具有WLC和Windows Server 2012的本地有效证书(LSC)配置示例

目录

简介

本文档介绍如何使用无线局域网控制器(WLC)和新安装的Microsoft Windows Server 2012 R2配置本地有效证书(LSC)。

> **注意**：实际部署可能在很多方面有所不同，您应完全控制并了解Microsoft Windows Server 2012上的设置。此配置示例仅作为参考模板提供，供思科客户实施和调整其Microsoft Windows Server配置以使LSC工作。

先决条件

要求

思科建议您了解在Microsoft Windows Server中所做的每次更改，并在需要时检查相关的Microsoft文档。

> **注意**：中间CA不支持WLC上的LSC，因为根CA将从WLC丢失，因为控制器仅获取中间CA。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- WLC版本7.6
- Microsoft Windows Server 2012 R2

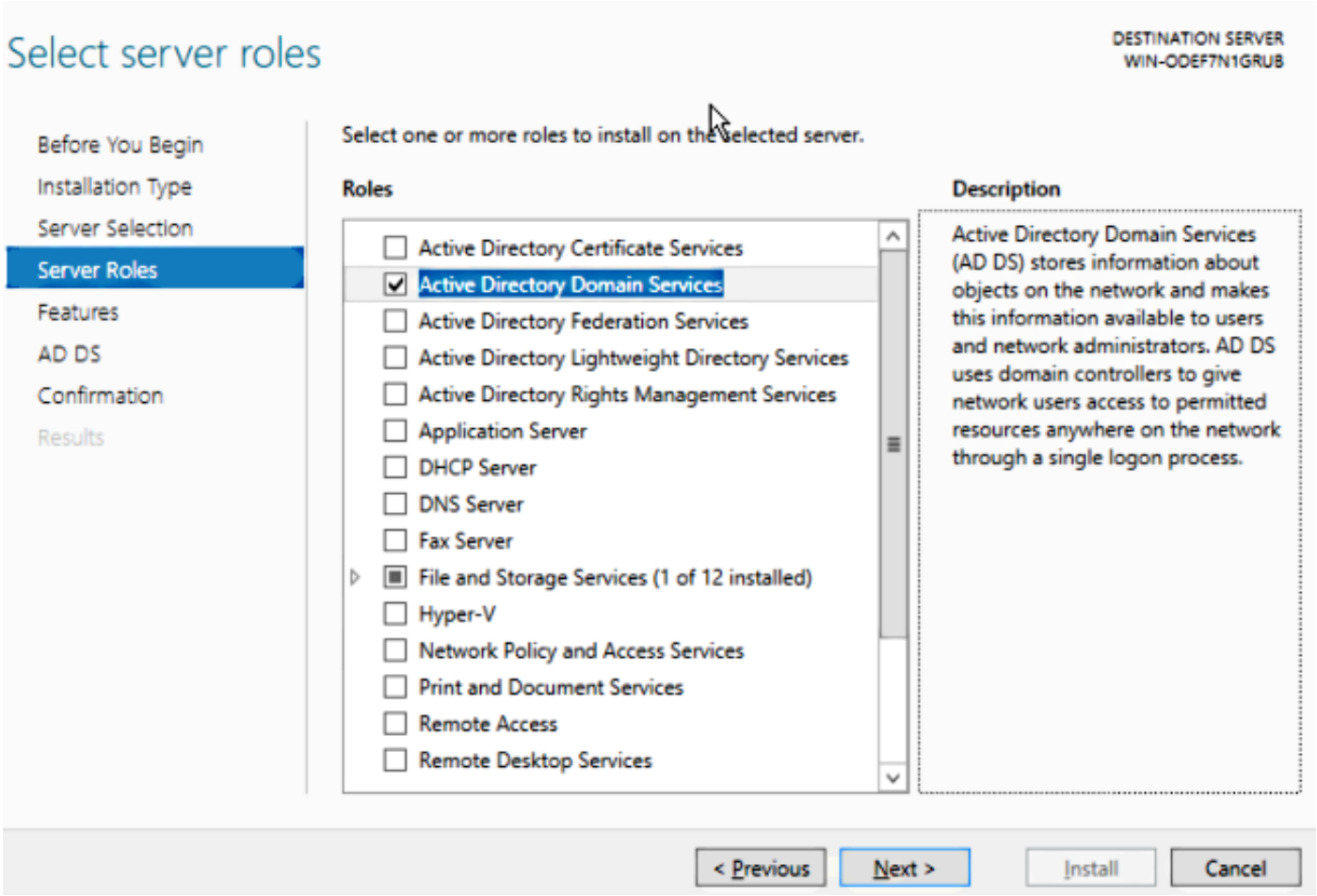
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

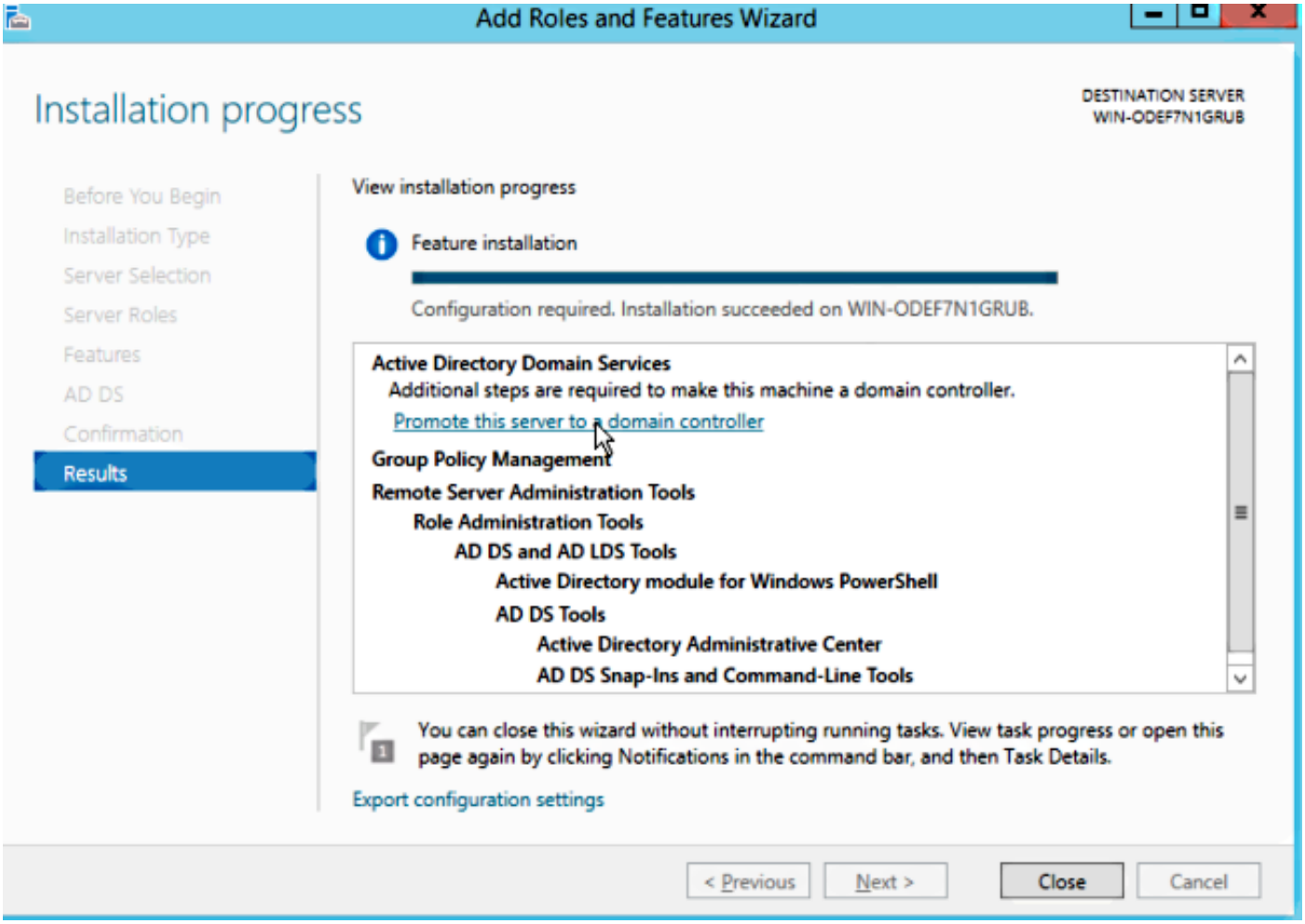
Microsoft Windows Server配置

此配置显示为在新安装的Microsoft Windows Server 2012上执行。您必须根据域和配置调整步骤。

步骤1.为角色和功能向导安装Active Directory域服务。

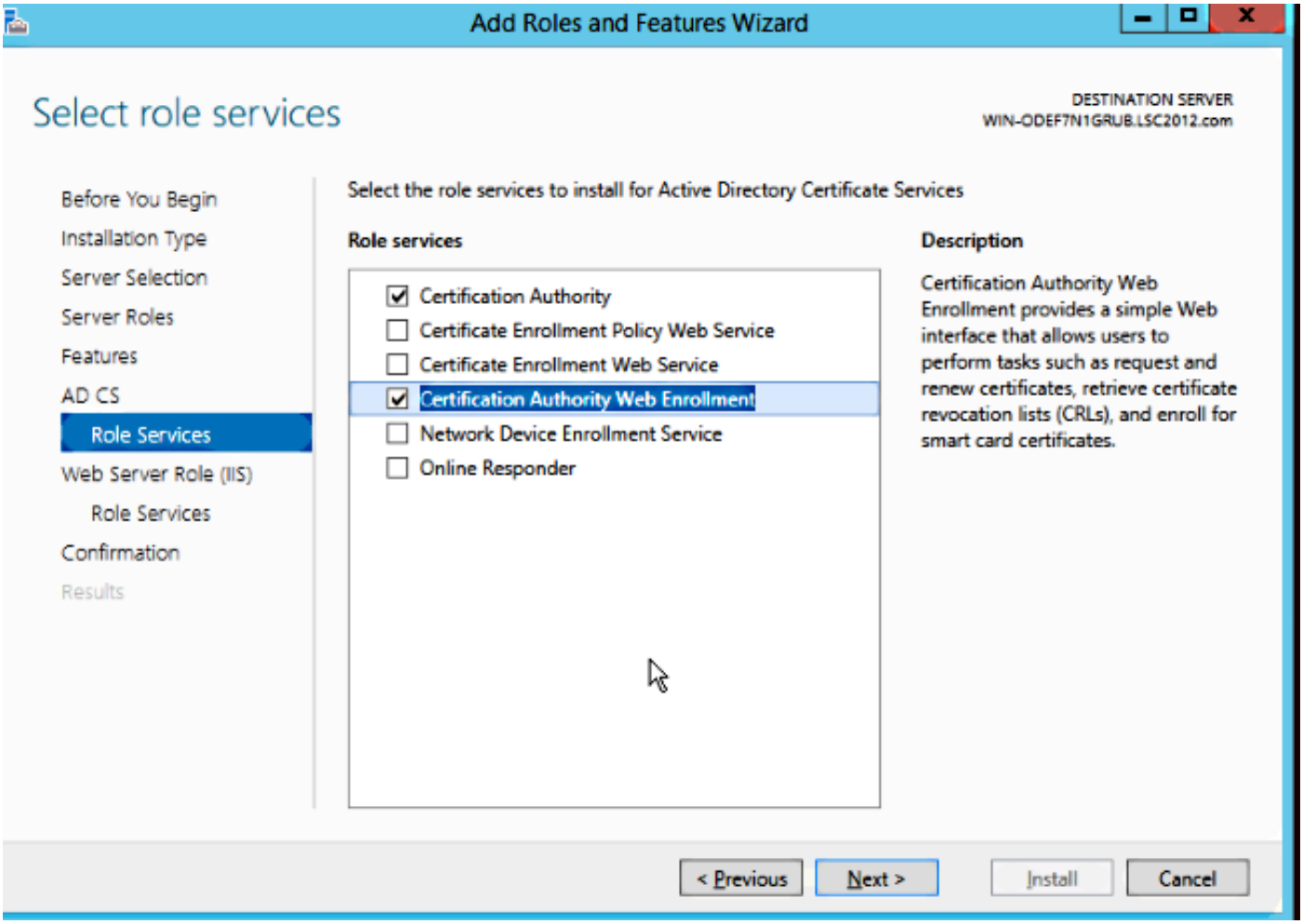


步骤2.安装后，必须将服务器升级到域控制器。

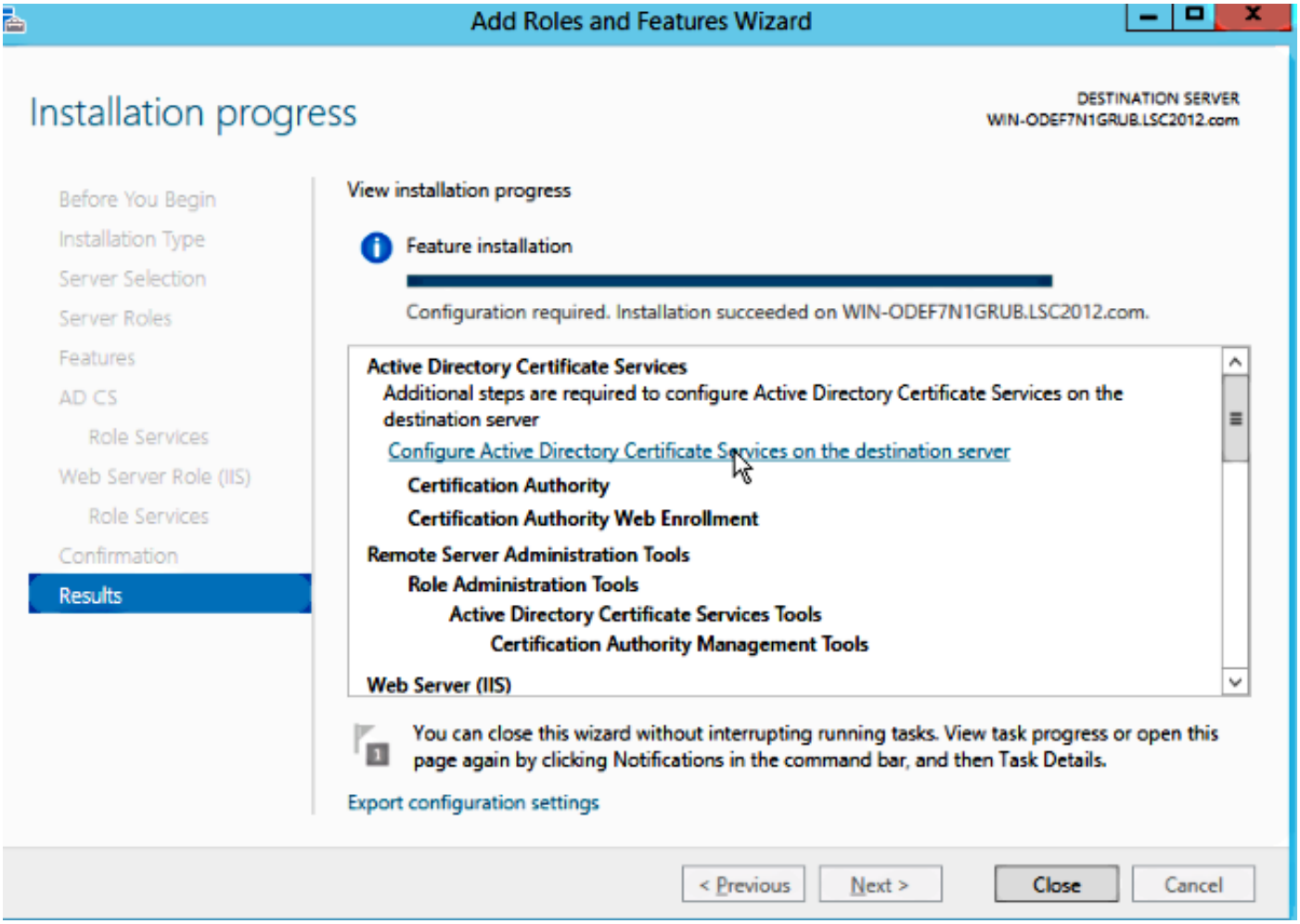


步骤3.由于这是新设置，因此您配置了新林；但通常在现有部署中，只需在域控制器上配置这些点。此处，您选择**LSC2012.com**域。这也会激活域名服务器(DNS)功能。

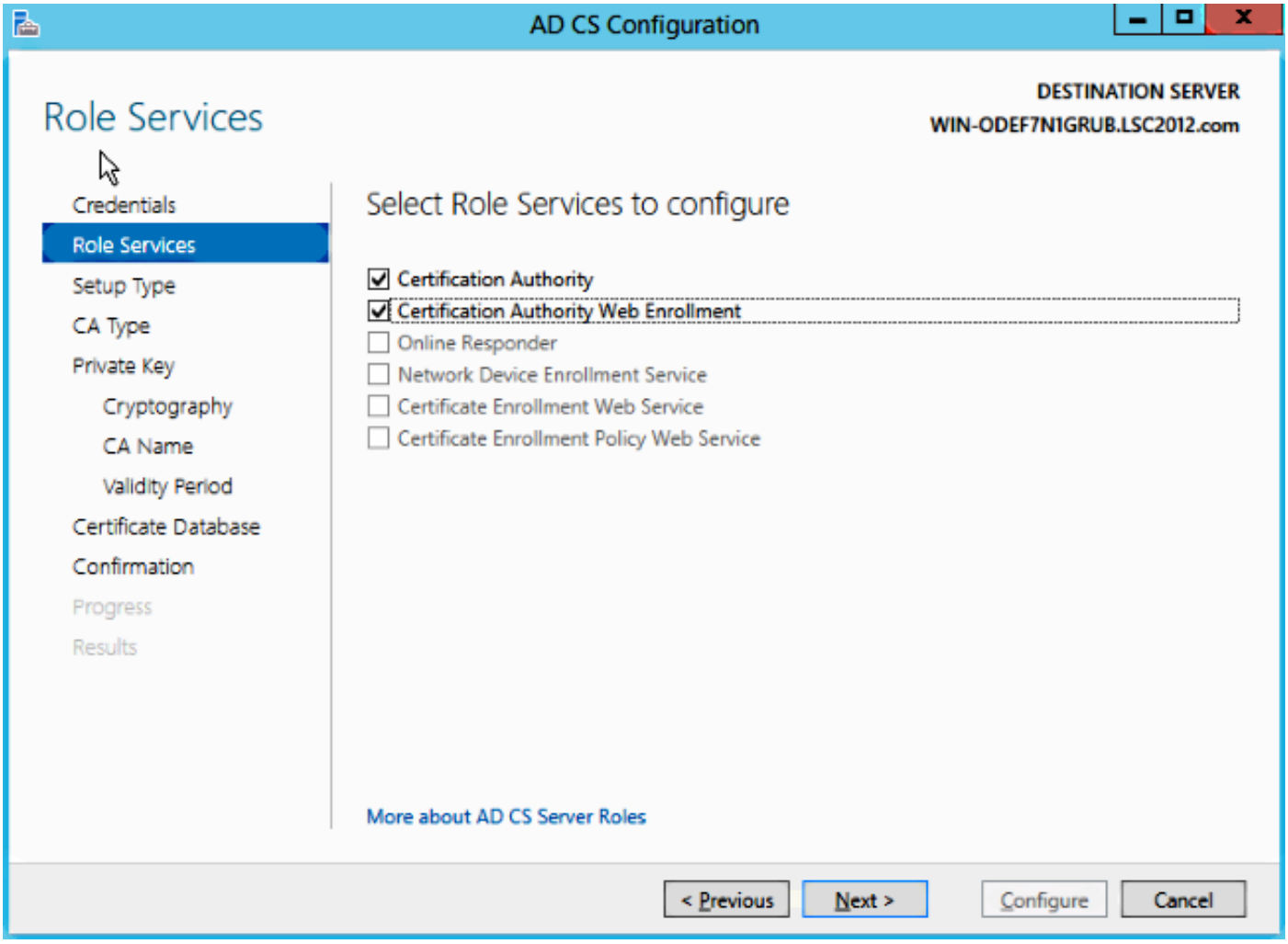
步骤4.重新启动后，安装证书颁发机构(CA)服务和Web注册。


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

步骤5.配置它们。



步骤6.选择企业CA并保留所有默认值。

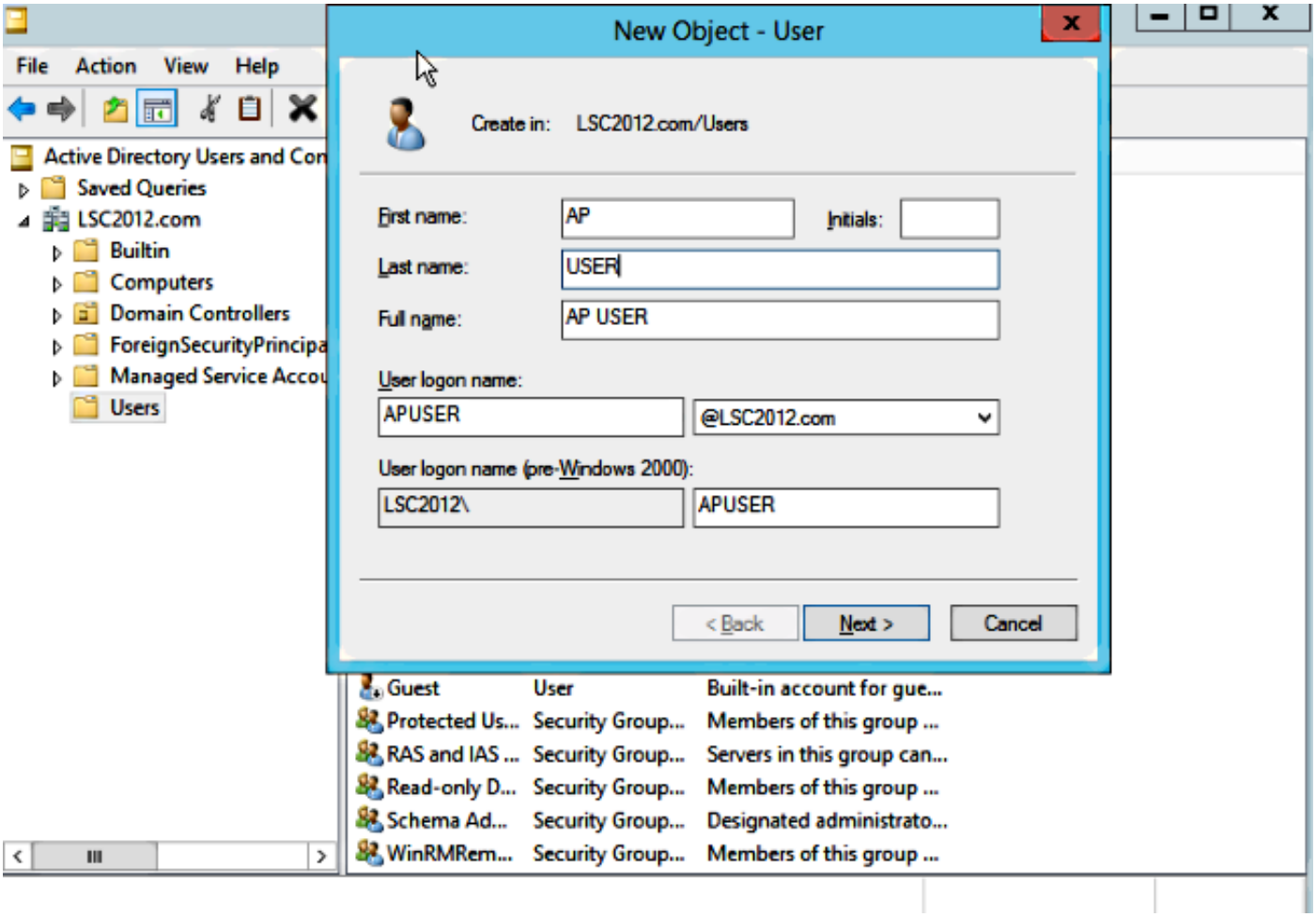


步骤7.单击“Microsoft Windows/开始”菜单。

步骤8.单击管理工具。

步骤9.单击“Active Directory用户和计算机”。

步骤10.展开域，右键单击“用户”文件夹，然后选择“新建对象”>“用户”。



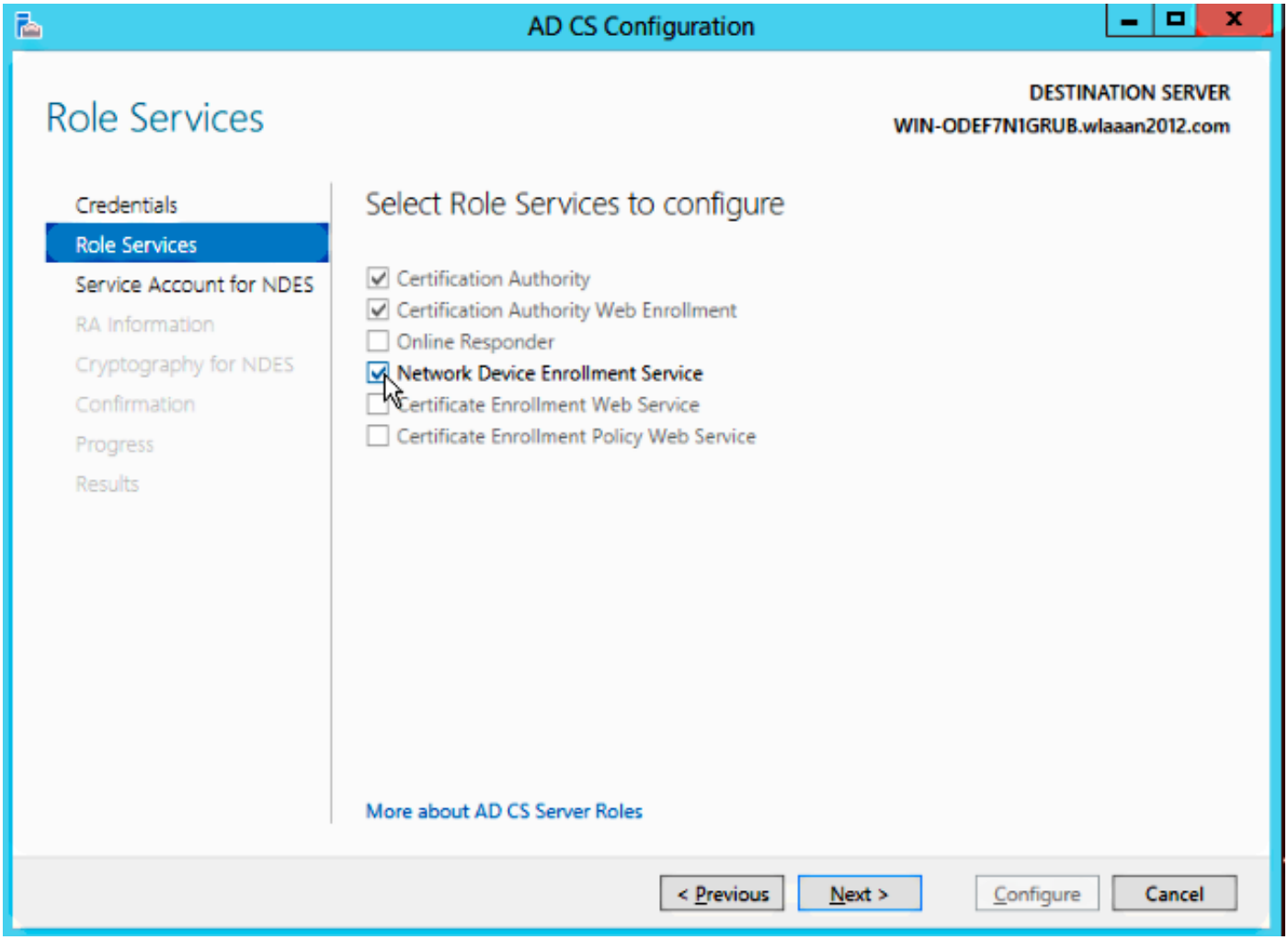
步骤11.在本例中，它命名为**APUSER**。创建后，必须编辑用户并单击**MemberOf**选项卡，并将其设置为IIS_IUSRS组的成员

所需的用户权限分配包括：

— 允许本地登录

— 以服务身份登录

步骤12.安装网络设备注册服务(NDES)。



- 在本例中，选择IIS_USRS组的帐户成员**APUSER**作为NDES的服务帐户。

步骤13.导航至Administrative Tools。

步骤14.单击“**Internet信息服务(IIS)**”。

步骤15.展开Server **> Sites > Default web site > Cert Srv**。

步骤16.对于mscep和**mscep_admin**，单击身份验证。确保已启用匿名身份验证。

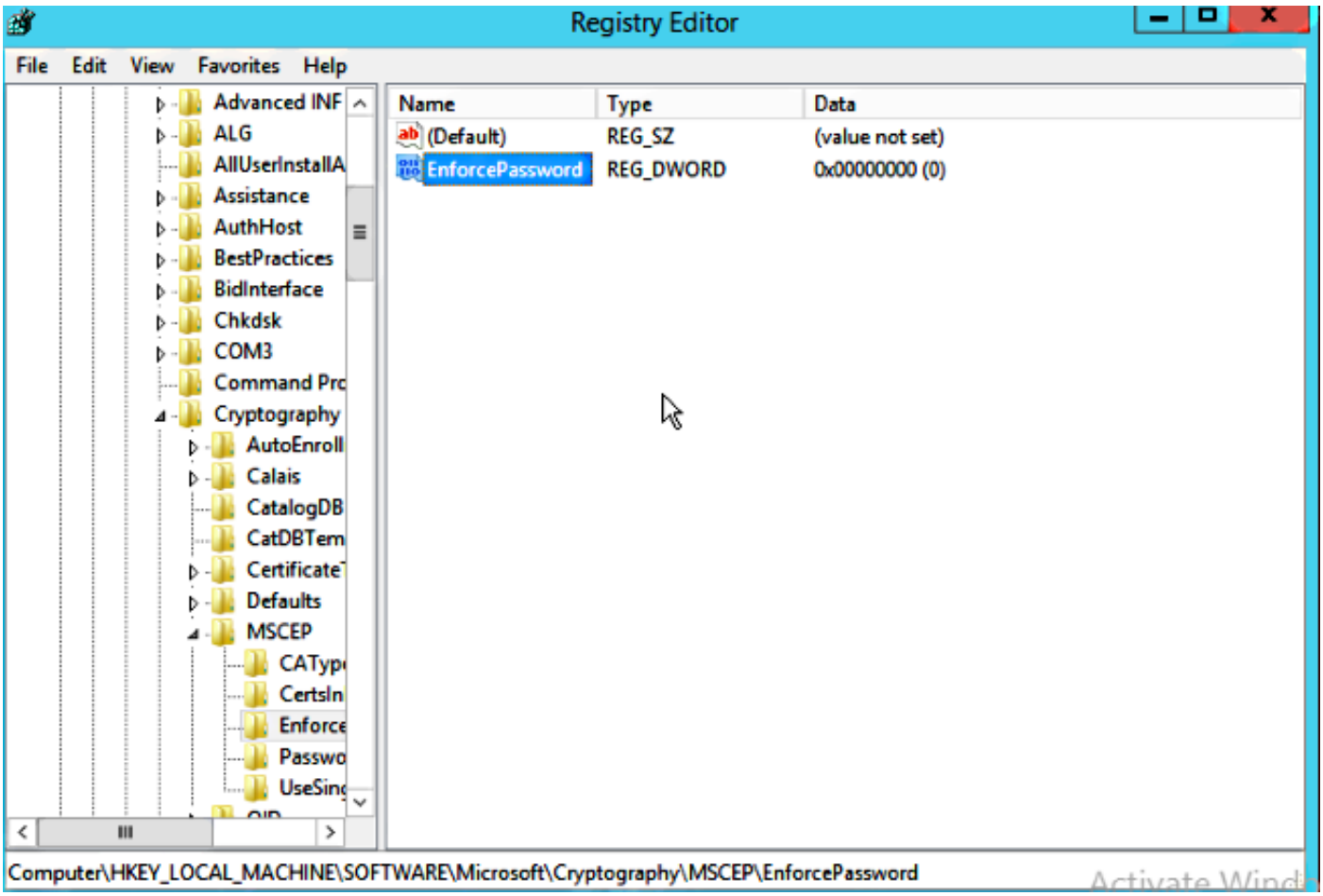
步骤17.右键单击Windows身**份验**证并选择**提供程**序。确保NT LAN Manager(NTLM)在列表中处于首位。

步骤18.在注册表设置中禁用身份验证质询，否则简单证书注册协议(SCEP)需要质询密码身份验证，WLC不支持该身份验证。

步骤19.打开regedit**应用程序**。

步骤20.转到HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\Cryptography\MSCEP\。

步骤21.将EnforcePassword设置为0。



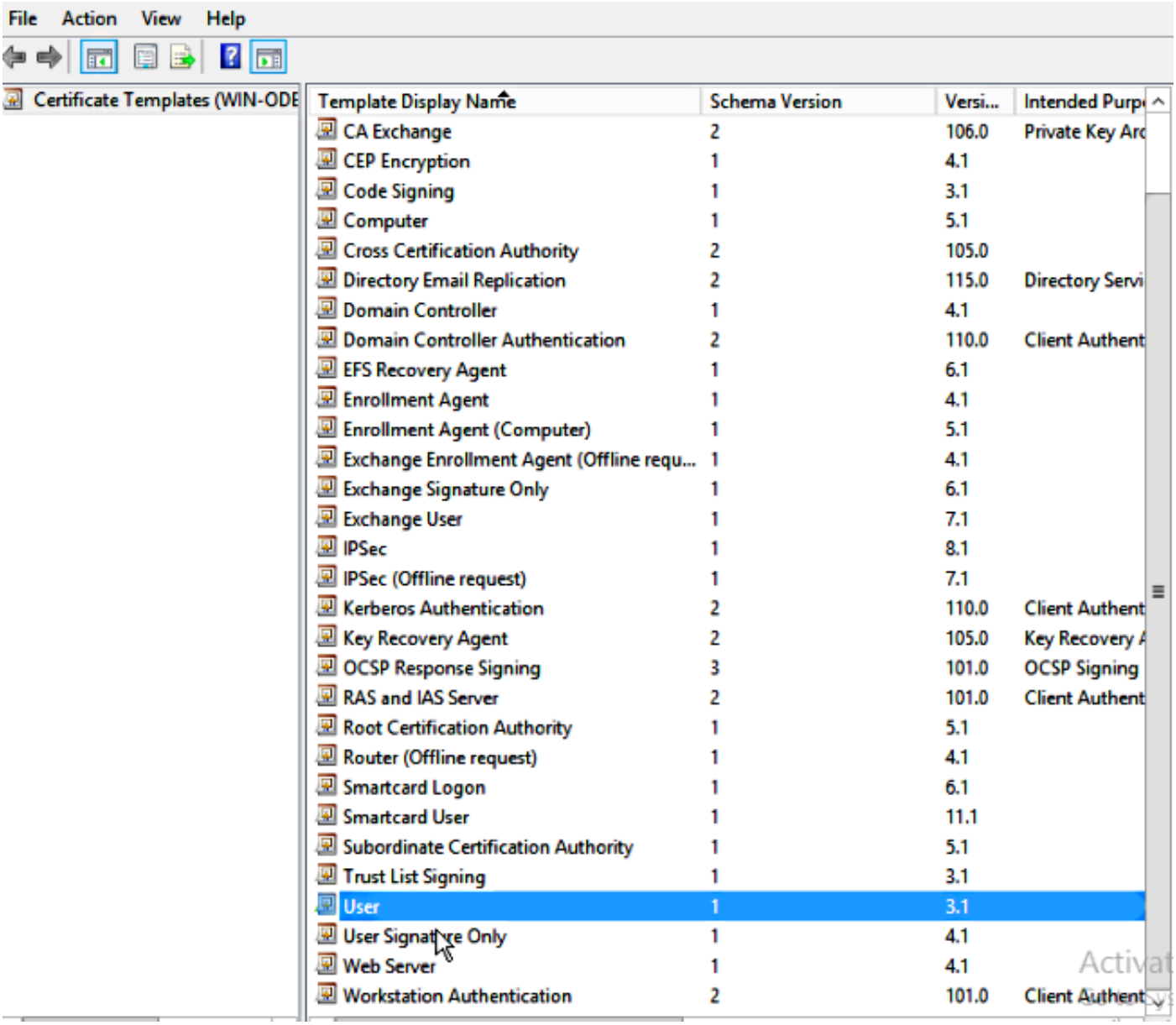
步骤22.单击“Microsoft Windows/开始”菜单。

步骤23.键入MMC。

步骤24.在“文件”菜单中，选择“添加/删除管理单元”。选择Certification Authority。

步骤25.右键单击Certificate Template(证书模板)文件夹，然后单击Manage。

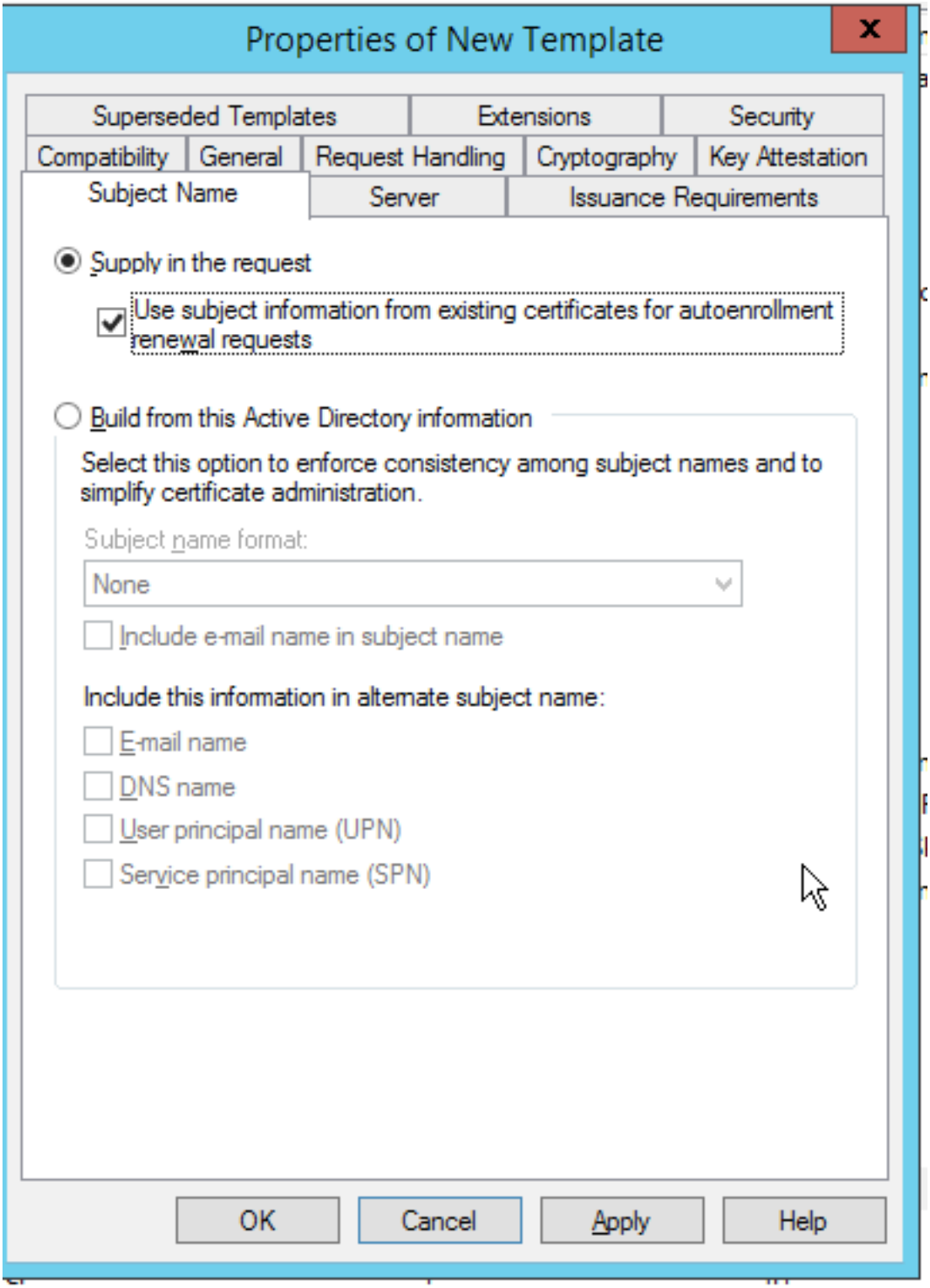
步骤26.右键单击现有模板（如用户），然后选择“复制模板”。



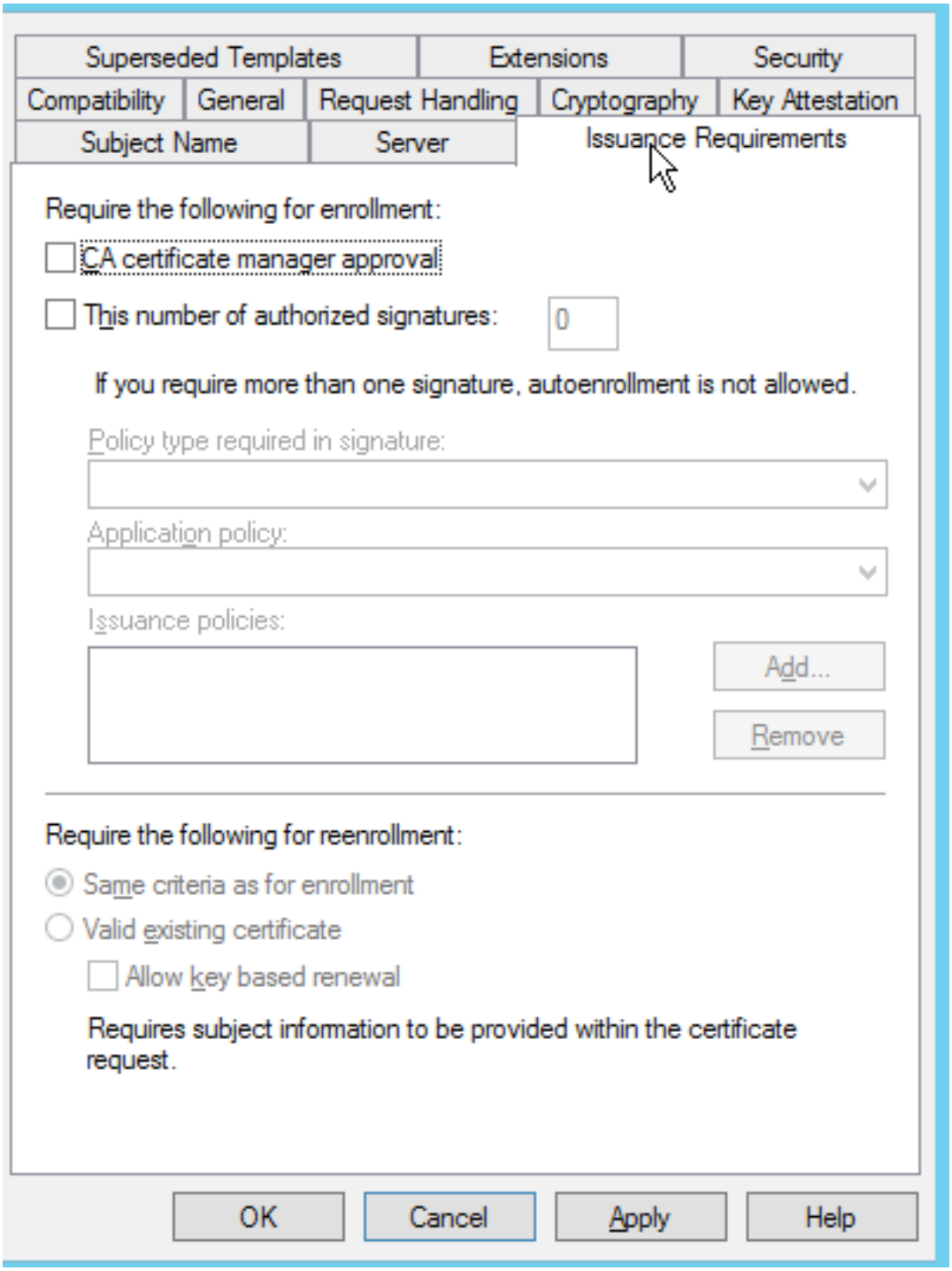
步骤27.选择CA作为Microsoft Windows 2012 R2。

步骤28.在 General选项卡上，添加显示名称（如WLC）和有效期。

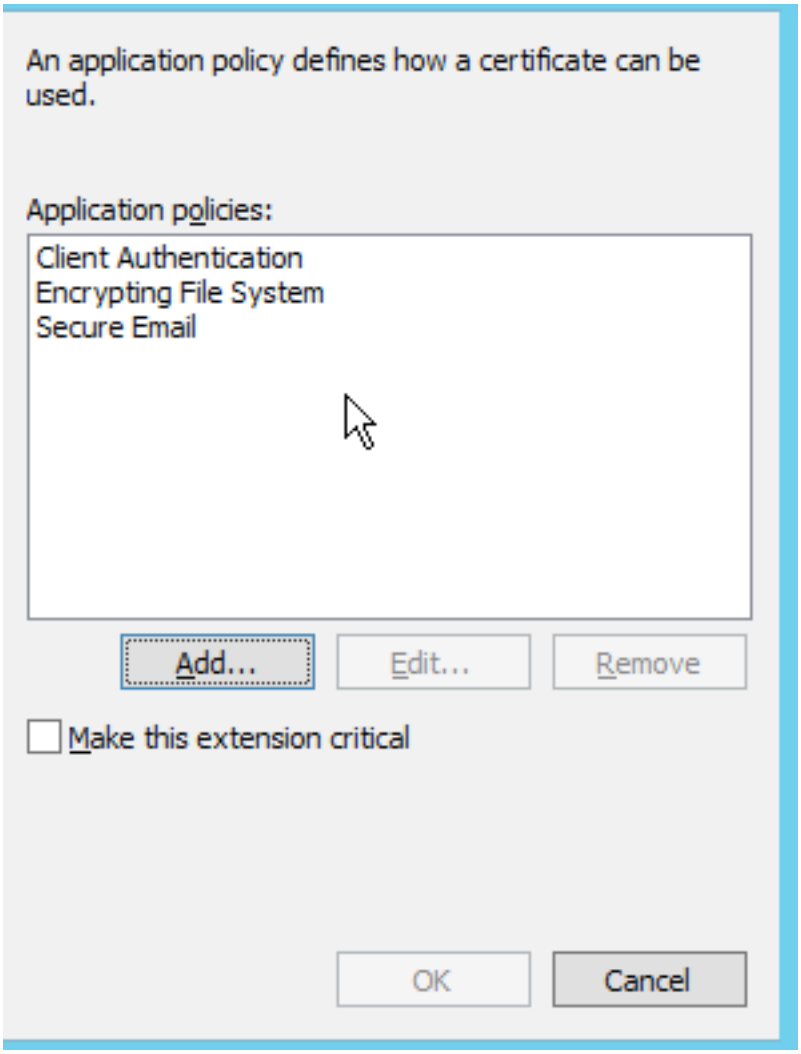
步骤29.在“主题名称”选项卡中，确认选**择了“请求中**的供应”。



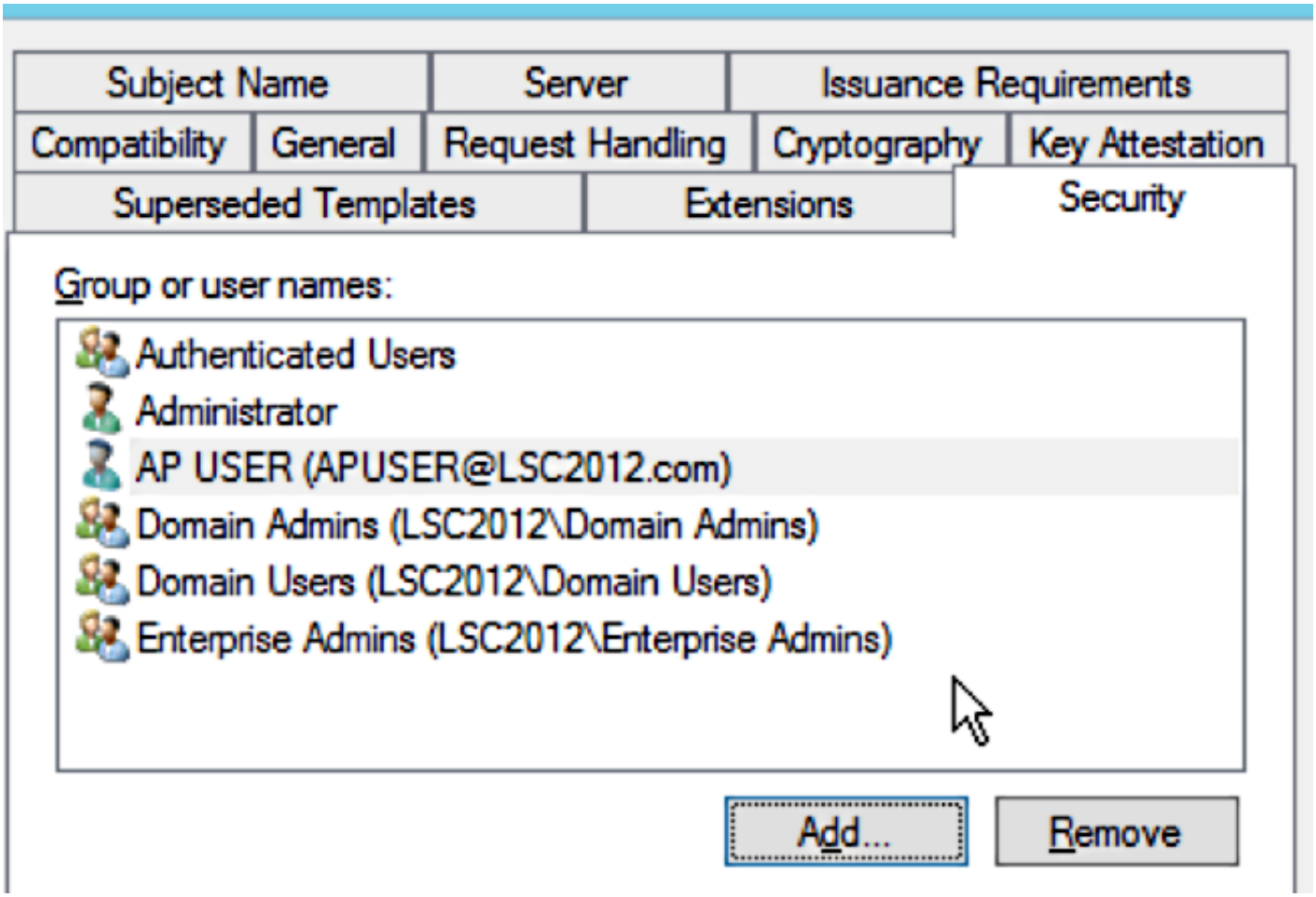
步骤30.单击Issuance Requirements**选项**卡。思科建议您在典型的分层CA环境中将颁发策略留空：



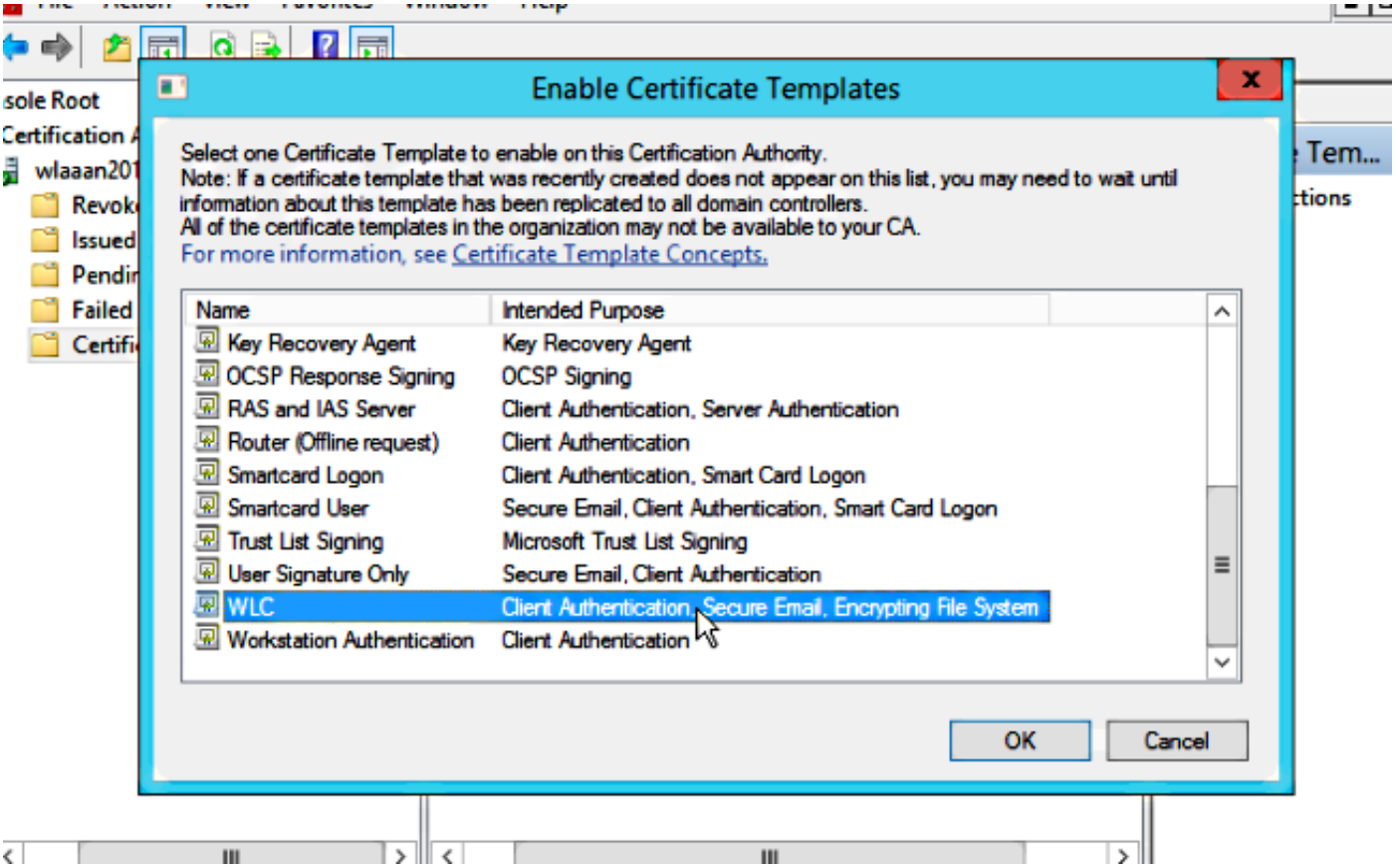
步骤31.单击“扩展”选项卡、“应用策略”和“编辑”。单击**Add**，并确保将Client Authentication添加为应用策略。Click **OK**.



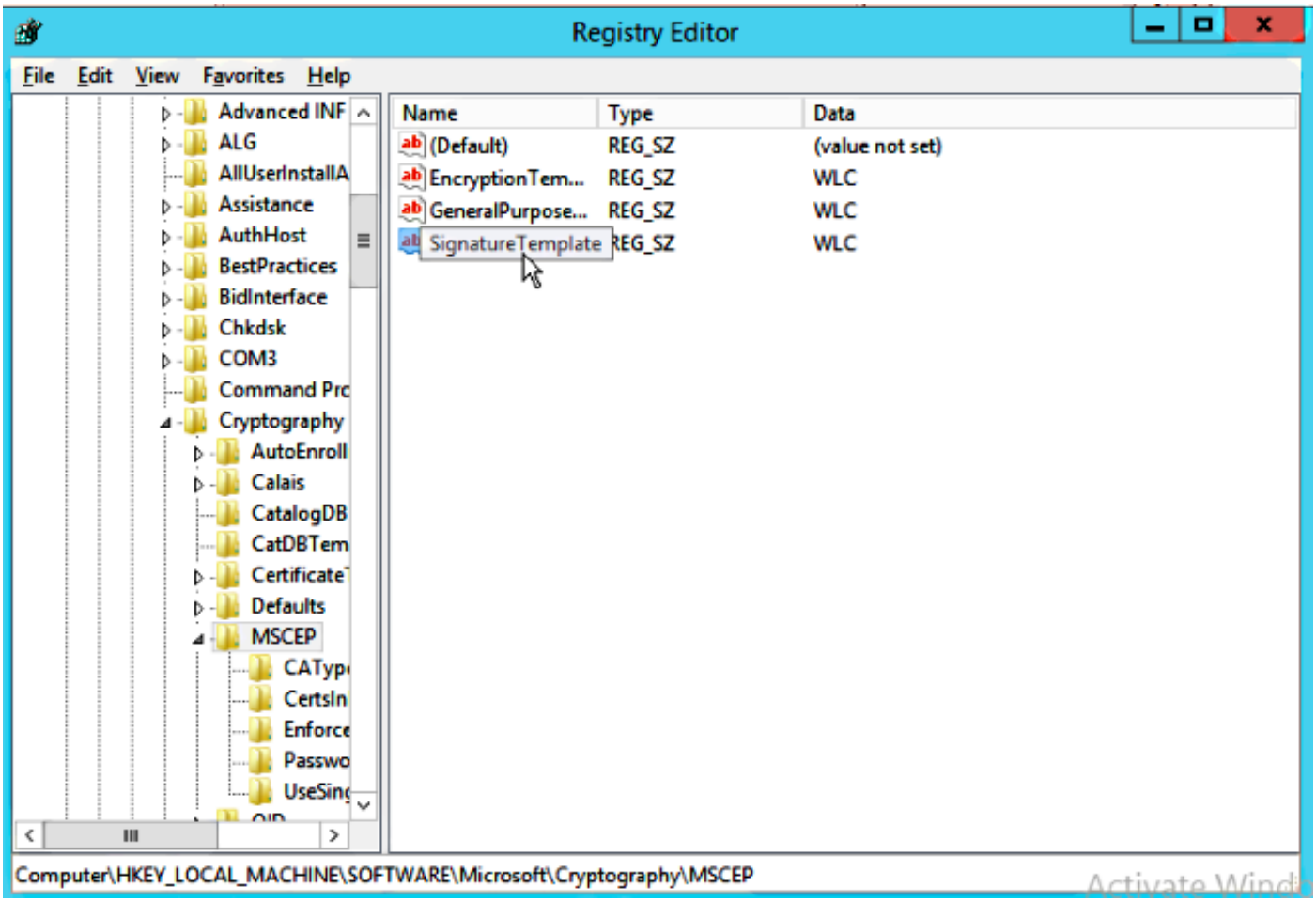
步骤32.单击“安全”选项卡，然后单击“添加……。确保在NDES服务安装中定义的SCEP服务帐户对模板具有完全控制权，然后单击OK。



步骤33.返回到证书颁发机构GUI界面。右键单击“证书模**板”目录**。导航至“**新建”>“要颁发的证书模板**”。选择之前配置的WLC模板，然后单击**OK。**



步骤34.在“计算机”>“HKEY_LOCAL_MACHINE”>“软件”>“Microsoft”>“加密”>“MSCEP”下的注册表设置中更改默认的SCEP模板。将EncryptionTemplate、GeneralPurposeTemplate和SignatureTemplate密钥从IPsec（脱机请求）更改为先前创建的WLC模板。



步骤35.重新启动系统。

配置 WLC

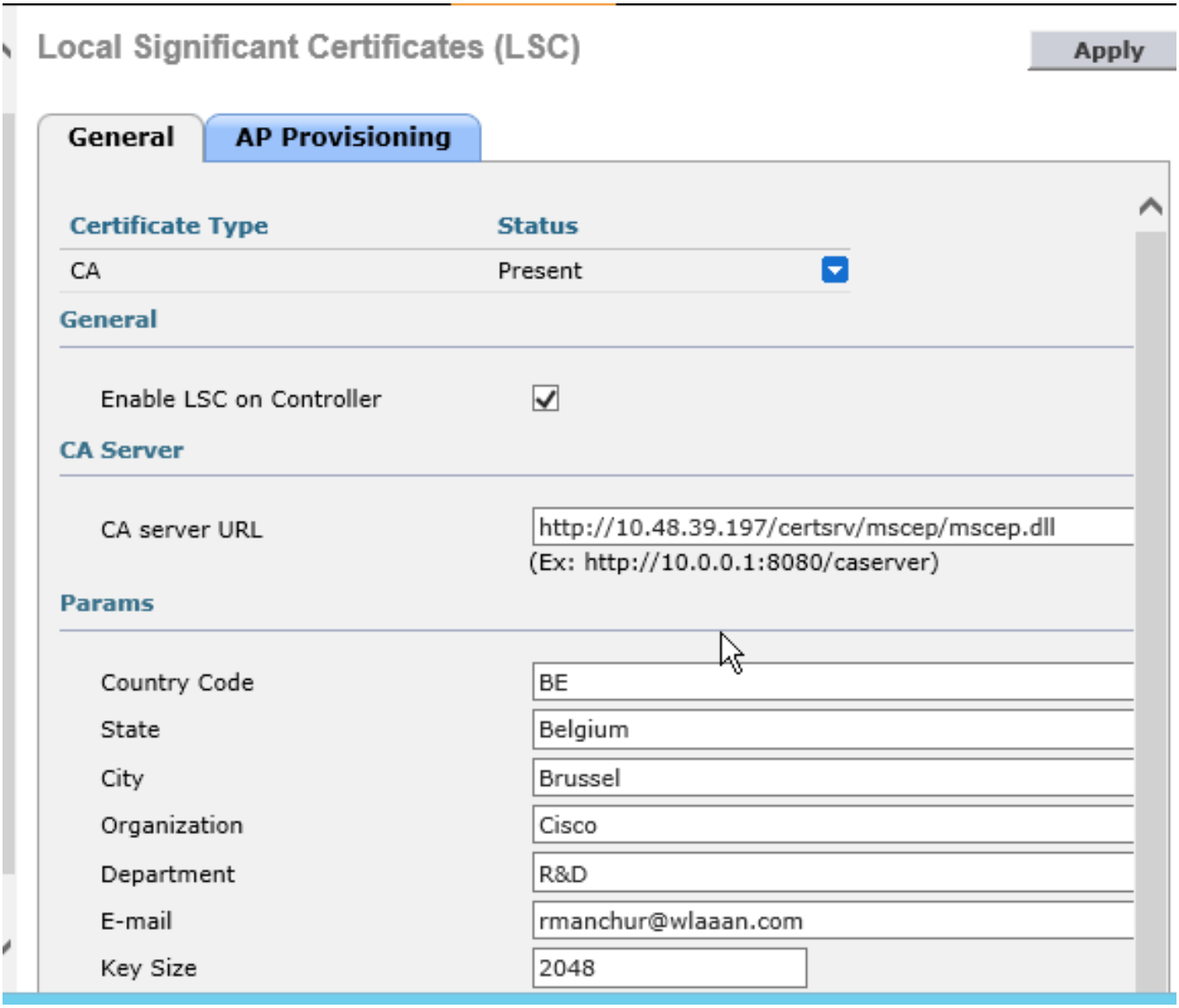
步骤1.在WLC上，导航至Security菜单。单击**Certificates > LSC**。

步骤2.选中Enable LSC on **Controller复选**框。

步骤3.输入Microsoft Windows Server 2012 URL。默认情况下，会附加**/certsrv/mscep/mscep.dll**。

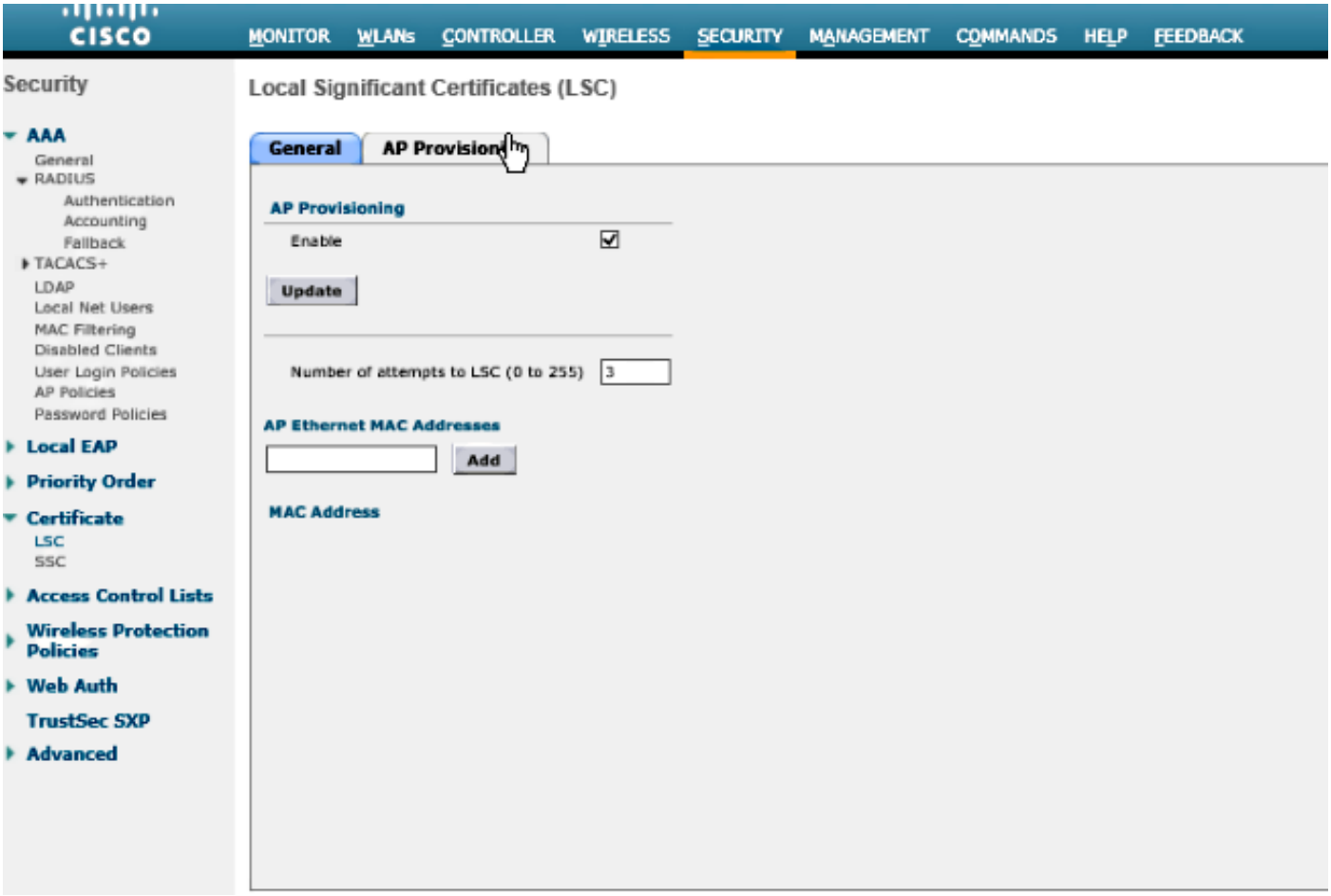
步骤4.在“参数”部分输入**详细**信息。

步骤5.应用更改。



步骤6.单击CA上行的蓝色箭头并选择“添**加”**。它应将状态从“不**存在”**更改**为“存在**”

步骤7.单击AP**调配选项卡**。



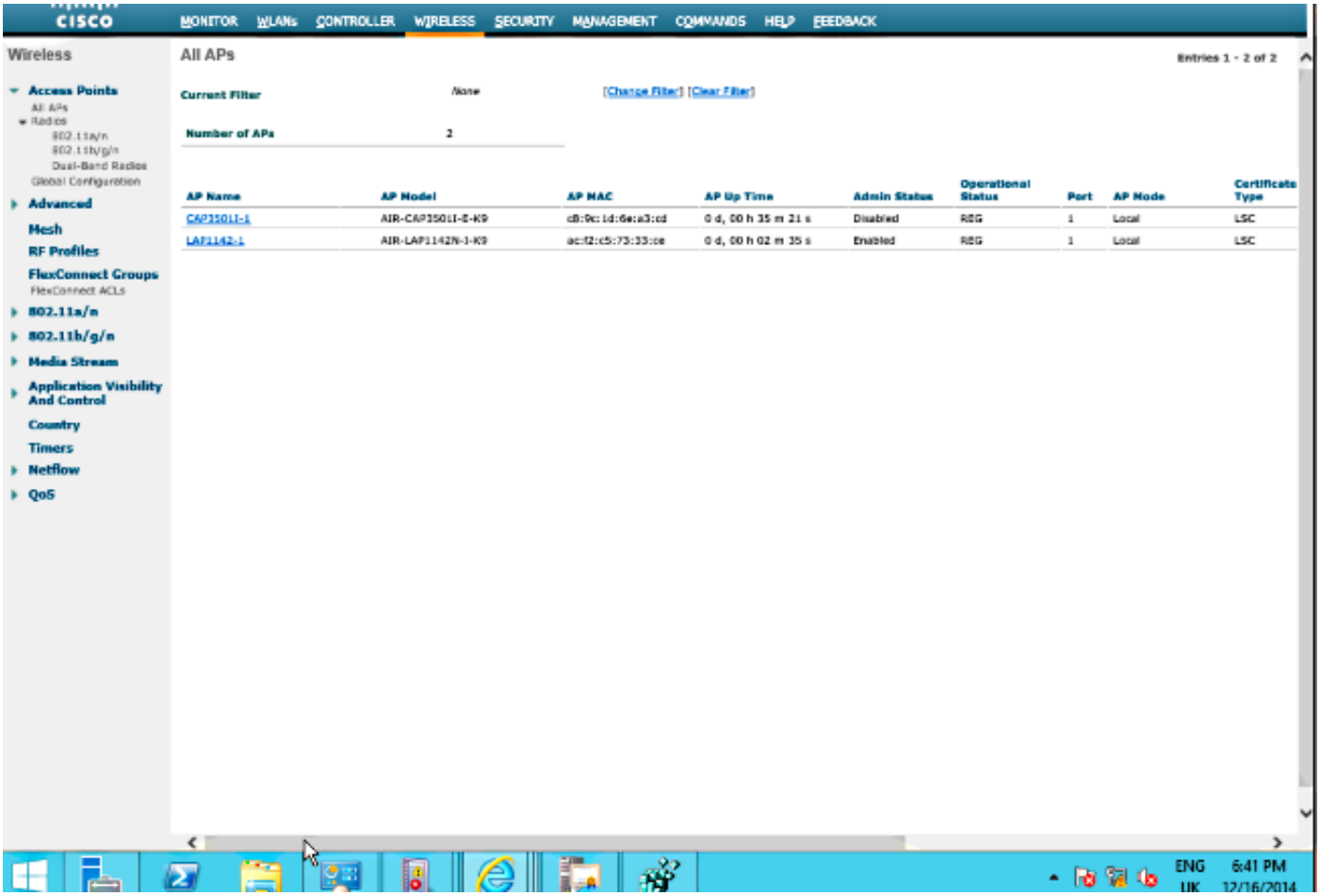
步骤8.选中AP Provisioning下**的**Enable复选框，然后单击**Update**。

步骤9.如果接入点没有自行重新启动，请重新启动它们。

验证

使用本部分可确认配置能否正常运行。

重新启动后，接入点会重新连接并以LSC作为证书类型显示在Wireless（无线）菜单中。



注意：在8.3.112之后，MIC AP在启用LSC后，将无法加入。因此，“尝试LSC”计数功能的使用有限。

故障排除

目前没有针对此配置的故障排除信息。