使用WLC和Windows Server 2012的本地重要證書(LSC)配置示例

目錄

簡介

本文說明如何使用無線LAN控制器(WLC)和新安裝的Microsoft Windows Server 2012 R2設定本機重要憑證(LSC)。

> **附註**：實際部署在很多方面可能有所不同，您應該對Microsoft Windows Server 2012上的設定擁有完全的控制和知識。此配置示例僅作為思科客戶實施並調整其Microsoft Windows Server配置以使LSC正常工作的參考模板提供。

必要條件

需求

思科建議您瞭解Microsoft Windows Server中的每一項更改，如果需要，請檢視相關Microsoft文檔。

> **附註**：中間CA不支援WLC上的LSC，因為控制器僅取得中間CA，WLC會遺失根CA。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- WLC版本7.6
- Microsoft Windows Server 2012 R2

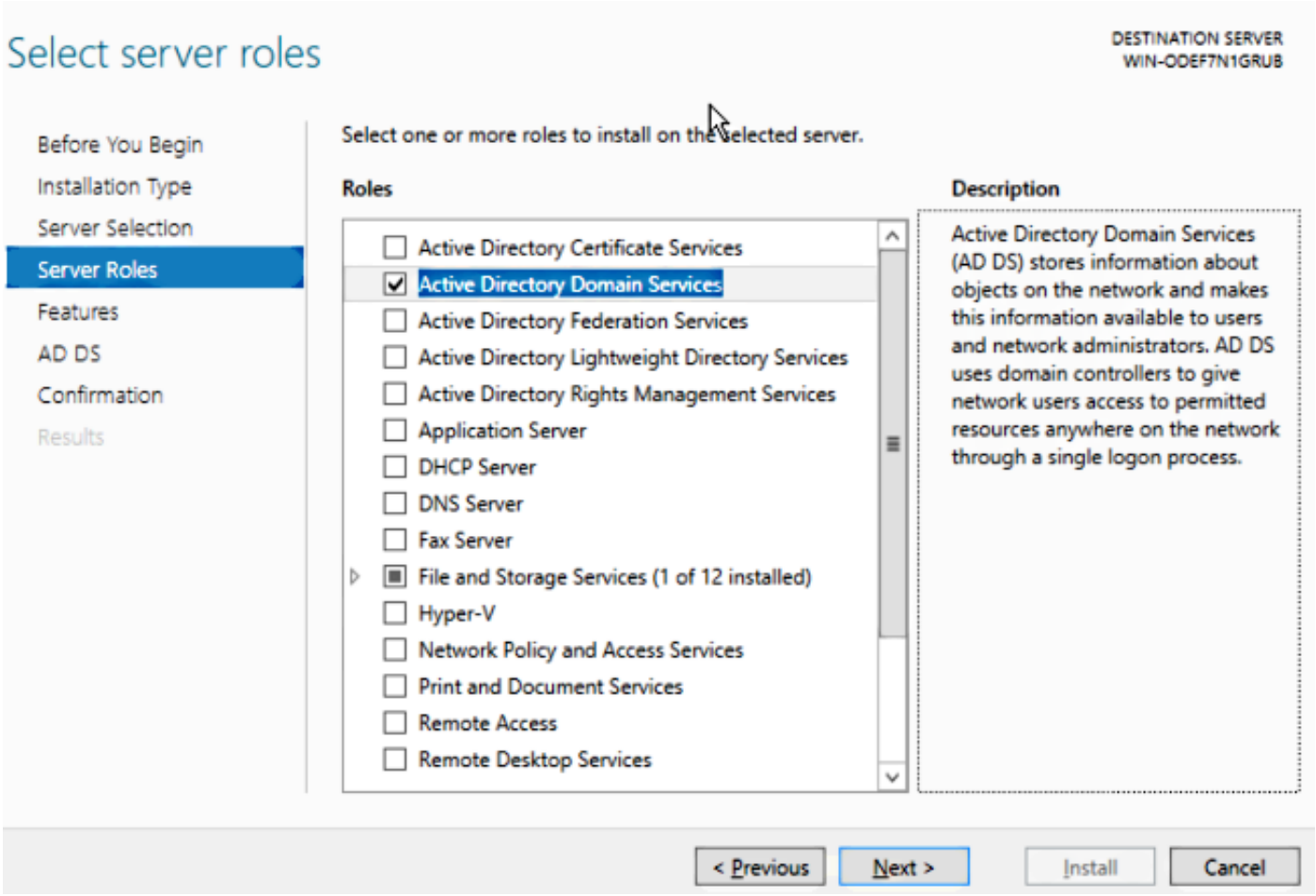
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

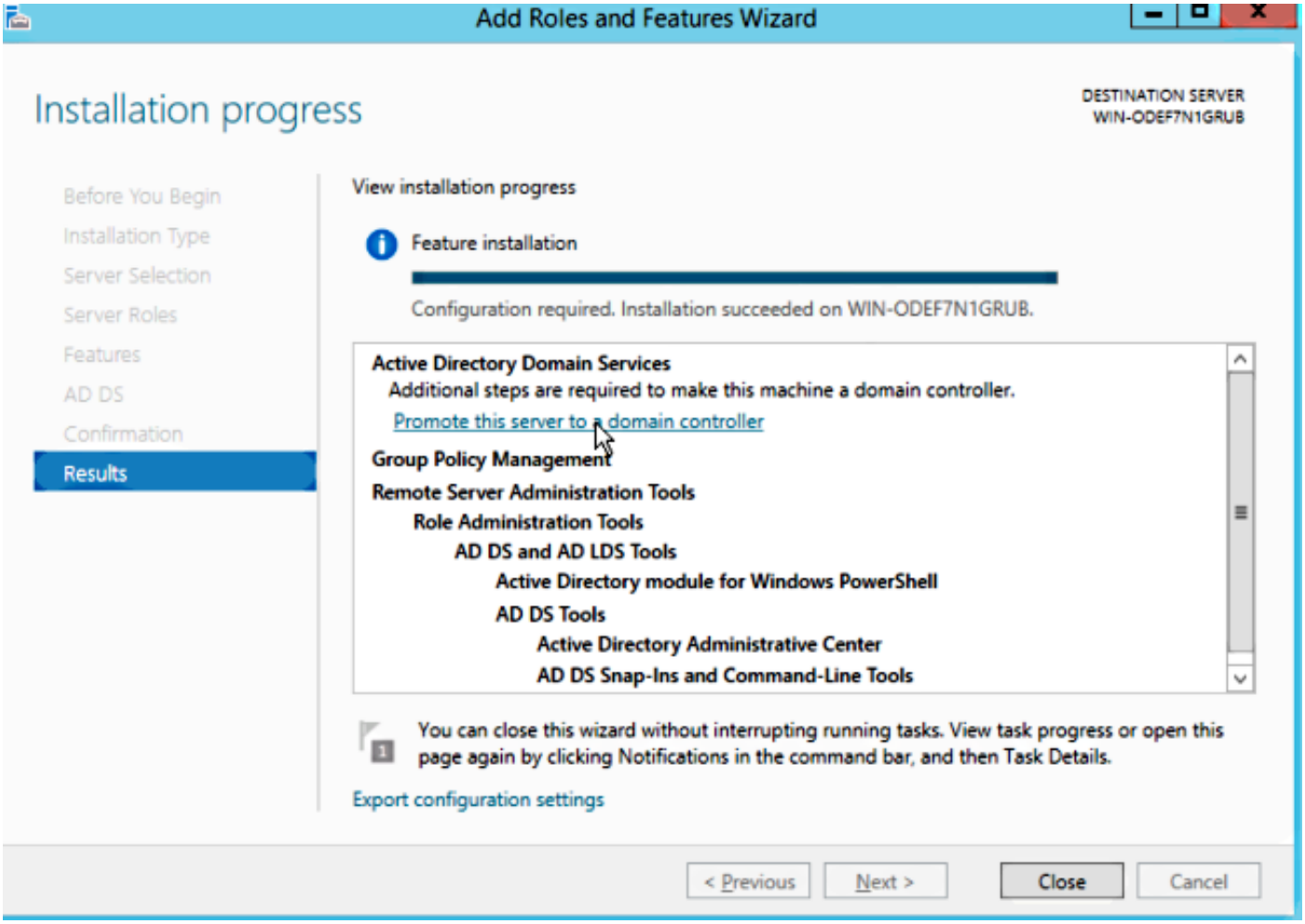
Microsoft Windows Server配置

此配置顯示為在新安裝的Microsoft Windows Server 2012上執行。您必須根據您的域和配置調整步驟。

步驟1.為角色和功能嚮導安裝Active Directory域服務。

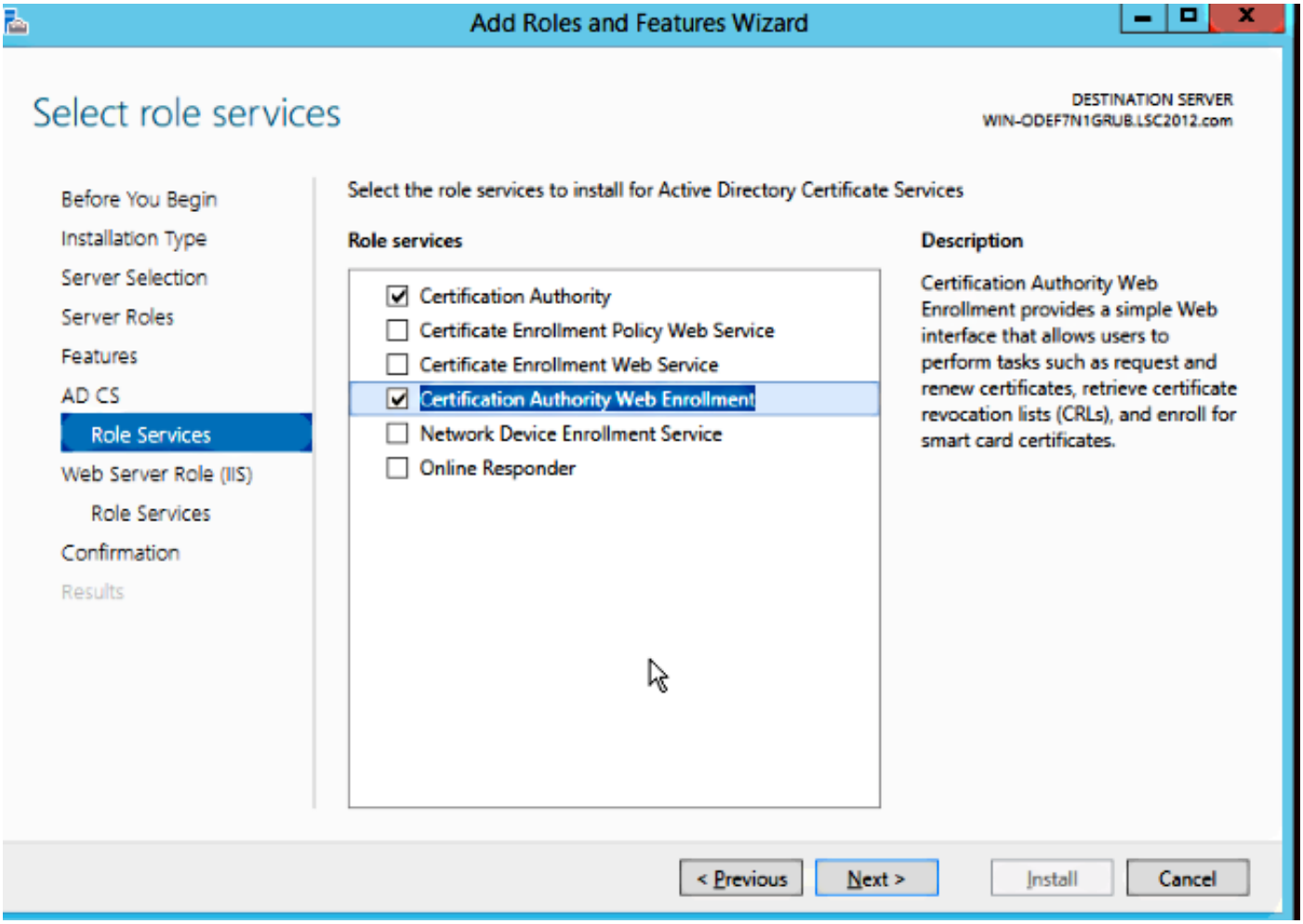


步驟2.安裝後，必須將伺服器升級為域控制器。

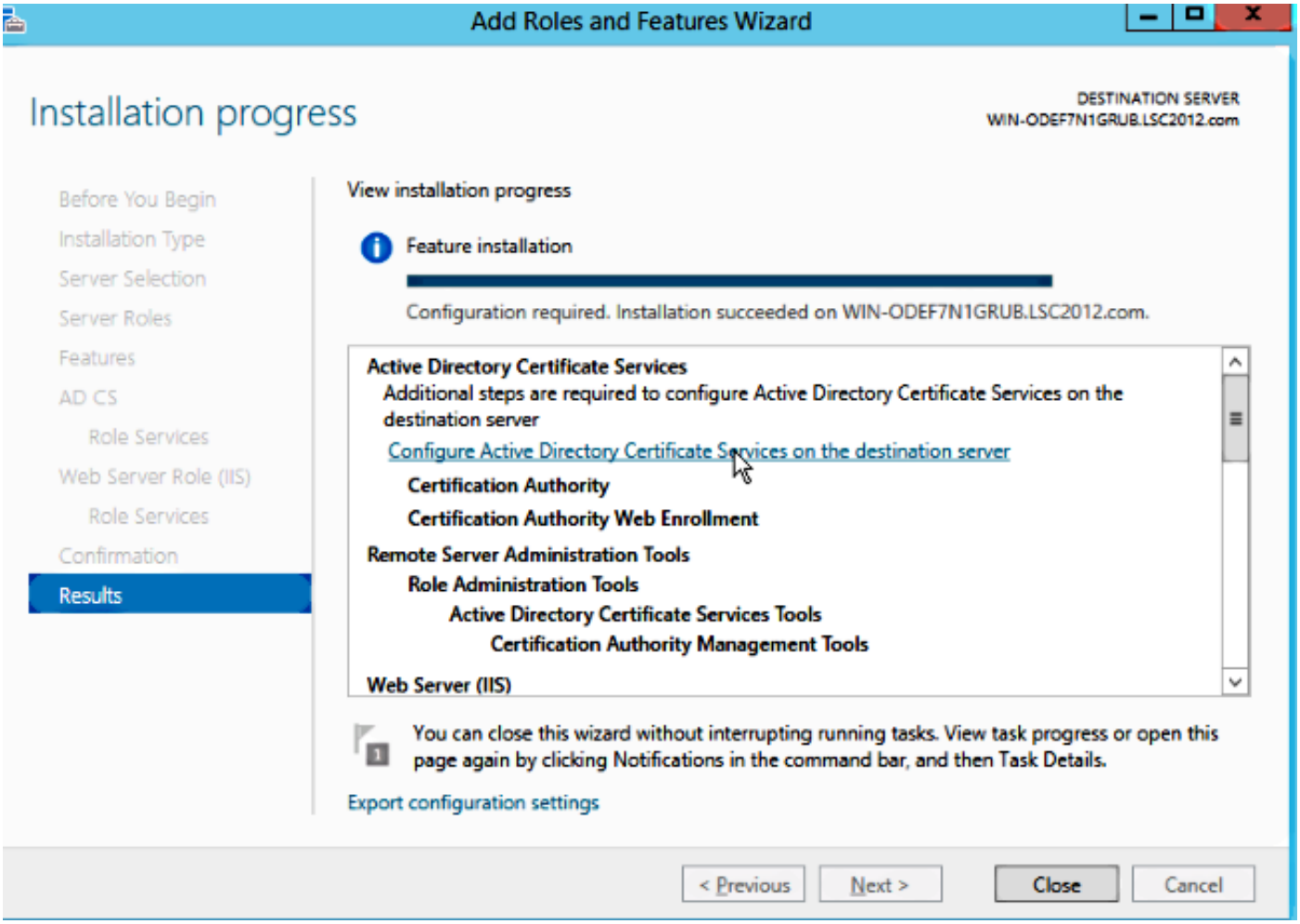


步驟3. 由於這是新設定，因此請配置新的林；但在現有部署中，通常只需在域控制器上配置這些點即可。在這裡，您選擇**LSC2012.com**域。這也會啟用域名伺服器(DNS)功能。

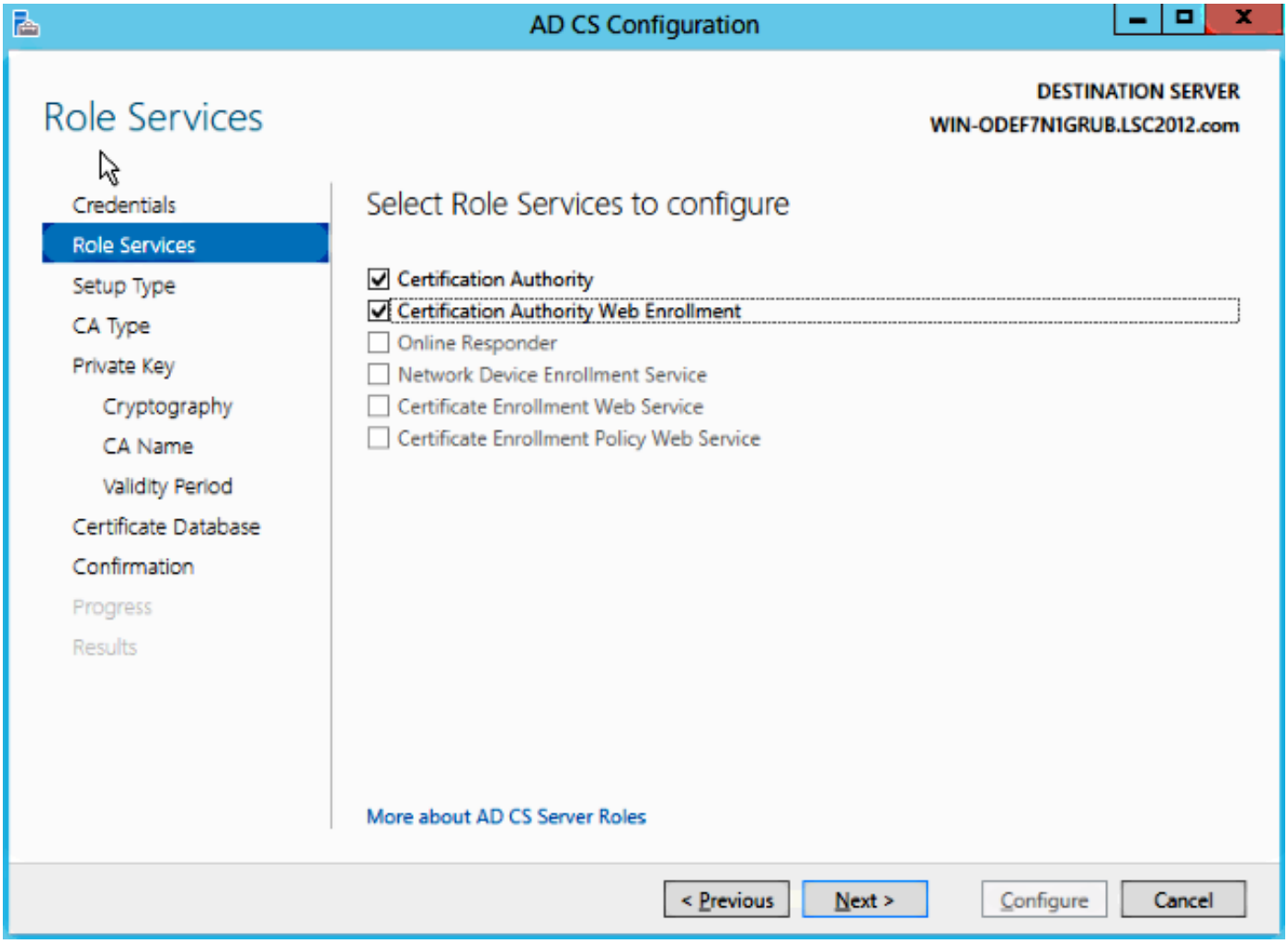
步驟4.重新開機後，安裝憑證授權單位(CA)服務和Web註冊。


Add Roles and Features Wizard
Select role services
DESTINATION SERVER
WIN-ODEF7N1GRUB.LSC2012.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD CS
Role Services
Web Server Role (IIS)
Role Services
Confirmation
Results
Select the role services to install for Active Directory Certificate Services
Role services
Certification Authority
Certificate Enrollment Policy Web Service
Certificate Enrollment Web Service
Certification Authority Web Enrollment
Network Device Enrollment Service
Online Responder
Description
Certification Authority Web Enrollment provides a simple Web interface that allows users to perform tasks such as request and renew certificates, retrieve certificate revocation lists (CRLs), and enroll for smart card certificates.
< Previous
Next >
Install
Cancel

步驟5.進行設定。



步驟6.選擇企業CA，並將所有內容保留為預設值。

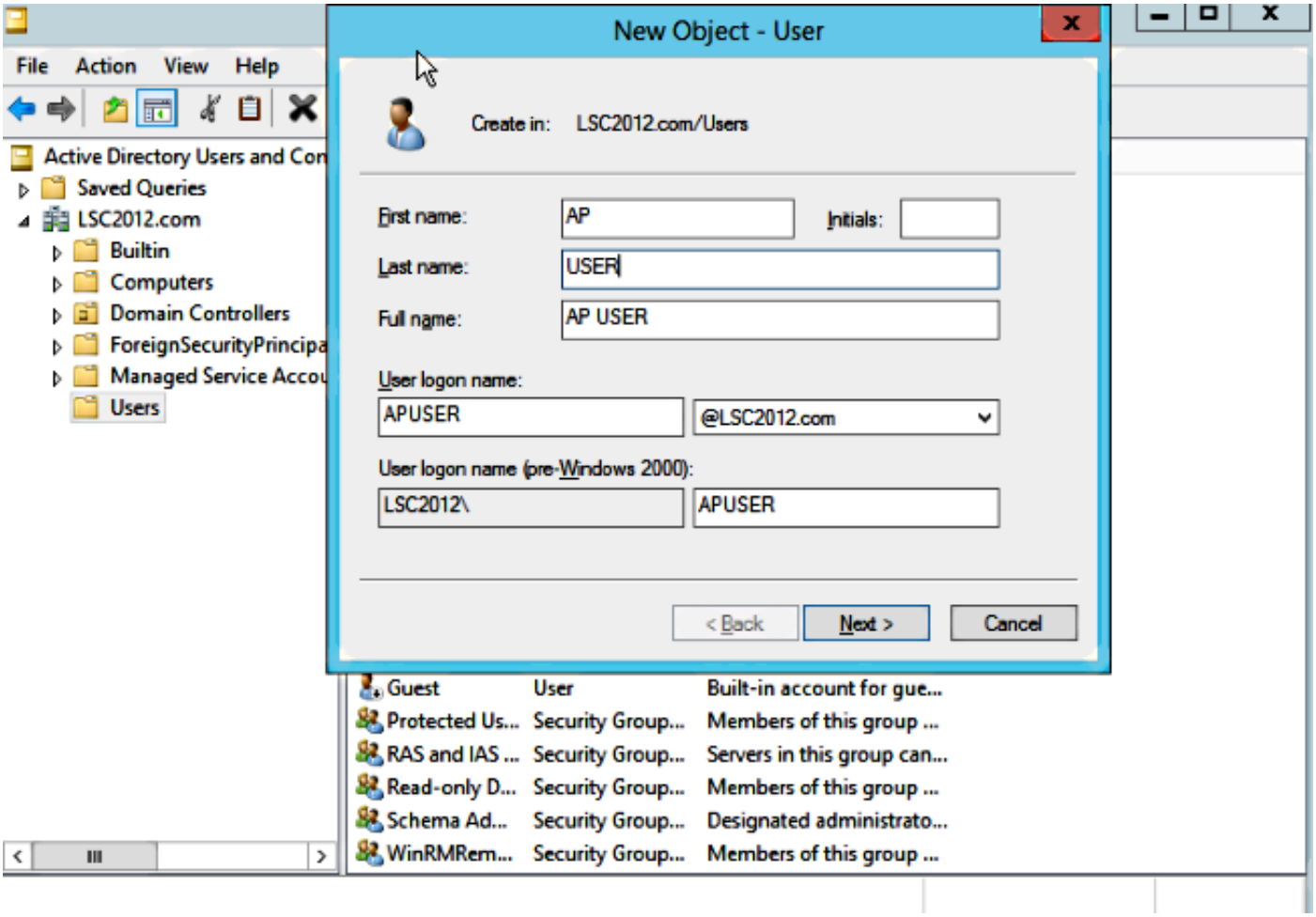


步驟7.按一下**Microsoft Windows/開始選單**。

步驟8.單擊管理工具。

步驟9.單擊Active Directory使用者和電腦。

步驟10.展開域，按一下右鍵**Users資料夾**，然後選擇**New Object > User**。



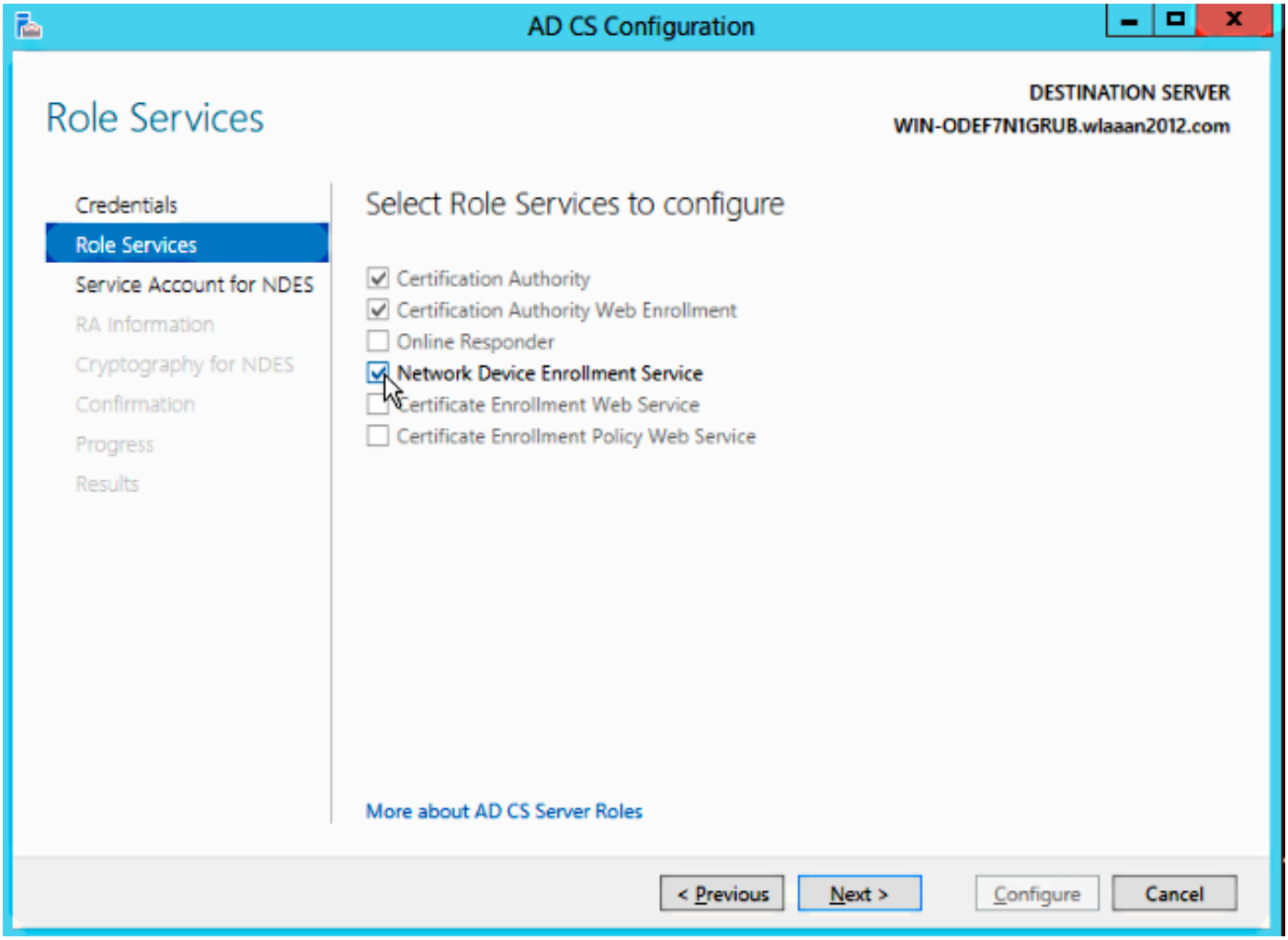
步驟11.在本範例中，它命名為**APUSER**。建立後，必須編輯使用者並按一下**MemberOf**頁籤，並使其成為IIS_IUSRS組的成員

所需的使用者許可權分配包括：

— 允許在本地登入

— 作為服務登入

步驟12.安裝網路裝置註冊服務(NDES)。



- 選擇IIS_USRS組的帳戶成員(在本例中為**APUSER**)，作為NDES的服務帳戶。

步驟13.導覽至Administrative Tools。

步驟14.單擊Internet Information Services(IIS)。

步驟15.展開Server > Sites > Default web site > Cert Srv。

步驟16.對於**mscep和mscep_admin，請按一下authentication。**確保啟用了匿名身份驗證。

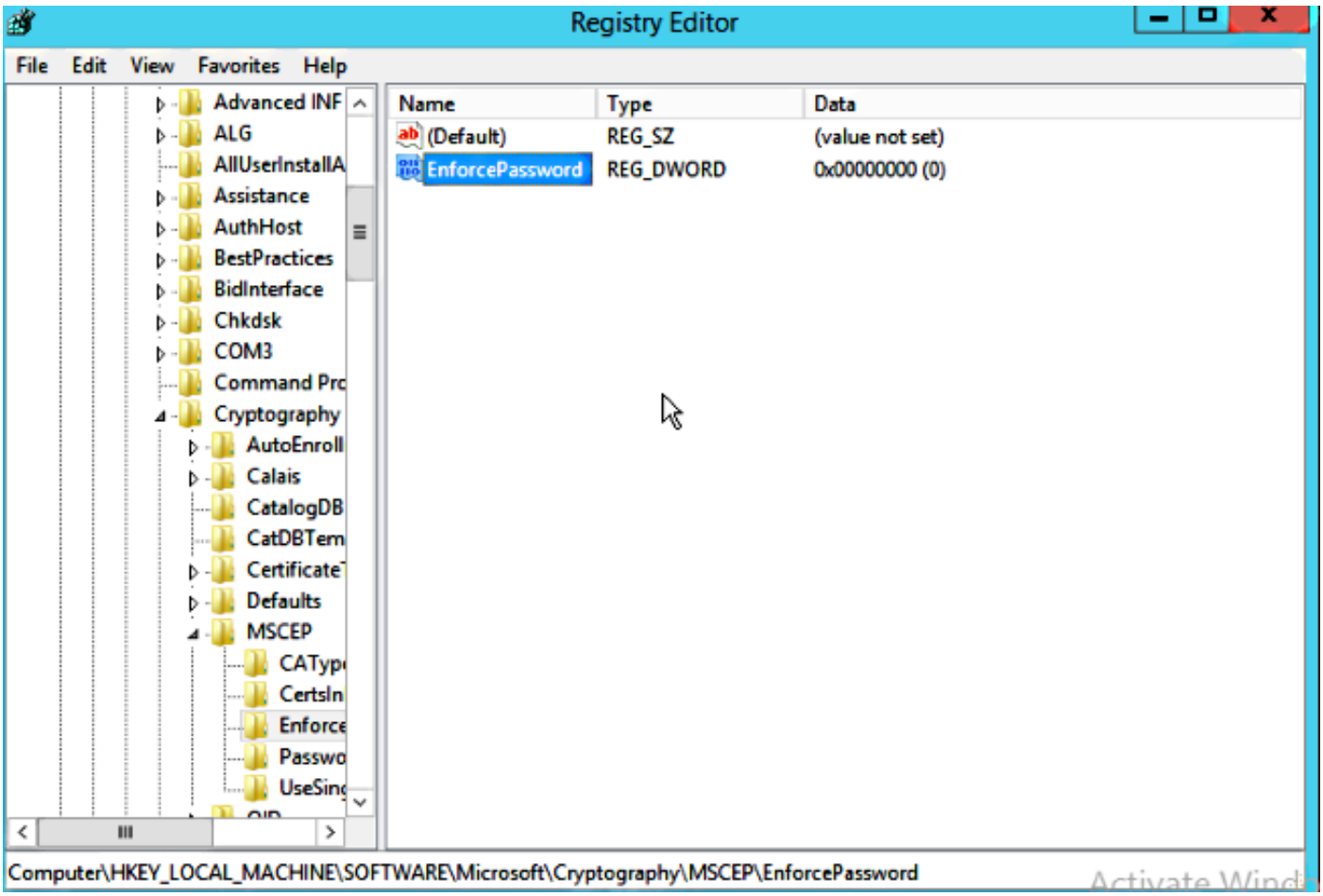
步驟17.右鍵按一下**windows authentication並**選擇**Providers。**確保NT LAN Manager(NTLM)在清單中位於首位。

步驟18.在登錄檔設定中禁用身份驗證質詢，否則簡單證書註冊協定(SCEP)要求質詢密碼身份驗證，而WLC不支援該身份驗證。

步驟19.開啟**regedit application。**

步驟20.前往HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\Cryptography\MSCEP\。

步驟21.將EnforcePassword設定為0。



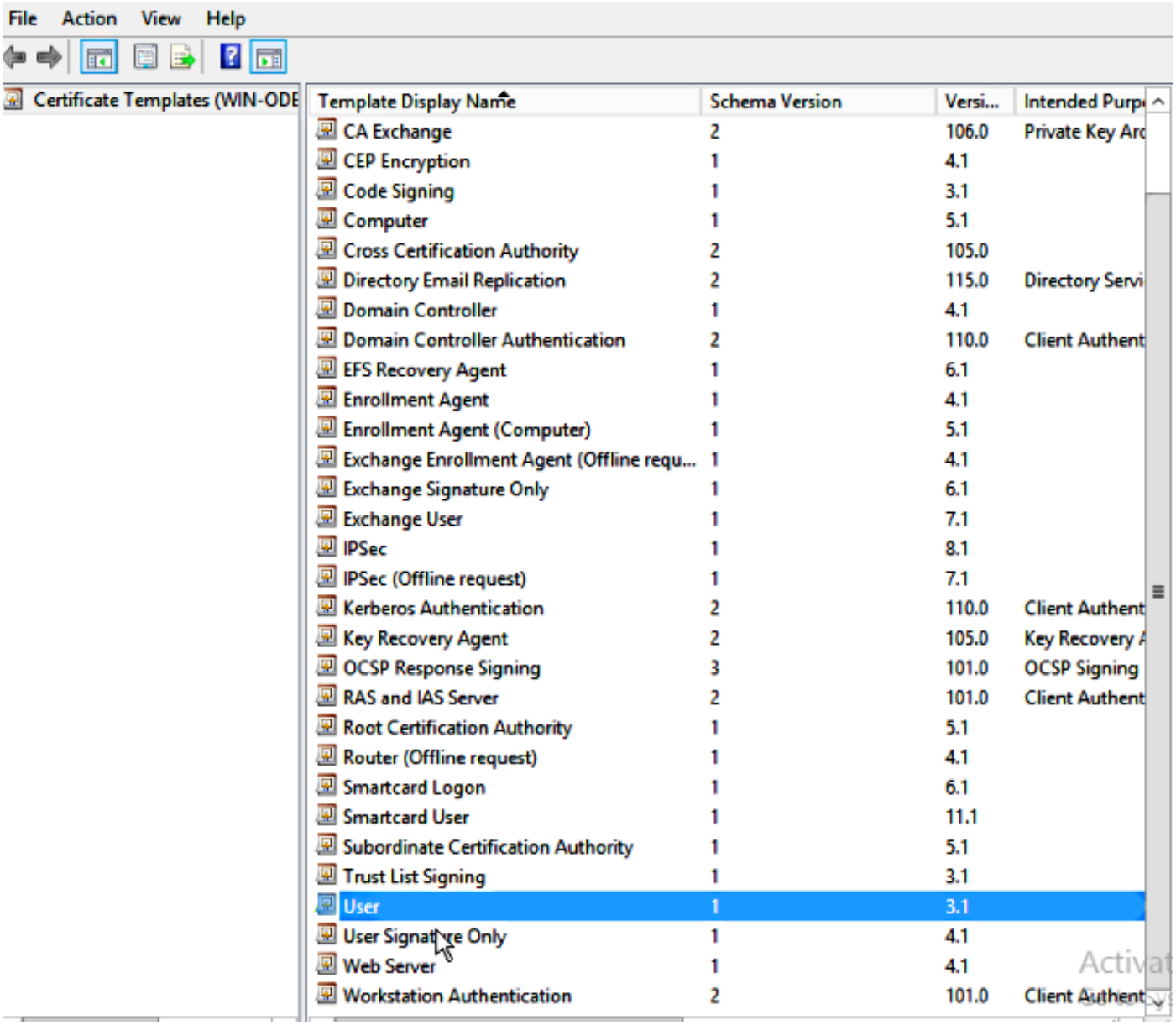
步驟22.按一下Microsoft Windows/**開始選單**。

步驟23.鍵入MMC。

步驟24.在「檔案」選單上，選擇**「新增/刪除管理單元」**。選擇Certification Authority。

步驟25.右鍵點選Certificate Template**資料夾**，然後點**擊**Manage。

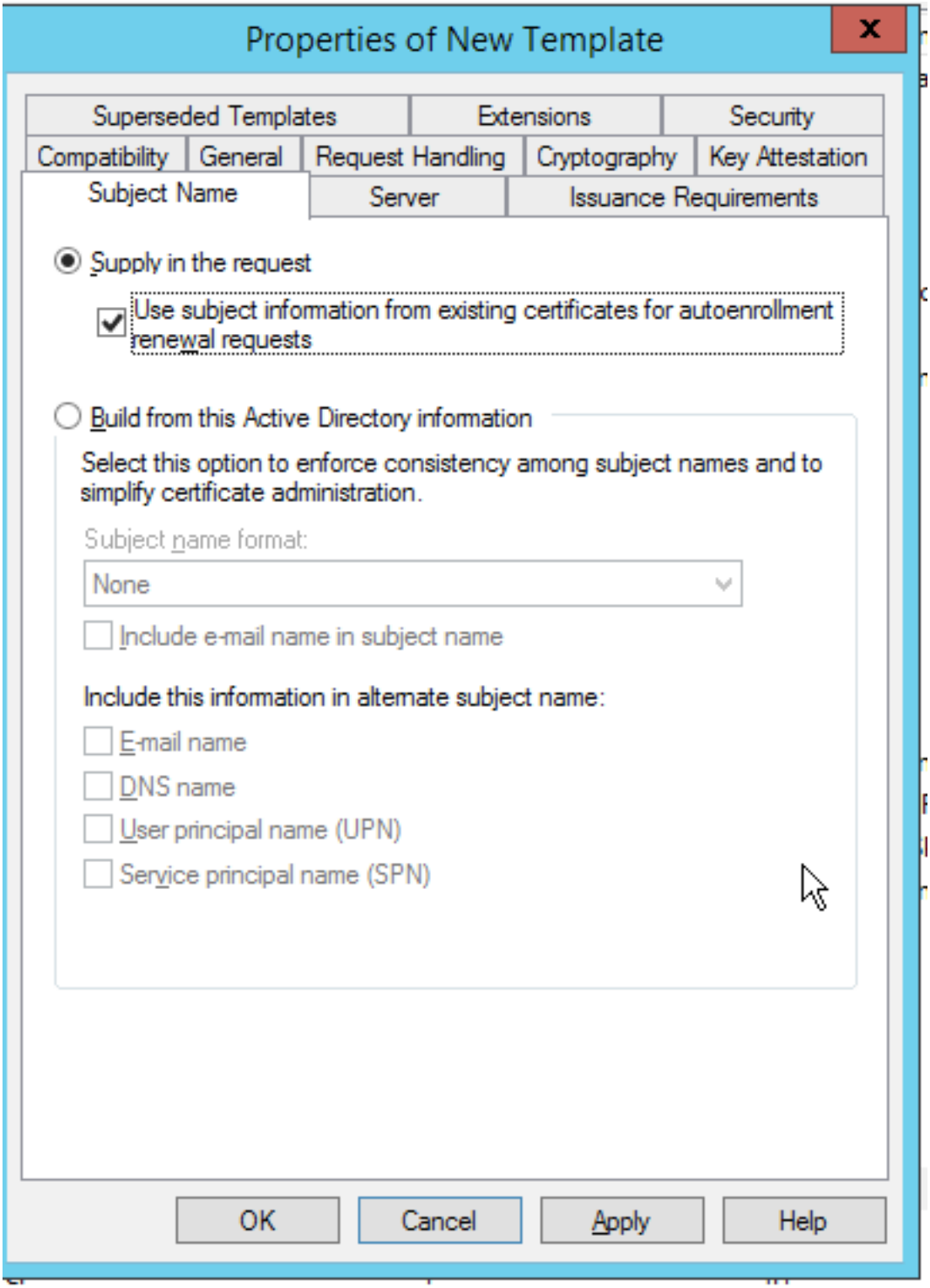
步驟26.按一下右鍵現有模板（如User），然後選擇「複製**模板**」。



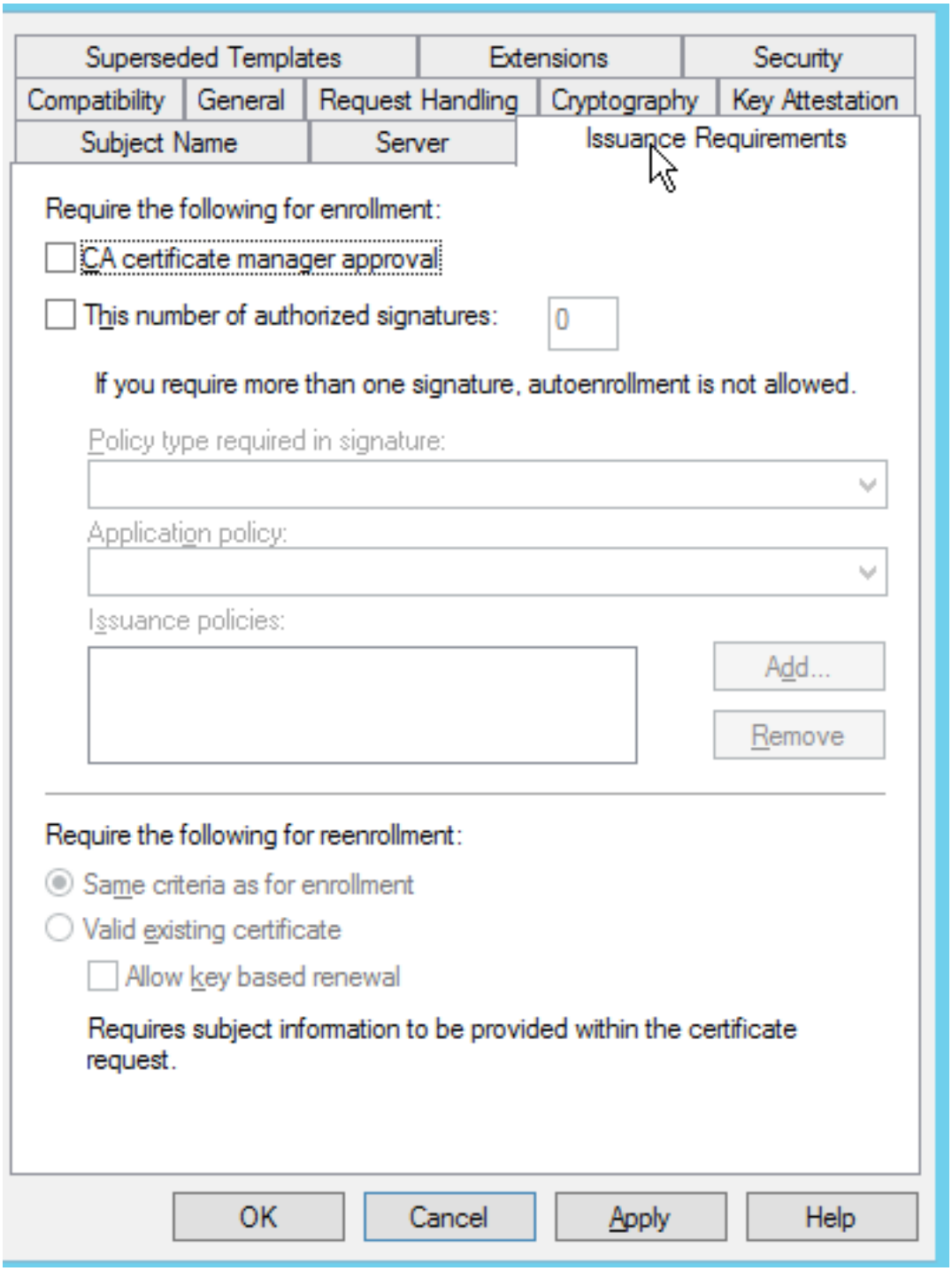
步驟27.選擇CA作為Microsoft Windows 2012 R2。

步驟28.在「General」索引標籤上，新增顯示名稱，例如WLC和有效期。

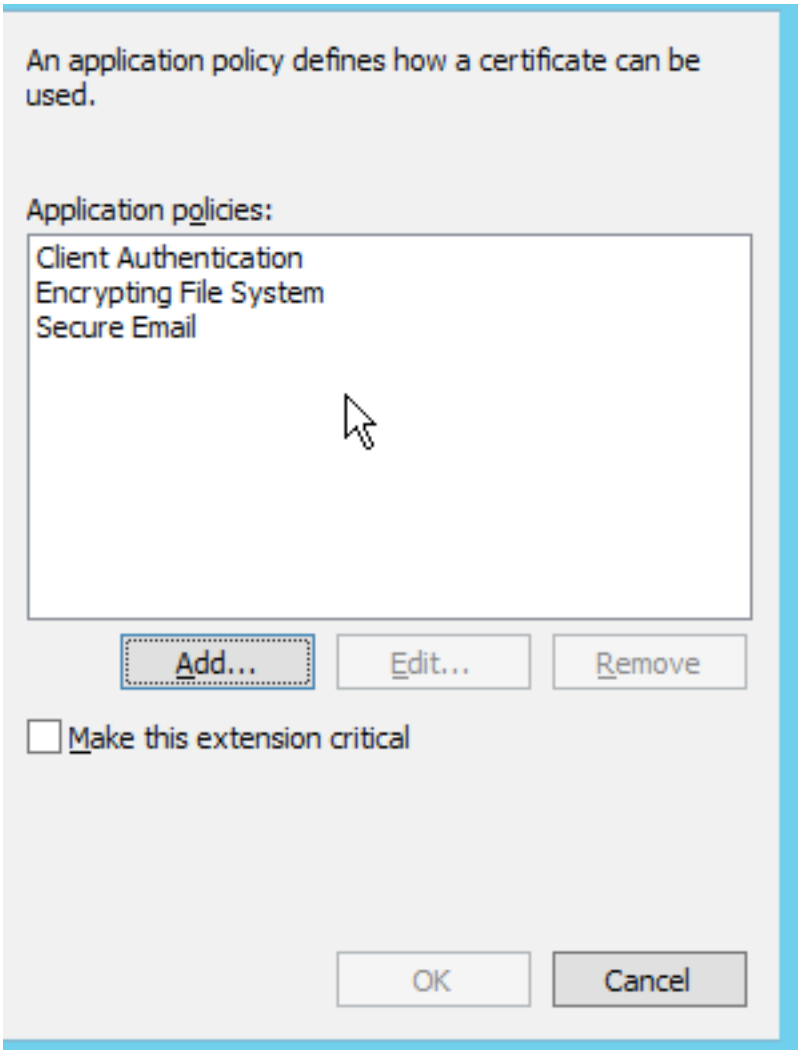
步驟29.在「使用者名稱」標籤中，確認已選**擇了請求中的**「供應」。



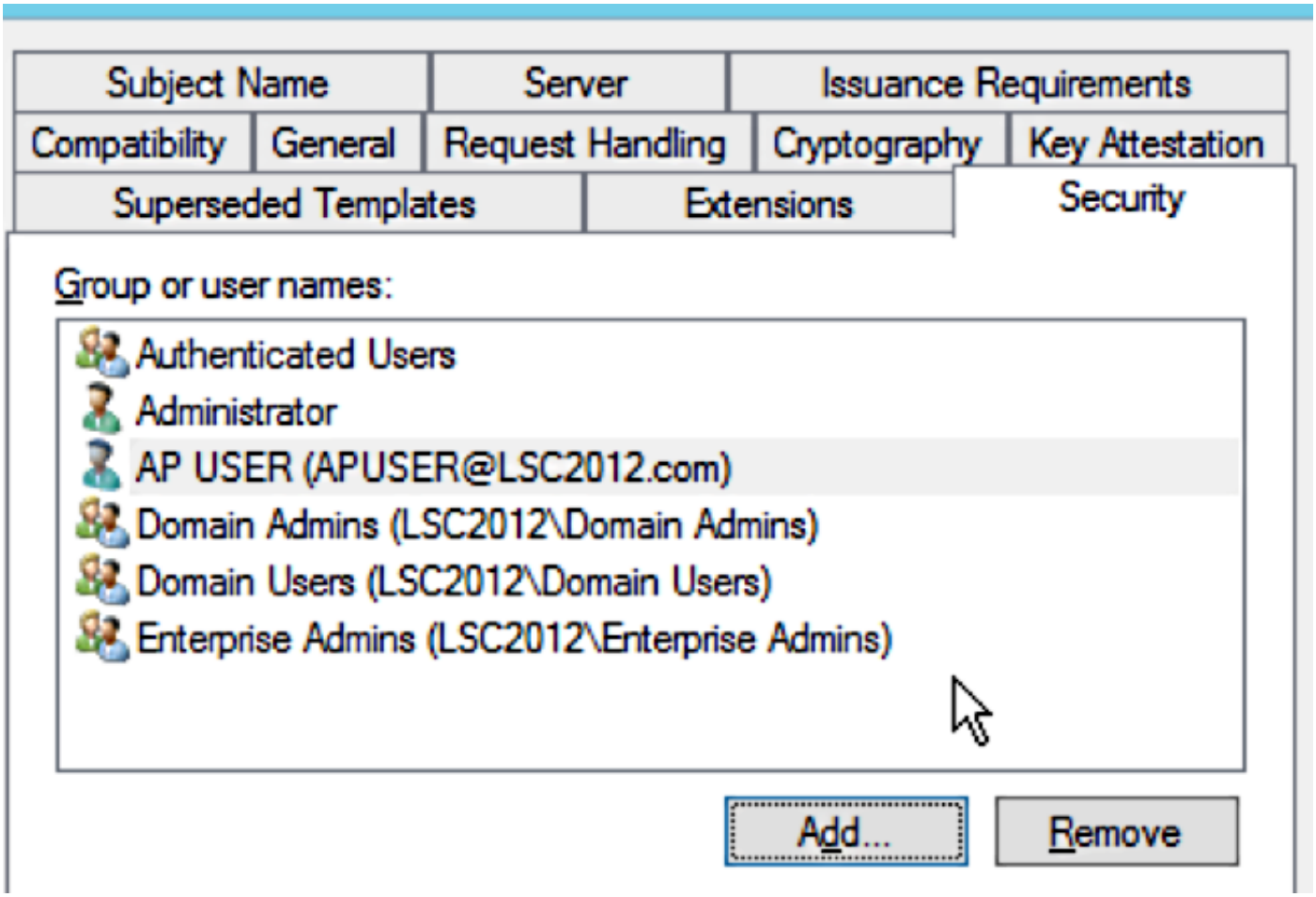
步驟30.單擊Issuance Requirements選項卡。Cisco建議您在典型的分層CA環境中將頒發策略留空：



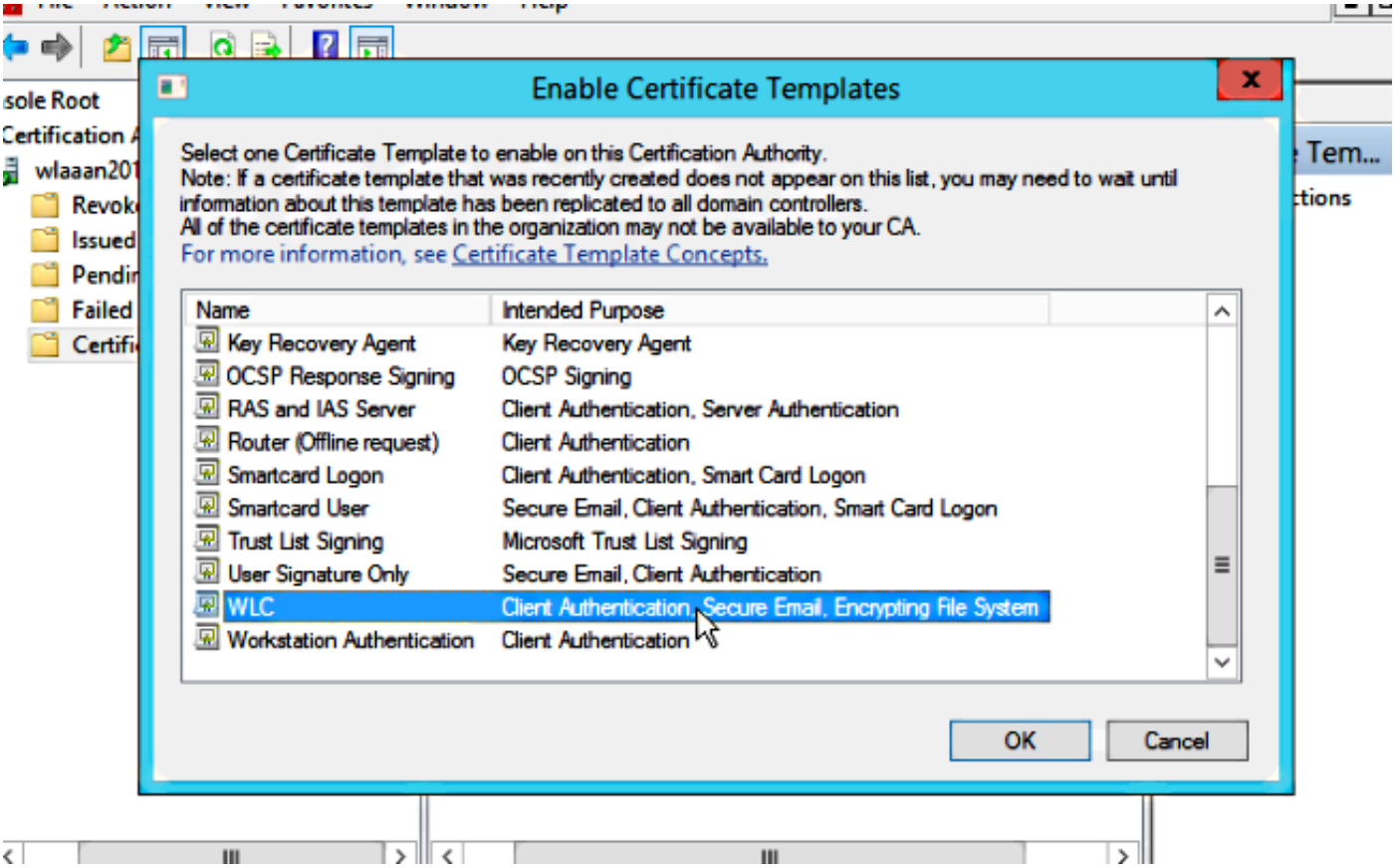
步驟31.單擊**Extensions（擴展）頁籤**、**Application Policies**，然後**Edit**。按一下**Add**，並確保將Client Authentication新增為應用程式策略。按一下「**OK**」（確定）。



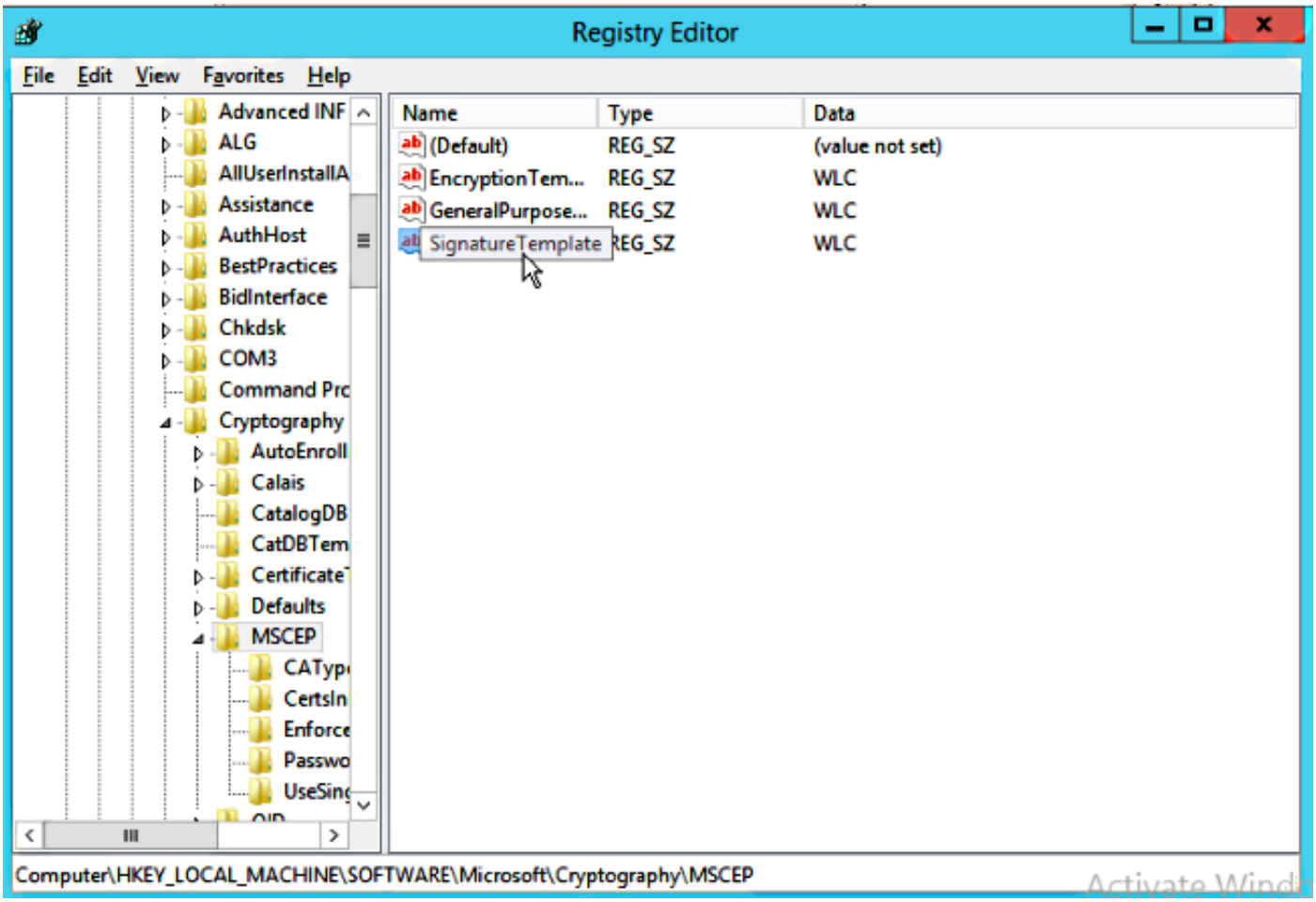
步驟32.單擊**Security選項**卡，然後單擊**Add...**.確保在NDES服務安裝中定義的SCEP服務帳戶完全控制模板，然後按一下**確定**。



步驟33.返回證書頒發機構GUI介面。按一下右鍵**Certificate Templates**目錄。導覽至**New > Certificate Template to Issue**。選擇先前配置的WLC模板，然後點選**確定。**



步驟34.在「電腦」>「HKEY_LOCAL_MACHINE」>「軟體」>「Microsoft」>「加密」>「MSCEP」下的登錄檔設定中更改預設SCEP模板。將EncryptionTemplate、GeneralPurposeTemplate和SignatureTemplate金鑰從IPsec（離線請求）更改為先前建立的WLC模板。



步驟35.重新啟動系統。

設定WLC

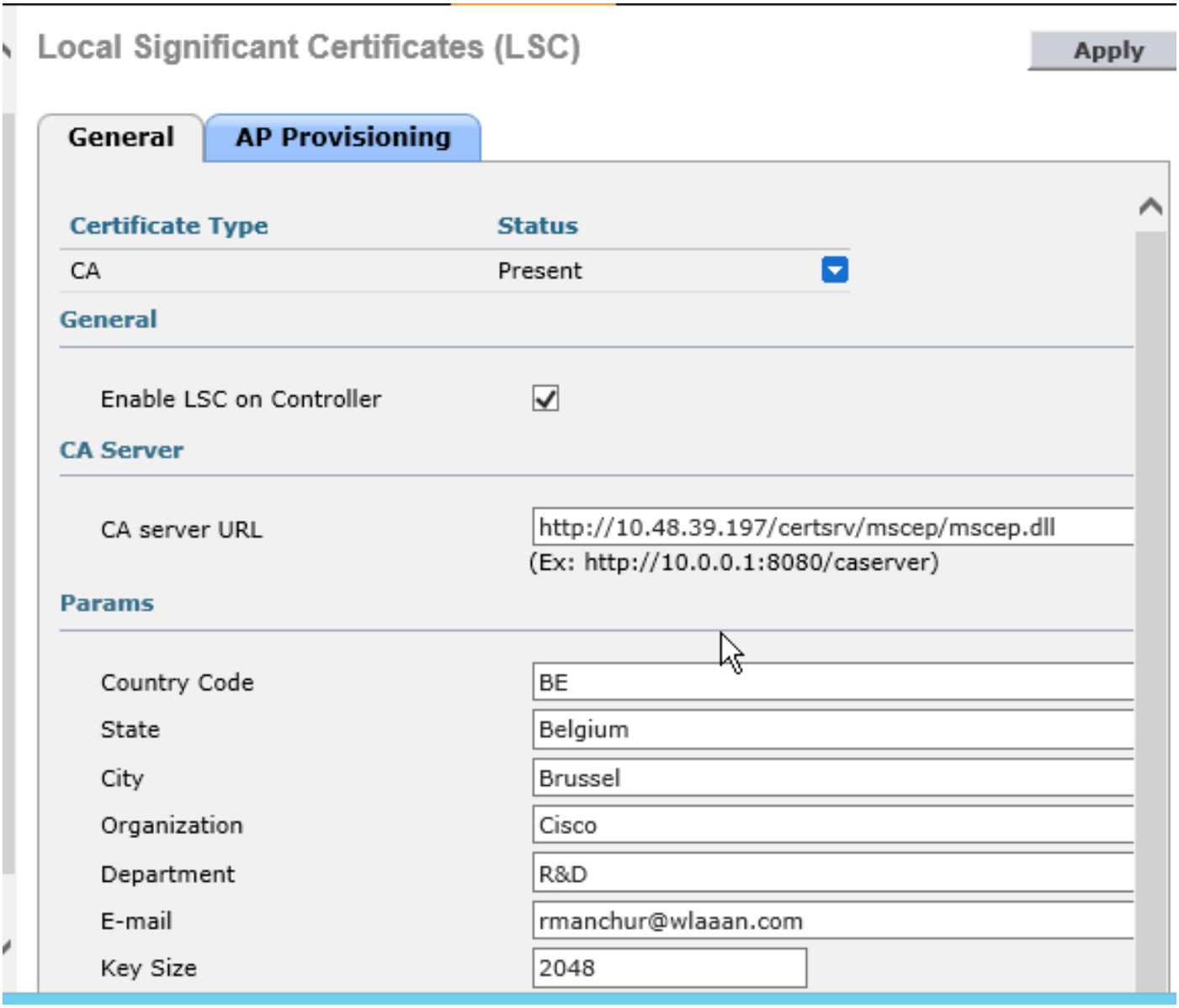
步驟1。在WLC上，導覽至Security功能表。按一下「**Certificates > LSC**」。

步驟2.勾選**在控制器上啟用LSC**覈取方塊。

步驟3.輸入您的Microsoft Windows Server 2012 URL。預設情況下，它會附加在**/certsrv/mscep/mscep.dll**中。

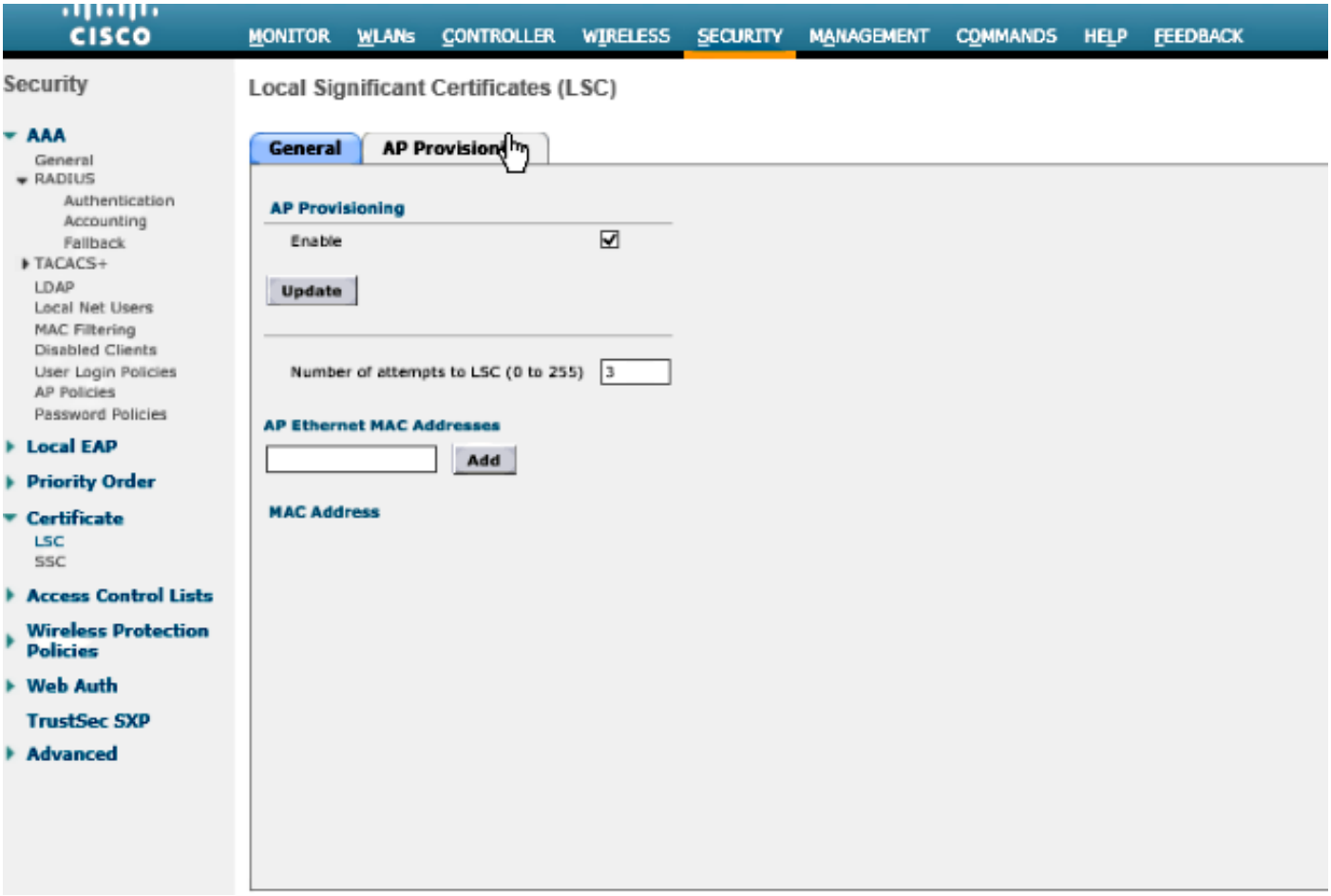
步驟4.在「引數」部分輸入您**的詳細**資訊。

步驟5.應用變更。



步驟6.按一下CA上方線上的藍色箭頭並選擇Add。應該將狀態從Not presence更改為presence。

步驟7.單擊AP調配頁籤。



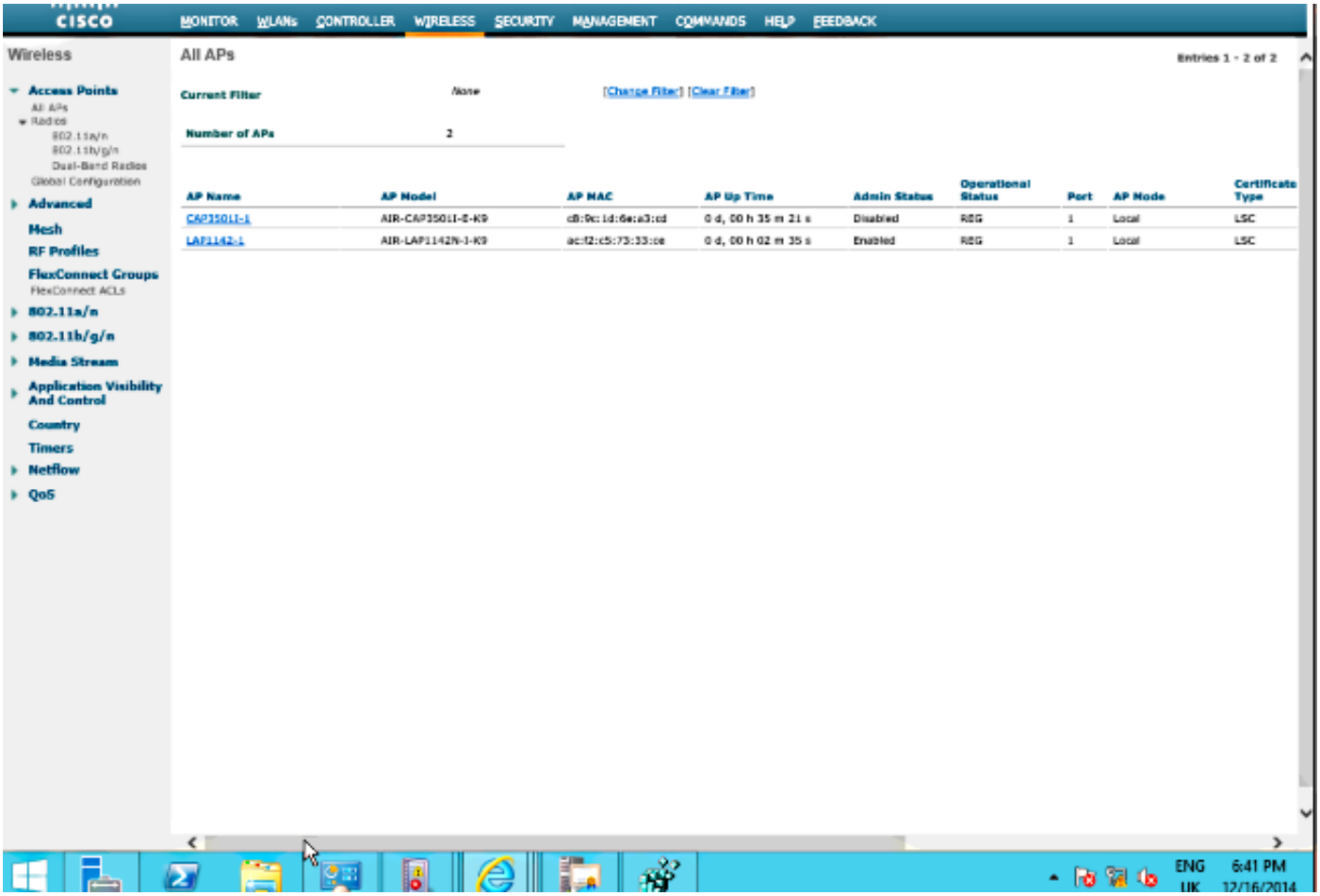
步驟8.選中AP Provisioning下的**Enable**覈取方塊，然後點選**Update。**

步驟9.如果接入點沒有自行重新啟動，請重新啟動它們。

驗證

使用本節內容，確認您的組態是否正常運作。

重新引導後，接入點會返回並顯示LSC作為「無線」選單中的證書型別。



附註：在8.3.112之後，一旦啟用LSC，MIC AP就根本無法加入。因此，「嘗試LSC」計數功能使用受到限制。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。