NTDS Quotas,DC=labrat,DC=com
    CN=Program Data,DC=labrat,DC=com
    CN=System,DC=labrat,DC=com
    CN=test,DC=labrat,DC=com
    CN=Users,DC=labrat,DC=com
    DC=ForestDnsZones,DC=labrat,DC=com
    DC=DomainDnsZones,DC=labrat,DC=com
    CN=Configuration,DC=labrat,DC=com
```

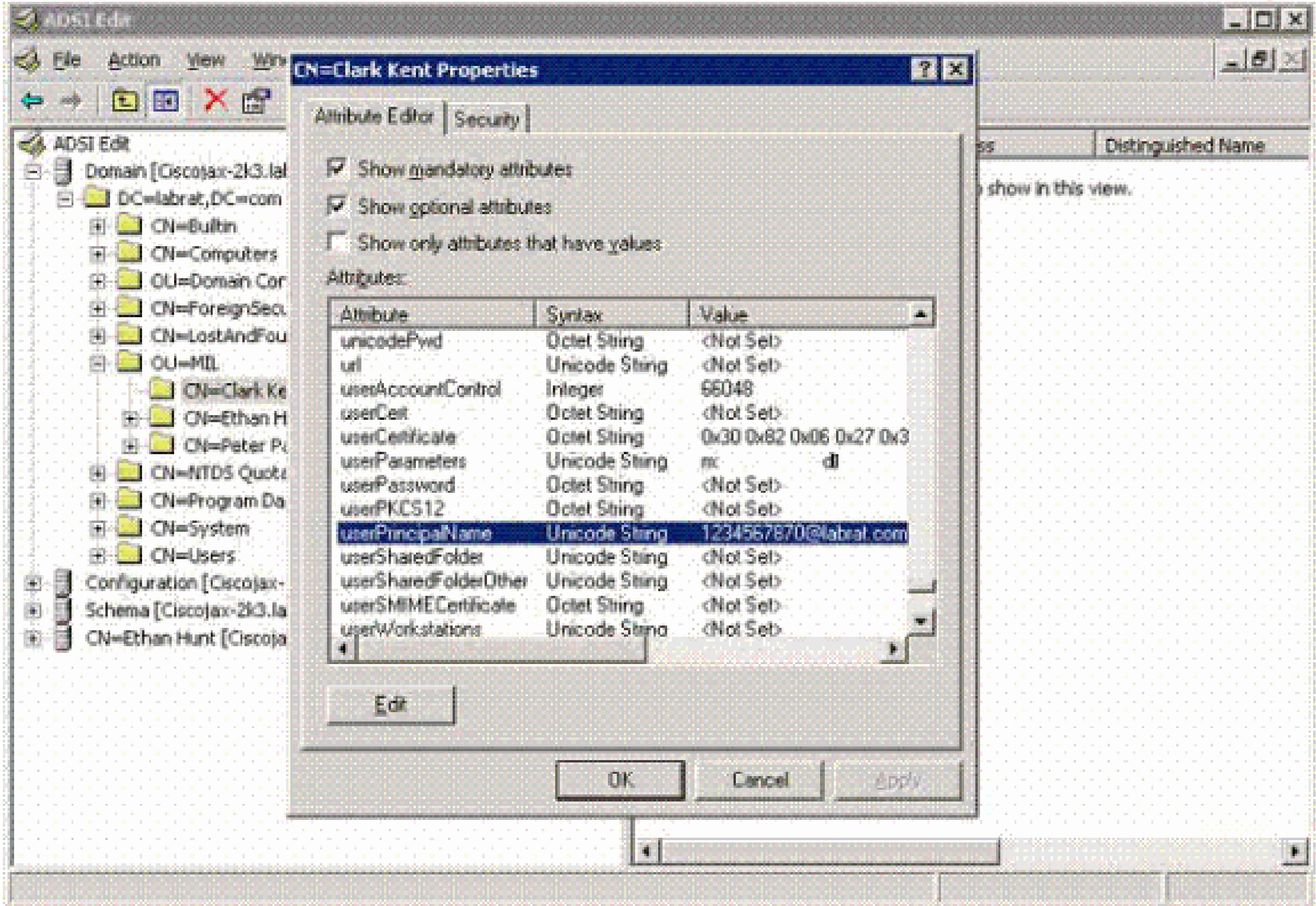
```
Expanding base 'CN=Clark Kent,OU=MIL,DC=labrat,DC=com'...
Result <0>: (null)
Matched DNs:
Getting 1 entries:
>> Dn: CN=Clark Kent,OU=MIL,DC=labrat,DC=com
        4> objectClass: top; person; organizationalPerson; user;
        1> cn: Clark Kent;
        1> sn: Kent;
        1> physicalDeliveryOfficeName: Welcome to LDAP!!!;
        2> userCertificate: <ldp: Binary blob>; <ldp: Binary blob>;
        1> givenName: Clark;
        1> distinguishedName: CN=Clark Kent,OU=MIL,DC=labrat,DC=com;
        1> instanceType: 0x4 = ( IT_WRITE );
        1> whenCreated: 06/13/2006 12:50:21 Eastern Standard Time Eastern Daylight Time;
        1> whenChanged: 06/21/2006 13:31:54 Eastern Standard Time Eastern Daylight Time;
        1> displayName: Clark Kent;
        1> uSNCreated: 14072;
        1> uSNChanged: 14701;
        1> name: Clark Kent;
        1> objectGUID: 44039cf4-a12a-4fee-9337-3240c26ccf79;
        1> userAccountControl: 0x10200 = ( UF_NORMAL_ACCOUNT | UF_DONT_EXPIRE_PASSWD
);
        1> badPwdCount: 0;
        1> codePage: 0;
        1> countryCode: 0;
        1> badPasswordTime: 06/14/2006 15:19:36 Eastern Standard Time Eastern Daylight Time;
        1> lastLogoff: 01/01/1601 00:00:00 UNC ;
        1> lastLogon: 06/14/2006 16:28:44 Eastern Standard Time Eastern Daylight Time;
        1> pwdLastSet: 06/13/2006 12:50:21 Eastern Standard Time Eastern Daylight Time;
        1> primaryGroupID: 513;
        1> userParameters: m:                d                    ;
        1> objectSid: S-1-5-21-3541408364-2458291825-1839989643-1115;
        1> accountExpires: 09/14/30828 02:48:05 UNC ;
        1> logonCount: 11;
        1> sAMAccountName: 1234567870;
        1> sAMAccountType: 805306368;
        1> userPrincipalName: 1234567870@labrat.com;
        1> objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=labrat,DC=com;
        1> msNPAllowDialin: TRUE;
        1> mail: Clark.Kent@labrat.com;
```

Active Directory服務介面編輯器

- 在Active Directory伺服器中，選擇Start > Run。
- 鍵入adsiedit.msc。這會啟動編輯器。
- 按一下右鍵對象，然後按一下屬性。

此工具顯示特定物件的所有屬性。請參閱圖D2。

圖D2：ADSI編輯



CN=Clark Kent Properties

Attribute Editor | Security

☑ Show mandatory attributes

☑ Show optional attributes

☐ Show only attributes that have values

Attributes:

Attribute	Syntax	Value
unicodePwd	Octet String	<Not Set>
url	Unicode String	<Not Set>
userAccountControl	Integer	66048
userCert	Octet String	<Not Set>
userCertificate	Octet String	0x30 0x82 0x06 0x27 0x3
userParameters	Unicode String	m: d
userPassword	Octet String	<Not Set>
userPKCS12	Octet String	<Not Set>
userPrincipalName	Unicode String	1234567870@labrat.com
userSharedFolder	Unicode String	<Not Set>
userSharedFolderOther	Unicode String	<Not Set>
userSMIMECertificate	Octet String	<Not Set>
userWorkstations	Unicode String	<Not Set>

附錄E

可以建立AnyConnect配置檔案並將其增加到工作站。配置檔案可以引用各種值（如ASA主機）或證書匹配引數（如可分辨名稱或頒發者）。設定檔會儲存為.xml檔案，並可使用記事本編輯。檔案可以手動增加到每個客戶端，也可以透過組策略從ASA推送到每個客戶端。檔案儲存在：

```
C:\Documents and Settings\All Users\Application Data\Cisco\Cisco
AnyConnect VPN Client\Profile
```

請完成以下步驟：

1. 選擇AnyConnectProfile.tmpl並使用記事本打開檔案。

2. 對檔案進行適當的修改，例如簽發者或主機IP。有關示例，請參見圖F1。

3. 完成後，將檔案另存為.xml。

有關配置檔案管理，請參閱Cisco AnyConnect文檔。簡而言之：

- 設定檔必須是貴公司的唯一名稱。例如：CiscoProfile.xml
- 設定檔名稱必須相同，即使公司內的個別群組名稱不同。

該檔案由Secure Gateway管理員維護，然後與客戶端軟體一起分發。基於此XML的配置檔案可以隨時分發到客戶端。支援的發佈機制是軟體發佈隨附的檔案，或是自動下載機制的一部分。自動下載機制僅適用於某些Cisco Secure Gateway產品。

> 注意：強烈建議管理員使用聯機驗證工具或透過ASDM中的配置檔案導入功能來驗證他們建立的XML配置檔案。可透過在此目錄中找到的AnyConnectProfile.xsd完成驗證。AnyConnectProfile是代表AnyConnect客戶端配置檔案的根元素。

這是Cisco AnyConnect VPN客戶端配置檔案XML檔案的示例。

```
<#root>

xml version="1.0" encoding="UTF-8"
- - <AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/
AnyConnectProfile.xsd">


!--- The ClientInitialization section represents global settings !--- for the client. In some cases, fo
!--

-->
-

 <ClientInitialization>


!--- The Start Before Logon feature can be used to activate !--- the VPN as part of the logon sequence.


-->
<UseStartBeforeLogon UserControllable="false">false</UseStartBeforeLogon>


!--- This control enables an administrator to have a one time !--- message displayed prior to a users f




<ShowPreConnectMessage>false</ShowPreConnectMessage>


!-- This section enables the definition of various attributes !--- that can be used to refine client ce
```

```
-->
-

<CertificateMatch>


!--- Certificate Distinguished Name matching allows !--- for exact match criteria in the choosing of ac



- <DistinguishedName>
- <DistinguishedNameDefinition Operator="Equal" Wildcard="Disabled">
<Name>ISSUER-CN</Name>
<Pattern>DoD-Issuer-ABC</Pattern>
</DistinguishedNameDefinition>
</DistinguishedName>
</CertificateMatch>
</ClientInitialization>

-
!-- This section contains the list of hosts from which !--- the user is able to select.

-

<ServerList>




!--- This is the data needed to attempt a connection to !--- a specific host.

-->
-

<HostEntry>
<HostName>host-02</HostName>
<HostAddress>host-02.dod.gov</HostAddress>
</HostEntry>
- <HostEntry>
<HostName>host-01</HostName>
<HostAddress>192.168.1.1</HostAddress>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

相關資訊

- X.509和RFC 3280指定的憑證和CRL
- RFC 2560指定的OCSP
- 公鑰基礎設施簡介
- 按草案標準分析的「輕量OCSP」
- RFC 2246指定的SSL/TLS
- 技術支援與文件 - 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）。