使用CAC和智慧卡讀卡器配置VCS

目錄

簡介

本文檔介紹安裝和使用智慧卡讀卡器和通用訪問卡登入的逐步指南，以便用於需要對VCS環境（如銀行、醫院或具有安全設施的政府）進行雙因素身份驗證的組織。

必要條件

需求

本文件沒有特定需求。

採用元件

本文檔中的資訊基於Cisco Expressway管理員(X14.0.2)。

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。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

CAC提供所需的身份驗證，以便「系統」瞭解誰獲得了對其環境的訪問許可權，以及基礎架構的哪個部分是物理或電子的。在政府機密環境和其他安全網路中，「最低許可權訪問」或「需要知道」的規則普遍適用。登入可以被任何人使用，驗證需要使用者擁有的東西，例如2006年出現的CAC，也稱為通用訪問卡，因此個人不需要使用多種裝置，無論是家庭用具、身份證或軟體加密狗來訪問其就業場所或系統。

什麼是智慧卡？

智慧卡是Microsoft用於整合到Windows平台的公鑰基礎設施(PKI)的關鍵元件，因為智慧卡增強了僅軟體解決方案，如客戶端身份驗證、登入和安全電子郵件。智慧卡是公鑰證書和關聯金鑰的聚合點，因為它們是：

- 為保護私鑰和其他形式的個人資訊提供防篡改儲存。
- 隔離安全關鍵計算，這涉及身份驗證、數位簽章和來自系統其他不需要知道的部分的金鑰交換。
- 支援在工作、家中或路上的電腦之間攜帶憑證和其他私人資訊。

智慧卡已成為Windows平台不可缺少的一部分，因為智慧卡提供了一些新的和理想的功能，如滑鼠或CD-ROM的引入對電腦行業具有革命性的意義。 如果您目前沒有內部PKI基礎設施，則需要首先確保執行此操作。本文檔沒有介紹如何在此特定文章中安裝此角色，但是有關如何實施此角色的資訊可以在以下網址找到：http://technet.microsoft.com/en-us/library/hh831740.aspx。

設定

本實驗假定您已將LDAP與VCS整合，並且擁有可以使用LDAP憑據登入的使用者。

1. 實驗裝置
2. 安裝智慧卡
3. 配置證書頒發機構模板
4. 註冊代理證書
5. 代表……註冊
6. 為通用接入卡配置VCS

所需裝置：

具有以下角色/已安裝軟體的Windows 2012R2域伺服器：

- 證書頒發機構
- Active Directory
- DNS
- 連線了智慧卡的Windows PC
- vSEC:用於管理智慧卡的CMS K系列管理軟體：

Versa讀卡器軟體

安裝智慧卡

智慧卡讀卡器通常會提供有關如何連線任何必要電纜的說明。以下是此組態的安裝範例。

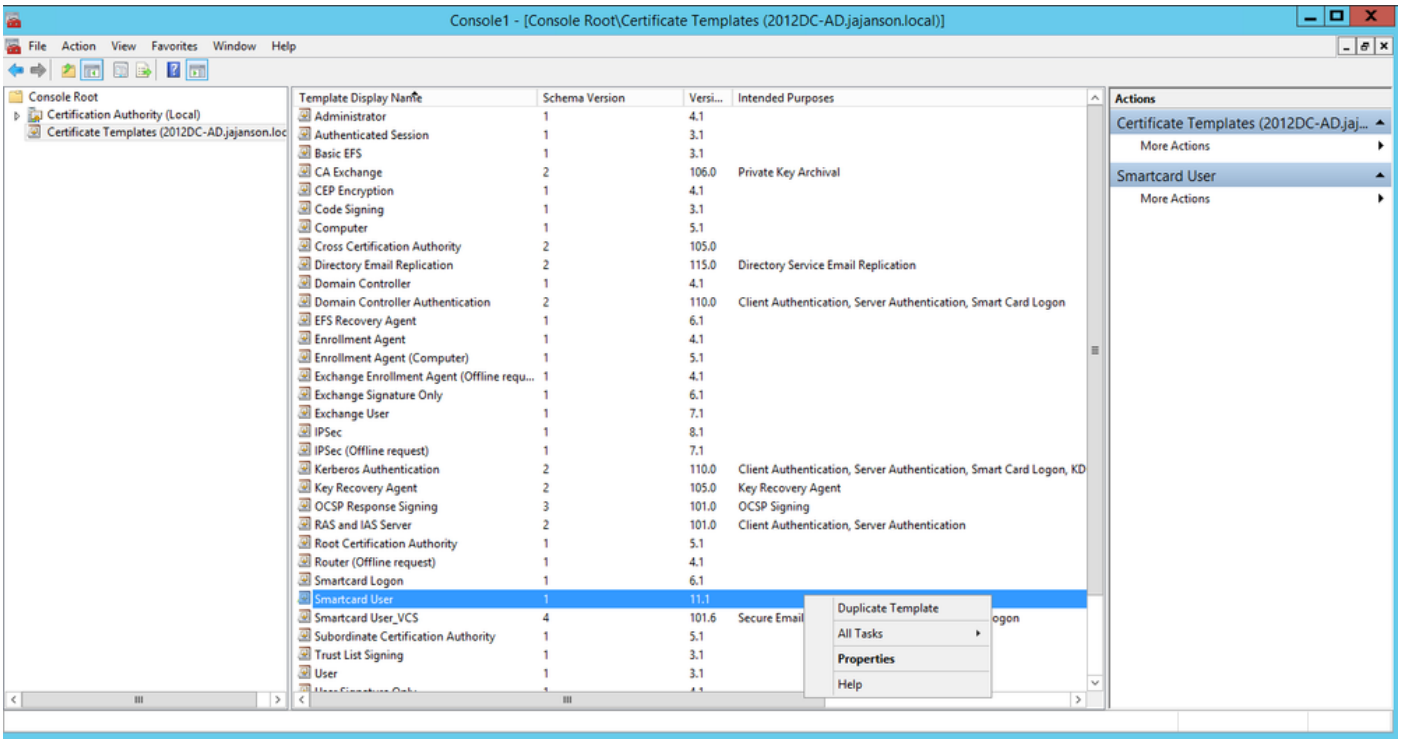
如何安裝智慧卡讀卡器裝置驅動程式

如果檢測到並安裝了智慧卡讀卡器，歡迎使用Windows登入螢幕會確認這一點。如果不是：

1. 將智慧卡連線到Windows PC上的USB埠
2. 按照螢幕上的說明安裝裝置驅動程式軟體。這需要在Windows中發現智慧卡製造商或驅動程式的驅動程式介質。就我而言，我使用的是製造商的下載站點驅動程式。**不信任WINDOWS。**
3. 按一下右鍵案頭上的**My Computer**圖示，然後按一下子選單上的**Manage**。
4. 展開**服務和應用**節點，然後按一下**服務**。
5. 在右窗格中，按一下右鍵**智慧卡**。在子選單上按一下**Properties**。
6. 在「**General** 」索引標籤上，在「**Startup Type**」下拉式清單中選擇**Automatic**。按一下「**OK**」（確定）。
7. 如果硬體嚮導指示您重新啟動電腦，請重新啟動電腦。

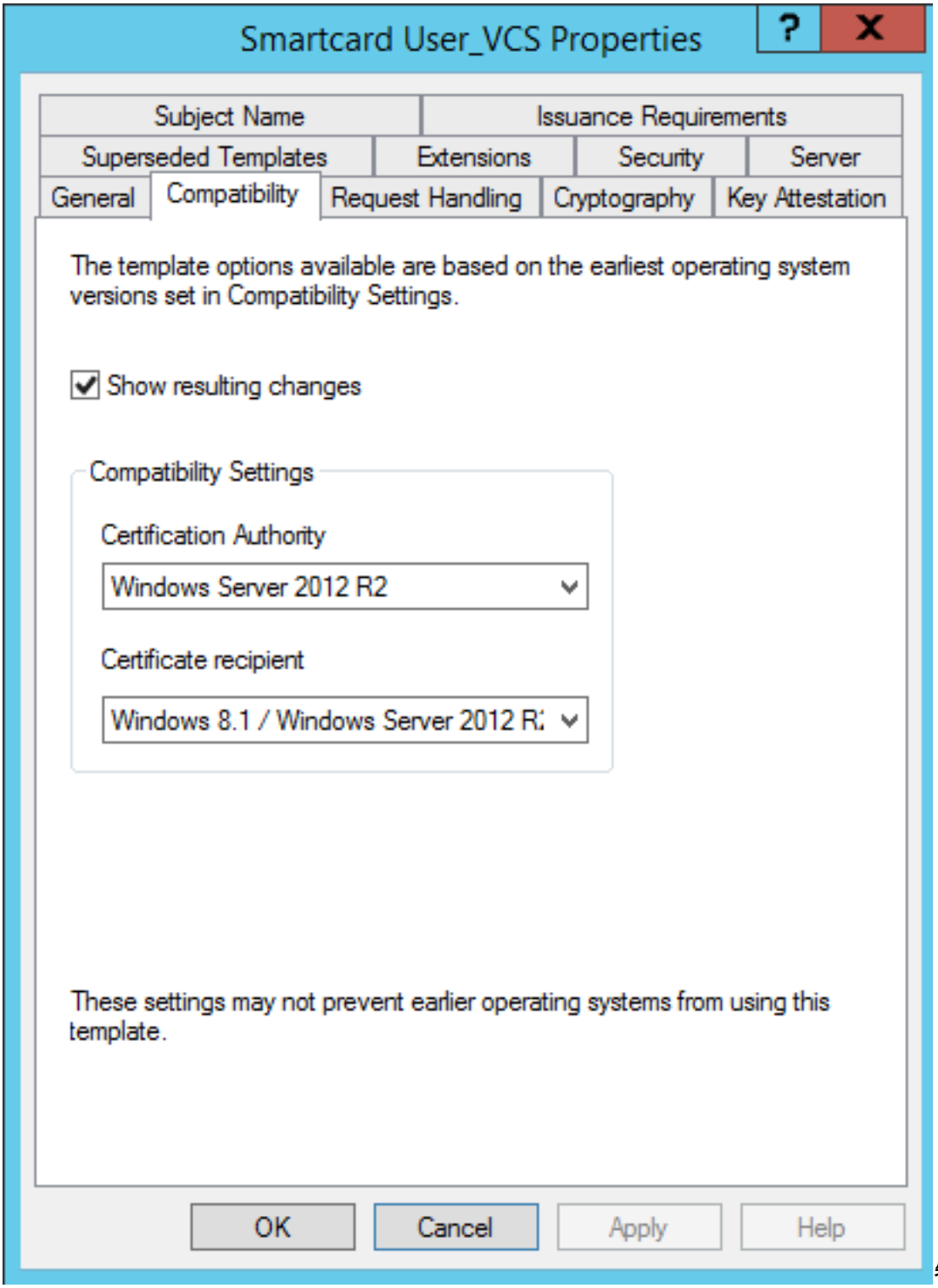
配置證書頒發機構模板

1. 從管理工具啟動證書頒發機構MMC。
2. 按一下或選擇「**Certificate Templates**」節點，然後選擇「**Manage**」。
3. 按一下右鍵或選擇**Smartcard User** Certificate Template，然後選擇**Duplicate**，如下圖所示。



域控制器證書模板

4.在**Compatibility**頁籤的**Certification Authority**下，檢查選擇內容並根據需要進行更改。

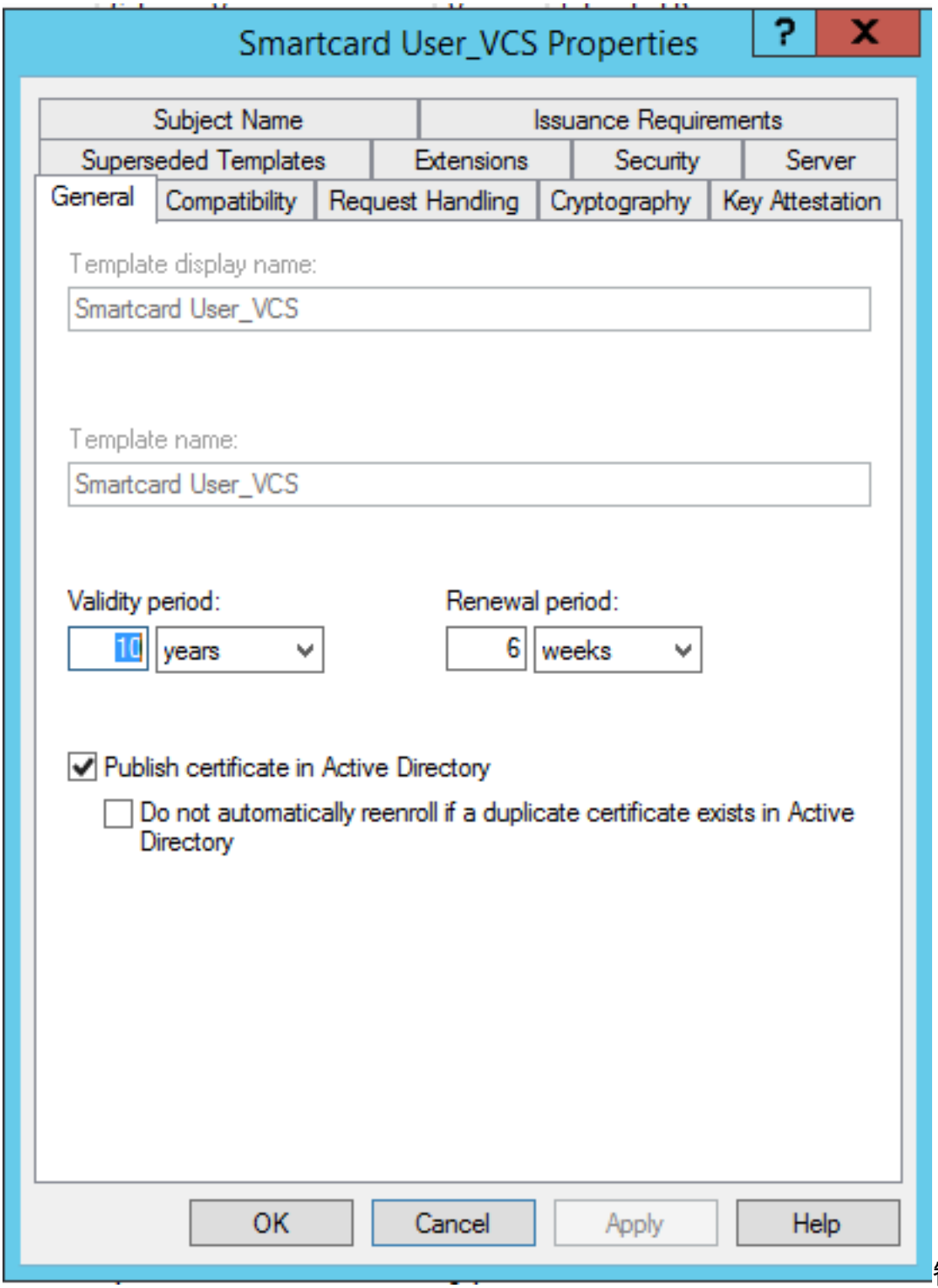


智慧卡相容性設定

5.在**General**索引標籤上：

a.指定名稱，例如**Smartcard User_VCS**。

b.將有效期設定為所需值。按一下「**Apply**」。

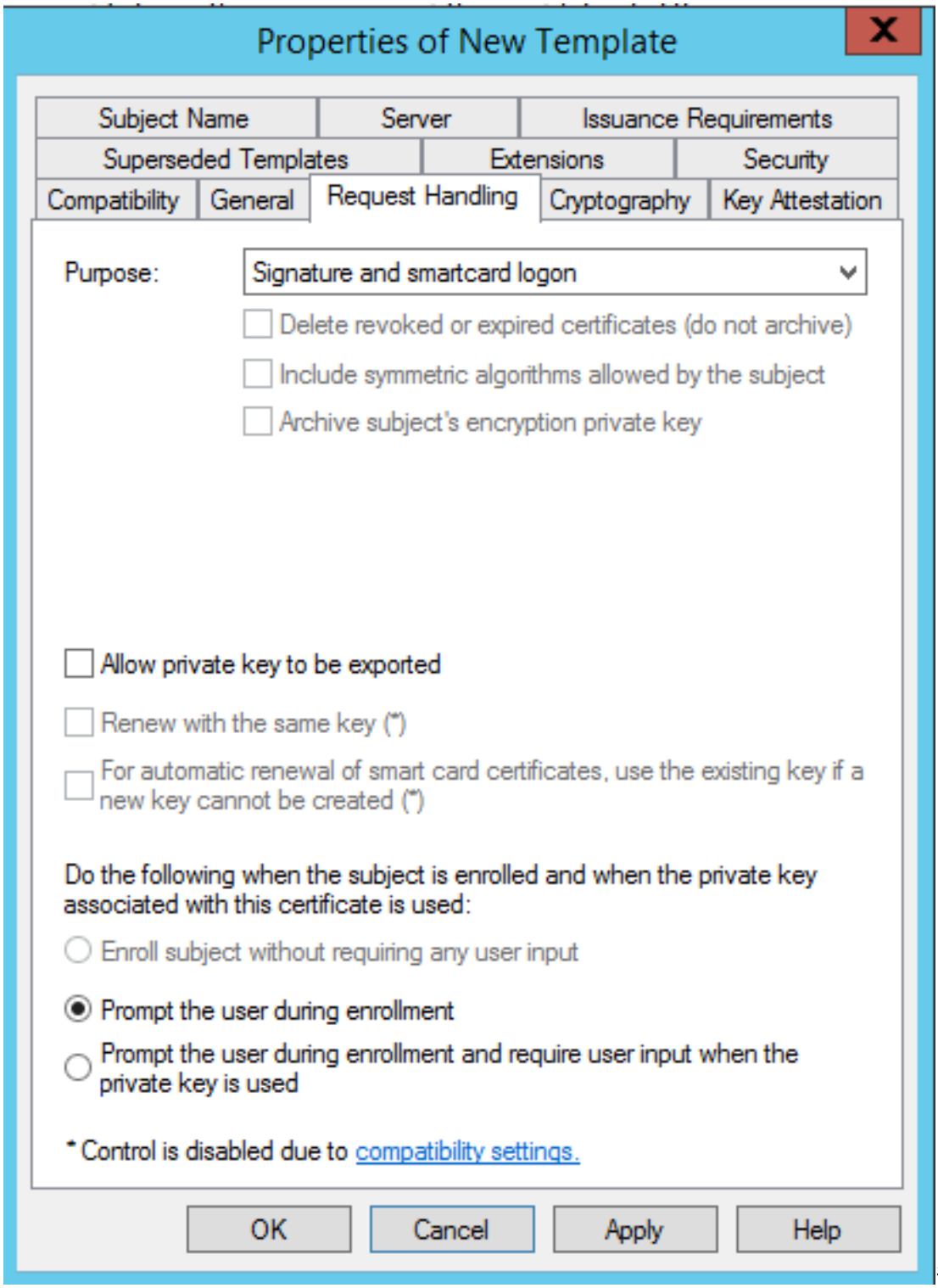


智慧卡常規時間開始過期

6.在「請求處理」選項卡上：

a.將Purpose設定為Signature and smartcard logon。

b.按一下註冊過程中提示使用者。按一下「Apply」。

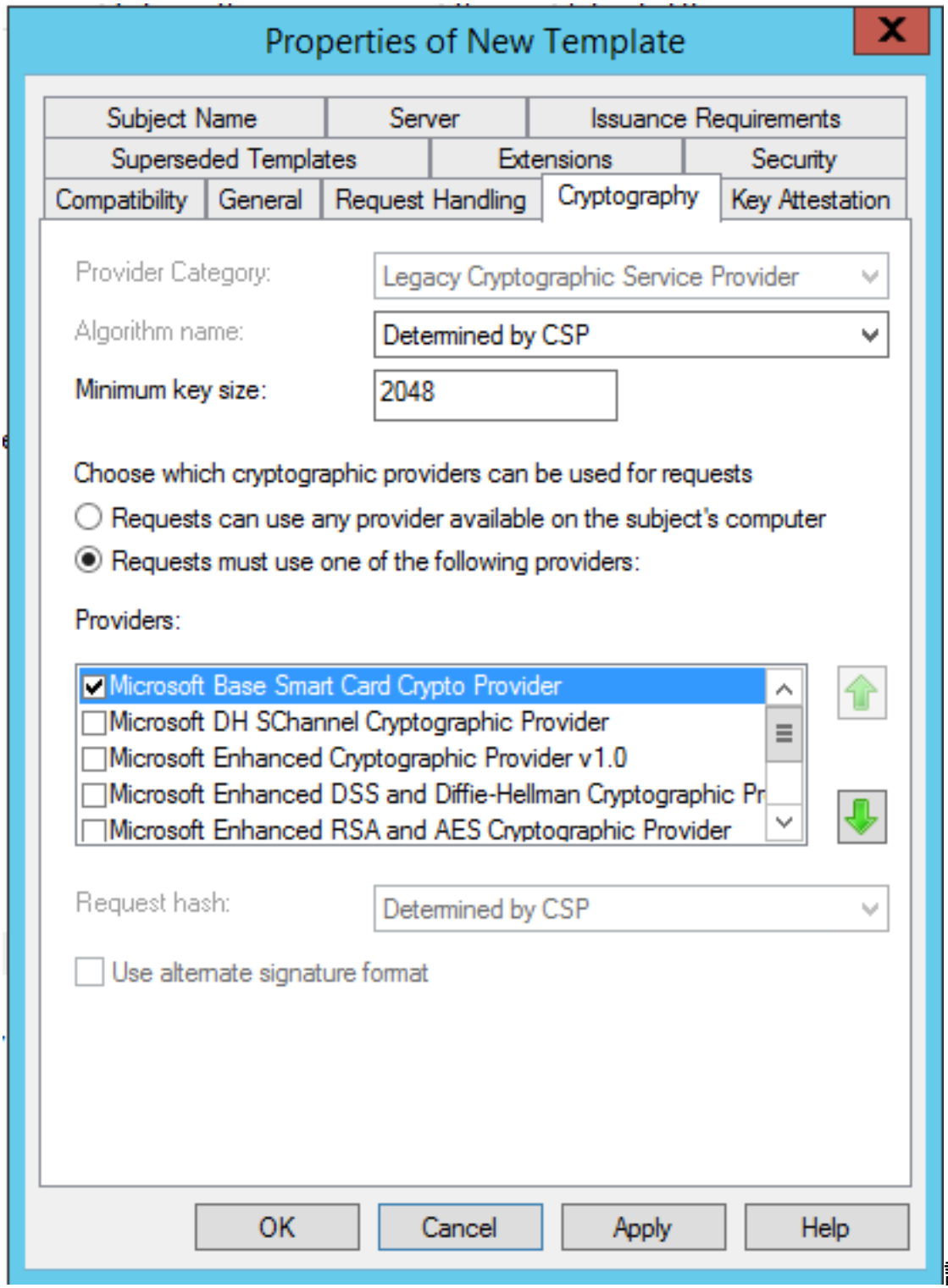


智慧卡請求處理

7.在**加密**頁籤上，將最小金鑰大小設定為2048。

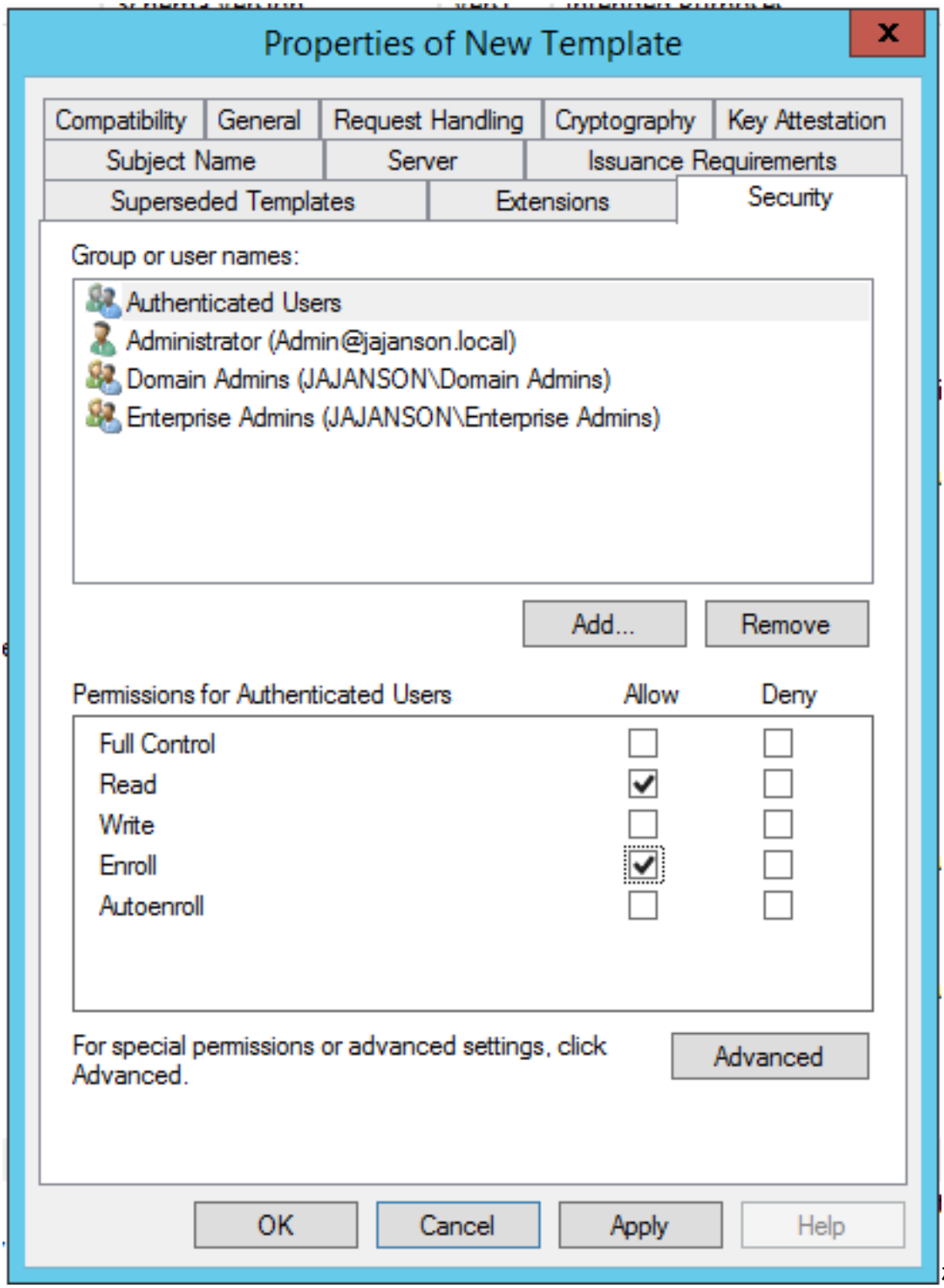
a.按一下**Requests must use of the following providers**，然後選擇**Microsoft Base Smart Card Crypto Provider**。

b.按一下**Apply**。



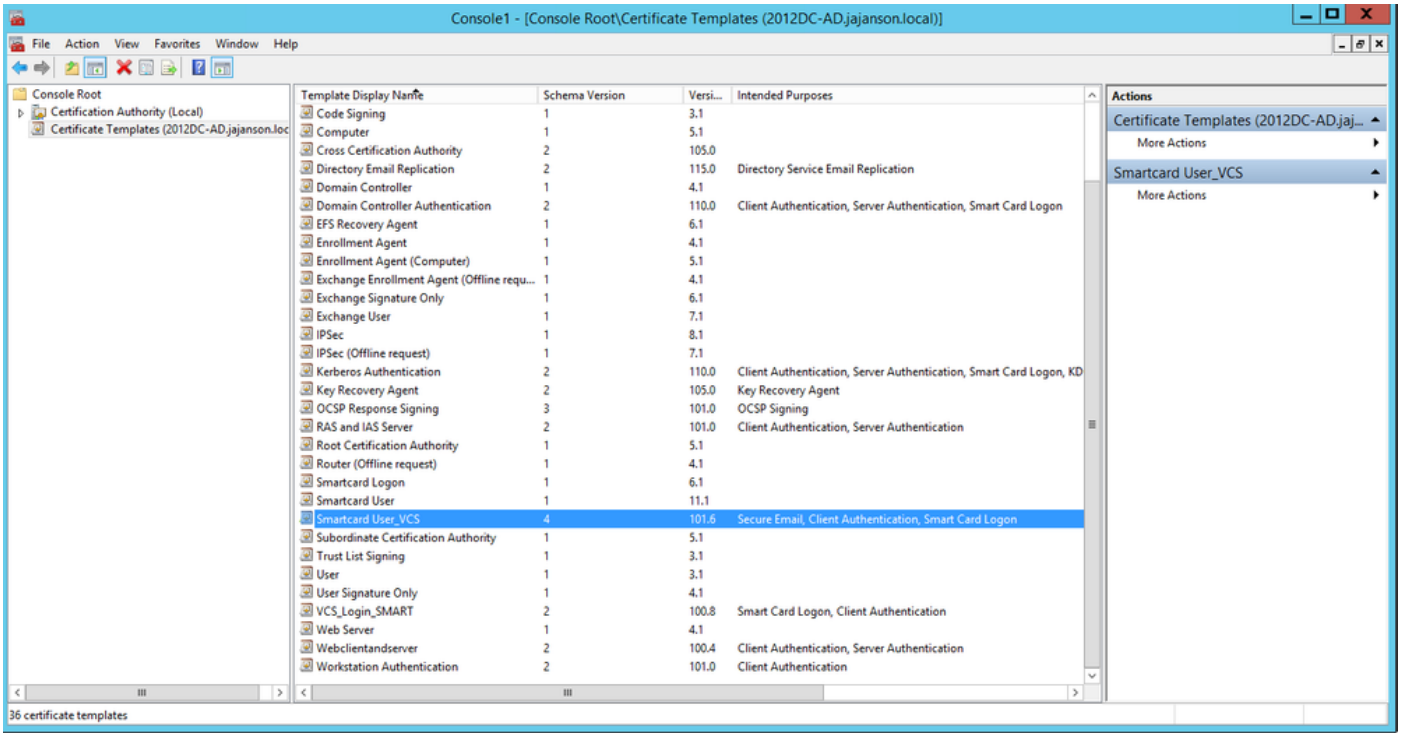
證書加密設定

8. 在「安全」頁籤上，新增要授予註冊訪問許可權的安全組。例如，如果要授予所有使用者的訪問許可權，請選擇「已驗證使用者」組，然後選擇**註冊**這些使用者的許可權。



模板安全性

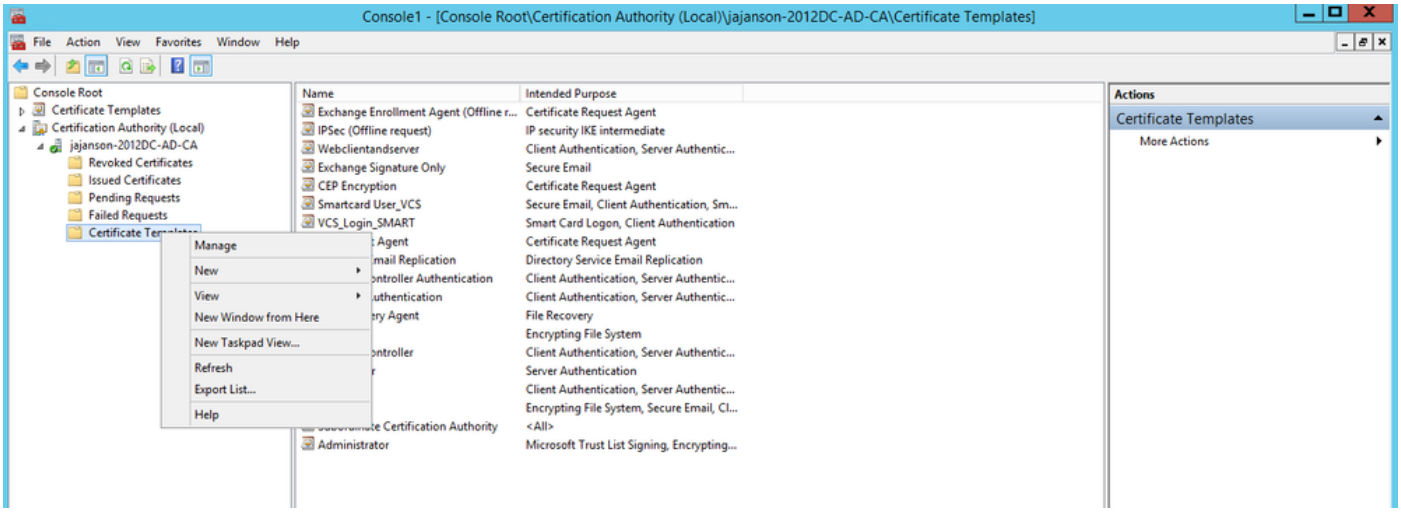
9.按一下**確定**以完成更改並建立新模板。您的新模板現在必須出現在證書模板清單中。



域控制中顯示的模板

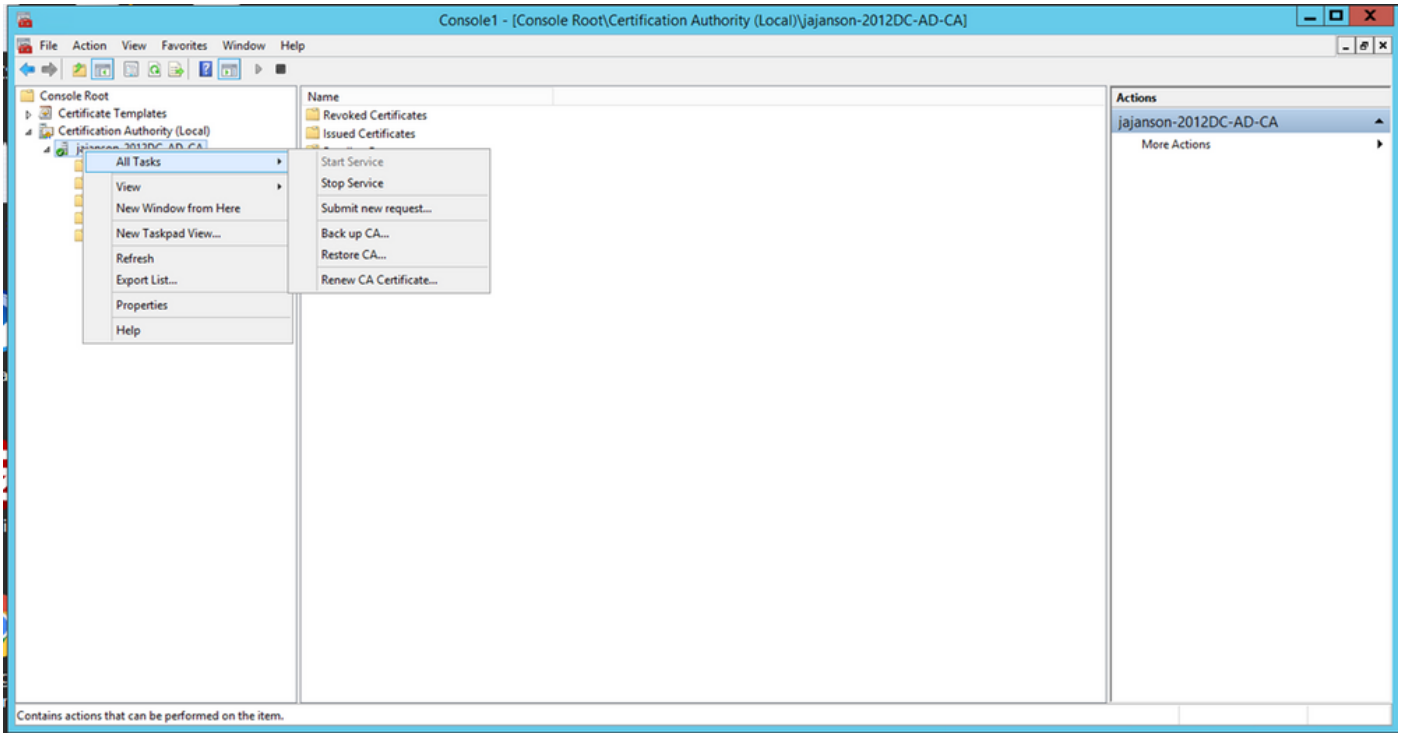
10. 在MMC的左窗格中，展開「證書頒發機構（本地）」，然後在「證書頒發機構」清單中展開CA。

按一下右鍵「Certificate Templates」，按一下「**New**」，然後按一下「**Certificate Template**」以核發。然後選擇新建立的智慧卡模板。



發佈新模板

11.複製模板後，在MMC中，按一下右鍵或選擇「證書頒發機構」清單，按一下「**所有任務**」，然後按一下「停止**服務**」。然後，再次按一下右鍵CA的名稱，按一下**All Tasks**，然後按一下**Start Service**。

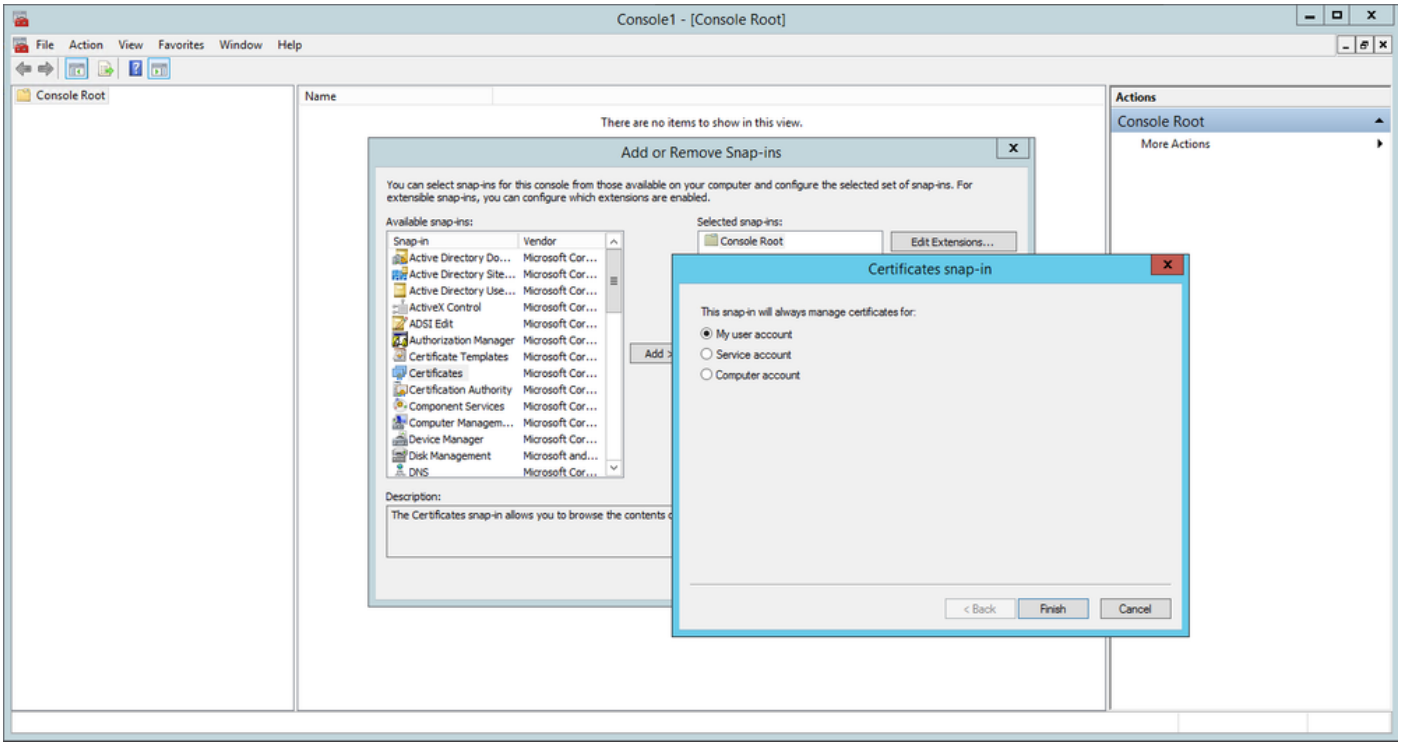


停止然後啟動證書服務

註冊代理證書上的註冊

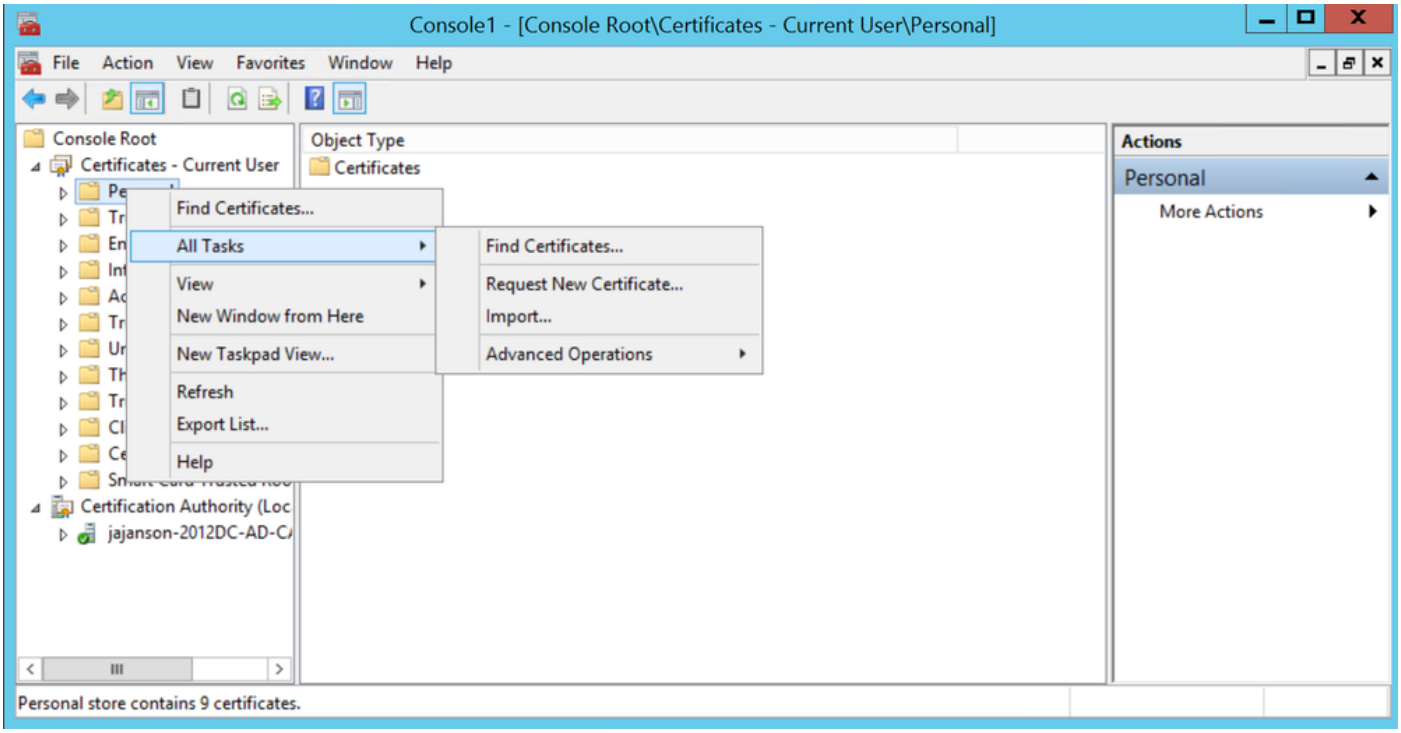
建議您在客戶端電腦（IT管理員案頭）上執行此操作。

1. 啟動MMC選擇**Certificates**，按一下**Add**，然後按一下**My User Account**的證書。



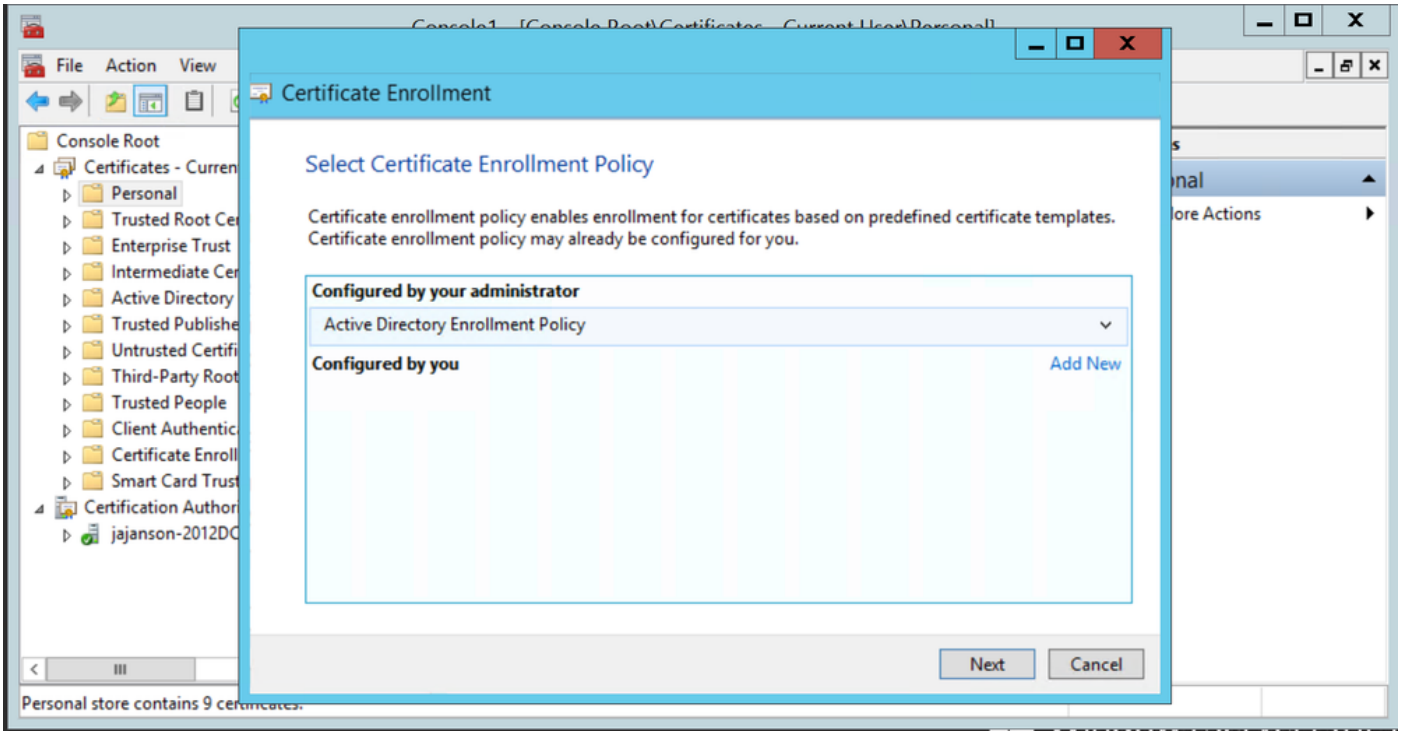
新增證書

2. 按一下右鍵或選擇**Personal Node**，選擇**All Tasks**，然後選擇**Request New Certificate**。



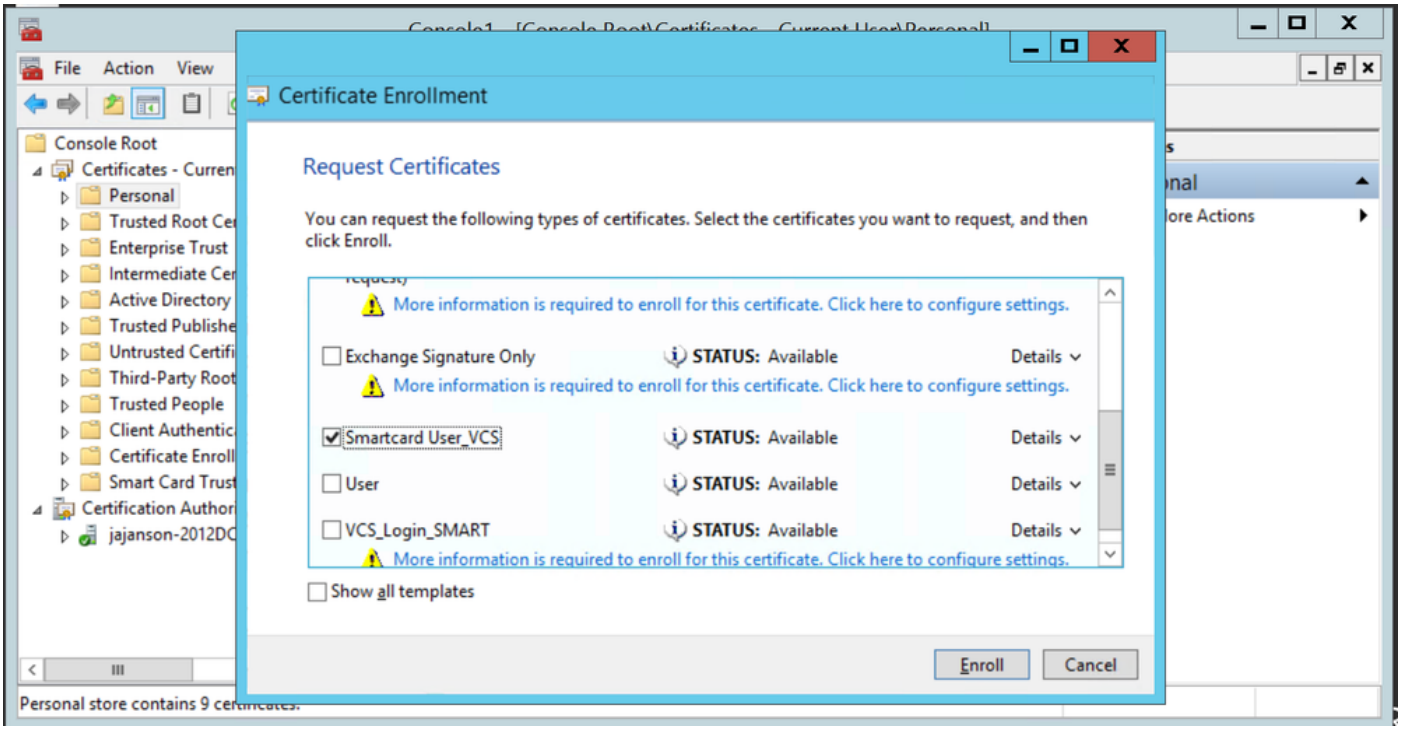
請求新證書

3.按一下嚮導上的**下一步**，然後選擇**Active Directory註冊策略**。然後再次按一下**Next**。



Active Directory註冊

4.選擇**Enrollment Agent Certificate**(本例中為**Smartcard User_VCS**)，然後按一下**Enroll（註冊）**。

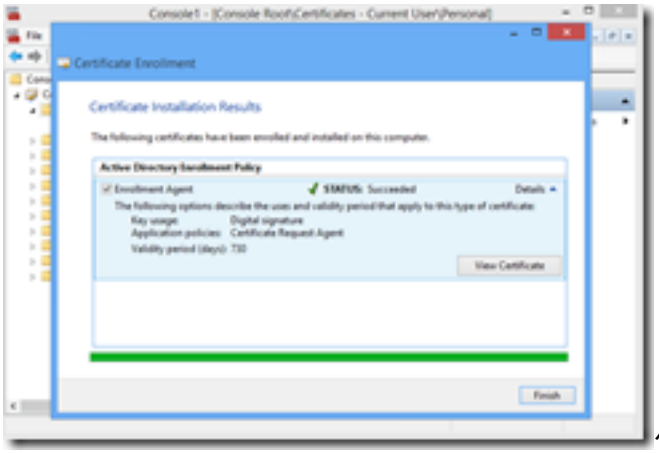


註冊證書代理

您的IT管理員案頭現已設定為註冊站，這使您能夠代表其他使用者註冊新的智慧卡。

代表……註冊

為了現在為員工提供用於身份驗證的智慧卡，您需要註冊這些智慧卡並生成證書，然後將其匯入到智慧卡中。

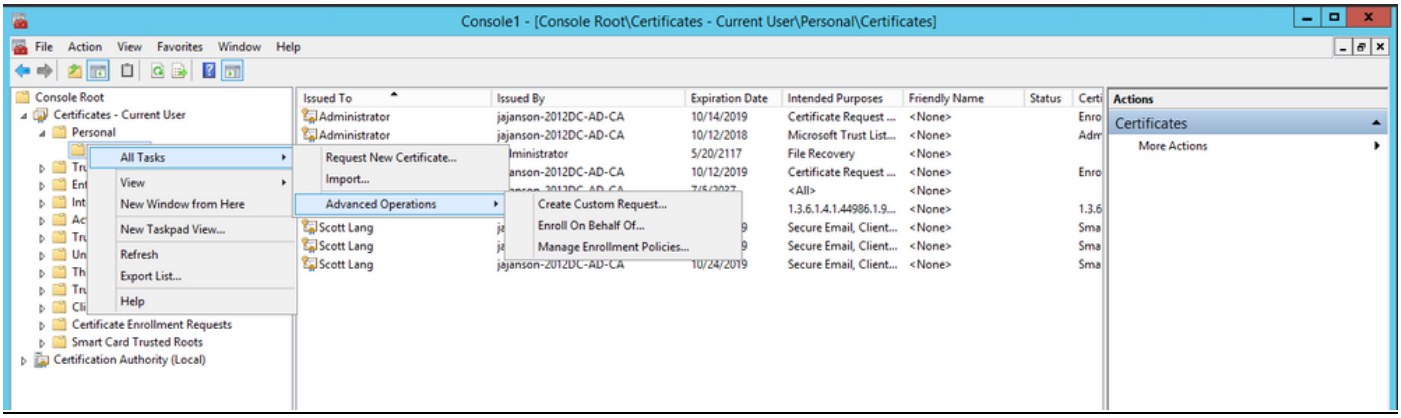


代表註冊

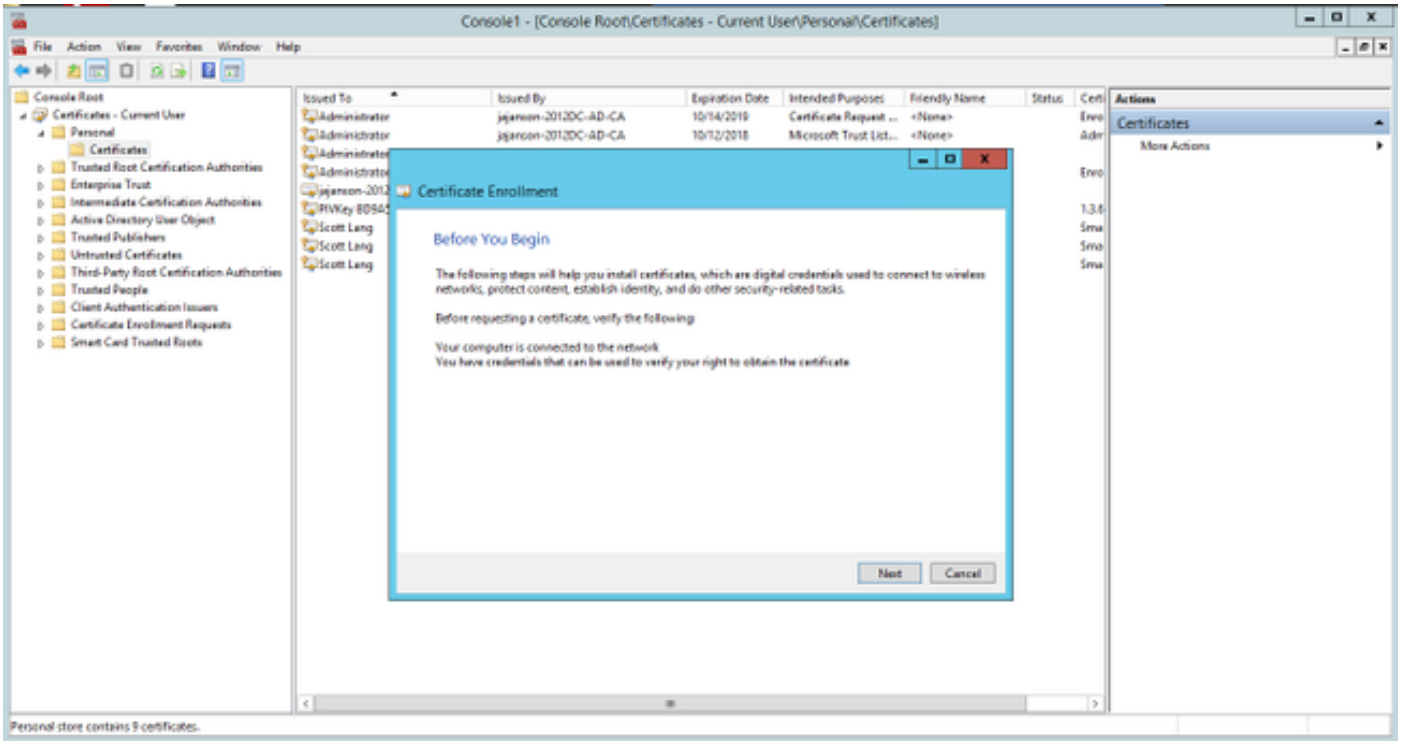
1.啟動MMC並匯入**Certificates Module & Manager**我的使用者帳戶的證書。

2.按一下右鍵或選擇**個人>證書**，然後選擇**所有任務>高級操作**，然後按一下**代表註冊……**

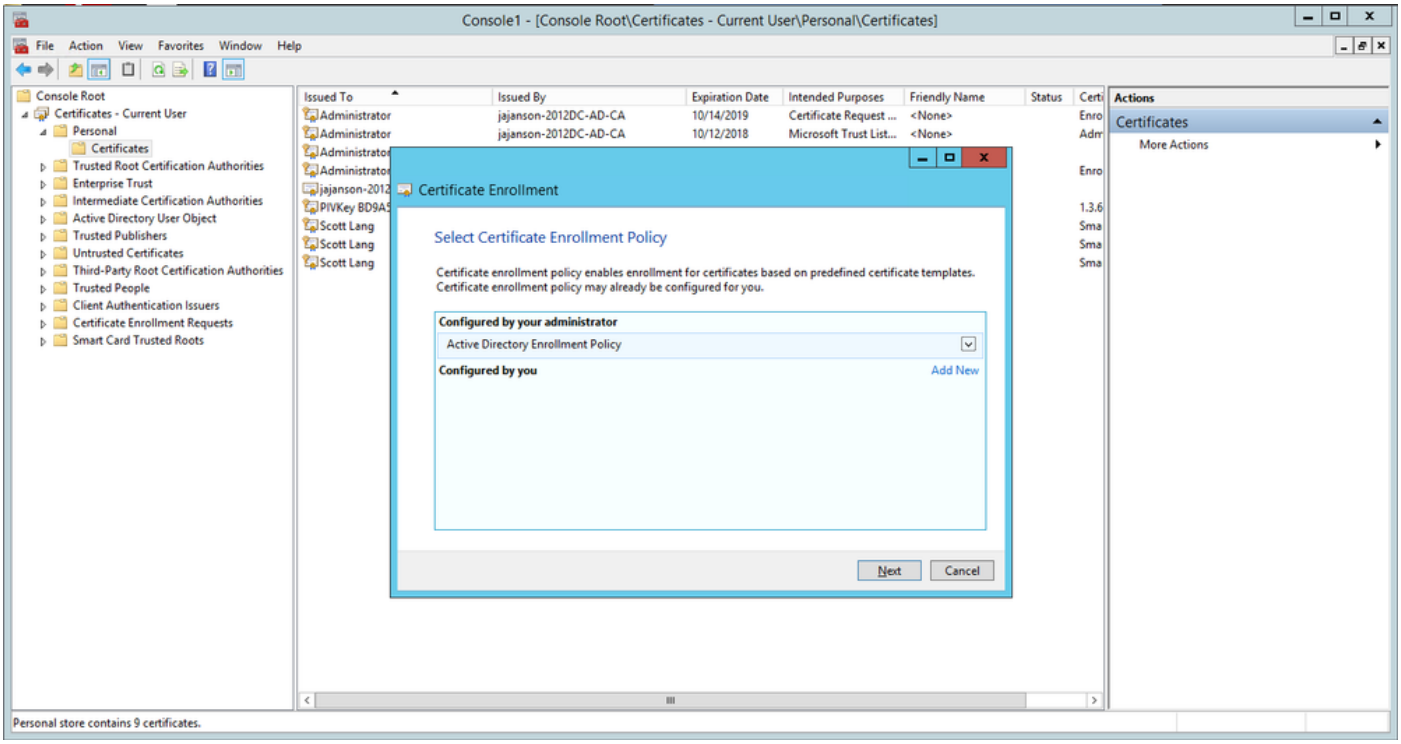
3.在嚮導上，選擇Active Directory註冊策略，然後按一下**下一步**。



代表高級註冊

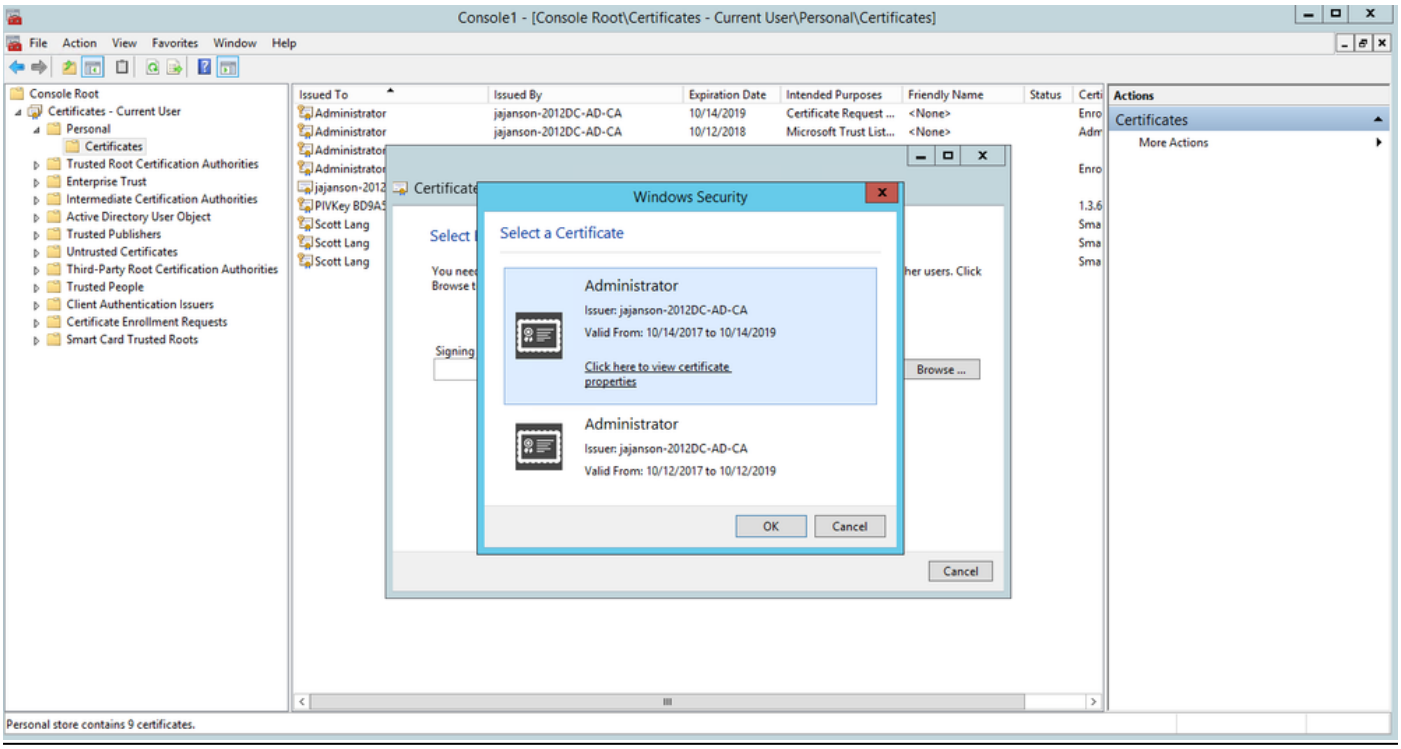


4.選擇Certificate Enrollment Policy（證書註冊策略），然後按一下**Next**。



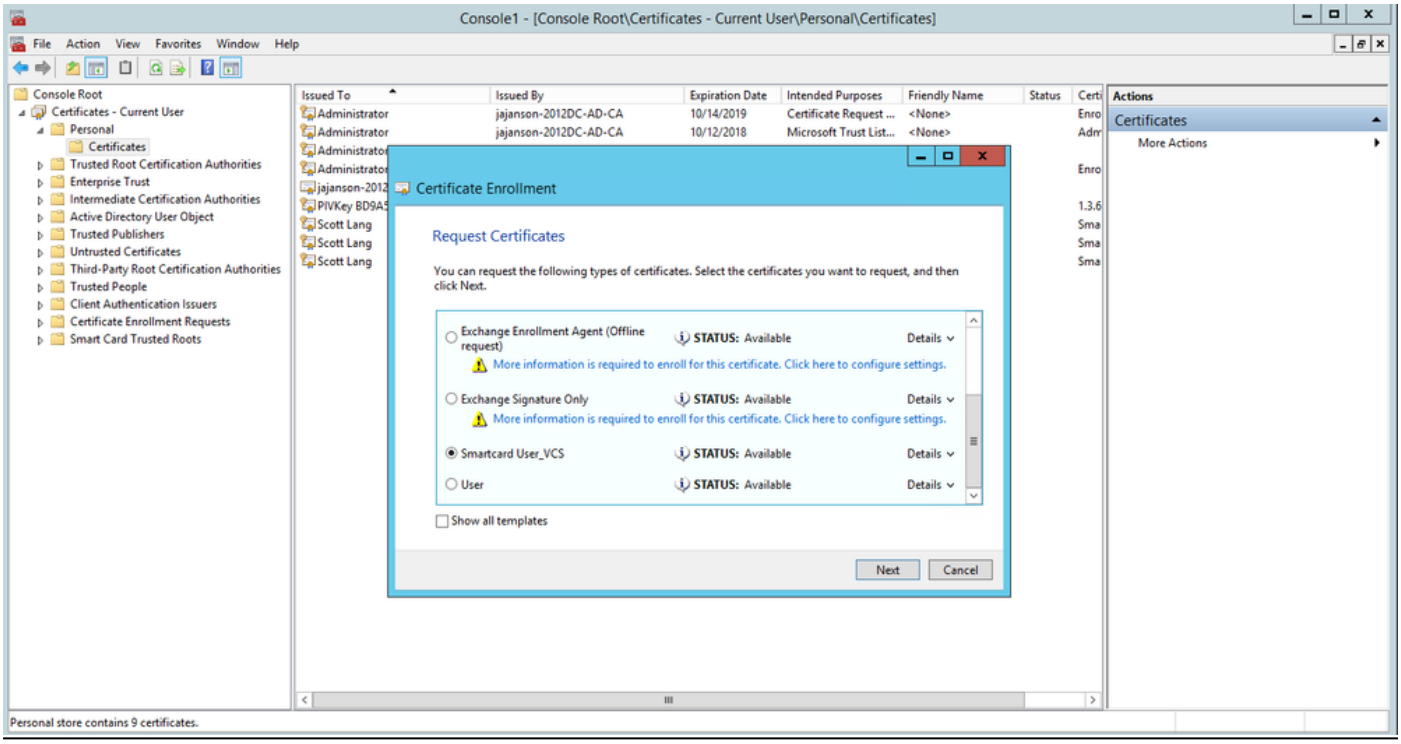
註冊策略

5.現在要求您選擇**簽名證書**。這是您之前請求的註冊證書。



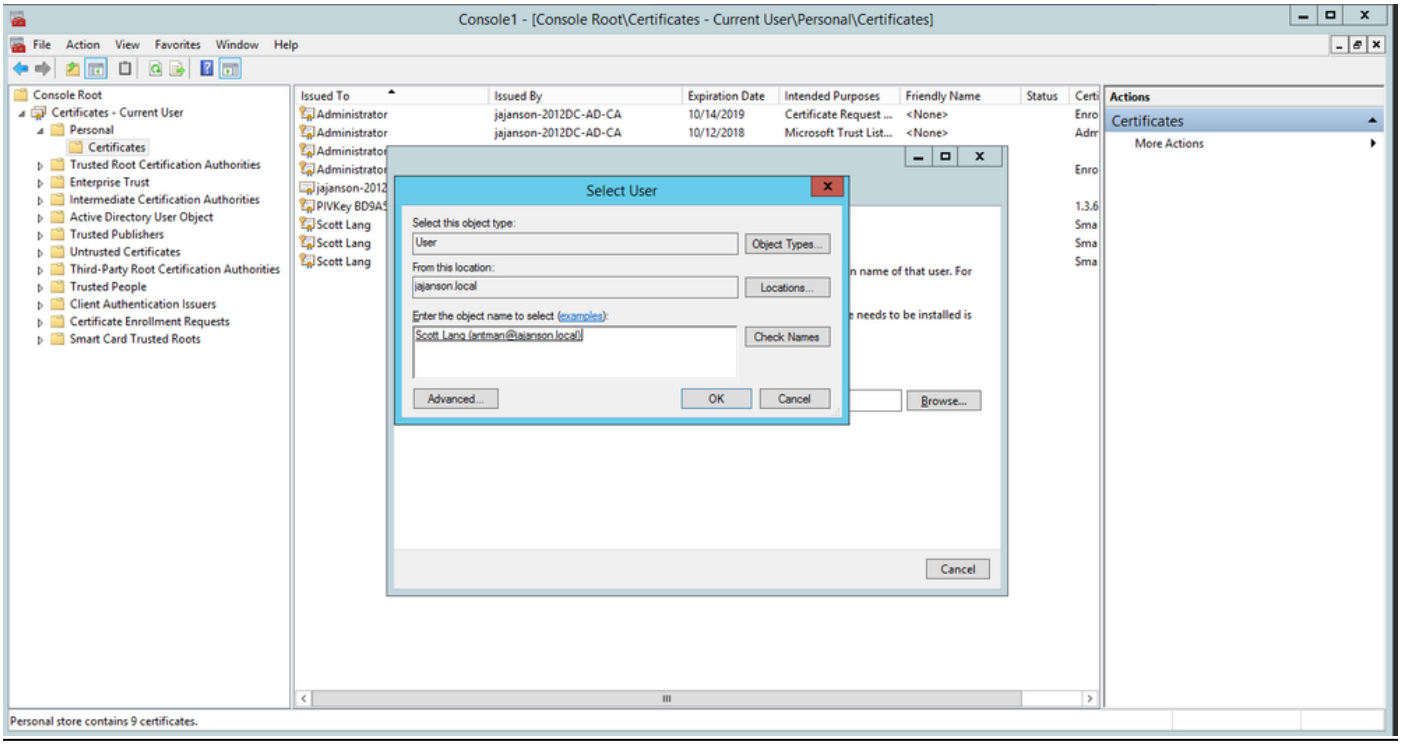
選擇簽名證書

6.在下一個螢幕上，您需要瀏覽到要請求的證書。在這種情況下，您之前建立的模板就是**Smartcard User_VCS**。



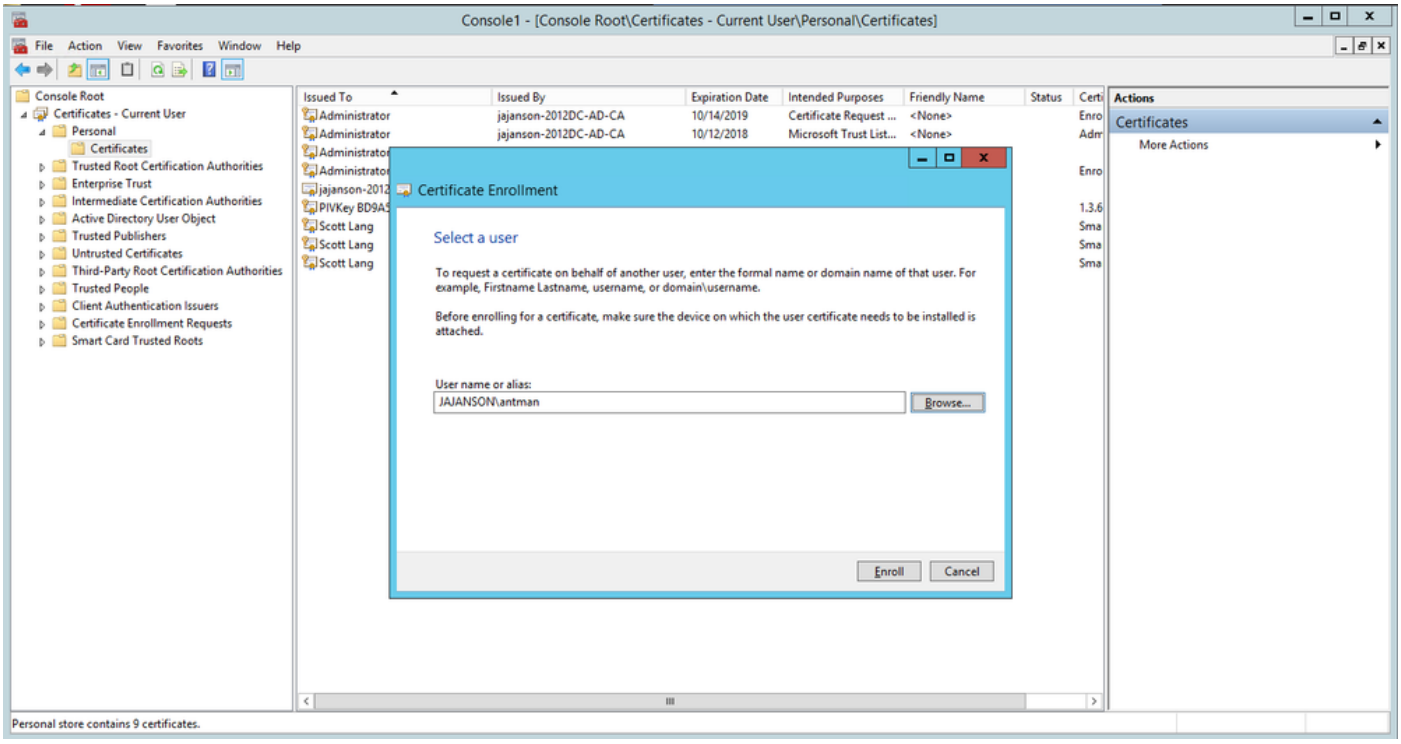
選擇VCS智慧卡

7.接下來，您需要選擇要代表其註冊的使用者。按一下**browse**，然後鍵入要註冊的員工的使用者名稱。在此例項中，使用Scott Lang 'antman@jajanson.local帳戶'。



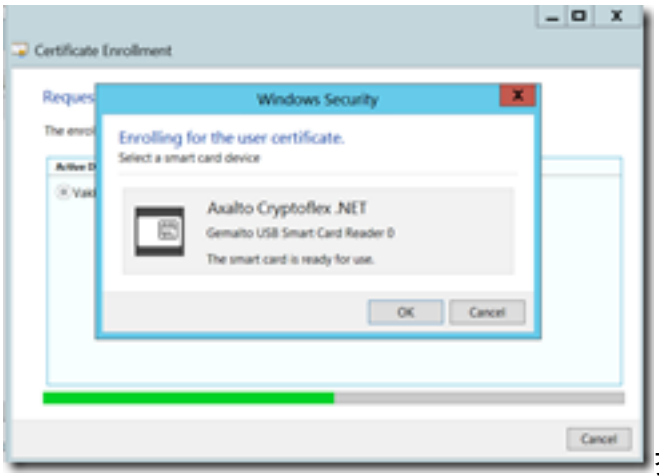
選擇使用者

8. 在下一個螢幕上，按一下**註冊**繼續進行註冊。現在，將智慧卡插入讀卡器。



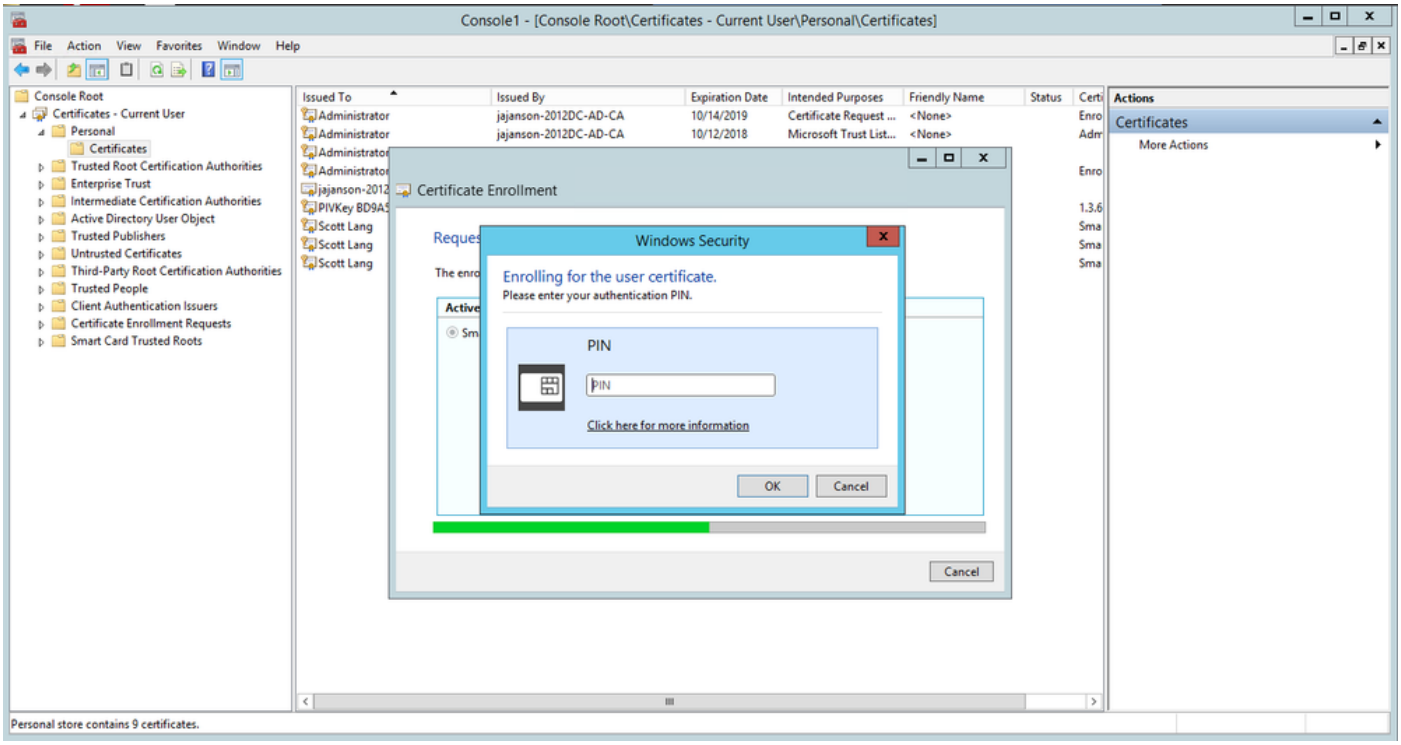
註冊

9. 插入智慧卡後，會按如下方式檢測：



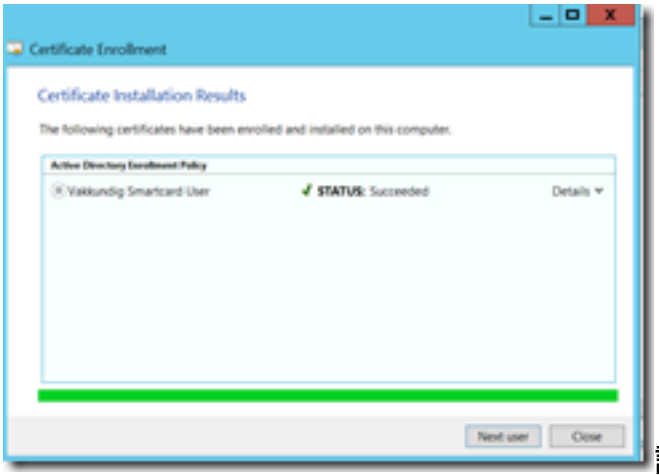
插入智慧卡

10. 然後要求您輸入智慧卡PIN碼(預設PIN:0000)。



輸入pin

11.最後，一旦您看到**Enrollment Successful**螢幕，就可以使用此智慧卡登入到加入域的伺服器，例如VCS（僅具有卡和已知的PIN）。但是，如果不是，則仍然需要準備VCS以將身份驗證請求重定向到智慧卡，並使用通用訪問卡釋放智慧卡上儲存的智慧卡證書以進行身份驗證。



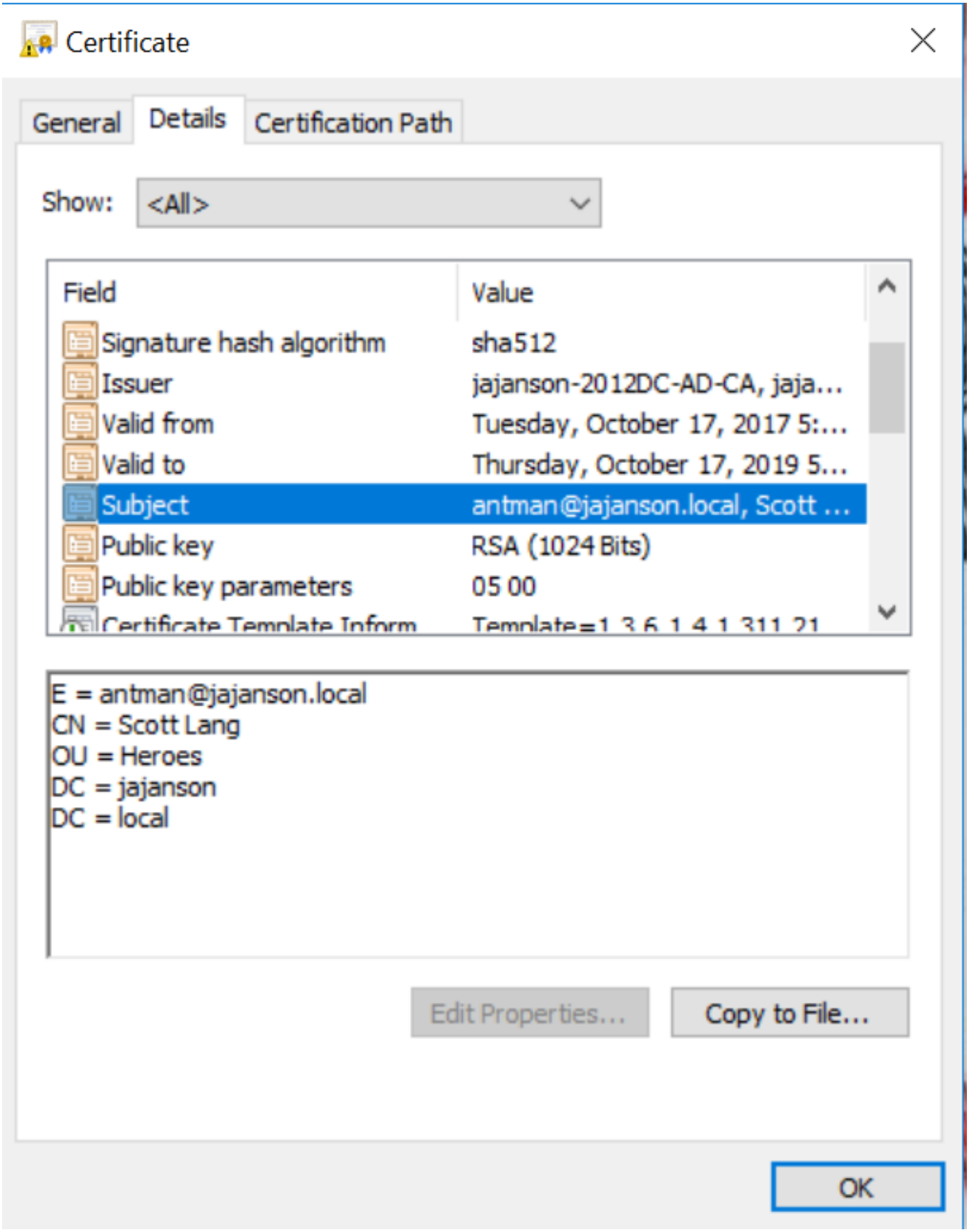
註冊成功

為通用接入卡配置VCS

導航到**Maintenance > Security > Trusted CA Certificate**，將根CA上傳到VCS中的Trusted CA Certificate清單。

2.將根CA簽名的證書吊銷清單上傳到VCS。導航到**維護>安全> CRL管理。**

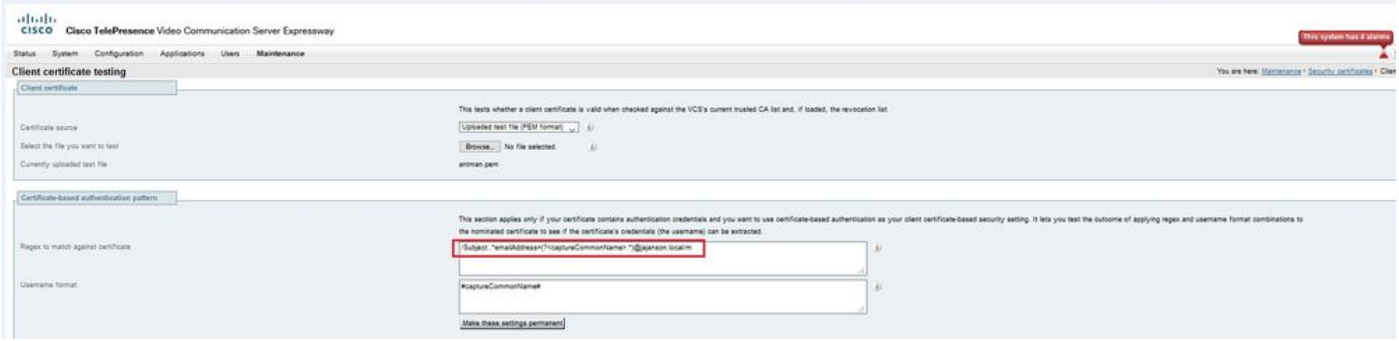
3.根據您的正規表示式測試您的客戶端證書，該表達式從證書中抽取使用者名稱用於針對LDAP或本地使用者的身份驗證。正規表示式將匹配證書的**Subject**。這可以是您的UPN、電子郵件等。在本實驗中，使用了與客戶端證書的客戶端證書匹配的電子郵件。


Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Signature hash algorithm
sha512
Issuer
jajanson-2012DC-AD-CA, jaja...
Valid from
Tuesday, October 17, 2017 5:...
Valid to
Thursday, October 17, 2019 5...
Subject
antman@jajanson.local, Scott ...
Public key
RSA (1024 Bits)
Public key parameters
05 00
E = antman@jajanson.local
CN = Scott Lang
OU = Heroes
DC = jajanson
DC = local
Edit Properties...
Copy to File...
OK

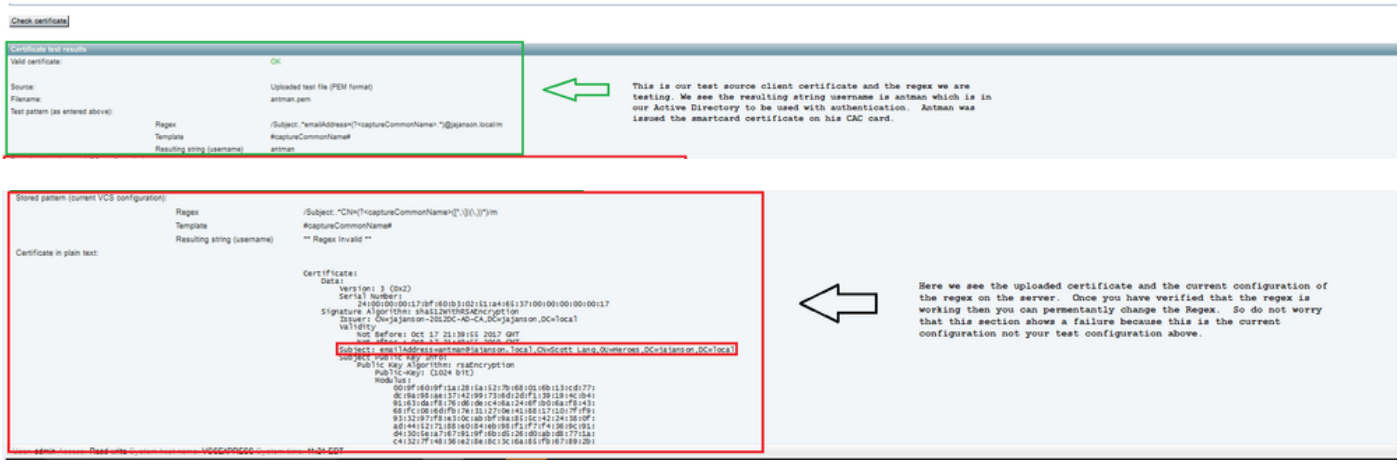
客戶端證書的主題

4. 導覽至**Maintenance > Security > Client Certificate Testing**。選擇要測試的客戶端證書，在我的實驗室中它是antman.pem，然後將其上傳到測試區域。在**Regex**下的**Certificate-based authentication pattern**部分中，根據證書匹配並貼上Regex以進行測試。請勿更改**Username format**欄位。

```
My Regex:  /Subject:.*emailAddress=(?.*)@jajanson.local/m
```



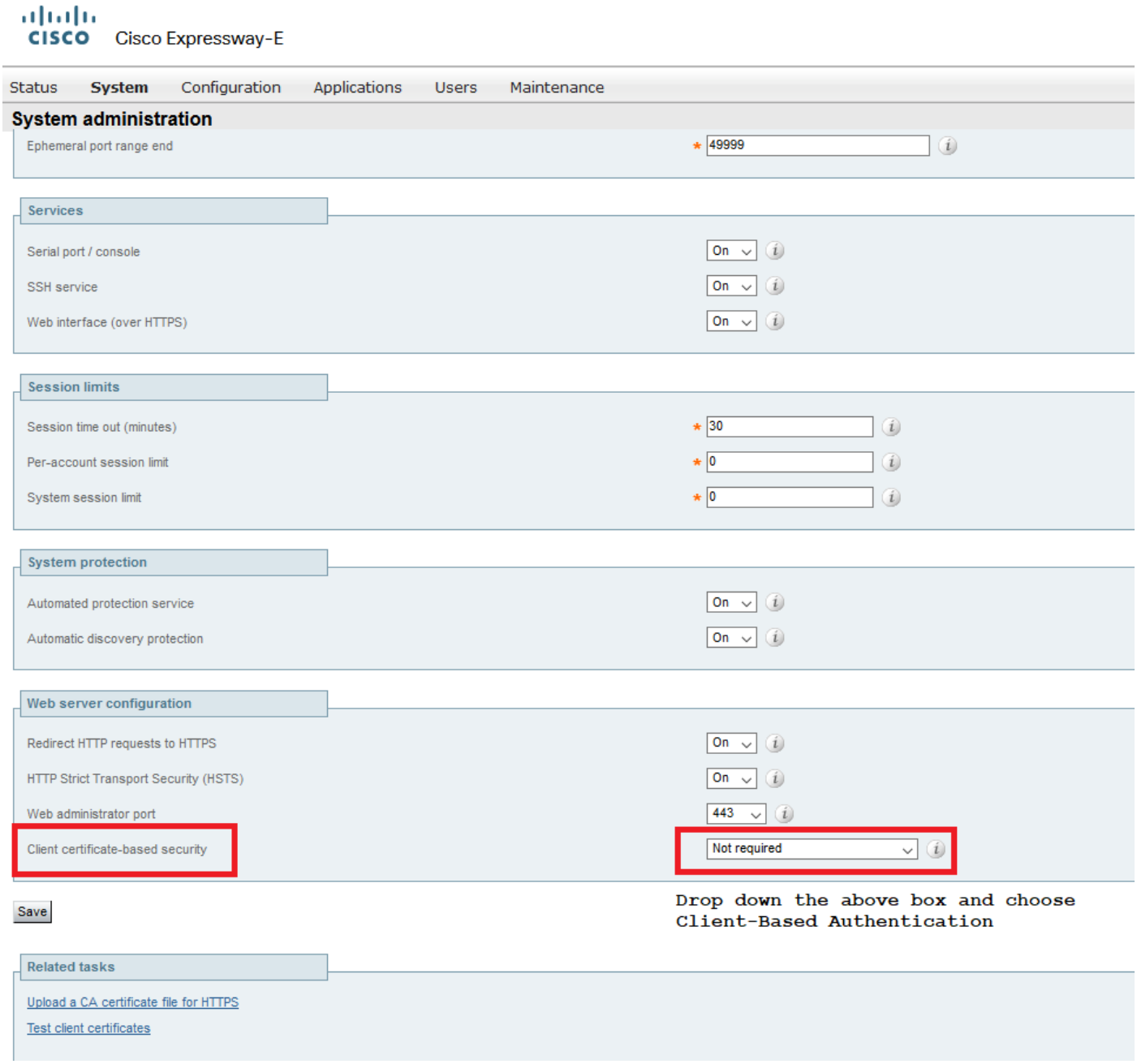
在VCS中測試您的正規表示式



測試結果

5.如果測試為您提供了所需的結果，您可以按一下**使這些更改永久生效**按鈕。這會更改伺服器的**基於證書的身份驗證**配置的正規表示式。若要驗證變更，請導覽至該組態，即**Maintenance > Security > Certificate-based authentication configuration。**

6. 導航到**System > Administrator**，然後按一下或選擇下拉框以選擇**Client certificate-based security = Client-Based Authentication，啟用基於客戶端的身份驗證。**通過此設定，使用者可以在瀏覽器中鍵入VCS伺服器的FQDN，並提示他選擇客戶端帳戶並輸入分配給其通用訪問卡的PIN。然後釋放證書，並返回VCS伺服器的Web GUI，他需要做的只是按一下或選擇Administrator按鈕。然後他被允許進入伺服器。如果選擇選項**Client certificate-based security = Client-Based Validation**，則過程相同，使用者按一下Administrator按鈕時除外，他再次提示輸入管理員密碼。通常，後者並不是該組織試圖通過集體行動條款達成的。



啟用基於客戶端的身份驗證

救命！我被鎖在外面了!!!

如果啟用了基於客戶端的身份驗證，並且VCS出於任何原因拒絕證書，您將無法再以傳統方式登入到Web GUI。但是，不要擔心有辦法重返你的系統。隨附的文檔可在思科網站上找到，並提供了有關如何從根使用者訪問禁用基於客戶端的身份驗證的資訊。

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。