ASA 8.X:AnyConnect SCEP註冊配置示例

目錄

簡介

SCEP註冊功能在AnyConnect獨立客戶端2.4中引入。在此過程中，可以修改AnyConnect XML配置檔案以包含與SCEP相關的配置，並為證書註冊建立特定的組策略和連線配置檔案。當AnyConnect使用者連線到此特定組時，AnyConnect向CA伺服器傳送證書註冊請求，並且CA伺服器自動接受或拒絕該請求。

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：

- 運行軟體版本8.x的Cisco ASA 5500系列自適應安全裝置
- Cisco AnyConnect VPN版本2.4

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

AnyConnect的自動SCEP註冊的目標是以安全且可擴展的方式向客戶端頒發證書。例如，使用者不需要從CA伺服器要求憑證。此功能整合在AnyConnect客戶端中。根據XML配置檔案中提到的證書引數，向客戶端頒發證書。

所需變更概述

AnyConnect SCEP註冊功能要求在XML配置檔案中定義某些證書引數。在ASA上為證書註冊建立組策略和連線配置檔案，XML配置檔案與該策略相關聯。AnyConnect客戶端連線到使用此特定策略的連線配置檔案，並傳送證書請求，該請求包含在XML檔案中定義的引數。證書頒發機構(CA)自動接受或拒絕該請求。如果在客戶端配置檔案中定義<CertificateSCEP>元素，AnyConnect客戶端將檢索使用SCEP協定的證書。

在AnyConnect嘗試自動檢索新證書之前，客戶端證書身份驗證必須失敗，因此，如果您已經安裝了有效的證書，則不會進行註冊。

當使用者登入到特定組時，將自動註冊。還有一種可用於證書檢索的手動方法，在該方法中，向使用者顯示**Get Certificate**按鈕。這只有在使用者端可以直接存取CA伺服器（而不是透過通道）時才能使用。

有關詳細資訊，請參閱Cisco AnyConnect VPN客戶端管理員指南2.4版。

啟用Anyconnect SCEP功能的XML設定

這些是需要在AnyConnect XML檔案中定義的重要元素。有關詳細資訊，請參閱Cisco AnyConnect VPN客戶端管理員指南2.4版。

- <AutomaticSEPPERost> — 指定為其配置SCEP證書檢索的ASA主機名和連線配置檔案（隧道組）。該值需要採用ASA\connection配置檔名稱的完全限定域名或ASA\connection配置檔名稱的IP地址的格式。
- <CAURL> — 標識SCEP CA伺服器。
- <CertificateSCEP> — 定義如何請求證書的內容。
- <DisplayGetCertButton> — 確定AnyConnect GUI是否顯示「獲取證書」按鈕。它使使用者能夠手動請求證書的續訂或調配。

以下是配置檔案範例：

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">false</UseStartBeforeLogon>
<AutomaticCertSelection UserControllable="true">true</AutomaticCertSelection>
<ShowPreConnectMessage>false</ShowPreConnectMessage>
<CertificateStore>All</CertificateStore>
<CertificateStoreOverride>false</CertificateStoreOverride>
<ProxySettings>Native</ProxySettings>
```

```
<AutoConnectOnStart UserControllable="true">true</AutoConnectOnStart>
<MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
<LocalLanAccess UserControllable="true">false</LocalLanAccess>
<AutoReconnect UserControllable="false">true
<AutoReconnectBehavior UserControllable="false">
     ReconnectAfterResume
   </AutoReconnectBehavior>
</AutoReconnect>
<AutoUpdate UserControllable="false">true</AutoUpdate>
<RSASecurIDIntegration UserControllable="false">
    Automatic
  </RSASecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
<WindowsVPNEstablishment>AllowRemoteUsers</WindowsVPNEstablishment>
<AutomaticVPNPolicy>false</AutomaticVPNPolicy>
<PPPExclusion UserControllable="false">Automatic
<PPPExclusionServerIP UserControllable="false"></PPPExclusionServerIP>
</PPPExclusion>
<EnableScripting UserControllable="false">false</EnableScripting>
<CertificateEnrollment>
<AutomaticSCEPHost>asa2.cisco.com/certenroll</AutomaticSCEPHost>
<CAURL PromptForChallengePW="false">
     http://10.11.11.1/certsrv/mscep/mscep.dll
   </CAURL>
<CertificateSCEP>
<Name_CN>cisco</Name_CN>
<Company_O>Cisco</Company_O>
<DisplayGetCertButton>true</DisplayGetCertButton>
</CertificateSCEP>
</CertificateEnrollment>
</ClientInitialization>
<ServerList>
<HostEntry>
<HostName>asa2.cisco.com</HostName>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

配置ASA以支援AnyConnect的SCEP協定

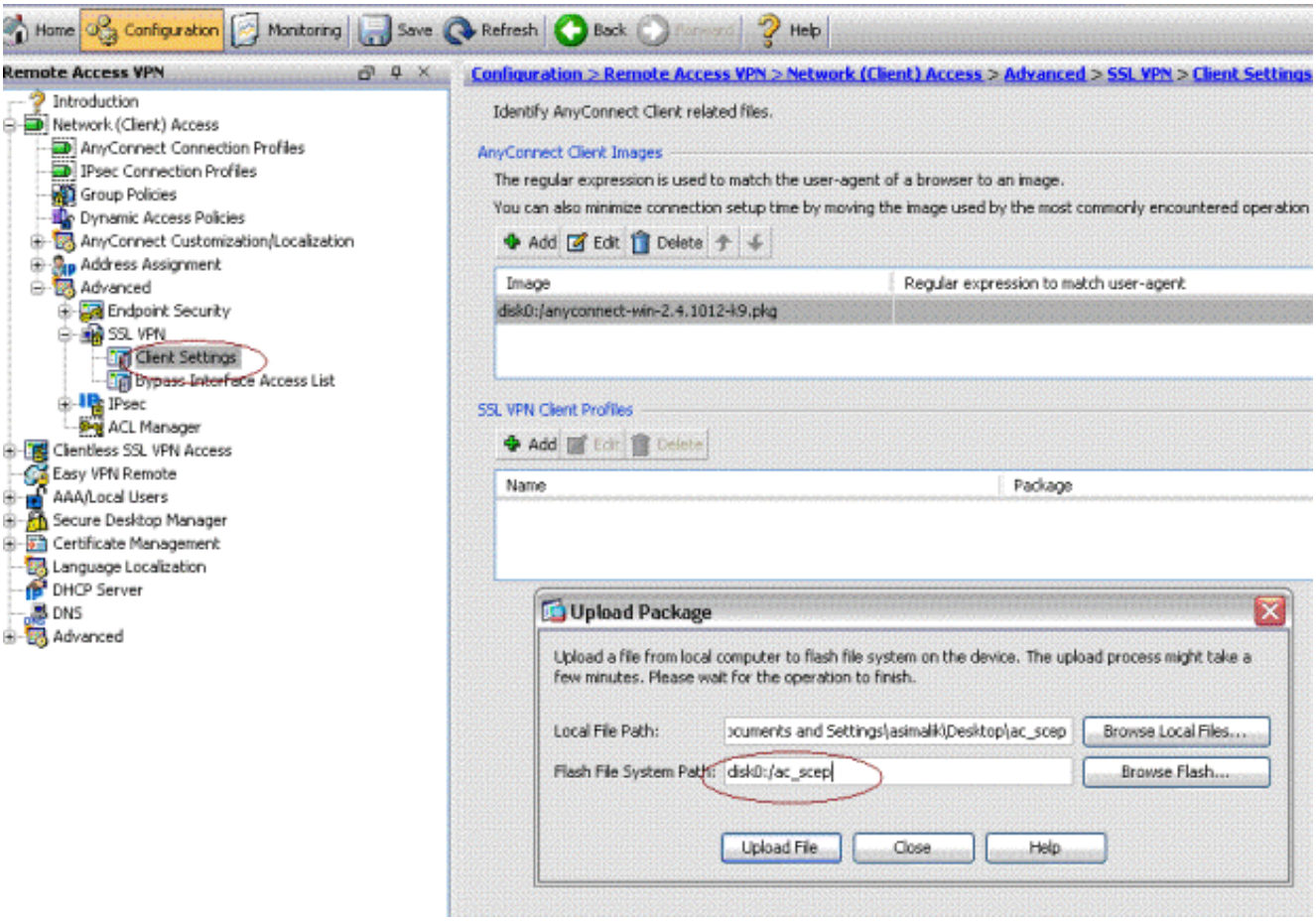
為了提供對專用註冊機構(RA)的訪問，ASA管理員必須建立一個別名，該別名的ACL限制專用端與所需RA的網路連線。為了自動檢索證書，使用者連線到此別名並進行身份驗證。

請完成以下步驟：

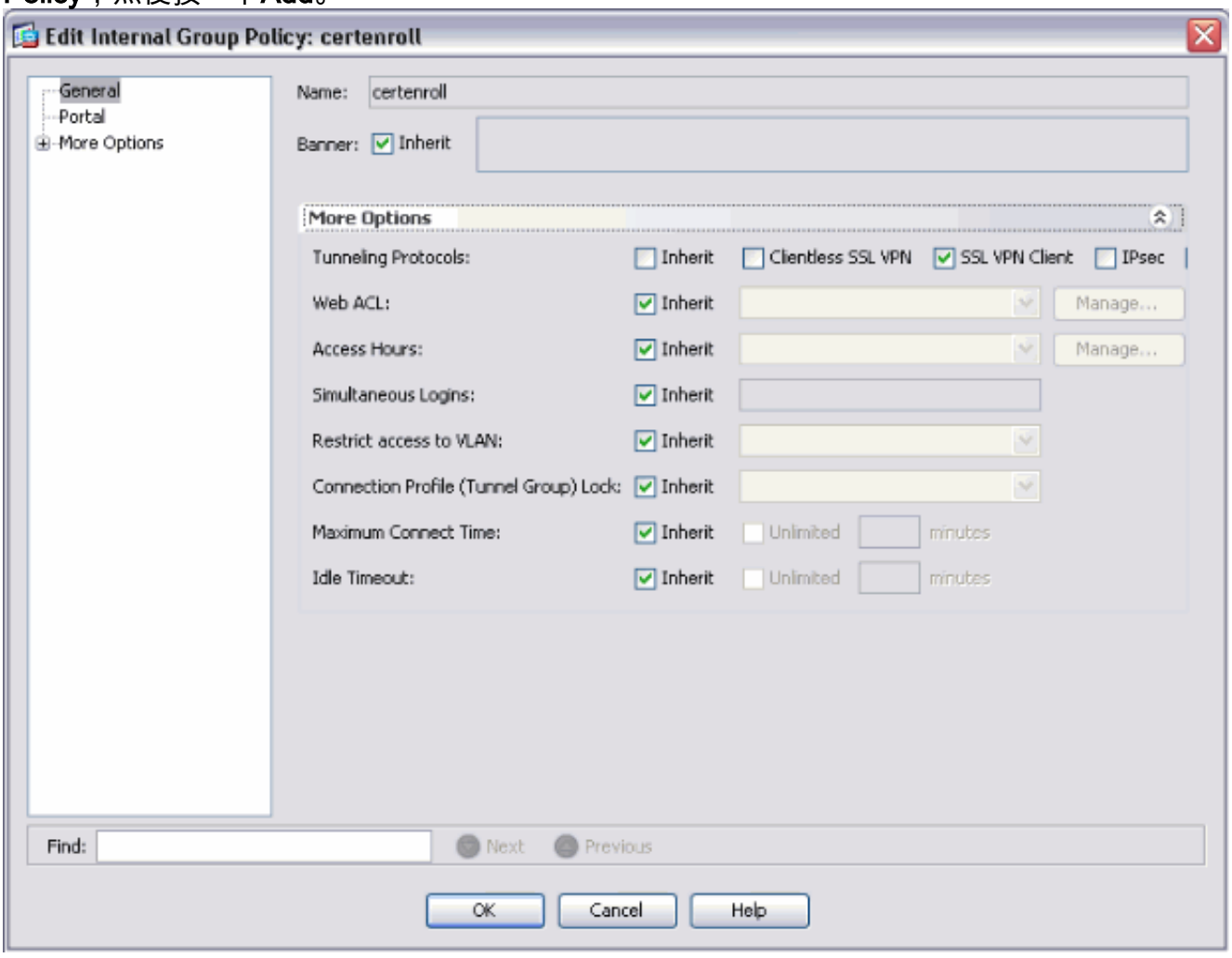
1. 在ASA上建立指向特定配置組的別名。
2. 在使用者客戶端配置檔案的<AutomaticSEPPERost>元素中指定別名。
3. 將包含<CertificateEnrollment>部分的客戶端配置檔案附加到特定配置組。
4. 為特定配置組設定ACL以限制流向私有RA的流量。

請完成以下步驟：

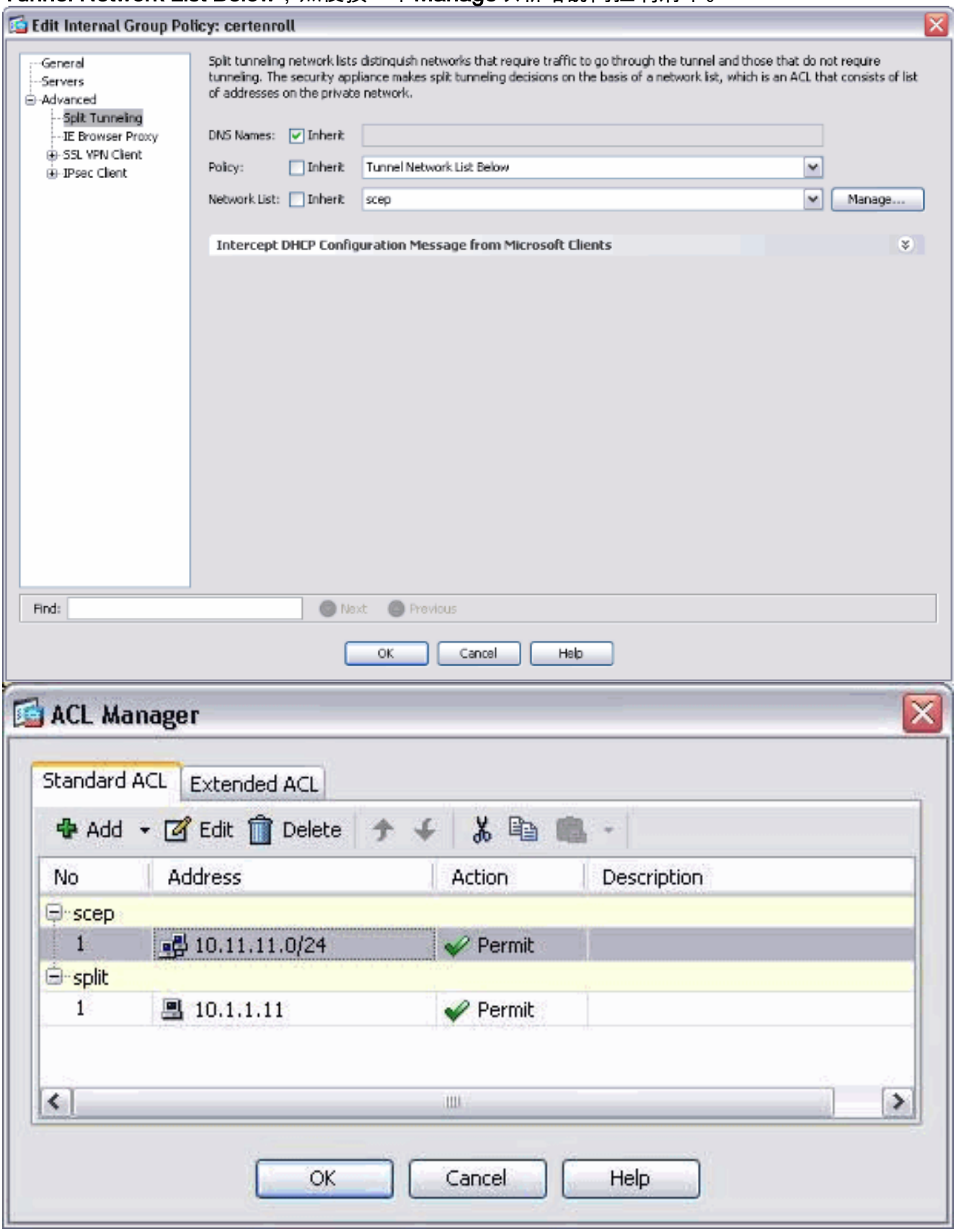
1. 將XML配置檔案上傳到ASA。選擇**Remote Access VPN > Network(client)access > Advanced > SSL VPN > Client settings**。在SSL VPN Client profiles下，按一下**Add**。按一下「**Browse Local Files**」以選擇設定檔檔案，然後按一下「**Browse Flash**」以指定快閃記憶體檔案名稱。按一下「**Upload File**」。



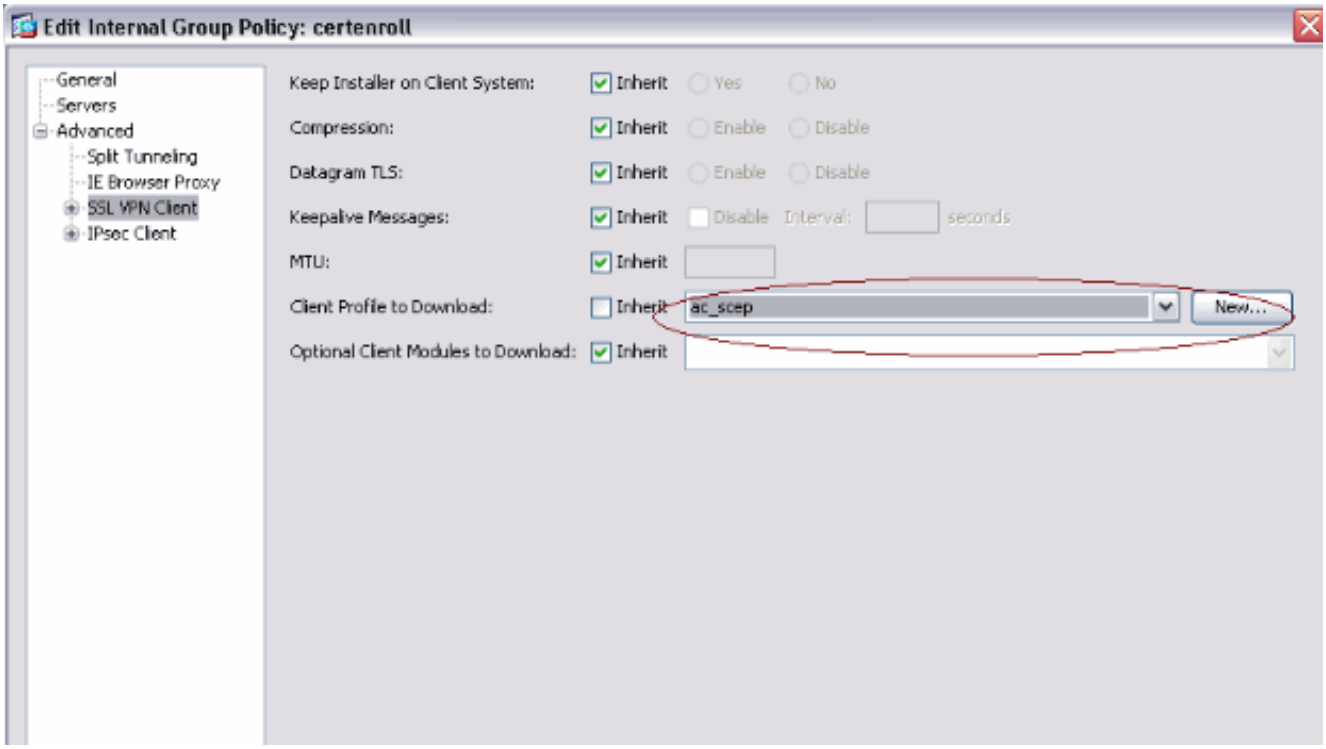
2. 為證書註冊設置certenroll組策略。選擇Remote access VPN > Network client access > Group Policy，然後按一下Add。



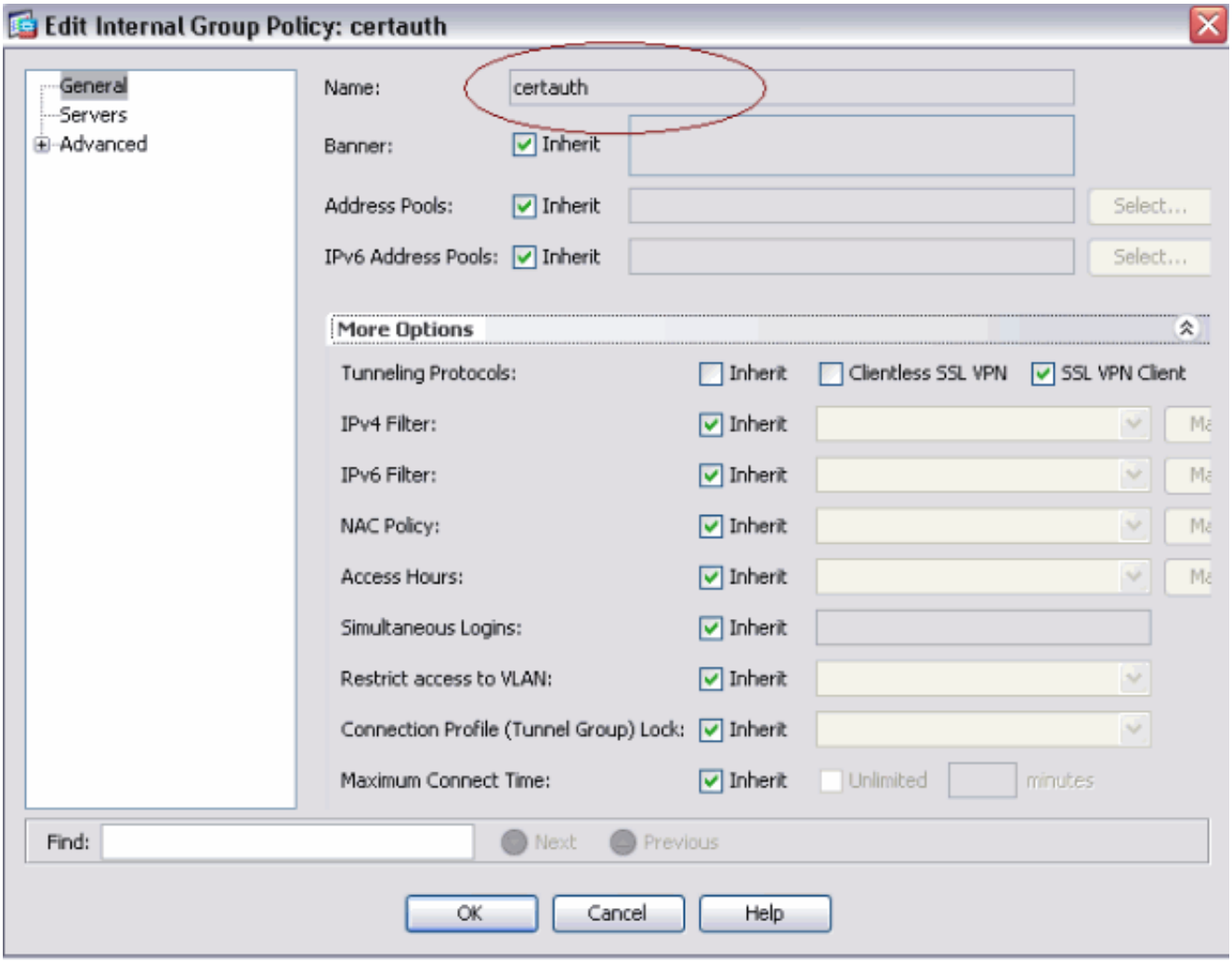
為CA伺服器新增拆分隧道。展開**Advanced**，然後選擇**Split Tunneling**。從Policy選單中選擇**Tunnel Network List Below**，然後按一下**Manage**以新增訪問控制清單。



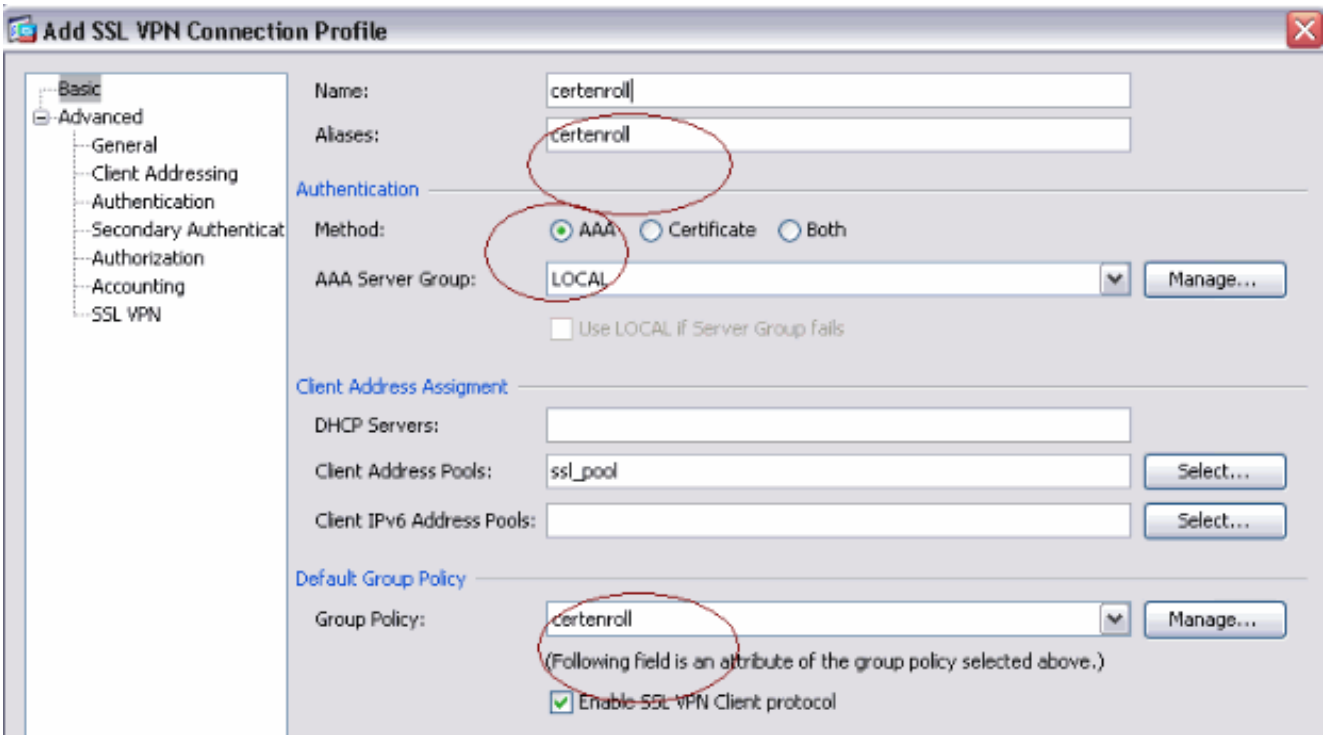
選擇**SSL VPN Client**，然後從**Client Profile to Download**選單中選擇certenroll的配置檔案。



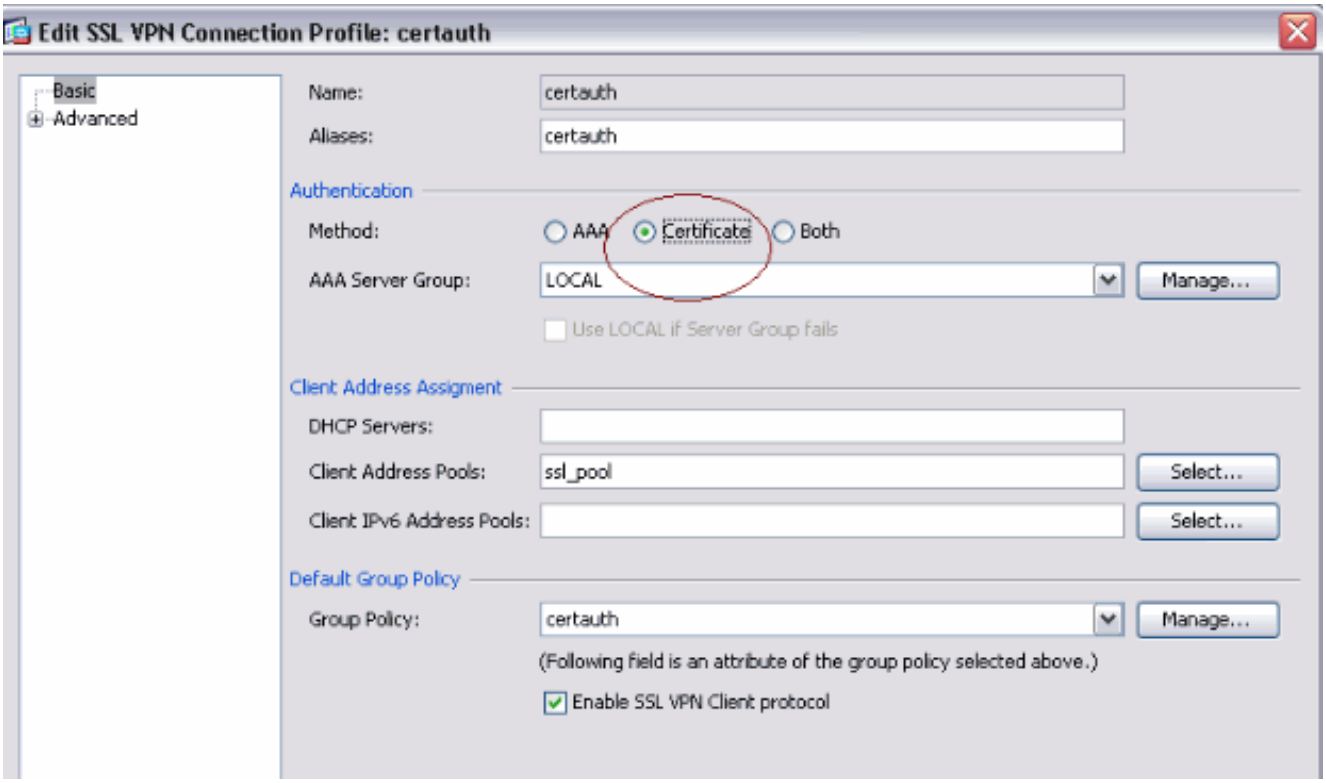
3. 為證書身份驗證建立另一個名為**certauth**的組。



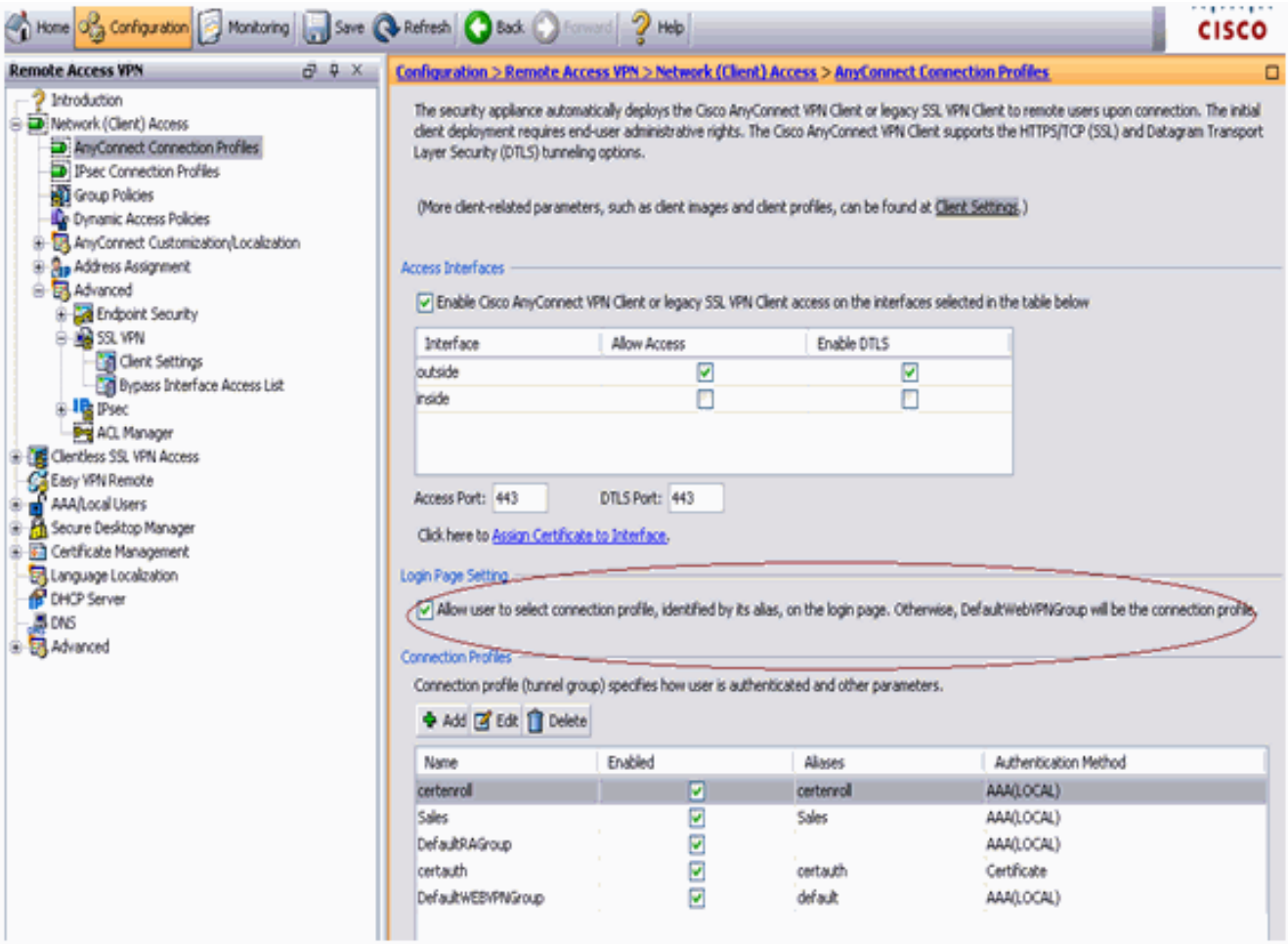
4. 建立certenroll連線配置檔案。選擇**Remote access VPN > Network client access > AnyConnect connection profiles**，然後按一下**Add**。在「別名」欄位中輸入**certenroll**組。**注意**：別名必須與AutomaticSEPPERost下的AnyConnect配置檔案中使用的值匹配。



5. 使用證書身份驗證製作另一個名為**certauth**的連線配置檔案。這是註冊後使用的實際連線配置檔案。



6. 為了確保啟用別名使用，請在登入頁面上選中**Allow user to select connection profile，identified by its alias。否則，DefaultWebVPNGroup是連線配置檔案。**



測試AnyConnect SCEP

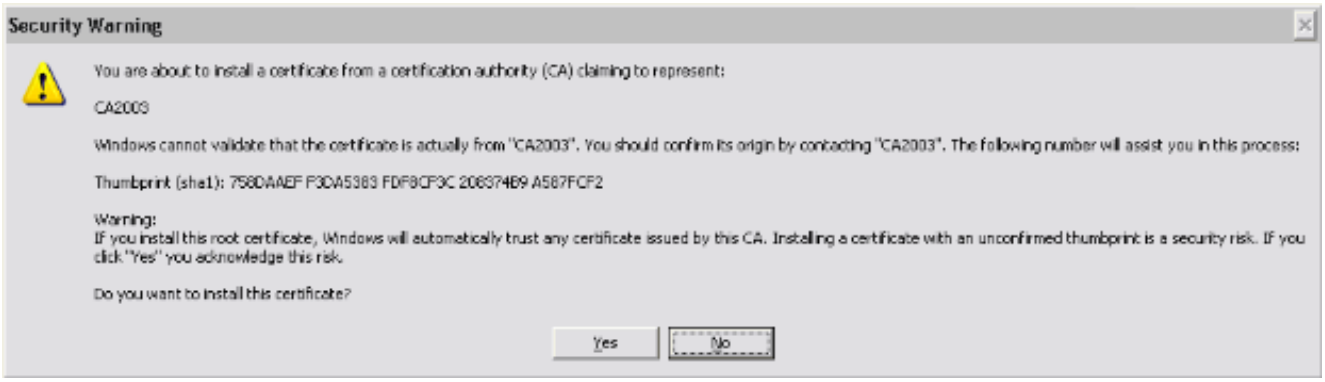
使用本節內容，確認您的組態是否正常運作。

1. 啟動AnyConnect客戶端，並連線到certenroll配置檔案。

AnyConnect通過SCEP將註冊

請求傳遞到CA伺服器。如果使用**Get Certificate**按鈕，AnyConnect會直接傳遞註冊請求，而不通過隧道。

2. 出現此警告。按一下**Yes**安裝使用使用者和根證書



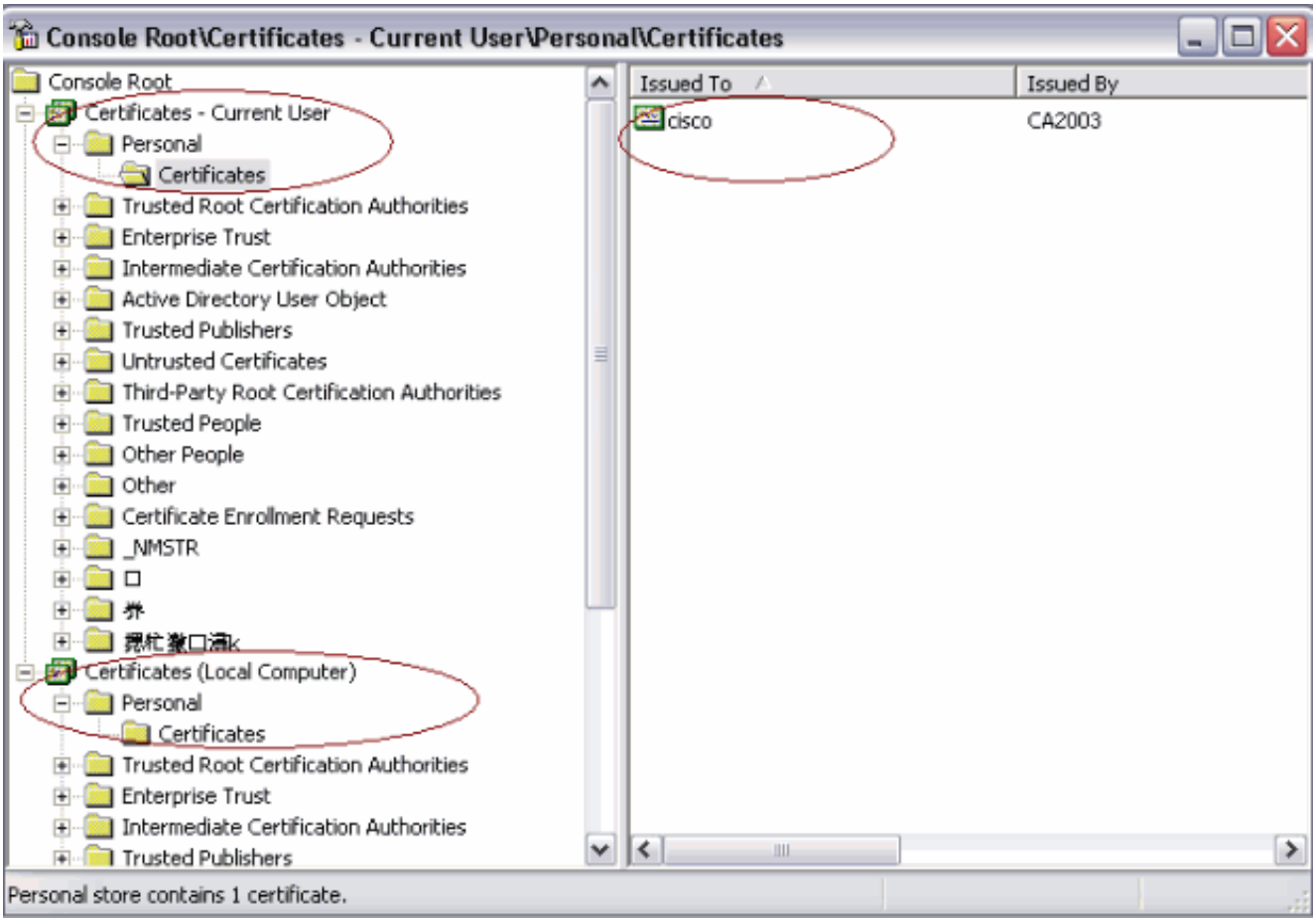
3. 註冊證書後，連線到**certauth**配置檔案。

SCEP請求後Microsoft Windows上的證書儲存

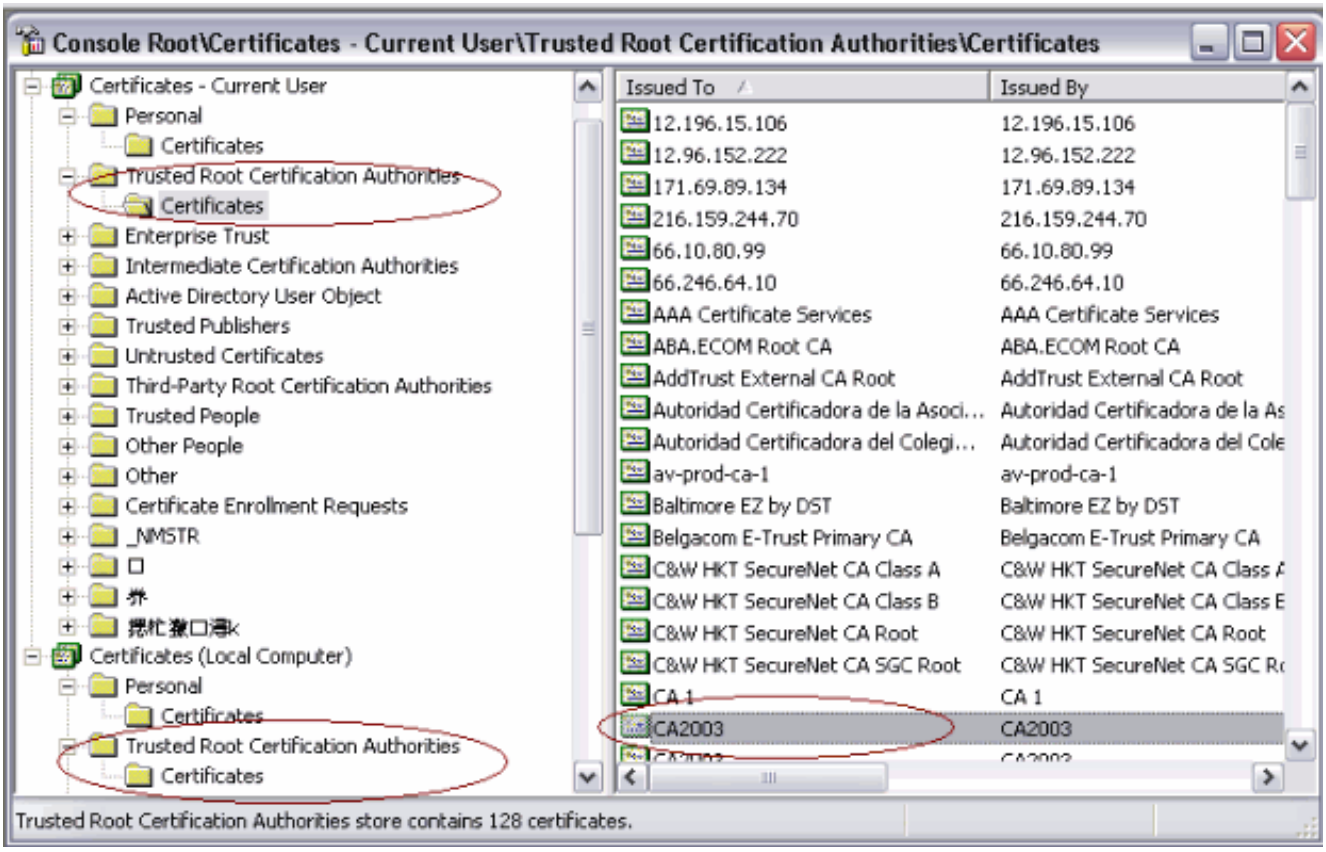
請完成以下步驟：

1. 按一下**開始>運行> mmc**。
2. 按一下**Add/remove snap in**。
3. 按一下「**Add**」，然後選擇「**certificates**」。

4. 新增My user account和computer account證書。此圖顯示安裝在Windows證書儲存中的使用者證書
:



此圖顯示安裝在Windows證書儲存中的CA證書
:



疑難排解

本節提供的資訊可用於對組態進行疑難排解。

- AnyConnect SCEP註冊僅在證書身份驗證失敗時起作用。如果未註冊，請檢查證書儲存。如果已安裝證書，請刪除這些證書，然後重新測試。
- 除非使用**ssl certificate-authentication interface outside port 443**命令，否則SCEP註冊不起作用。如需詳細資訊，請參閱以下思科錯誤ID:思科錯誤ID CSCtf06778(僅供註冊客戶使用)- AnyConnect SCEP註冊不適用於Per Group Cert Auth 2思科漏洞ID CSCtf06844(僅限註冊客戶)- AnyConnect SCEP註冊不用於ASA每組證書身份驗證
- 如果CA伺服器位於ASA外部，請確保使用**same-security-traffic permit intra-interface**命令允許髮夾操作。另外新增nat outside和access-list命令，如以下示例所示：
```
nat (outside) 1
access-list natoutside extended permit ip 172.16.1.0 255.255.255.0 host 171.69.89.87
```
其中172.16.1.0是AnyConnect池，171.69.89.87是CA伺服器IP地址。
- 如果CA伺服器位於內部，請確保將其包括在certenroll組策略的拆分隧道訪問清單中。在本文檔中，假設CA伺服器位於內部。
```
group-policy certenroll attributes
split-tunnel-policy tunnelspecified
 split-tunnel-network-list value scep

access-list scep standard permit 171.69.89.0 255.255.255.0
```

相關資訊

- Cisco AnyConnect VPN客戶端管理員指南2.4版
- 技術支援與文件 - Cisco Systems