Locally Significant Certificates (LSC) with WLC and Windows Server 2012 Configuration Example

Contents

Introduction

This document describes how to configure Locally Significant Certificates (LSC) with a Wireless LAN Controller (WLC) and a newly-installed Microsoft Windows Server 2012 R2.

> **Note**: Real deployments might differ in many points and you should have full control and knowledge of the settings on Microsoft Windows Server 2012. This configuration example is only provided as a reference template for Cisco customers to implement and adapt their Microsoft Windows Server configuration in order to make LSC work.

Prerequisites

Requirements

Cisco recommends that you understand every change made in Microsoft Windows Server and check the relevant Microsoft documentation if needed.

> **Note**: LSC on WLC is not supported with intermediate-CA, as the root CA will is missed from WLC since the controller only gets the intermediate CA.

Components Used

The information in this document is based on these software and hardware versions:

- WLC Version 7.6
- Microsoft Windows Server 2012 R2

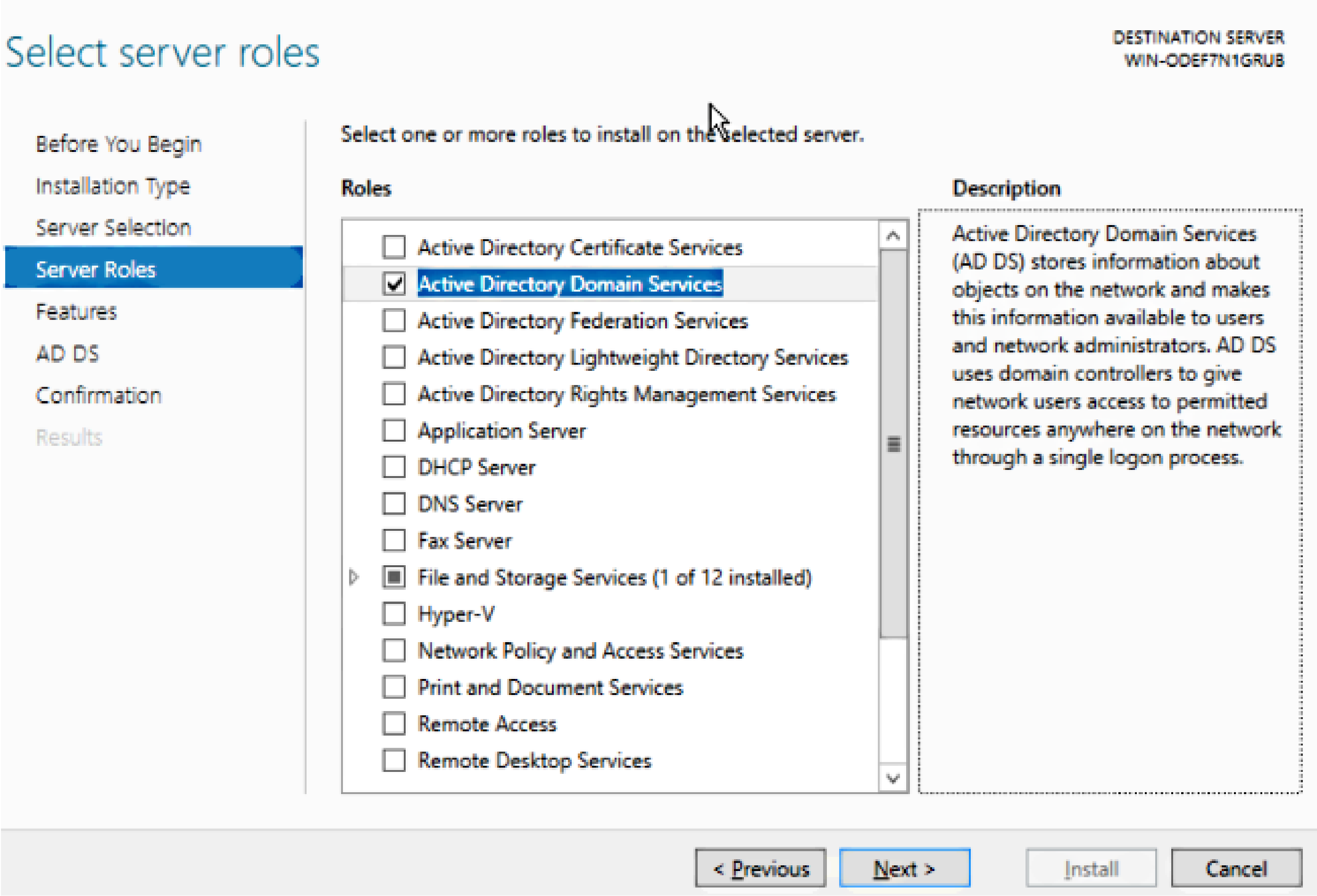
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configure

Microsoft Windows Server Configuration

This configuration is shown as performed on a newly-installed Microsoft Windows Server 2012. You must adapt the steps to your domain and your configuration.

Step 1. Install Active Directory Domain Services for the roles and features wizard.



Select server roles

DESTINATION SERVER
WIN-ODEF7N1GRUB

Select one or more roles to install on the selected server.

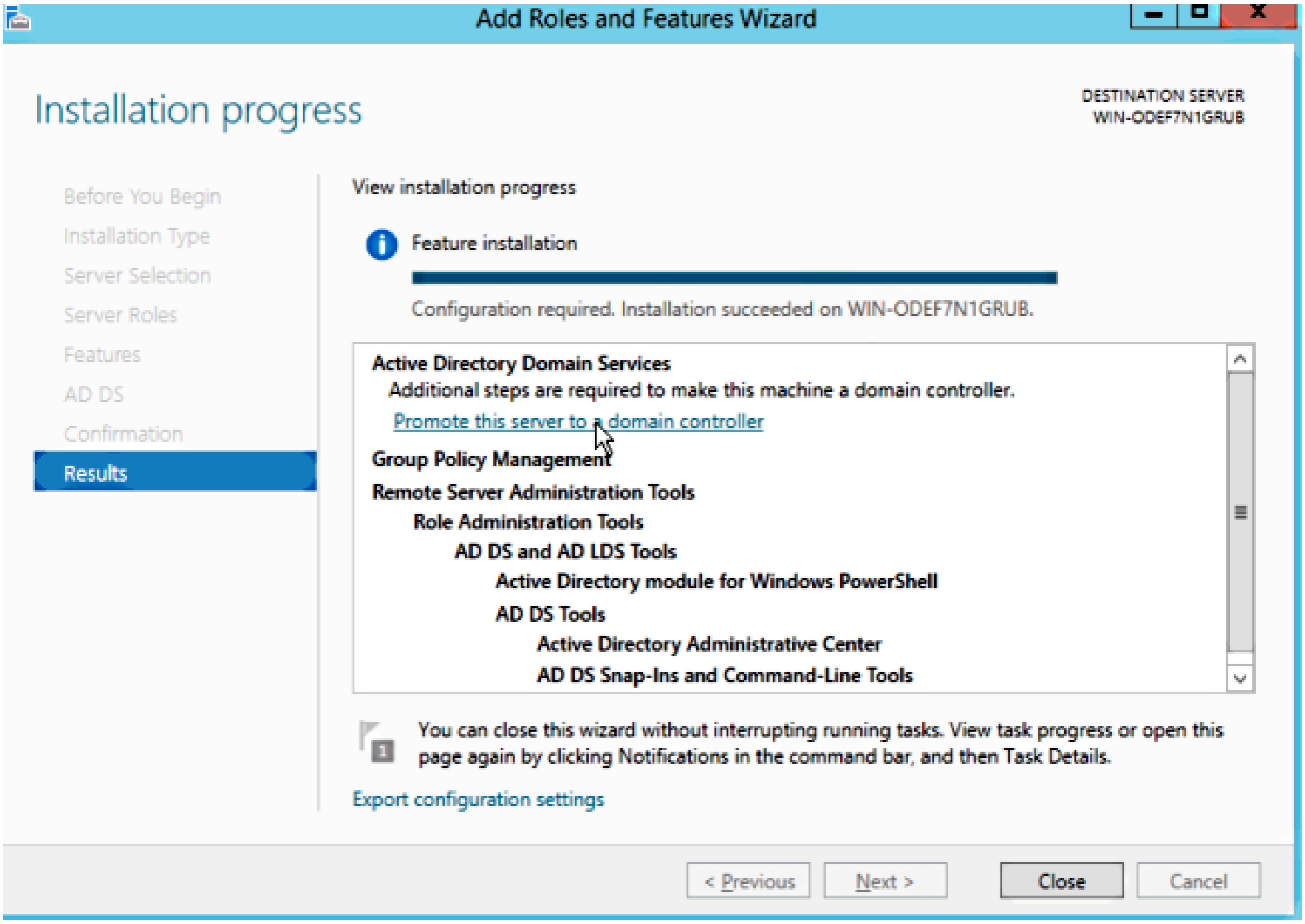
Roles

- □ Active Directory Certificate Services
- ☑ Active Directory Domain Services
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Application Server
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- ■ File and Storage Services (1 of 12 installed)
- □ Hyper-V
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services

Description

Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.

Step 2. After installation, you must promote the server to domain controller.



View installation progress

Feature installation

Configuration required. Installation succeeded on WIN-ODEF7N1GRUB.

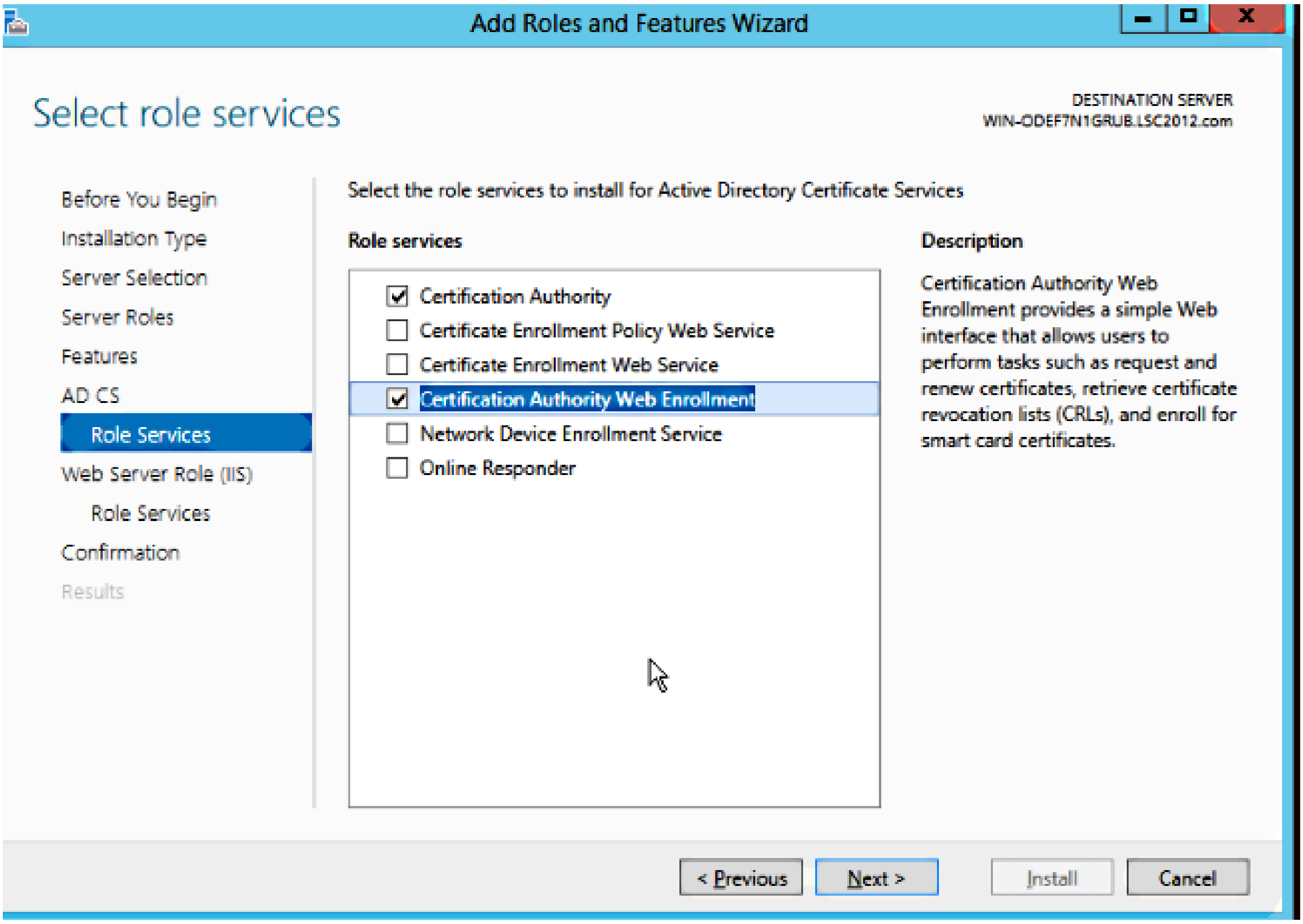
Active Directory Domain Services
Additional steps are required to make this machine a domain controller.
Promote this server to a domain controller
Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
Active Directory Administrative Center
AD DS Snap-Ins and Command-Line Tools

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

Step 3. Since this is a new setup, you configure a new forest; but typically in existing deployments, simply configure these points on a domain controller. Here, you choose the **LSC2012.com** domain. This activates the Domain Name Server (DNS) feature as well.

Step 4. After a reboot, install the Certificate Authority (CA) service as well as web enrollment.



Select role services

DESTINATION SERVER
WIN-ODEF7N1GRUB.LSC2012.com

Select the role services to install for Active Directory Certificate Services

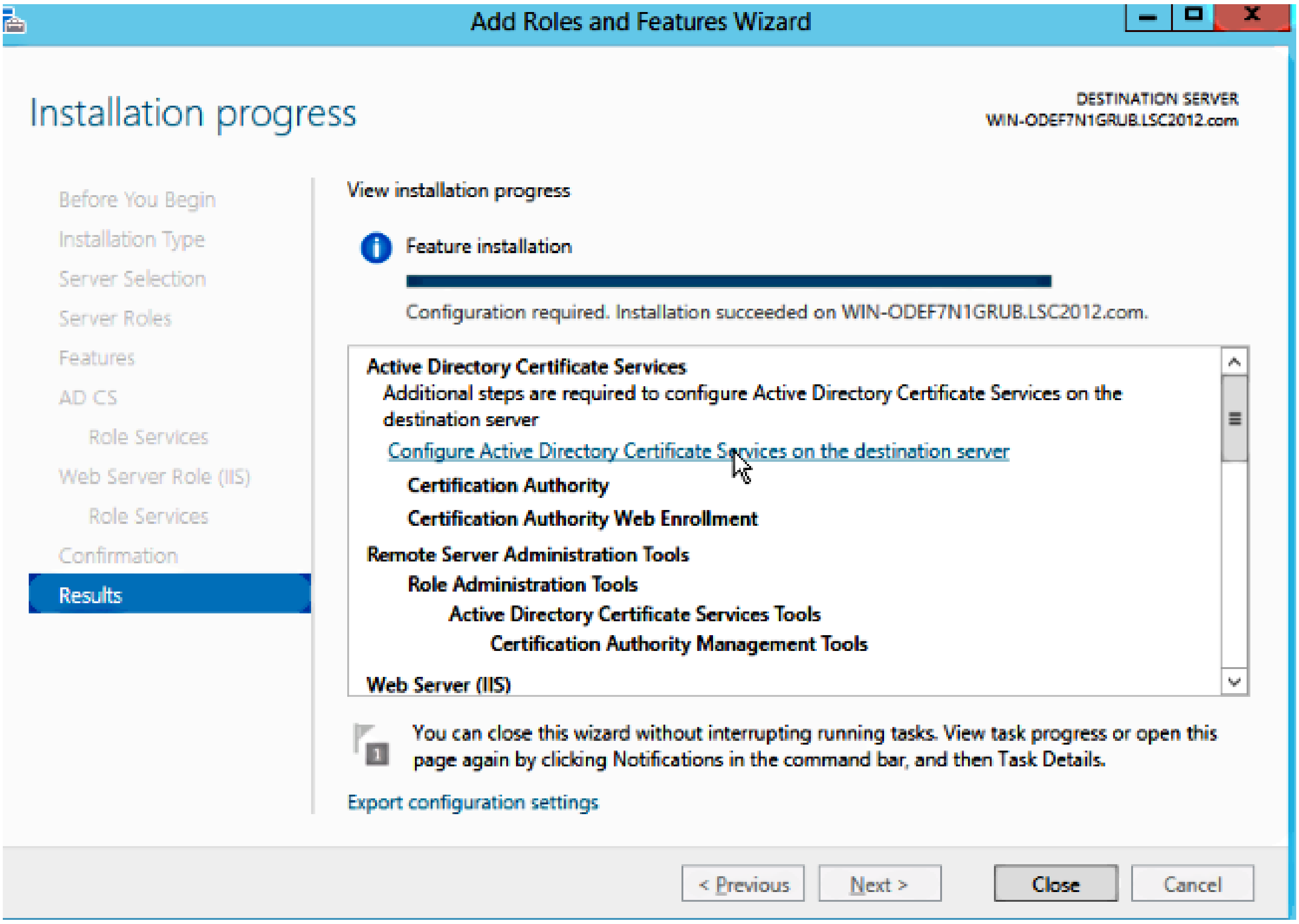
Role services

☑ 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.

Step 5. Configure them.



View installation progress

Feature installation

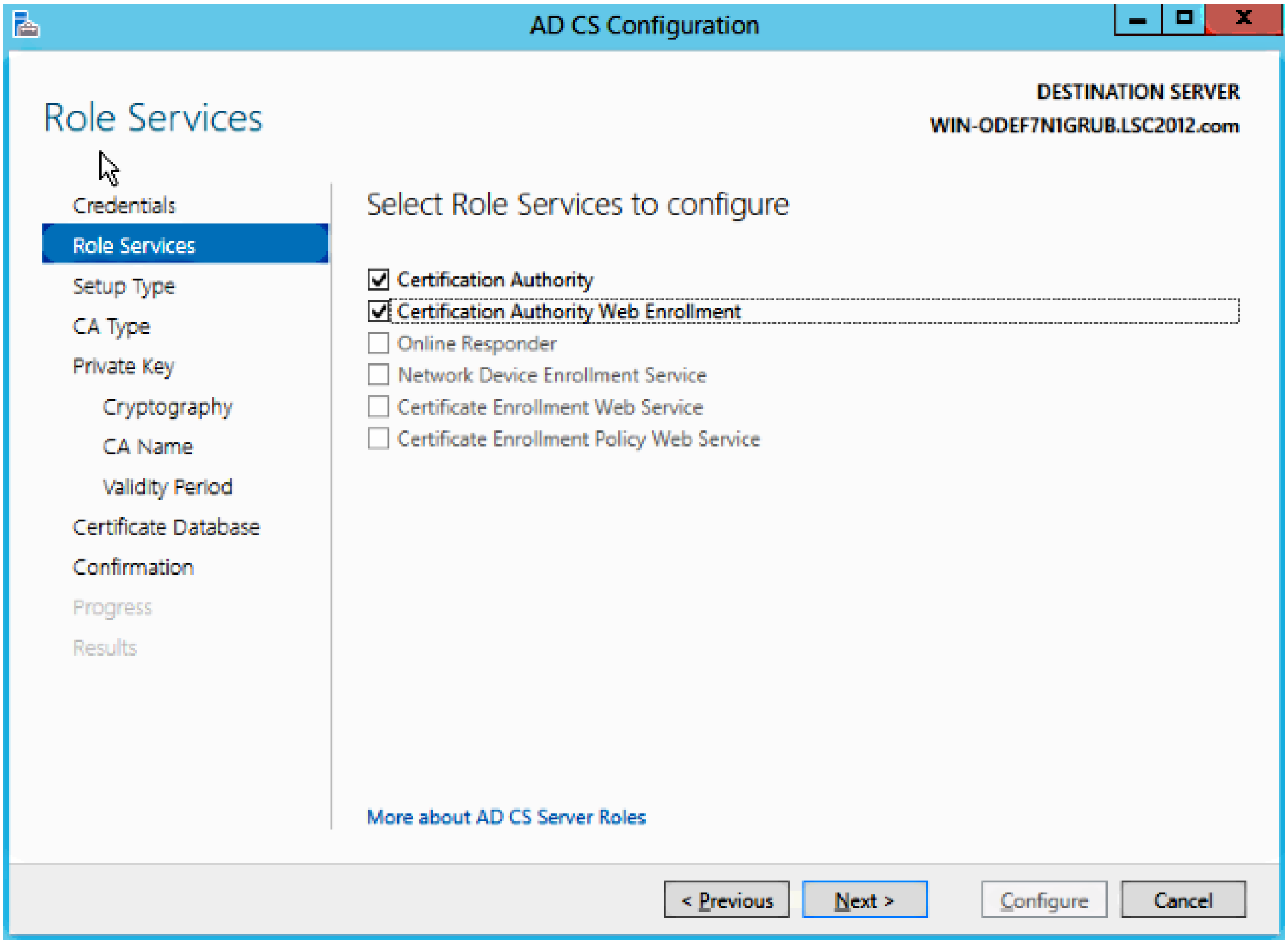
Configuration required. Installation succeeded on WIN-ODEF7N1GRUB.LSC2012.com.

Active Directory Certificate Services
Additional steps are required to configure Active Directory Certificate Services on the destination server
Configure Active Directory Certificate Services on the destination server
Certification Authority
Certification Authority Web Enrollment
Remote Server Administration Tools
Role Administration Tools
Active Directory Certificate Services Tools
Certification Authority Management Tools
Web Server (IIS)

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

Step 6. Choose Enterprise CA and leave everything as default.



Role Services

DESTINATION SERVER
WIN-ODEF7N1GRUB.LSC2012.com

Select Role Services to configure

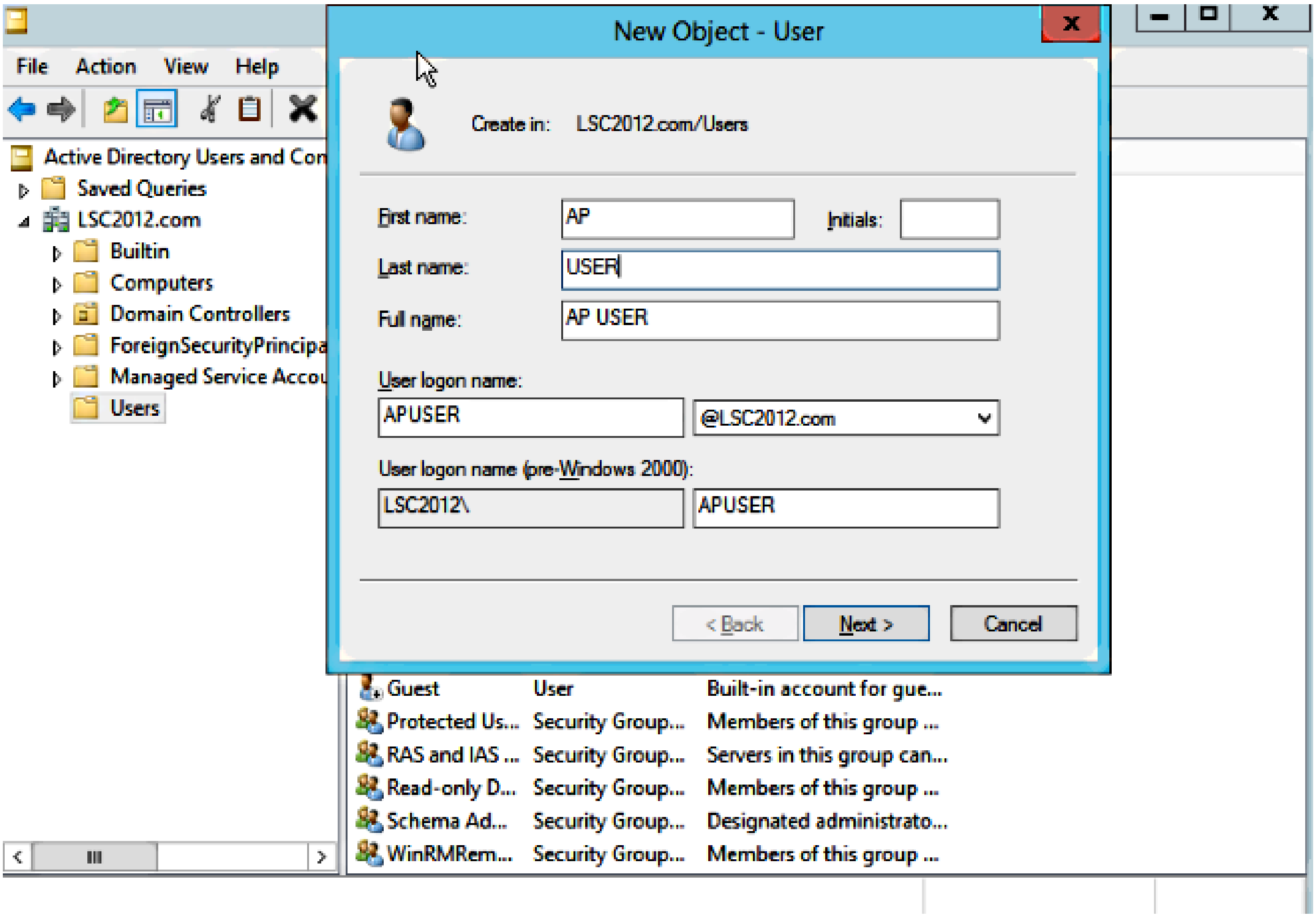
☑ Certification Authority
☑ Certification Authority Web Enrollment
□ Online Responder
□ Network Device Enrollment Service
□ Certificate Enrollment Web Service
□ Certificate Enrollment Policy Web Service

Step 7. Click the **Microsoft Windows/Start menu**.

Step 8. Click **Administrative tools**.

Step 9. Click **Active Directory Users and Computers**.

Step 10. Expand the domain, right-click the **Users folder**, and choose **New Object > User**.



Create in: LSC2012.com/Users

First name: AP

Initials:

Last name: USER

Full name: AP USER

User logon name: APUSER @LSC2012.com

User logon name (pre-Windows 2000): LSC2012\ APUSER

Guest	User	Built-in account for gue...
Protected Us...	Security Group...	Members of this group ...
RAS and IAS ...	Security Group...	Servers in this group can...
Read-only D...	Security Group...	Members of this group ...
Schema Ad...	Security Group...	Designated administrato...
WinRMRem...	Security Group...	Members of this group ...

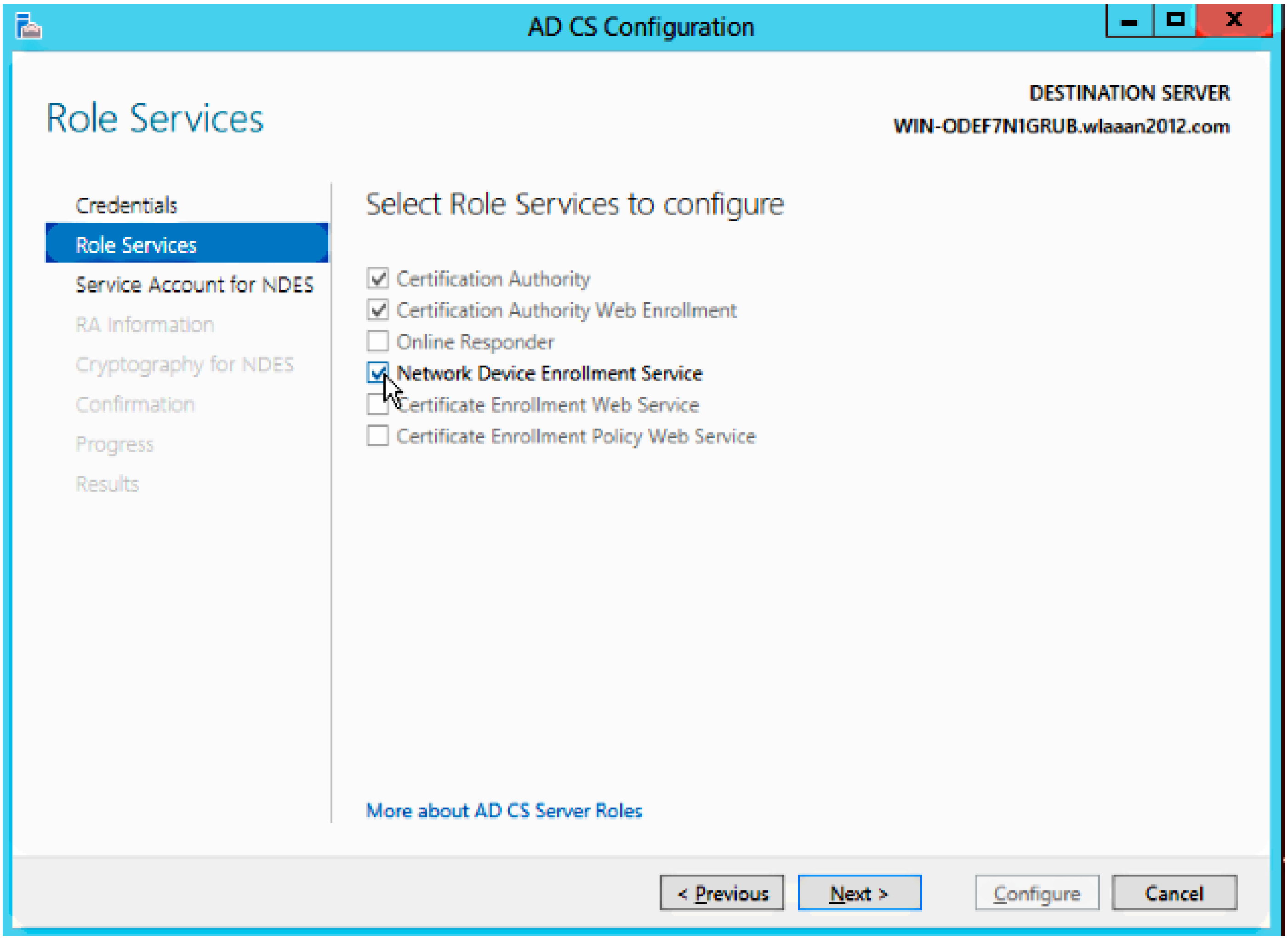
Step 11. In this example, it is named **APUSER**. Once created, you must edit the user and click the **MemberOf tab**, and make it a member of the IIS_IUSRS group

The required User Rights Assignments are:

- Allow log on locally

- Log on as a service

Step 12. Install the Network Device Enrollment Service (NDES).



Role Services

DESTINATION SERVER
WIN-ODEF7N1GRUB.wlaaan2012.com

Select Role Services to configure

☑ Certification Authority
☑ Certification Authority Web Enrollment
☐ Online Responder
☑ Network Device Enrollment Service
☐ Certificate Enrollment Web Service
☐ Certificate Enrollment Policy Web Service

- Choose the account member of the IIS_USRS group, **APUSER** in this example, as the service account for NDES.

Step 13. Navigate to Administrative Tools.

Step 14. Click **Internet Information Services (IIS)**.

Step 15. Expand the **Server > Sites > Default web site > Cert Srv**.

Step 16. For both **mscep** and **mscep_admin**, click **authentication**. Make sure that anonymous authentication is enabled.

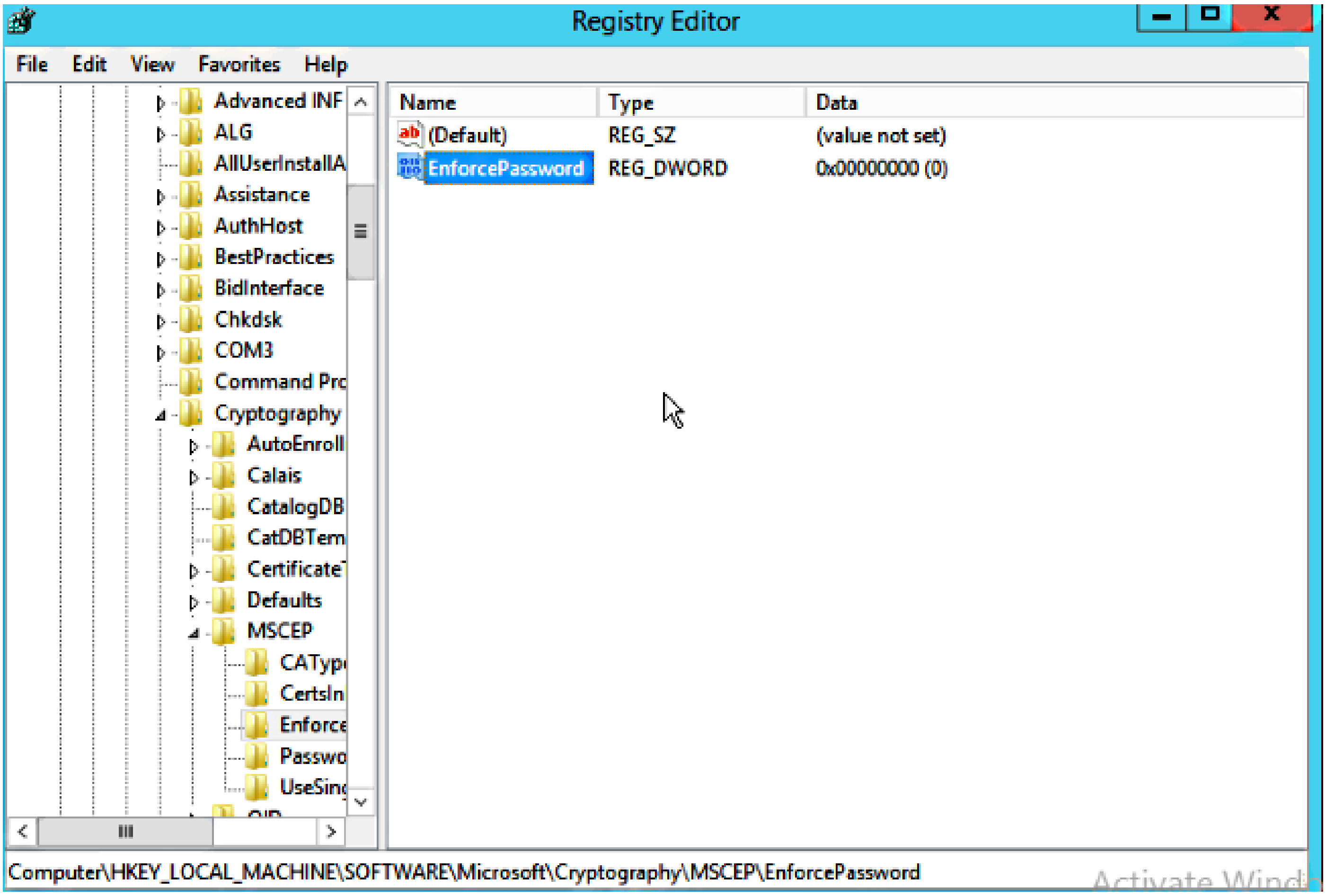
Step 17. Right-click **windows authentication** and choose **Providers**. Make sure that NT LAN Manager (NTLM) is first in the list.

Step 18. Disable the authentication challenge in the registry settings, otherwise Simple Certificate Enrollment Protocol (SCEP) expects challenge password authentication, which is not supported by the WLC.

Step 19. Open the **regedit application**.

Step 20. Go to **HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\Cryptography\MSCEP\**.

Step 21. Set EnforcePassword to **0**.



Name	Type	Data
(Default)	REG_SZ	(value not set)
EnforcePassword	REG_DWORD	0x00000000 (0)

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP\EnforcePassword

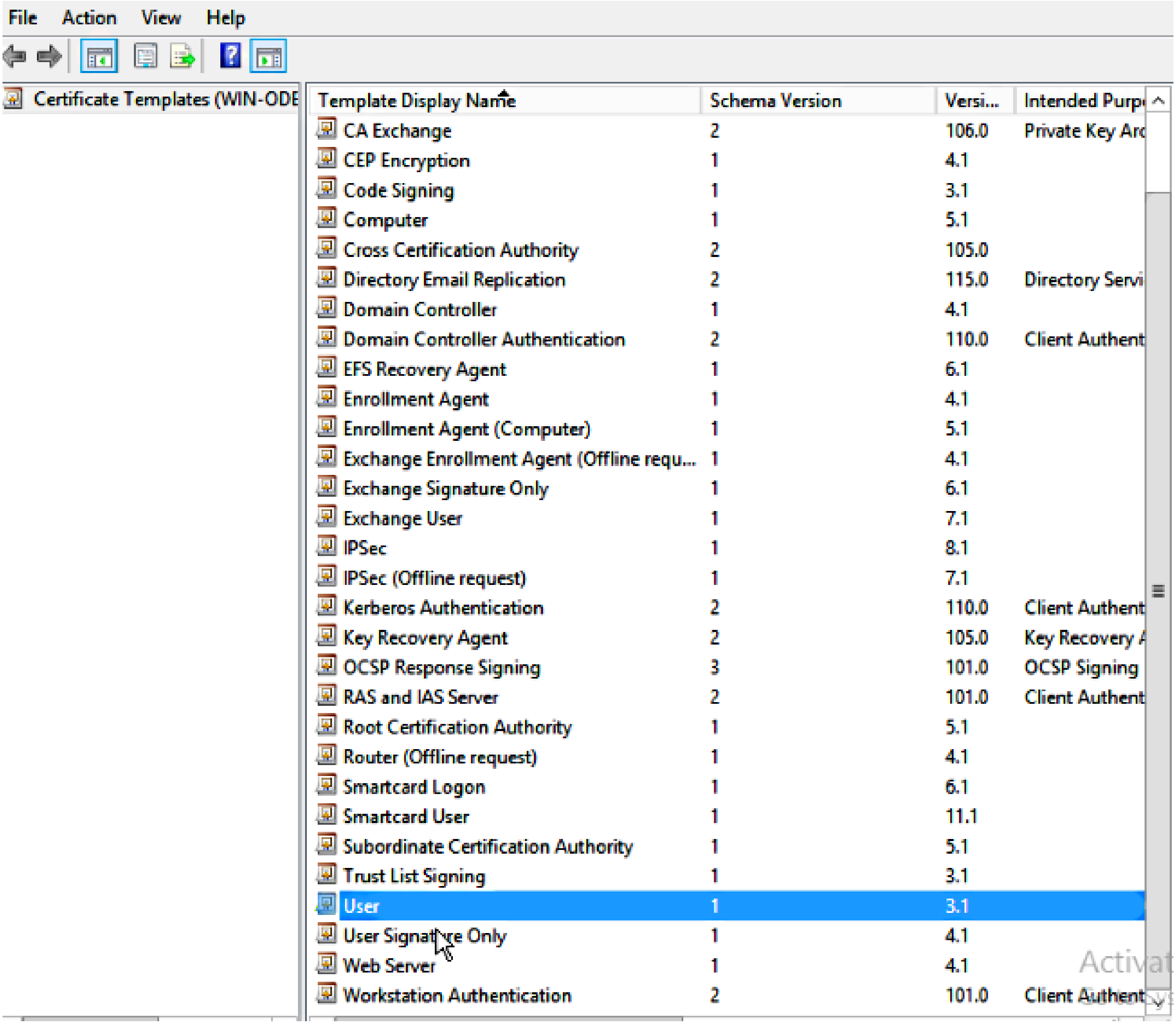
Step 22. Click the **Microsoft Windows/Start menu**.

Step 23. Type **MMC**.

Step 24. On the File menu, choose **Add/Remove Snap-in**. Choose **Certification Authority**.

Step 25. Right-click the **Certificate Template folder** and click **Manage**.

Step 26. Right-click an existing template, such as User, and choose **Duplicate Template**.

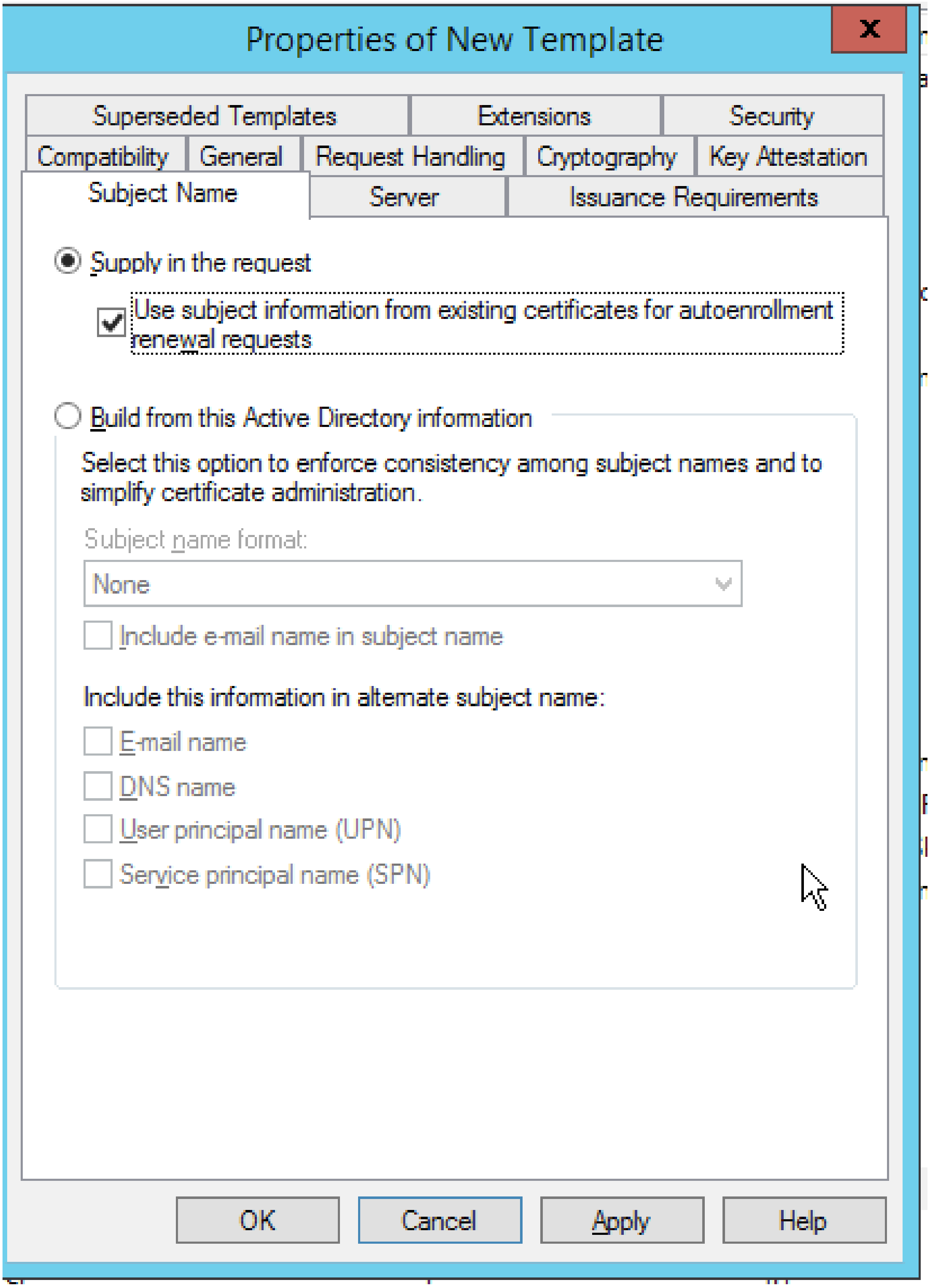


Template Display Name	Schema Version	Versi...	Intended Purp
CA Exchange	2	106.0	Private Key Arc
CEP Encryption	1	4.1	
Code Signing	1	3.1	
Computer	1	5.1	
Cross Certification Authority	2	105.0	
Directory Email Replication	2	115.0	Directory Servi
Domain Controller	1	4.1	
Domain Controller Authentication	2	110.0	Client Authent
EFS Recovery Agent	1	6.1	
Enrollment Agent	1	4.1	
Enrollment Agent (Computer)	1	5.1	
Exchange Enrollment Agent (Offline requ...	1	4.1	
Exchange Signature Only	1	6.1	
Exchange User	1	7.1	
IPSec	1	8.1	
IPSec (Offline request)	1	7.1	
Kerberos Authentication	2	110.0	Client Authent
Key Recovery Agent	2	105.0	Key Recovery A
OCSP Response Signing	3	101.0	OCSP Signing
RAS and IAS Server	2	101.0	Client Authent
Root Certification Authority	1	5.1	
Router (Offline request)	1	4.1	
Smartcard Logon	1	6.1	
Smartcard User	1	11.1	
Subordinate Certification Authority	1	5.1	
Trust List Signing	1	3.1	
User	1	3.1	
User Signature Only	1	4.1	
Web Server	1	4.1	
Workstation Authentication	2	101.0	Client Authent

Step 27. Choose the CA to be Microsoft Windows 2012 R2.

Step 28. On the General tab, add a display name such as WLC and a validity period.

Step 29. In the Subject Name tab, confirm that **Supply in the request** is selected.



Properties of New Template

● Supply in the request

☑ Use subject information from existing certificates for autoenrollment renewal requests

○ Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format:

None

□ Include e-mail name in subject name

Include this information in alternate subject name:

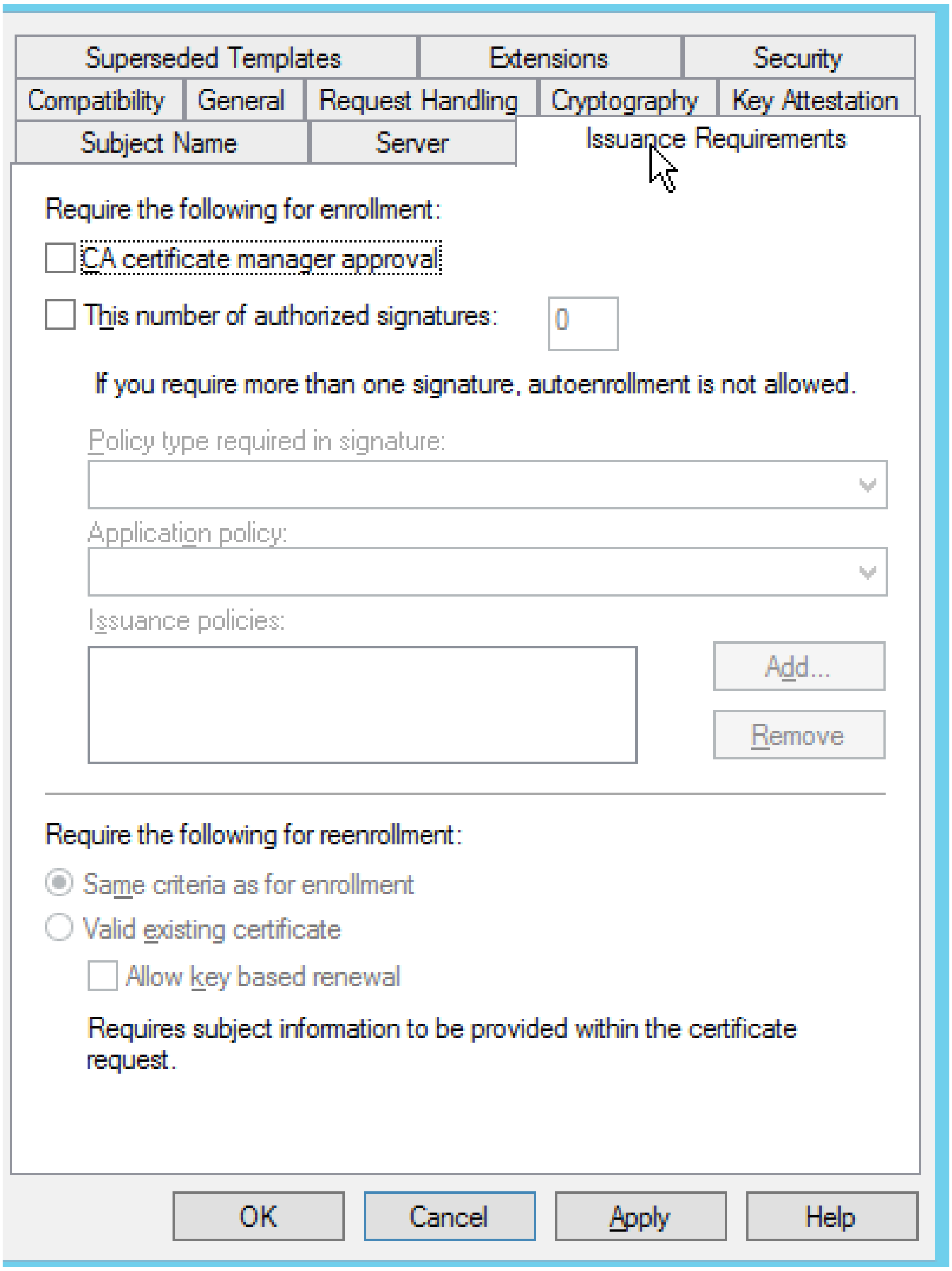
□ E-mail name

□ DNS name

□ User principal name (UPN)

□ Service principal name (SPN)

Step 30. Click the **Issuance Requirements** tab. Cisco recommends that you leave issuance policies blank in a typical hierarchical CA environment:



Require the following for enrollment:

□ CA certificate manager approval

□ This number of authorized signatures: 0

If you require more than one signature, autoenrollment is not allowed.

Policy type required in signature:

Application policy:

Issuance policies:

Require the following for reenrollment:

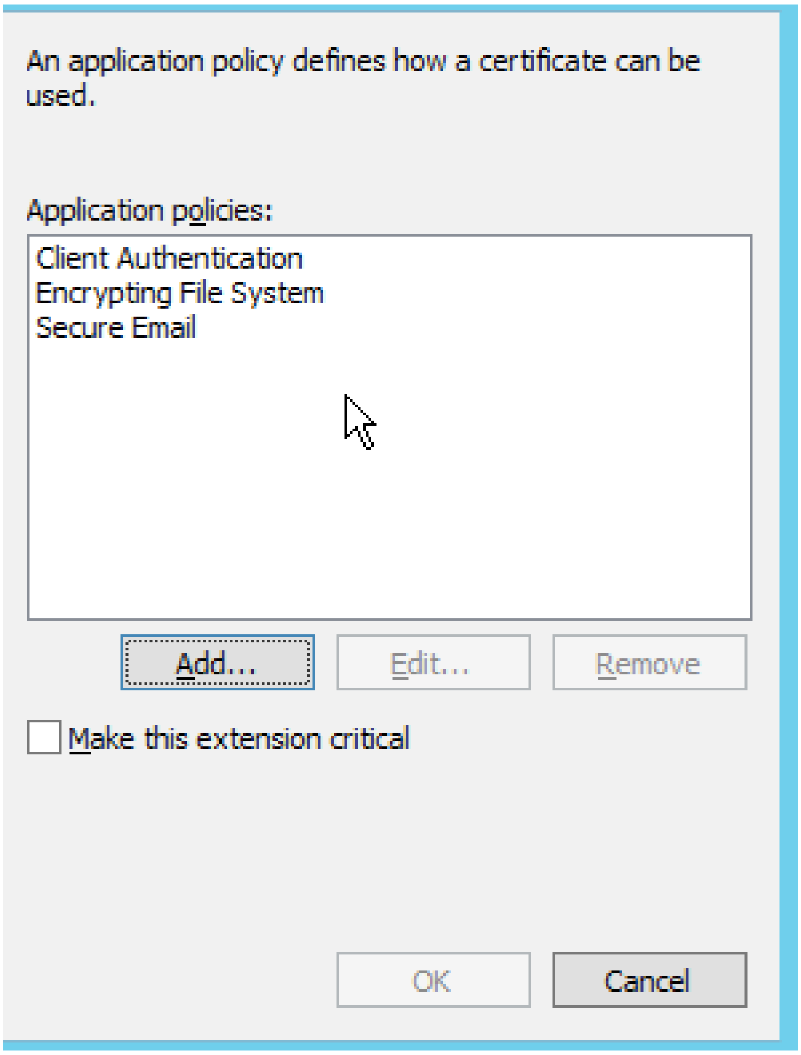
● Same criteria as for enrollment

○ Valid existing certificate

□ Allow key based renewal

Requires subject information to be provided within the certificate request.

Step 31. Click the **Extensions tab**, **Application Policies**, and then **Edit**. Click **Add**, and ensure that Client Authentication is added as an application policy. Click **OK**.



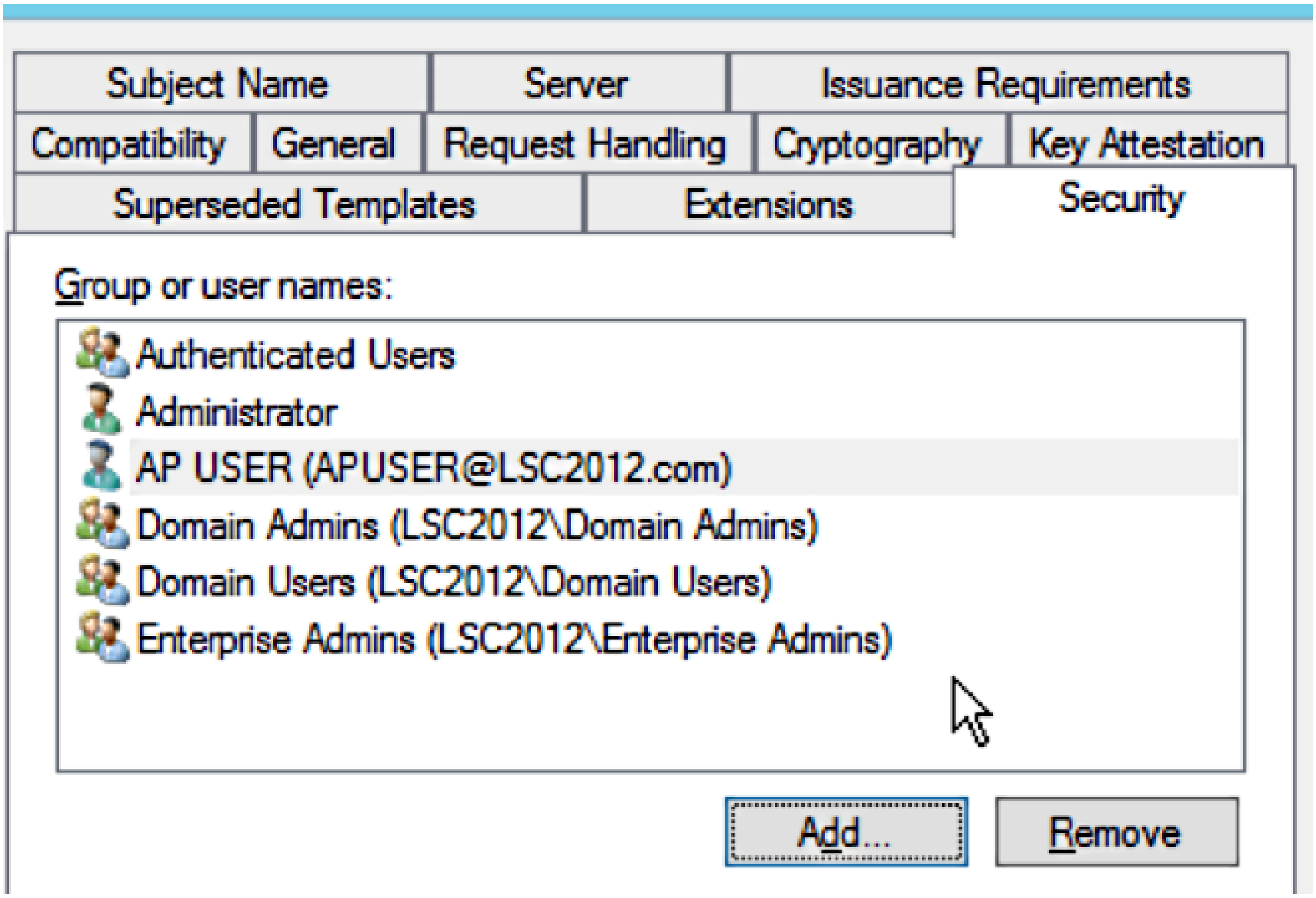
An application policy defines how a certificate can be used.

Application policies:

Client Authentication
Encrypting File System
Secure Email

□ Make this extension critical

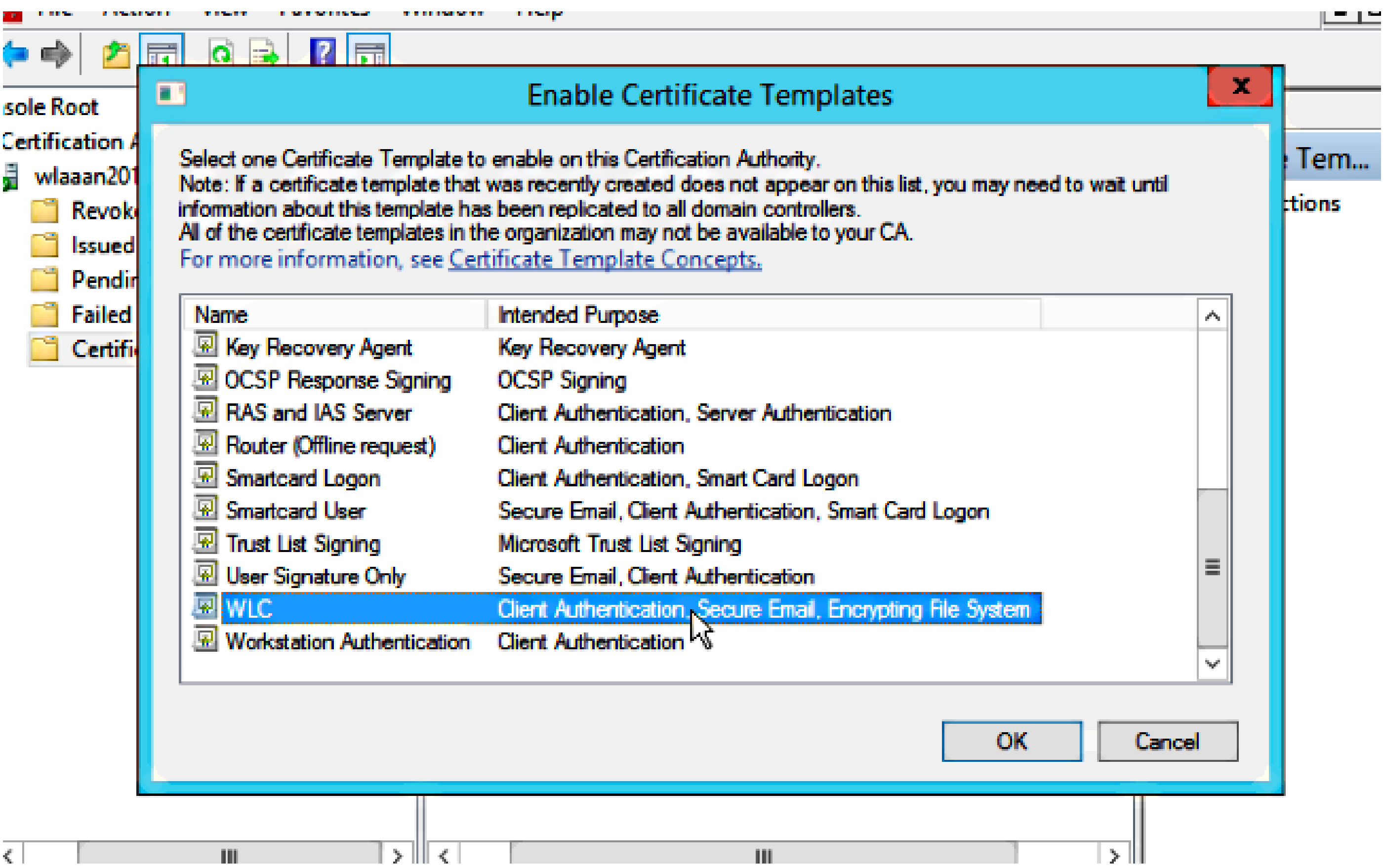
Step 32. Click the **Security tab**, and then click **Add...**. Ensure that the SCEP service account defined in the NDES service installation has full control of the template, and click **OK**.



Group or user names:

- Authenticated Users
- Administrator
- AP USER (APUSER@LSC2012.com)
- Domain Admins (LSC2012\Domain Admins)
- Domain Users (LSC2012\Domain Users)
- Enterprise Admins (LSC2012\Enterprise Admins)

Step 33. Return to the Certification Authority GUI interface. Right-click the **Certificate Templates directory**. Navigate to **New > Certificate Template to Issue**. Select the WLC template configured previously, and click **OK.**

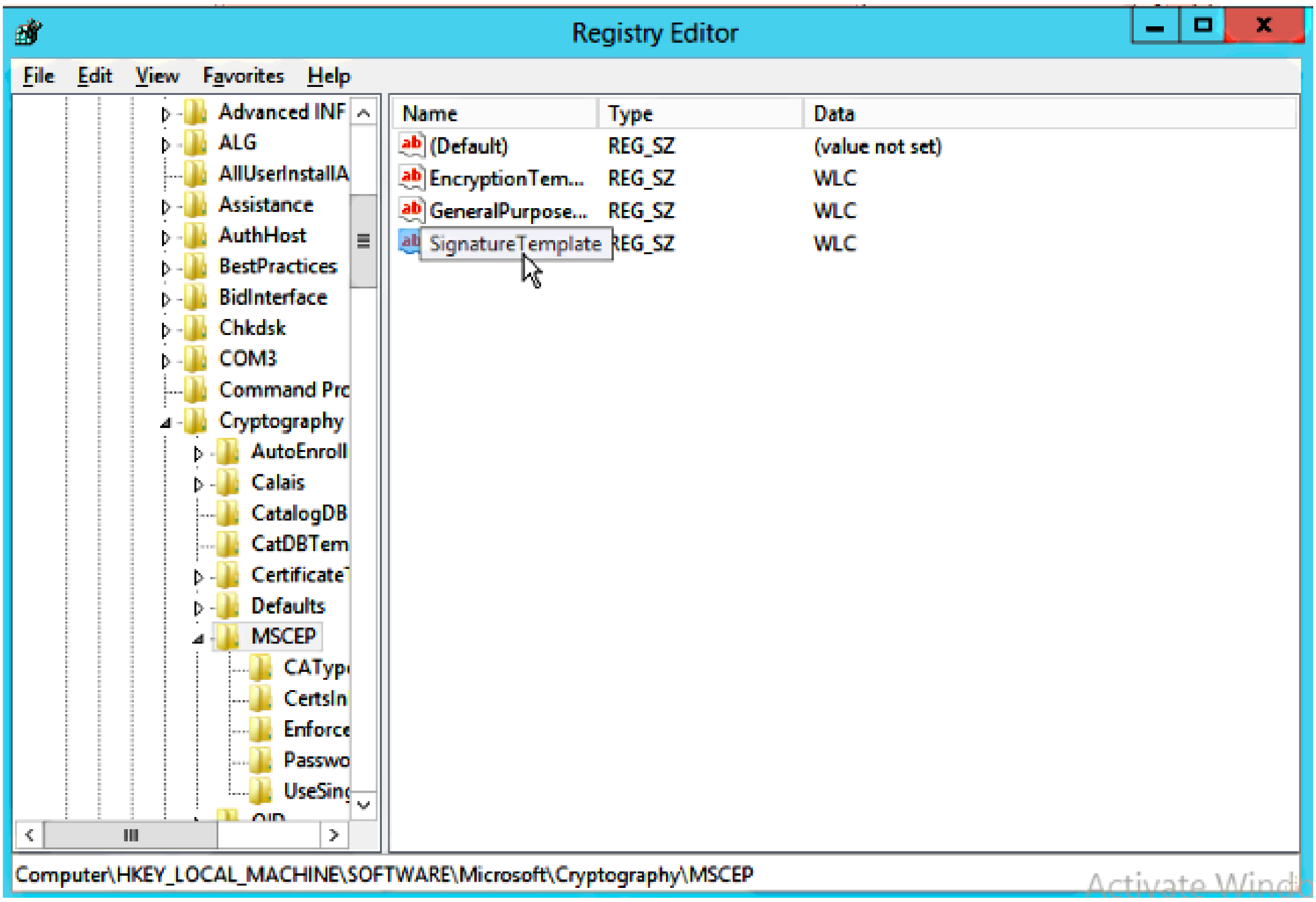


Enable Certificate Templates

Select one Certificate Template to enable on this Certification Authority.
Note: If a certificate template that was recently created does not appear on this list, you may need to wait until information about this template has been replicated to all domain controllers.
All of the certificate templates in the organization may not be available to your CA.
For more information, see Certificate Template Concepts.

Name	Intended Purpose
Key Recovery Agent	Key Recovery Agent
OCSP Response Signing	OCSP Signing
RAS and IAS Server	Client Authentication, Server Authentication
Router (Offline request)	Client Authentication
Smartcard Logon	Client Authentication, Smart Card Logon
Smartcard User	Secure Email, Client Authentication, Smart Card Logon
Trust List Signing	Microsoft Trust List Signing
User Signature Only	Secure Email, Client Authentication
WLC	Client Authentication, Secure Email, Encrypting File System
Workstation Authentication	Client Authentication

Step 34. Change the default SCEP template in the registry settings under **Computer > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptography > MSCEP**. Change the EncryptionTemplate, GeneralPurposeTemplate, and SignatureTemplate keys from IPsec (Offline Request) to the WLC template previously created.



Name	Type	Data
(Default)	REG_SZ	(value not set)
EncryptionTem...	REG_SZ	WLC
GeneralPurpose...	REG_SZ	WLC
SignatureTemplate	REG_SZ	WLC

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP

Step 35. Reboot the system.

Configure the WLC

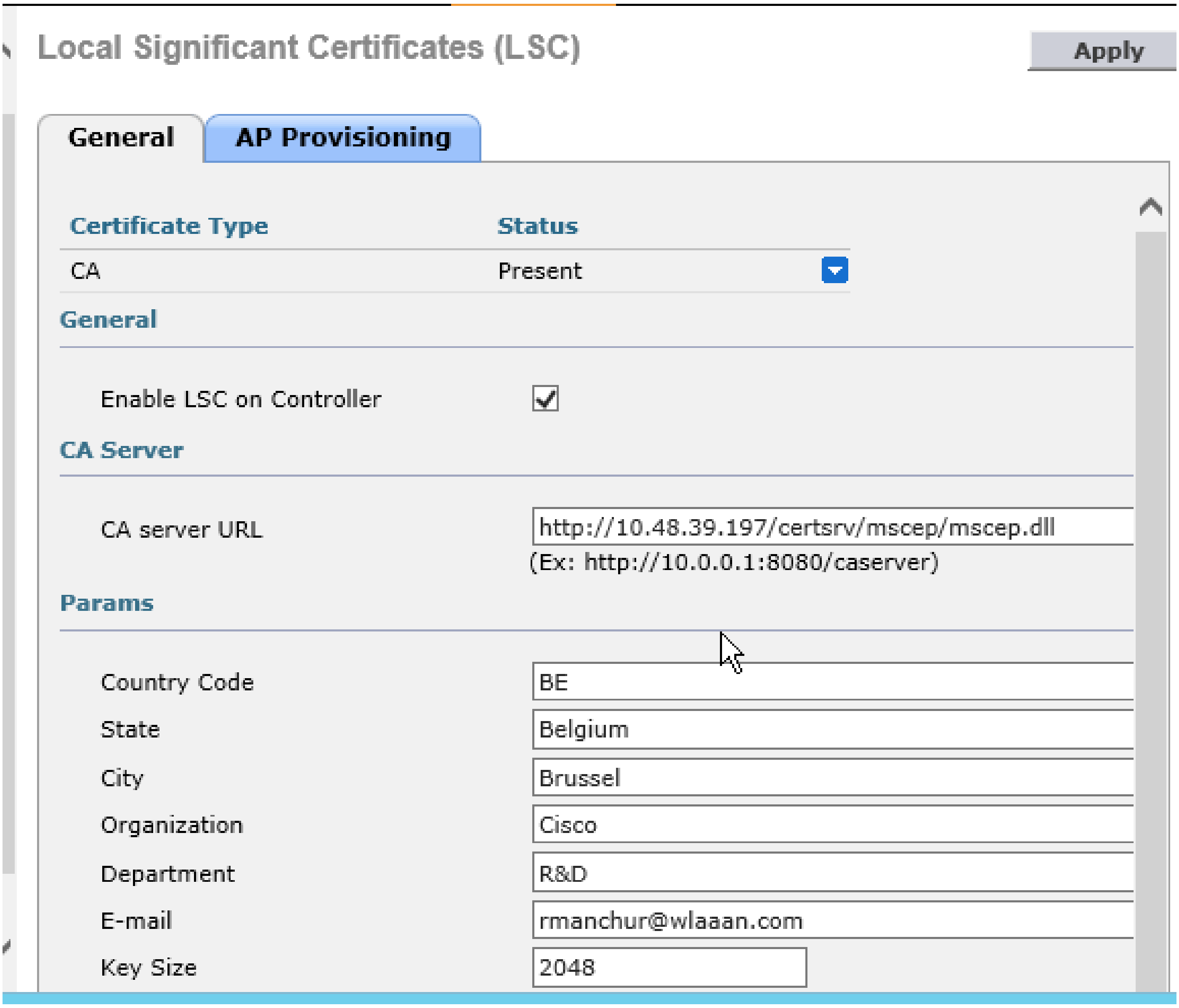
Step 1. On the WLC, navigate to the Security menu. Click **Certificates > LSC**.

Step 2. Check the **Enable LSC on Controller** checkbox.

Step 3. Enter your Microsoft Windows Server 2012 URL. By default, it is appended with **/certsrv/mscep/mscep.dll**.

Step 4. Enter your details in the **Params** section.

Step 5. Apply the change.



Local Significant Certificates (LSC)

Certificate Type	Status
CA	Present

General

Enable LSC on Controller ☑

CA Server

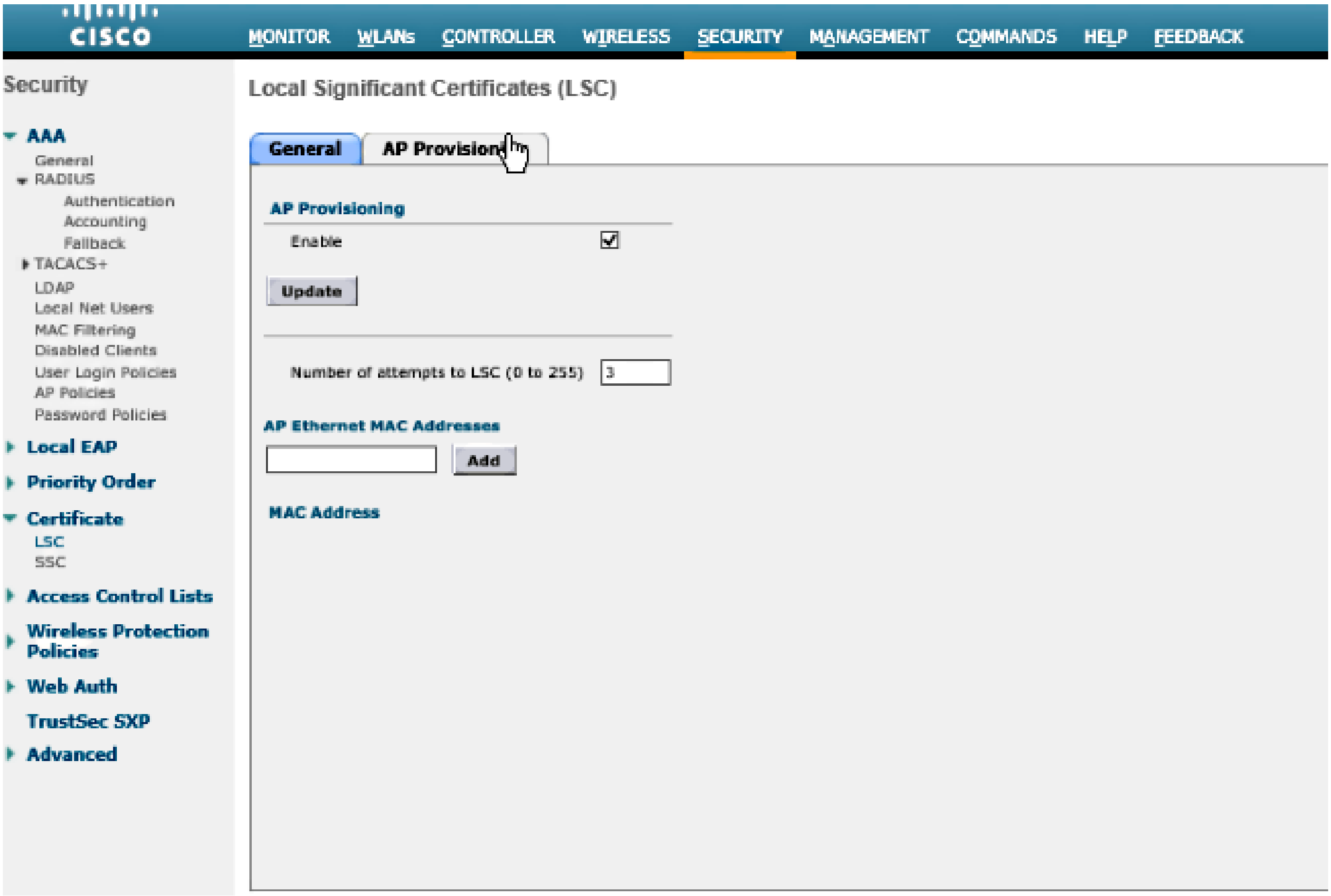
CA server URL: http://10.48.39.197/certsrv/mscep/mscep.dll
(Ex: http://10.0.0.1:8080/caserver)

Params

Country Code	BE
State	Belgium
City	Brussel
Organization	Cisco
Department	R&D
E-mail	rmanchur@wlaaan.com
Key Size	2048

Step 6. Click the blue arrow on the upper CA line and choose **Add**. It should change the status from **Not present** to **present**.

Step 7. Click the **AP provisioning tab**.



Local Significant Certificates (LSC)

AP Provisioning

Enable ☑

Number of attempts to LSC (0 to 255) 3

AP Ethernet MAC Addresses

MAC Address

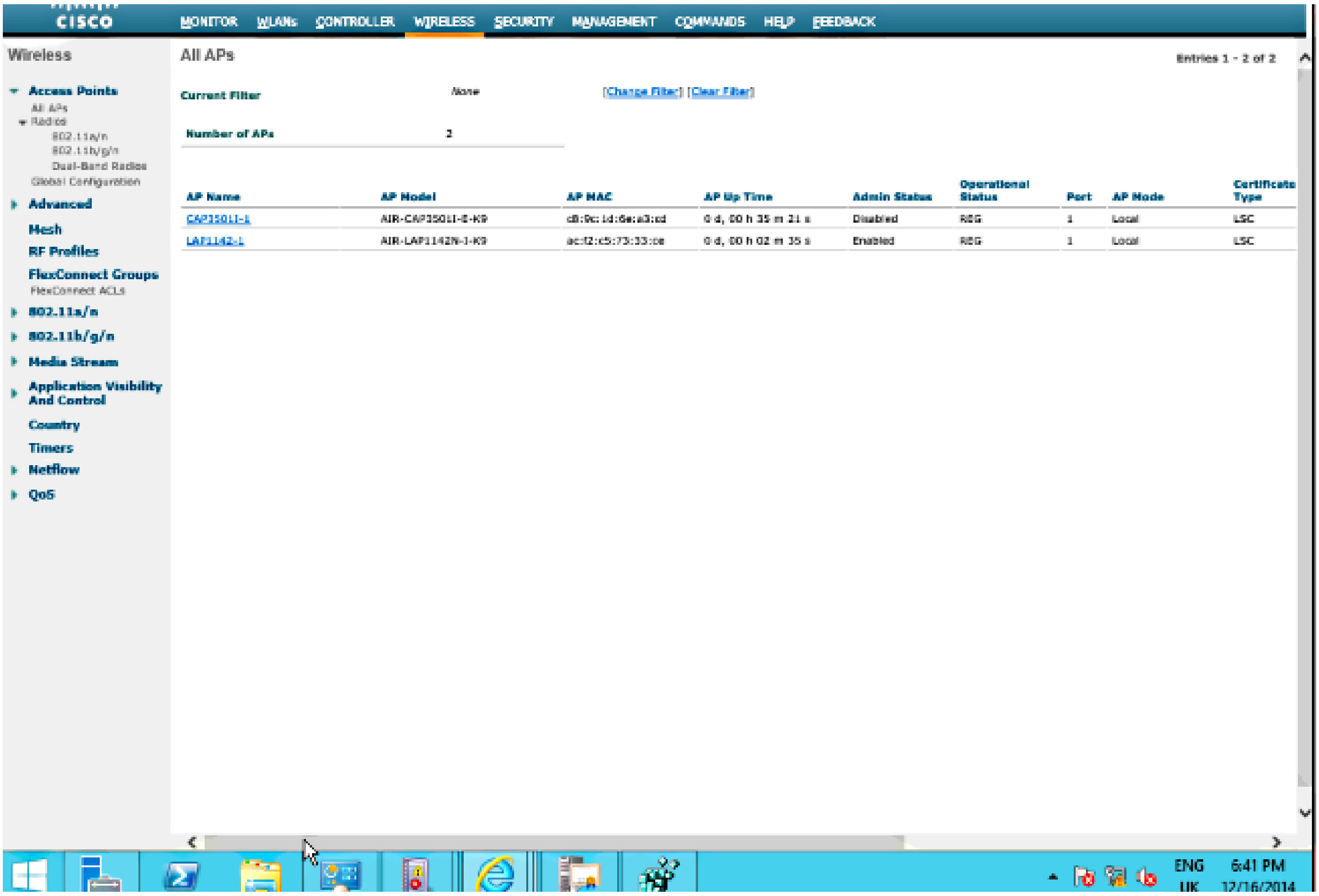
Step 8. Check the **Enable** checkbox under AP Provisioning and click **Update**.

Step 9. Reboot your access points if they have not rebooted themselves.

Verify

Use this section in order to confirm that your configuration works properly.

The access point, after reboot, joins back and displays with LSC as the certificate type in the Wireless menu.



All APs

Entries 1 - 2 of 2

Current Filter None [Change Filter] [Clear Filter]

Number of APs 2

AP Name	AP Model	AP MAC	AP Up Time	Admin Status	Operational Status	Port	AP Mode	Certificate Type
CAP3501I-1	AIR-CAP3501I-E-K9	c8:9c:1d:6e:a3:cd	0 d, 00 h 35 m 21 s	Disabled	REG	1	Local	LSC
LAP1142-1	AIR-LAP1142N-I-K9	ac:f2:c5:73:33:ce	0 d, 00 h 02 m 35 s	Enabled	REG	1	Local	LSC

Note: After 8.3.112, MIC APs cannot join at all once LSC is enabled. Therefore the "attempts to LSC" count feature becomes of limited use.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.