使用EAP-FAST和LDAP伺服器配置的無線LAN控制器上的本地EAP身份驗證示例

目錄

簡介

本檔案將說明如何在無線LAN控制器(WLC)上設定可擴充驗證通訊協定(EAP) — 透過安全通道進行彈性驗證(FAST)本地EAP驗證。本文檔還說明了如何將輕量級目錄訪問協定(LDAP)伺服器配置為本地EAP的後端資料庫，以檢索使用者憑據並對使用者進行身份驗證。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 執行韌體4.2的Cisco 4400系列WLC
- Cisco Aironet 1232AG系列輕量型存取點(LAP)
- Microsoft Windows 2003伺服器配置為域控制器、LDAP伺服器以及證書頒發機構伺服器。
- 執行韌體版本4.2的Cisco Aironet 802.11 a/b/g使用者端配接器
- 運行韌體版本4.2的Cisco Aironet案頭實用程式(ADU)

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

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

背景資訊

無線LAN控制器上的本地EAP身份驗證是隨無線LAN控制器4.1.171.0版引入的。

本地EAP是一種身份驗證方法，它允許使用者和無線客戶端在控制器上進行本地身份驗證。它適用於想要在後端系統中斷或外部身份驗證伺服器關閉時保持與無線客戶端連線的遠端辦公室。啟用本地EAP時，控制器用作身份驗證伺服器和本地使用者資料庫，因此它消除對外部身份驗證伺服器的依賴。本地EAP從本地使用者資料庫或LDAP後端資料庫中檢索使用者憑證以驗證使用者。本地EAP支援控制器與無線客戶端之間的LEAP、EAP-FAST、EAP-TLS、P EAPv0/MSCHAPv2和PEAPv1/GTC身份驗證。

本地EAP可以使用LDAP伺服器作為其後端資料庫來檢索使用者憑據。

LDAP後端資料庫允許控制器向LDAP伺服器查詢特定使用者的憑證（使用者名稱和密碼）。然後使用這些憑證對使用者進行身份驗證。

LDAP後端資料庫支援以下本地EAP方法：

- EAP-FAST/GTC
- EAP-TLS
- PEAPv1/GTC。

還支援LEAP、EAP-FAST/MSCHAPv2和PEAPv0/MSCHAPv2，但前提是將LDAP伺服器設定為返回明文密**碼**。例如，不支援Microsoft Active Directory，因為它不返回明文密碼。如果無法將LDAP伺服器配置為返回明文密碼，則不支援LEAP、EAP-FAST/MSCHAPv2和PEAPv0/MSCHAPv2。

注意：如果在控制器上配置了任何RADIUS伺服器，則控制器會先嘗試使用RADIUS伺服器對無線客戶端進行身份驗證。僅當未找到RADIUS伺服器時嘗試本地EAP，原因可能是RADIUS伺服器超時或未配置RADIUS伺服器。如果設定了四個RADIUS伺服器，則控制器會嘗試使用第一個RADIUS伺服器、第二個RADIUS伺服器、以及本地EAP來驗證使用者端。如果使用者端嘗試然後手動重新驗證，則控制器會先嘗試第三個RADIUS伺服器，然後嘗試第四個RADIUS伺服器，最後嘗試本地EAP。

此示例使用EAP-FAST作為WLC上的本地EAP方法，WLC又配置為查詢LDAP後端資料庫以獲取無線客戶端的使用者憑證。

設定

本文檔使用客戶端和伺服器端證書的EAP-FAST。為此，安裝程式使用**Microsoft Certificate Authority(CA)服**務器生成客戶端和伺服器證書。

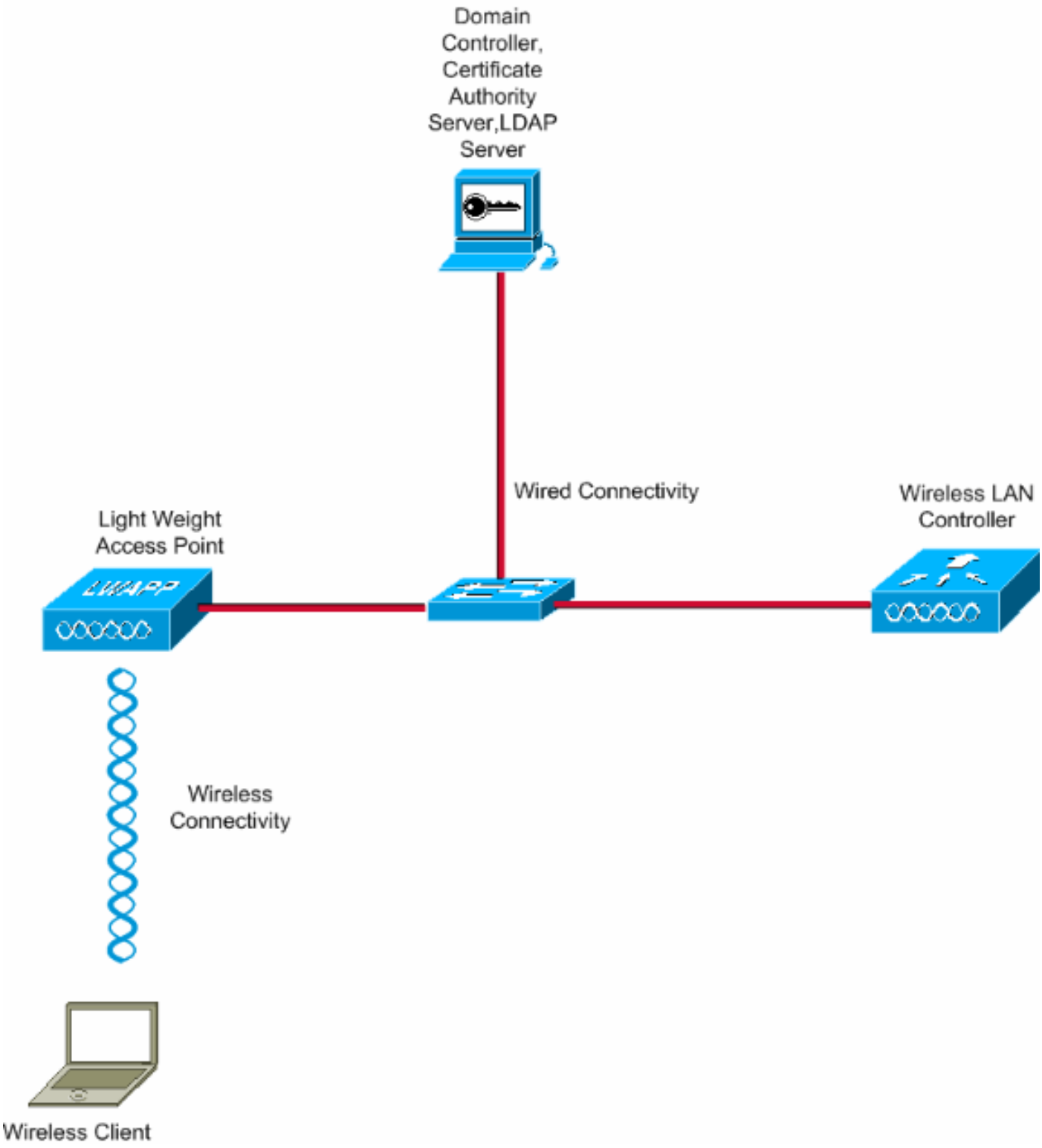
使用者憑證儲存在LDAP伺服器中，以便在證書驗證成功時，控制器將查詢LDAP伺服器以檢索使用者憑證並對無線客戶端進行身份驗證。

本檔案假設以下設定已經就位：

- LAP已註冊到WLC。有關註冊過程的詳細資訊，請參閱向無線LAN控制器(WLC)註冊輕量AP(LAP)。
- DHCP伺服器配置為向無線客戶端分配IP地址。
- Microsoft Windows 2003 server配置為域控制器以及CA伺服器。此範例使用**wireless.com**作為網域。有關將Windows 2003伺服器配置為域控制器的詳細資訊，請參閱將Windows 2003配置為域控制器。請參閱安裝並配置Microsoft Windows 2003 Server作為證書頒發機構(CA)伺服器，以便將Windows 2003 Server配置為企業CA伺服器。

網路圖表

本檔案會使用以下網路設定：



組態

完成以下步驟即可實作此組態：

- 在WLC上將EAP-FAST配置為本地EAP身份驗證方法
- 配置LDAP伺服器
- 配置無線客戶端

在WLC上將EAP-FAST配置為本地EAP身份驗證方法

如前所述，本文檔使用客戶端和伺服器端證書的EAP-FAST作為本地EAP身份驗證方法。第一步是下載下列憑證並將其安裝至伺服器（在此案例中為WLC）和使用者端。

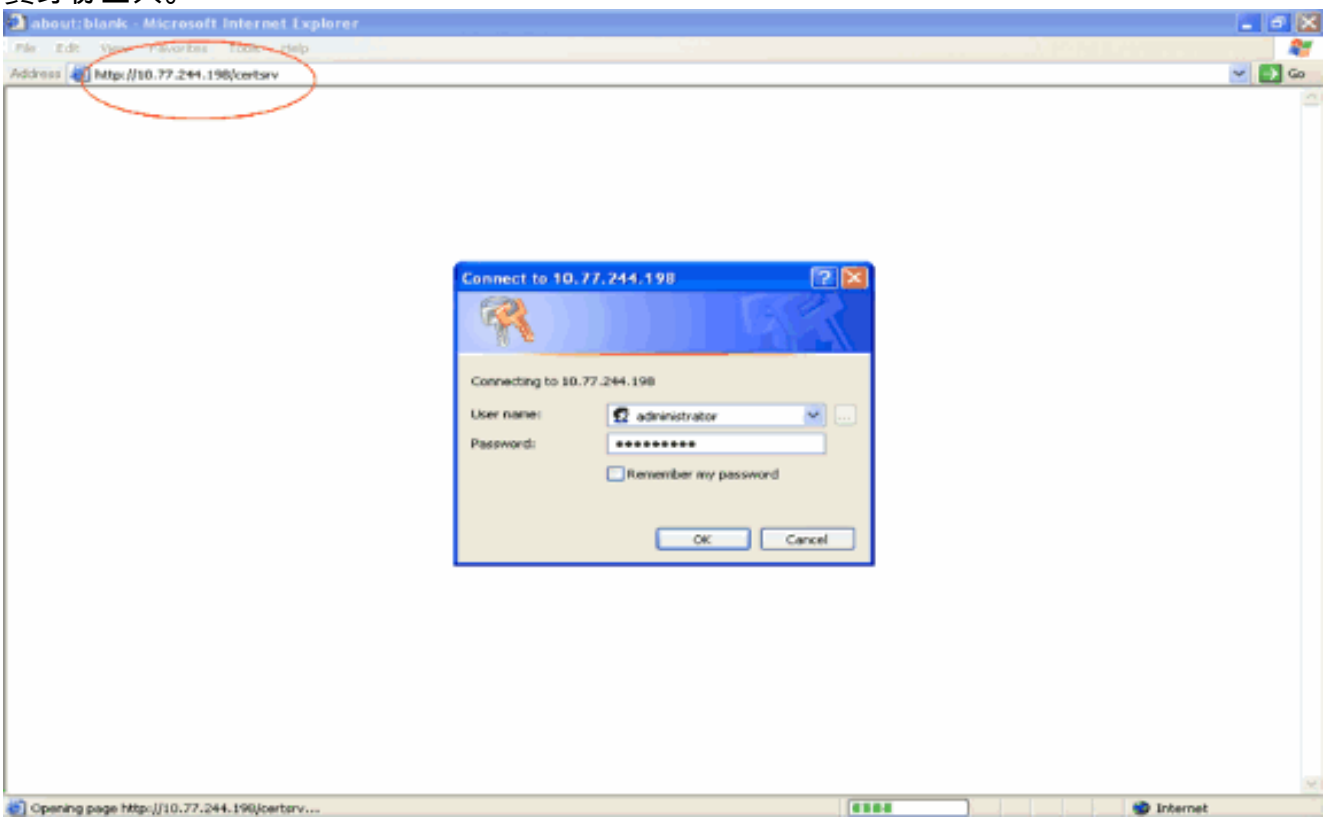
WLC和使用者端都需要從CA伺服器下載這些憑證：

- 裝置憑證（一個用於WLC，一個用於使用者端）
- WLC的公鑰基礎架構(PKI)的根憑證以及使用者端的CA憑證

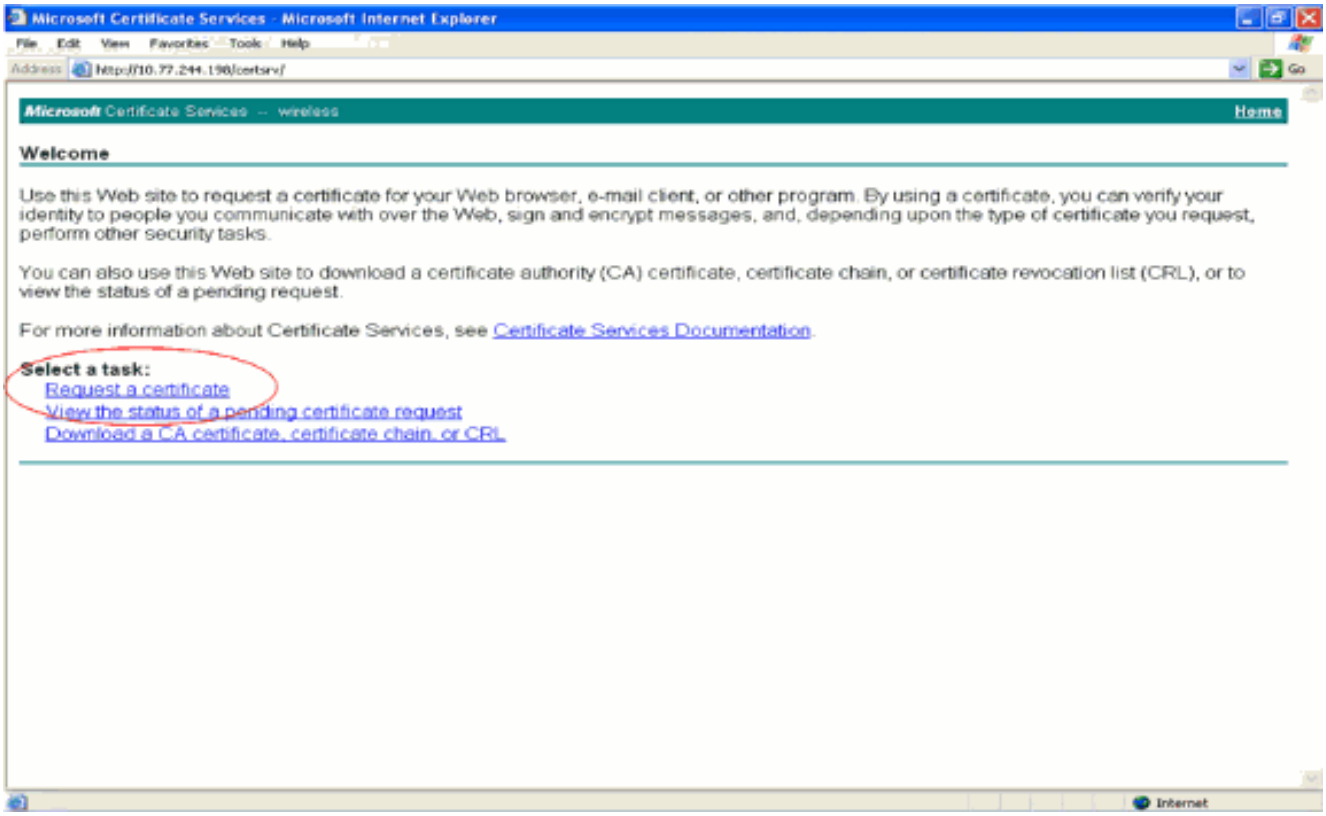
產生WLC的裝置憑證

執行以下步驟，以便從CA伺服器為WLC生成裝置證書。WLC使用此裝置憑證對使用者端進行驗證。

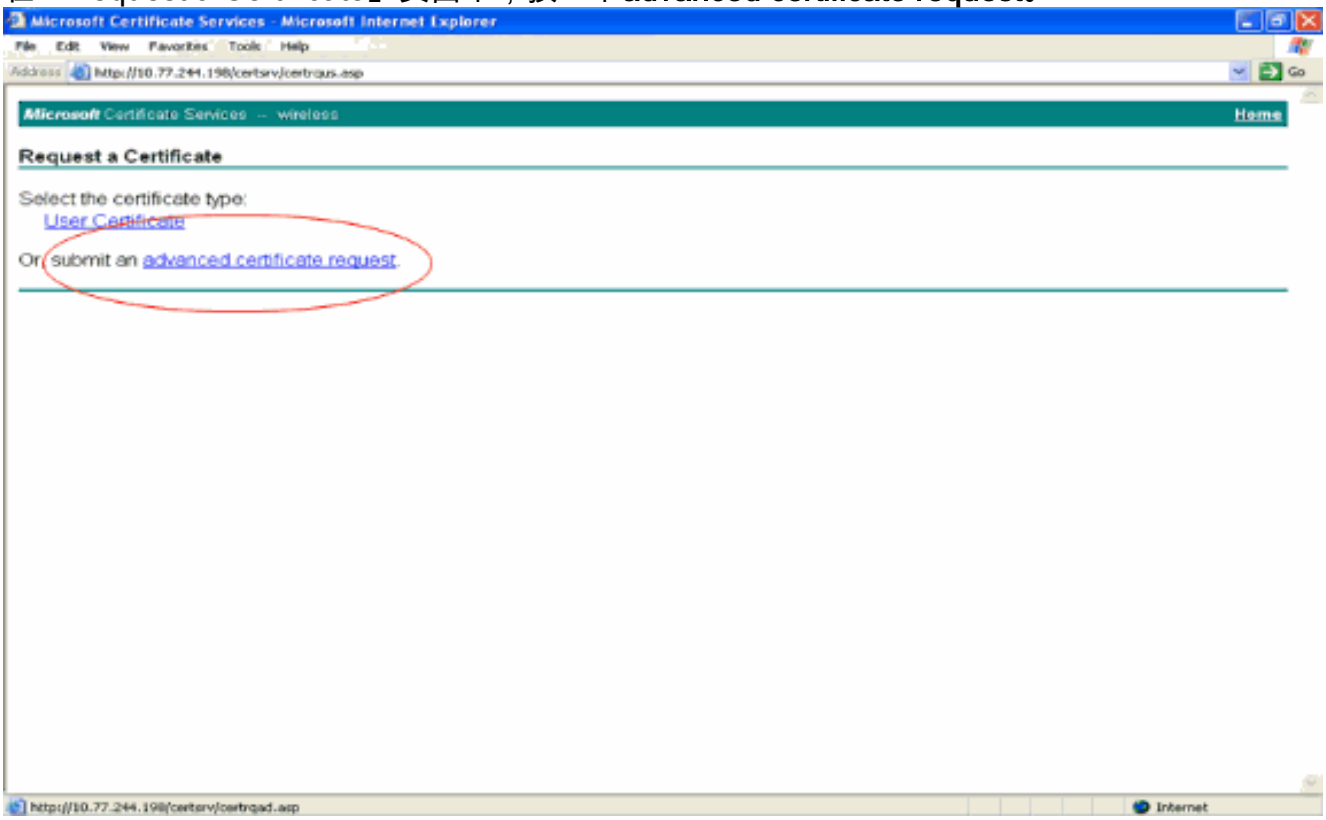
1. 從與CA伺服器具有網路連線的PC轉到**http://<CA伺服器的IP地址>/certsrv**。以CA伺服器管理員身份登入。



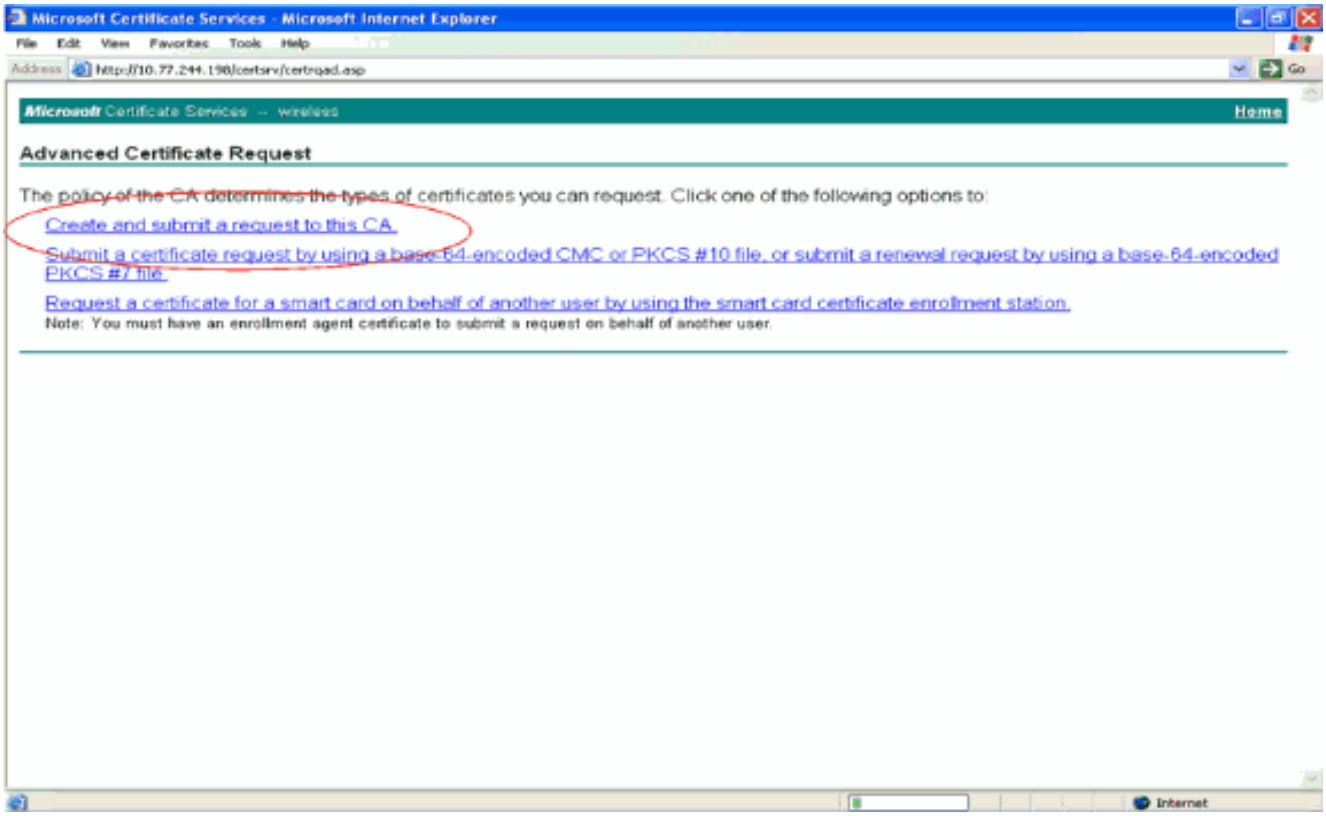
2. 選擇**請求證書**。



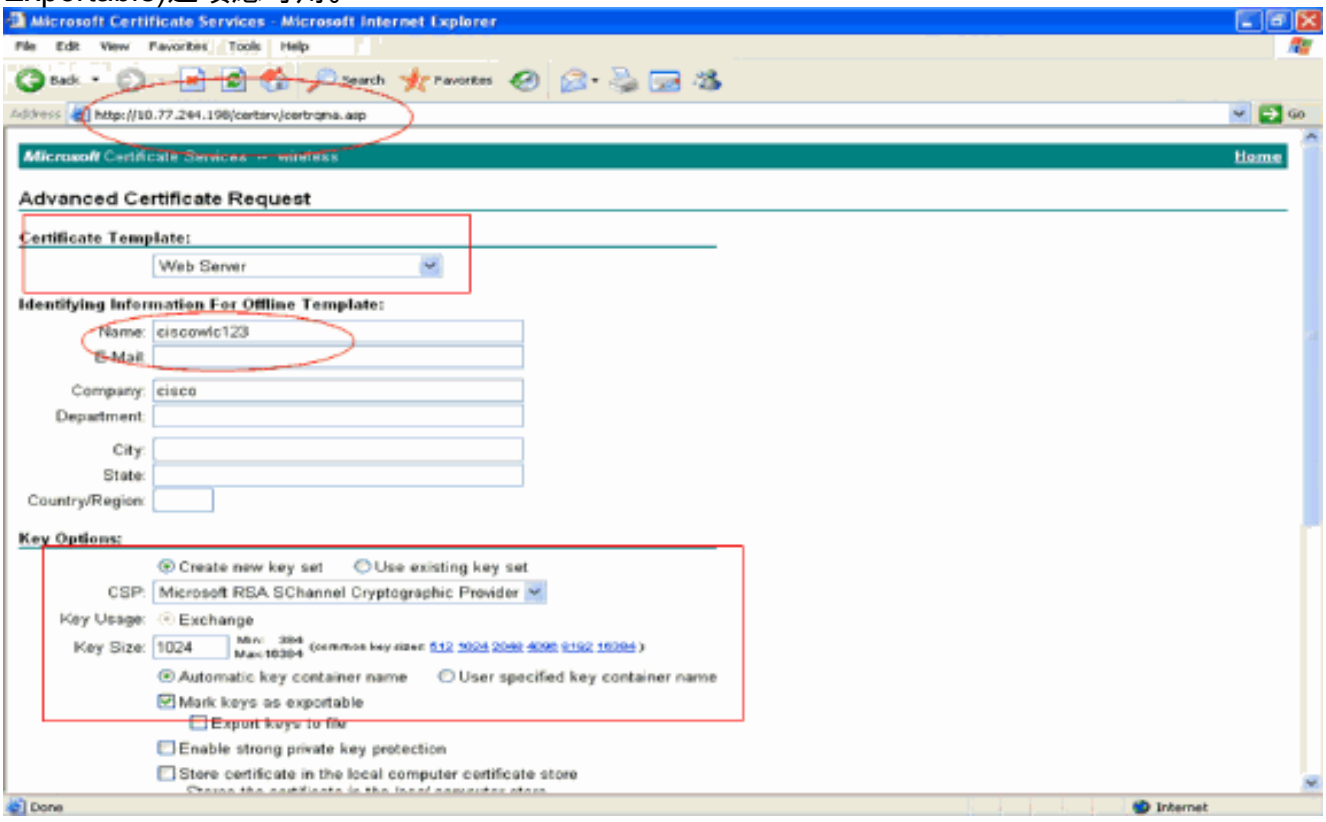
3. 在「Request a Certificate」頁面中，按一下**advanced certificate request**。



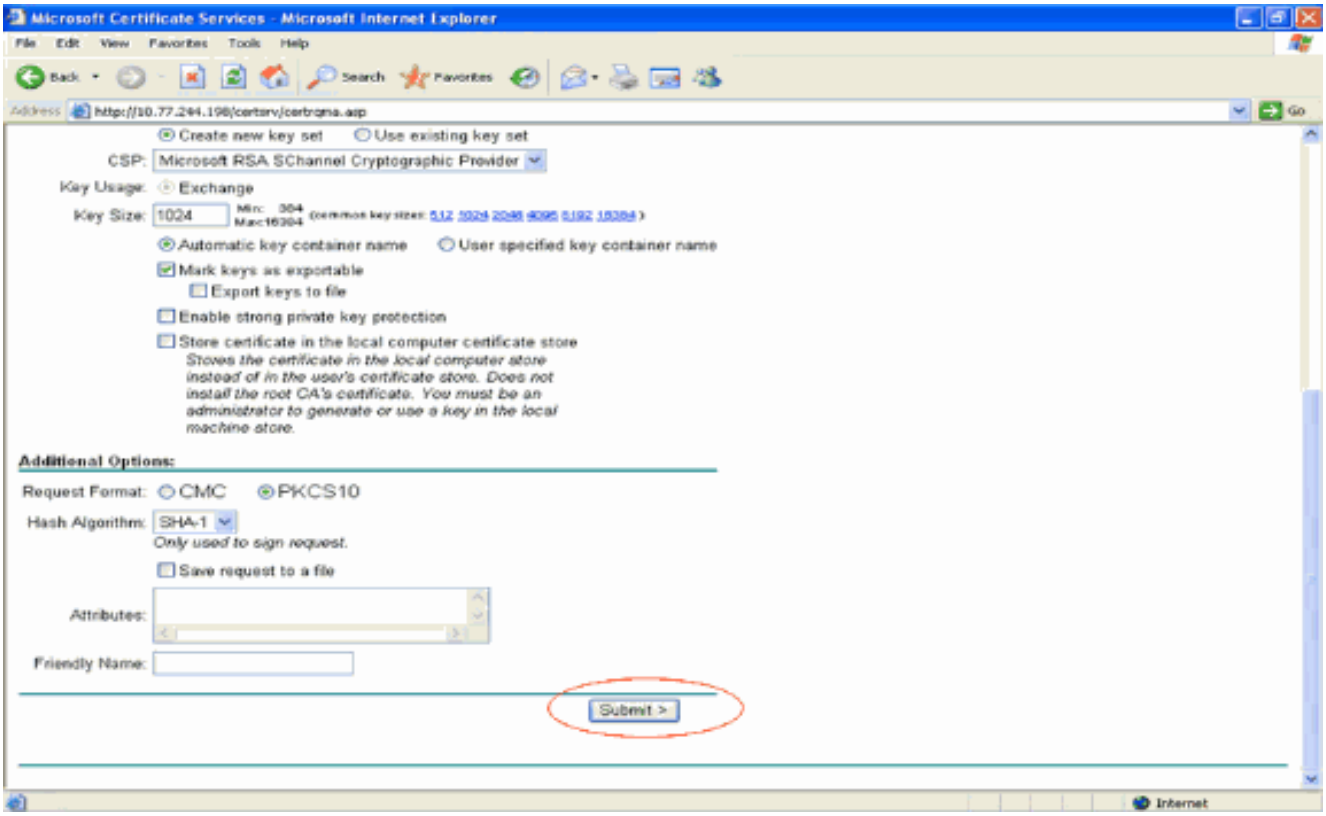
4. 在「高級證書請求」頁中，單**擊「建立」並將請求提交到此CA**。這會將您帶到「高級證書請求」表單。



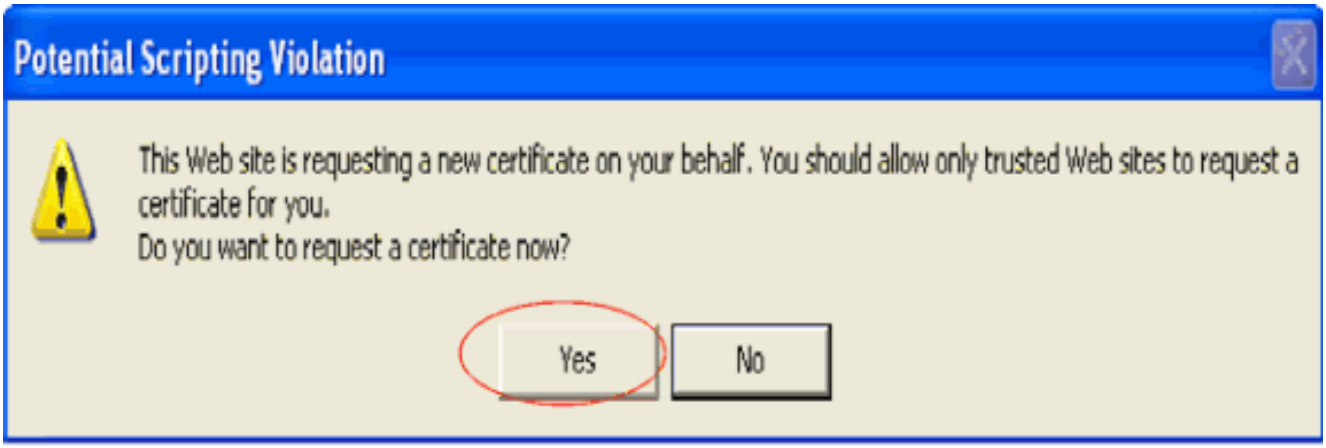
5. 在「高級證書請求」表單中，選擇**Web Server**作為「證書模板」。然後，為此裝置證書指定一個名稱。此範例將憑證名稱用作ciscowlc123。根據您的要求填寫其他標識資訊。
6. 在**Key Options**部分下，選擇**Mark Keys as Exportable**選項。有時，此特定選項會灰顯，如果您選擇Web伺服器模板，則無法啟用或禁用。在這種情況下，從瀏覽器選單中按一下**上一步**，返回一頁，然後再次返回此頁。這一次，「將金鑰標籤為可匯出」(Mark Keys as Exportable)選項應可用。



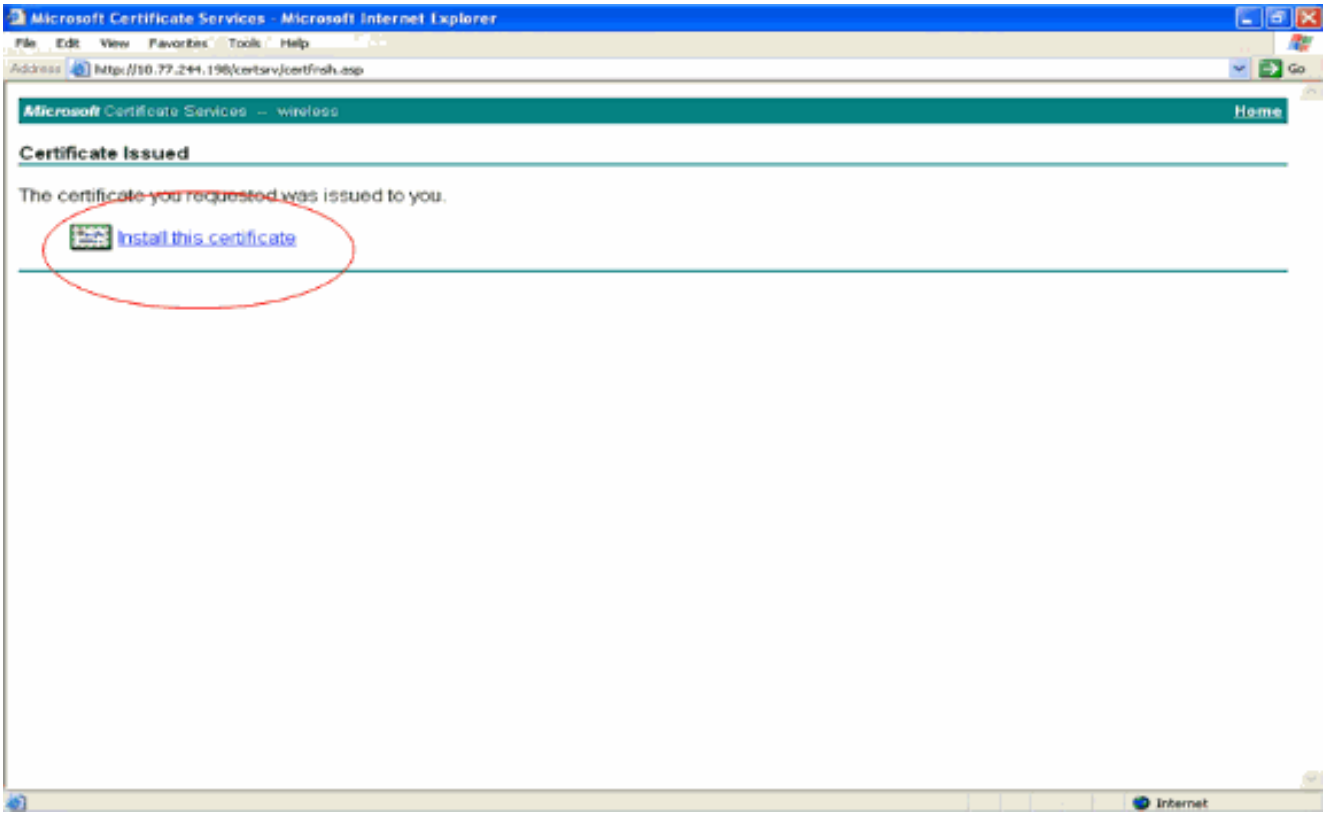
7. 配置所有其他必要的欄位，然後按一下**Submit**。



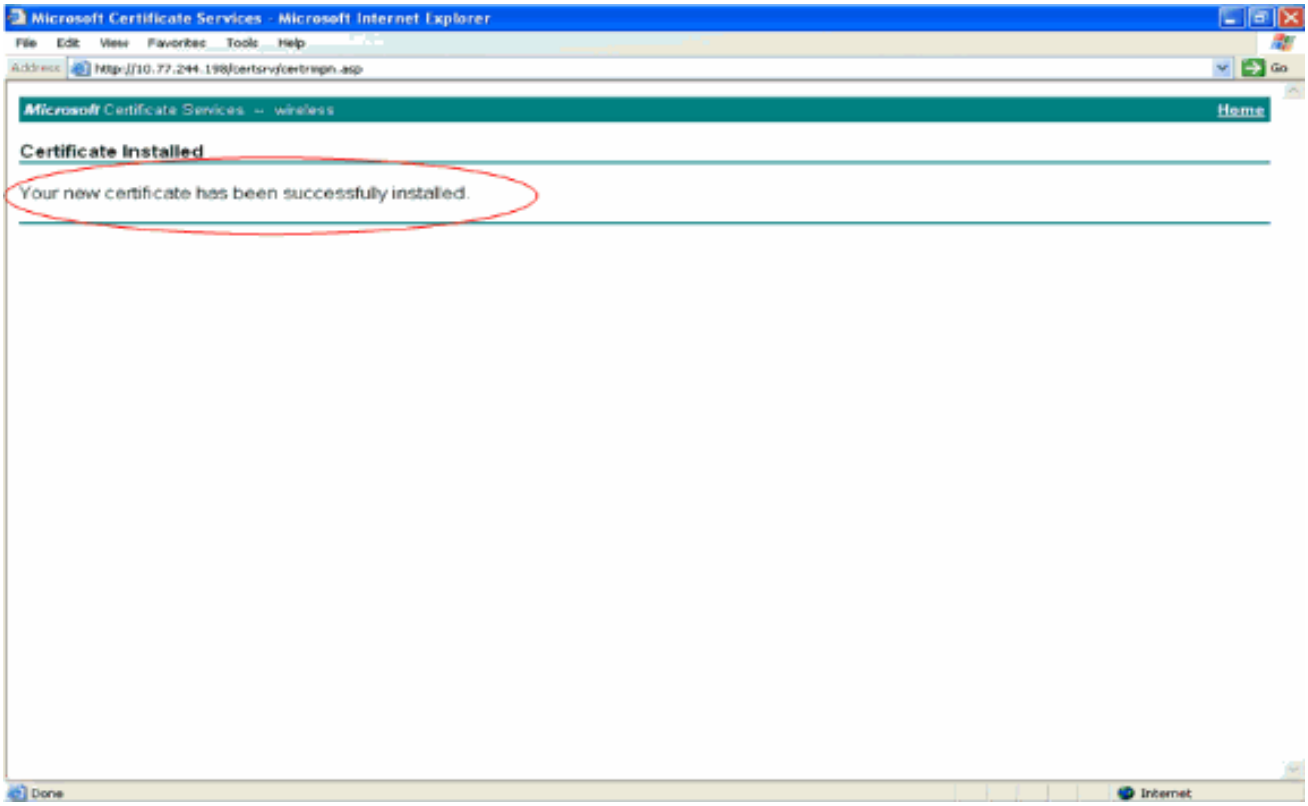
8. 在下一個視窗中按一下**Yes**以允許證書請求進程。



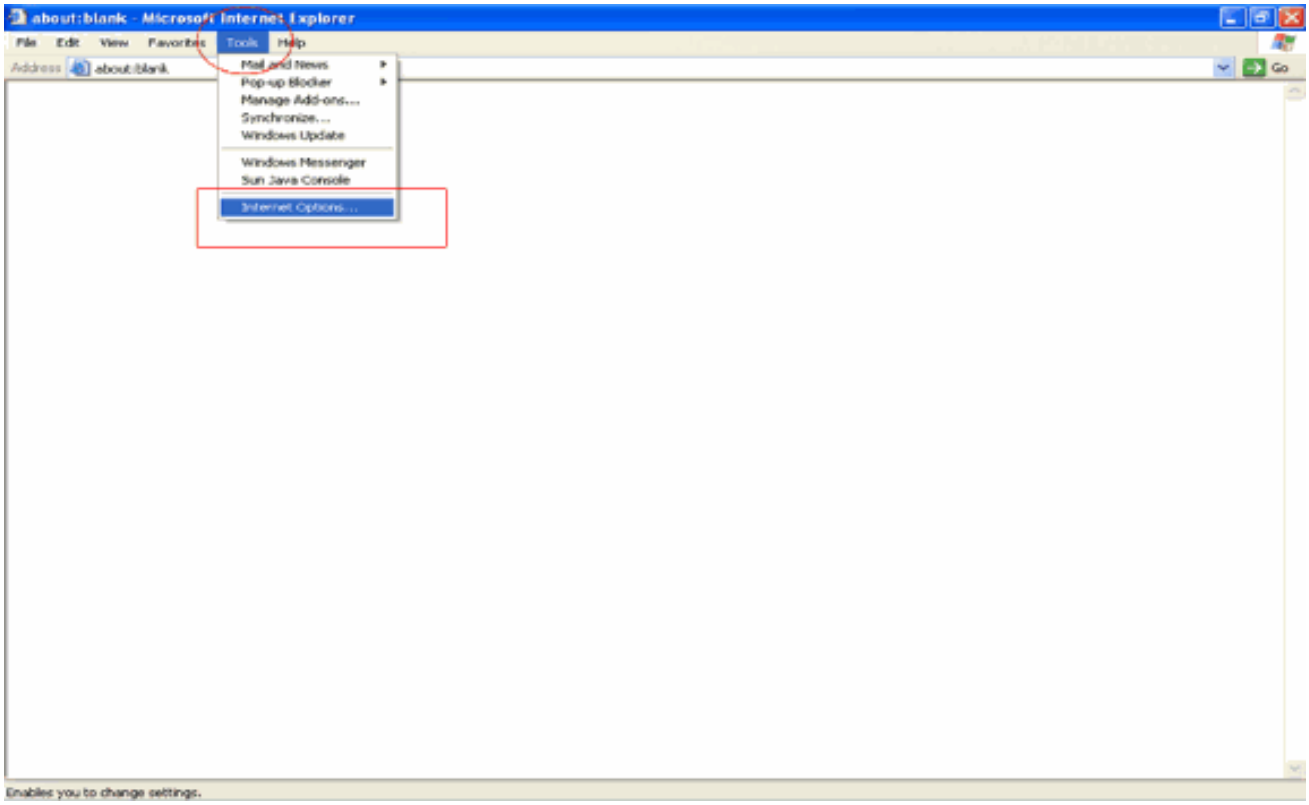
9. 出現「Certificate Issued（已頒發的證書）」視窗，指示成功的證書請求過程。下一步是將頒發的證書安裝到此PC的證書儲存區。按一下「**Install this certificate**」。



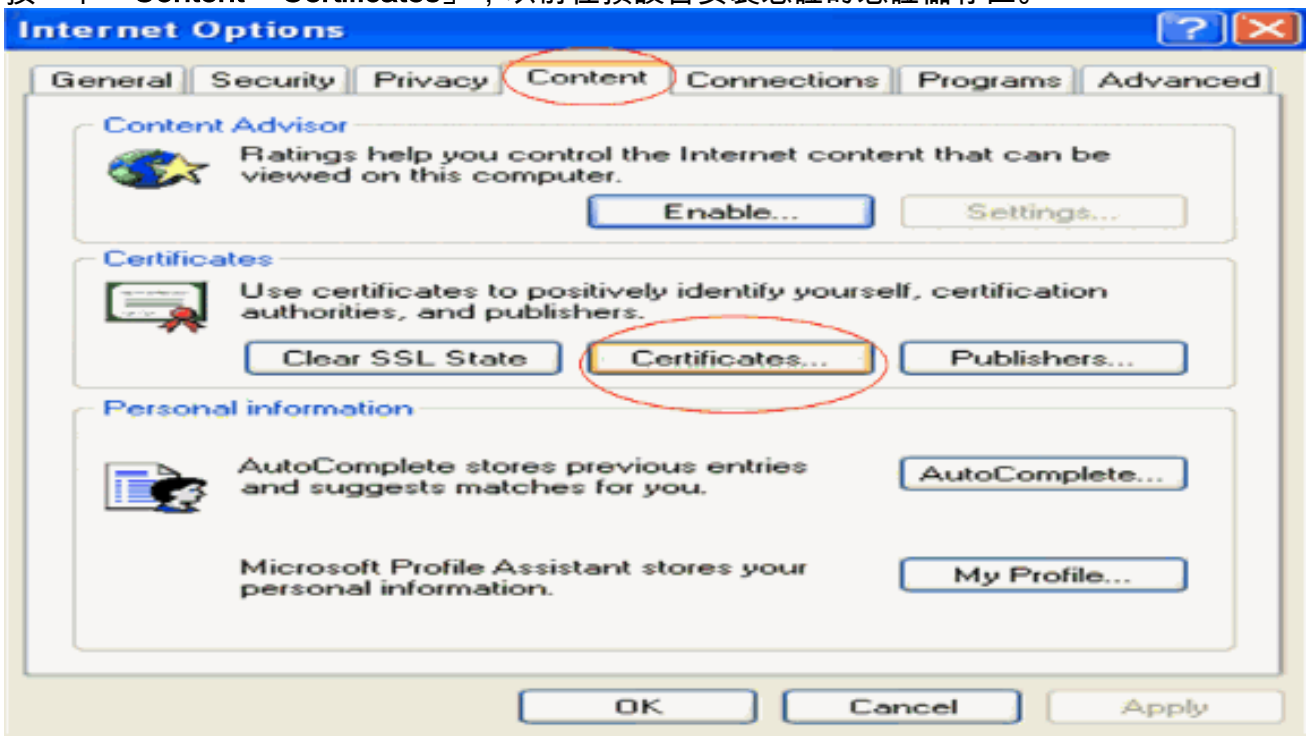
10. 新證書已成功安裝到從中生成請求到CA伺服器的PC。



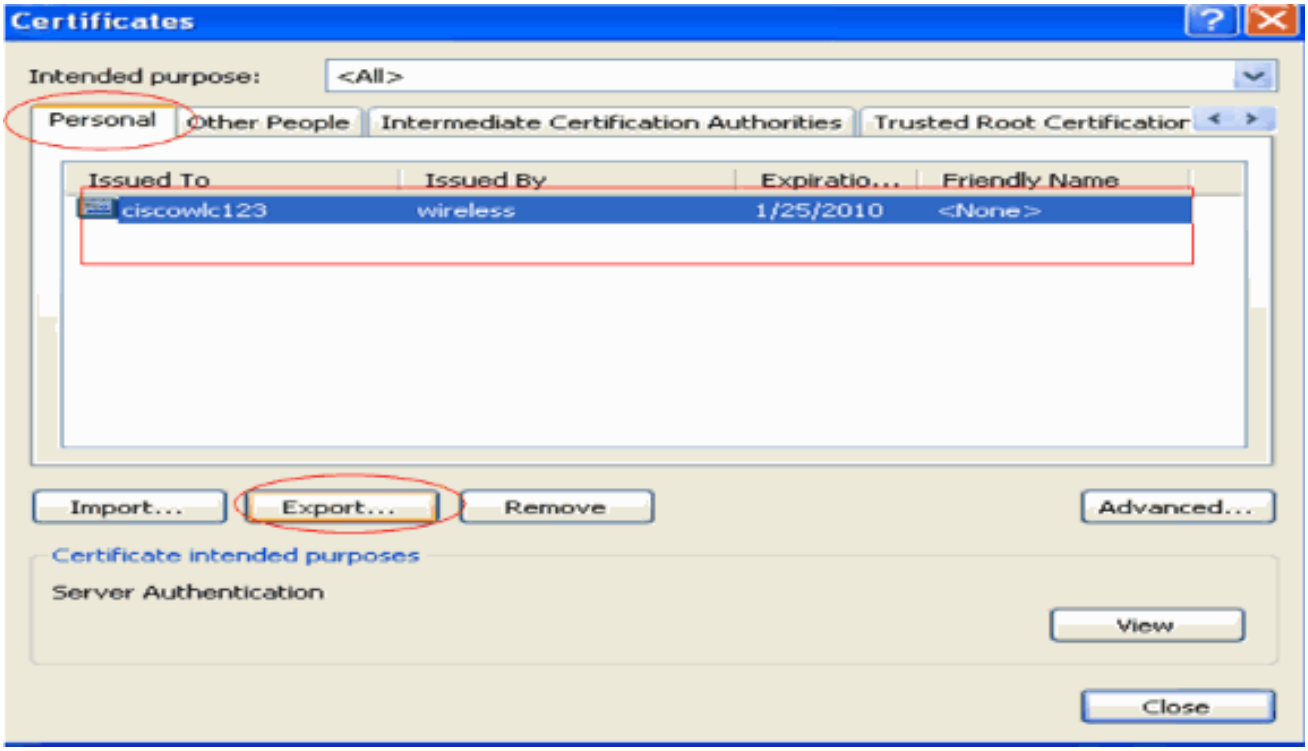
11. 下一步是將此證書從證書儲存區作為檔案匯出到硬碟。此憑證檔案稍後會用於下載憑證到WLC。若要從證書儲存匯出證書，請開啟Internet Explorer瀏覽器，然後按一下**工具> Internet選項**。



12. 按一下「**Content > Certificates**」，以前往預設會安裝憑證的憑證儲存區。

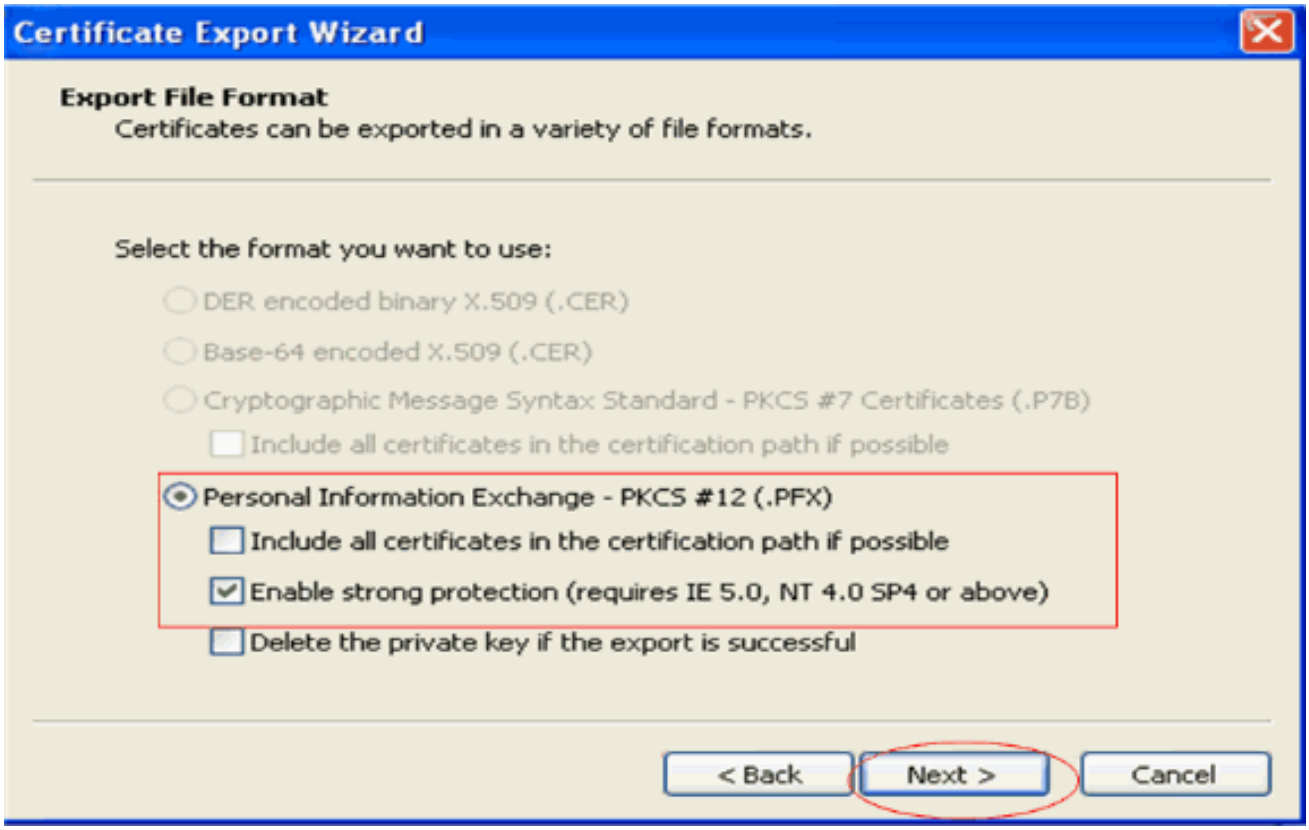


13. 裝置證書通常安裝在**Personal**證書清單下。在此，您應該看到新安裝的證書。選擇憑證並按一下**Export**。

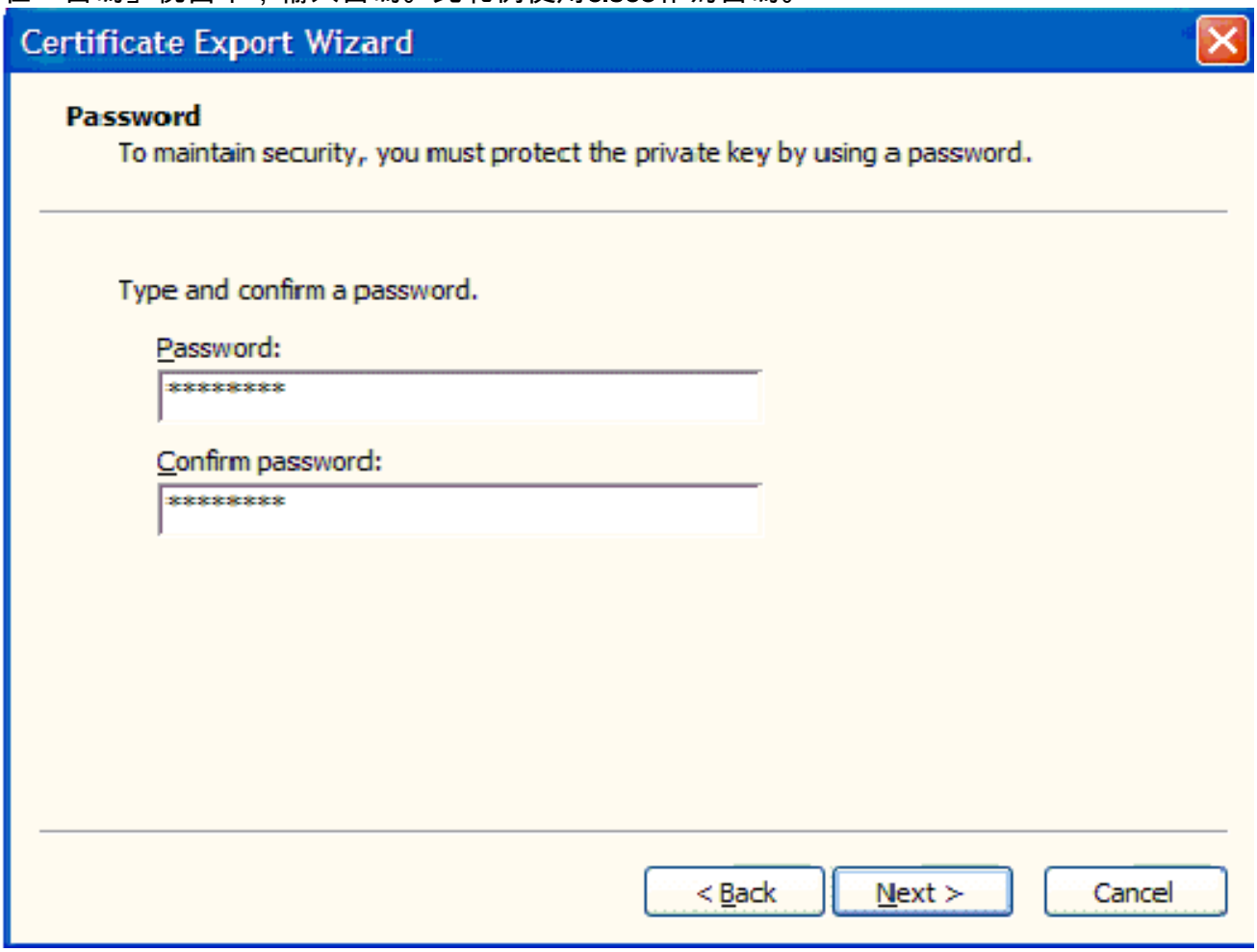


14. 在以下視窗中按一下Next。在「Certificate Export Wizard」視窗中選擇Yes，export the private key選項。按「Next」（下一步）。

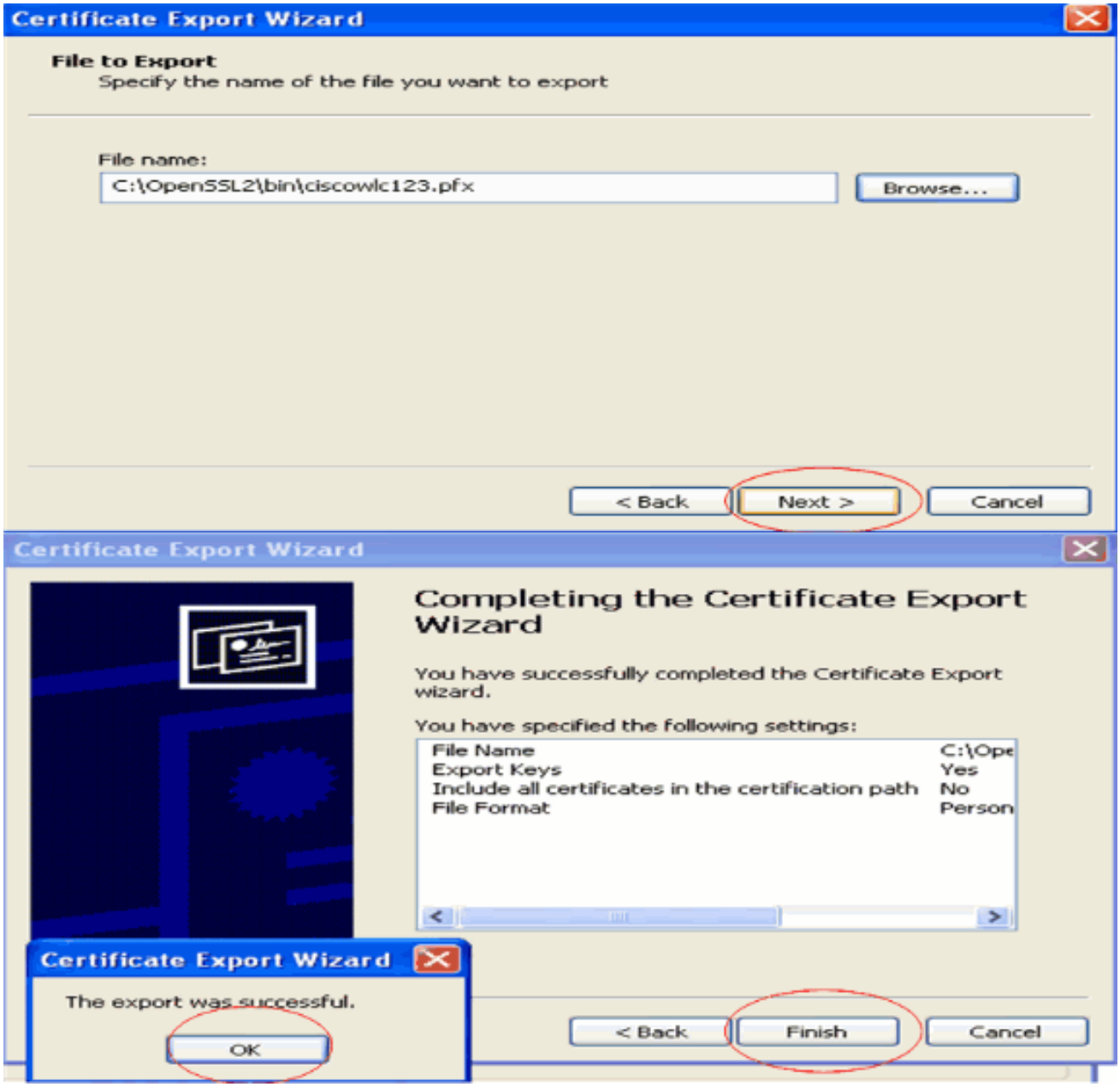
15. 選擇匯出檔案格式為.PFX，然後選擇Enable strong protection選項。按「Next」（下一步）。



16. 在「密碼」視窗中，輸入密碼。此範例使用cisco作為密碼。



17. 將證書檔案（.PFX檔案）儲存到硬碟。按一下「Next」，然後成功完成匯出程式。



將裝置證書下載到WLC

現在，WLC裝置證書可以作為.PFX檔案使用，下一步是將該檔案下載到控制器。Cisco WLC僅接受.PEM格式的證書。因此，您需要首先使用openSSL程式將.PFX或PKCS12格式檔案轉換為PEM檔案。

使用openSSL程式將PFX格式證書轉換為PEM格式

您可以將憑證複製到任何安裝了openSSL的PC，以將其轉換為PEM格式。在openSSL程式的bin資料夾中的Openssl.exe檔案上輸入以下命令：

注意：您可以從OpenSSL網站下載openSSL。

```
openssl>pkcs12 -in ciscowlc123.pfx -out ciscowlc123.pem
!--- ciscowlc123 is the name used in this example for the exported file. !--- You can specify
any name to your certificate file. Enter Import Password : cisco
!--- This is the same password that is mentioned in step 16 of the previous section. MAC
verified Ok Enter PEM Pass phrase : cisco
```

```
!--- Specify any passphrase here. This example uses the PEM passphrase as cisco. Verifying - PEM
pass phrase : cisco
```

證書檔案將轉換為PEM格式。下一步是將PEM格式裝置憑證下載到WLC。

注意：在此之前，您需要在要從中下載PEM檔案的PC上安裝TFTP伺服器軟體。這台電腦應該能連線到WLC。TFTP伺服器的當前目錄和基目錄應指定PEM檔案的儲存位置。

將轉換後的PEM格式裝置證書下載到WLC

此範例說明透過WLC的CLI下載程式。

1. 登入控制器CLI。
2. 輸入**transfer download datatype eapdevcert**命令。
3. 輸入**transfer download serverip** ***10.77.244.196*** 命令。10.77.244.196是TFTP伺服器的IP地址。
4. 輸入**transfer download filename** ***ciscowlc.pem*** 指令。ciscowlc123.pem是本範例中使用的檔案名稱。
5. 輸入**transfer download certpassword**命令以設定憑證的密碼。
6. 輸入**transfer download start**命令檢視更新的設定。然後，當系統提示確認當前設定並開始下載過程時，請回答**y**。此範例顯示download指令輸出：

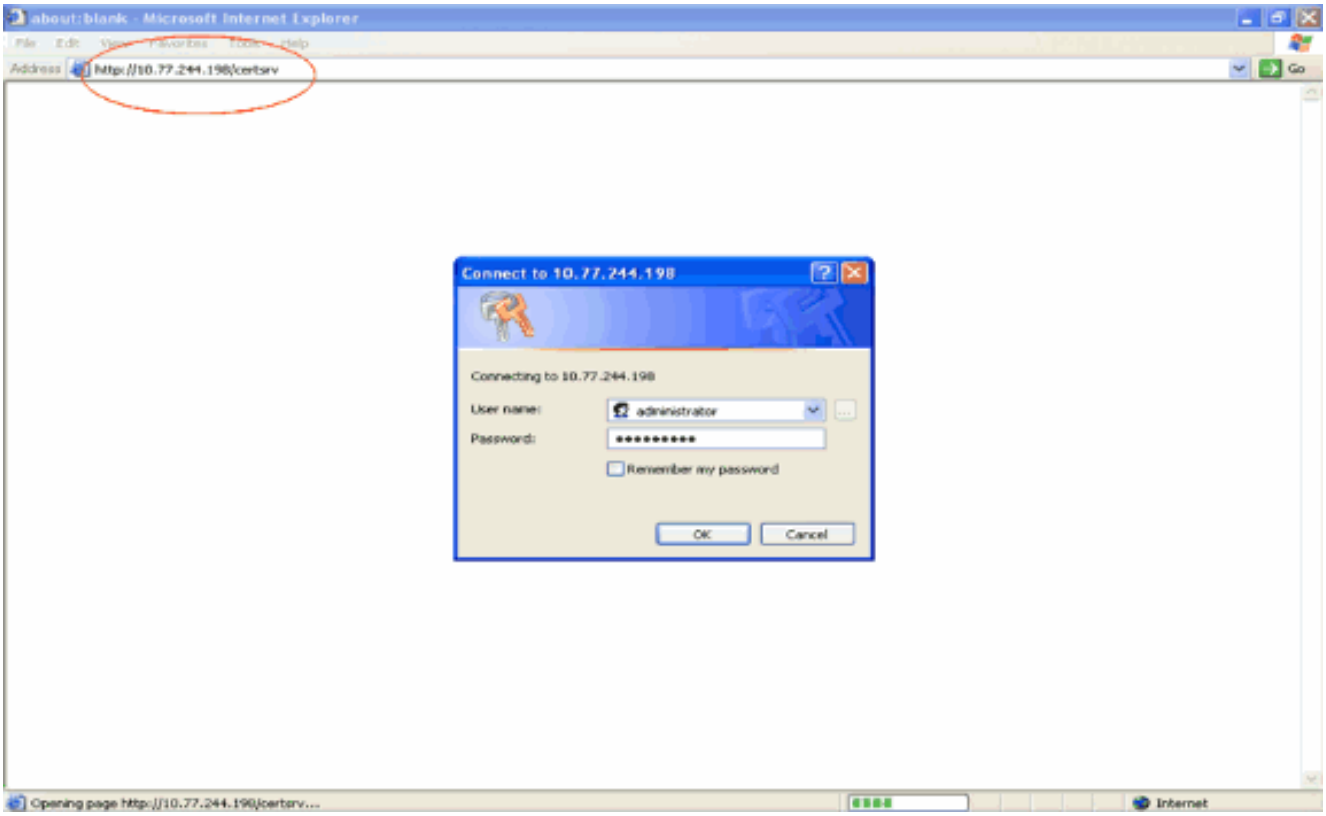
```
(Cisco Controller) >transfer download start

Mode............................................ TFTP
Data Type....................................... Vendor Dev Cert
TFTP Server IP.................................. 10.77.244.196
TFTP Packet Timeout............................. 6
TFTP Max Retries................................ 10
TFTP Path.......................................
TFTP Filename................................... ciscowlc.pem

This may take some time.
Are you sure you want to start? (y/N) y
TFTP EAP CA cert transfer starting.
Certificate installed.
Reboot the switch to use the new certificate.
Enter the reset system command to reboot the controller.
     The controller is now loaded with the device certificate.
```

7. 輸入**reset system**指令以重新啟動控制器。控制器現在載入了裝置證書。

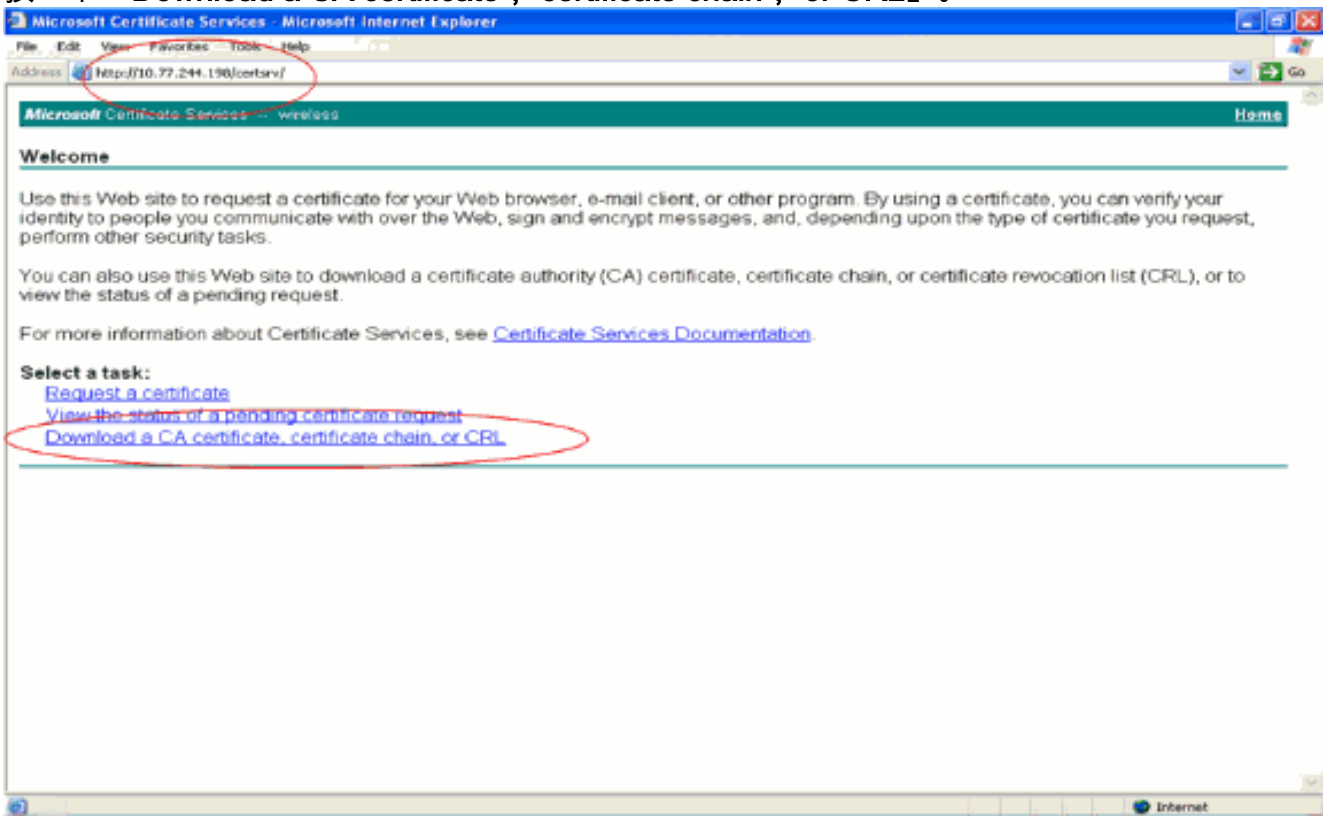
將PKI的根證書安裝到WLC中

現在裝置證書安裝在WLC中，下一步是將PKI的根證書從CA伺服器安裝到WLC。執行以下步驟：

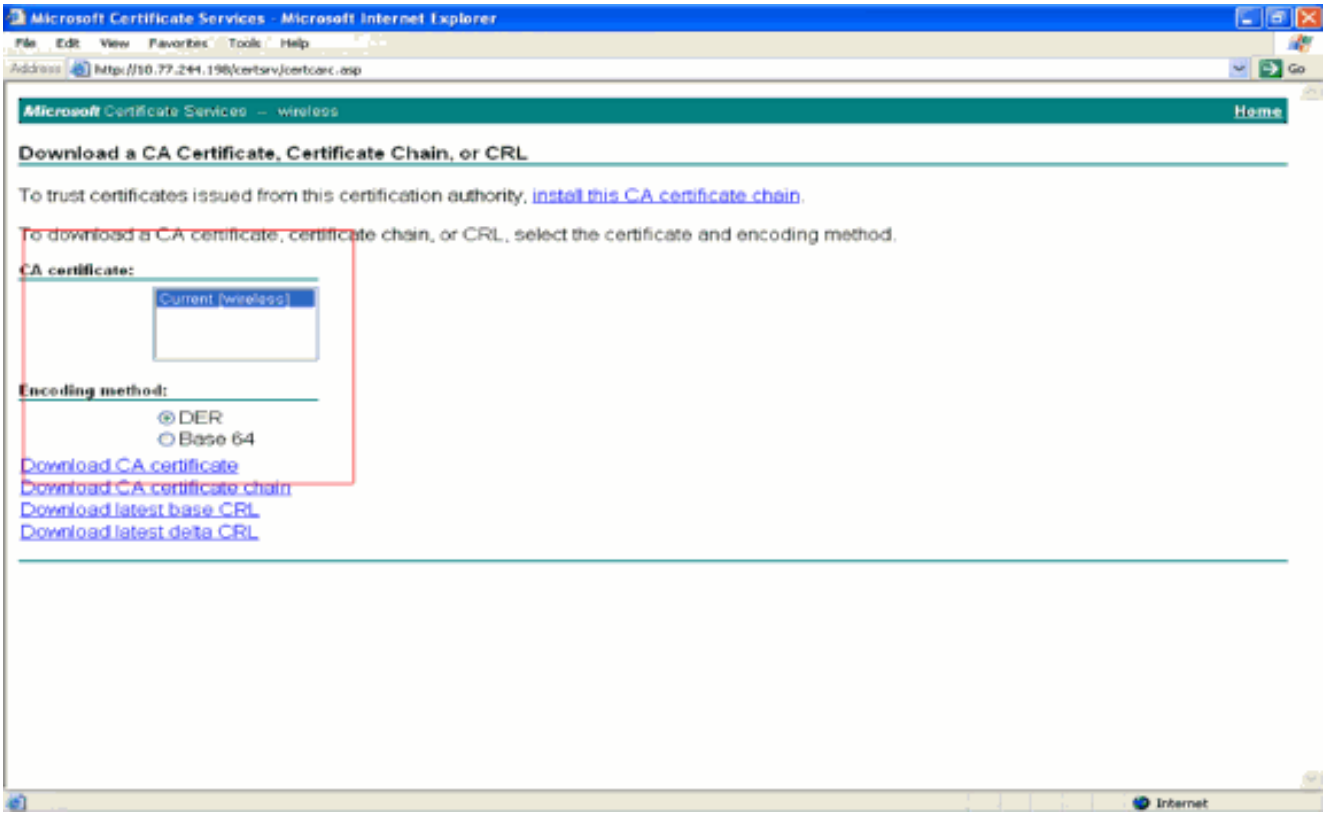
1. 從與CA伺服器具有網路連線的PC轉到**http://<CA伺服器的IP地址>/certsrv**。以CA伺服器管理員身份登入。



2. 按一下「**Download a CA certificate， certificate chain， or CRL**」。



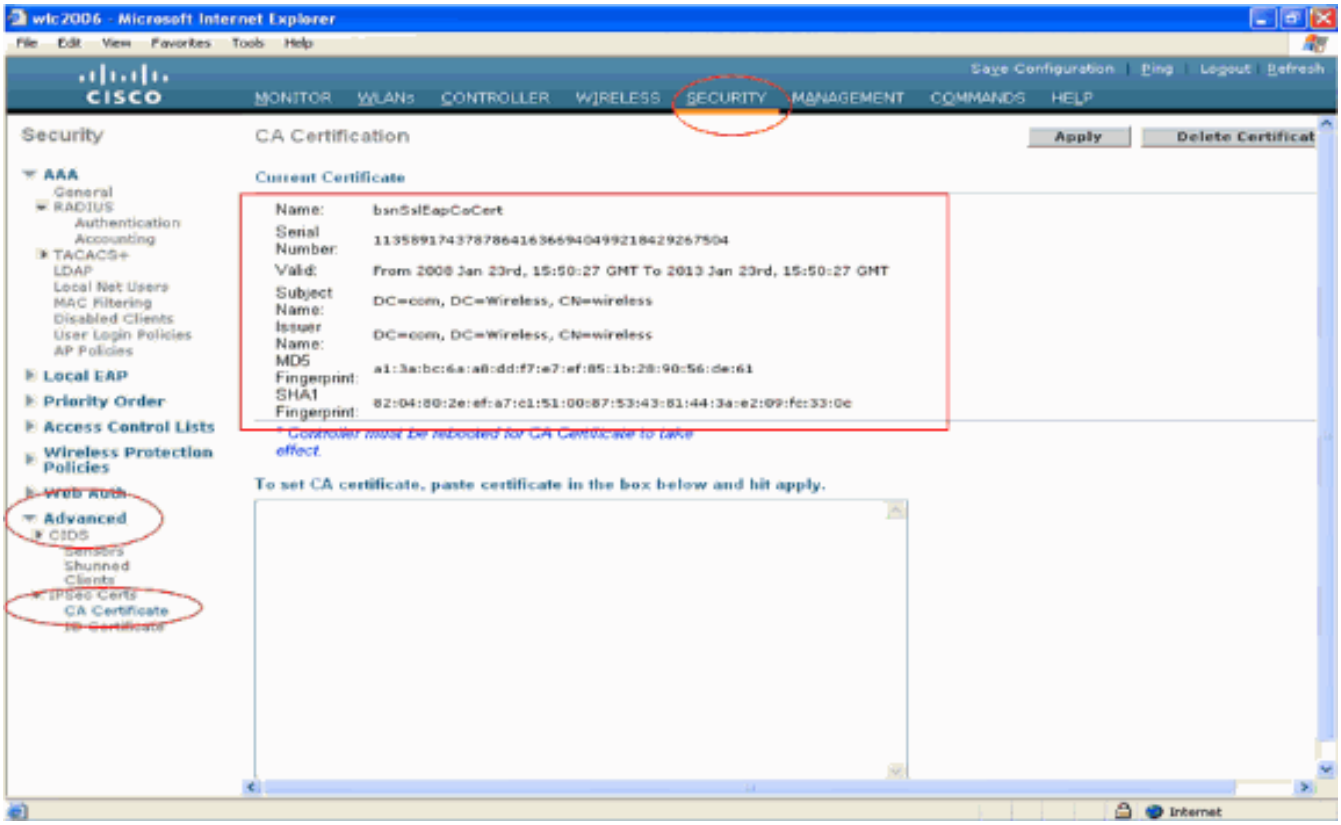
3. 在結果頁面中，您可以在**CA證書**框下看到CA伺服器上可用的當前CA證書。選擇**DER**作為Encoding方法，然後按一下**Download CA certificate**。



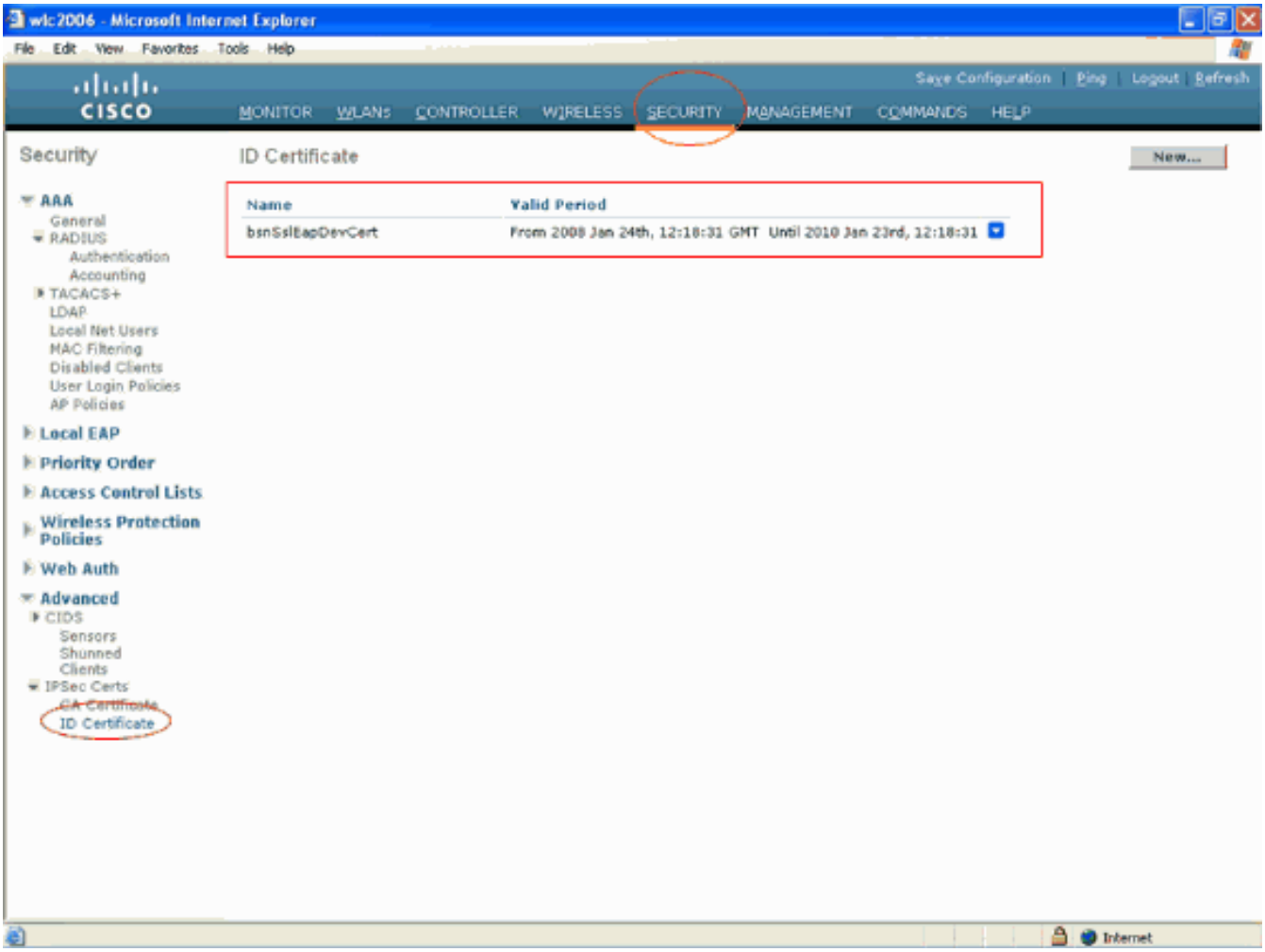
4. 將憑證另存為**.cer檔**案。此示例使用**certnew.cer**作為檔名。
5. 下一步是將.cer檔案轉換為PEM格式並下載到控制器。若要執行這些步驟，請重複在[將裝置憑證下載到WLC](#)一節中說明的相同程式，並執行以下變更：openSSL "-in"和"-out"檔案是**certnew.cer**和**certnew.pem**。此外，此過程不需要PEM密碼或匯入密碼。此外，用於將.cer檔案**轉換**為.pem檔案**的openSSL**命令為：**x509 -in *certnew.cer* -inform DER -out *certnew.pem* -outform PEM**在[將轉換的PEM格式裝置憑證下載到WLC](#)一節的步驟2中，將憑證下載到WLC的命令如下：（思科控制器）**>transfer download datatype eapcacert**要下載到WLC的檔案為**certnew.pem**。

您可以透過控制器GUI驗證憑證是否安裝在WLC上，如下所示：

- 在WLC GUI上，按一下「**Security**」。在Security頁面中，從左側顯示的任務中按一下**Advanced > IPSec Certs**。按一下「**CA Certificate**」以檢視已安裝的CA證書。以下是範例：



- 若要確認裝置憑證是否安裝在WLC上，請在WLC GUI上按一下「**Security**」。在Security頁面中，從左側顯示的任務中按一下**Advanced > IPSec Certs**。按一下**ID Certificate**以檢視安裝的裝置證書。以下是範例
：

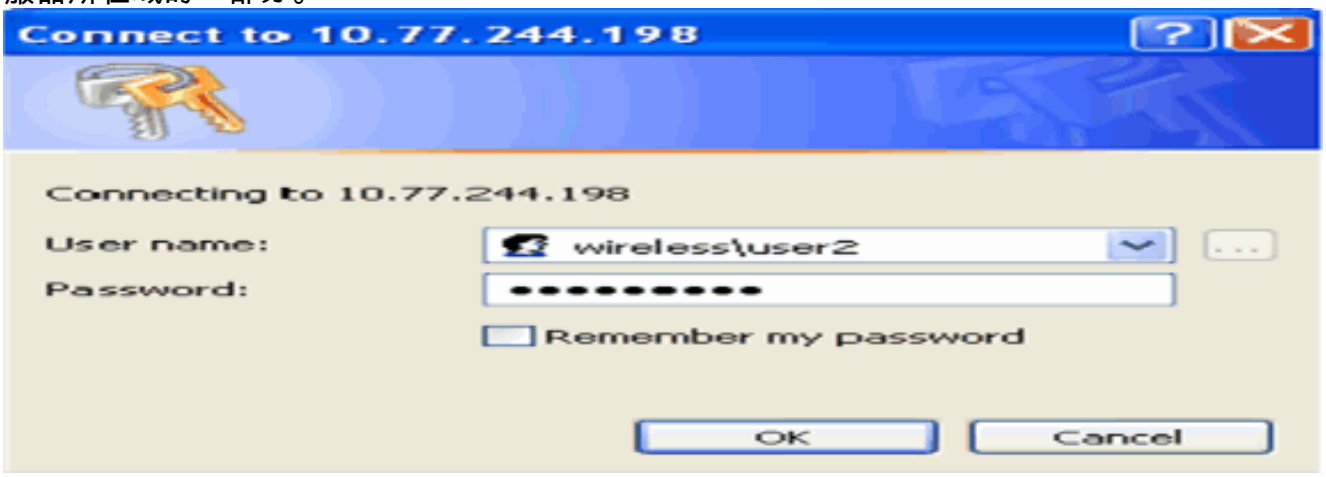


生成客戶端的裝置證書

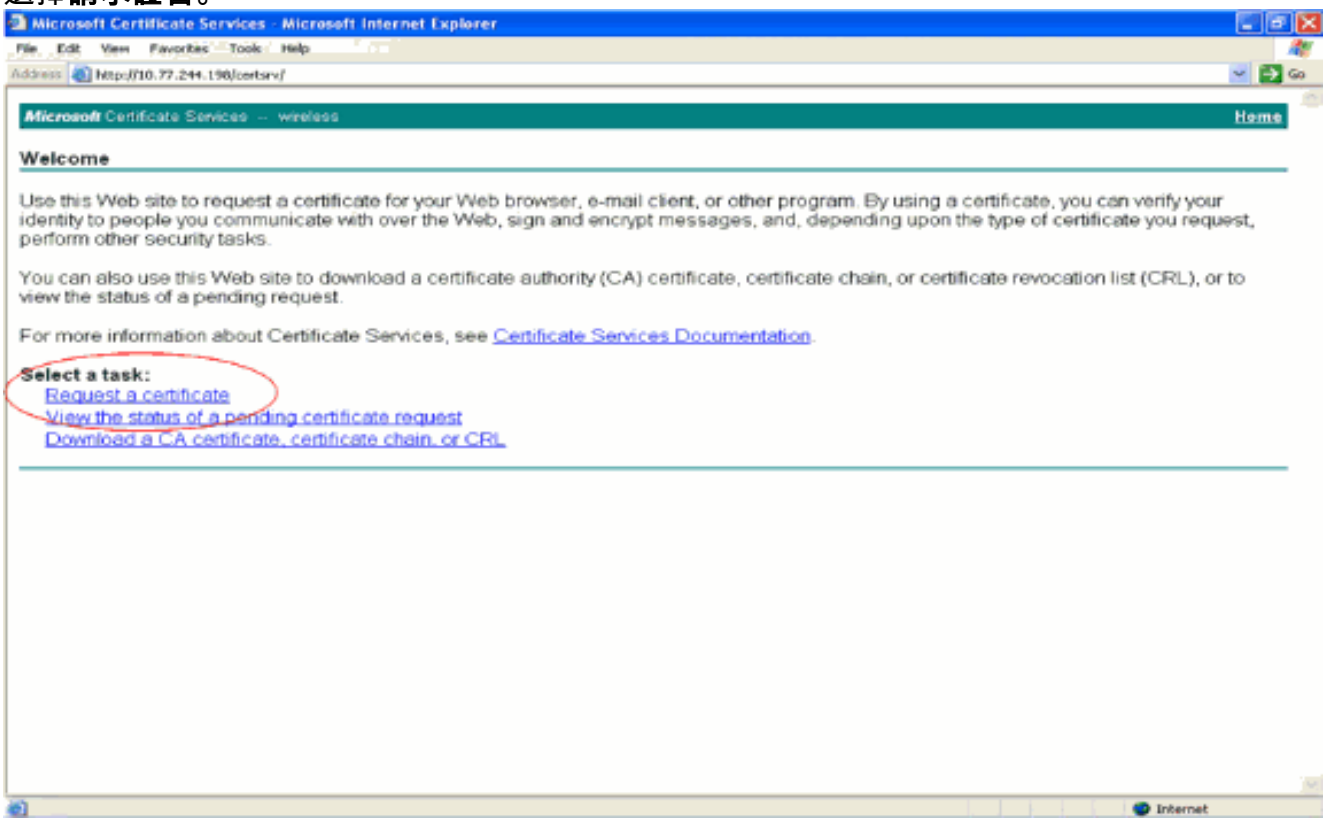
由於裝置憑證和CA憑證已安裝在WLC上，下一步是產生使用者端的這些憑證。

執行這些步驟，以便為客戶端生成裝置證書。使用者端會使用此憑證對WLC進行驗證。本文檔介紹為Windows XP專業版客戶端生成證書所涉及的步驟。

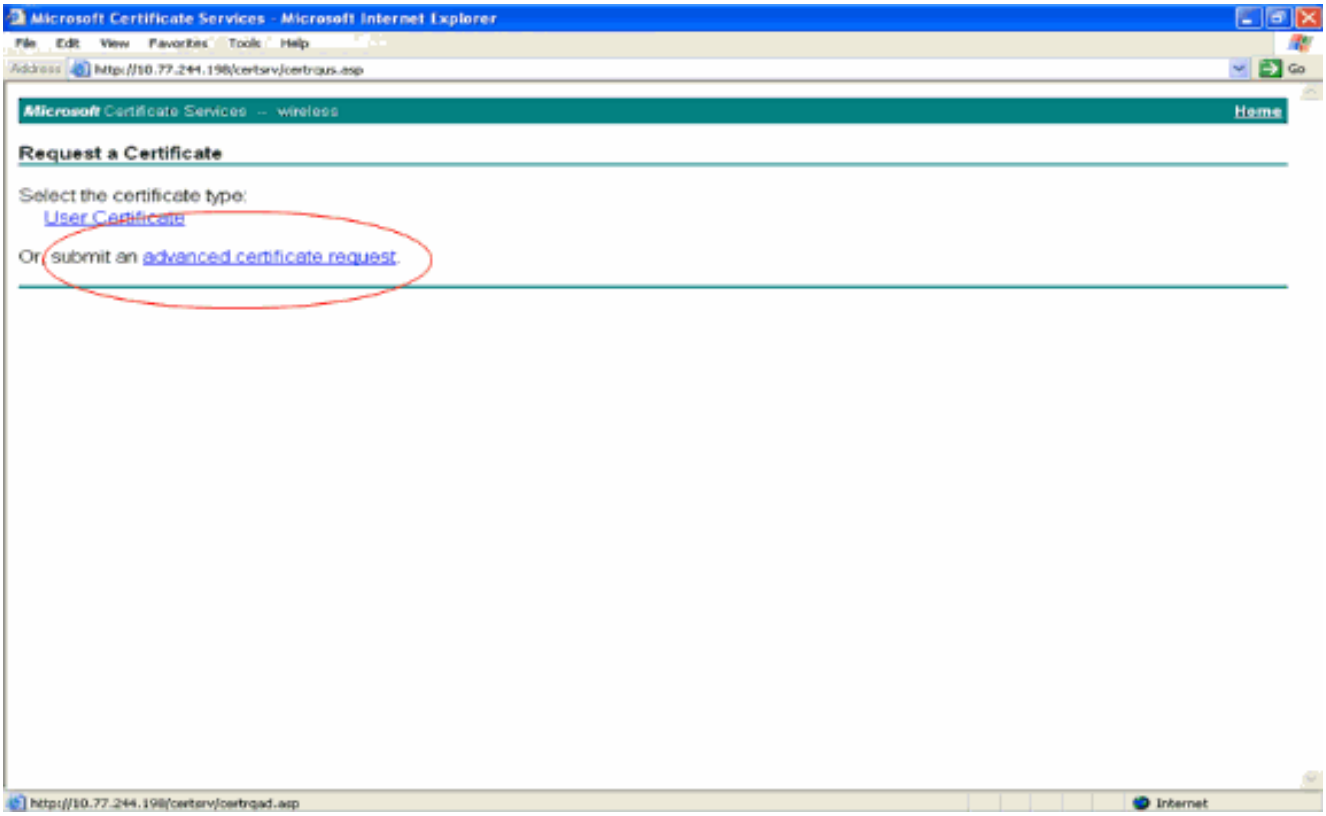
1. 從需要安裝證書的客戶端轉到**http://<CA伺服器的IP地址>/certsrv**。以域名\使用者名稱登入到CA伺服器。使用者名稱應該是使用此XP電腦的使用者的名稱，該使用者應該已經配置為CA伺服器所在域的一部分。



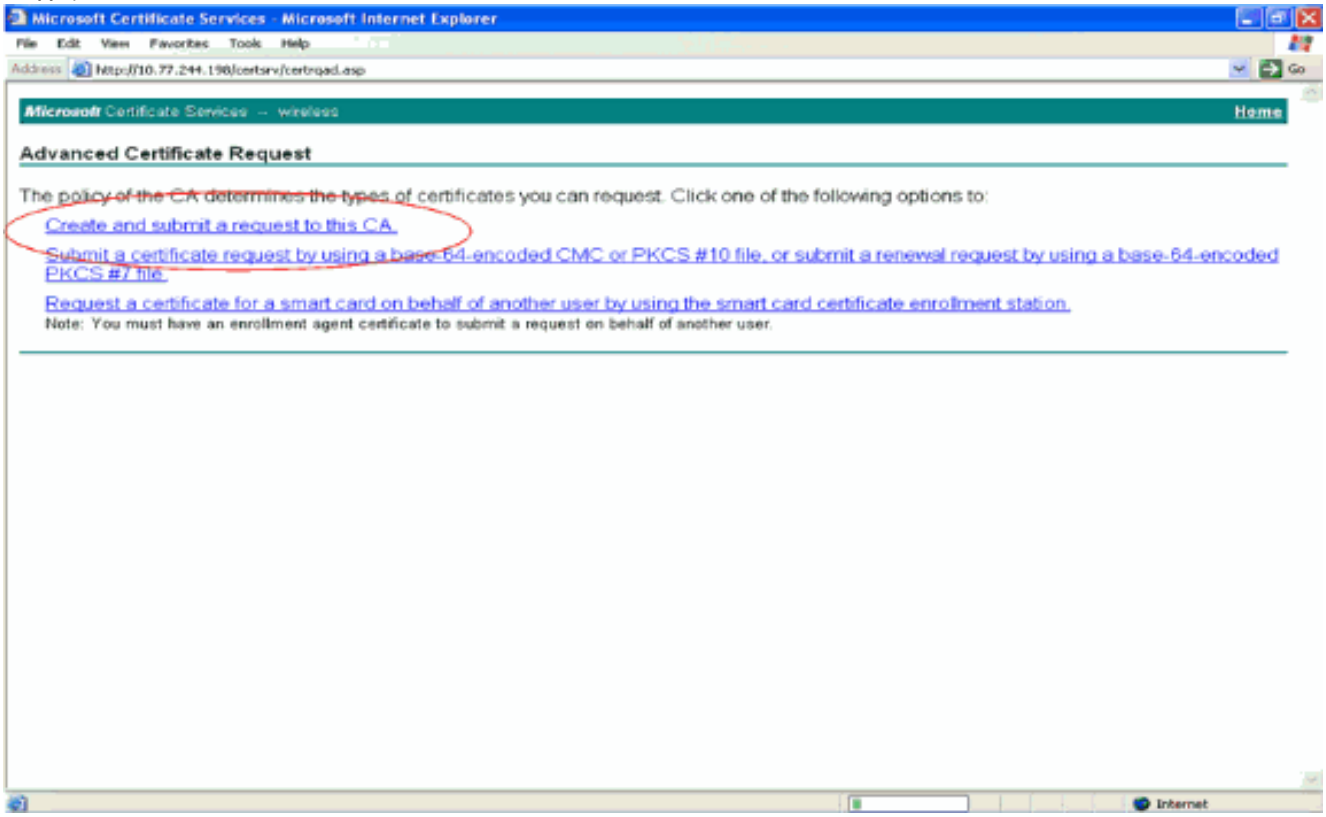
2. 選擇**請求證書**。



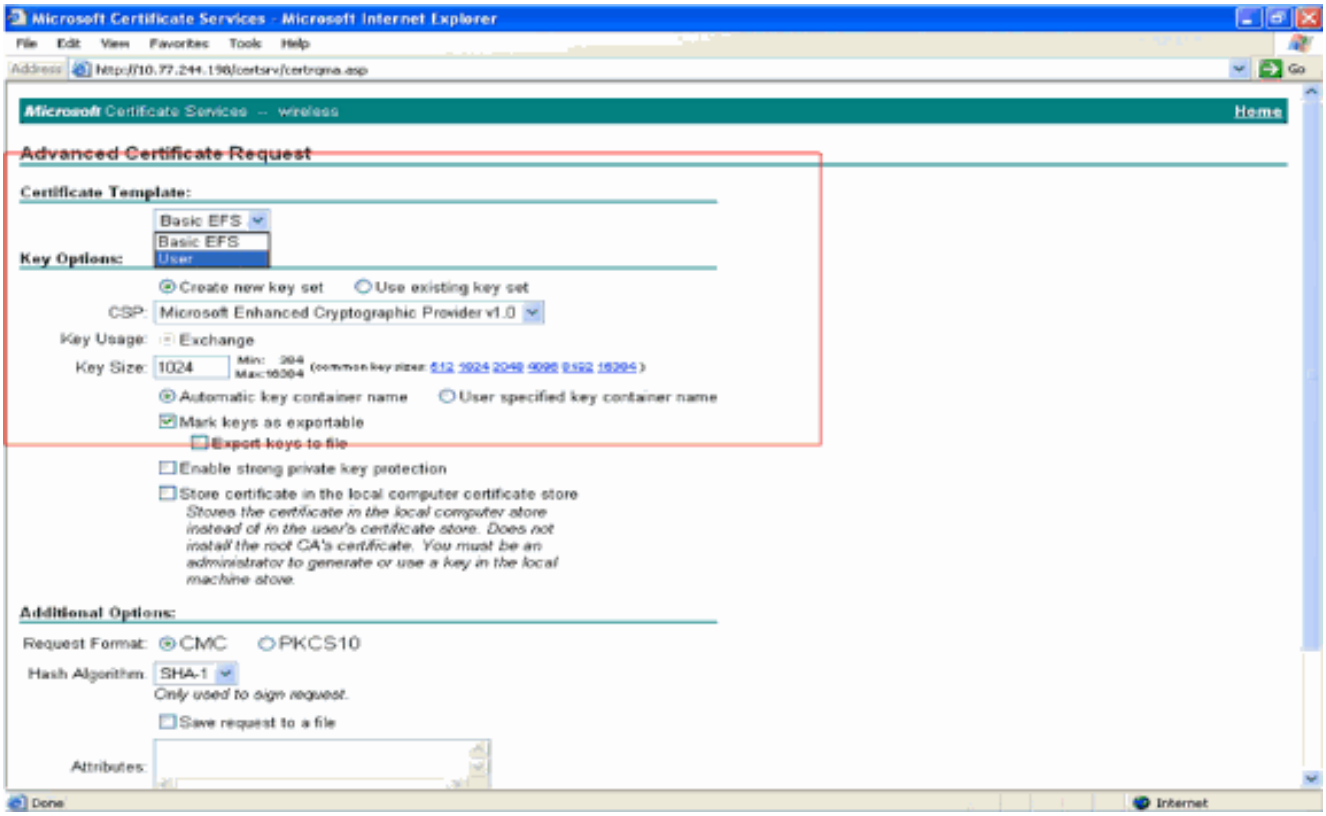
3. 在「Request a Certificate」頁面中，按一下**advanced certificate request**。



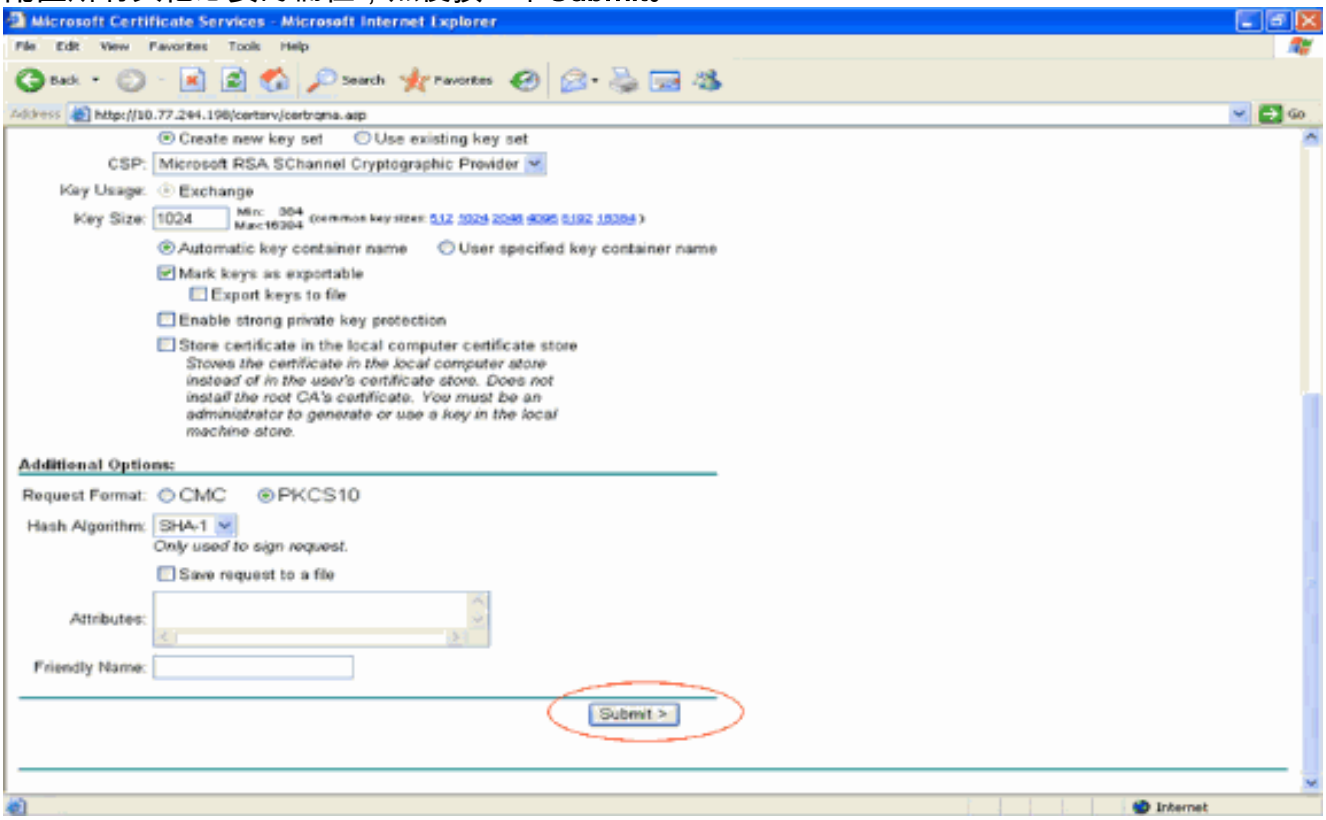
4. 在「高級證書請求」頁中，單**擊「建立」並將請求提交到此CA**。這會將您帶到「高級證書」申請表。



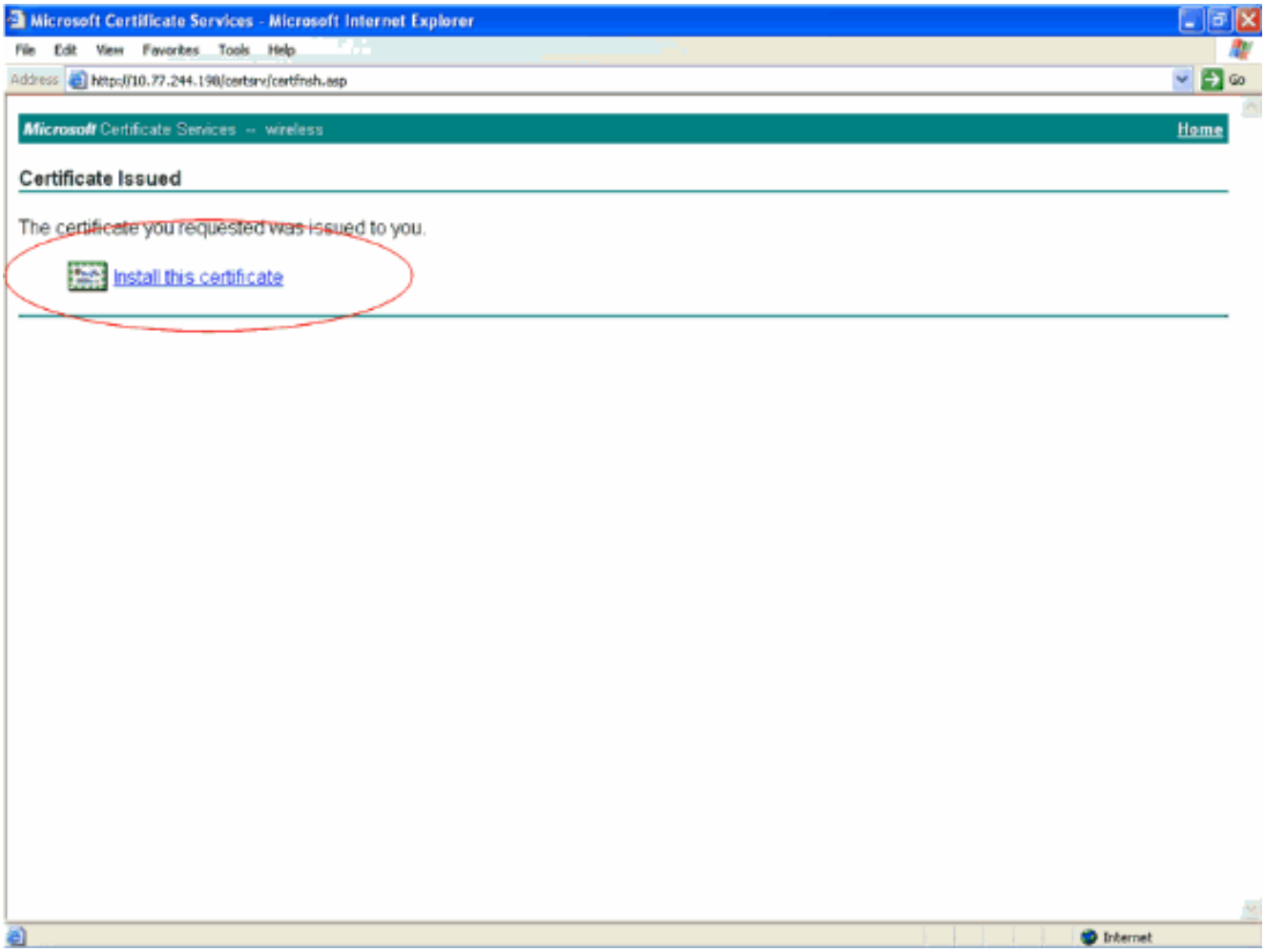
5. 在「Advanced Certificate request」表單中，從「Certificate Template」下拉選單中選擇**User**。在Key options部分下，選擇以下引數：在Key Size欄位中輸入金鑰大小。本示例使用**1024**。選中**Mark Keys as Exportable**選項。



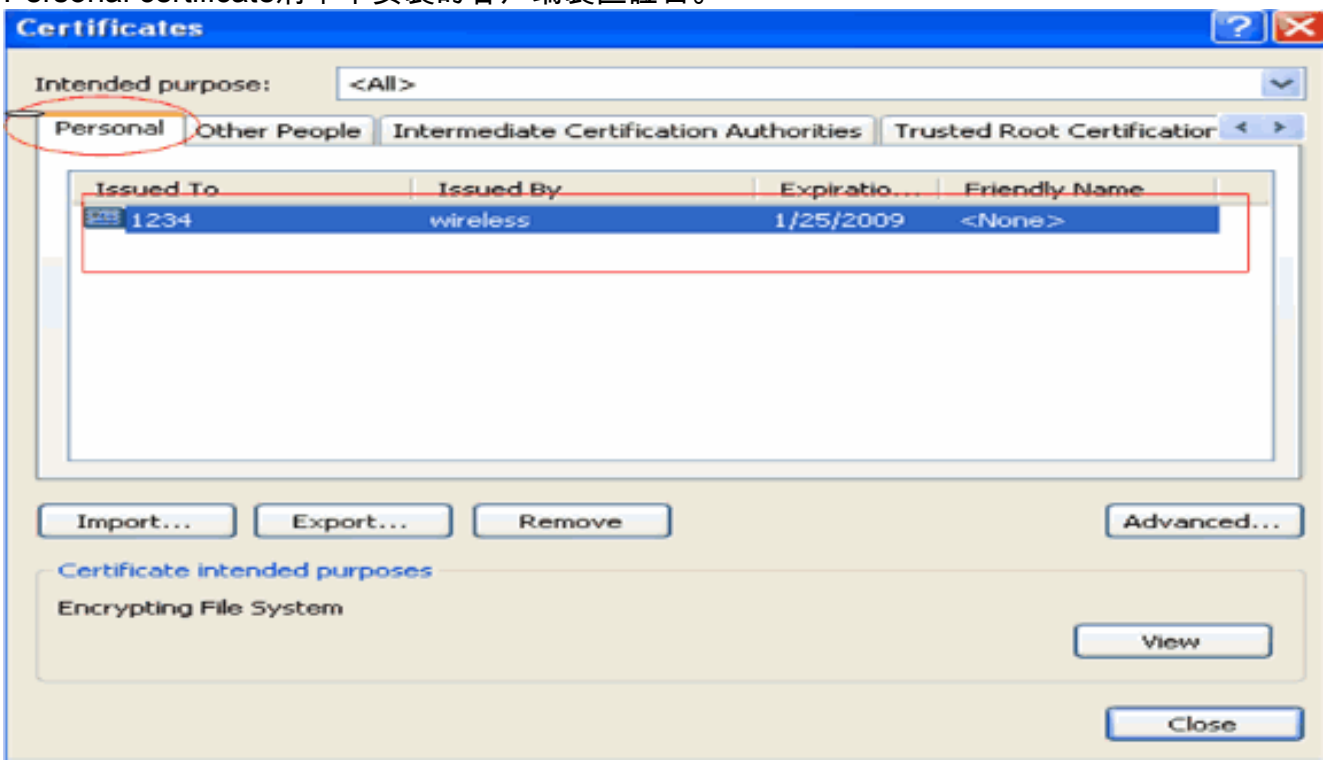
6. 配置所有其他必要的欄位，然後按一下**Submit**。



7. 現在將根據請求生成客戶端的裝置證書。按一下「**Install the certificate**」，將憑證安裝到憑證庫中。



8. 您應該能夠找到客戶端的IE瀏覽器上**Tools > Internet Options > Content > Certificates**下的Personal certificate清單中安裝的客戶端裝置證書。

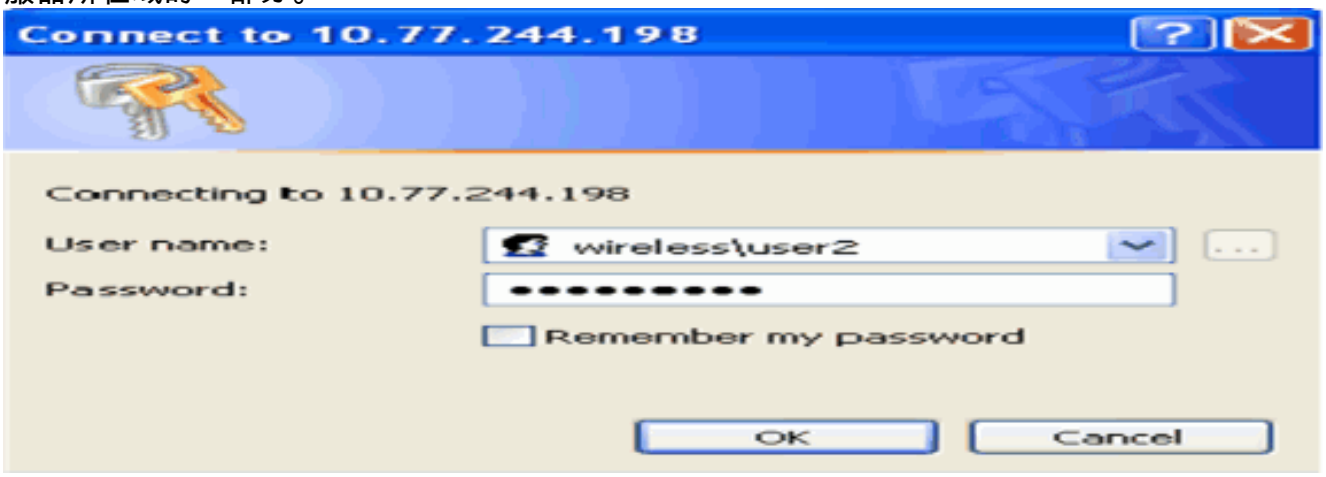


客戶端的裝置證書已安裝在客戶端上。

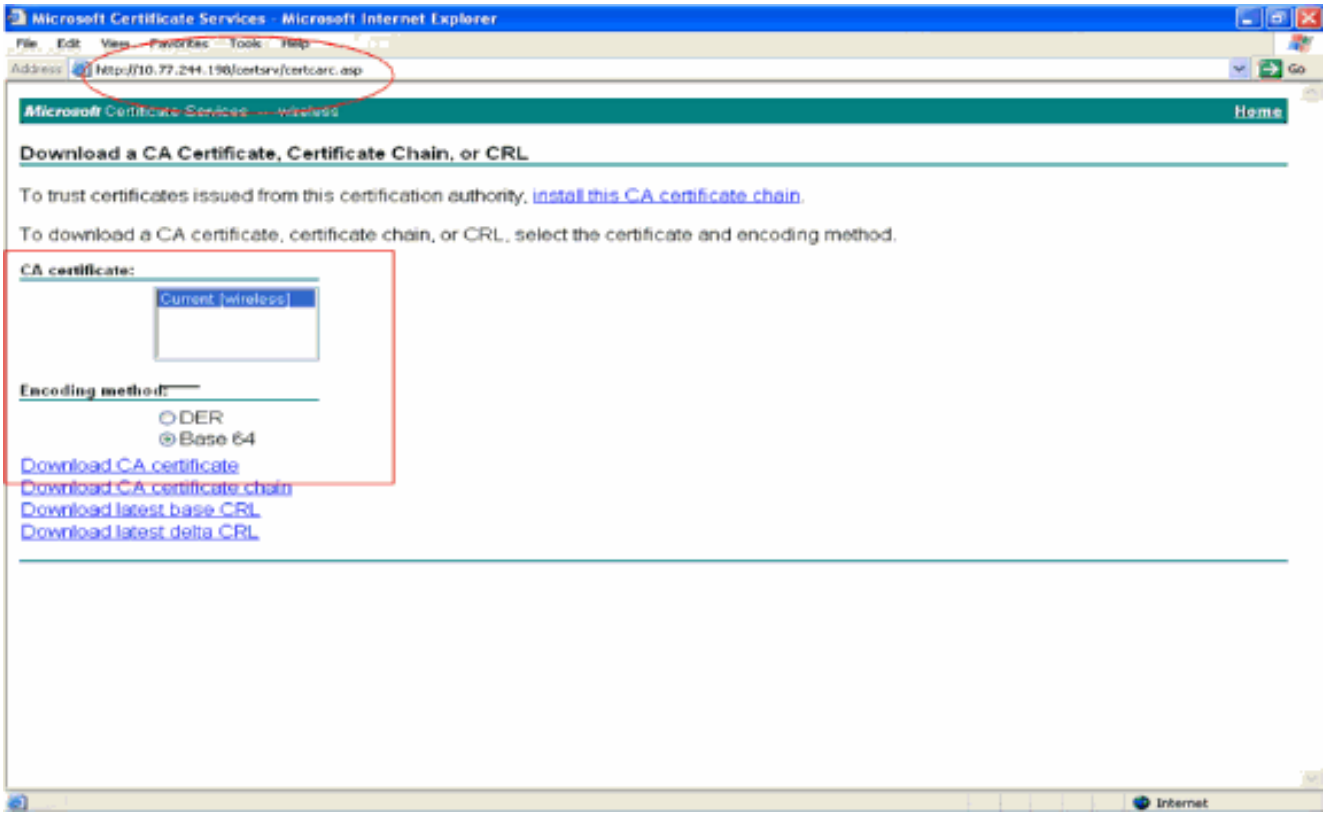
生成客戶端的根CA證書

下一步是產生使用者端的CA憑證。從客戶端PC完成以下步驟：

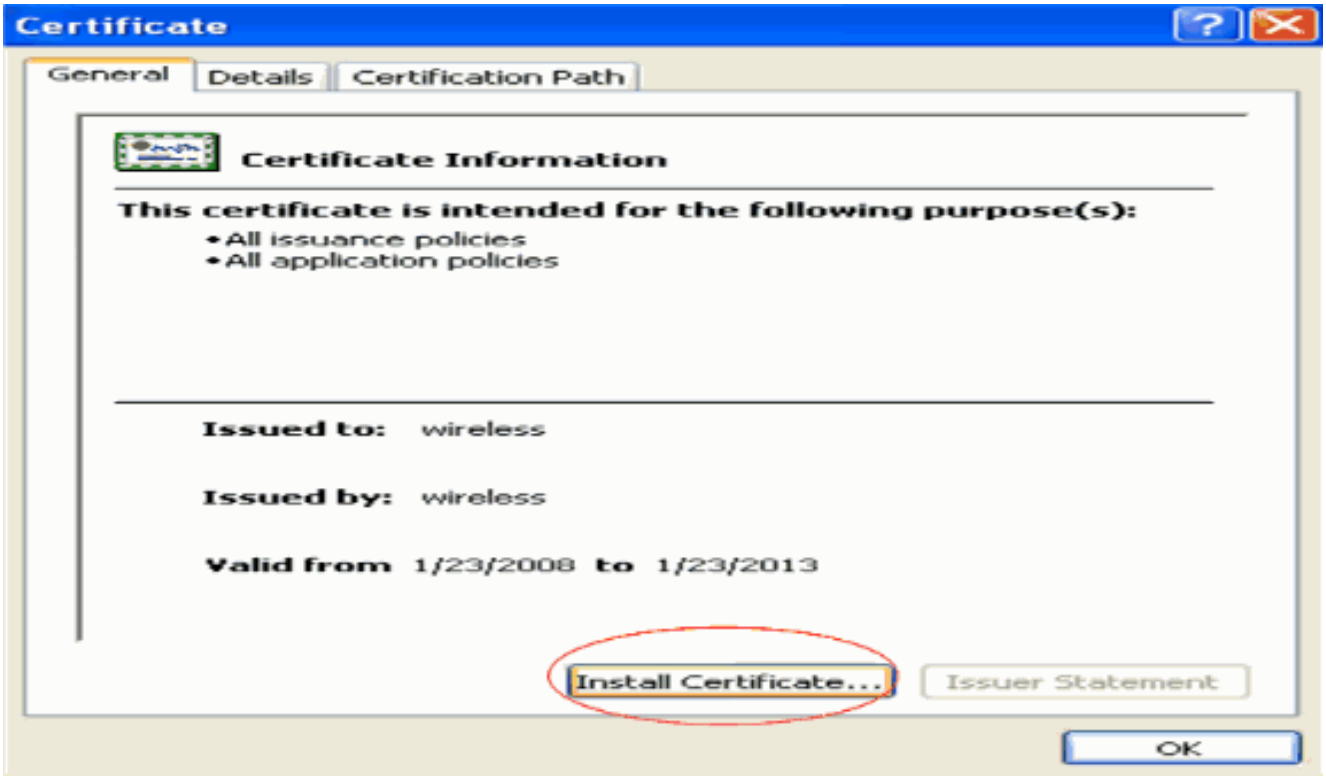
1. 從需要安裝證書的客戶端轉到**http://<CA伺服器的IP地址>/certsrv**。以域名\使用者名稱登入到CA伺服器。使用者名稱應該是使用此XP電腦的使用者的名稱，該使用者應該已經配置為CA伺服器所在域的一部分。



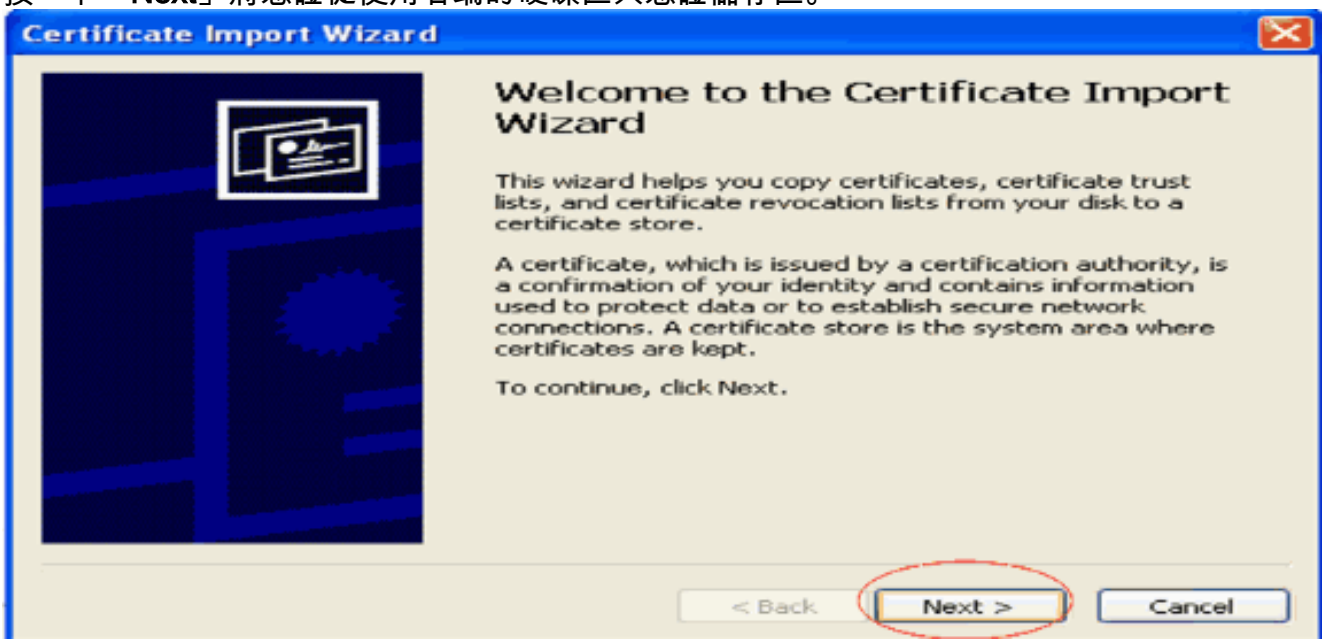
2. 在結果頁面中，您可以在**CA證書**框下看到CA伺服器上可用的當前CA證書。選擇**Base 64**作為Encoding方法。然後，按一下**Download CA certificate**，將該檔案另存為.cer檔案到客戶**端的**PC。此示例使用**rootca.cer**作為檔名。



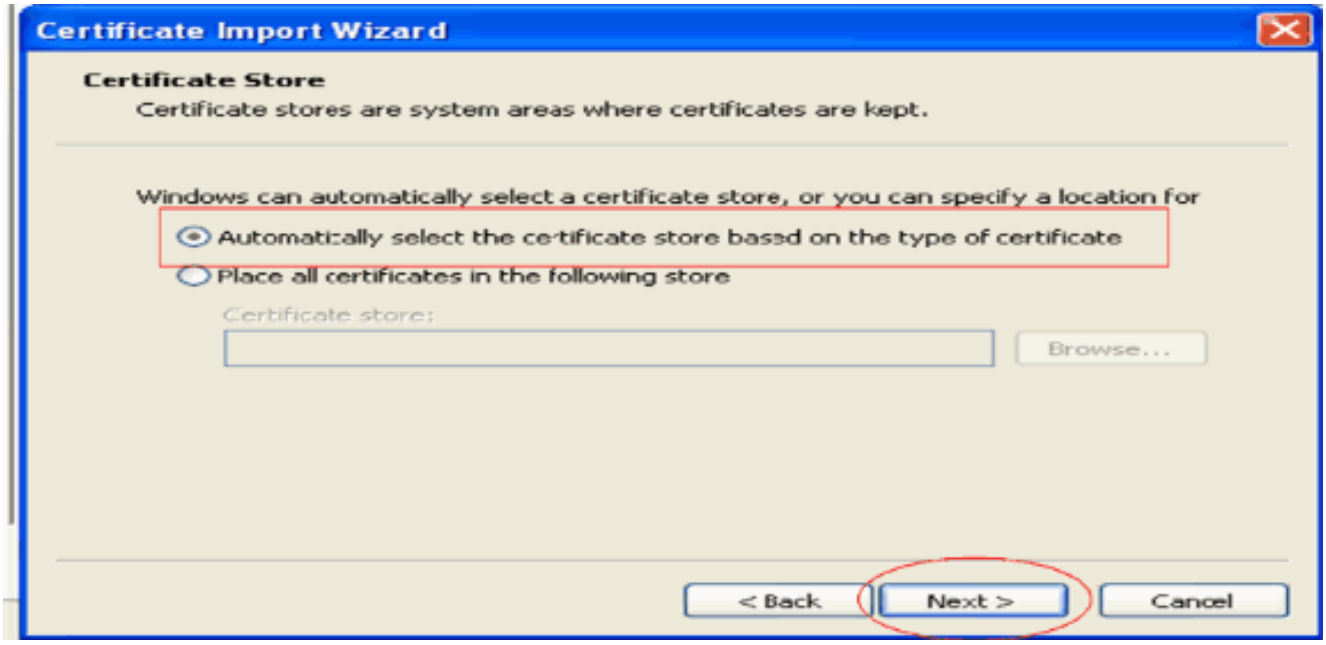
3. 接下來，將以.cer格式儲存的CA證書安裝到客戶端的證書儲存中。按兩下rootca.cer檔案，然後按一下**Install Certificate**。



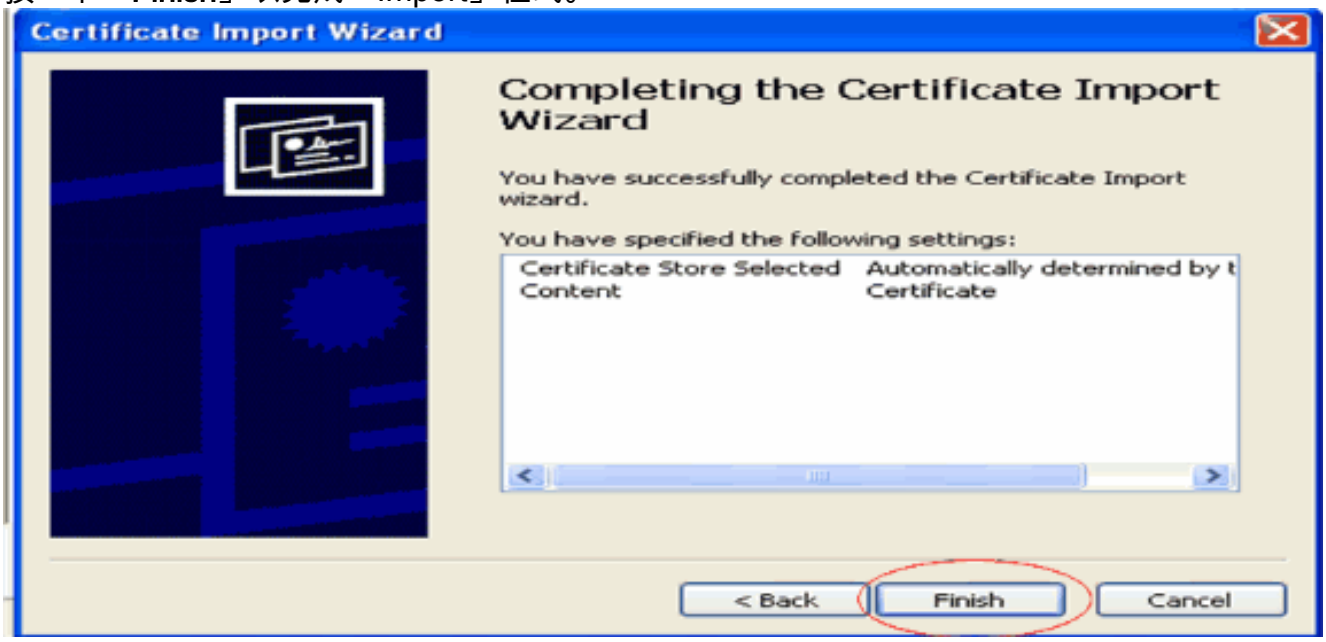
4. 按一下「Next」將憑證從使用者端的硬碟匯入憑證儲存區。



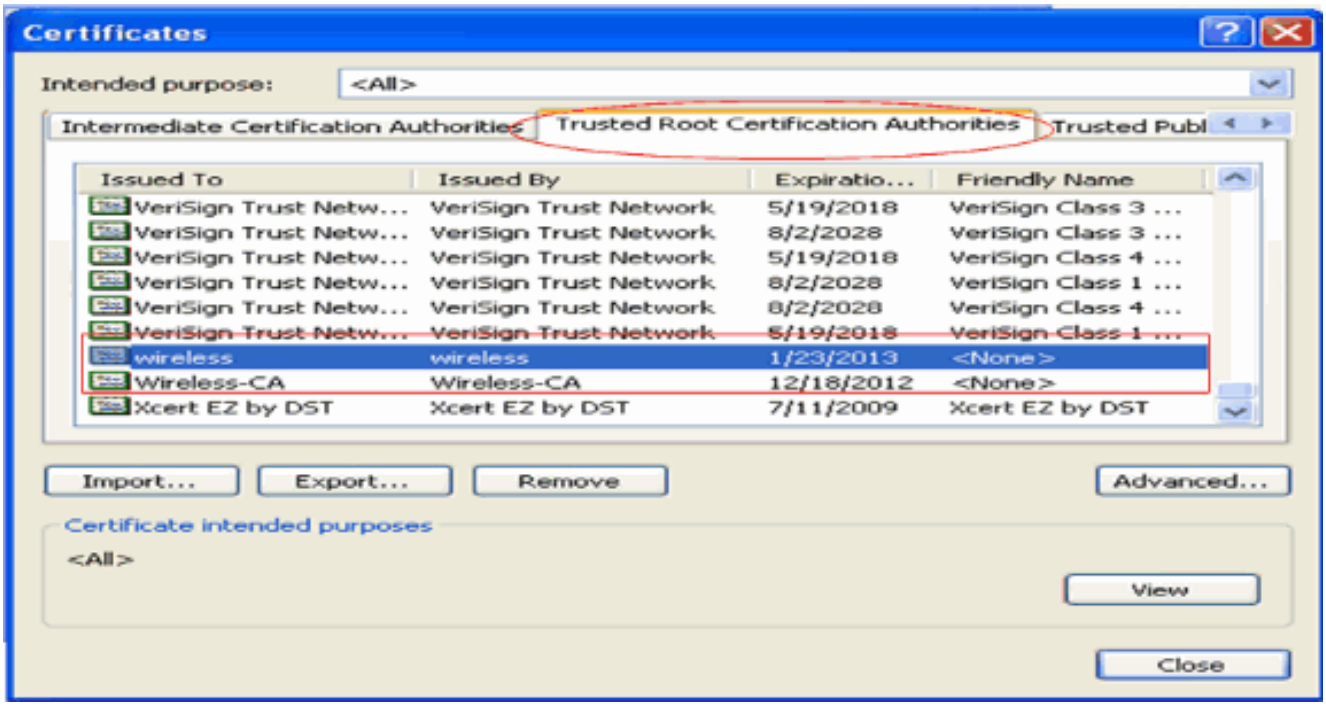
5. 選擇Automatically select the certificate store based on the type of certificate，然後按一下Next。



6. 按一下「**Finish**」以完成「Import」程式。



7. 預設情況下，CA證書安裝在客戶端IE瀏覽器中**工具> Internet選項>內容>證書**下的「受信任的根證書頒發機構」清單下。以下是範例：

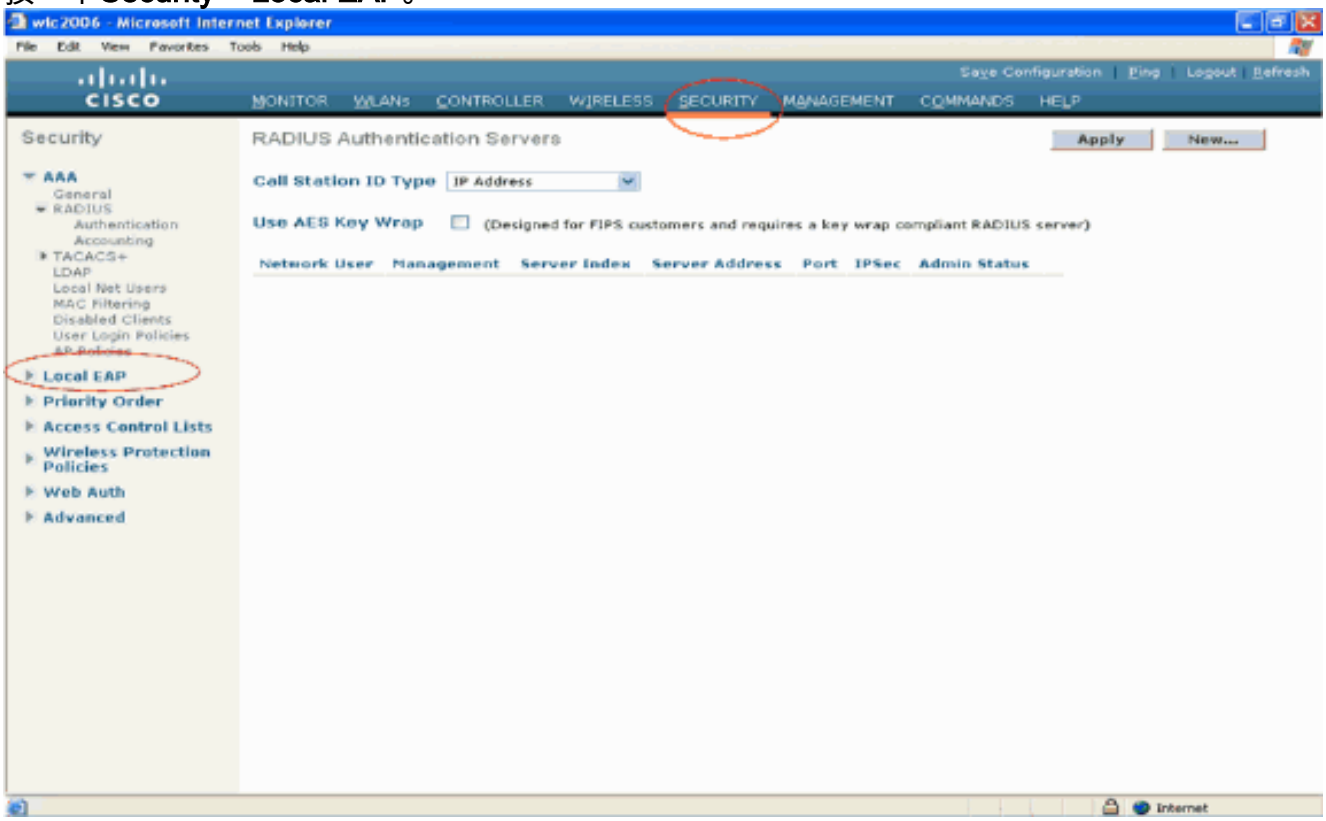


WLC和客戶端上都安裝了所需的所有證書，以進行EAP-FAST本地EAP身份驗證。下一步是將WLC配置為本地EAP身份驗證。

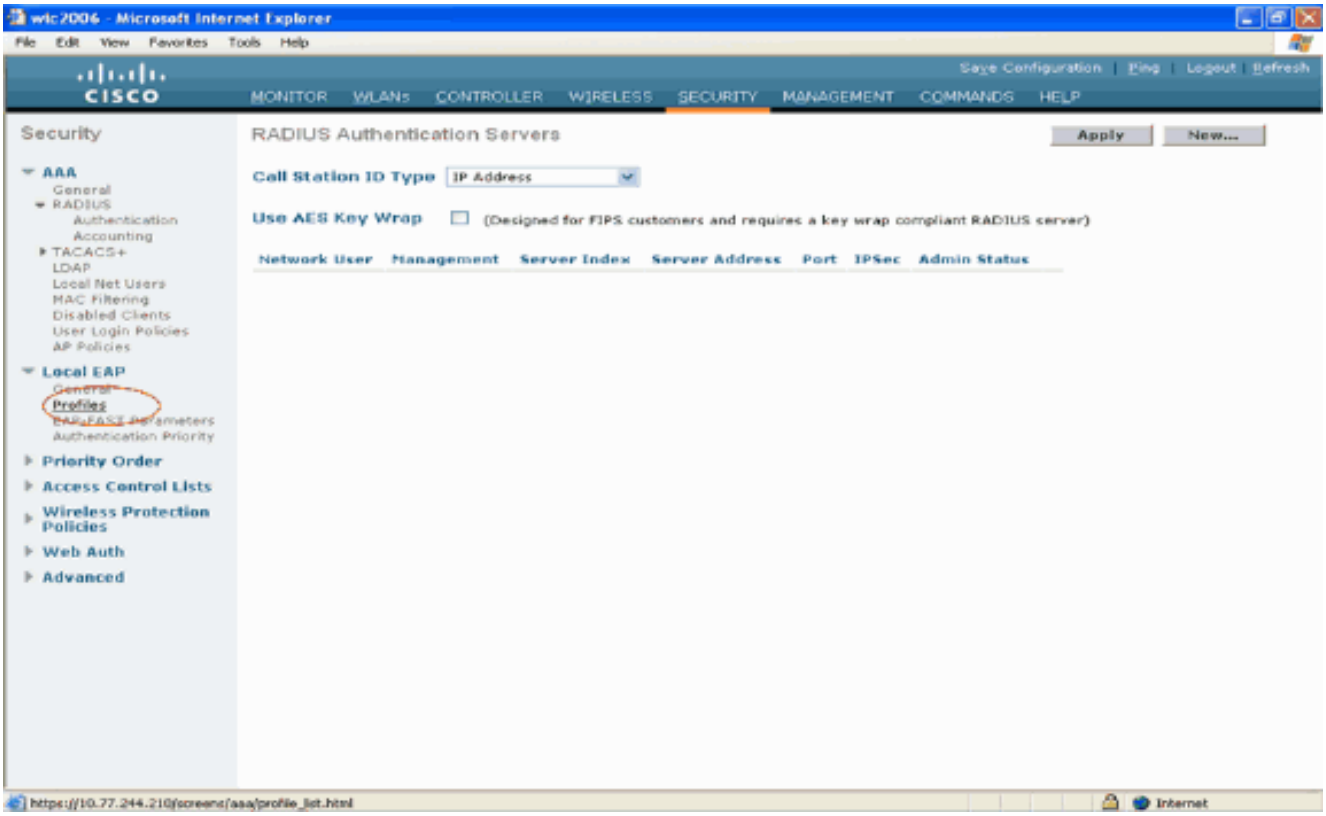
在WLC上配置本地EAP

在**WLC GUI模式**中完成以下步驟，以便在WLC上設定本地EAP驗證：

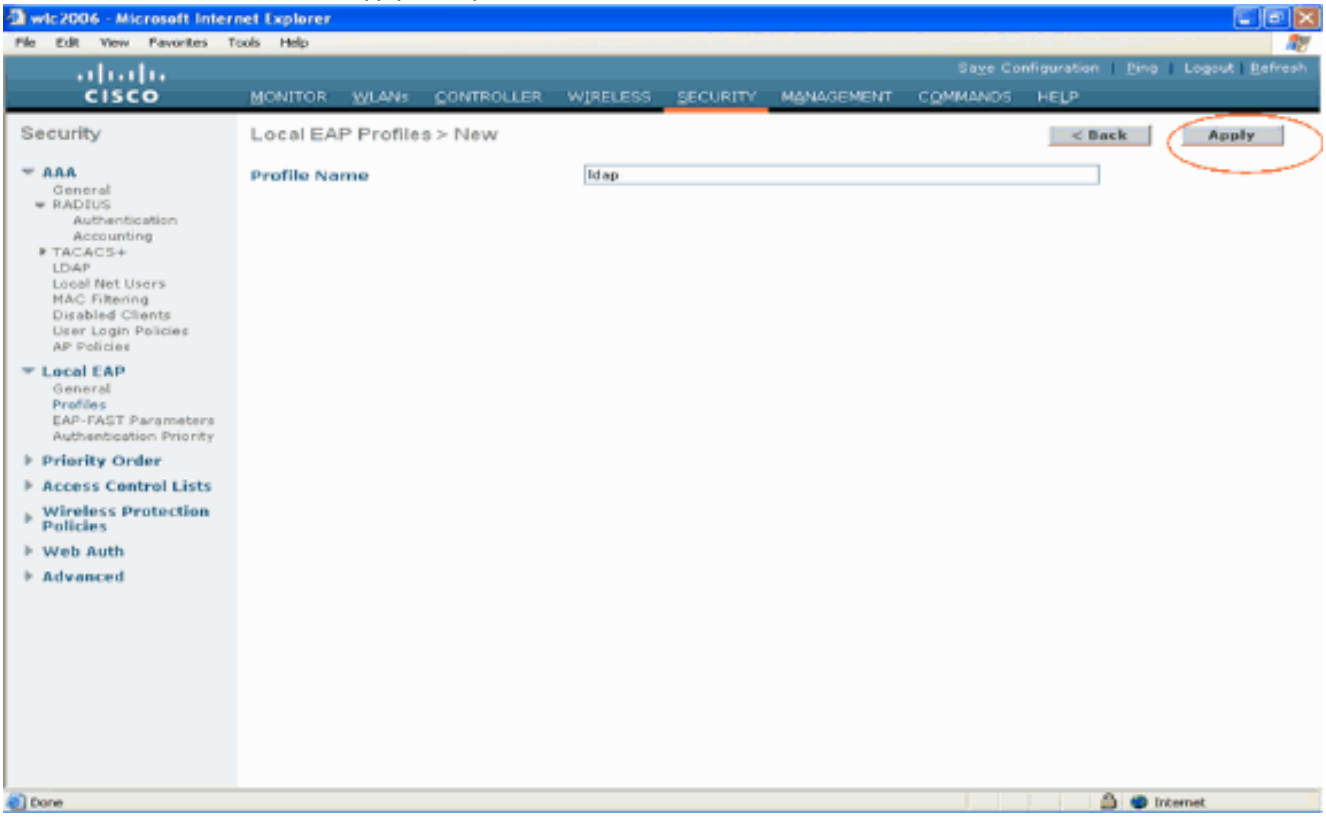
1. 按一下**Security > Local EAP**。



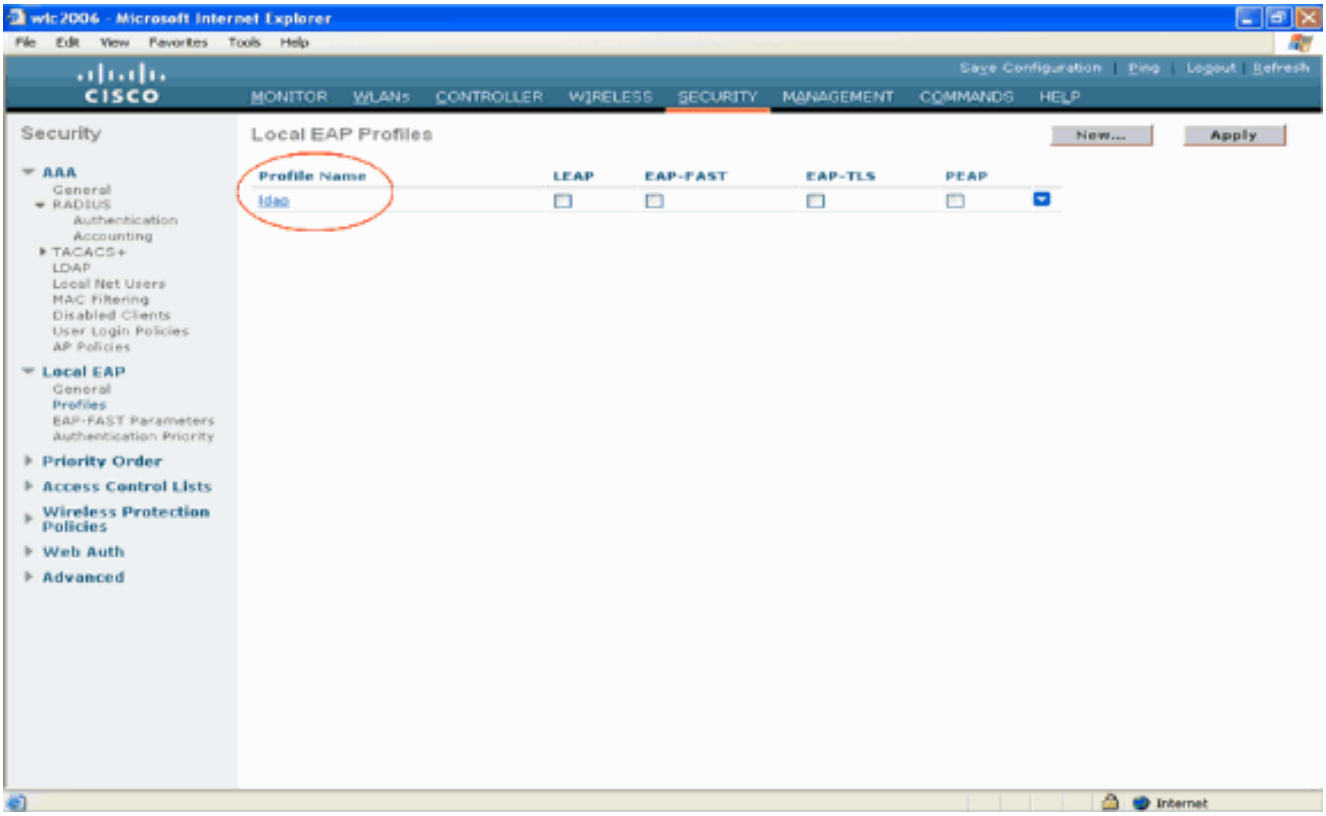
2. 在Local EAP下，按一下**Profiles**以配置本地EAP配置檔案。



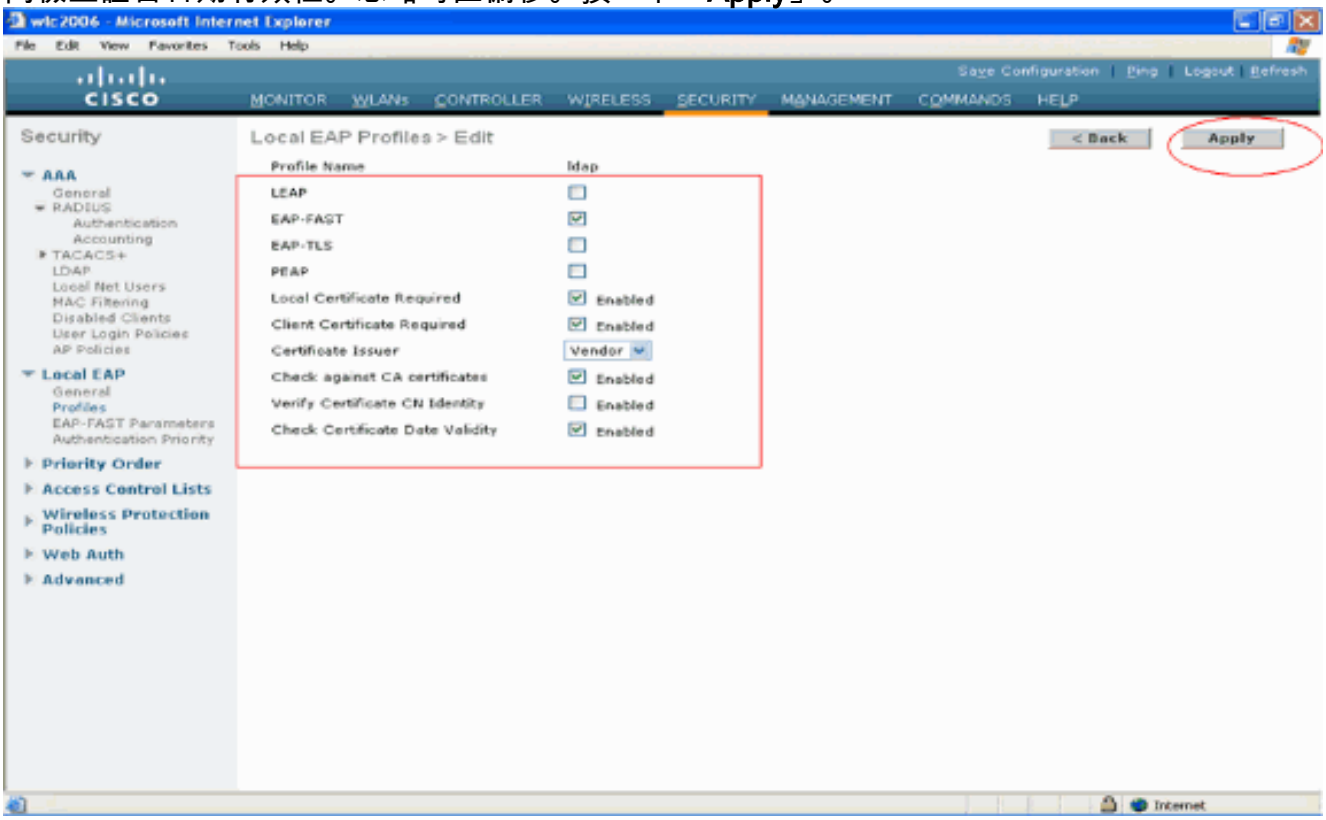
3. 按一下**New**以建立新的本地EAP配置檔案。
4. 為此配置檔案配置名稱，然後按一下**Apply**。在此示例中，配置檔名稱為**ldap**。這會將您引導到WLC上建立的本地EAP配置檔案。



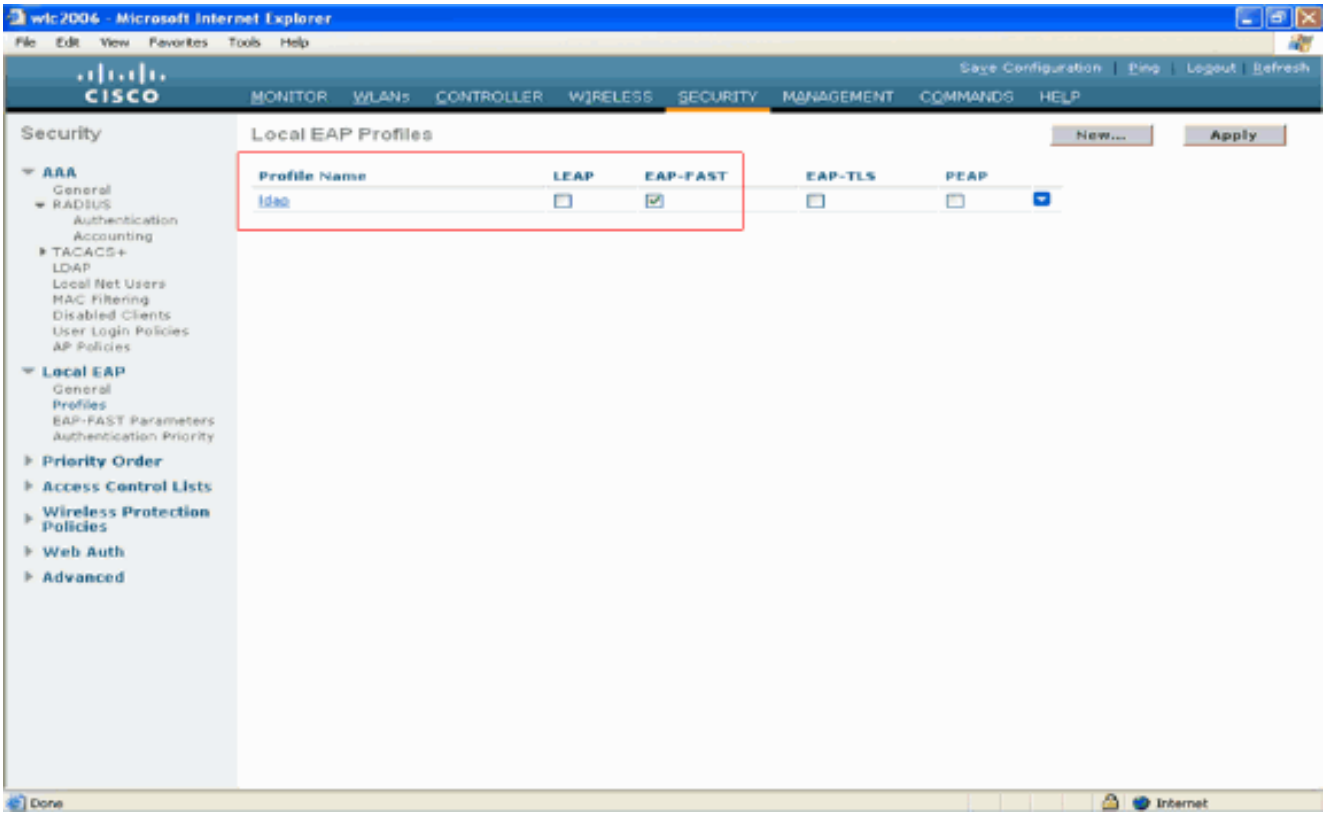
5. 按一下剛建立的**ldap**配置檔案，該配置檔案顯示在「本地EAP配置檔案」頁的「配置檔名稱」欄位下。這會將您帶到**本地EAP配置檔案>編輯**頁面。



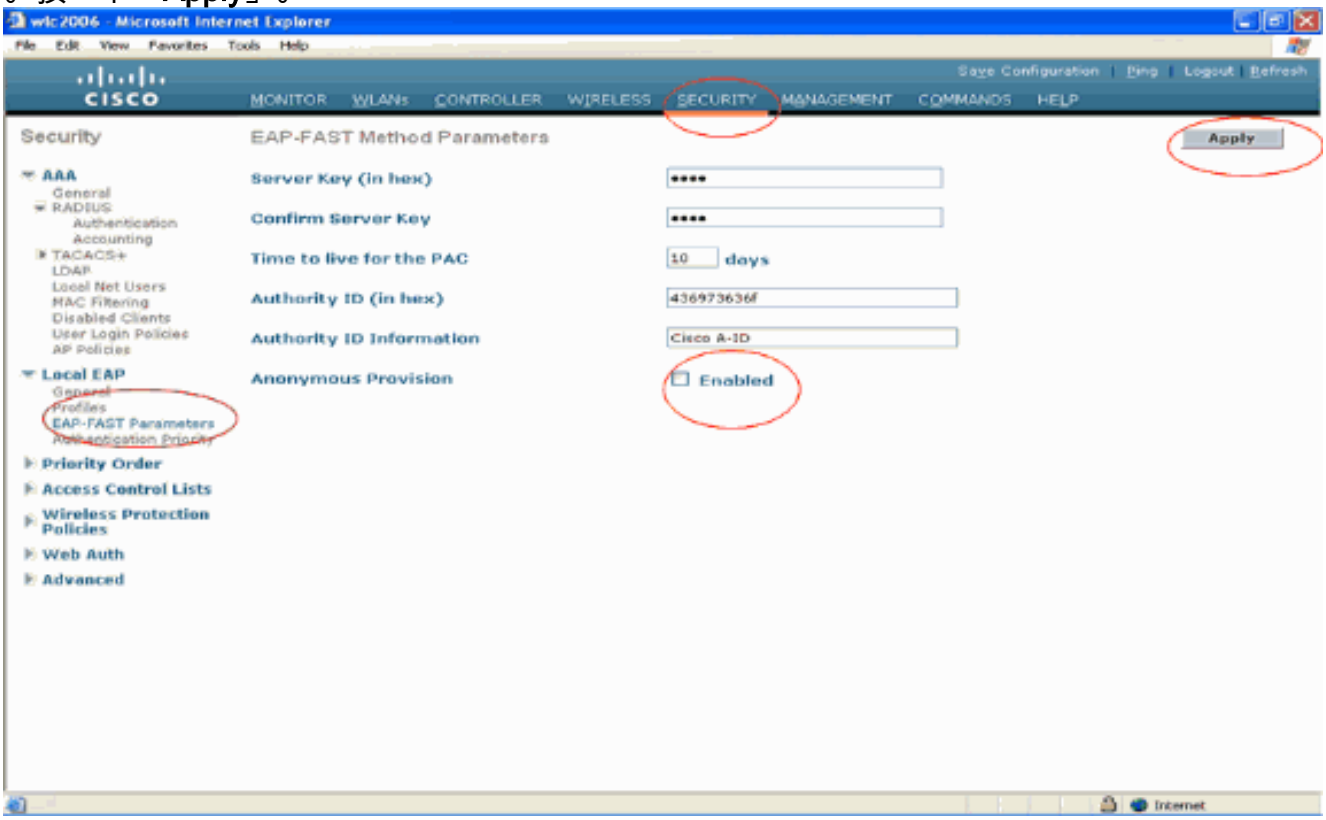
6. 在Local EAP Profiles > Edit頁面上配置特定於此配置檔案的引數。選擇EAP-FAST作為本地EAP身份驗證方法。啟用Local Certificate Required和Client Certificate Required旁邊的覈取方塊。選擇Vendor作為證書頒發者，因為本文檔使用第三方CA伺服器。啟用**檢查CA憑證**旁邊的覈取方塊，以允許根據控制器上的CA憑證驗證來自使用者端的傳入憑證。如果要對照控制器上的CA憑證的CN來驗證傳入憑證中的公用名稱(CN)，請選中Verify Certificate CN Identity覈取方塊。預設設定已禁用。若要允許控制器驗證傳入的裝置證書是否仍然有效且尚未過期，請選中Check Certificate Date Validity覈取方塊。**注意**：根據控制器上配置的當前UTC(GMT)時間檢查證書日期有效性。忽略時區偏移。按一下「Apply」。



7. 現在，在WLC上建立了採用EAP-FAST身份驗證的本地EAP配置檔案。



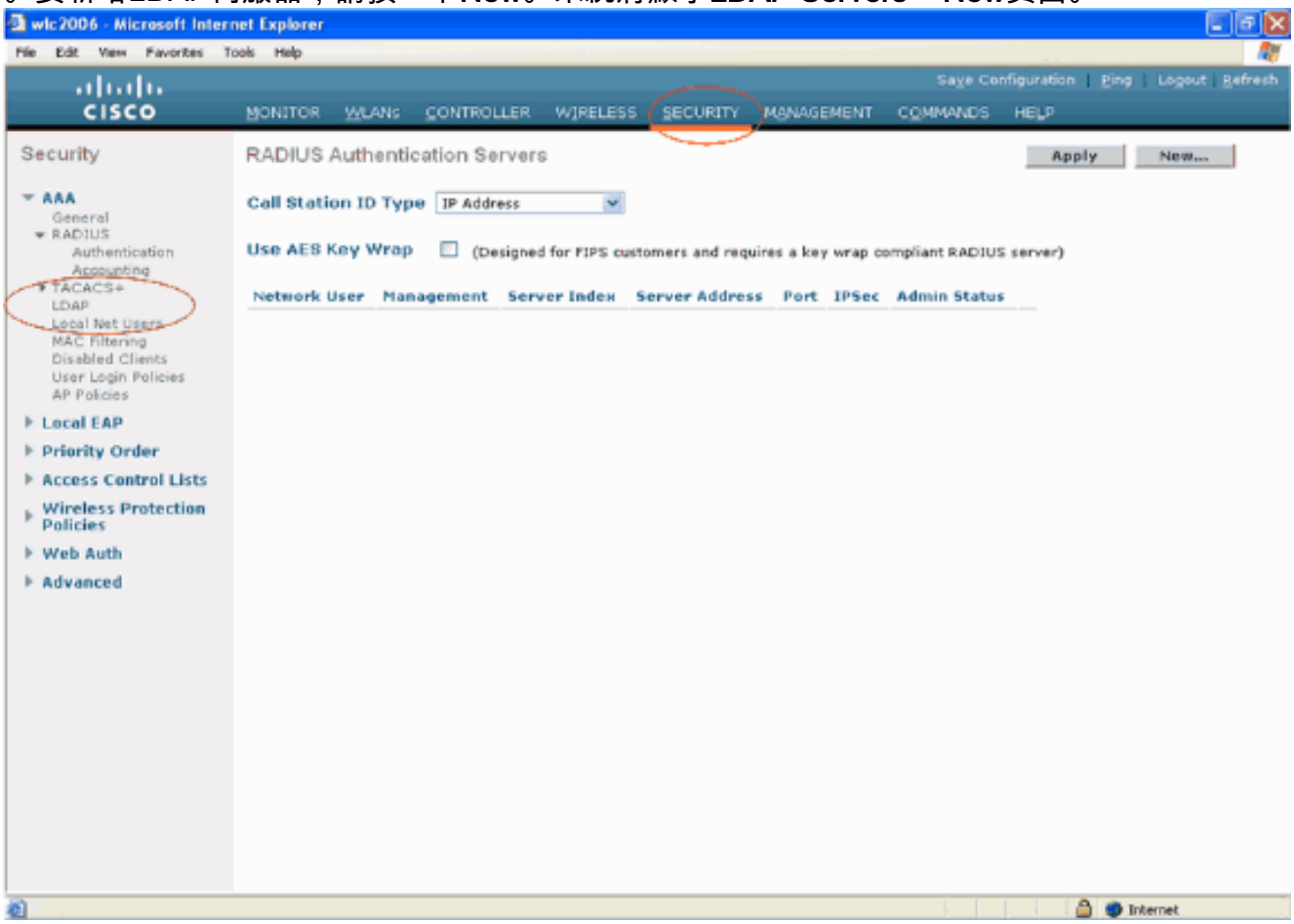
8. 下一步是在WLC上設定EAP-FAST特定引數。在WLC Security頁面中，按一下**Local EAP > EAP-FAST Parameters**以轉到EAP-FAST Method Parameters頁面。取消選中**Anonymous Provision**覈取方塊，因為此示例說明了使用證書的EAP-FAST。將所有其他引數保留為預設值。按一下「**Apply**」。



使用LDAP伺服器的詳細資訊配置WLC

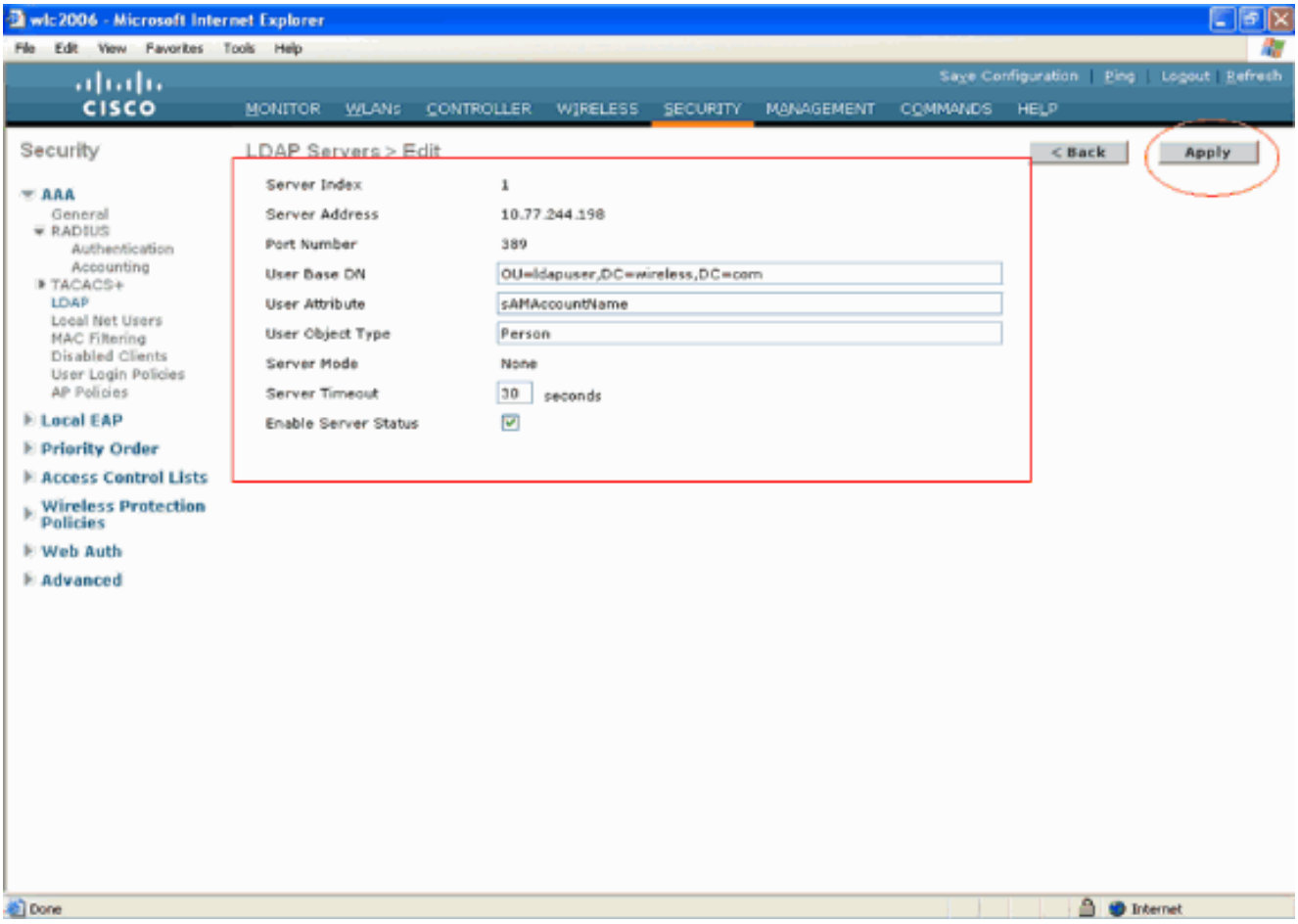
現在已使用本地EAP配置檔案和相關資訊配置WLC，下一步是使用LDAP伺服器的詳細資訊配置WLC。在WLC上完成以下步驟：

1. 在WLC的**Security**頁面中，從左側任務窗格中選擇**AAA > LDAP**，以轉到LDAP伺服器配置頁面。要新增LDAP伺服器，請按一下**New**。系統將顯示**LDAP Servers > New**頁面。



2. 在「LDAP伺服器編輯」頁中，指定LDAP伺服器的詳細資訊，例如LDAP伺服器的IP地址、埠號、啟用伺服器狀態等。從**Server Index(Priority)**下拉框中選擇一個數字，以指定此伺服器相對於任何其他已配置的LDAP伺服器的優先順序順序。最多可以配置17台伺服器。如果控制器無法連線到第一個伺服器，便會嘗試清單中的第二個伺服器，以此類推。在**Server IP Address**欄位中輸入LDAP伺服器的IP地址。在**Port Number**欄位中輸入LDAP伺服器的TCP埠號。有效範圍為1至65535，預設值為**389**。在**User Base DN**欄位中，輸入包含所有使用者清單的LDAP伺服器子樹的可分辨名稱(DN)。例如，ou=組織單位、.ou=next organizational unit和o=corporation.com。如果包含使用者的樹是基本DN，請輸入o=corporation.com或dc=corporation， dc=com。在本示例中，使用者位於Organizational Unit(OU)**ldapuser**下，該使用者又建立為**Wireless.com域的一部**分。使用者基礎DN應指向使用者資訊（根據EAP-FAST身份驗證方法的使用者憑證）所在的完整路徑。在本示例中，使用者位於基本DN OU=ldapuser、DC=Wireless、DC=com下。有關OU及使用者配置的更多詳細資訊，請參閱本文檔的在域控制器上建立使用者部分。在「**User Attribute**」欄位中，輸入包含使用者名稱的使用者記錄中的屬性名稱。在**User Object Type**欄位中，輸入將記錄標識為使用者的LDAP objectType屬性的值。通常，使用者記錄有若干objectType屬性值，其中某些值對於使用者是唯一的，而某些值則與其他對象型別共用。**注意：**您可以使用LDAP瀏覽器實用程式（作為Windows 2003支援工具的一部分）從目錄伺服器獲取這兩個欄位的值。**此Microsoft LDAP瀏覽器工具稱為LDP。**藉助此工具，您可以瞭解此特定使用者的「使用者基礎DN」、「使用者屬性」和「使用者對象型別」欄位。有關使用LDP瞭解這些使用者特定屬性的詳細資訊，請參閱本文檔的使用LDP識別使用者屬性部分。如果希望所有LDAP事務使用安全TLS隧道，請從「伺服器模式」下拉框中選擇**安全**。否則，請選擇**None**，這是預設設定。在**Server Timeout**欄位中，輸入重新傳輸之間的秒數。有效範圍為2到30秒，預設值為2秒。選中**Enable Server Status**覈取方塊以啟用此LDAP伺服器，或取消選中以禁用。預設值已停用。按一下**Apply**提交更改。以下是已使用以下資訊設定的範例

:

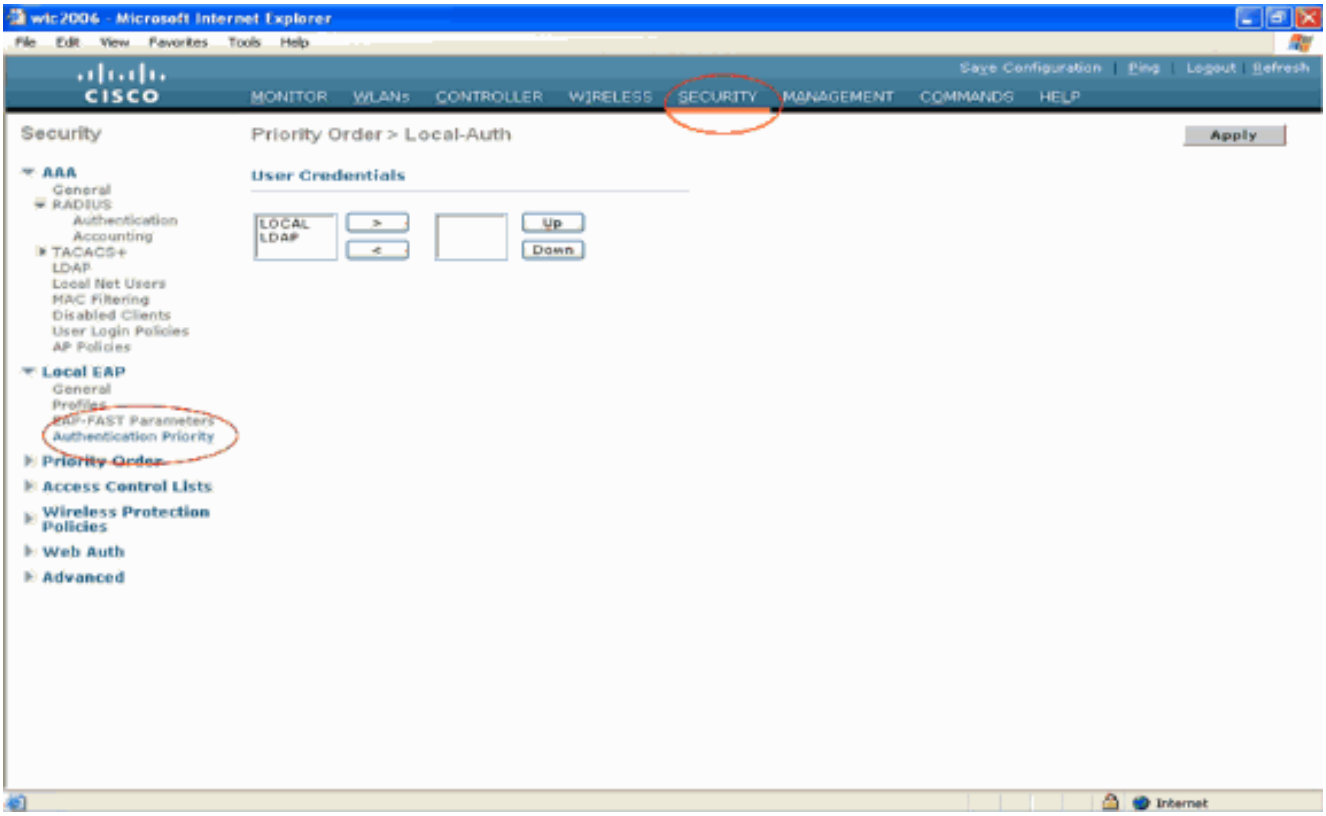


現在已在WLC上配置有關LDAP伺服器的詳細資訊，下一步是將LDAP配置為優先順序後端資料庫，以便WLC首先檢視LDAP資料庫以獲取使用者憑據，而不是任何其他資料庫。

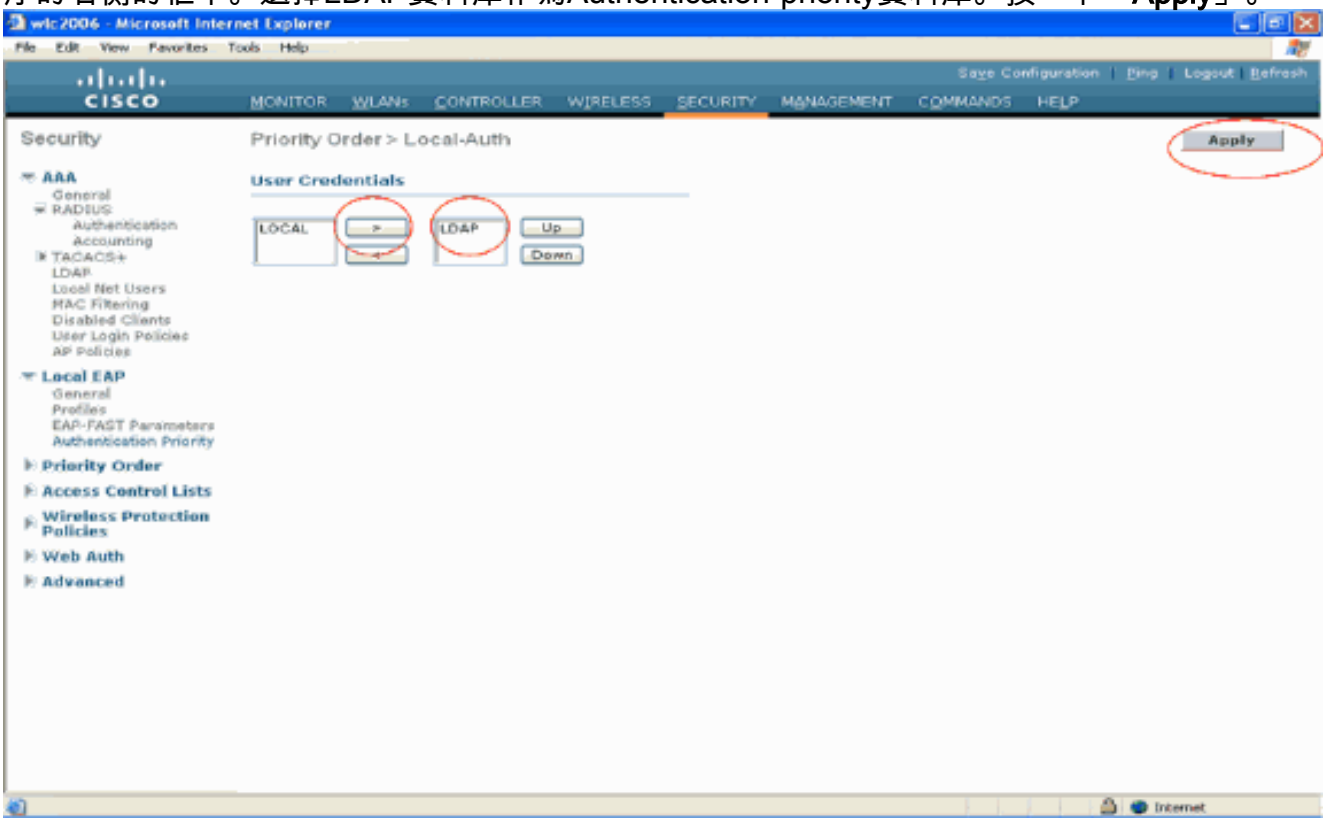
將LDAP配置為優先順序後端資料庫

在WLC上完成以下步驟，以便將LDAP配置為優先順序後端資料庫：

1. 在Security頁面中，按一下**Local EAP > Authentication Priority**。在Priority Order > Local-Auth頁面中，您可以找到兩個可以儲存使用者憑據的資料庫（Local和LDAP）。要將LDAP作為優先順序資料庫，請從左側使用者憑據框中選擇**LDAP**，然後按一下 **>**按鈕將LDAP移動到右側優先順序順序框中。



2. 此示例清楚地說明在左側框中選擇了LDAP，並且選中了>按鈕。因此，LDAP移到決定優先順序的右側的框中。選擇LDAP資料庫作為Authentication-priority資料庫。按一下「**Apply**」。

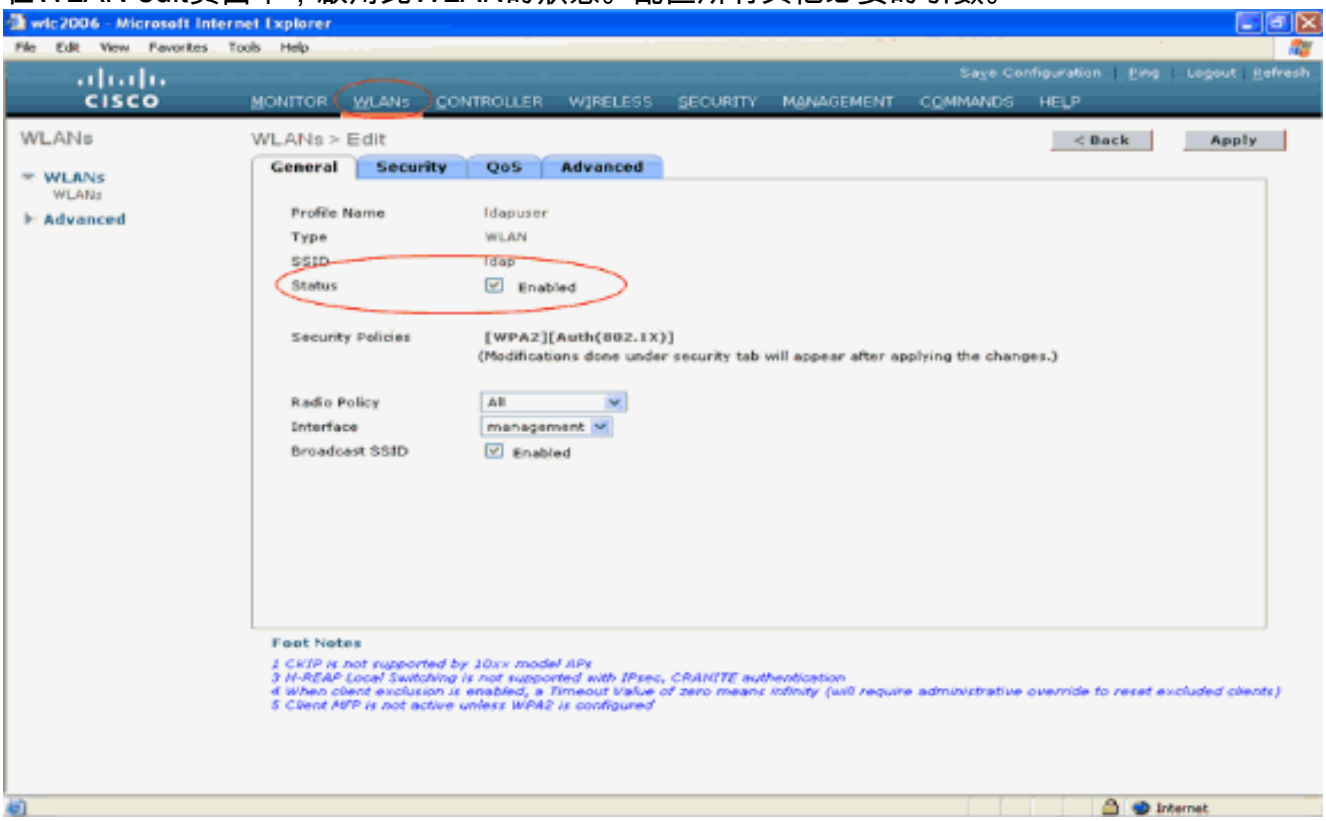


注意：如果LDAP和LOCAL都顯示在右側的「使用者身份證明」框中，其中LDAP位於頂部，LOCAL位於底部，則Local EAP會嘗試使用LDAP後端資料庫對客戶端進行身份驗證，並且如果LDAP伺服器無法訪問，則故障轉移到本地使用者資料庫。如果找不到該使用者，則會拒絕身份驗證嘗試。如果LOCAL位於頂部，Local EAP將嘗試僅使用本地使用者資料庫進行身份驗證。它不會故障切換到LDAP後端資料庫。

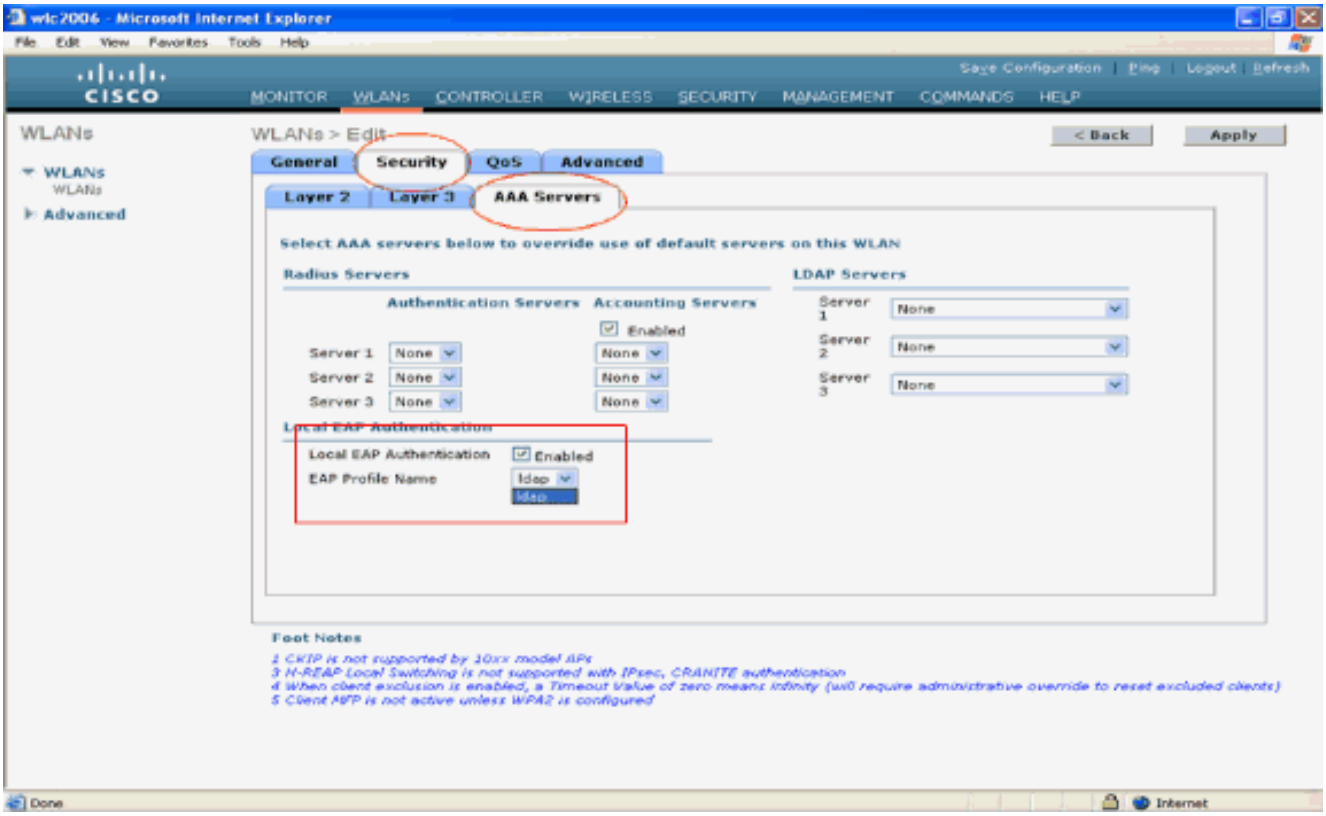
使用本地EAP身份驗證在WLC上配置WLAN

WLC的最後一步是配置一個WLAN，該WLAN使用Local EAP作為其身份驗證方法，LDAP作為其後端資料庫。執行以下步驟：

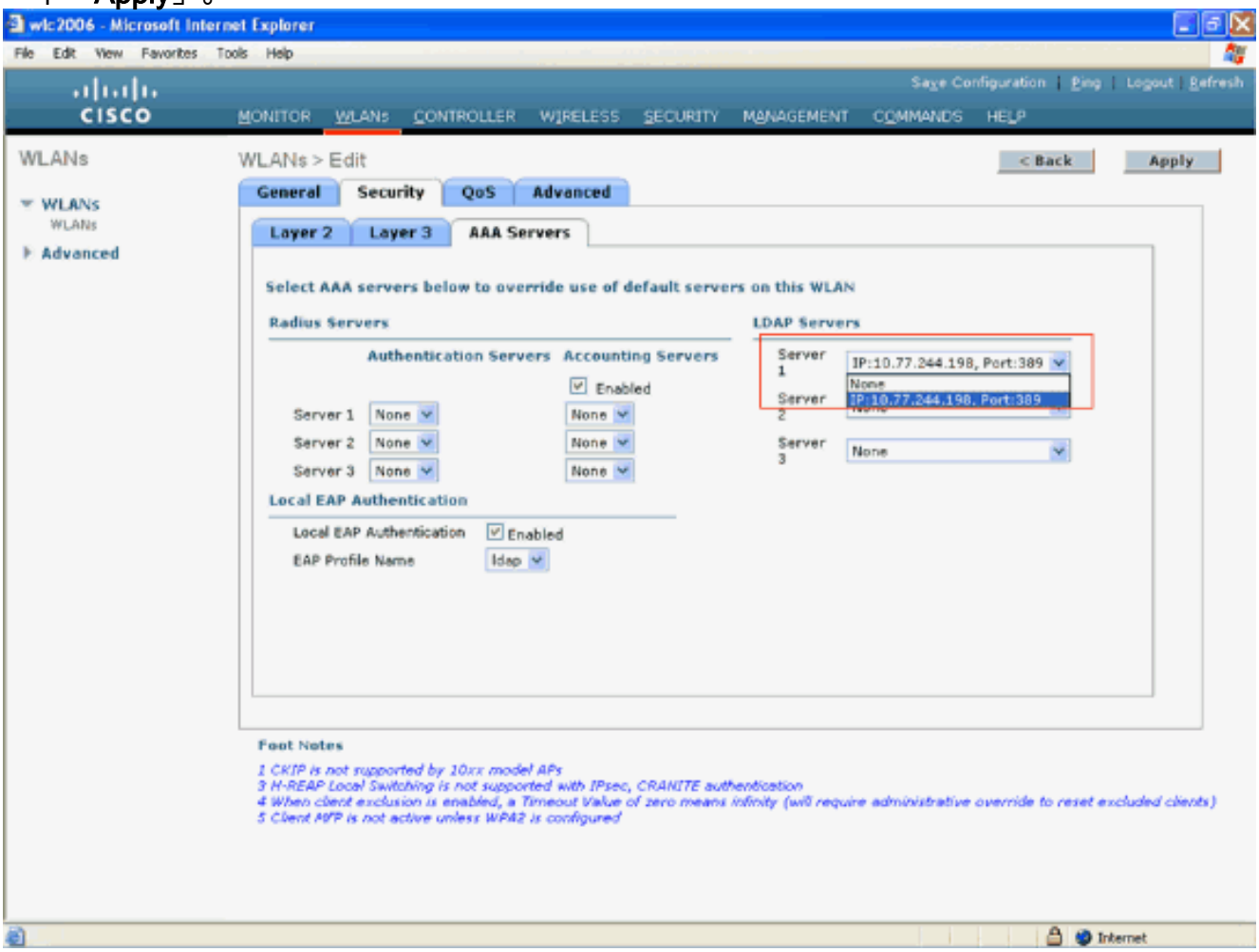
1. 在「Controller Main（控制器主選單）」中，按一下「**WLANs**」以進入WLANs配置頁面。在WLANs頁面中，按一下**New**以建立一個新的WLAN。本示例建立一個新的WLAN **ldap**。按一下「**Apply**」。下一步是在「WLANs」>「Edit」頁面中設定WLAN引數。
2. 在WLAN edit頁面中，啟用此WLAN的狀態。配置所有其他必要的引數。



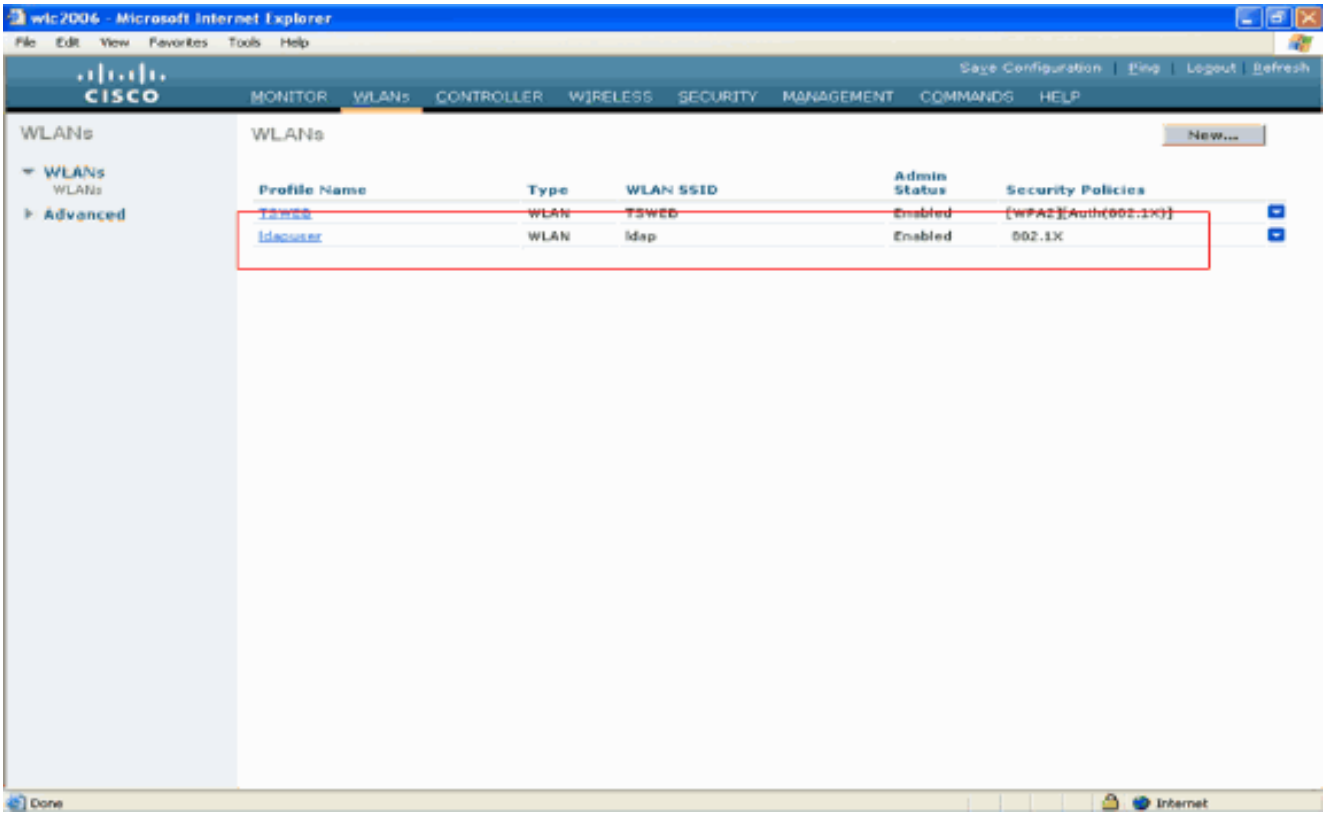
3. 按一下「**Security**」以設定此WLAN的安全相關引數。此示例將第2層安全用作802.1x和104位動態WEP。**注意：**本文檔使用帶動態WEP的802.1x作為示例。建議使用更安全的身份驗證方法，例如WPA/WPA2。
4. 在WLAN Security配置頁面中，按一下**AAA servers選項**卡。在AAA servers頁面中，啟用Local EAP Authentication方法，並從與EAP配置檔名稱引數對應的下拉框中選擇**ldap**。這是在本示例中建立的本地EAP配置檔案。



5. 從下拉框中選擇LDAP伺服器（之前在WLC上配置）。確保可以從WLC訪問LDAP伺服器。按一下「**Apply**」。



6. 已在WLC上配置新的WLAN ldaphas。此WLAN使用本地EAP身份驗證（本例中為EAP-FAST）對客戶端進行身份驗證，並查詢LDAP後端資料庫以進行客戶端憑據驗證。



配置LDAP伺服器

現在，在WLC上配置了本地EAP，下一步是配置LDAP伺服器，該伺服器用作後端資料庫，以便在證書驗證成功時驗證無線客戶端。

配置LDAP伺服器的第一步是在LDAP伺服器上建立使用者資料庫，以便WLC可以查詢此資料庫以驗證使用者。

在域控制器上建立使用者

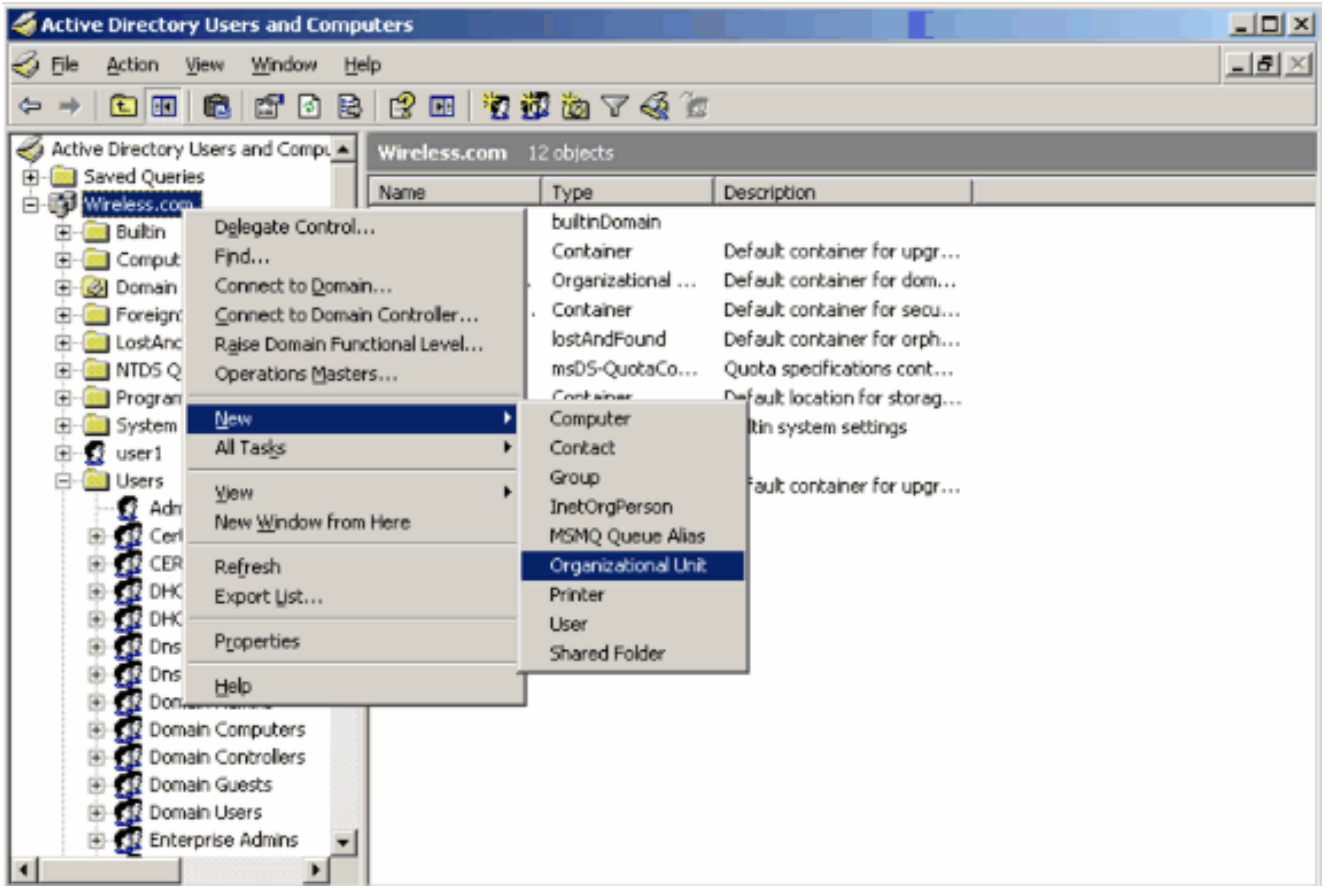
在本示例中，將建立新的OU **ldapuser**，並在此OU下建立使用者**user2**。通過配置此使用者以進行LDAP訪問，WLC可以查詢此LDAP資料庫以進行使用者身份驗證。

本示例中使用的域是**wireless.com**。

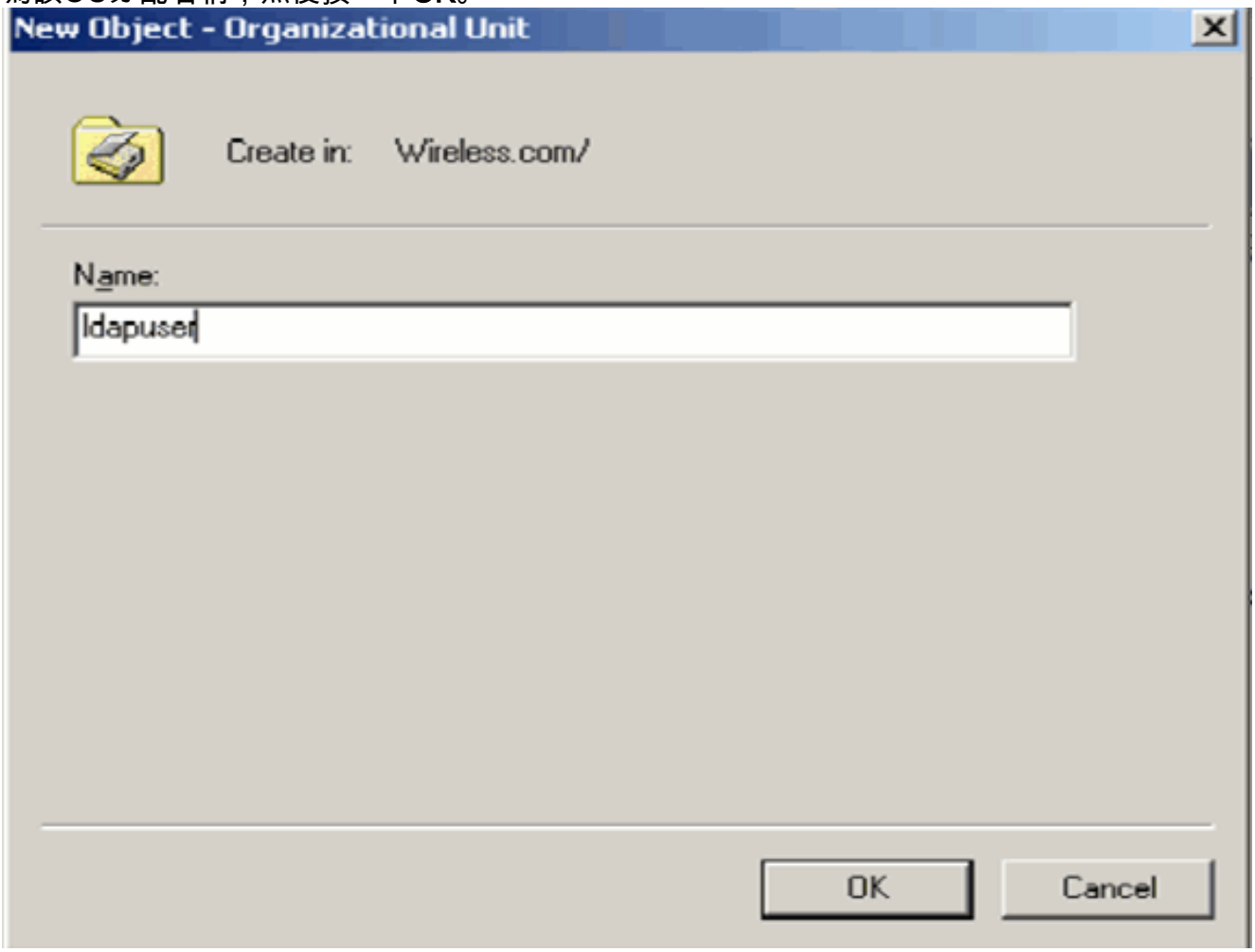
在OU下建立使用者資料庫

本節介紹如何在您的域中建立新的OU並在此OU上建立新使用者。

1. 在域控制器中，按一下**開始>程式>管理工具> Active Directory使用者和電腦**，以啟動**Active Directory使用者和電腦**管理控制檯。
2. 按一下右鍵您的域名(本例中為wireless.com)，然後從上下文選單中選擇**New > Organizational Unit**以建立新的OU。

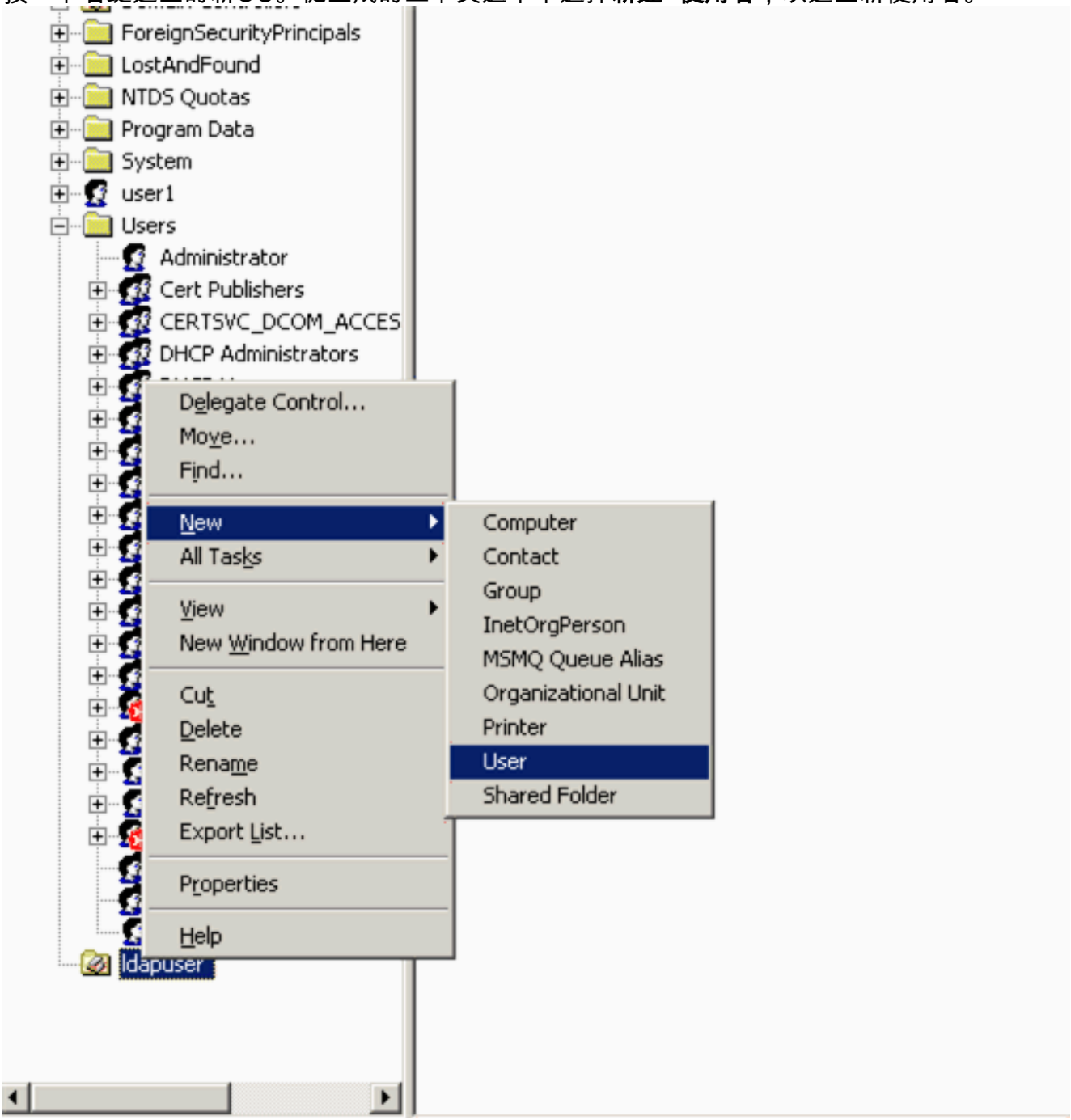


3. 為該OU分配名稱，然後按一下**OK**。

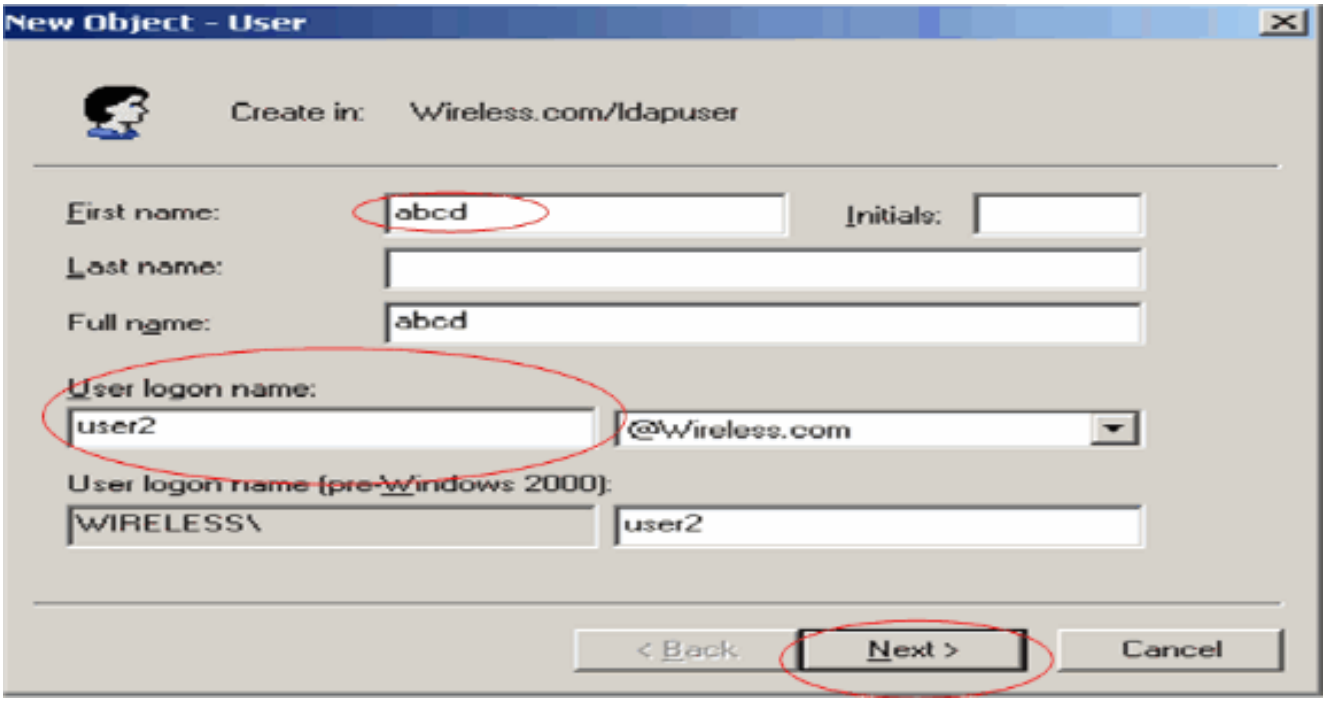


現在，在LDAP伺服器上建立了新的OU **ldapuser**，下一步是在此OU下建立**user2**。為了達成此目的，請完成以下步驟：

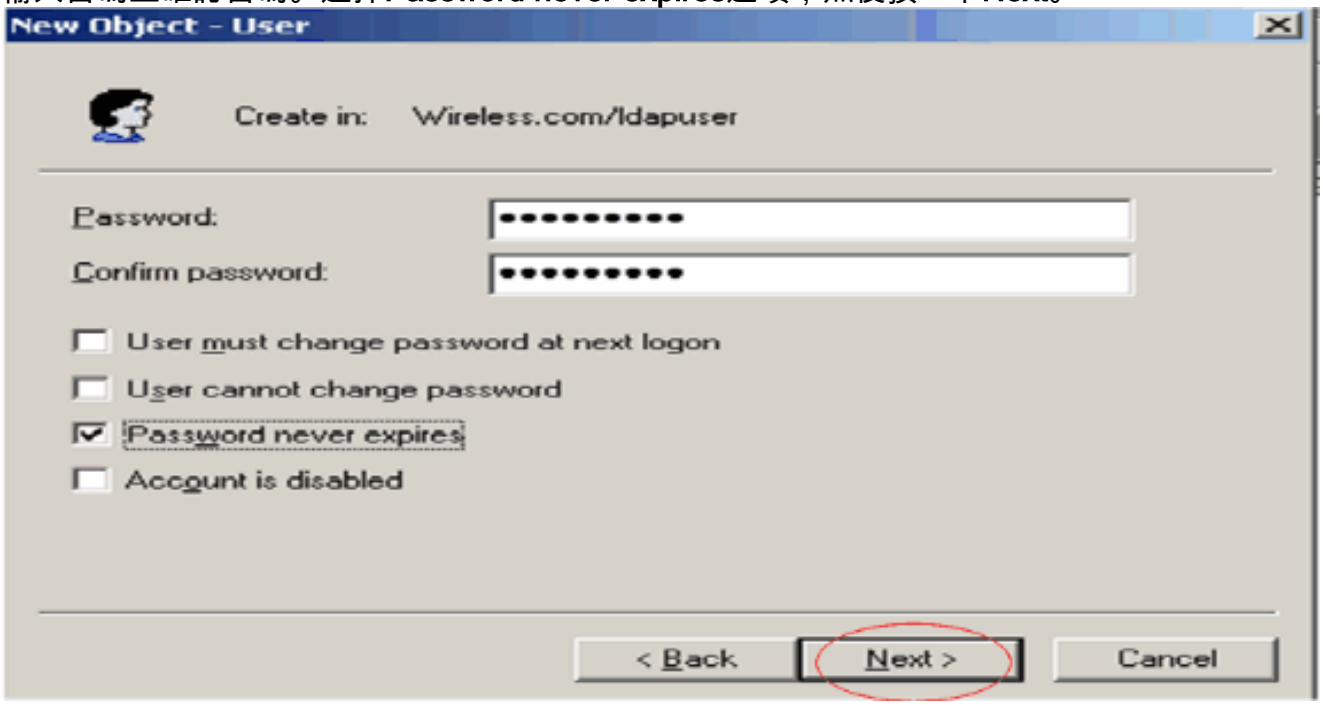
1. 按一下右鍵建立的新OU。從生成的上下文選單中選擇**新建>使用者**，以建立新使用者。



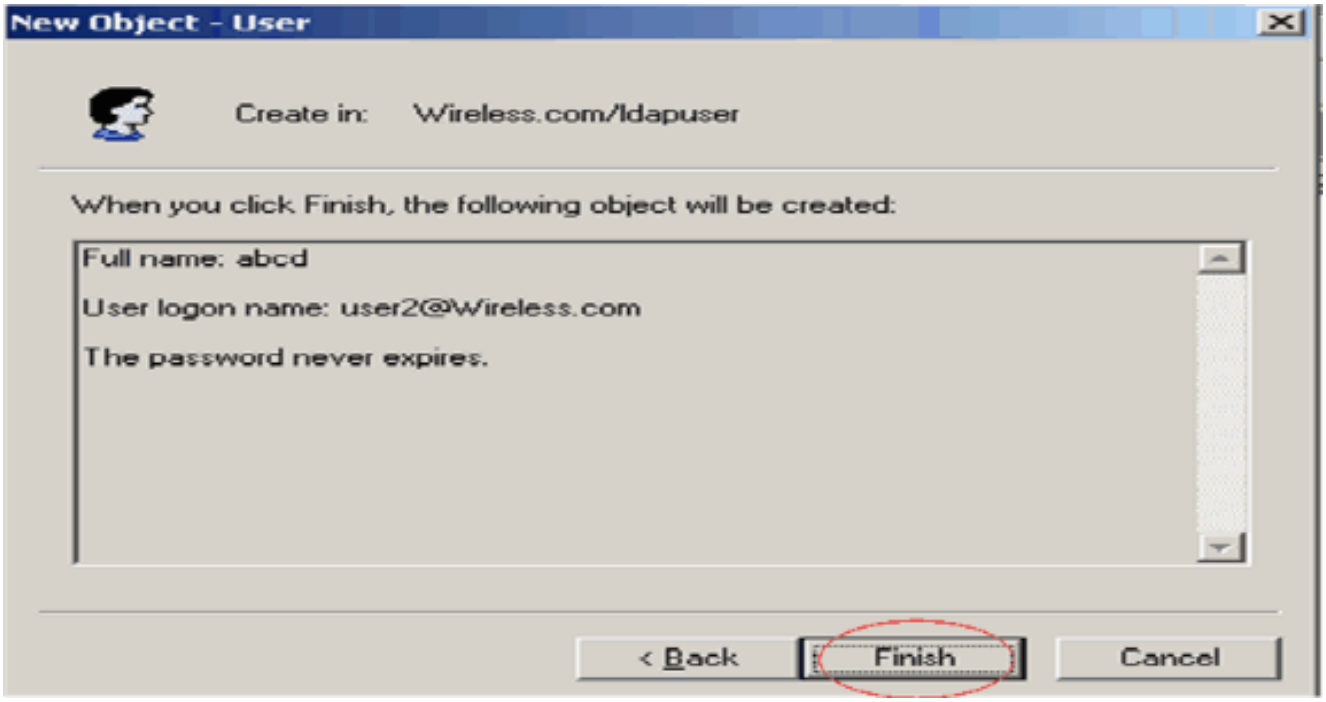
2. 在「使用者設定」頁面中，填寫所需欄位，如本例所示。此示例將**user2**用作使用者登入名。這是將在LDAP資料庫中驗證用於驗證客戶端的使用者名稱。本示例使用**abcd**作為名字和姓氏。按「**Next**」（下一步）。



3. 輸入密碼並確認密碼。選擇Password never expires選項，然後按一下Next。



4. 按一下「Finish」（結束）。在OU ldapuser下建立新的使用者user2。使用者憑據為：使用者名稱:user2密碼
：Laptop123



現在建立了OU下的使用者，下一步是配置此使用者以進行LDAP訪問。

配置使用者的LDAP訪問

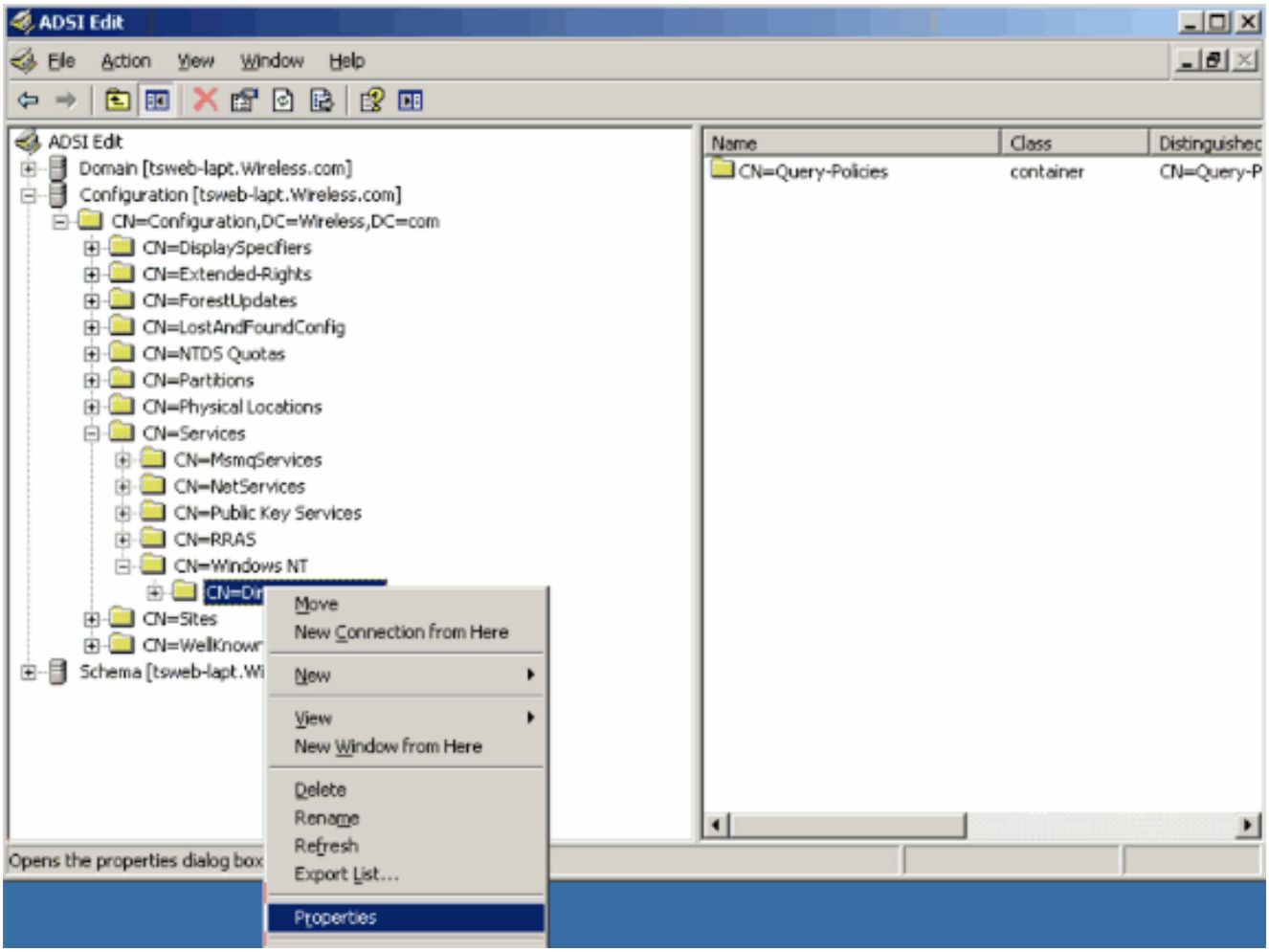
執行本節中的步驟，配置使用者進行LDAP訪問。

在Windows 2003 Server上啟用匿名繫結功能

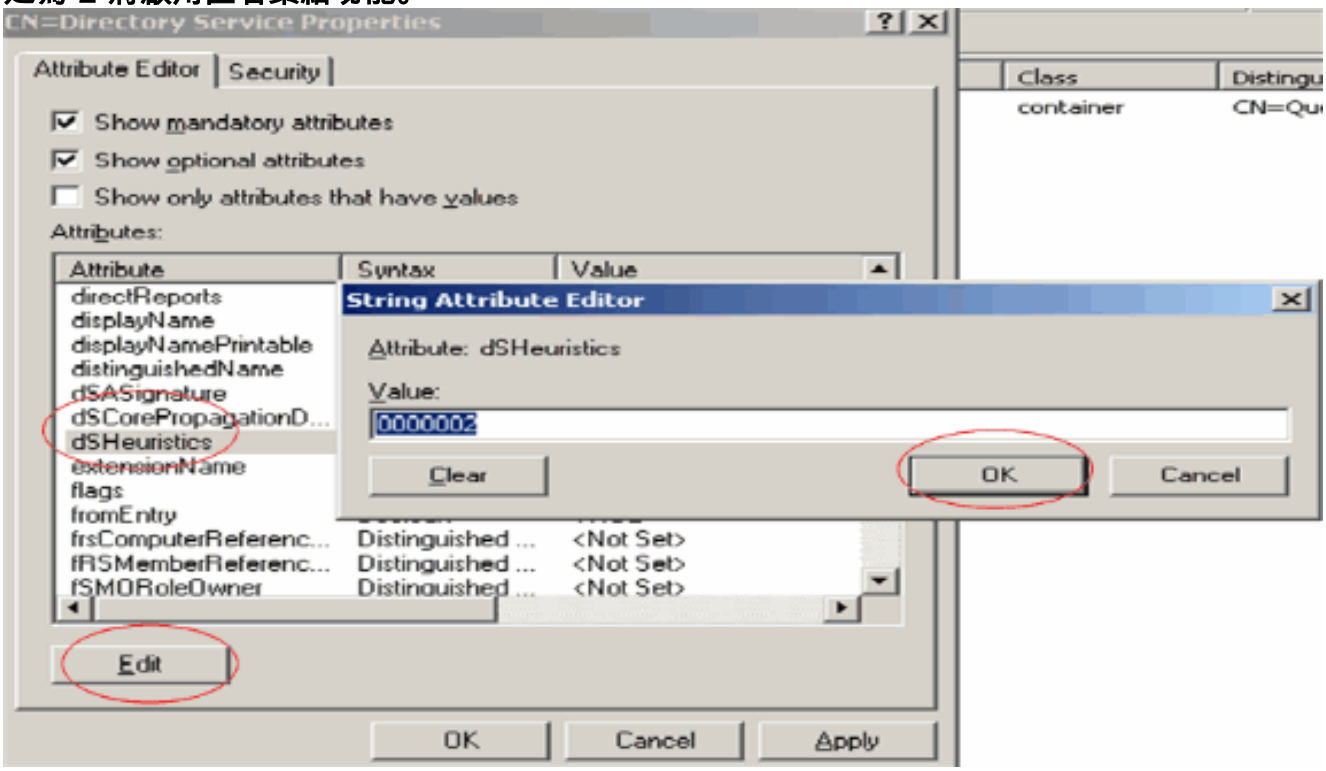
對於要在LDAP上訪問Windows 2003 AD的任何第三方應用程式，應在Windows 2003上啟用匿名繫結功能。預設情況下，在Windows 2003域控制器上不允許匿名LDAP操作。

執行以下步驟以啟用匿名繫結功能：

1. 從位置**開始>運行>型別：ADSI Edit.msc**啟動**ADSI Edit**工具。此工具是Windows 2003支援工具的一部分。
2. 在ADSI Edit視窗中，展開Root domain(Configuration [tsweb-lapt.Wireless.com])。展開**CN=Services > CN=Windows NT > CN=Directory Service**。按一下右鍵**CN=Directory Service**容器，然後從上下文選單中選擇**properties**。



3. 在**CN=Directory Service Properties**視窗中，按一下Attribute欄位下的**dsHeuristics**屬性，然後選擇**Edit**。在此屬性的**字串屬性編輯器**視窗中，輸入值**0000002**，然後按一下**Apply**和**OK**。在Windows 2003 Server上啟用了匿名繫結功能。**注意：**最後一個字元（第七）是控制繫結到LDAP服務的方式的字元。「0」或無第七個字元表示已禁用匿名LDAP操作。**將第七個字元設定為"2"將啟用匿名繫結功能。**



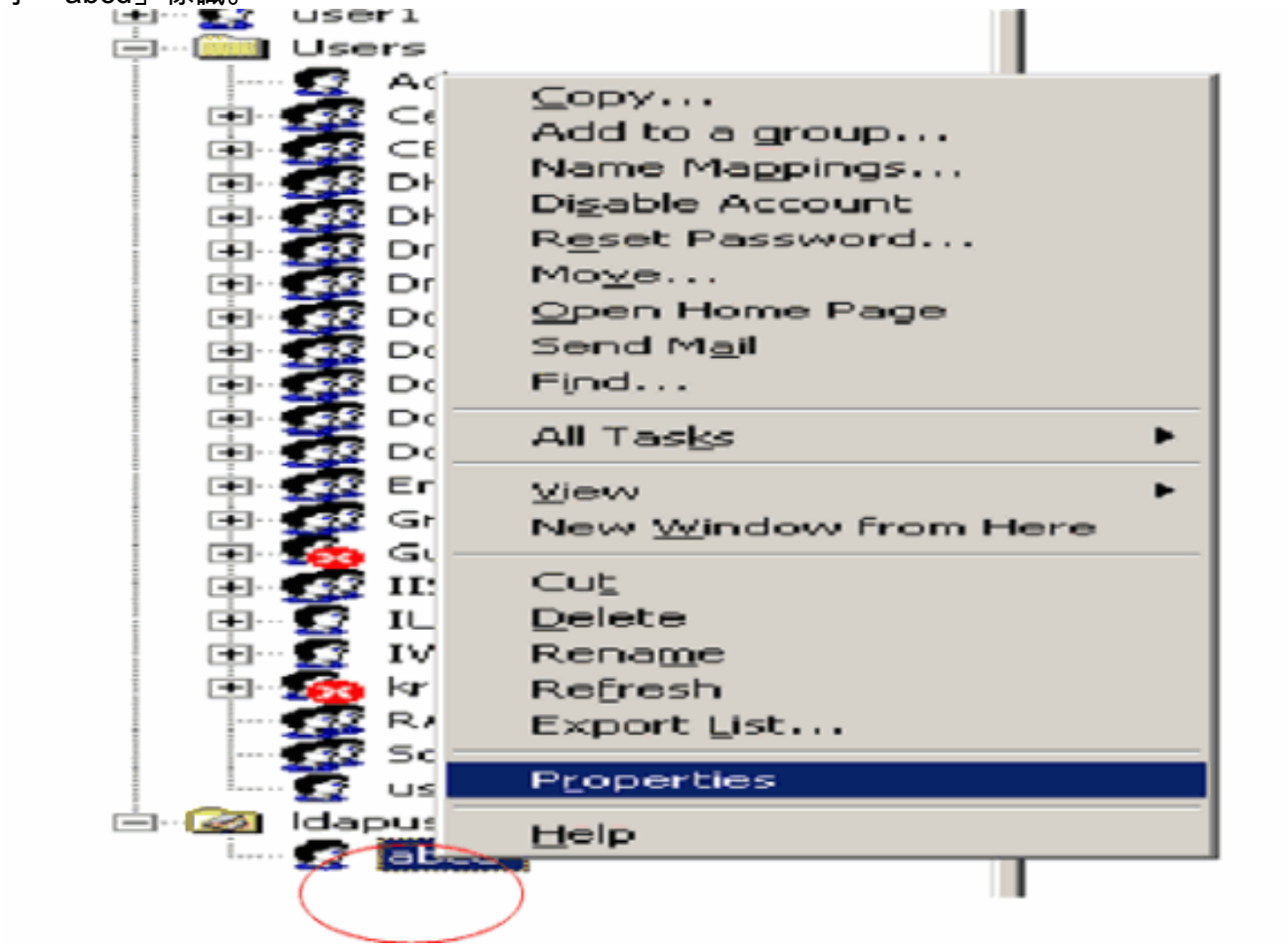
注意：如果此屬性已經包含值，請確保僅更改左側的第七個字元。這是唯一需要更改的字元，以便啟用匿名繫結。例如，如果當前值為「0010000」，則需要將其更改為「0010002」。

如果當前值少於7個字元，則需要在未使用的位置中置零：「001」將變為「0010002」。

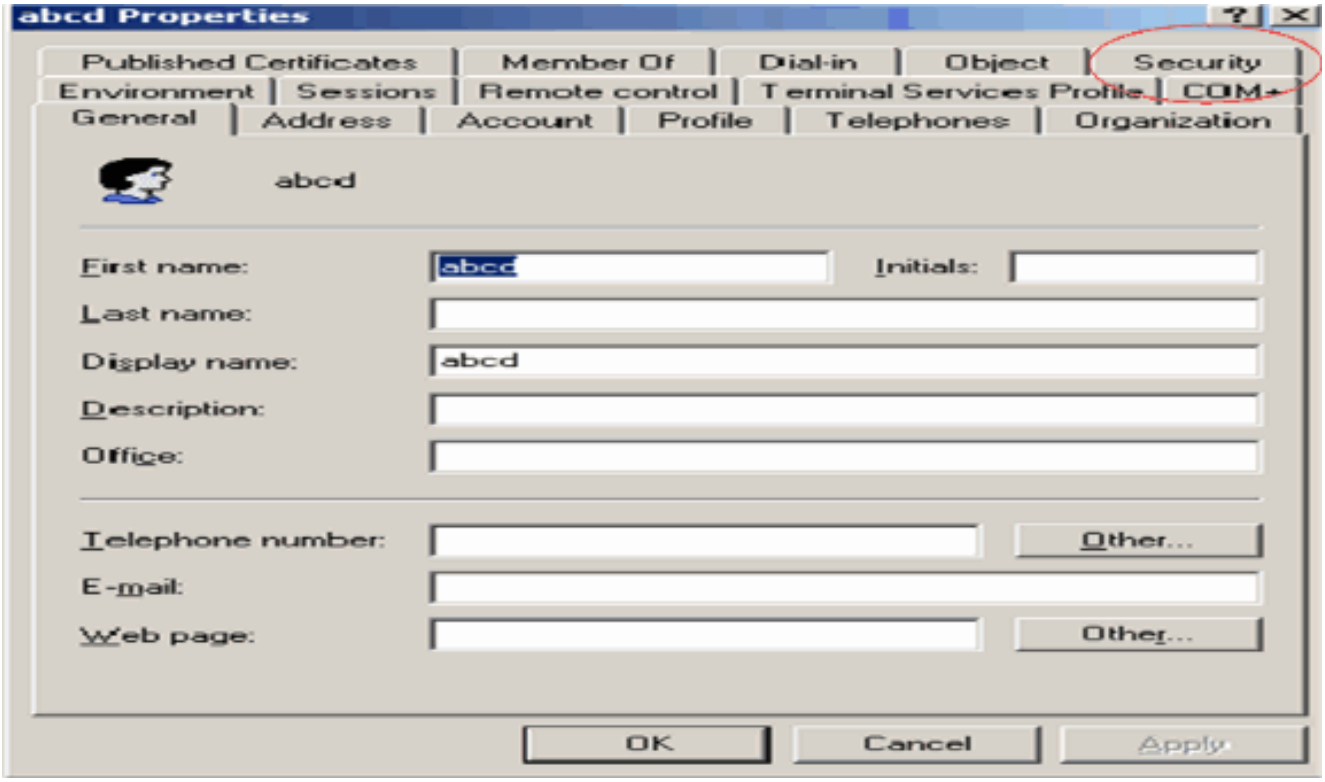
向使用者「user2」授予ANONYMOUS LOGON訪問許可權

下一步是向使用者user2授予ANONYMOUS LOGON訪問許可權。完成以下步驟即可完成以下操作：

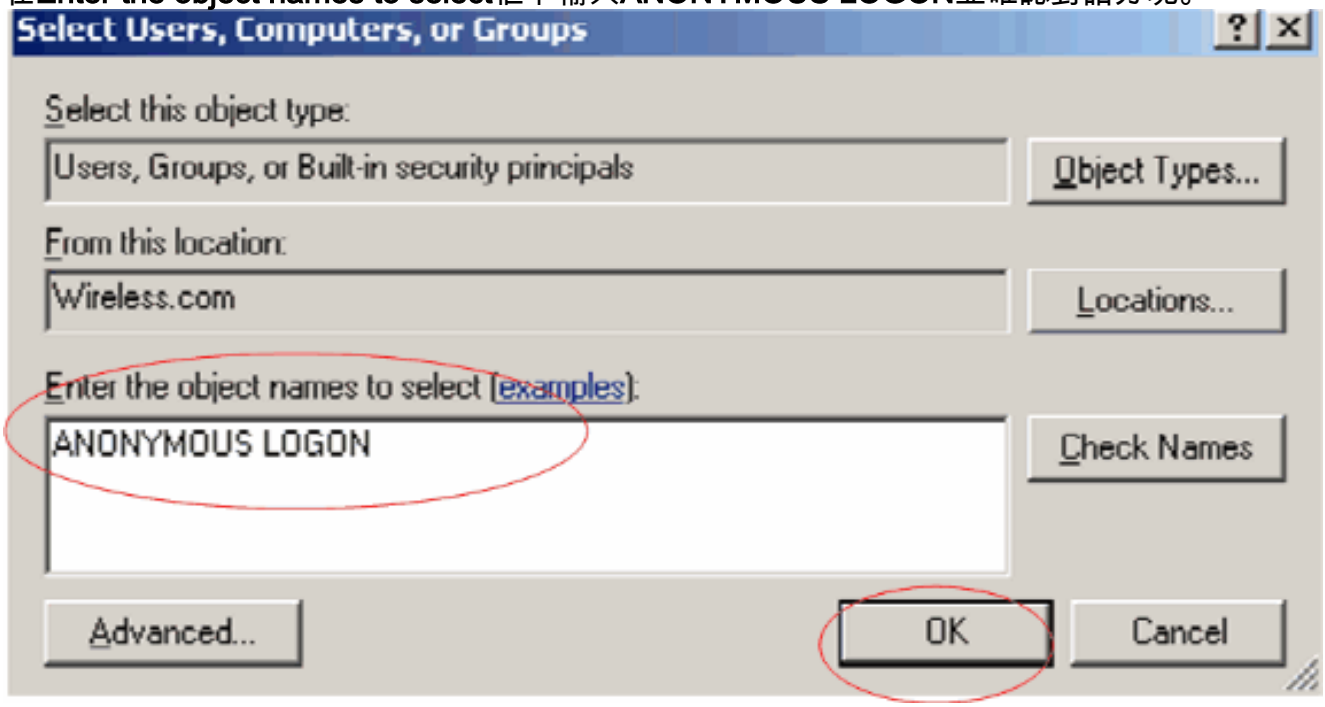
1. 開啟**Active Directory使用者和電腦**。
2. 確保選中**View Advanced Features**。
3. 導航到使用者**user2**，然後按一下右鍵該使用者。從上下文選單中選擇**屬性**。此使用者使用名字「abcd」標識。



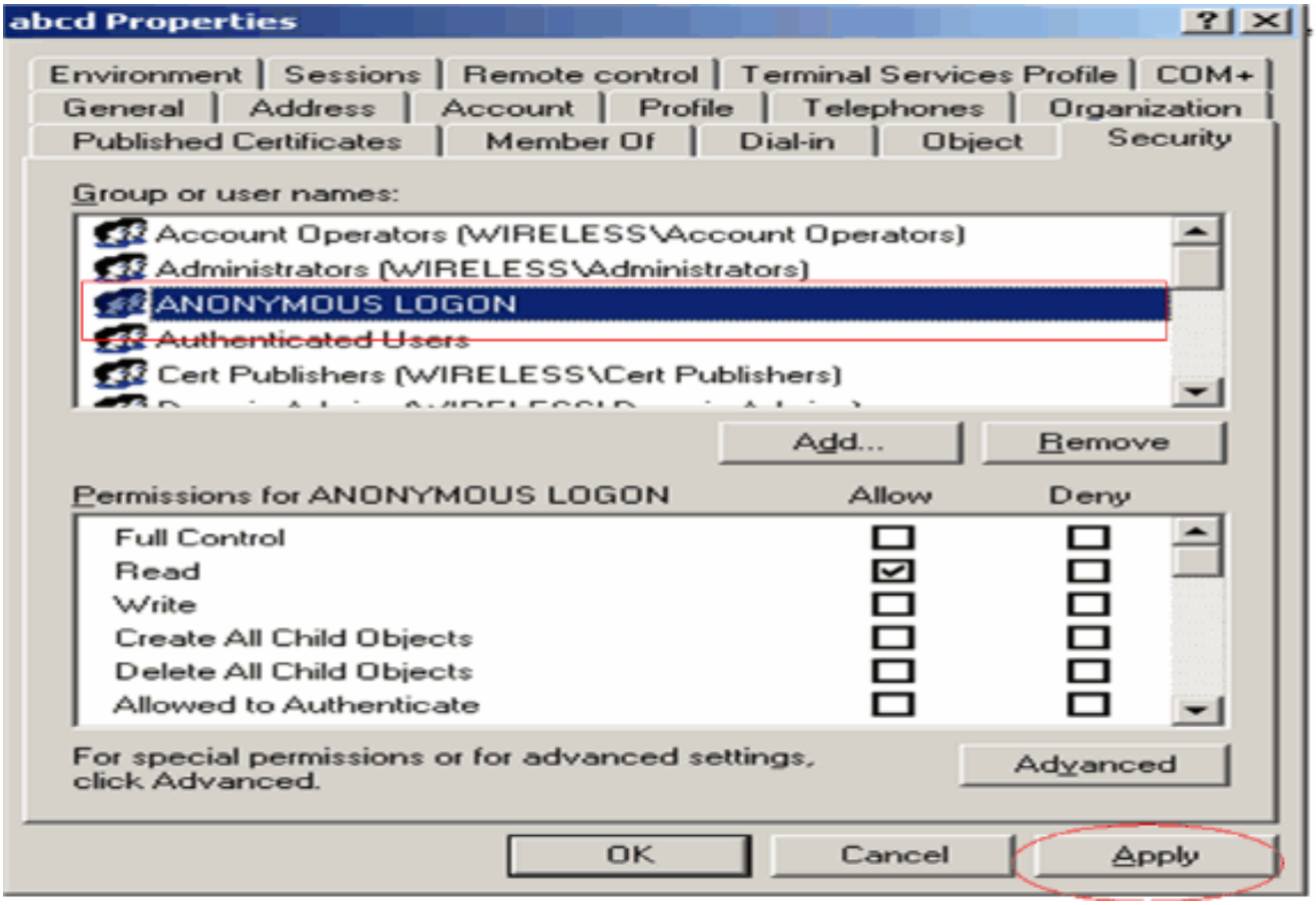
4. 在「shu xing屬性」視窗中，轉到**安全**。



5. 在生成的視窗中按一下**Add**。
6. 在**Enter the object names to select**框下輸入**ANONYMOUS LOGON**並確認對話方塊。



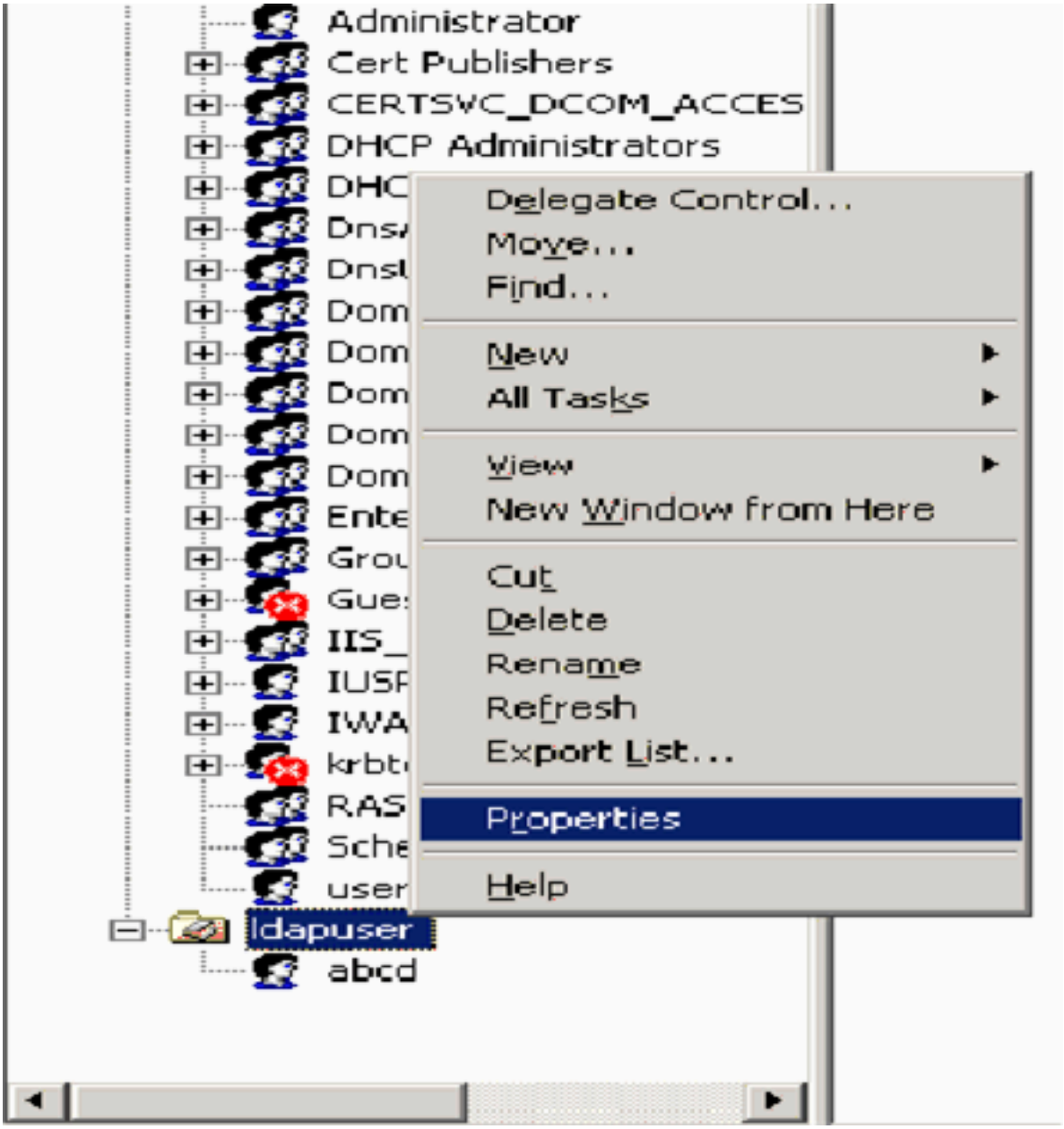
7. 在ACL中，您會注意到**ANONYMOUS LOGON**有權訪問使用者的一些屬性集。按一下「**OK**」（確定）。已授予此使用者的ANONYMOUS登入訪問許可權。



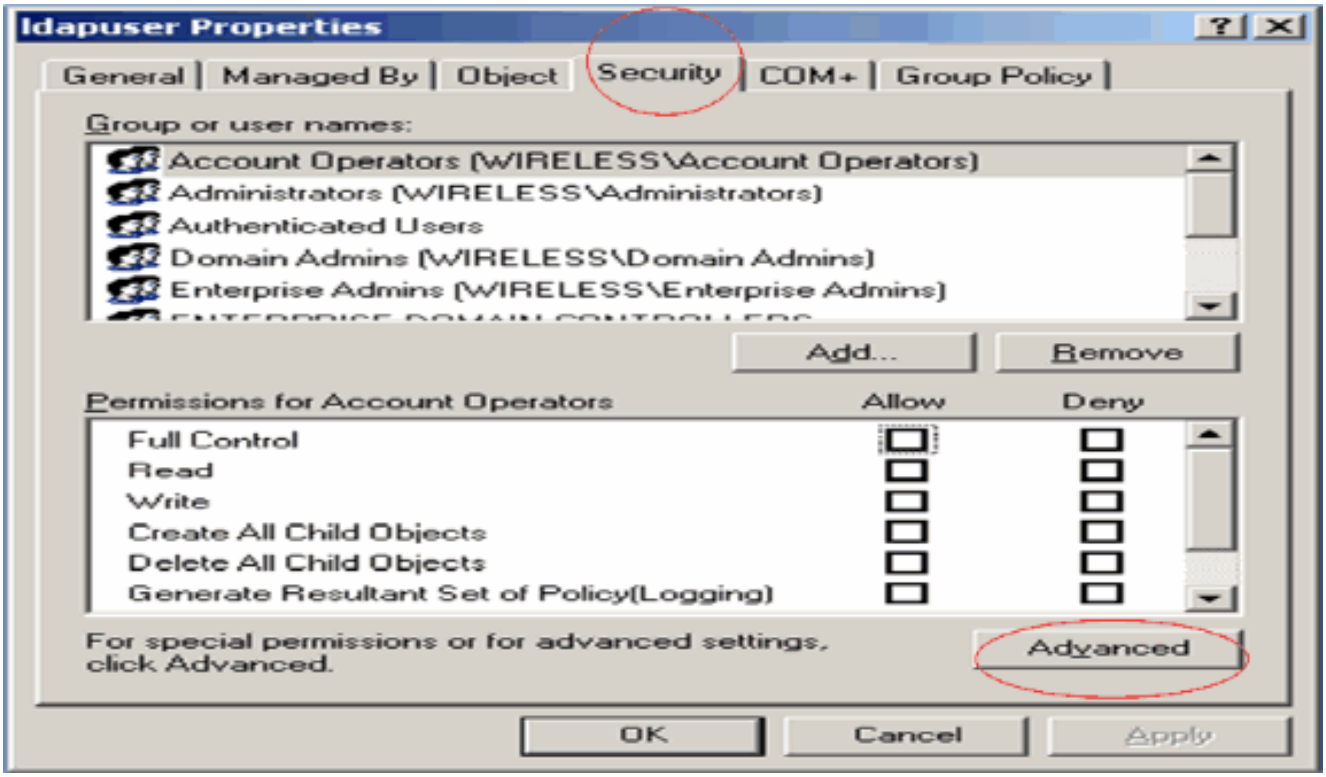
對OU授予清單內容許可權

下一步是至少向使用者所在的OU上的**ANONYMOUS LOGON**授予**List Contents**許可權。在本示例中，「user2」位於OU "ldapuser"上。完成以下步驟即可完成以下操作：

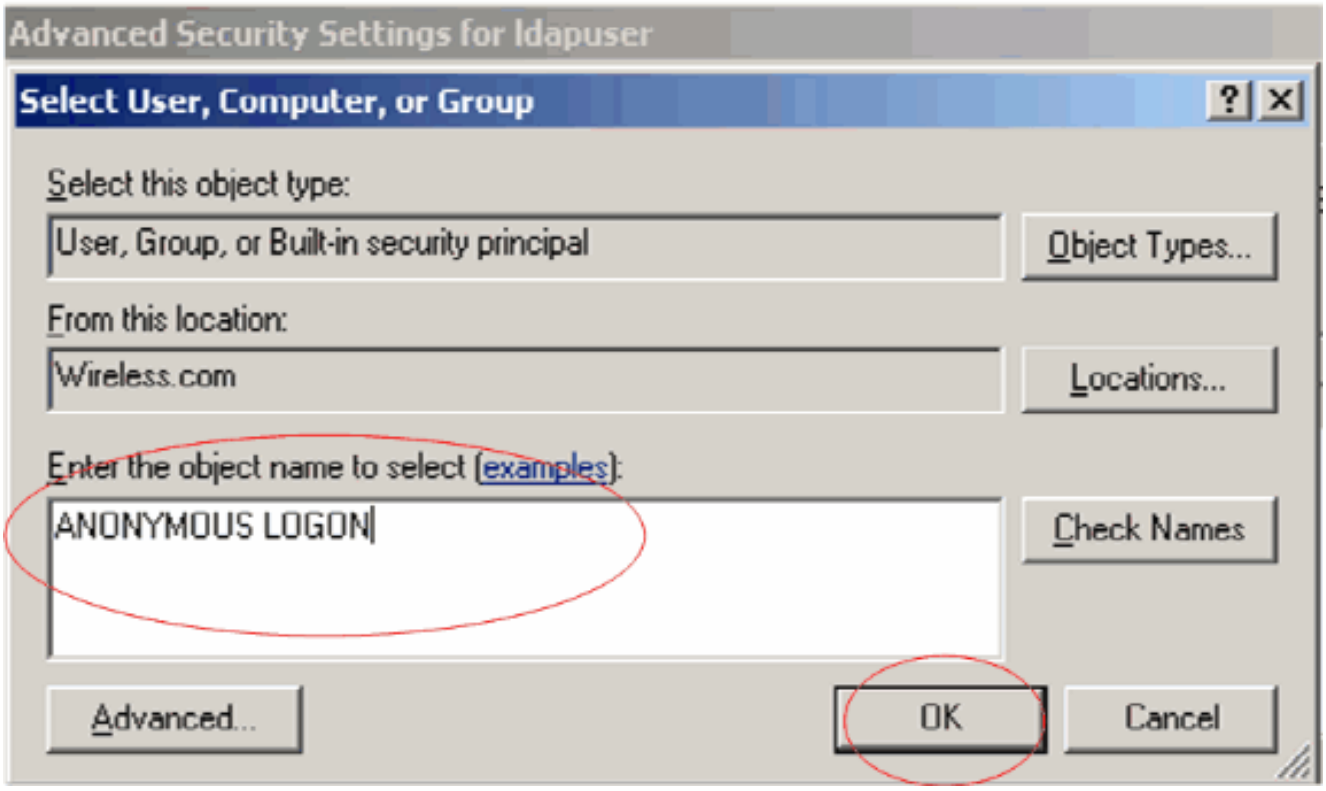
1. 在Active Directory使用者和電腦中，按一下右鍵OU **ldapuser**並選擇**屬性**。



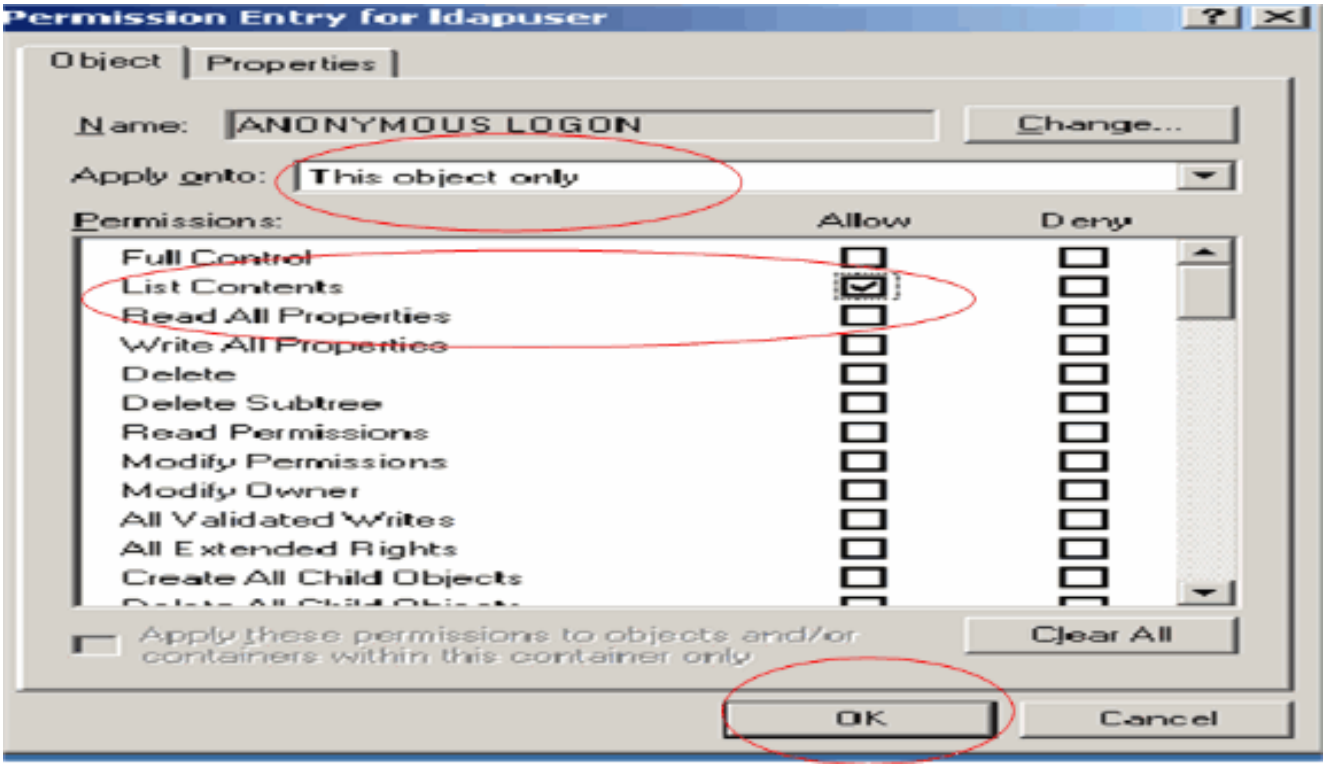
2. 按一下「Security」，然後「Advanced」。



3. 按一下「**Add**」。在開啟的對話方塊中，輸入**ANONYMOUS LOGON**。



4. 確認對話方塊。這將開啟一個新的對話方塊視窗。
5. 在**Apply to**下拉框中，選擇**This object only**，並啟用**List Contents** Allow覈取方塊。

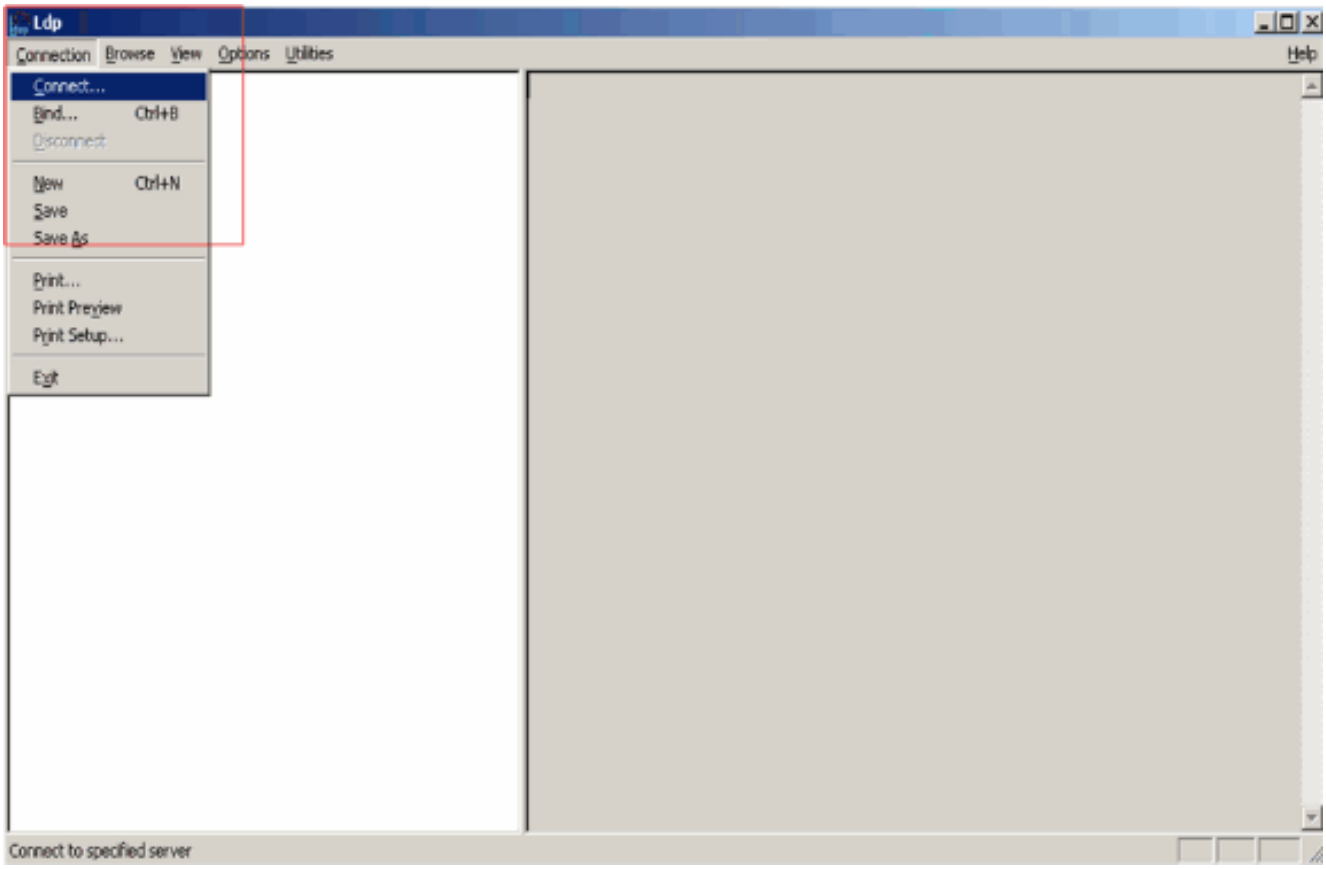


使用LDP標識使用者屬性

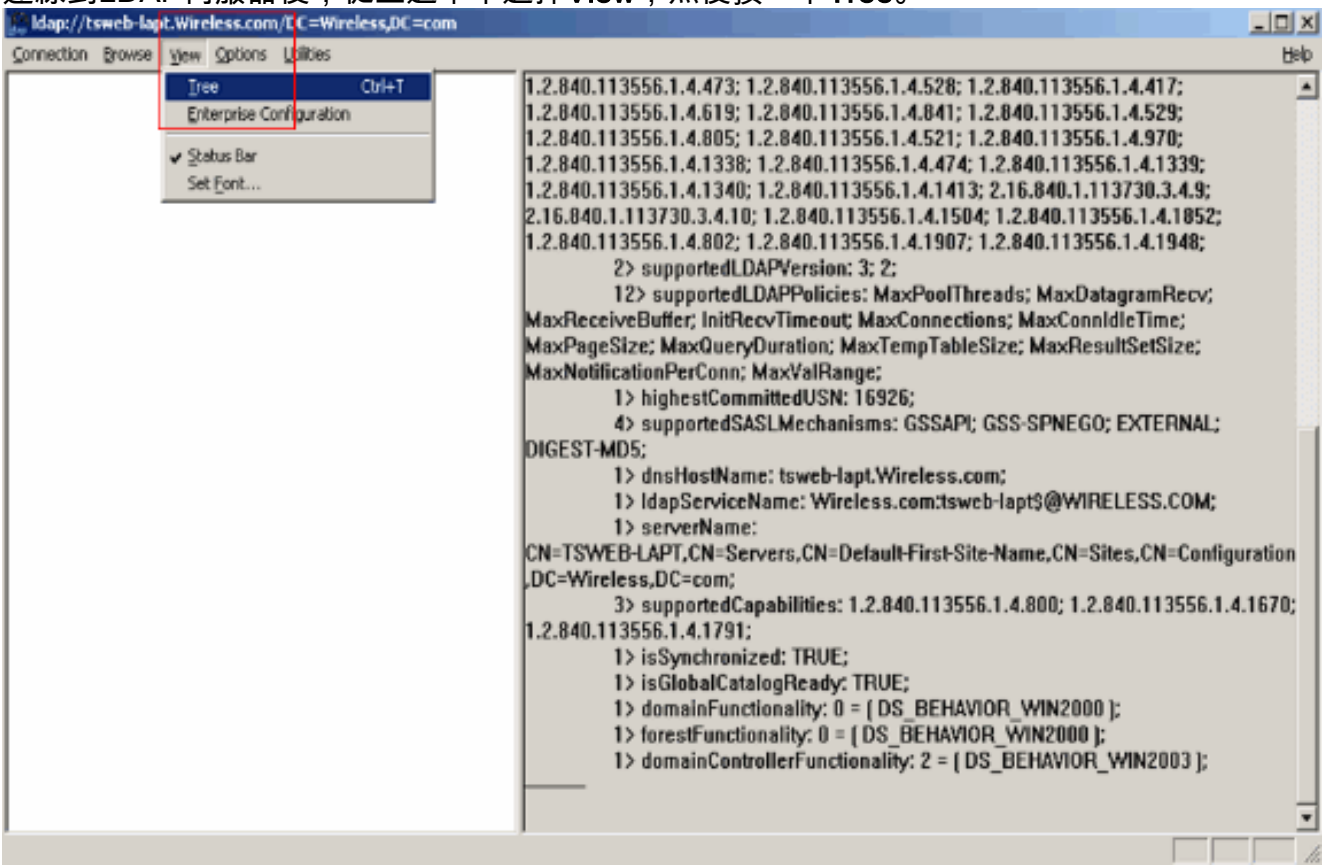
此GUI工具是一個LDAP客戶端，允許使用者針對任何與LDAP相容的目錄（如Active Directory）執行操作（如連線、繫結、搜尋、修改、新增、刪除）。LDP用於檢視Active Directory中儲存的對象及其後設資料，如安全描述符和複製後設資料。

從產品CD安裝Windows Server 2003支援工具時，會包括LDP GUI工具。本節介紹使用LDP實用程式標識與使用者**user2**關聯的特定**屬性**。其中有些屬性用於填寫WLC上的LDAP伺服器配置引數，例如「使用者屬性」型別和「使用者對象」型別。

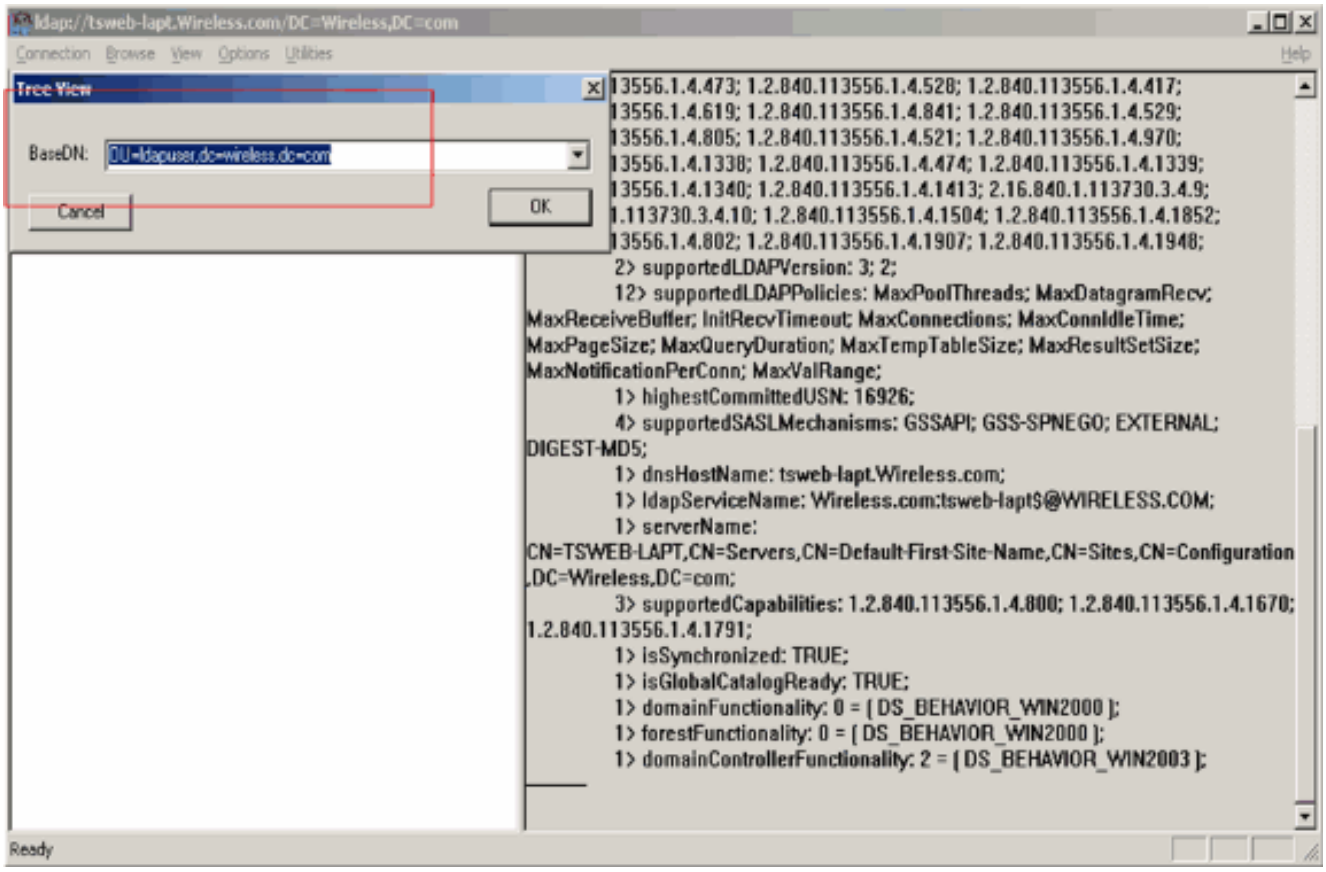
1. 在Windows 2003伺服器上（即使在同一個LDAP伺服器上），按一下**Start > Run**並輸入**LDP**以訪問LDP瀏覽器。
2. 在LDP主視窗中，按一下**Connection > Connect**，然後通過輸入LDAP伺服器的IP地址連線到LDAP伺服器。



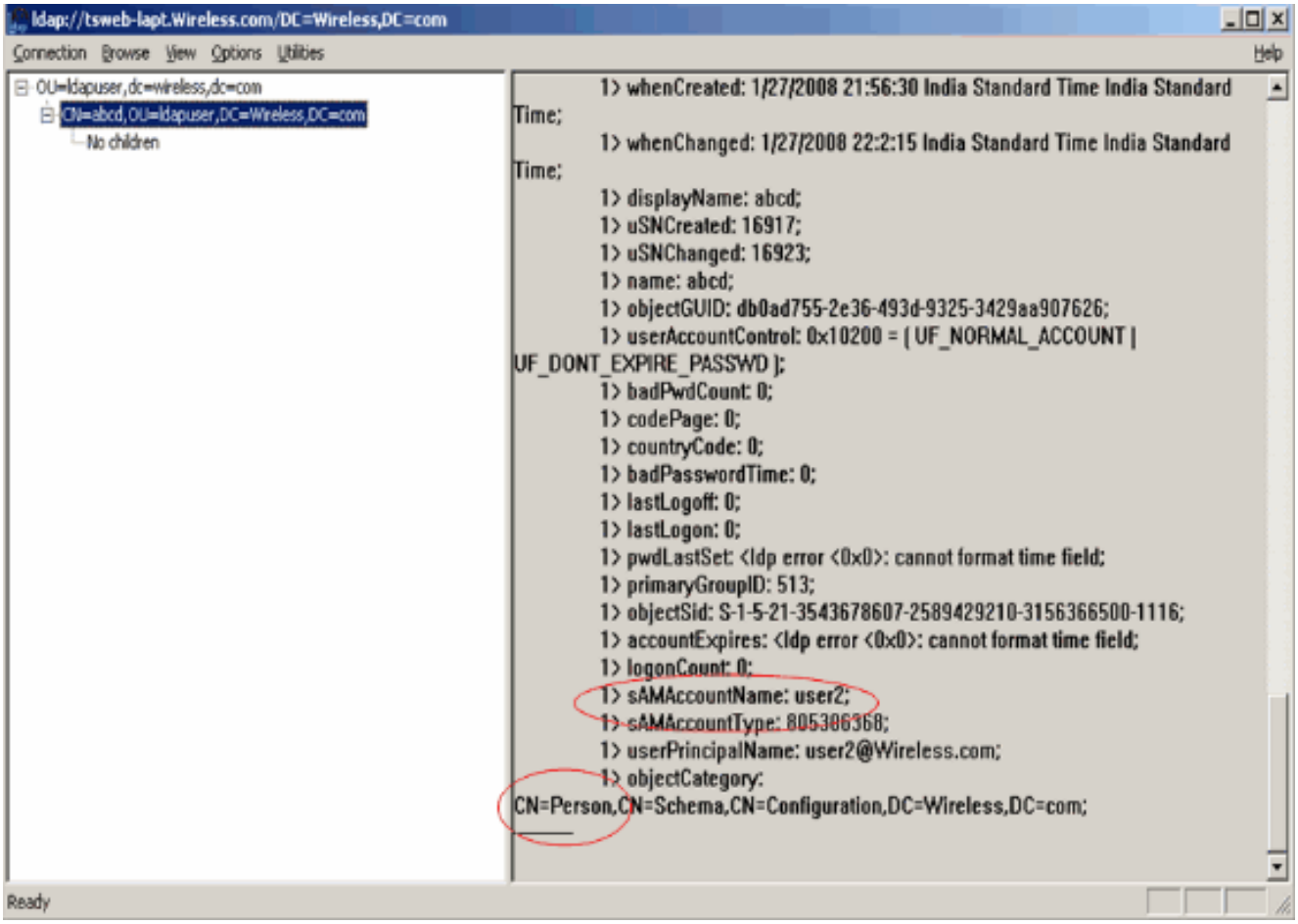
3. 連線到LDAP伺服器後，從主選單中選擇**View**，然後按一下**Tree**。



4. 在生成的「樹檢視」視窗中，輸入使用者的BaseDN。在本示例中，**user2位於域Wireless.com下的OU "ldapuser"下**。因此，使用者**user2**的BaseDN為**OU=ldapuser，dc=wireless， dc=com**。按一下「**OK**」（確定）。



5. LDP瀏覽器的左側顯示出現在指定BaseDN(**OU=ldapuser， dc=wireless， dc=com)下的整個樹**。展開樹以找到使用者**user2**。此使用者可以使用代表該使用者名稱字的CN值進行標識。在本例中，它是**CN=abcd**。按兩下**CN=abcd**。在LDP瀏覽器的右側窗格中，LDP**將顯示與user2關聯的所有屬性**。以下範例將說明此步驟
：



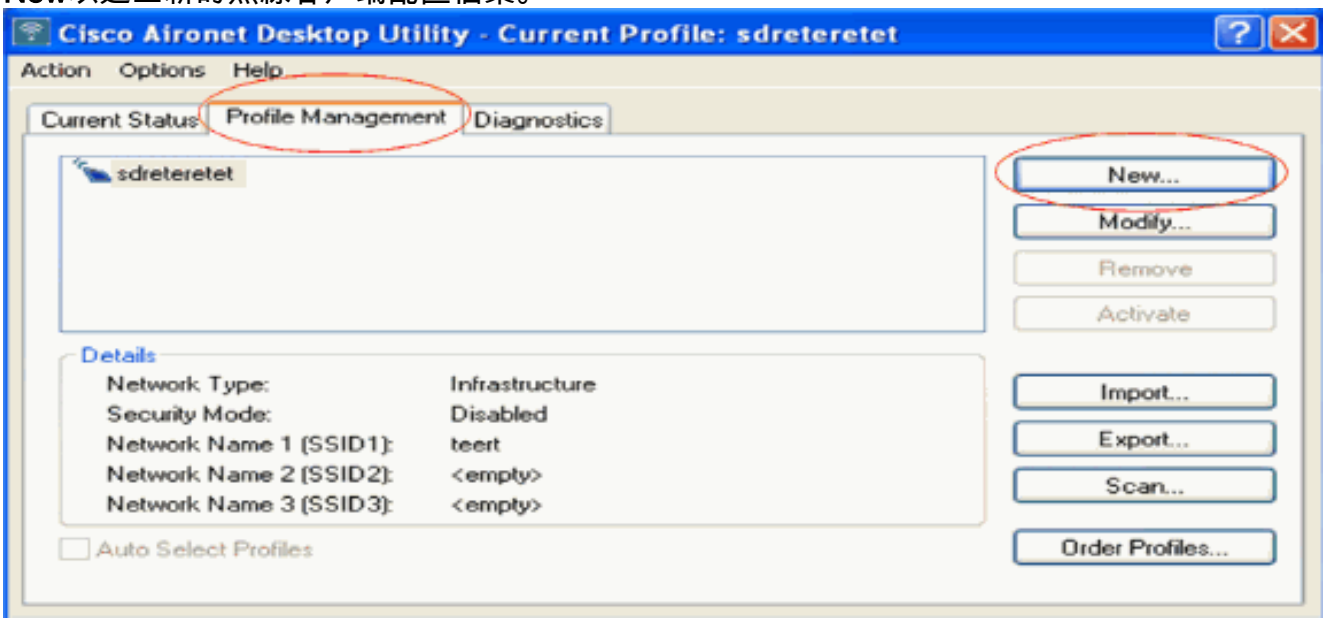
在此示例中，請觀察右側的環繞欄位。

6. 如本文檔的使用LDAP伺服器的詳細資訊配置WLC部分中所述，在**User Attribute**欄位中，在包含使用者名稱的使用者記錄中輸入屬性的名稱。從此LDP輸出中，可以看到**sAMAccountName**是包含使用者名稱「user2」的一個屬性。因此，請輸入與WLC上的**User Attribute**欄位對應的**sAMAccountName**屬性。
7. 在**User Object Type**欄位中，輸入將記錄標識為使用者的LDAP objectType屬性的值。通常，使用者記錄有若干objectType屬性值，其中某些值對於使用者是唯一的，而某些值則與其他對象型別共用。在LDP輸出中，**CN=Person**是將記錄標識為使用者的值。因此，在WLC上指定**Person**作為**User Object Type**屬性。

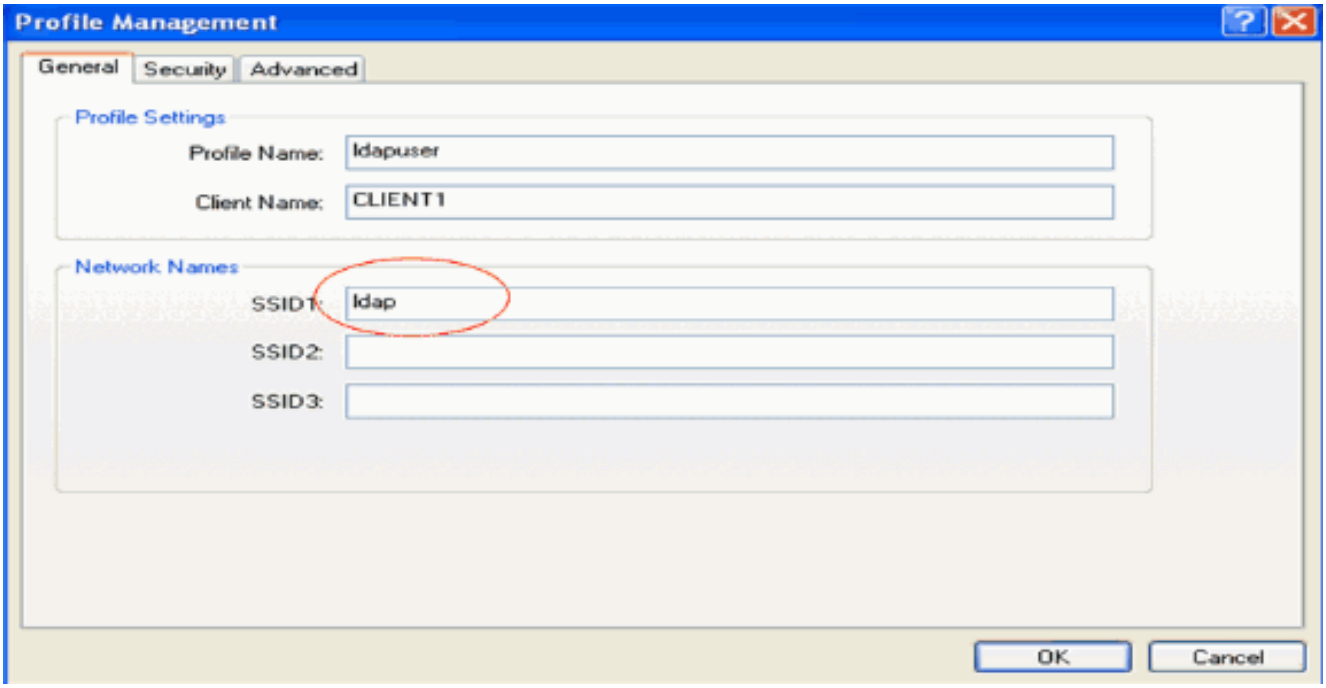
配置無線客戶端

最後一步是配置無線客戶端，使其使用客戶端和伺服器證書進行EAP-FAST身份驗證。完成以下步驟即可完成以下操作：

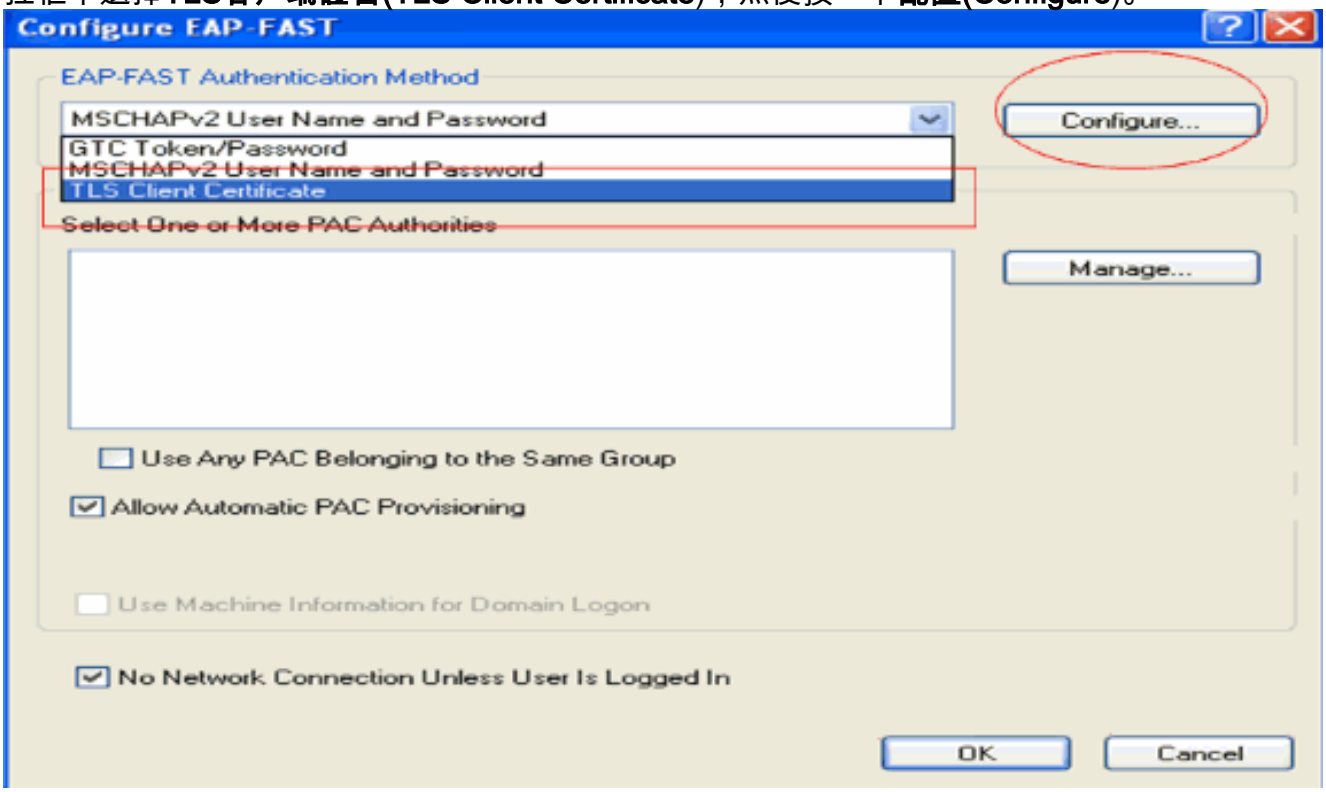
1. 啟動**Cisco Aironet Desktop Utility**(ADU)。在ADU主視窗中，按一下**Profile Management > New**以建立新的無線客戶端配置檔案。



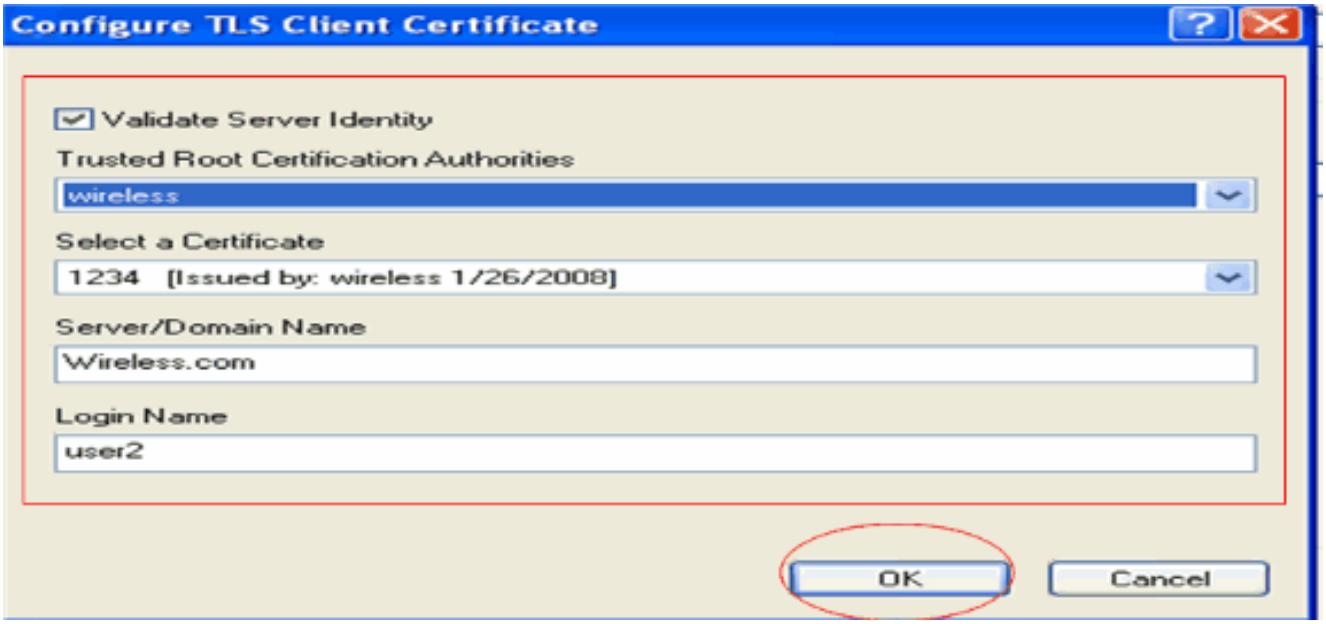
2. 指定配置檔名稱，並為該配置檔案分配SSID名稱。此SSID名稱應該與WLC上配置的相同。在本示例中，SSID名稱為**ldap**。



3. 按一下**Security**頁籤，然後選擇**802.1x/EAP**作為第2層安全。選擇**EAP-FAST**作為EAP方法，然後按一下**Configure**。
4. 在EAP-FAST配置頁面中，從EAP-FAST身份驗證方法(EAP-FAST Authentication Method)下拉框中選擇**TLS客戶端證書(TLS Client Certificate)**，然後按一下**配置(Configure)**。



5. 在「TLS客戶端證書配置」視窗中：啟用**Validate Server Identity**覈取方塊，並選擇客戶端上安裝的CA證書(請參閱本文檔的為客戶端生成根CA證書部分)作為受信任的根證書頒發機構。選擇安裝在客戶端上的裝置證書(本文檔的為客戶端生成裝置證書一節中有說明)作為客戶端證書。按一下「**OK**」（確定）。以下範例將說明此步驟：



無線客戶端配置檔案已建立。

驗證

執行以下步驟以驗證您的配置是否正常工作。

1. 啟用ADU上的ldap SSID。
2. 根據需要在下一視窗中按一下Yes或OK。您應該能夠在ADU上看到客戶端身份驗證和關聯的所有步驟，這樣才能成功。

使用本節內容，確認您的組態是否正常運作。使用WLC CLI模式。

- 為了驗證WLC是否能夠與LDAP伺服器通訊並找到使用者，請從WLC CLI指定**debug aaa ldap enable**命令。此示例說明了一個成功的通訊LDAP過程：**注意：**由於空間方面的考慮，本節中的某些輸出已移至第二行。(Cisco Controller)**>debug aaa ldap enable**

```
Sun Jan 27 09:23:46 2008: AuthenticationRequest: 0xba96514
Sun Jan 27 09:23:46 2008:       Callback.....................................0x8
344900
Sun Jan 27 09:23:46 2008:       protocolType.................................0x0
0100002
Sun Jan 27 09:23:46 2008:       proxyState...................................00:
40:96:AC:E6:57-00:00
Sun Jan 27 09:23:46 2008:       Packet contains 2 AVPs (not shown)
Sun Jan 27 09:23:46 2008: ldapTask [1] received msg 'REQUEST' (2) in state 'IDLE' (1)
Sun Jan 27 09:23:46 2008: LDAP server 1 changed state to INIT
Sun Jan 27 09:23:46 2008: ldapInitAndBind [1] called lcapi_init (rc = 0 - Success)
Sun Jan 27 09:23:46 2008: ldapInitAndBind [1] called lcapi_bind (rc = 0 - Success)
Sun Jan 27 09:23:46 2008: LDAP server 1 changed state to CONNECTED
Sun Jan 27 09:23:46 2008: LDAP server 1 now active
Sun Jan 27 09:23:46 2008: LDAP_CLIENT: UID Search (base=OU=ldapuser,DC=wireless,
DC=com, pattern=(&(objectclass=Person)(sAMAccountName=user2)))
Sun Jan 27 09:23:46 2008: LDAP_CLIENT: Returned msg type 0x64
Sun Jan 27 09:23:46 2008: ldapAuthRequest [1] called lcapi_query base="OU=ldapus
er,DC=wireless,DC=com" type="Person" attr="sAMAccountName" user="user2" (rc = 0
- Success)
Sun Jan 27 09:23:46 2008: LDAP ATTR> dn = CN=abcd,OU=ldapuser,DC=Wireless,DC=com
 (size 38)
Sun Jan 27 09:23:46 2008: Handling LDAP response Success
```

從此調試輸出中突出顯示的資訊可以清楚地看到，WLC會使用在WLC上指定的使用者屬性來查

詢LDAP伺服器，並且LDAP進程成功。

- 若要驗證本地EAP身份驗證是否成功，請從WLC CLI指定**debug aaa local-auth eap method events enable**命令。以下是範例：(Cisco Controller)**>debug aaa local-auth eap method events enable**

```
Sun Jan 27 09:38:28 2008: eap_fast.c-EVENT: New context
(EAP handle = 0x1B000009)

Sun Jan 27 09:38:28 2008: eap_fast.c-EVENT: Allocated new EAP-FAST context
(handle = 0x22000009)

Sun Jan 27 09:38:28 2008: eap_fast_auth.c-AUTH-EVENT: Process Response
(EAP handle = 0x1B000009)

Sun Jan 27 09:38:28 2008: eap_fast_auth.c-AUTH-EVENT: Received Identity

Sun Jan 27 09:38:28 2008: eap_fast_tlv.c-AUTH-EVENT: Adding PAC A-ID TLV
(436973636f000000000000000000000000)

Sun Jan 27 09:38:28 2008: eap_fast_auth.c-AUTH-EVENT: Sending Start

Sun Jan 27 09:38:29 2008: eap_fast.c-AUTH-EVENT: Process Response, type: 0x2b

Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Process Response
(EAP handle = 0x1B000009)

Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT:
Received TLS record type: Handshake in state: Start

Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Local certificate found

Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Reading Client Hello handshake

Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT:
TLS_DHE_RSA_AES_128_CBC_SHA proposed...

Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: Proposed ciphersuite(s):

Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT:     TLS_DHE_RSA_WITH_AES_128_CBC_SHA

Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT:     TLS_RSA_WITH_AES_128_CBC_SHA

Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT:     TLS_RSA_WITH_RC4_128_SHA

Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: Selected ciphersuite:

Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT:     TLS_DHE_RSA_WITH_AES_128_CBC_SHA

Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Building Provisioning Server Hello

Sun Jan 27 09:38:29 2008: eap_fast_crypto.c-EVENT:
Starting Diffie Hellman phase 1 ...

Sun Jan 27 09:38:30 2008: eap_fast_crypto.c-EVENT:
Diffie Hellman phase 1 complete

Sun Jan 27 09:38:30 2008: eap_fast_auth.c-AUTH-EVENT: DH signature length = 128

Sun Jan 27 09:38:30 2008: eap_fast_auth.c-AUTH-EVENT: Sending Provisioning Serving Hello

Sun Jan 27 09:38:30 2008: eap_fast.c-EVENT: Tx packet fragmentation required

Sun Jan 27 09:38:30 2008: eap_fast.c-AUTH-EVENT: eap_fast_rx_packet():
```

```
EAP Fast NoData (0x2b)

Sun Jan 27 09:38:30 2008: eap_fast.c-AUTH-EVENT: eap_fast_rx_packet():
EAP Fast NoData (0x2b)

Sun Jan 27 09:38:30 2008: eap_fast.c-AUTH-EVENT: eap_fast_rx_packet():
EAP Fast NoData (0x2b)

Sun Jan 27 09:38:32 2008: eap_fast.c-AUTH-EVENT: Process Response, type: 0x2b

Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Reassembling TLS record

Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Sending EAP-FAST Ack

.....................................................................

.....................................................................

.....................................................................

Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT:
Received TLS record type: Handshake in state: Sent provisioning Server Hello

Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT:
Reading Client Certificate handshake

Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Added certificate 1 to chain

Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Added certificate 2 to chain

Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Successfully validated received certificate

Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT: Rx'd I-ID:
"EAP-FAST I-ID" from Peer Cert

Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT:
Reading Client Key Exchange handshake

Sun Jan 27 09:38:32 2008: eap_fast_crypto.c-EVENT:
Starting Diffie Hellman phase 2 ...

Sun Jan 27 09:38:32 2008: eap_fast_crypto.c-EVENT:
Diffie Hellman phase 2 complete.

Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT:
Reading Client Certificate Verify handshake

Sun Jan 27 09:38:32 2008: eap_fast_crypto.c-EVENT:
Sign certificate verify succeeded (compare)

.....................................................................................

.....................................................................................

.....................................................................................

.....................................................................................
.
```

- debug aaa local-auth db enable命令也非常有用。以下是範例：(Cisco Controller)>debug aaa local-auth db enable

```
Sun Jan 27 09:35:32 2008: LOCAL_AUTH: EAP: Received an auth request

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Creating new context
```

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Local auth profile name for context 'ldapuser'

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Created new context eap session handle fb000007

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: (EAP:8) Sending the Rxd EAP packet
(id 2) to EAP subsys

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Found matching context for id - 8

**Sun Jan 27 09:35:32 2008: LOCAL_AUTH: (EAP) Sending user credential
request username 'user2' to LDAP**

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Found context matching MAC address - 8

.....

.....

.....

.....

Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) Sending the Rxd EAP packet
(id 12) to EAP subsys

Sun Jan 27 09:35:36 2008: LOCAL_AUTH: Found matching context for id - 8

Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) ---> [KEY AVAIL] send_len 64, recv_len 0

Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) received keys waiting for success

Sun Jan 27 09:35:36 2008: LOCAL_AUTH: Found matching context for id - 8

Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) Received success event

Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) Processing keys success

- 若要檢視WLC中安裝用於本機驗證之憑證，請從WLC CLI發出**show local-auth certificates**命令。以下是範例：（思科控制器）**>show local-auth certificates**

```
Certificates available for Local EAP authentication:


Certificate issuer ............................ vendor

  CA certificate:

    Subject: DC=com, DC=Wireless, CN=wireless

     Issuer: DC=com, DC=Wireless, CN=wireless

      Valid: 2008 Jan 23rd, 15:50:27 GMT to 2013 Jan 23rd, 15:50:27 GMT

  Device certificate:

    Subject: O=cisco, CN=ciscowlc123

     Issuer: DC=com, DC=Wireless, CN=wireless

      Valid: 2008 Jan 24th, 12:18:31 GMT to 2010 Jan 23rd, 12:18:31 GMT
```

```
Certificate issuer ............................. cisco

  CA certificate:

    Subject: O=Cisco Systems, CN=Cisco Manufacturing CA

     Issuer: O=Cisco Systems, CN=Cisco Root CA 2048

      Valid: 2005 Jun 10th, 22:16:01 GMT to 2029 May 14th, 20:25:42 GMT

   Device certificate:

            Not installed.
```

- 若要從CLI模式檢視WLC上的本機驗證組態，請發出**show local-auth config**指令。以下是範例：（思科控制器）**>show local-auth config**

```
User credentials database search order:

    Primary ..................................... LDAP



Timer:

    Active timeout ............................. 300



Configured EAP profiles:

    Name ........................................ ldapuser

      Certificate issuer ....................... vendor

      Peer verification options:

        Check against CA certificates ........... Enabled

        Verify certificate CN identity .......... Disabled

        Check certificate date validity ......... Disabled

      EAP-FAST configuration:

        Local certificate required .............. Yes

        Client certificate required ............. Yes

      Enabled methods ........................... fast

      Configured on WLANs ....................... 2



EAP Method configuration:

    EAP-FAST:

--More-- or (q)uit

      Server key ................................ <hidden>
```

```
TTL for the PAC ..................... 10

Anonymous provision allowed ............. No

.......................................

.......................................

Authority Information ................... Cisco A-ID
```

疑難排解

您可以使用以下命令對組態進行疑難排解：

- debug aaa local-auth eap method events enable
- debug aaa all enable
- debug dot1x packet enable

相關資訊

- 使用無線LAN控制器和外部RADIUS伺服器的EAP-FAST身份驗證配置示例
- 採用Microsoft Internet身份驗證服務(IAS)的統一無線網路下的PEAP
- 使用基於ACS的WLC進行動態VLAN分配到Active Directory組對映配置示例
- 思科無線LAN控制器組態設定指南 — 設定安全解決方案
- Cisco無線LAN控制器組態設定指南 — 管理控制器軟體和組態
- 使用WLAN控制器(WLC)的EAP驗證組態範例
- 無線區域網路控制器(WLC)設計和功能常見問題
- 採用EAP-FAST驗證的思科安全服務使用者端
- 無線 LAN 控制器 (WLC) 常見問題
- 控制器無線LAN控制器(WLC)錯誤和系統消息常見問題
- 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）。