ASA 8.x:帶MAC支援的AnyConnect SSL VPN CAC-SmartCards配置

目錄

簡介

本文檔提供思科自適應安全裝置(ASA)上用於MAC支援的AnyConnect VPN遠端訪問的示例配置，以及用於身份驗證的通用訪問卡(CAC)。

本文檔的範圍是涵蓋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

基本瞭解Cisco ASA、Cisco AnyConnect客戶端、Microsoft AD/LDAP和公鑰基礎設施(PKI)有助於理解完整的設定。熟悉AD組成員身份、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：

- 執行軟體版本8.0(x)和更新版本的Cisco 5500系列調適型安全裝置(ASA)
- 適用於ASA 8.x的Cisco調適型安全裝置管理器(ASDM)版本6.x
- 含MAC支援的Cisco AnyConnect VPN使用者端2.2

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

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

Cisco ASA配置

本節介紹通過ASDM配置Cisco ASA。它包括通過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，證書中的使用者主體名稱(UPN)屬性填充在active directory中以進行授權。

部署注意事項

- 本指南不包括基本配置，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強制進行OCSP檢查，但隧道在未配置OCSP的情況下工作。
- 以藍色突出顯示的部分是高級功能，可以隨附這些功能，為設計增加更多安全性。
- 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上的埠以獲得訪問許可權。例如，將埠445用於ASDM，將443用於AC/SSL VPN。8.x中的ASDM URL訪問已更改。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。
- 請參閱附錄A（針對LDAP和動態訪問策略對映示例）以瞭解其他策略實施。
- 有關如何檢查MS中的LDAP對象的資訊，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。

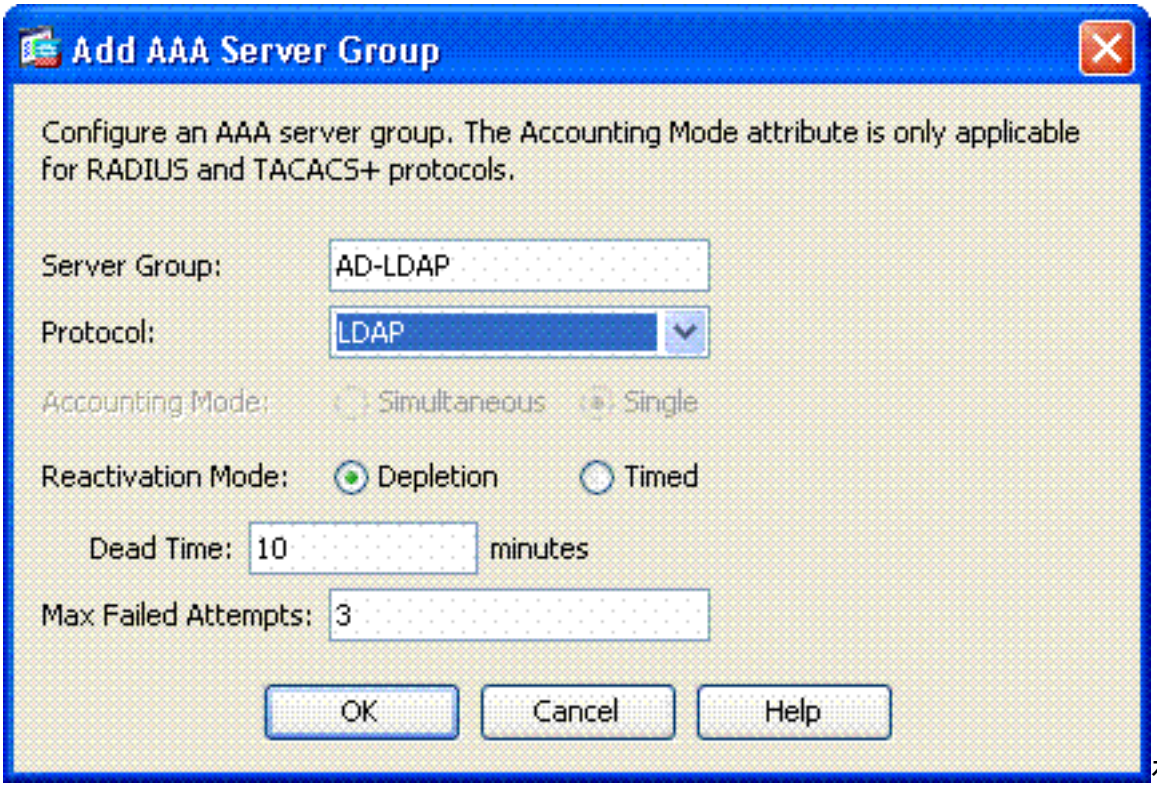
驗證、授權、記帳(AAA)配置

您會透過憑證授權單位(CA)伺服器或他們自己組織的CA伺服器，透過使用他們的通用存取卡(CAC)中的憑證進行驗證。該證書必須對於遠端訪問網路有效。除身份驗證外，還必須授權您使用Microsoft Active Directory或輕量級目錄訪問協定(LDAP)對象。國防部(DoD)需要使用使用者主體名稱(UPN)屬性進行授權，這是證書的使用者替代名稱(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。有關使用LDAP對象對映的其他配置，請參閱附錄A。

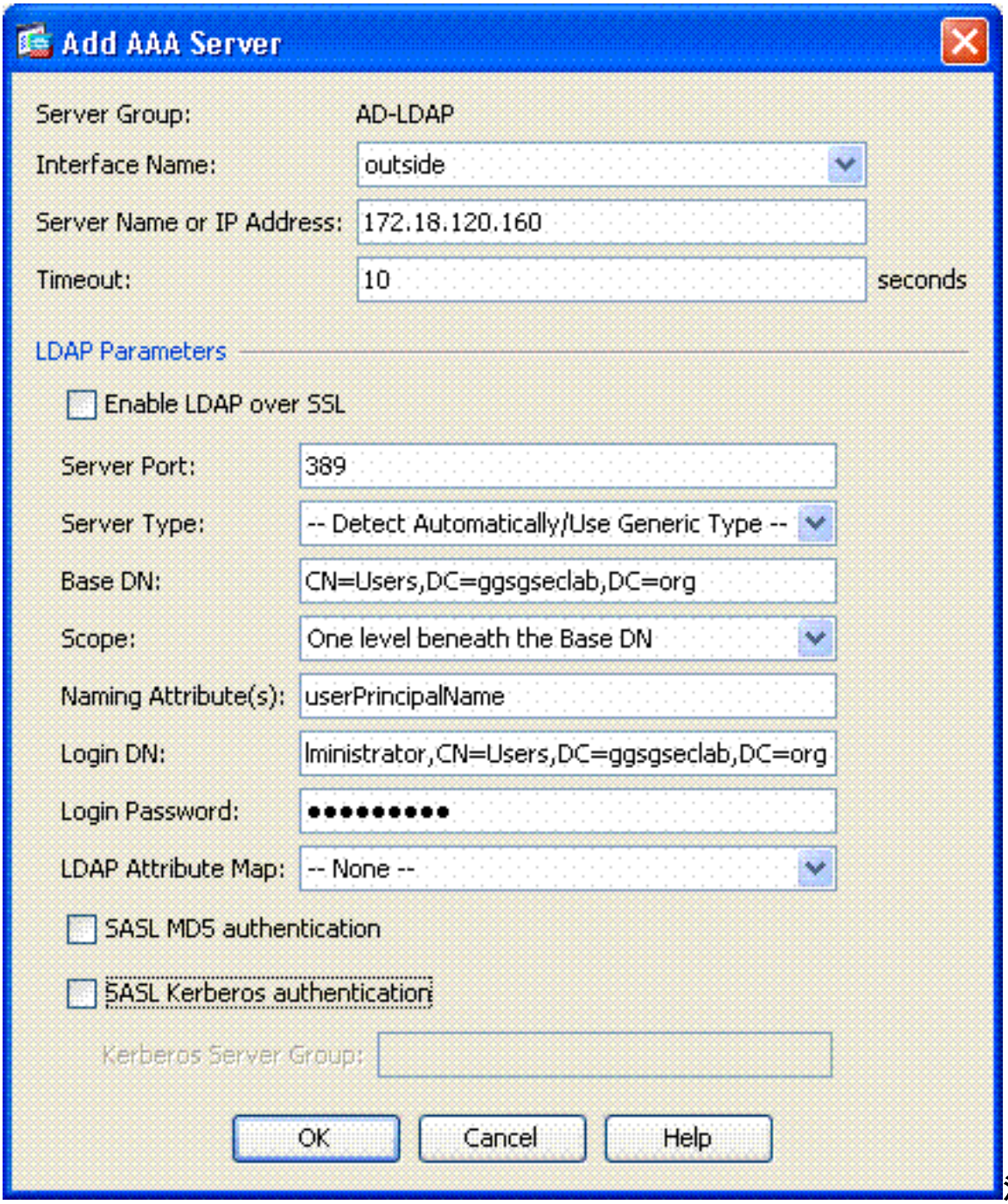
配置LDAP伺服器

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，並在協定單選按鈕中選擇**LDAP**。請參見圖1。
4. 在選定組表的伺服器中，按一下**Add**。確保在上表中突出顯示您建立的伺服器。
5. 在編輯AAA伺服器視窗中，完成以下步驟。請參見圖2。**注意：如**果您的**LDAP/AD已配**置為此類連線，請選擇**Enable LDAP over SSL**（通過SSL啟用LDAP）選項。選擇LDAP所在的介面。本指南顯示介面內部。輸入伺服器的IP地址。輸入**server port**。預設LDAP埠為389。選擇**Server Type**。輸入**Base DN**。請向AD/LDAP管理員諮詢這些值。**圖1**



在scope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。在命名屬性中，輸入**userPrincipalName**。此屬性用於AD/LDAP伺服器中的使用者授權。在登入DN中，輸入管理員DN。**注意：您**具有檢視/搜尋包含使用者對象和組成員資格的LDAP結構的管理許可權或許可權。在登入密碼中，輸入管理員的密碼。將LDAP屬性保留為**none**。**圖2**



注意：以後在配置中使用此選項可以新增其他AD/LDAP對象以進行授權。選擇**OK**。

6. 選擇**OK**。

管理憑證

在ASA上安裝證書有兩個步驟。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使用這些證書、根CA2、3類根、CA##中間（ASA註冊時使用）、ASA ID證書和OCSP證書。但是，如果您選擇不使用OCSP，則不需要安裝OCSP證書。

注意：請與您的安全POC聯絡以獲取根證書以及如何註冊裝置的身份證書的說明。SSL證書應足以供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。可以在Microsoft Certificate Store with Internet Explorer中檢視證書。DoD已生成一個批處理檔案，該檔案會自動將所有CA新增到電腦。有關更多資訊，請諮詢您的PKI POC。

注意：DoD CA2和3類根以及頒發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，只要新增了CA2和3類根，就可以信任它們。

生成金鑰

請完成以下步驟：

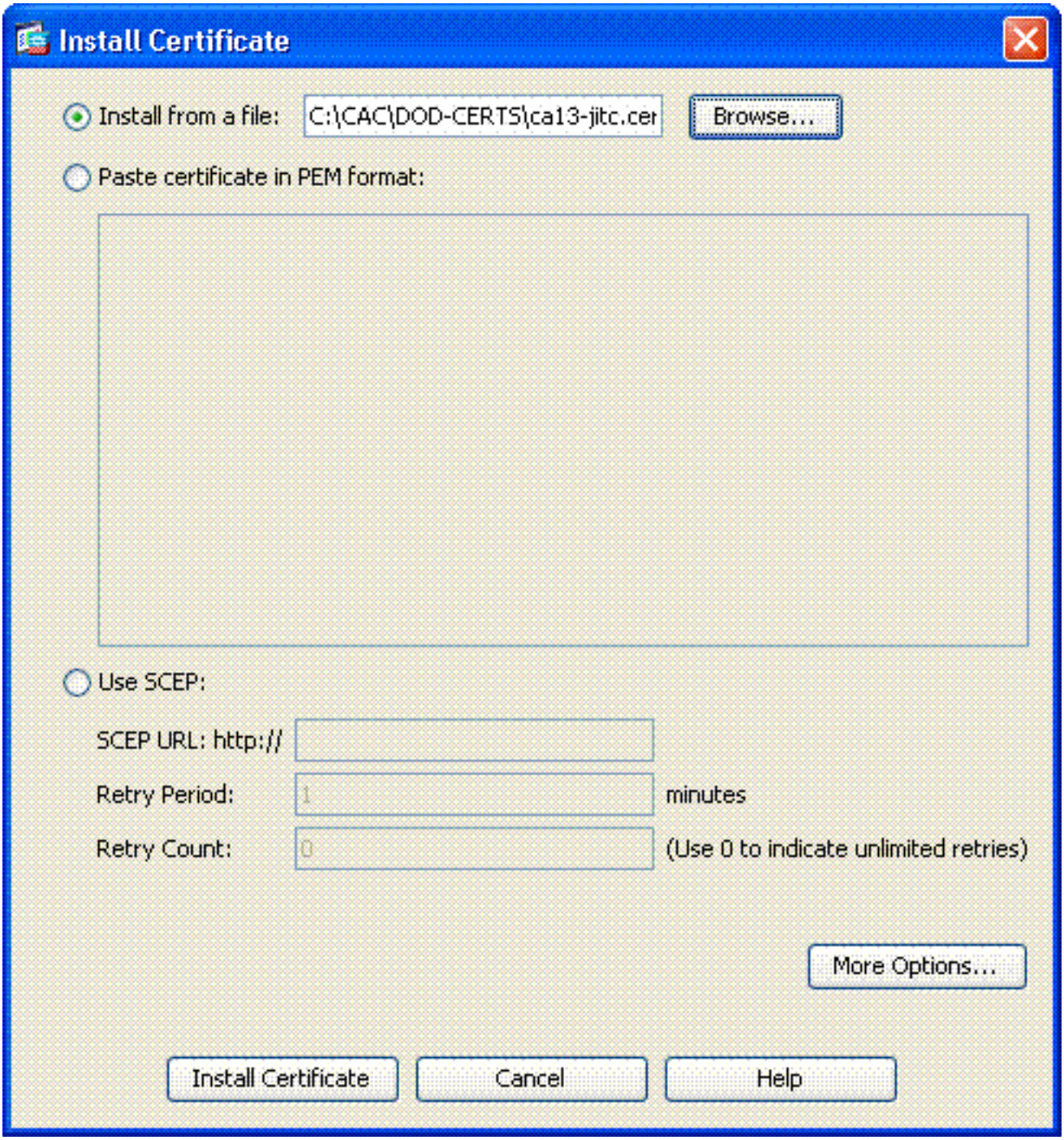
1. 選擇**Remote Access VPN > Certificate Management > Identity Certificate > Add**。
2. 選擇**Add a new id certificate**，然後選擇**New** by the key pair選項。
3. 在「新增金鑰對」視窗中，輸入金鑰名稱**DoD-1024**。按一下無線電以新增新金鑰。請參見圖3。**圖3**

4. 選擇金鑰的大小。
5. 保持通用的**使用狀態**。
6. 按一下「**Generate Now**」。**注意：**DoD根CA 2使用2048位金鑰。應生成第二個使用2048位金鑰對的金鑰，以便能夠使用此CA。完成上述步驟以新增第二個鍵。

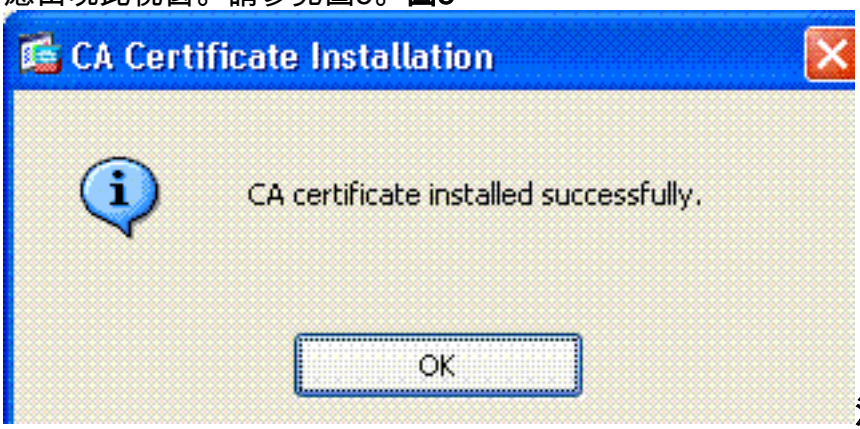
安裝根CA證書

請完成以下步驟：

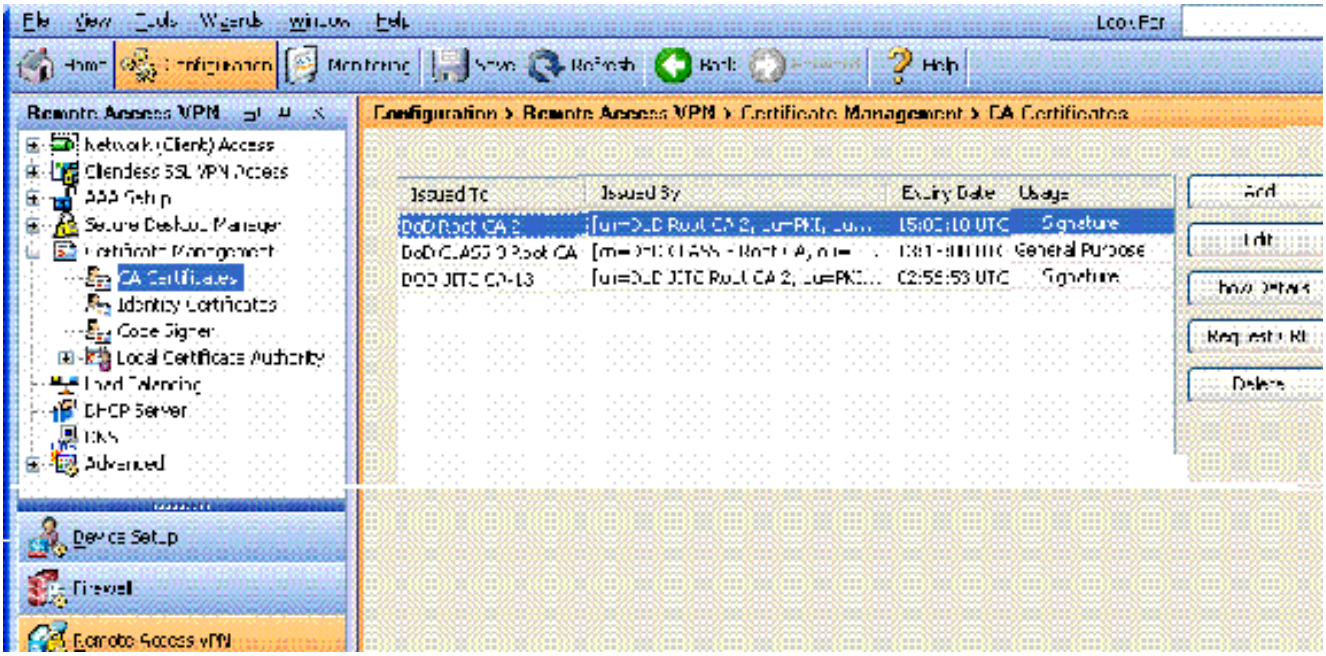
1. 選擇**Remote Access VPN > Certificate Management > CA Certificate > Add**。
2. 選擇「**Install from File**」，然後瀏覽到證書。
3. 選擇**Install Certificate**。**圖4:正在安裝根證書**



4. 應出現此視窗。請參見圖5。**圖5**

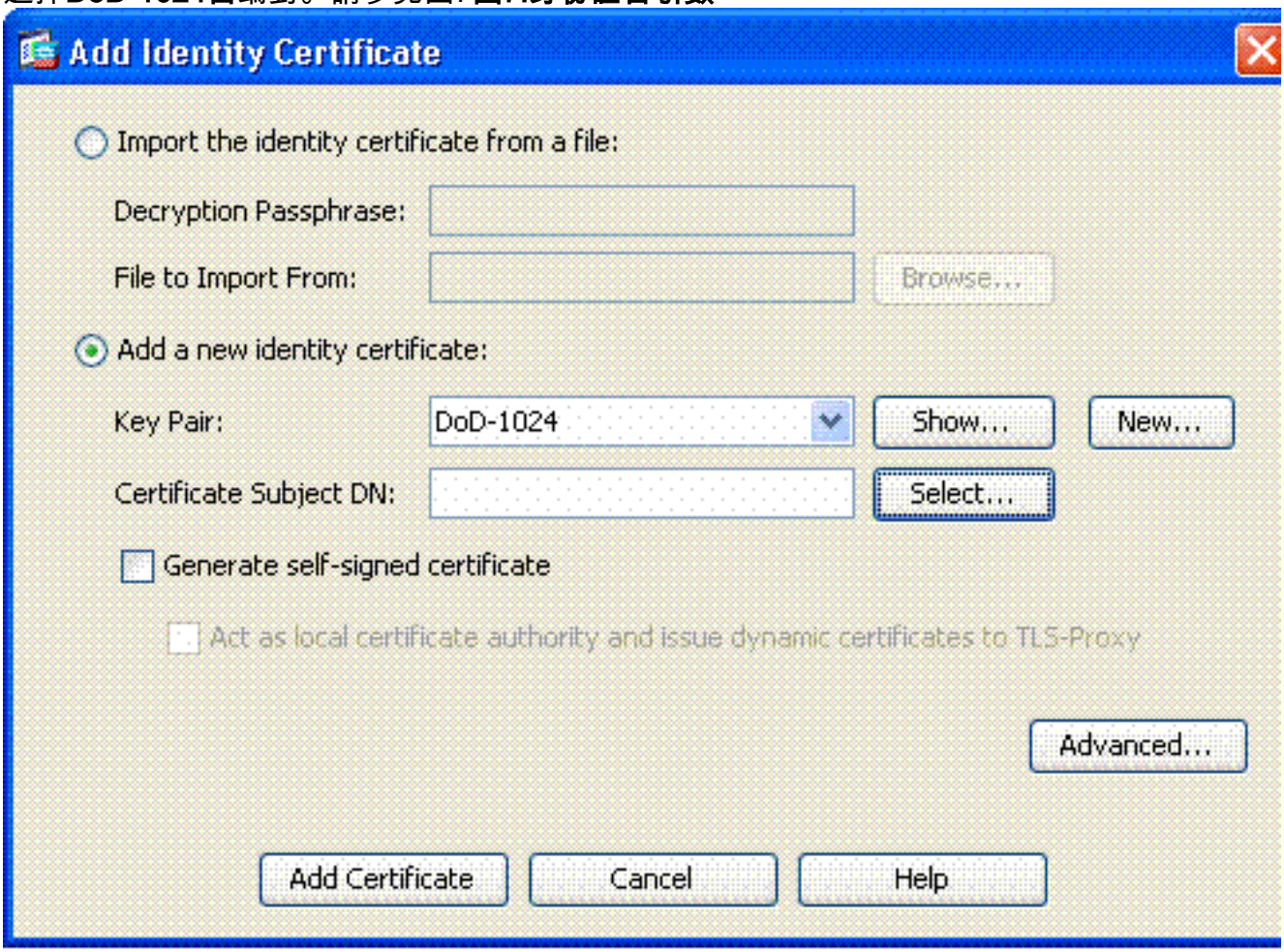


注意：對要安裝的每個證書重複步驟1到3。DoD PKI需要以下每個項的證書：根CA 2、Class 3 Root、CA## Intermediate、ASA ID和OCSP伺服器。如果不使用OCSP，則不需要OCSP證書。**圖6:正在安裝根證書**

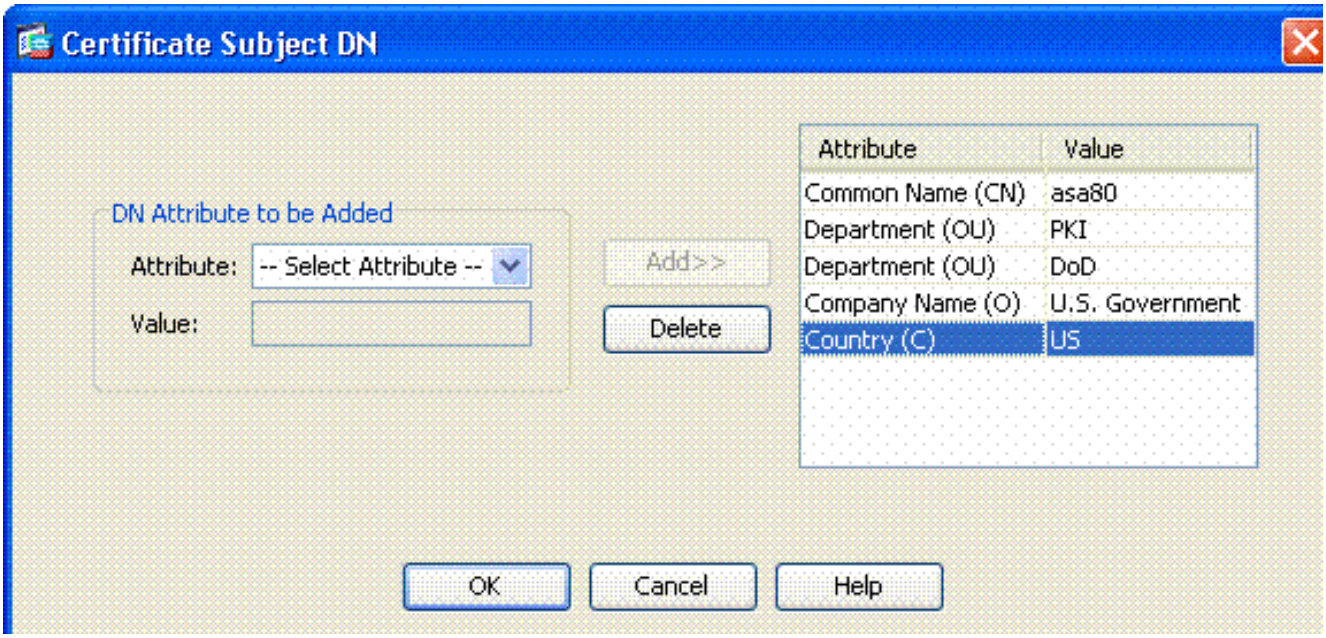


註冊ASA並安裝身份證書

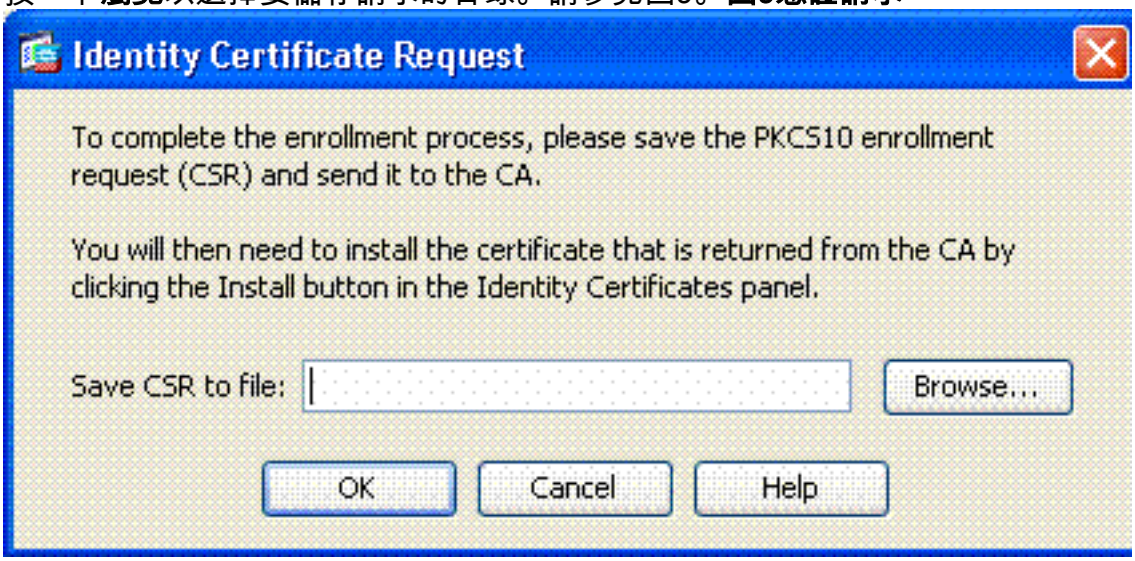
1. 選擇Remote Access VPN > Certificate Management > Identity Certificate > Add。
2. 選擇Add a new id certificate。
3. 選擇DoD-1024密鑰對。請參見圖7**圖7:身份證書引數**



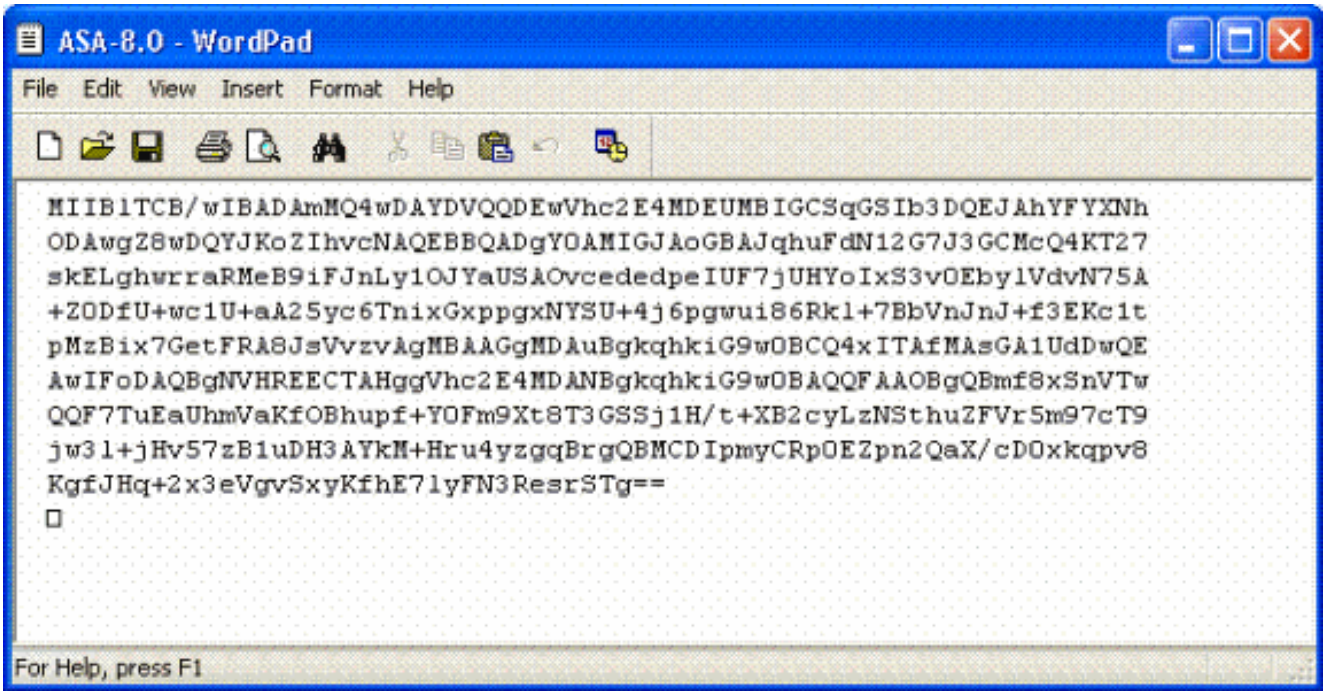
4. 轉到Certificate subject DN框，然後按一下**Select**。
5. 在Certificate Subject DN視窗中，輸入裝置的資訊。例如，請參見圖8。**圖8:編輯DN**



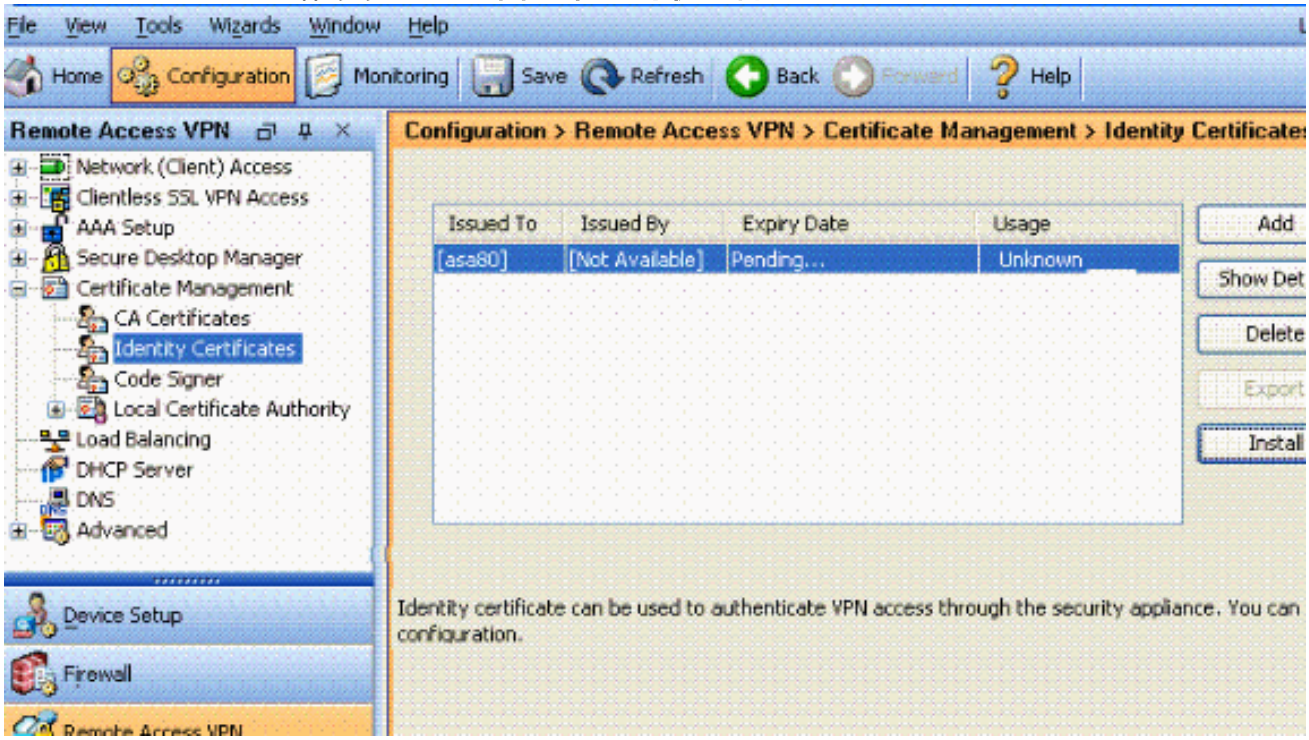
6. 選擇**OK**。**注意**：新增主題DN時，請確保使用系統中配置的裝置的主機名。PKI POC可以告訴您所需的必填欄位。
7. 選擇**Add certificate**。
8. 按一下**瀏覽**以選擇要儲存請求的目錄。請參見圖9。**圖9憑證請求**



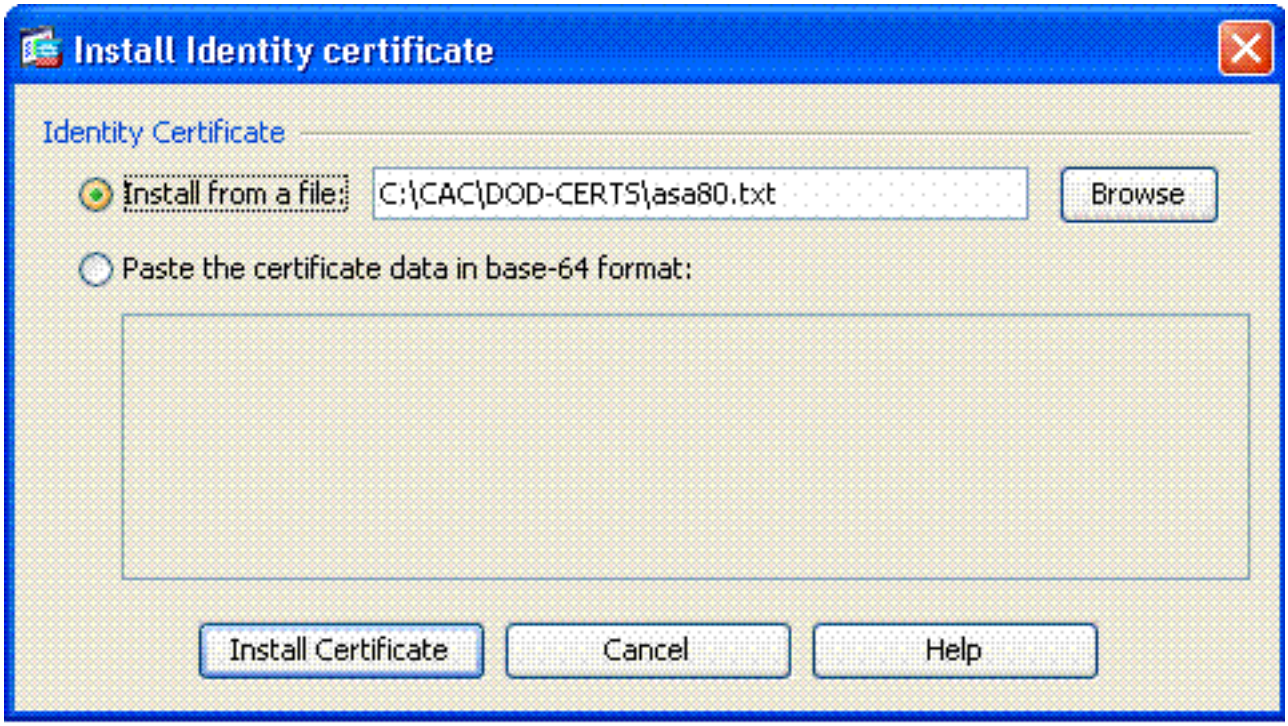
9. 使用寫字板開啟檔案，將請求複製到相應的文檔，然後傳送到您的PKI POC。請參見圖10。**圖10:註冊請求**



10. 收到來自CA管理員的證書後，選擇**Remote Access VPN > Certificate Management > ID Certificate > Install**。請參見圖11。**圖11:匯入身份證書**



11. 在「安裝證書」(Install certificate)視窗中，瀏覽到ID證書，然後選擇**「安裝證書」(Install Certificate)**。例如，請參見圖12。**圖12:正在安裝身份證書**



注意：建議匯出ID證書信任點以儲存頒發的證書和金鑰對。這允許ASA管理員在RMA或硬體故障時將證書和金鑰對匯入到新的ASA。有關詳細資訊，請參閱匯出和匯入信任點。**注意**：按一下**SAVE**，將組態儲存到快閃記憶體中。

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配置的使用者而言，這是一個易於使用的工具。第二個選項是手動執行並逐一執行每個選項。本配置指南使用手動方法。

注意：有兩種方法可以將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，並將其安裝在其電腦上。
2. 使用者可通過Web瀏覽器訪問ASA，並可下載客戶端。

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後，您只需從應用程式啟動AC客戶端。

建立IP地址池

如果您使用其他方法（例如DHCP），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「新增IP池」視窗中，輸入IP池的名稱、起始IP地址和結束IP地址並選擇子網掩碼。請參見

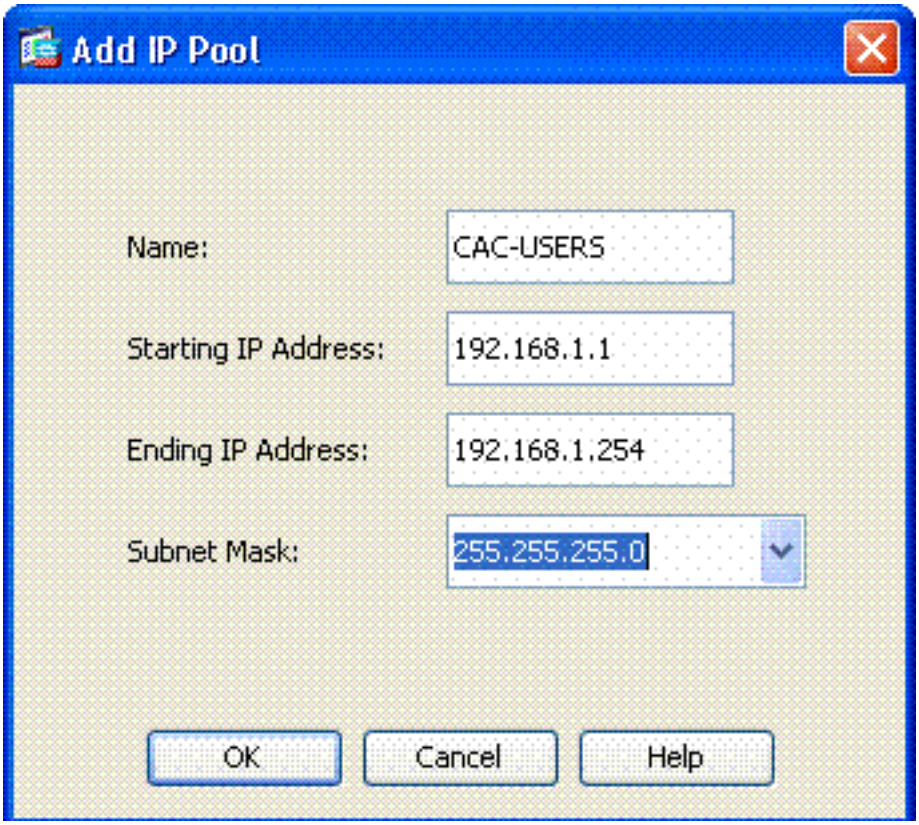
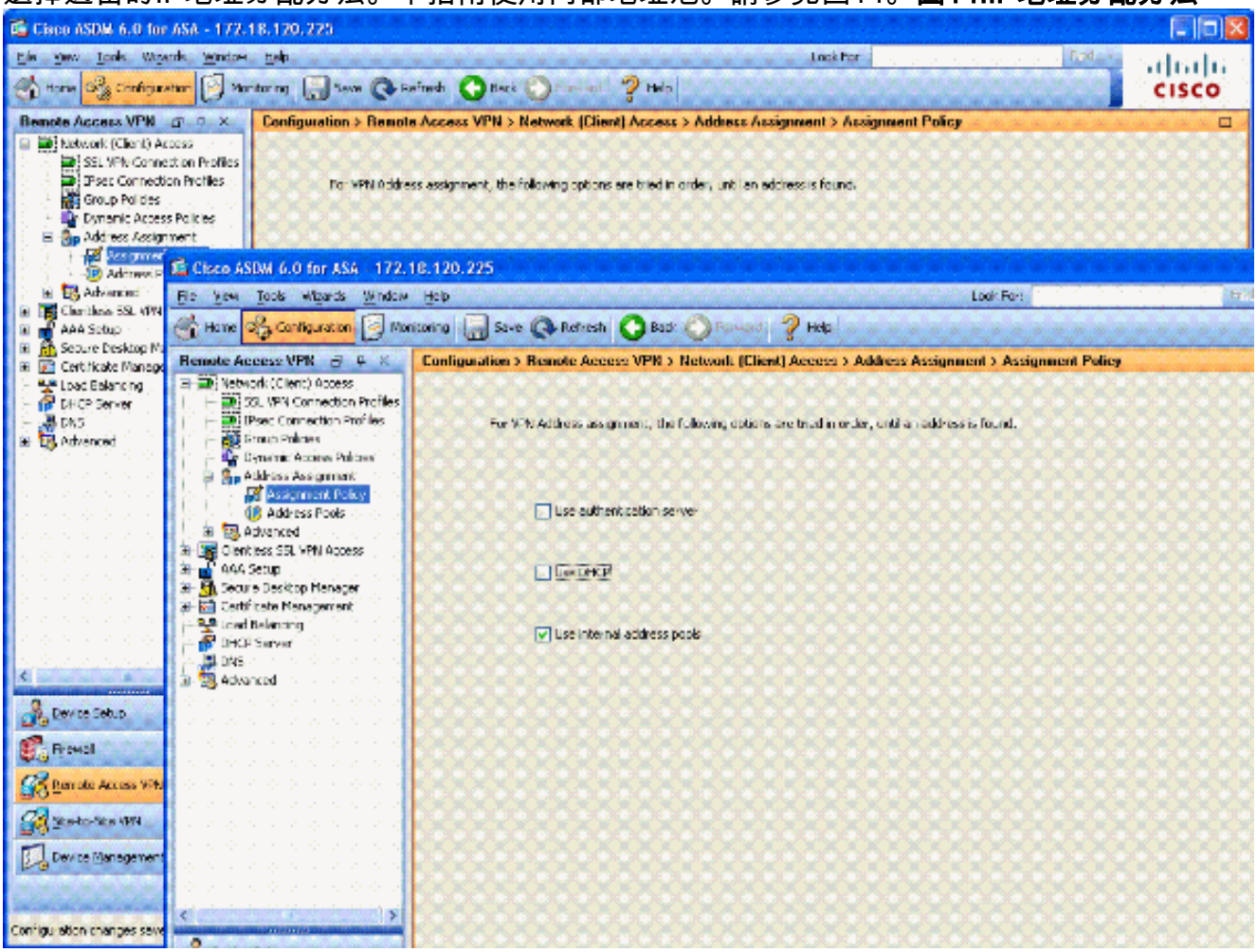


圖13。**圖13:新增IP池**

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。請參見圖14。**圖14:IP地址分配方法**



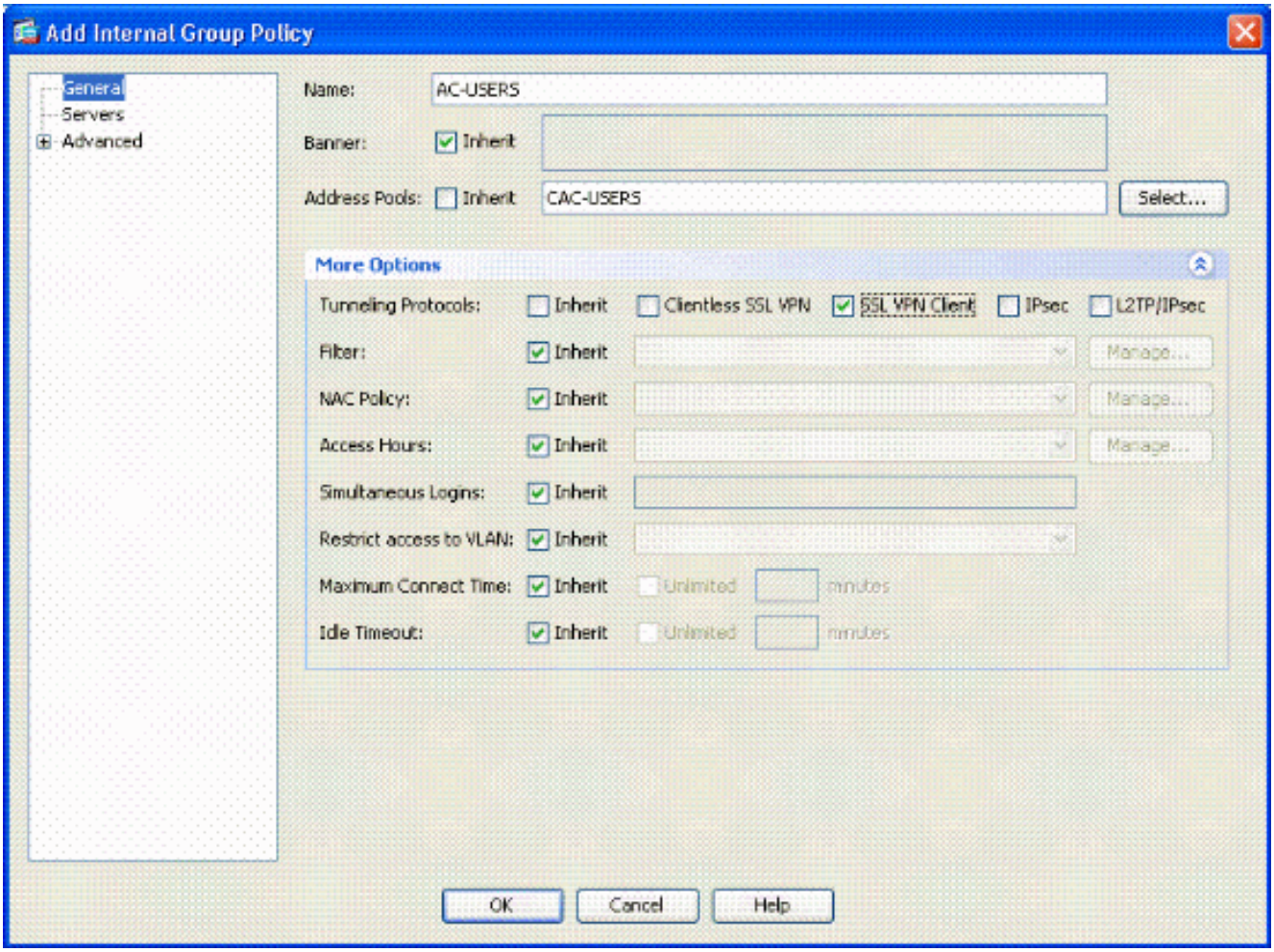
7. 按一下「Apply」。

建立隧道組和組策略

組策略

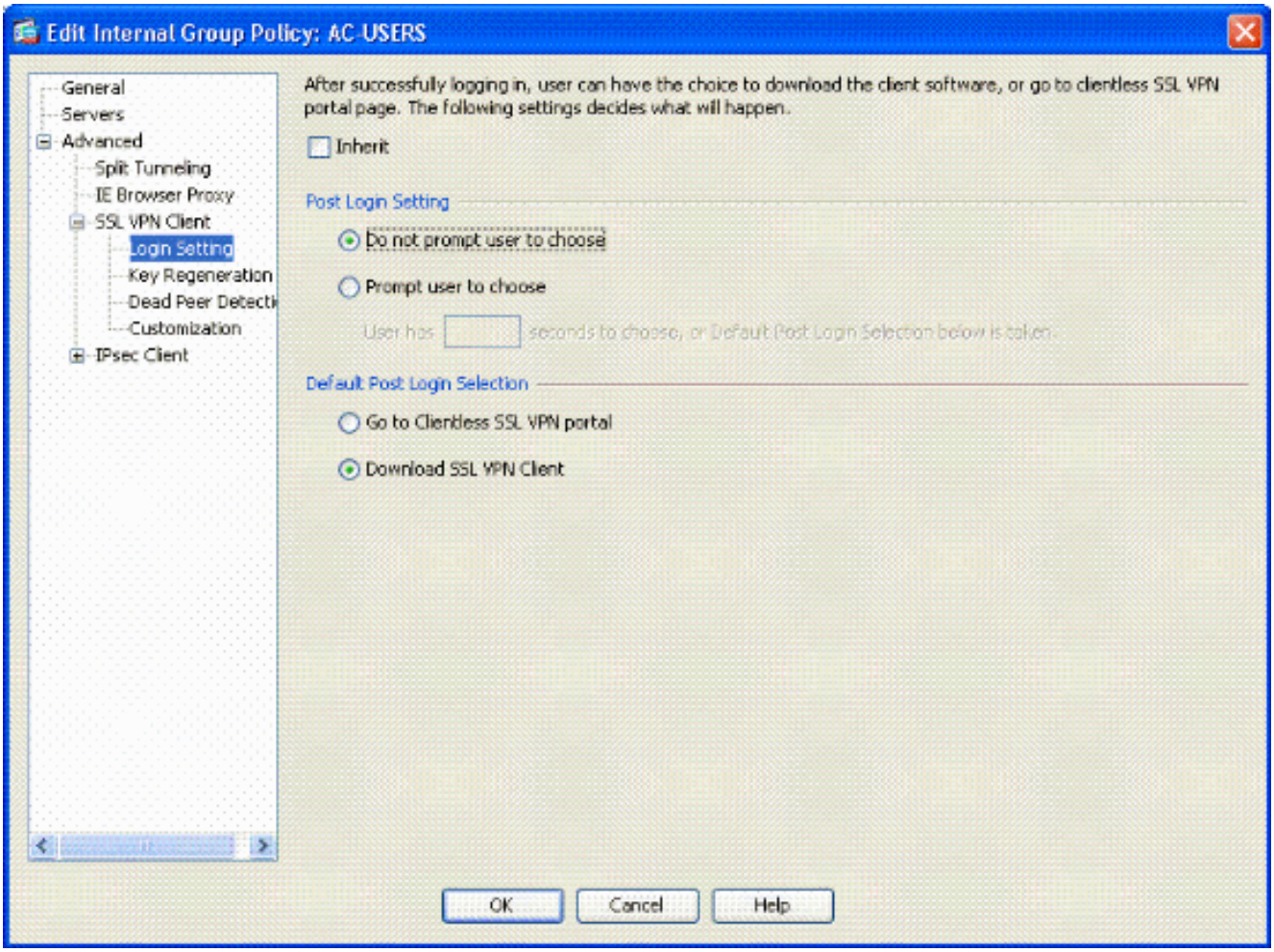
注意：如果不想建立新策略，您可以使用預設的內建組策略。

1. 選擇**Remote Access VPN -> Network(Client)Access -> Group Policies**。
2. 按一下**Add**並選擇**Internal Group Policy**。
3. 在新增內部組策略視窗中，在名稱文本框中輸入組策略的名稱。請參見圖15。**圖15:新增內部組策略**



在General頁籤中，選擇**SSL VPN Client in the Tunneling Protocols**選項，除非您使用其他協定，如無客戶端SSL。在Servers部分，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）。在Servers部分，取消選中Default Domain中的**inherit**覈取方塊並輸入相應的域名。在常規頁籤中，取消選中地址池部分中的**inherit**覈取方塊，然後新增在上一步中建立的地址池。如果您使用另一個IP地址分配方法，請保留該方法，以繼承並進行適當的更改。所有其他配置頁籤都保留為預設設定。**注意：**有兩種方法可將AC客戶端提供給終端使用者。方法之一是訪問Cisco.com並下載AC客戶端。第二種方法是當使用者嘗試連線時，讓ASA將客戶端下載到使用者。本示例顯示了後一種方法。

4. 接下來，選擇**Advanced > SSL VPN Client > Login Settings**。請參見圖16。**圖16:新增內部組策略**

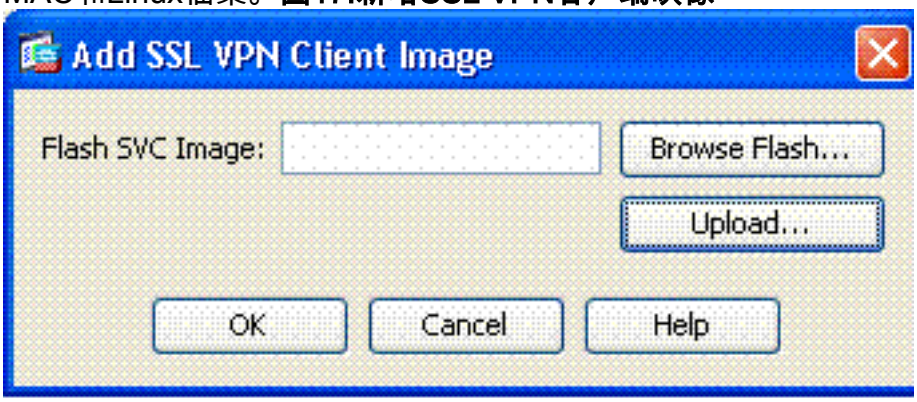


取消選中**Inherit**覈取方塊。選擇適合您環境的適當登入後設定。選擇適合您環境的適當預設登入後選擇。選擇**OK**。

隧道組介面和映像設定

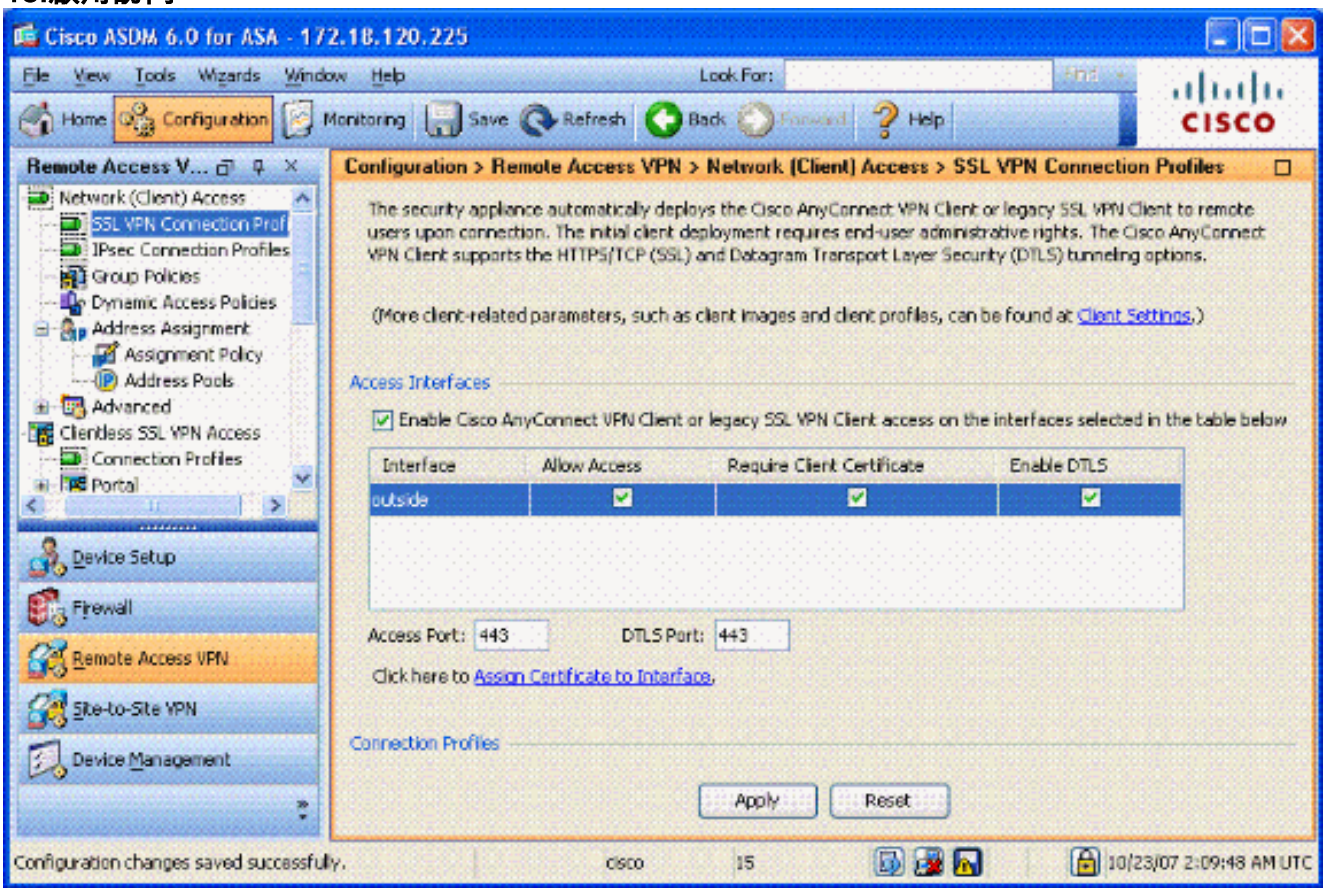
註：如果您不想建立新組，可以使用預設內建組。

1. 選擇**Remote Access VPN > Network(Client)Access > SSL VPN Connection Profile**。
2. 選擇**Enable Cisco AnyConnect Client.....**
3. 將出現一個對話方塊，其中提svc
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。如果映像不可用，請選擇**Upload**並瀏覽本地電腦上的檔案。請參閱圖17。可從Cisco.com下載檔案；有一個Windows、MAC和Linux檔案。**圖17:新增SSL VPN客戶端映像**

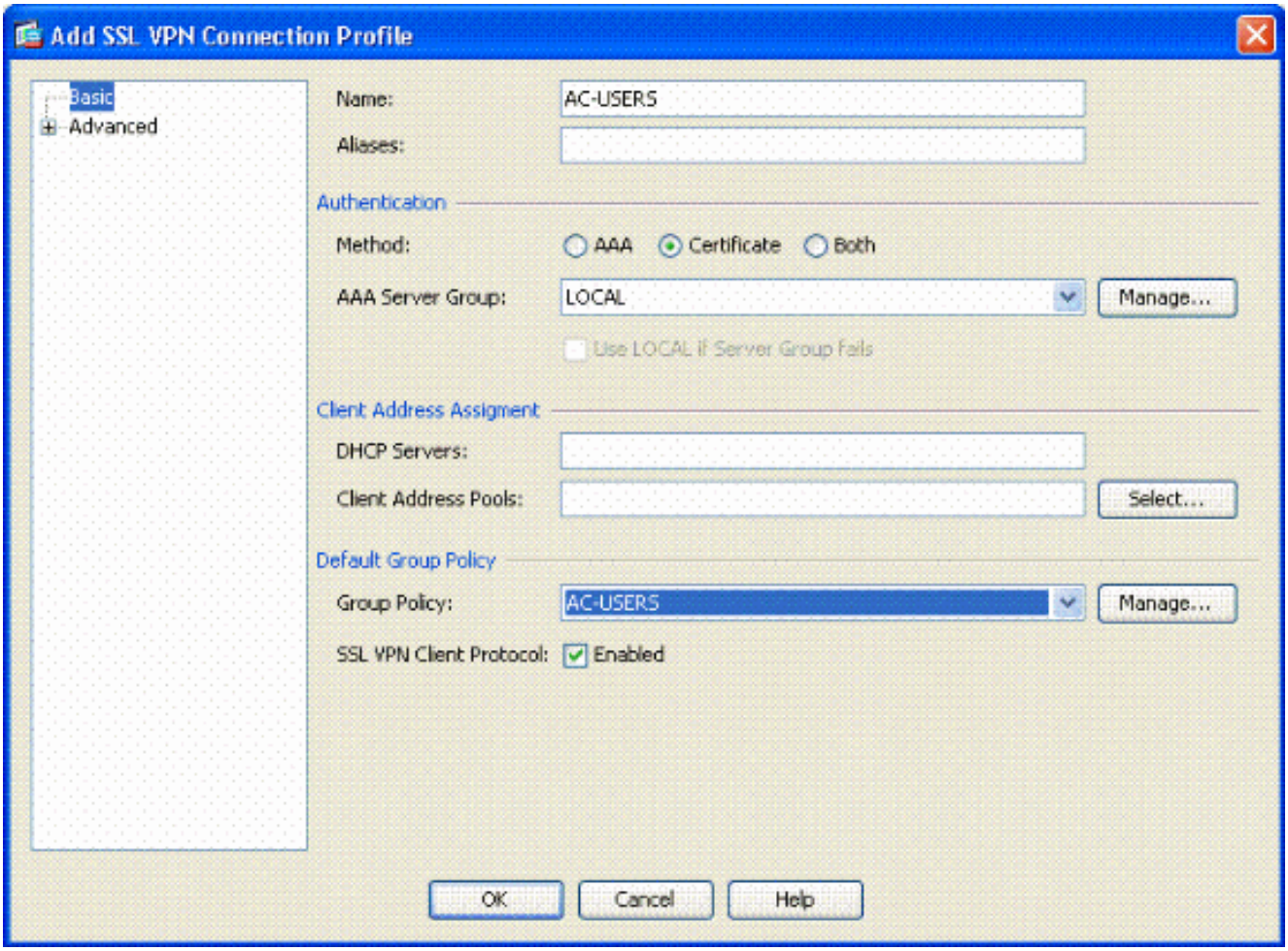


6. 接下來啟用**Allow Access、Require Client Cert**和**Enable DTLS**（可選）。請參見圖18。**圖**

18:啟用訪問

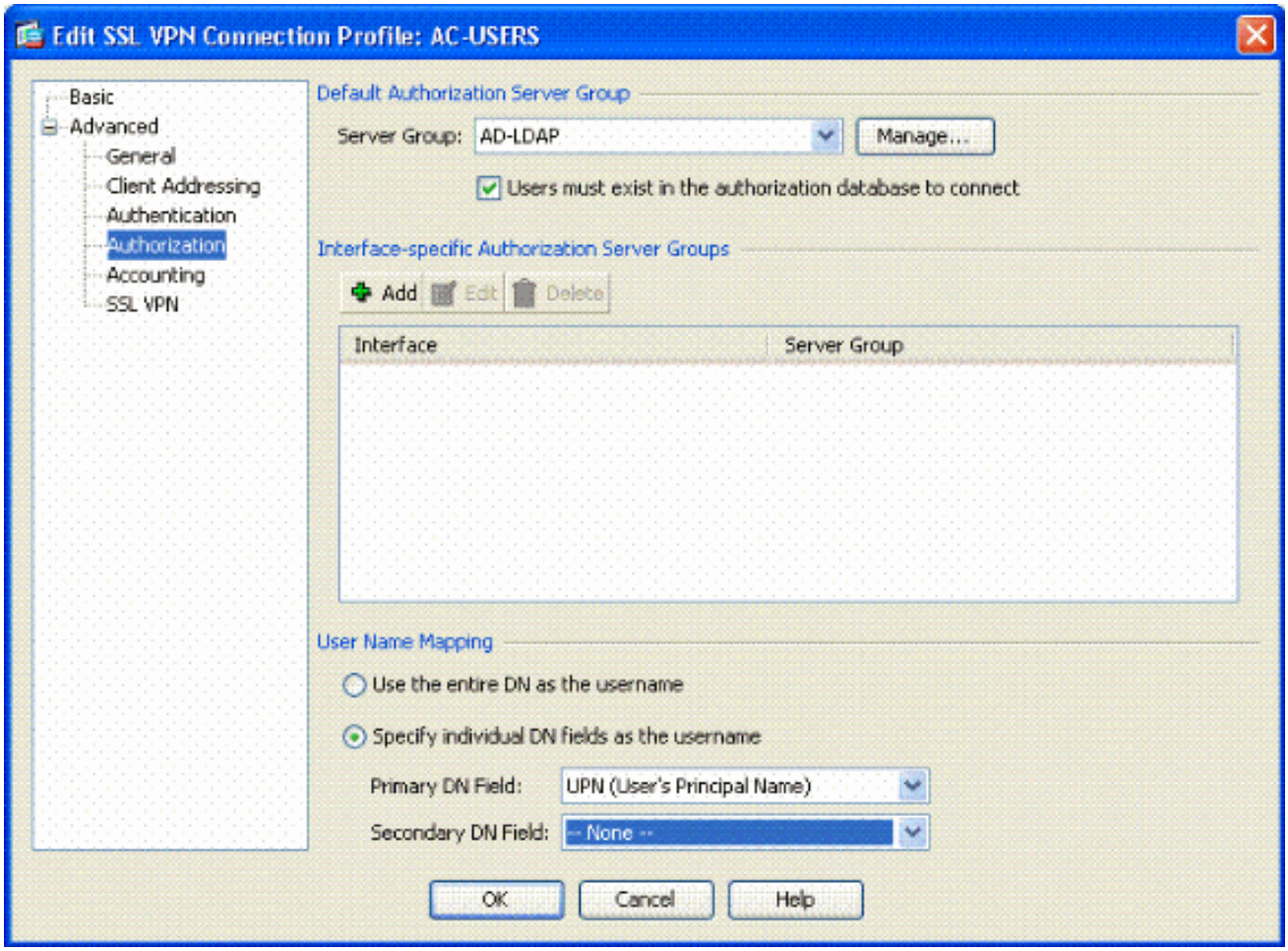


7. 按一下「Apply」。
8. 接下來，建立連線配置檔案/隧道組。選擇Remote Access VPN > Network(Client)Access > SSL VPN Connection Profile。
9. 在Connection Profiles部分，按一下Add。**圖19:新增連線配置檔案**



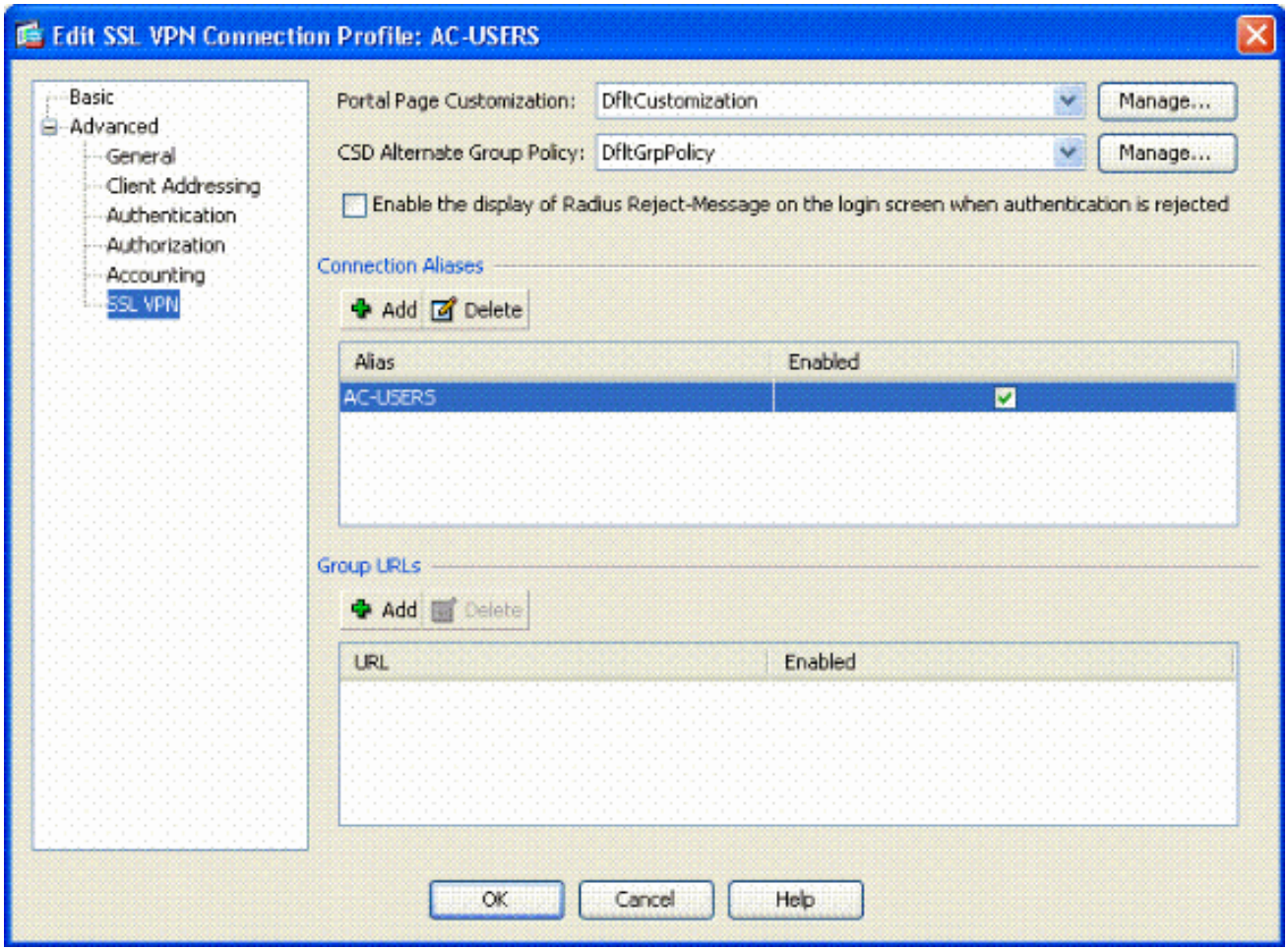
為組命名。在驗證方法中選擇**Certificate**。選擇以前建立的組策略。確保**SSL VPN Client**已啟用。保留其他選項為預設值。

10. 接下來，**選擇Advanced > Authorization**。請參見圖20**圖20:Authorization**



選擇以前建立的AD-LDAP組。選中**Users must exist...to connect。**在對映欄位中，為主節點選擇**UPN**，為輔助節點選擇**none。**

11. 選擇選單的**SSL VPN**部分。
12. 在「連線別名」部分，完成以下步驟：**圖21:連線別名**



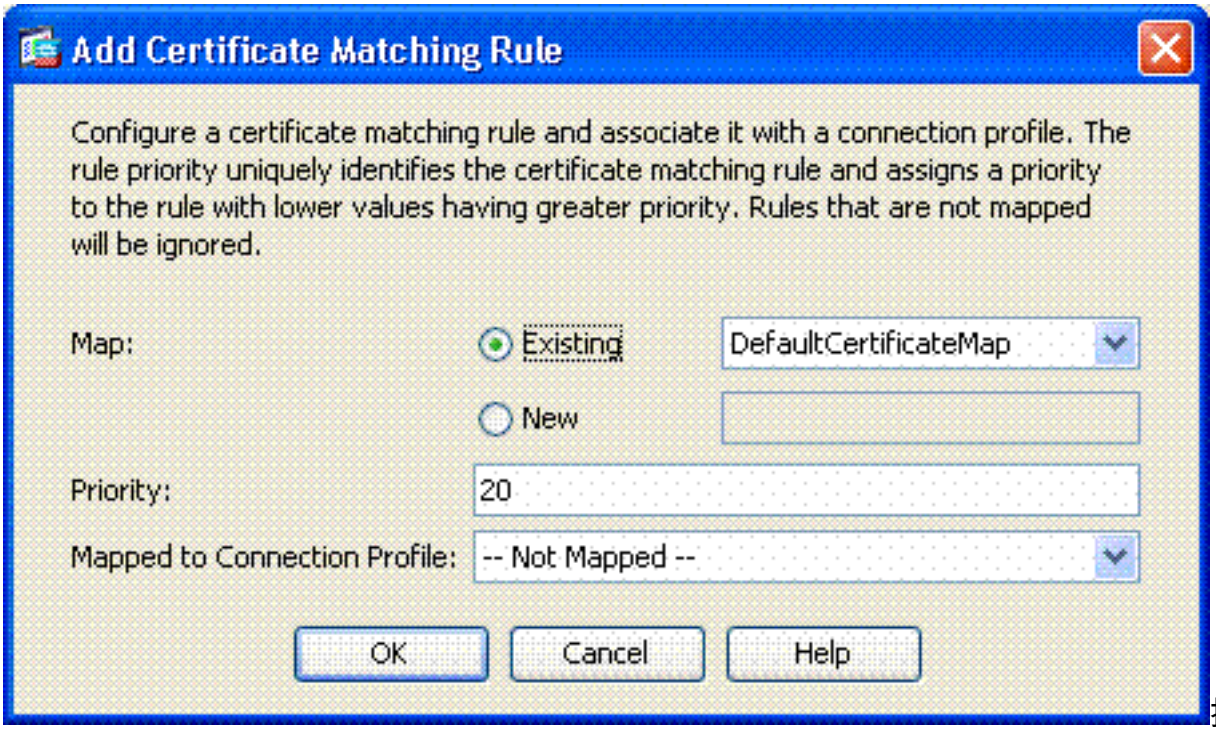
選擇**Add**。輸入要使用的組別名。確保選中**Enabled**。請參見圖21。

13. 按一下「**OK**」（確定）。

註：按一下**Save將配置儲存在快閃記憶體中。**

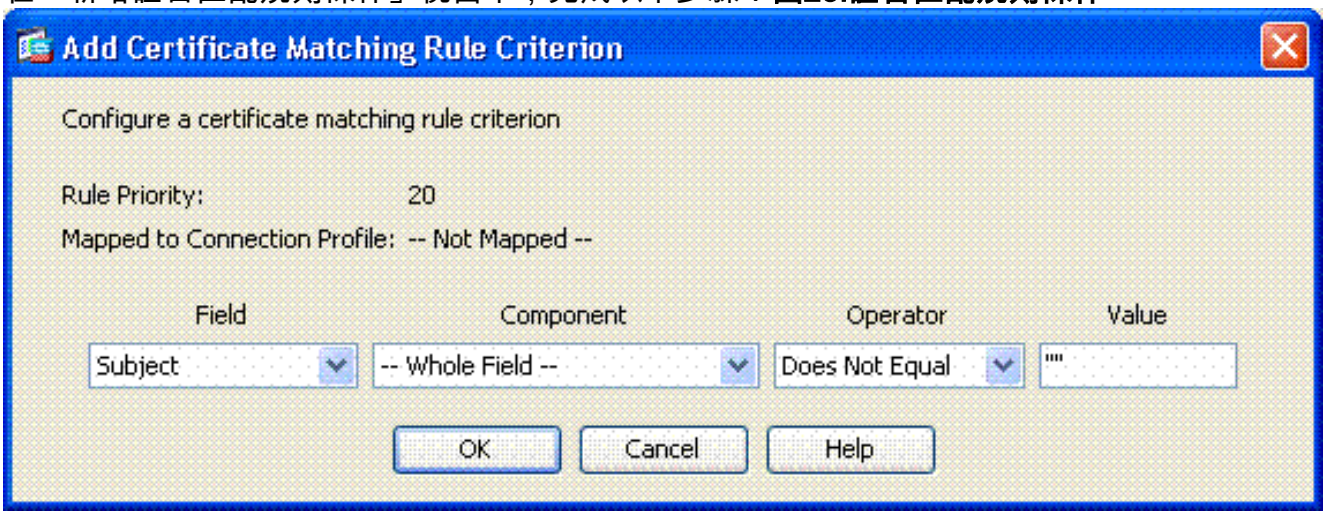
證書匹配規則（如果使用OCSP）

1. 選擇**Remote Access VPN > Advanced > Certificate to SSL VPN Connection Profile Maps**。請參見圖22。在Certificate to Connection Profile Maps部分中選擇**Add**。您可以在對映部分中將現有對映保留為DefaultCertificateMap，或者建立一個新對映（如果已經將證書對映用於IPsec）。保持規則優先順序。在對映組下，保留為**— Not Mapped —**。請參見圖22。**圖22:新增證書匹配規則**



按一下「**OK**」（確定）。

2. 按一下底部表上的**Add**。
3. 在「新增證書匹配規則條件」視窗中，完成以下步驟：**圖23:證書匹配規則條件**



將Field列保留為**Subject**。將「元件」列保留為**整個欄位**。將「運算子」列更改為**「不等於」**。在「值」列中，輸入兩個雙引號**「」**。按一下「**Ok**」和「**Apply**」。例如，請參見圖23。

配置OCSP

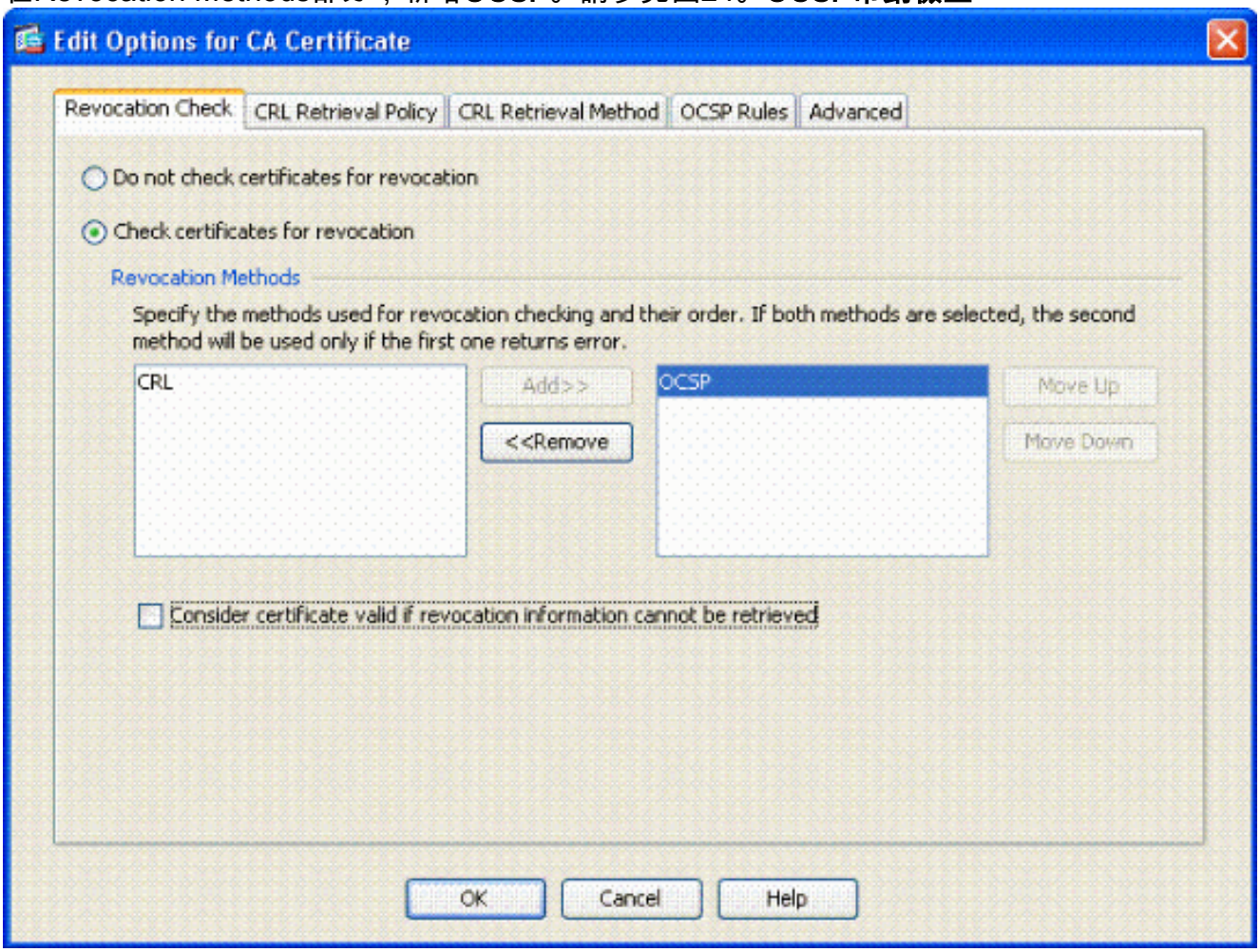
OCSP的配置可能有所不同，取決於OCSP響應方供應商。有關詳細資訊，請閱讀供應商手冊。

配置OCSP響應方證書

1. 從OCSP響應程式獲取自行生成的證書。
2. 完成前面提到的步驟，並安裝OSCP伺服器的證書。**注意：**確保**為OCSP證書信任點選**擇了「不檢查吊銷證書」。

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**檢查吊銷的**證書。
5. 在Revocation Methods部分，新增**OCSP**。請參見圖24。**OCSP吊銷檢查**



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**。

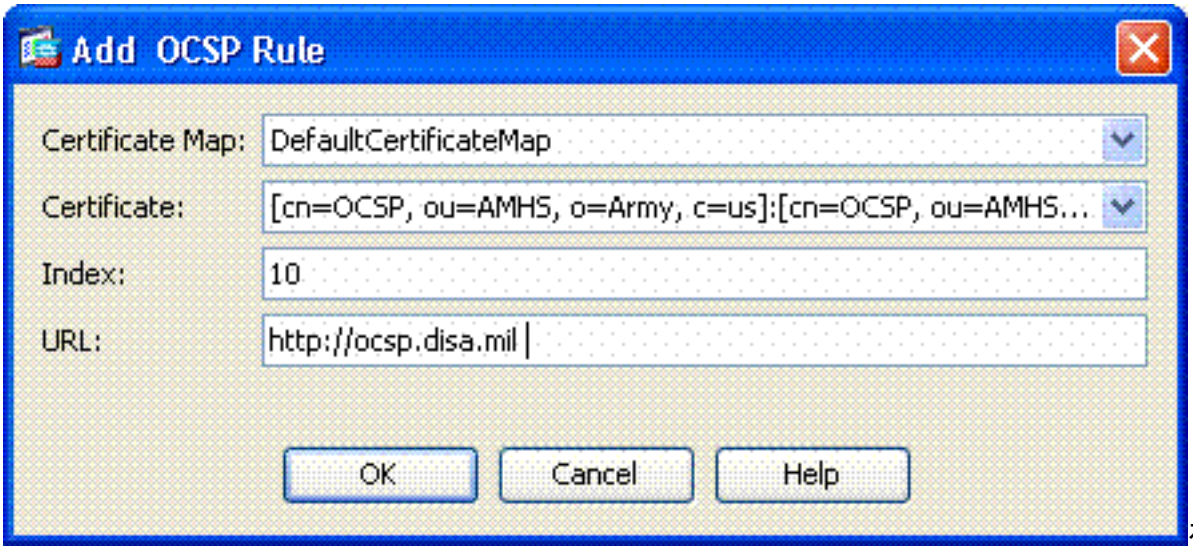
注意：配置/編輯使用OCSP進行吊銷的所有CA伺服器。

配置OCSP規則

注意：完成這些步驟之前，請確認已建立證書組匹配策略並配置了OCSP響應程式。

附註： 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. 在新增OCSP規則視窗中，完成以下步驟。請參見圖25。**圖25:新增OCSP規則**



在「證書對映」選項中，選擇**DefaultCertificateMap**或以前建立的對映。在Certificate選項中，選擇**OCSP responder**。在索引選項中，輸入**10**。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。按一下「**OK**」（確定）。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 — 主機PC中已安裝Cisco AnyConnect VPN客戶端和中介軟體應用程式。已測試ActivCard Gold和ActivClient。

注意：本指南僅對初始AC客戶端安裝使用group-url方法。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。

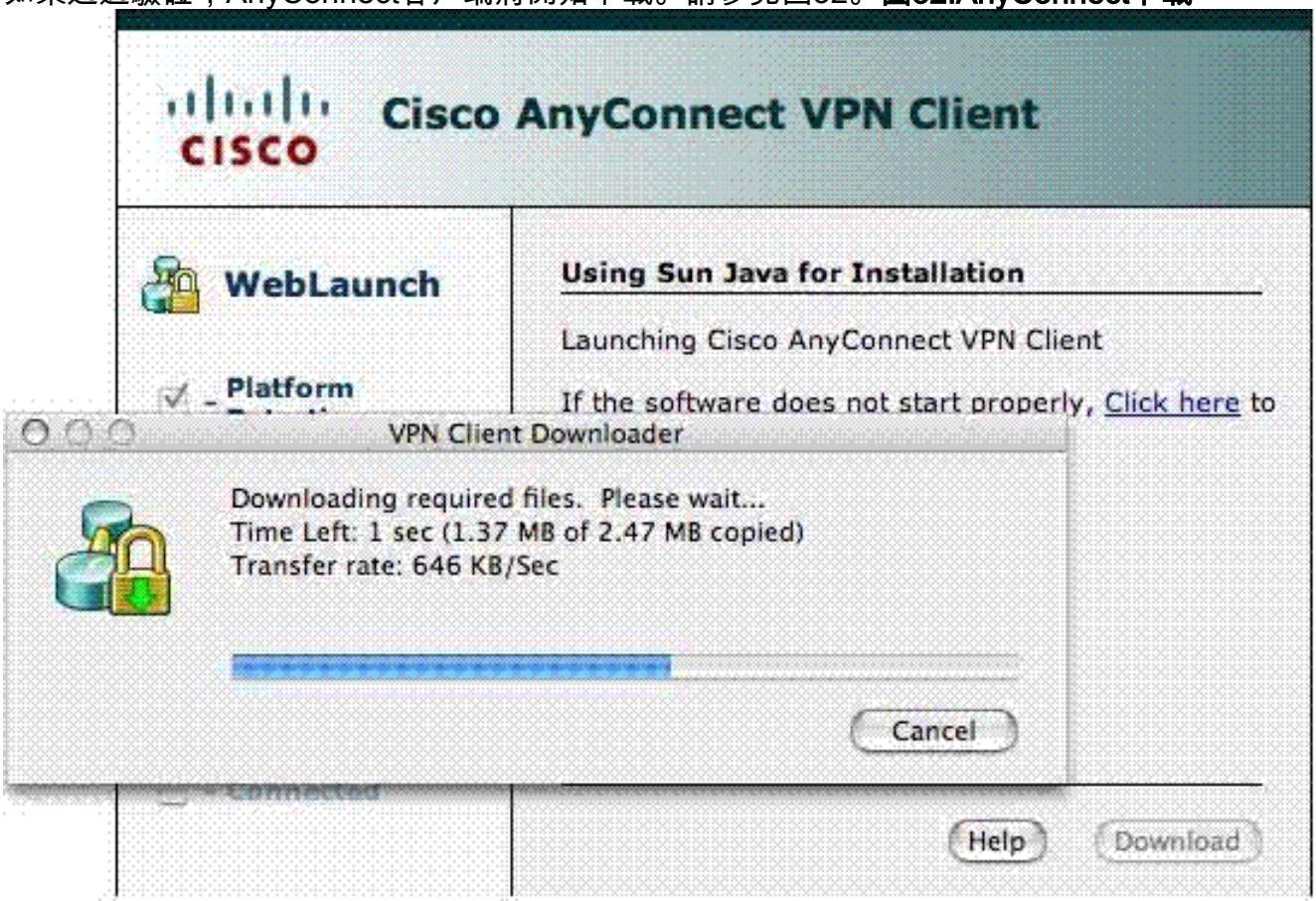
注意：需要在本地電腦上安裝DoD證書鏈。檢查PKI POC以獲取證書/批處理檔案。

注意：MAC OSX的讀卡器驅動程式已經安裝，並且與您使用的當前作業系統版本相容。

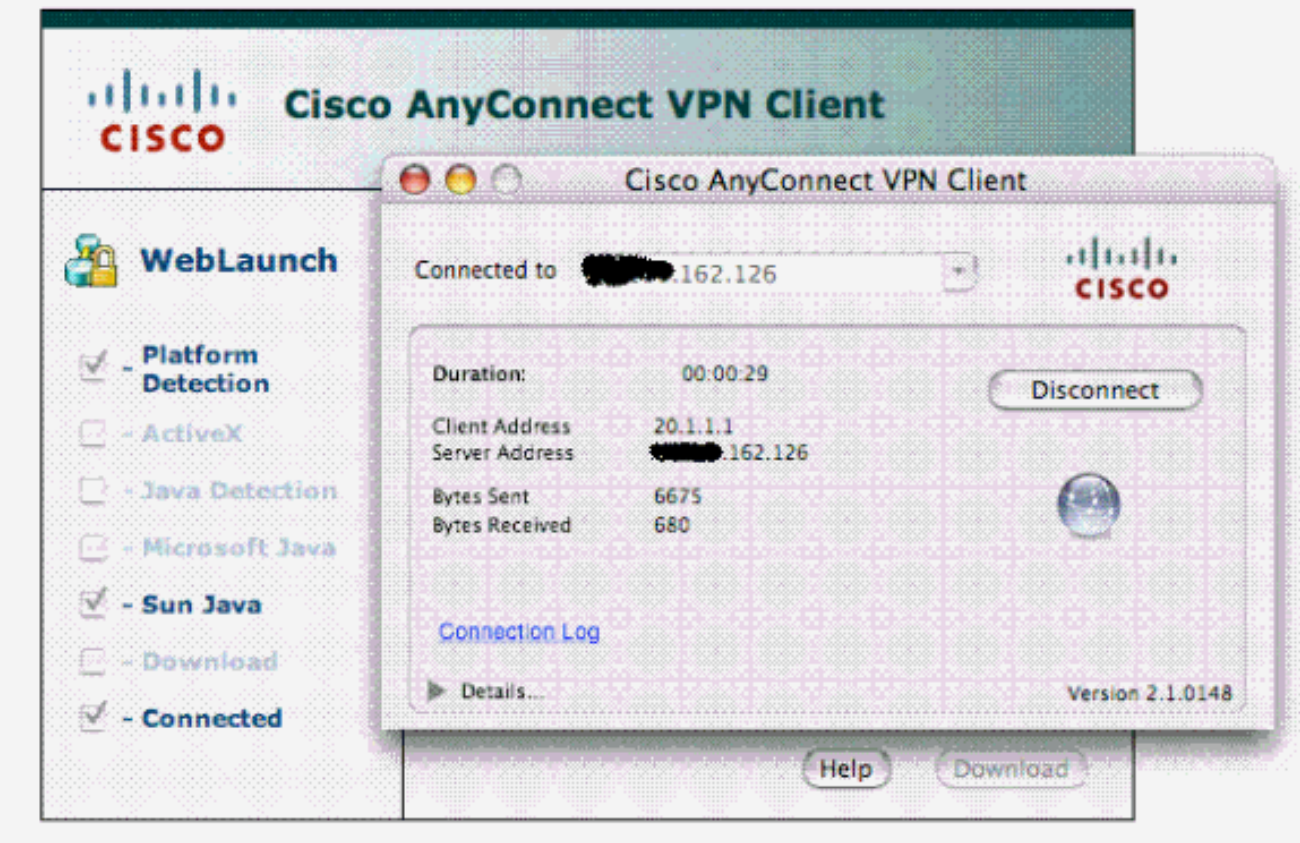
下載Cisco Anyconnect VPN客戶端 — Mac OS X

1. 通過Safari啟動與ASA的Web會話。地址格式應為https://Outside-Interface。例如，https://172.18.120.225。
2. 彈出視窗要求驗證ASA的證書。按一下「**Continue**」（繼續）。
3. 出現另一個彈出視窗以解鎖CAC金鑰鏈。輸入您的PIN碼。請參見圖31。**圖31:輸入PIN**

4. 出現SSL VPN服務網頁後，按一下**Continue**。
5. 解鎖金鑰鏈後，如果信任來自ASA的證書，瀏覽器會提示您進行提示。按一下「**trust**」。
6. 輸入根密碼以解鎖金鑰鏈以建立安全連線，然後按一下**確定**。
7. 選擇要用於客戶端身份驗證的證書，然後按一下**Ok**。
8. 然後，瀏覽器會要求根/使用者密碼，以允許下載AnyConnect客戶端。
9. 如果通過驗證，AnyConnect客戶端將開始下載。請參見圖32。**圖32:AnyConnect下載**



10. 下載應用程式後，瀏覽器會提示您接受ASA證書。按一下「**Accept**」。
11. 已建立連線。圖33.**圖33:AnyConnect已連線**



啟動Cisco AnyConnect VPN客戶端 — Mac OS X

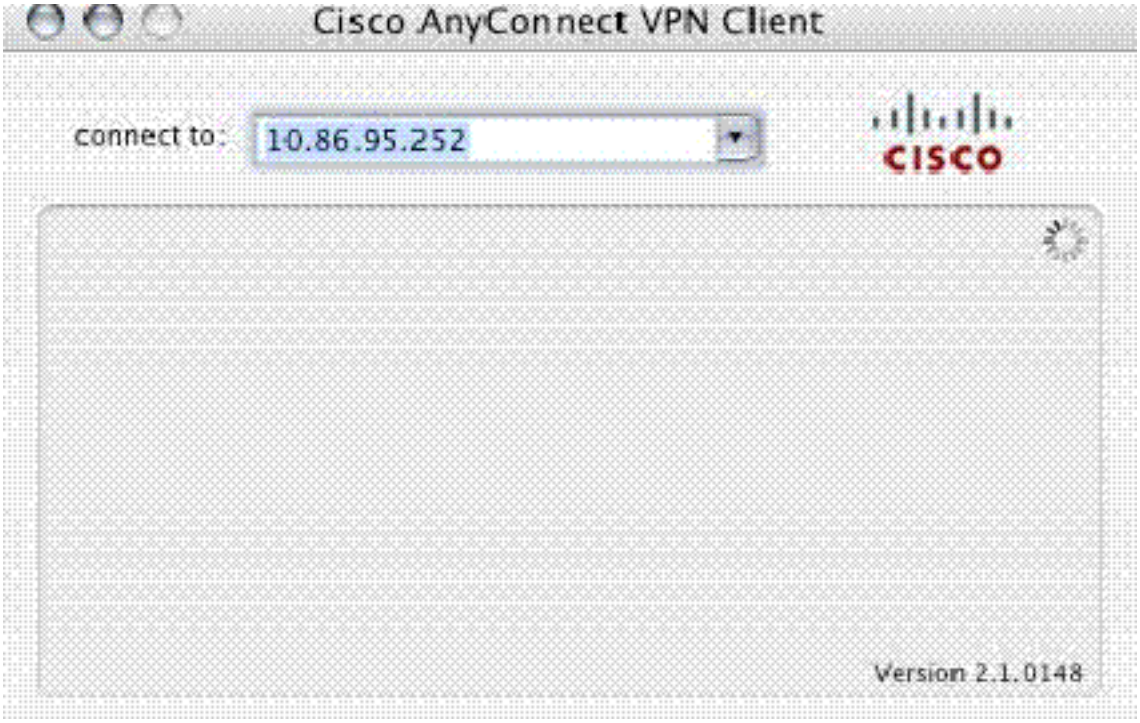
從Finder — 應用**> Cisco AnyConnect VPN客戶端**

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

出現AC視窗。請參見圖37。

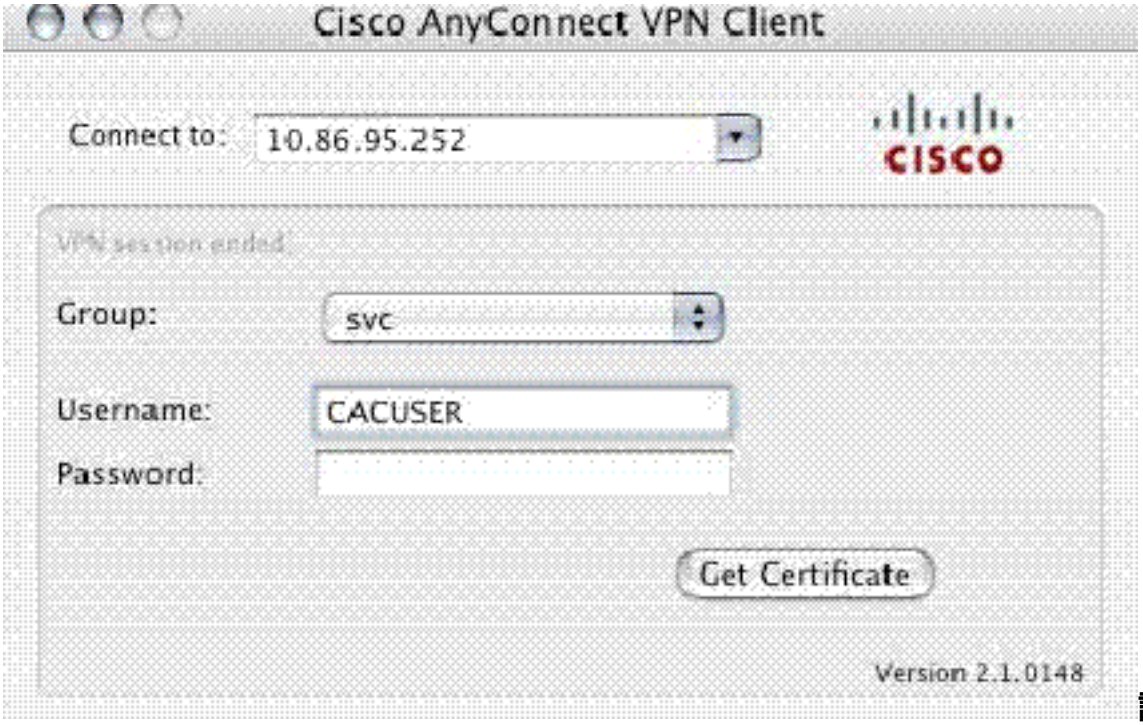
圖37:新建VPN連線



1. 如果AC沒有自動嘗試連線，請選擇相應的主機。
2. 出現提示時輸入您的PIN。請參見圖38。**圖38:輸入PIN**

啟動遠端訪問

1. 選擇要連線的組和主機。
2. 由於使用證書，請選擇Connect以建立VPN。請參見圖39。**注意**：由於連線使用證書，因此無需輸入使用者名稱和密碼。**圖39:正在連線**



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，這可以支援對遠端訪問連線執行其他策略。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伺服器中進行更改。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。

案例 1:使用遠端訪問許可權撥入的Active Directory實施 — 允許/拒絕訪問

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

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

對於ALLOW條件，對映：

- 真= 20

對於DENY撥入條件，請對映：

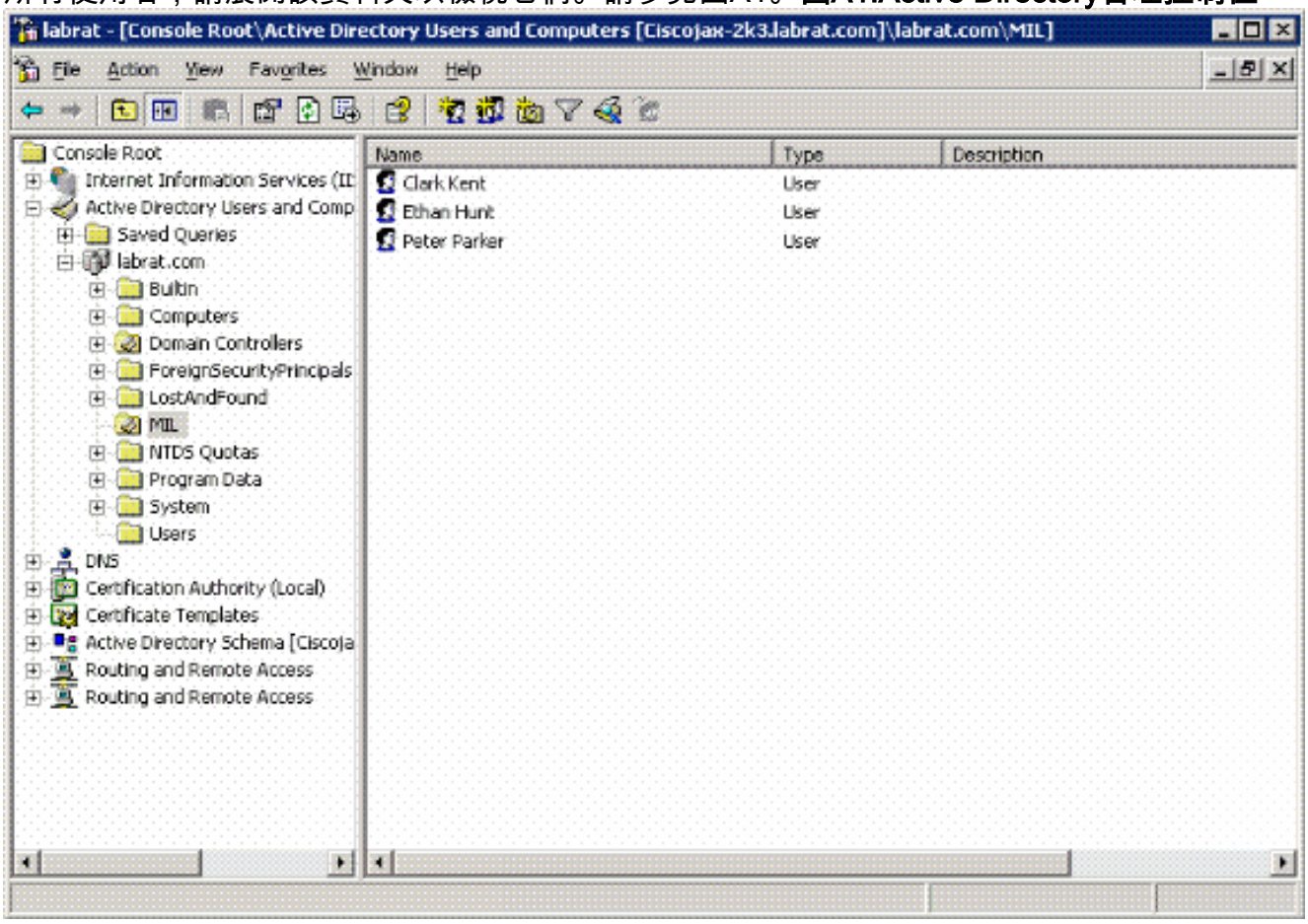
- FALSE = 1

注意：確保TRUE和FALSE在所有大寫字母中。有關詳細資訊，請參閱為安全裝置使用者授權配置外部伺服器。

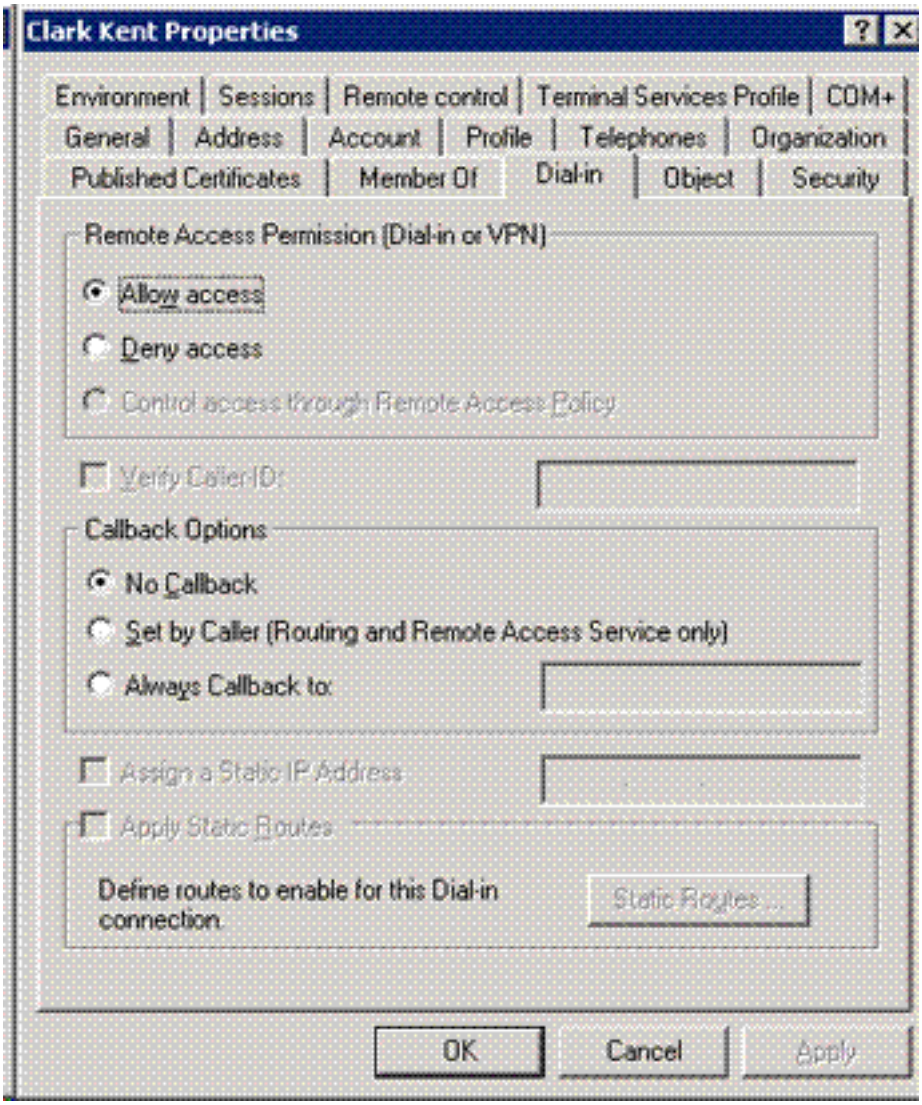
Active Directory安裝程式

1. 在Active Directory伺服器中，按一下**開始>運行**。
2. 在「開啟」文本框中，鍵入**dsa.msc**，然後按一下**確定**。這將啟動Active Directory管理控制檯。
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. 如果您為使用者建立了OU，請展開OU以檢視所有使用者；如果在「使用者」資料夾中分配了所有使用者，請展開該資料夾以檢視它們。請參見圖A1。**圖A1:Active Directory管理控制檯**



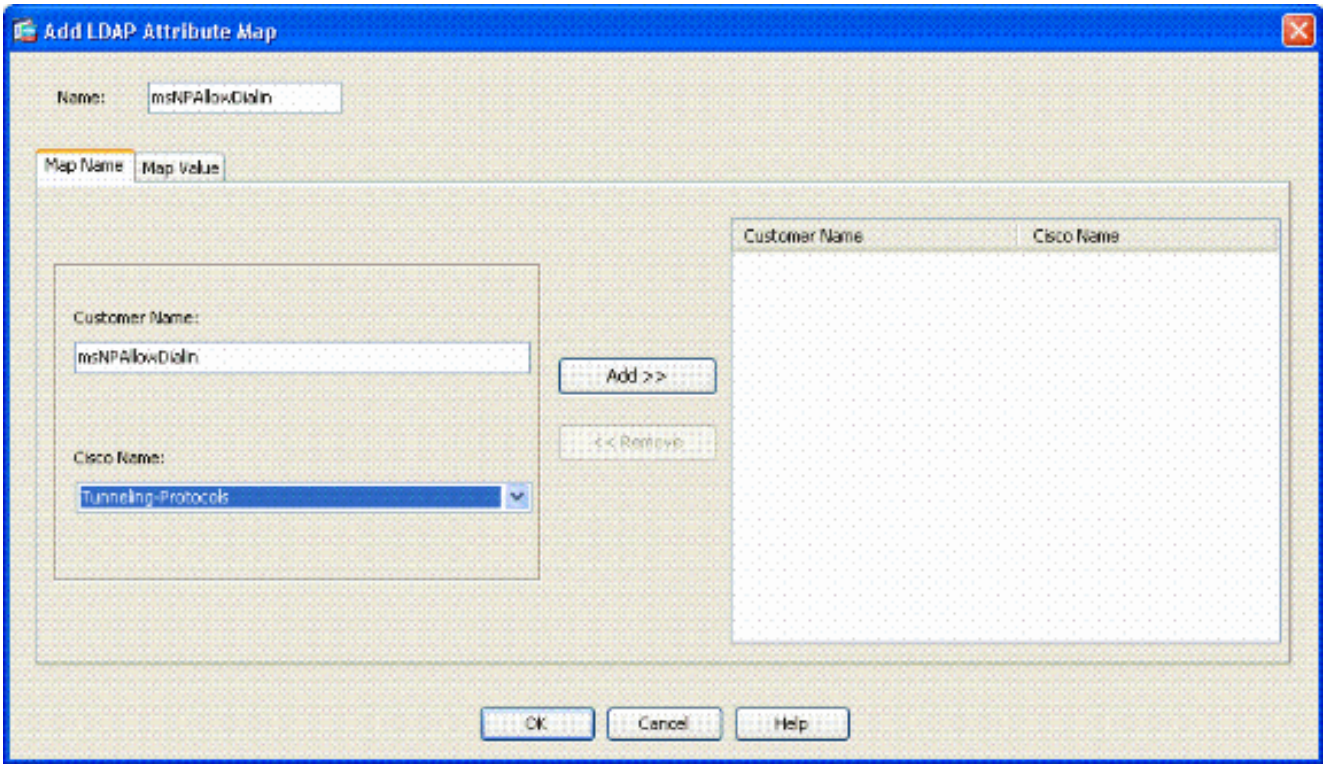
6. 按兩下要編輯的使用者。按一下使用者屬性頁中的「撥入」頁籤，然後按一下**allow**或**deny**。請參見圖A2。**圖A2:使用者屬性**



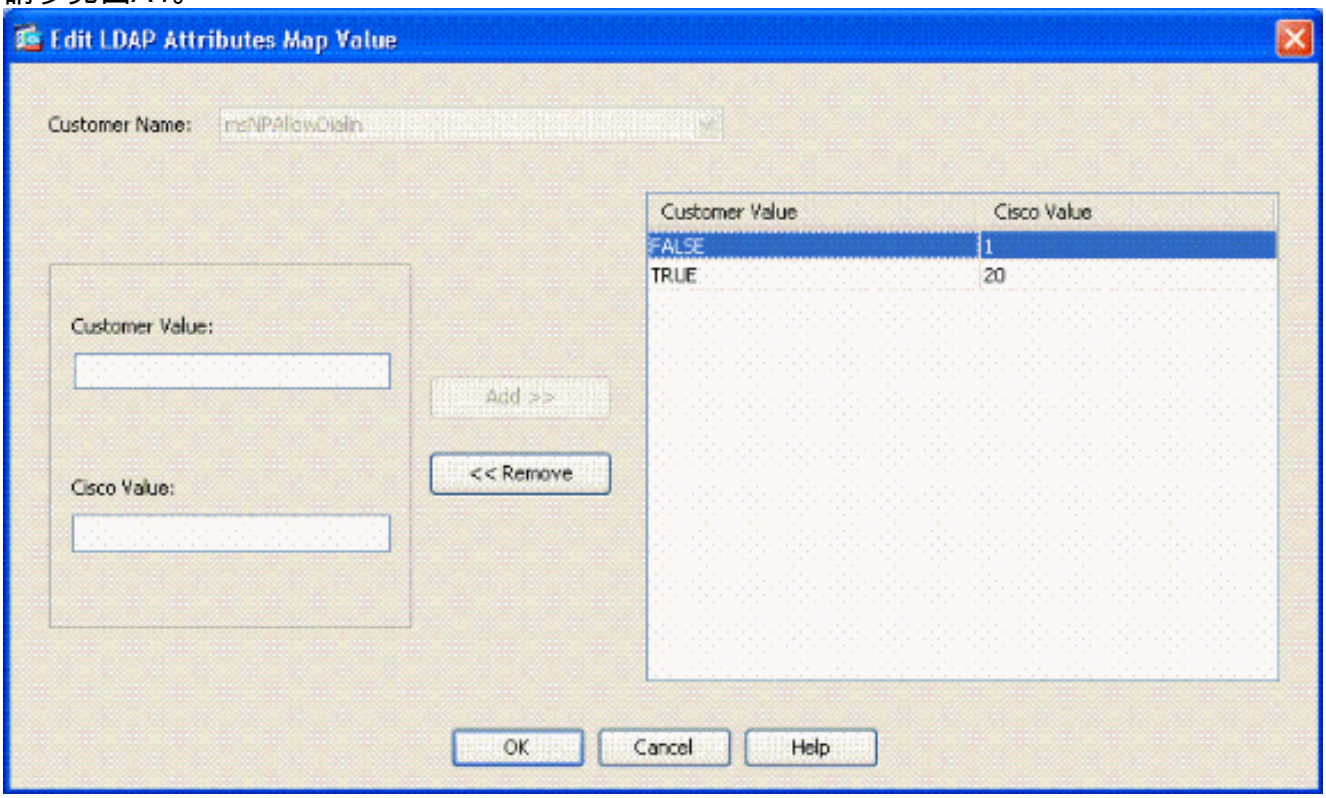
7. 然後按一下「**Ok**」。

ASA配置

1. 在ASDM中，選擇**Remote Access VPN> AAA Setup > LDAP Attribute Map**。
2. 按一下「**Add**」。
3. 在「新增LDAP屬性對映」視窗中，完成以下步驟。請參見圖A3。**圖A3:新增LDAP屬性對映**

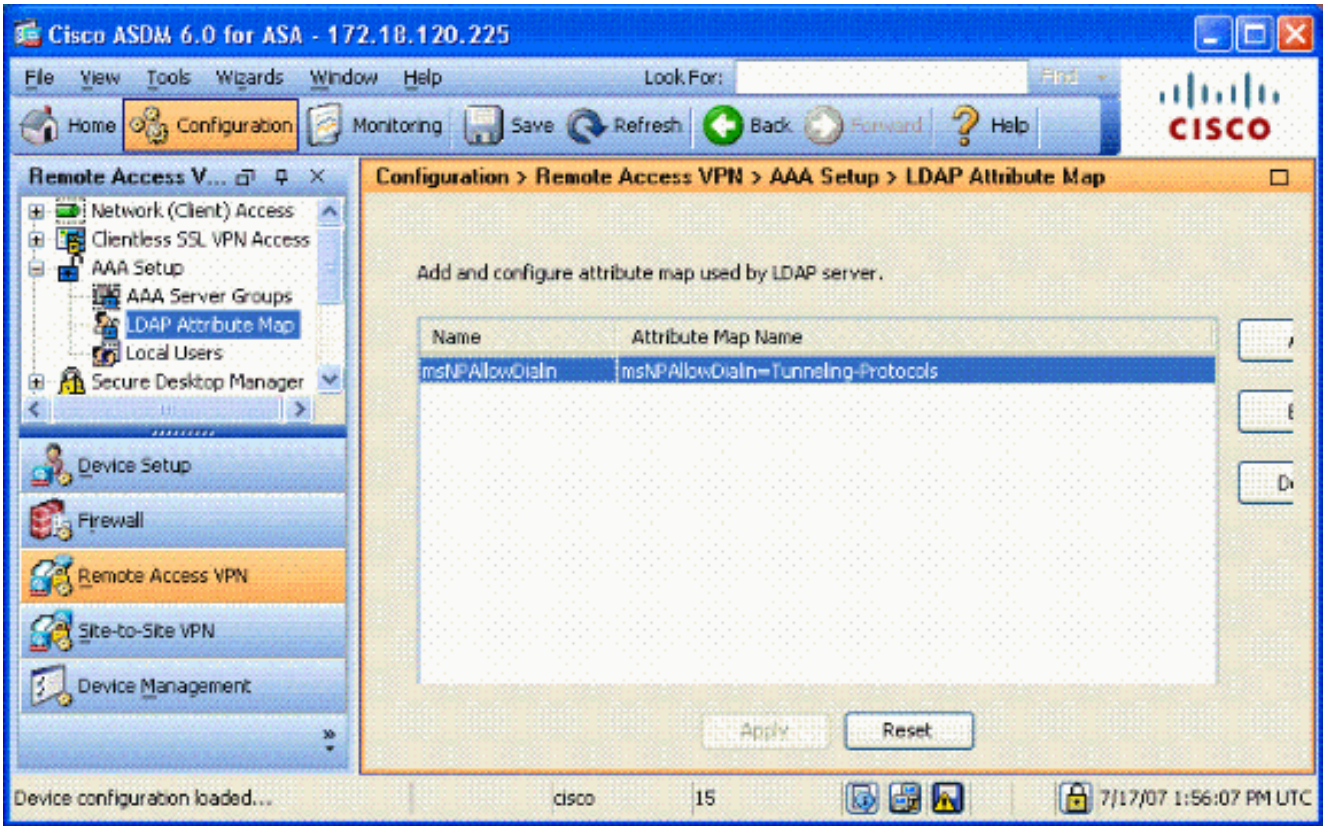


在「名稱」文本框中輸入名稱。在「對映名稱」頁籤的「客戶名稱」文本框中鍵入**msNPAllowDialin**。在Map Name頁籤中，在Cisco Name的下拉選項中選擇**Tunneling-Protocols**。按一下「**Add**」。選擇**對映值**頁籤。按一下「**Add**」。在Add Attribute LDAP Map Value視窗中，在Customer Name文本框中鍵入**TRUE**，然後在Cisco Value文本框中鍵入**20**。按一下「**Add**」。在「客戶名稱」文本框中鍵入**FALSE**，然後在「思科值」文本框中鍵入**1**。請參見圖A4。

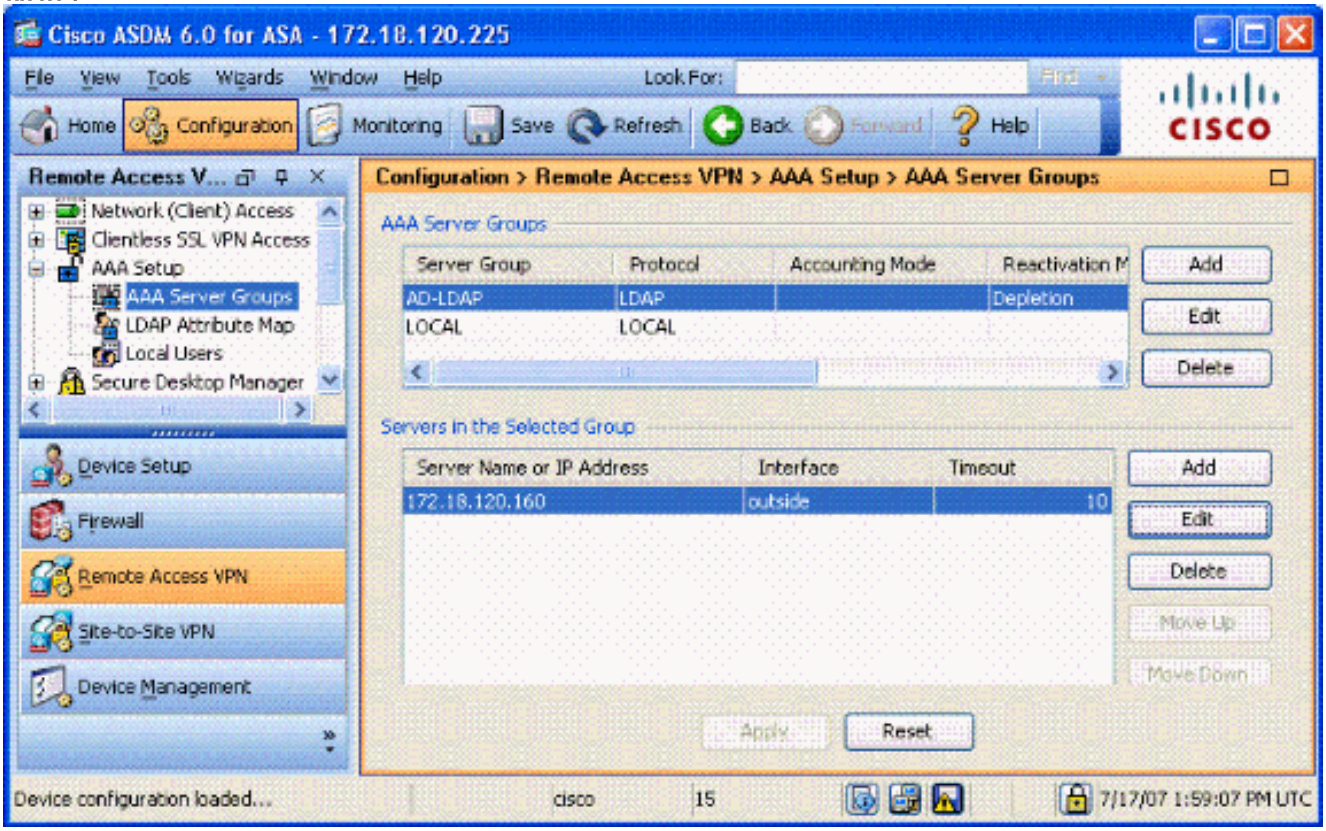


按一下「**OK**」（確定）。按一下「**OK**」（確定）。按一下「**Apply**」。配置應類似於圖A5。

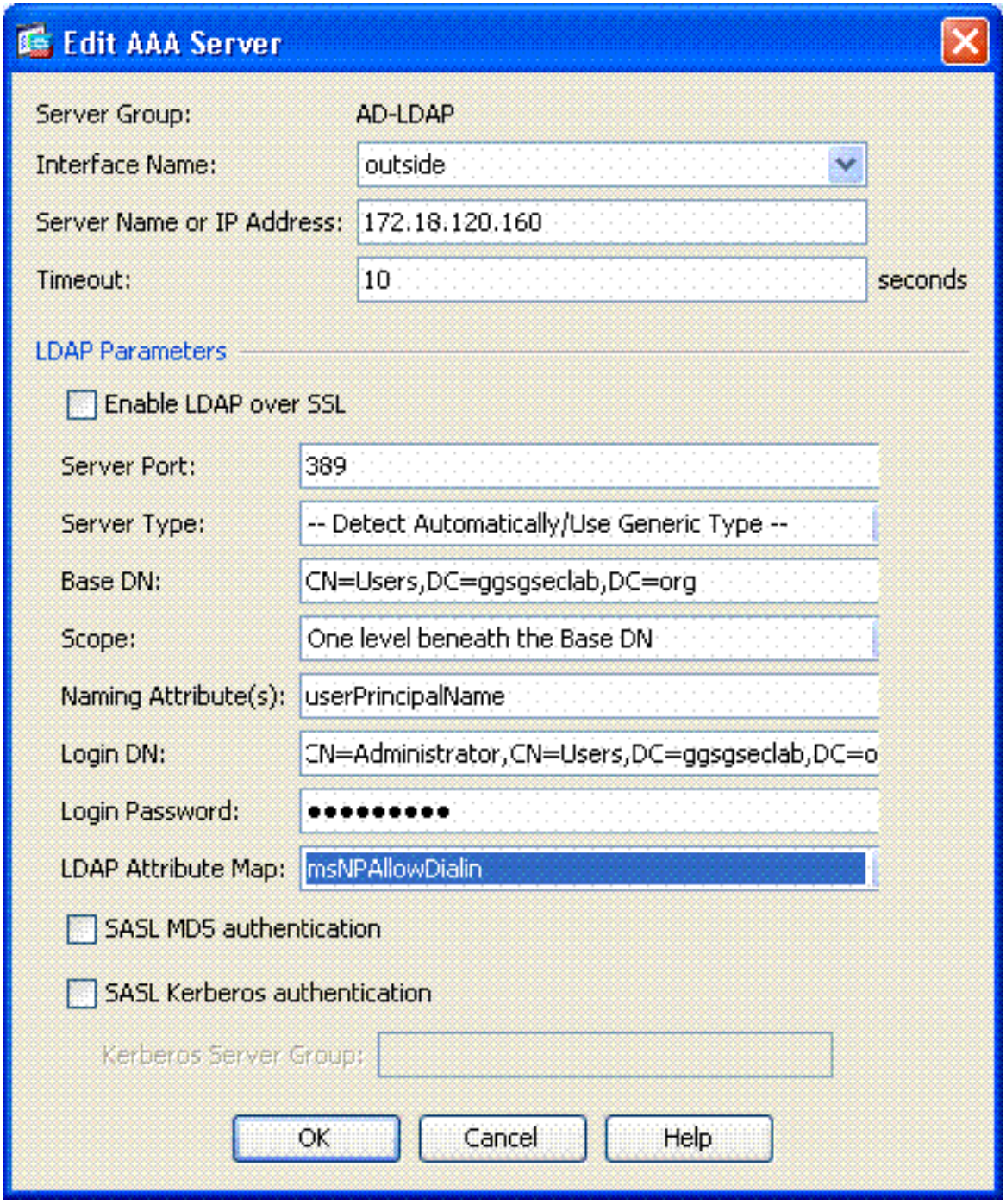
圖A5:LDAP屬性對映配置



4. 選擇**Remote Access VPN> AAA Setup > AAA Server Groups**。請參見圖A6。**圖A6:AAA伺服器群組**



5. 按一下要編輯的伺服器組。在Servers in the Selected Group部分，選擇伺服器IP地址或主機名，然後按一下**Edit**。
6. 在「編輯AAA伺服器」視窗的「LDAP屬性對映」文本框中，選擇下拉選單中建立的LDAP屬性對映。請參見圖A7**圖A7:新增LDAP屬性對映**



7. 按一下「**OK**」（確定）。

注意：在測試時開啟LDAP調試，以驗證LDAP繫結和屬性對映是否正常工作。如需指令疑難排解，請參閱附錄C。

案例 2:使用組成員身份允許/拒絕訪問的Active Directory實施

此示例使用LDAP屬性memberOf對映到隧道協定屬性，以便建立組成員資格作為條件。要使此策略起作用，必須具備以下條件：

- 使用已經存在的組或為ALLOW條件的ASA VPN使用者建立新組。
- 使用已經存在的組或為非ASA使用者建立一個新組以成為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，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。確保建立的新組位於清單頂部。另一種方法是在名稱前面加上特殊字元，因為AD首先檢視特殊字元。為了解決此問題，請

使用8.x軟體中的DAP檢視多個組。

注意：確保使用者是拒絕組的一部分或至少是另一個組的一部分，以便始終將memberOf傳送回ASA。您不必指定FALSE拒絕條件，但最佳實踐是這樣做。如果現有組名或組名包含空格，請按照以下方式輸入屬性：

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

注意：DAP允許ASA在memberOf屬性中檢視多個組，並對這些組進行基本授權。參見DAP部分。

對映

- AD屬性值：memberOf CN=ASAUsers，CN=Users，DC=ggsgseclab，DC=orgmemberOf CN=TelnetClients，CN=Users，DC=labrat，DC=com
- 思科屬性值：1 = FALSE， 20 = TRUE，

對於**ALLOW**條件，請對映：

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

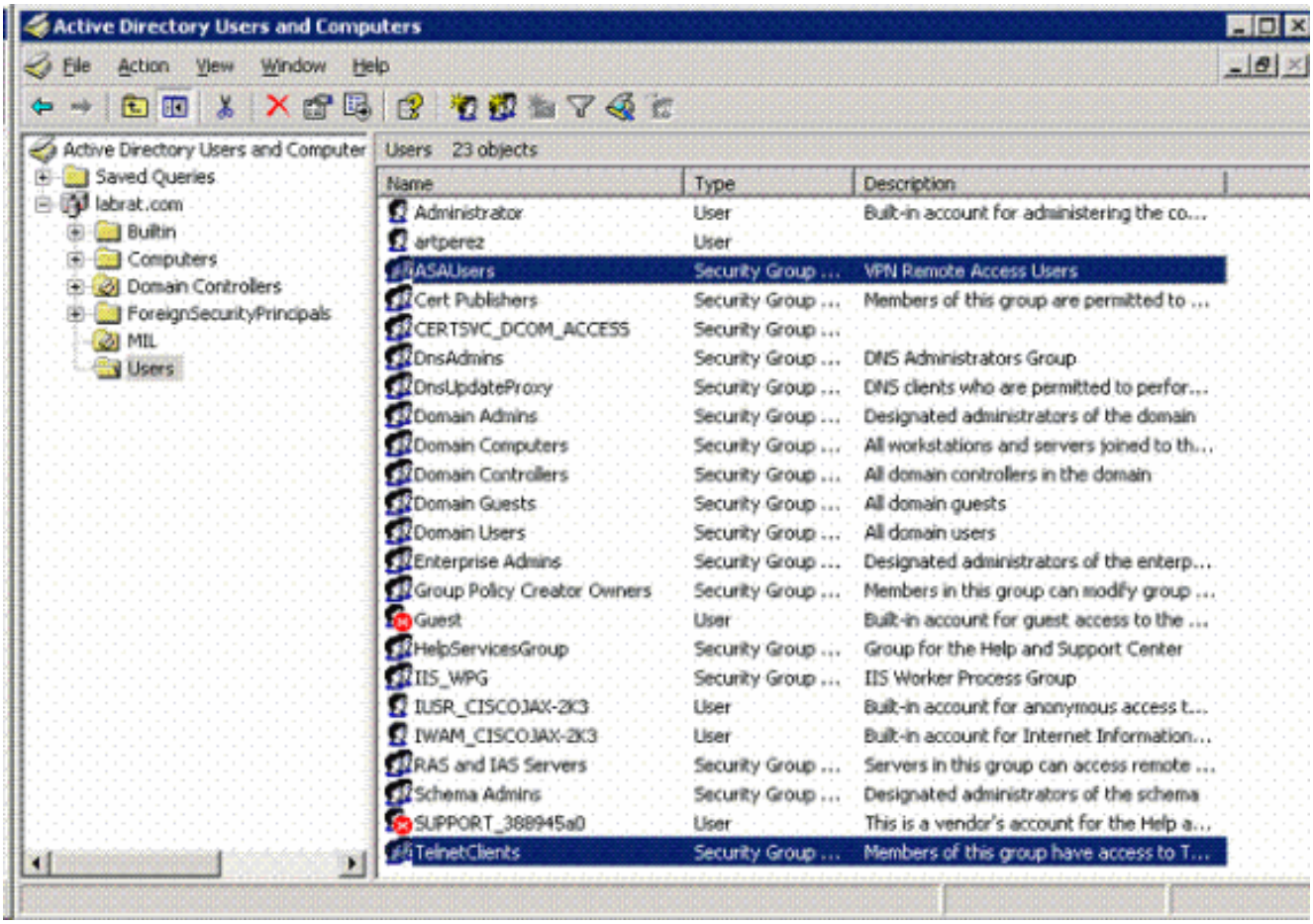
對於**DENY**條件，請對映：

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

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

Active Directory安裝程式

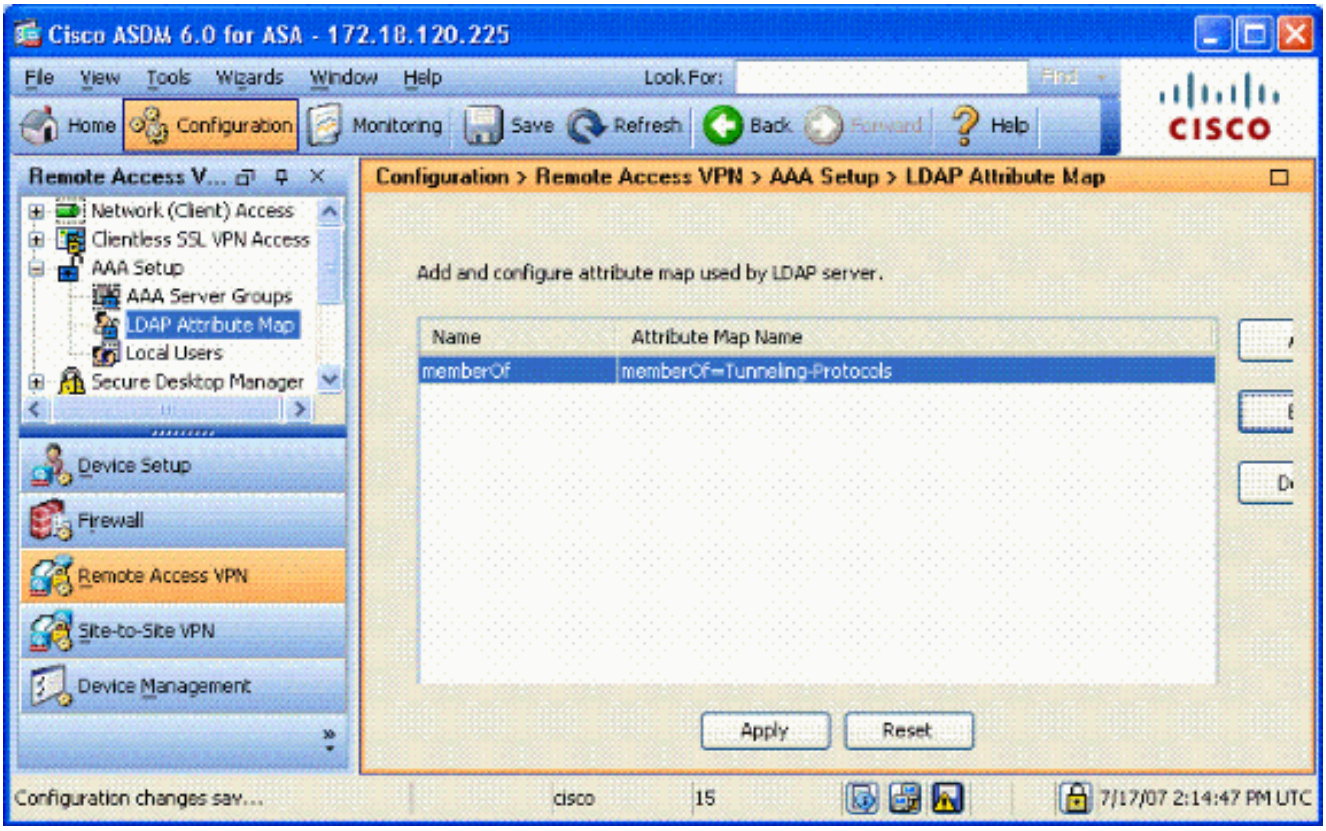
1. 在Active Directory伺服器中，選擇**開始>運行**。
2. 在「開啟」文本框中，鍵入**dsa.msc**，然後按一下**確定**。這將啟動Active Directory管理控制檯。
3. 在Active Directory管理控制檯中，按一下加號以展開Active Directory使用者和電腦。請參見圖A8**圖A8:Active Directory組**



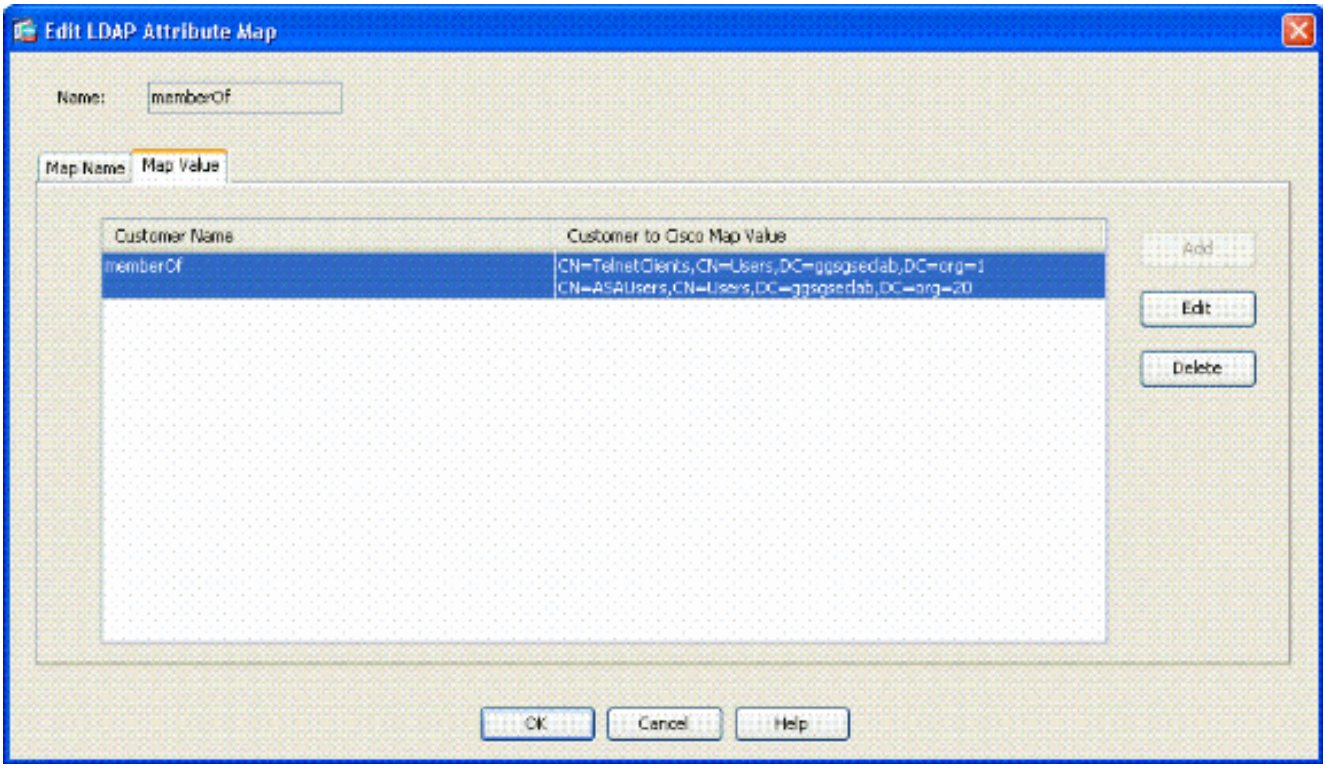
4. 按一下加號以展開域名。
5. 按一下右鍵**Users**資料夾，然後選擇**New > Group**。
6. 輸入組名稱。例如：ASAUsers。
7. 按一下「**OK**」（確定）。
8. 按一下**Users**資料夾，然後按兩下剛建立的組。
9. 選擇**Members**頁籤，然後按一下**Add**。
10. 鍵入要新增的使用者的名稱，然後按一下**Ok**。

ASA配置

1. 在ASDM中，選擇**Remote Access VPN > AAA Setup > LDAP Attribute Map**。
2. 按一下「**Add**」。
3. 在「新增LDAP屬性對映」視窗中，完成以下步驟。請參見圖A3。在「名稱」文本框中輸入名稱。在對映名稱頁籤中，在**客戶**名稱文本框c中鍵入memberOf。在Map Name頁籤中，在Cisco Name的下拉選項中選擇**Tunneling-Protocols**。選擇**Add**。按一下**對映值**頁籤。選擇**Add**。在「新增屬性LDAP對映值」視窗中，在「客戶名稱」文本框中鍵入**CN=ASAUsers，CN=Users，DC=ggsgseclab，DC=org**，並在「思科值」文本框中鍵入**20**。按一下「**Add**」。在「客戶名稱」文本框中鍵入**CN=TelnetClients，CN=Users，DC=ggsgseclab，DC=org**，並在「思科值」文本框中鍵入**1**。請參見圖A4。按一下「**OK**」（確定）。按一下「**OK**」（確定）。按一下「**Apply**」。配置應類似於圖A9。**圖A9 LDAP屬性對映**



4. 選擇**Remote Access VPN> AAA Setup > AAA Server Groups**。
5. 按一下要編輯的伺服器組。在Servers in the Selected Group部分，選擇伺服器IP地址或主機名，然後按一下
   Edit



6. 在「編輯AAA伺服器」視窗的「LDAP屬性對映」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：在測試時開啟LDAP調試，以驗證LDAP繫結和屬性對映是否正常工作。如需指令疑難排解，請參閱附錄C。

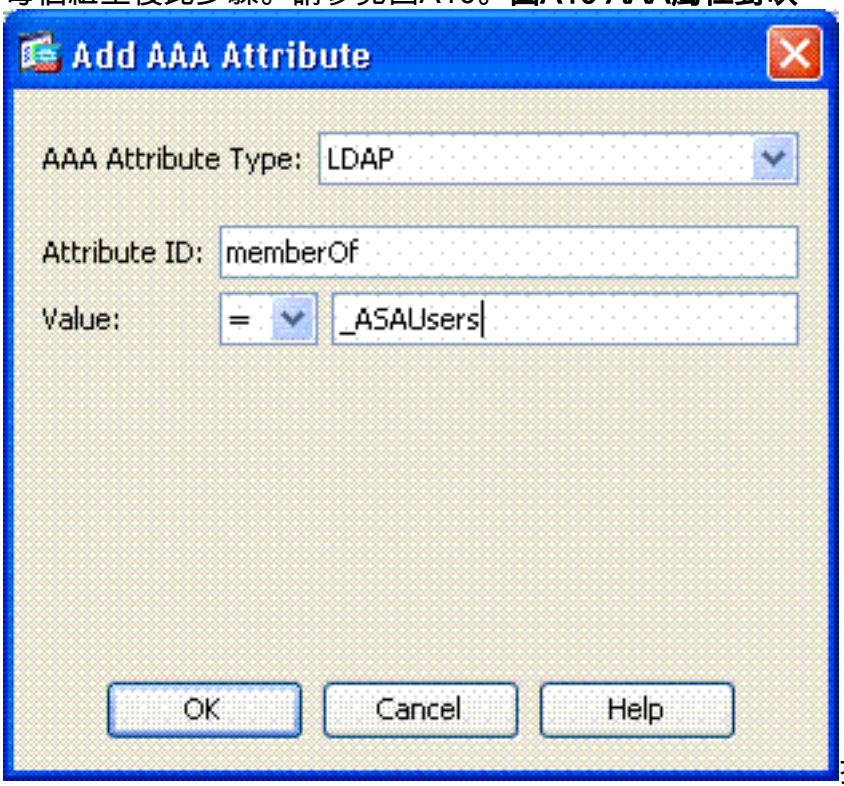
案例 3:多個屬性成員的動態訪問策略

此示例使用DAP檢視多個memberOf屬性，以便允許基於Active Directory組成員資格的訪問。在8.x之前，ASA僅讀取第一個memberOf屬性。在8.x及更高版本中，ASA可以檢視所有memberOf屬性。

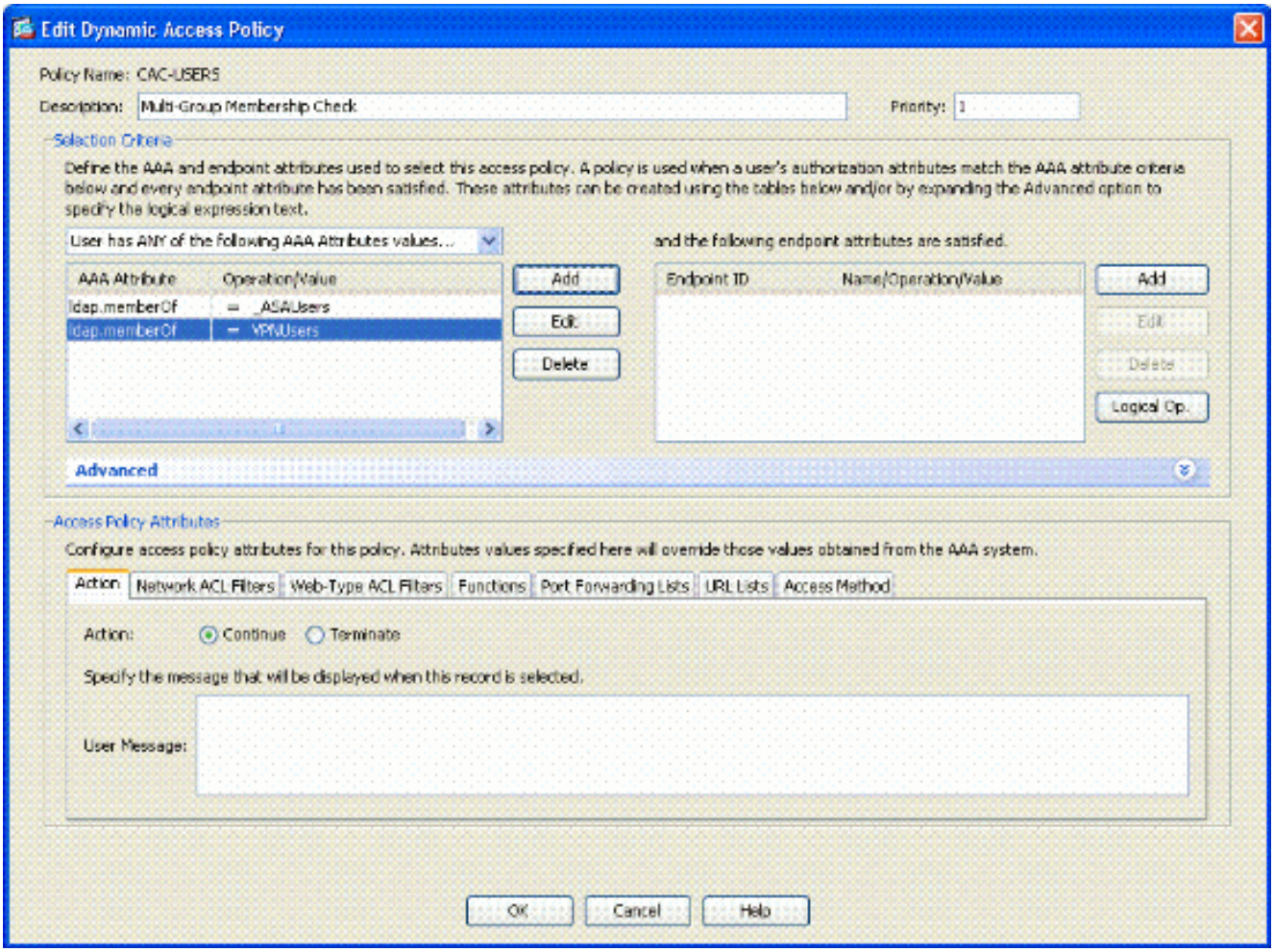
- 使用已經存在的組或為ALLOW條件的ASA VPN使用者建立新組（或多個組）。
- 使用已經存在的組或為非ASA使用者建立一個新組以成為DENY條件的成員。
- 確保在LDAP檢視器中檢查您擁有該組的正確DN。見附錄D。如果DN錯誤，對映無法正常工作。

ASA配置

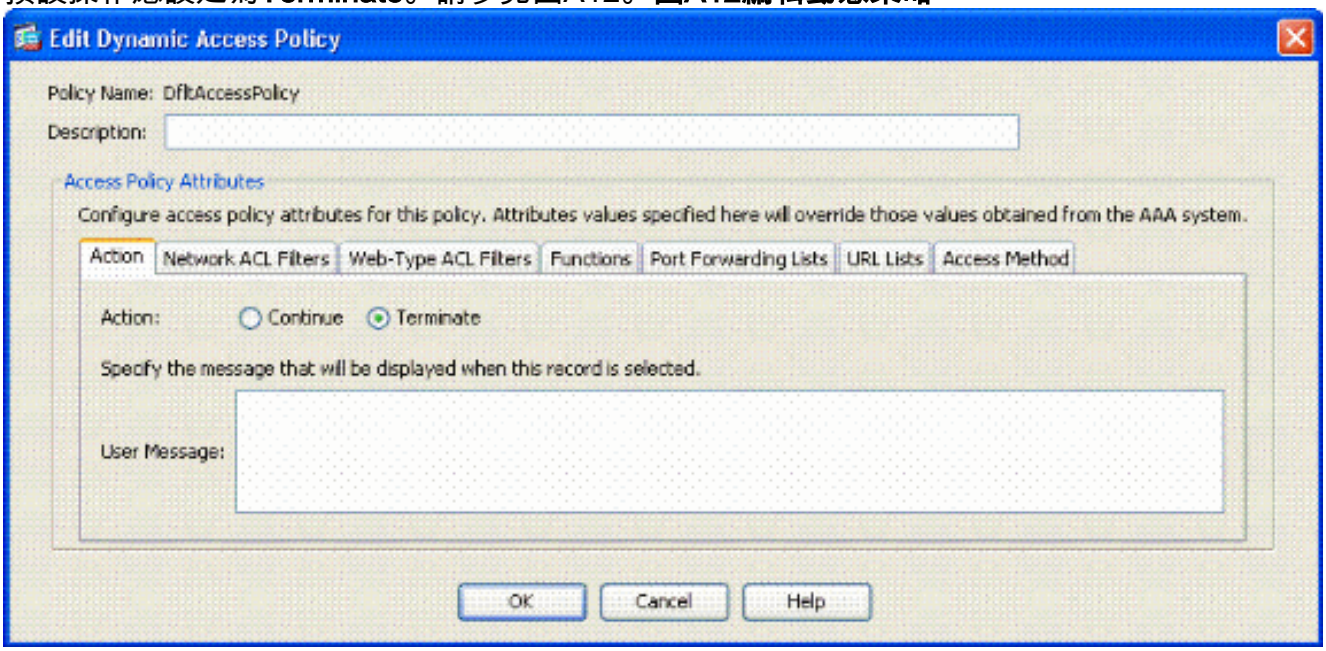
1. 在ASDM中，選擇**Remote Access VPN> Network(Client)Access > Dynamic Access Policies**。
2. 按一下「**Add**」。
3. 在新增動態訪問策略中，完成以下步驟：在「名稱」文本框b中輸入名稱。在「優先順序」部分中，輸入**1**或大於0的數字。在「選擇條件」中，按一下**新增**。在Add AAA Attribute中，選擇**LDAP**。在屬性ID部分中，輸入**memberOf**。在值部分，選擇**=**並輸入AD組名稱。對要引用的每個組重複此步驟。請參見圖A10。**圖A10 AAA屬性對映**



按一下「**OK**」（確定）。在Access Policy Attributes部分，選擇**Continue**。請參見圖A11。**圖A11新增動態策略**



4. 在ASDM中，選擇**Remote Access VPN> Network(Client)Access > Dynamic Access Policies**。
5. 選擇**Default Access Policy**，然後選擇**Edit**。
6. 預設操作應設定為**Terminate**。請參見圖A12。**圖A12編輯動態策略**



7. 按一下「**OK**」（確定）。

註：如果未選擇**Terminate**，則即使您不在任何組中，您仍可以加入，因為預設值為**Continue**。

附錄B - ASA CLI配置

ASA 5510

```
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
March 11, 2008 ASA – CAC Authentication for AnyConnect
VPN Access
Company Confidential. A printed copy of this document is
considered uncontrolled.
49
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---------------------
---------------
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-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-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

排除AAA和LDAP故障

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

範例 1：具有正確屬性對映的允許連線

此示例顯示成功連線附錄A所示場景2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#
```

範例 2：允許的Cisco屬性對映配置錯誤的連線

此示例顯示允許連線時與附錄A所示場景2的**debug ldap**和**debug aaa**的輸出。

圖C2:debug LDAP和debug aaa common output — 對映不正確

```
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=or
g
[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函式跟蹤

範例 1：允許與DAP的連線

此示例顯示成功連線附錄A所示的方案3期間**debug dap errors**和**debug dap trace**的輸出。注意多個

memberOf屬性。您可以同時屬於_ASAUsers和VPNUsers或任一個組，這取決於ASA配置。

圖C3:debug DAP

```
#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=or
g
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"]["physicalDeliveryOfficeN
```

```
ame"] =
"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=o
rg";
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.
```

範例 2：拒絕與DAP的連線

此範例顯示與附錄A中顯示的案例3建立未成功連線期間**debug dap errors**和**debug dap trace**的輸出。

圖C4:debug DAP

```
#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=or
g
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"]["physicalDeliveryOfficeN
ame"] =
"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=o
rg";
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
```

證書頒發機構/OCSP故障排除

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

以下示例顯示使用OCSP響應程式成功驗證證書以及失敗的證書組匹配策略。

圖C3顯示了調試輸出，該輸出具有已驗證的證書以及匹配策略的工作證書組。

圖C4顯示配置錯誤的證書組匹配策略的調試輸出。

圖C5顯示具有已撤銷證書的使用者的調試輸出。

圖C5:OCSP調試 — 成功的證書驗證

```
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:失敗的證書組匹配策略的輸出

圖C5:已吊銷證書的輸出

```
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:
```

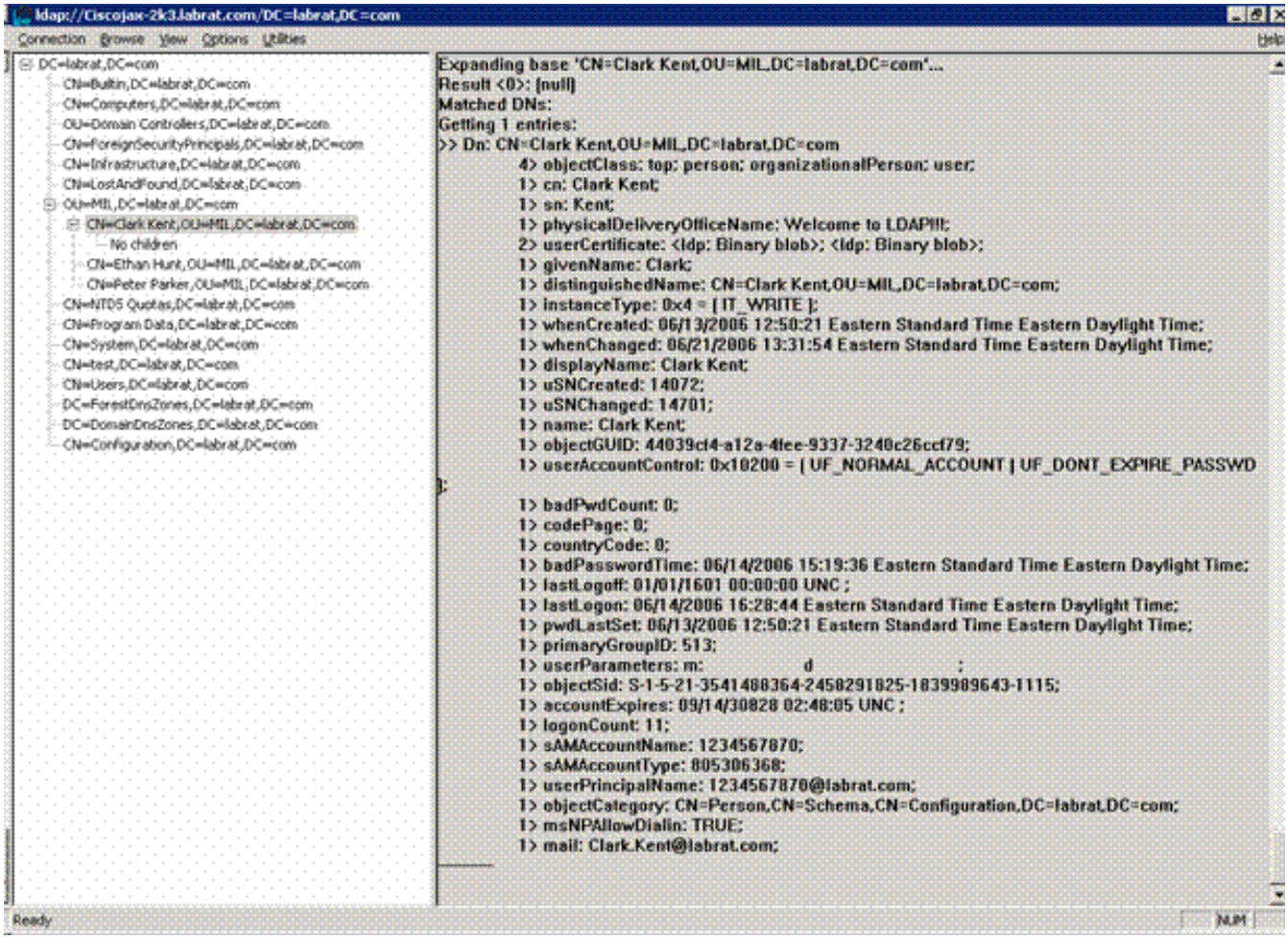
```
= cn=Ethan Hunt,ou=MIL,dc=ggsgseclab,dc=org, map rule:
subject-name
ne "".
CRYPTO_PKI: Peer cert has been authorized by map:
DefaultCertificateMap
sequence: 10.
CRYPTO_PKI: Found OCSP override match. Override URL:
http://ocsp.disa.mil, Override trustpoint: OCSP
CRYPTO_PKI: crypto_pki_get_cert_record_by_subject()
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 — 驗證MS中的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。若要安裝這些工具，請轉到CD中的**Support**目錄，然後按一下**Tools**。安裝**SUPTOOLS.MSI**。

LDAP檢視器

- 安裝後，選擇**Start > Run**。
- 鍵入**ldp**，然後按一下**Ok**。這將啟動LDAP檢視器。
- 選擇**Connection > Connect**。
- 輸入伺服器名稱，然後按一下**Ok**。
- 選擇**Connection > Bind**。
- 輸入使用者名稱和密碼。**注意：您**需要管理員許可權。
- 按一下「**OK**」（確定）。
- 檢視LDAP對象。請參見圖D1。**圖D1:LDAP檢視器**

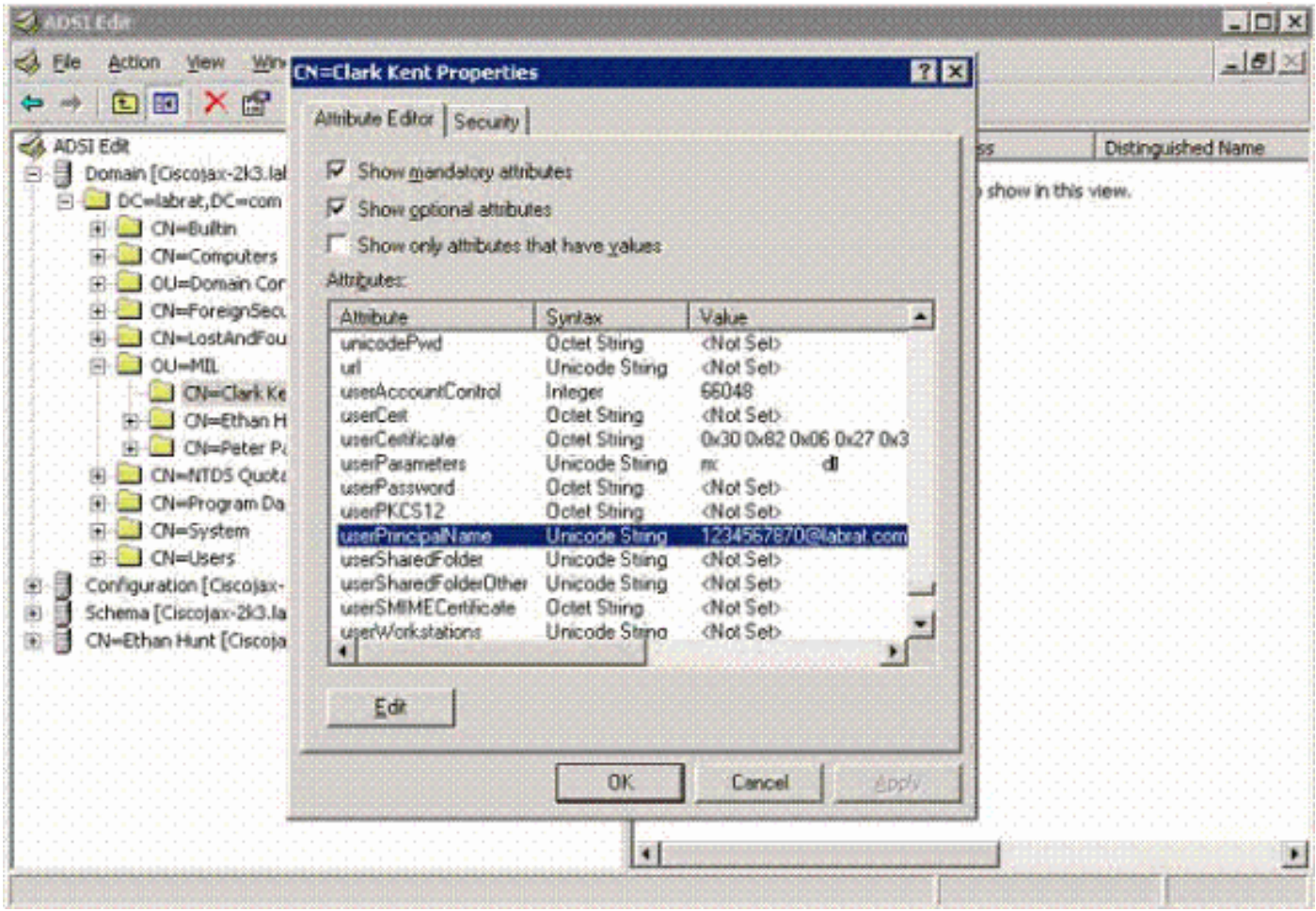


Active Directory服務介面編輯器

- 在Active Directory伺服器中，選擇**「開始」>「運行」**。
- 鍵入**adsiedit.msc**。這將啟動編輯器。
- 按一下右鍵對象，然後按一下**屬性**。

此工具顯示特定對象的所有屬性。請參見圖D2。

圖D2:ADSI編輯



附錄E

可以建立AnyConnect配置檔案並將其新增到工作站。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）。配置檔案儲存為.xml檔案，並可通過記事本進行編輯。檔案可以手動新增到每個客戶端，也可以通過組策略從ASA推送。檔案儲存於：

```
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並使用記事本開啟該檔案。
2. 對檔案（例如頒發者或主機IP）進行適當的修改。例如，請參見圖F1。
3. 完成後，將檔案另存為.xml。

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

有關配置檔案管理，請參閱Cisco AnyConnect文檔。簡言之：

- 個人資料應為貴公司唯一命名。例如：CiscoProfile.xml
- 配置檔名稱應相同，即使公司內各個組的配置檔名稱不同。

此檔案由Secure Gateway管理員維護，然後隨客戶端軟體一起分發。基於此XML的配置檔案可隨時分發到客戶端。支援的分發機制是作為軟體分發的捆綁檔案或者作為自動下載機制的一部分。自動下載機制僅適用於特定思科安全網關產品。

注意：強烈建議管理員使用線上驗證工具或通過ASDM中的配置檔案匯入功能驗證他們建立的XML配置檔案。可通過此目錄中的AnyConnectProfile.xsd完成驗證。AnyConnectProfile是表示

AnyConnect客戶端配置檔案的根元素。

```
xml version="1.0" encoding="UTF-8"
- -



!--- The ClientInitialization section represents global
settings !--- for the client. In some cases, for
example, BackupServerList, host specific !--- overrides
are possible. !-- --> -



!--- The Start Before Logon feature can be used to
activate !--- the VPN as part of the logon sequence. !--
- UserControllable: Does the administrator of this
profile allow the user !--- to control this attribute
for their own use. Any user setting !--- associated with
this attribute is stored elsewhere. -->



!--- This control enables an administrator to have a one
time !--- message displayed prior to a users first
connection attempt. As an !--- example, the message can
be used to remind a user to insert their smart !--- card
into its reader. !--- The message to be used with this
control is localizable and can be !--- found in the
AnyConnect message catalog. !--- (default: "This is a
pre-connect reminder message.")



!-- This section enables the definition of various
attributes !--- that can be used to refine client
certificate selection. --> -



!--- Certificate Distinguished Name matching allows for
exact !--- match criteria in the choosing of acceptable
client !--- certificates. -



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

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

-

相關資訊

- X.509和RFC 3280指定的證書和CRL
- RFC 2560指定的OCSP
- Public Key Infrastructure簡介
- 按標準草案分析的「輕量OCSP」
- 由RFC 2246指定的SSL/TLS
- 技術支援與文件 - Cisco Systems