

WLC および Windows サーバ 2012 でのローカルで有効な証明書 (LSC) の設定例

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[Microsoft Windows Server の設定](#)

[WLC の設定](#)

[確認](#)

[トラブルシューティング](#)

概要

このドキュメントでは、ワイヤレスLANコントローラ(WLC)と新しくインストールされた Microsoft Windows Server 2012 R2を使用して、ローカルで有効な証明書(LSC)を設定する方法について説明します。

注：実際の導入は多くの点で異なる場合があります。Microsoft Windows Server 2012の設定を完全に制御し、知識を持っている必要があります。この設定例は、シスコのお客様がLSCを機能させるためにMicrosoft Windows Serverの設定を実装および適応するための参照テンプレートとしてのみ提供されています。

前提条件

要件

Microsoft Windows Serverで行われたすべての変更を理解し、必要に応じて関連するMicrosoftのドキュメントを確認することをお勧めします。

注：コントローラが中間CAを取得するだけなので、WLC上のLSCは中間CAではサポートされません。これは、ルートCAがWLCから欠落するためです。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- WLC バージョン 7.6
- Microsoft Windows Server 2012 R2

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

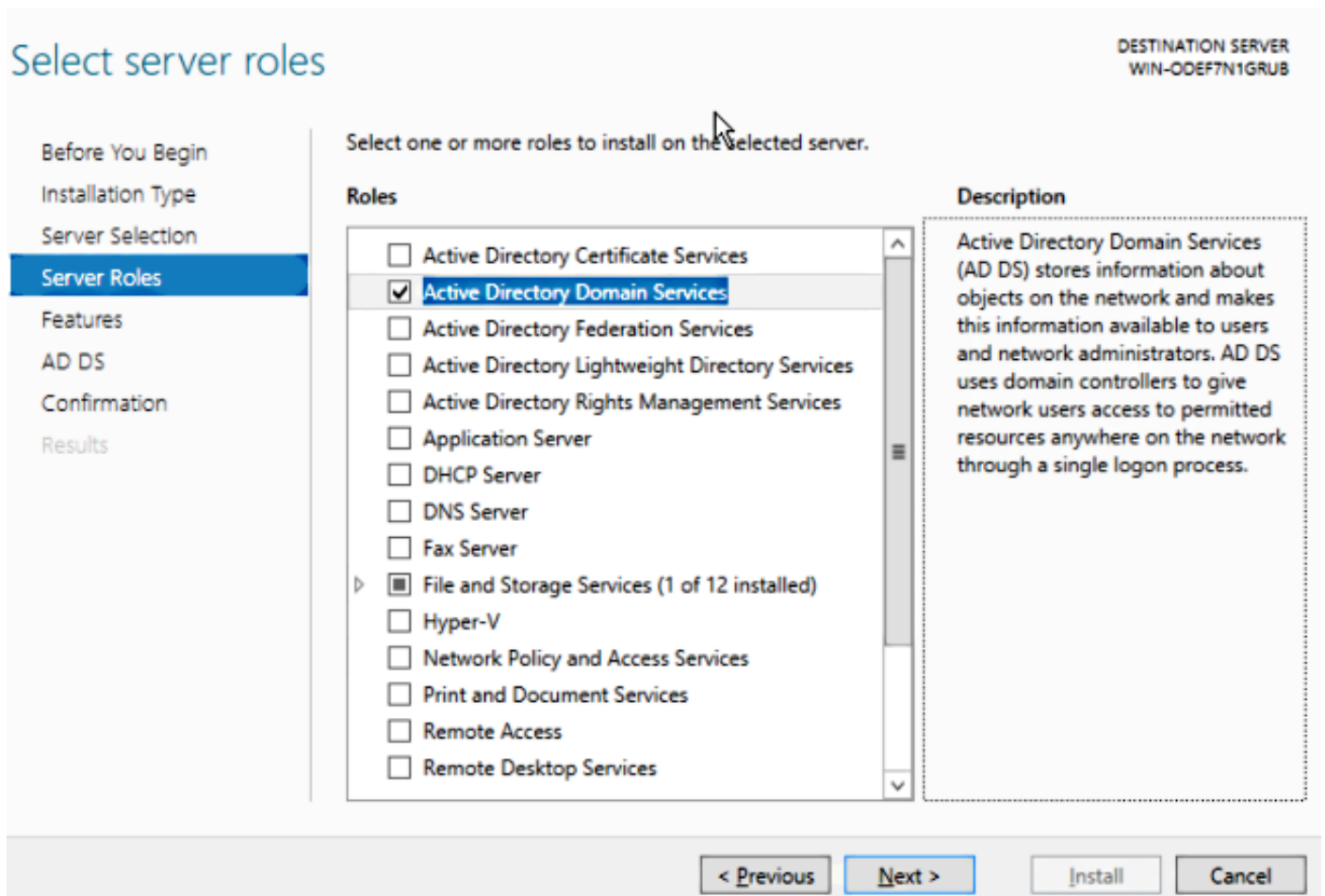
キュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

設定

Microsoft Windows Serverの設定

この設定は、新しくインストールされたMicrosoft Windows Server 2012で実行されたとおりに表示されます。手順をドメインと設定に合わせる必要があります。

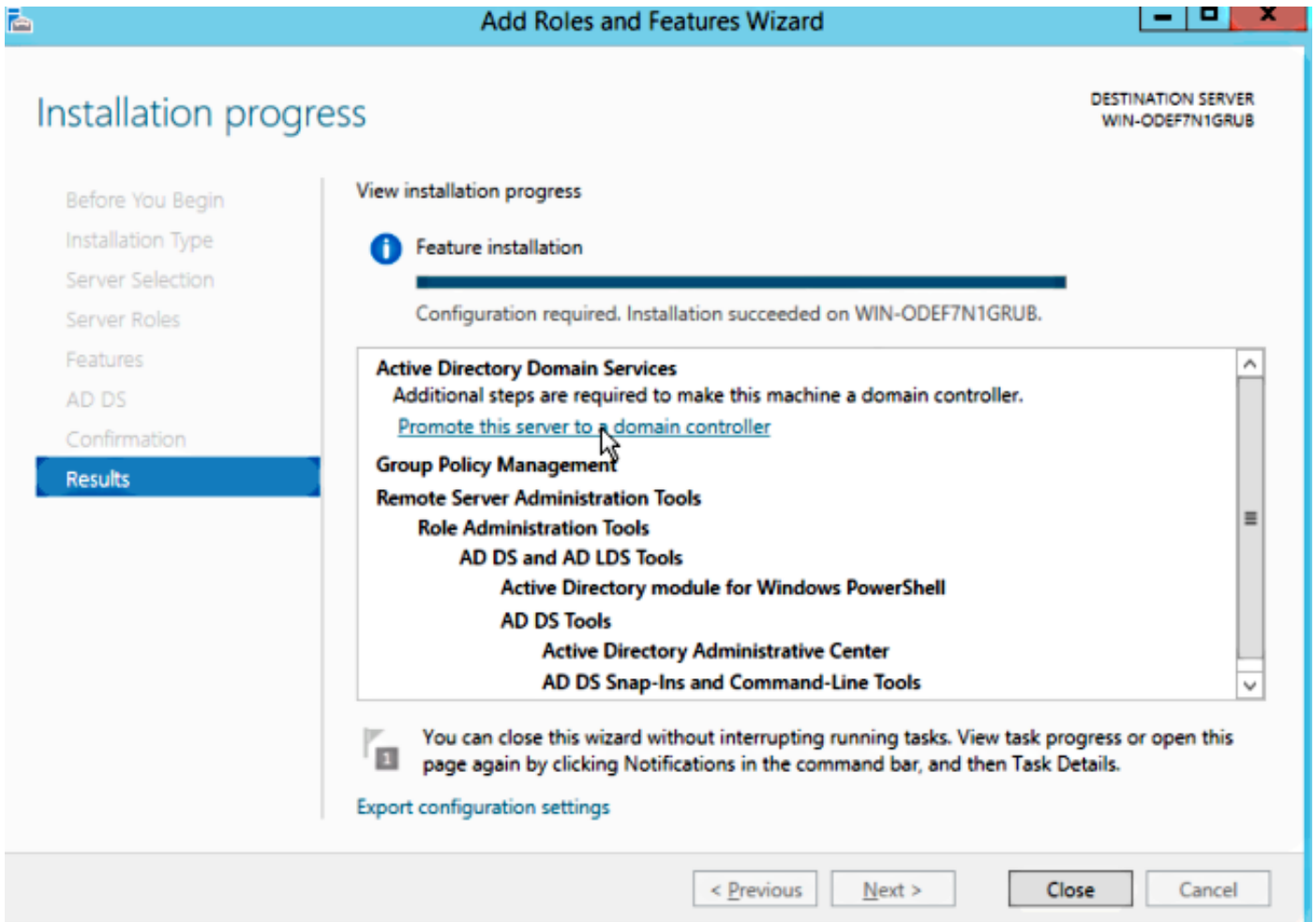
ステップ1:役割と機能ウィザードのActive Directoryドメインサービスをインストールします。



The screenshot shows the 'Select server roles' wizard. The title bar indicates 'DESTINATION SERVER WIN-0DEF7N1GRUB'. The left sidebar shows the navigation steps: 'Before You Begin', 'Installation Type', 'Server Selection', 'Server Roles' (highlighted), 'Features', 'AD DS', 'Confirmation', and 'Results'. The main area is titled 'Select one or more roles to install on the selected server.' and contains a list of roles. The 'Active Directory Domain Services' role is selected with a checkmark. The description for this role is displayed in a box on the right: '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.' At the bottom, there are buttons for '< Previous', 'Next >', 'Install', and 'Cancel'.

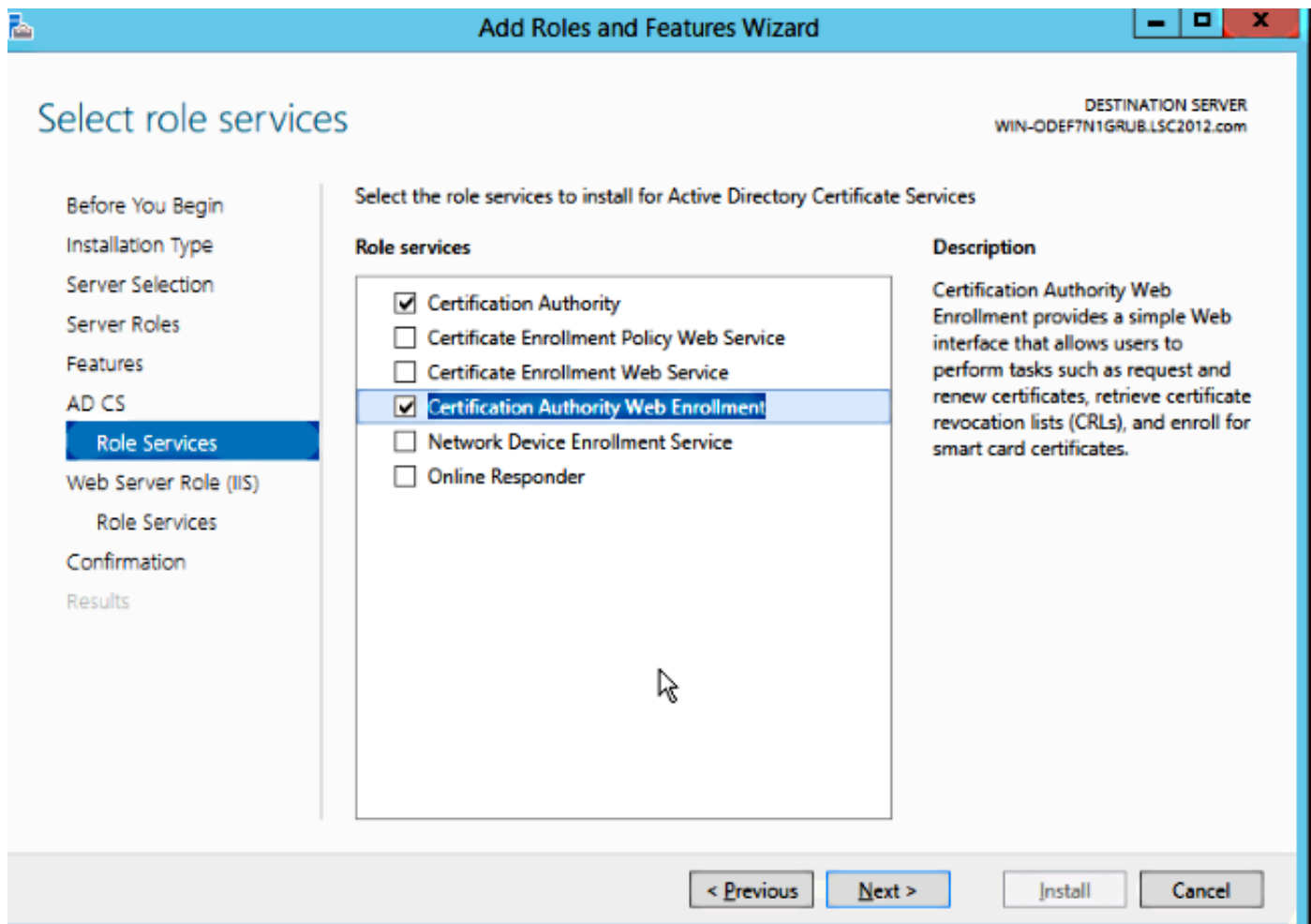
Roles	Description
<input type="checkbox"/> Active Directory Certificate Services	
<input checked="" type="checkbox"/> Active Directory Domain Services	Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.
<input type="checkbox"/> Active Directory Federation Services	
<input type="checkbox"/> Active Directory Lightweight Directory Services	
<input type="checkbox"/> Active Directory Rights Management Services	
<input type="checkbox"/> Application Server	
<input type="checkbox"/> DHCP Server	
<input type="checkbox"/> DNS Server	
<input type="checkbox"/> Fax Server	
<input type="checkbox"/> File and Storage Services (1 of 12 installed)	
<input type="checkbox"/> Hyper-V	
<input type="checkbox"/> Network Policy and Access Services	
<input type="checkbox"/> Print and Document Services	
<input type="checkbox"/> Remote Access	
<input type="checkbox"/> Remote Desktop Services	

ステップ2:インストール後、サーバをドメインコントローラに昇格する必要があります。

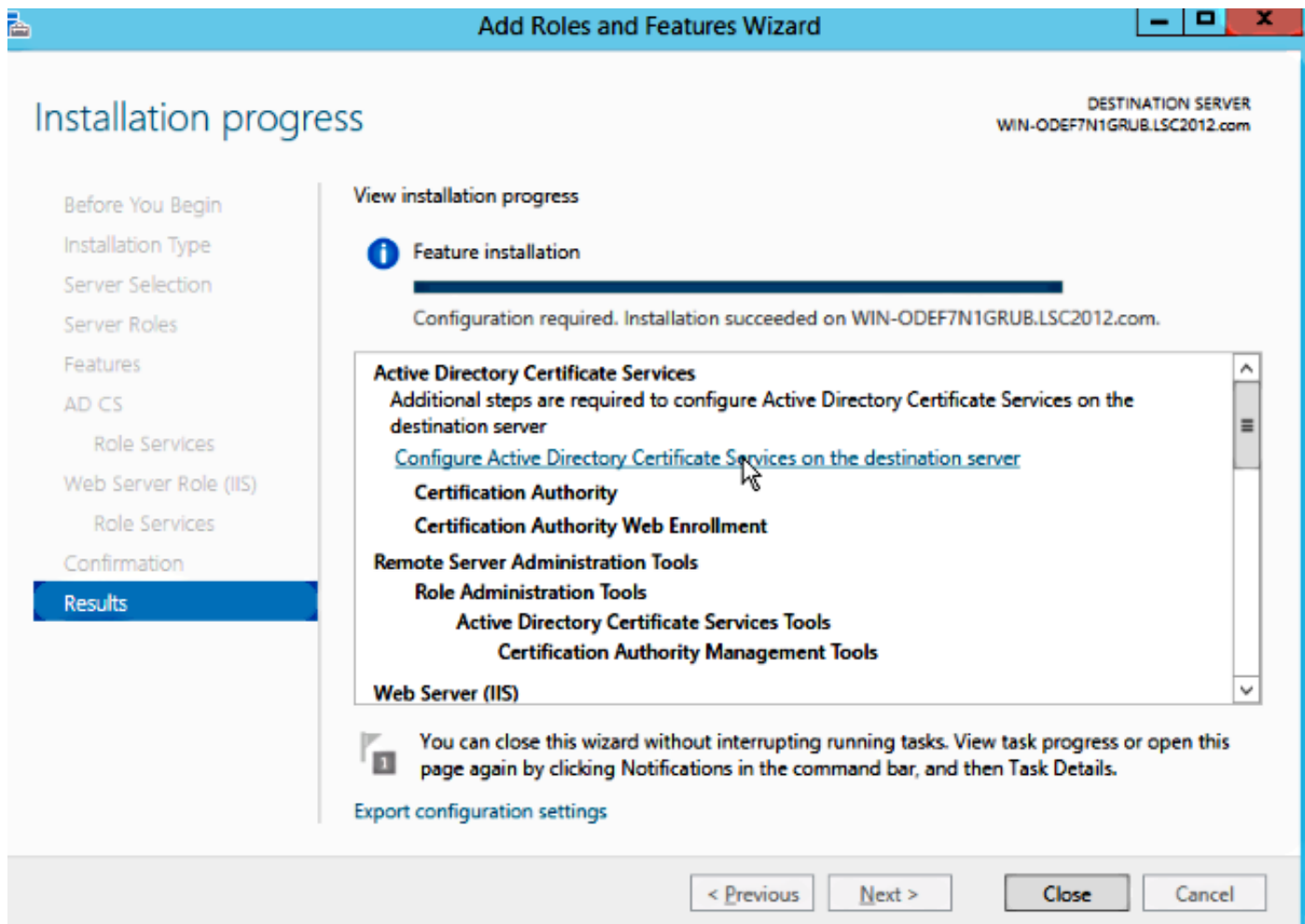


ステップ3:これは新しい設定であるため、新しいフォレストを設定します。ただし、通常は既存の展開では、ドメインコントローラ上でこれらのポイントを設定するだけです。ここでは、LSC2012.comドメインを選択します。これにより、ドメインネームサーバ(DNS)機能もアクティブになります。

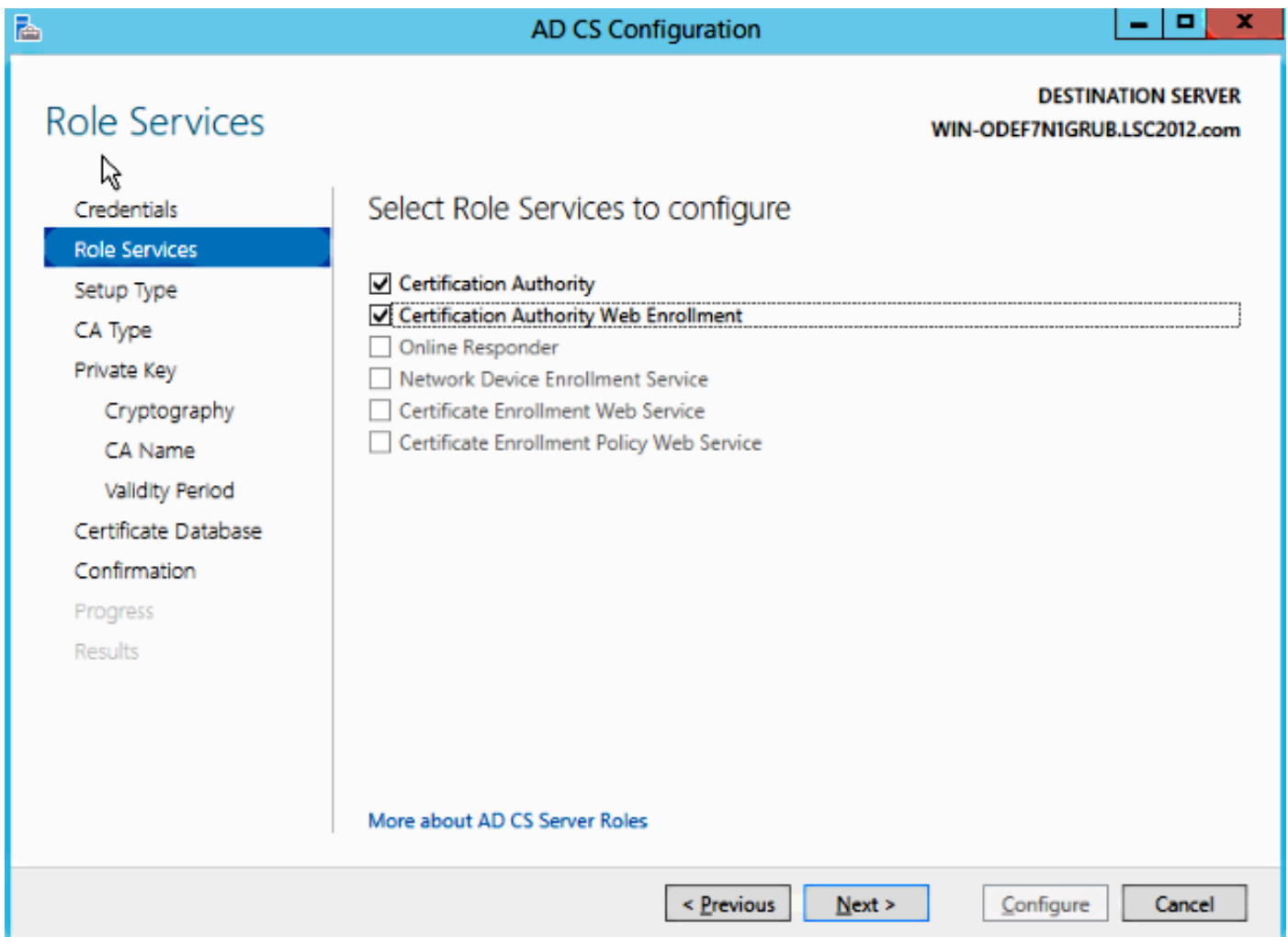
ステップ4:リポート後、認証局(CA)サービスとWeb登録をインストールします。



ステップ5:設定します。



ステップ6:[エンタープライズCA]を選択し、すべてデフォルトのままにします。

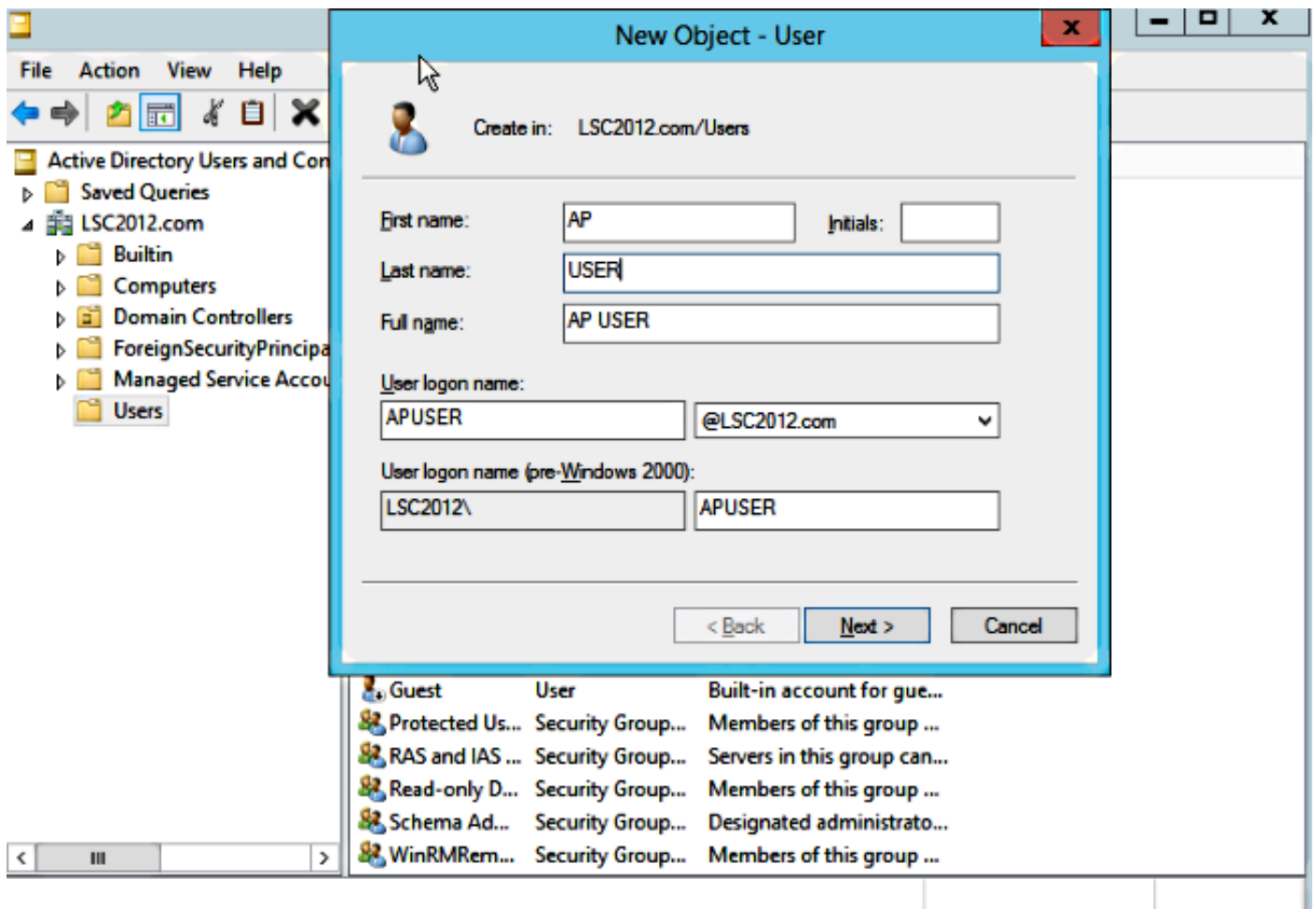


ステップ7:Microsoft Windows/スタートメニューをクリックします。

ステップ8:[管理ツール]をクリックします。

ステップ9:[Active Directory Users and Computers]をクリックします。

ステップ10 : ドメインを展開し、[Users]フォルダを右クリックして、[New Object] > [User]を選択します。

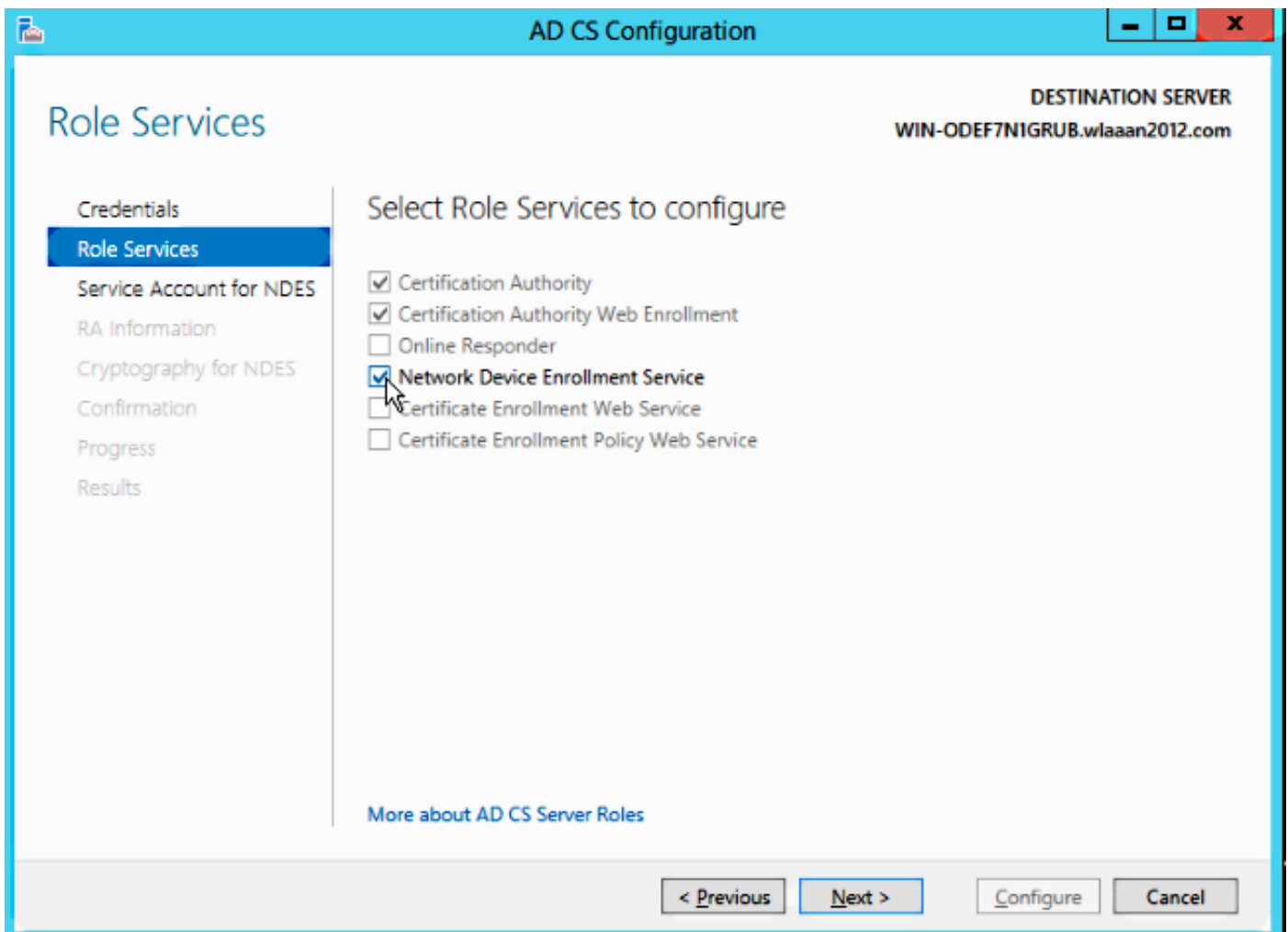


ステップ11:この例では、APUSERという名前です。作成したら、ユーザを編集し、[MemberOf]タブをクリックして、IIS_IUSRSグループのメンバにする必要があります

必要なユーザ権限の割り当ては次のとおりです。

- ローカルでログオンを許可
- サービスとしてログオン

ステップ12 : ネットワークデバイス登録サービス(NDES)をインストールします。



- IIS_USRSグループのアカウントメンバー(この例ではAPUSER)をNDESのサービスアカウントとして選択します。

ステップ13:[管理ツール]に移動します。

ステップ14:[インターネットインフォメーションサービス(IIS)]をクリックします。

ステップ15:[Server] > [Sites] > [Default web site] > [Cert Srv]の順に展開します。

ステップ16:mscepとmscep_adminの両方の場合は、[authentication]をクリックします。匿名認証が有効になっていることを確認します。

ステップ17:Windows認証を右クリックし、[Providers]を選択します。NT LAN Manager(NTLM)がリストの最初にあることを確認します。

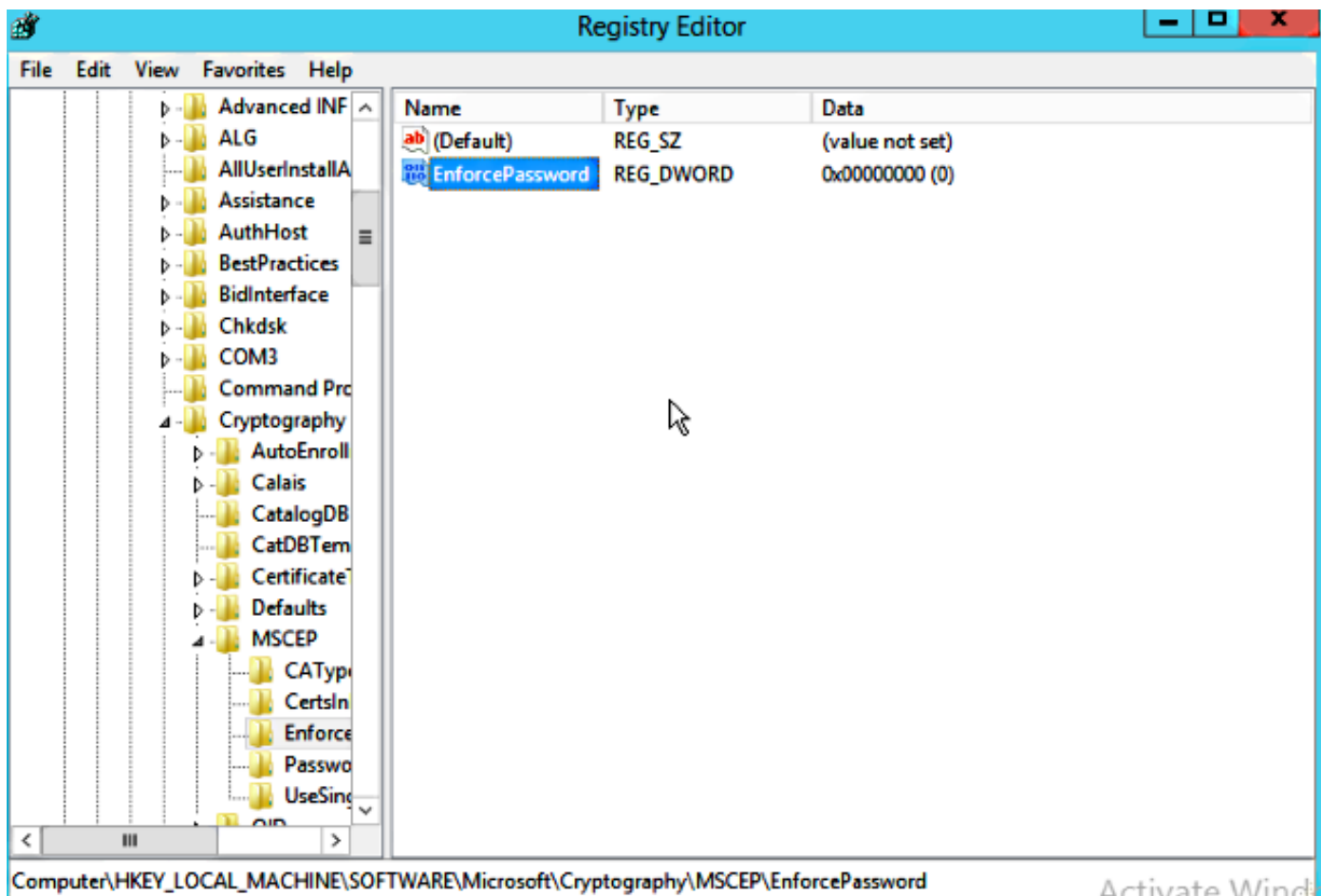
ステップ18 : レジストリ設定で認証チャレンジを無効にする。そうしないと、Simple Certificate Enrollment Protocol(SCEP)でチャレンジパスワード認証が必要になり、WLCではサポートされま

せん。

ステップ19:regeditアプリケーションを開きます。

ステップ20:HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\Cryptography\MSCEP\に移動します。

ステップ21: EnforcePasswordを0に設定します。



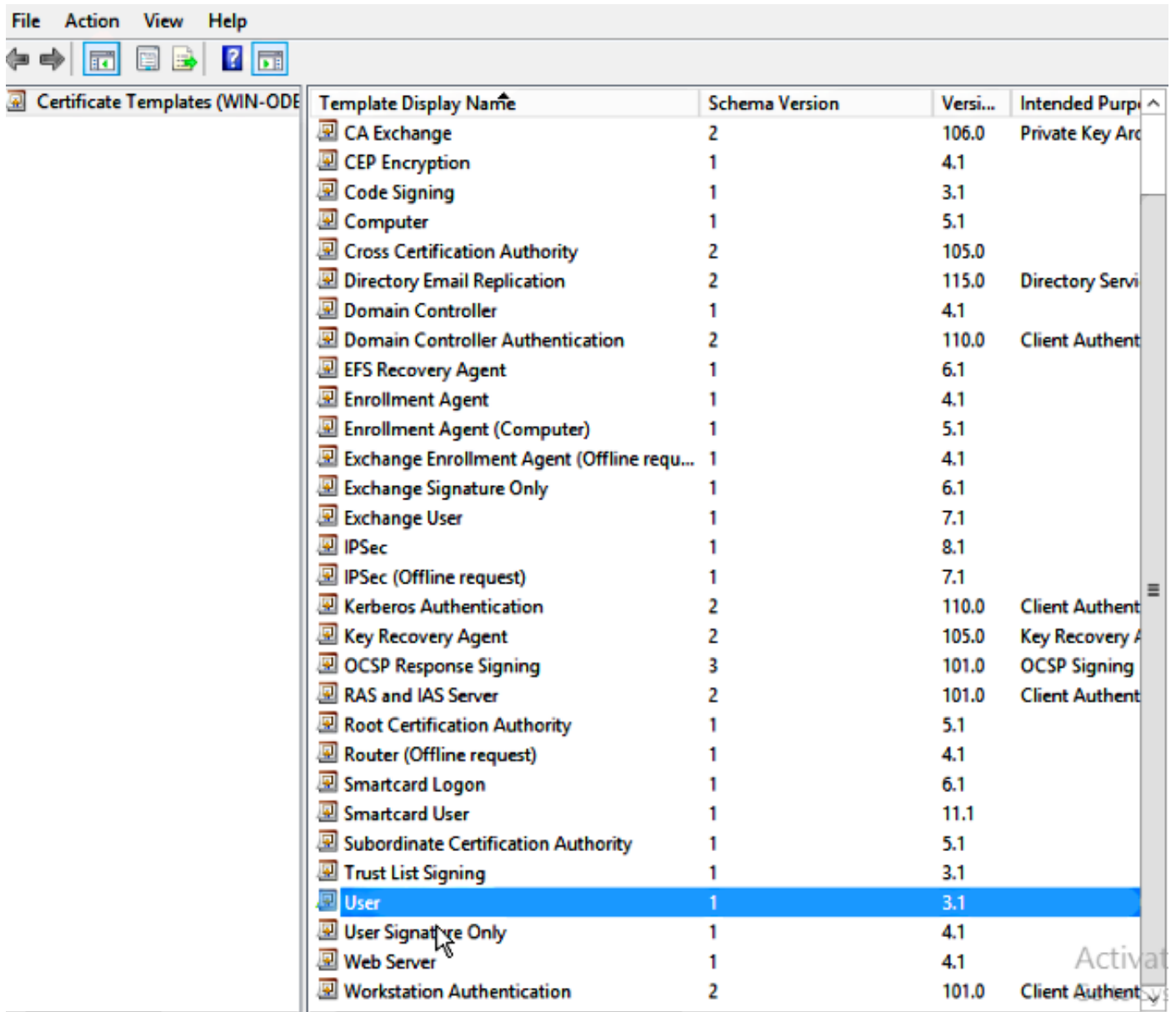
ステップ22:[Microsoft Windows/スタートメニュー]をクリックします。

ステップ23:MMCと入力します。

ステップ24:[ファイル]メニューで、[スナップインの追加と削除]を選択します。[Certification Authority]を選択します。

ステップ25:[証明書テンプレート]フォルダを右クリックし、[管理]をクリックします。

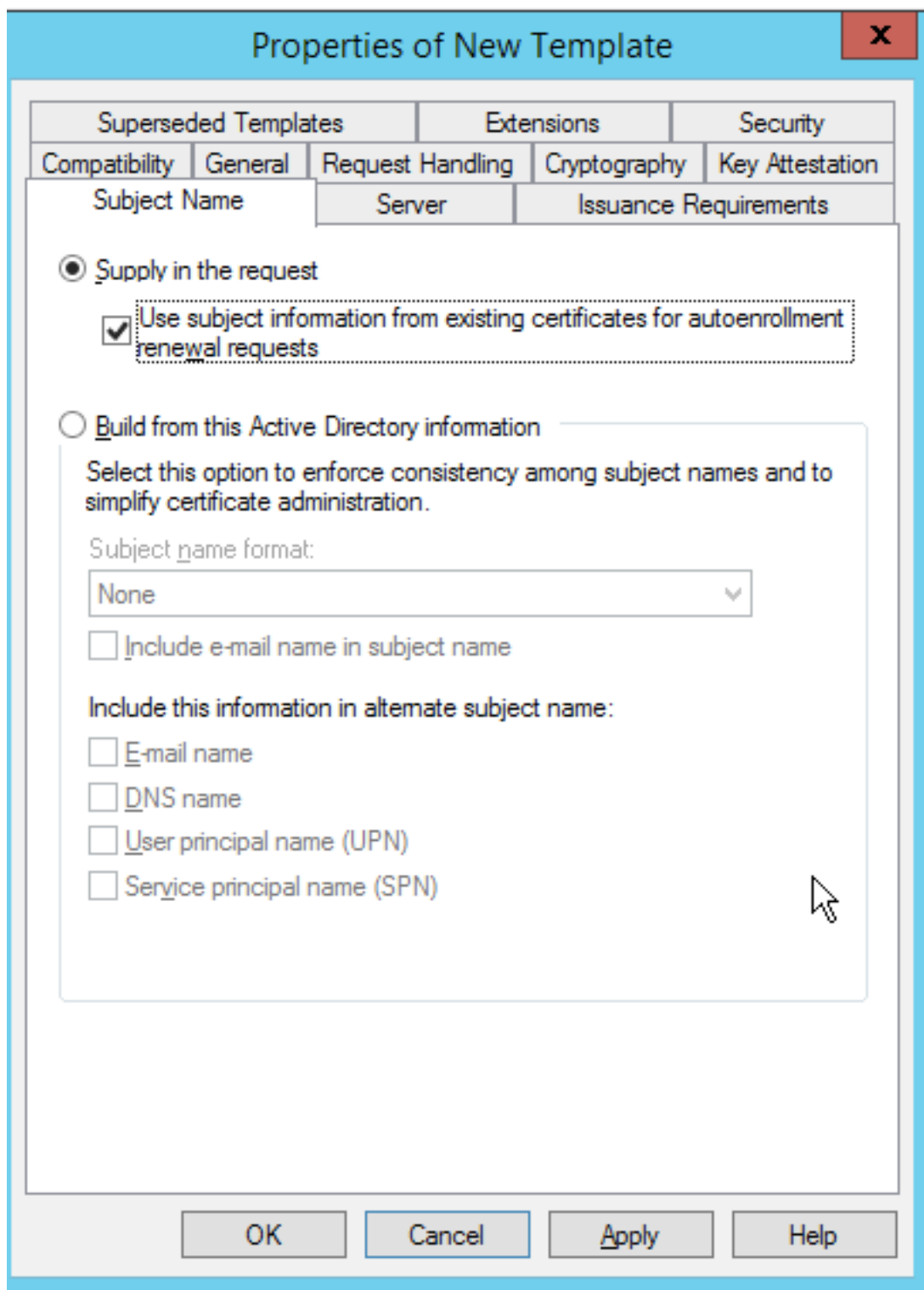
ステップ26:「ユーザー」などの既存のテンプレートを右クリックし、「テンプレートの複製」を選択します。



ステップ27:Microsoft Windows 2012 R2にするCAを選択します。

ステップ28: [General]タブで、WLCなどの表示名と有効期間を追加します。

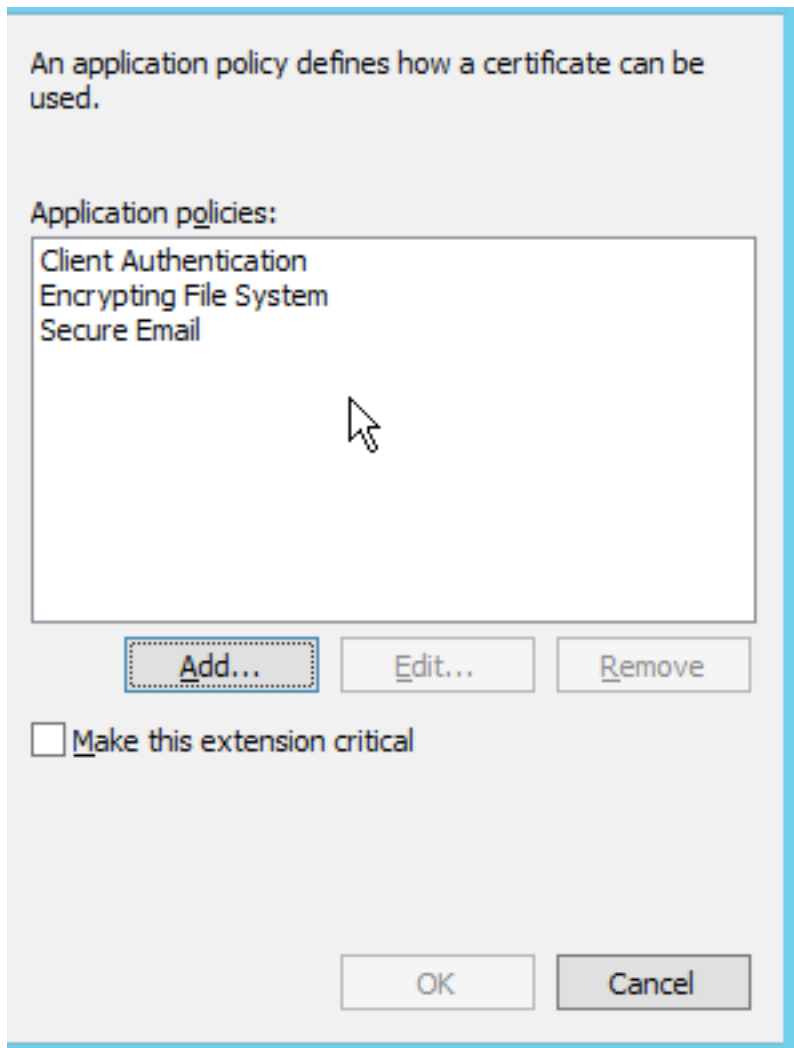
ステップ29:[Subject Name]タブで、[Supply in the request]が選択されていることを確認します。



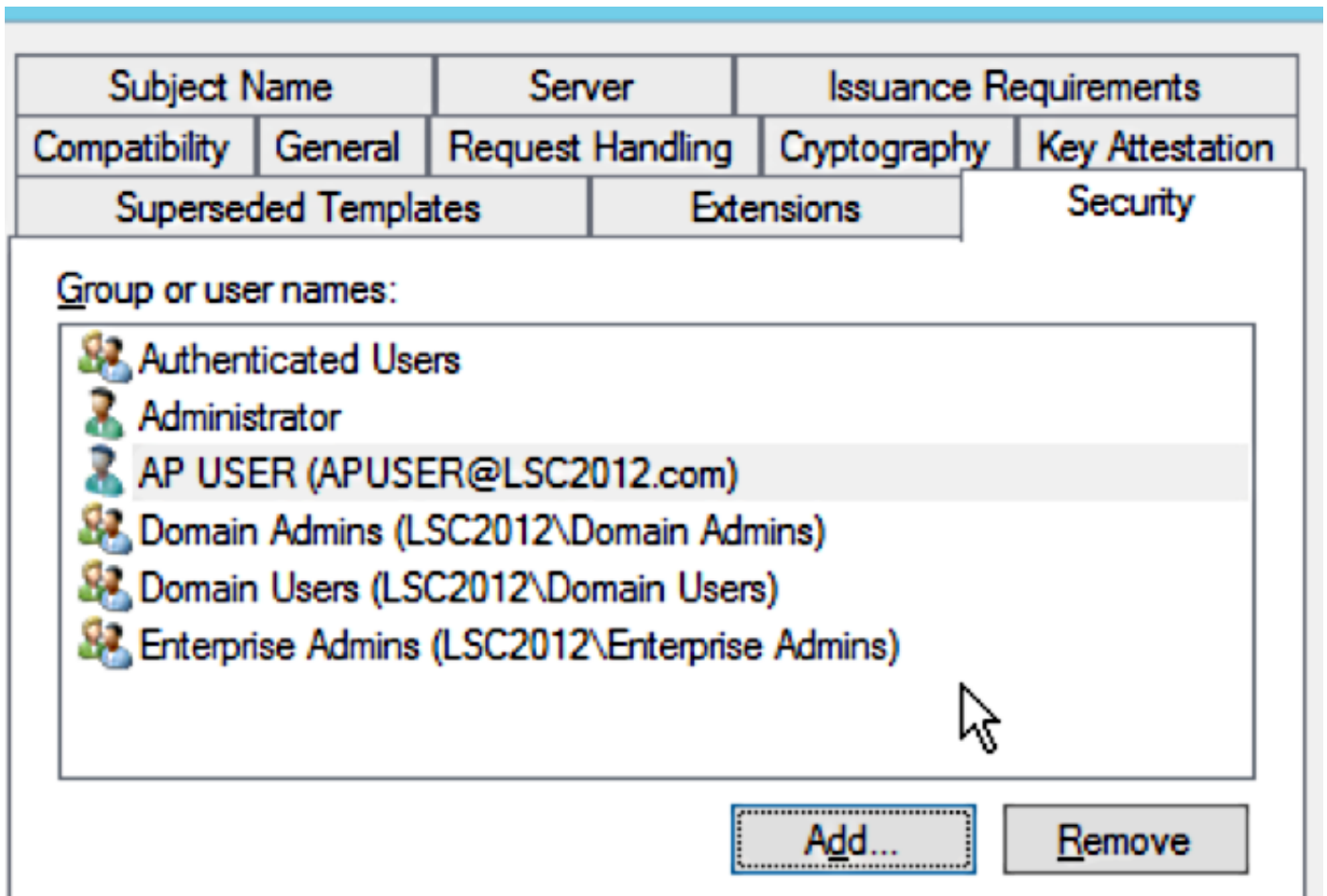
ステップ30:[発行要件]タブをクリックします。一般的な階層型CA環境では、発行ポリシーを空白のままにしておくことを推奨します。

Superseded Templates		Extensions		Security
Compatibility	General	Request Handling	Cryptography	Key Attestation
Subject Name		Server		Issuance Requirements
Require the following for enrollment:				
<input type="checkbox"/> CA certificate manager approval				
<input type="checkbox"/> This number of authorized signatures: <input type="text" value="0"/>				
If you require more than one signature, autoenrollment is not allowed.				
Policy type required in signature:				
<input type="text"/>				
Application policy:				
<input type="text"/>				
Issuance policies:				
<input type="text"/>				<input type="button" value="Add..."/>
				<input type="button" value="Remove"/>
Require the following for reenrollment:				
<input checked="" type="radio"/> Same criteria as for enrollment				
<input type="radio"/> Valid existing certificate				
<input type="checkbox"/> Allow key based renewal				
Requires subject information to be provided within the certificate request.				
<input type="button" value="OK"/> <input type="button" value="Cancel"/> <input type="button" value="Apply"/> <input type="button" value="Help"/>				

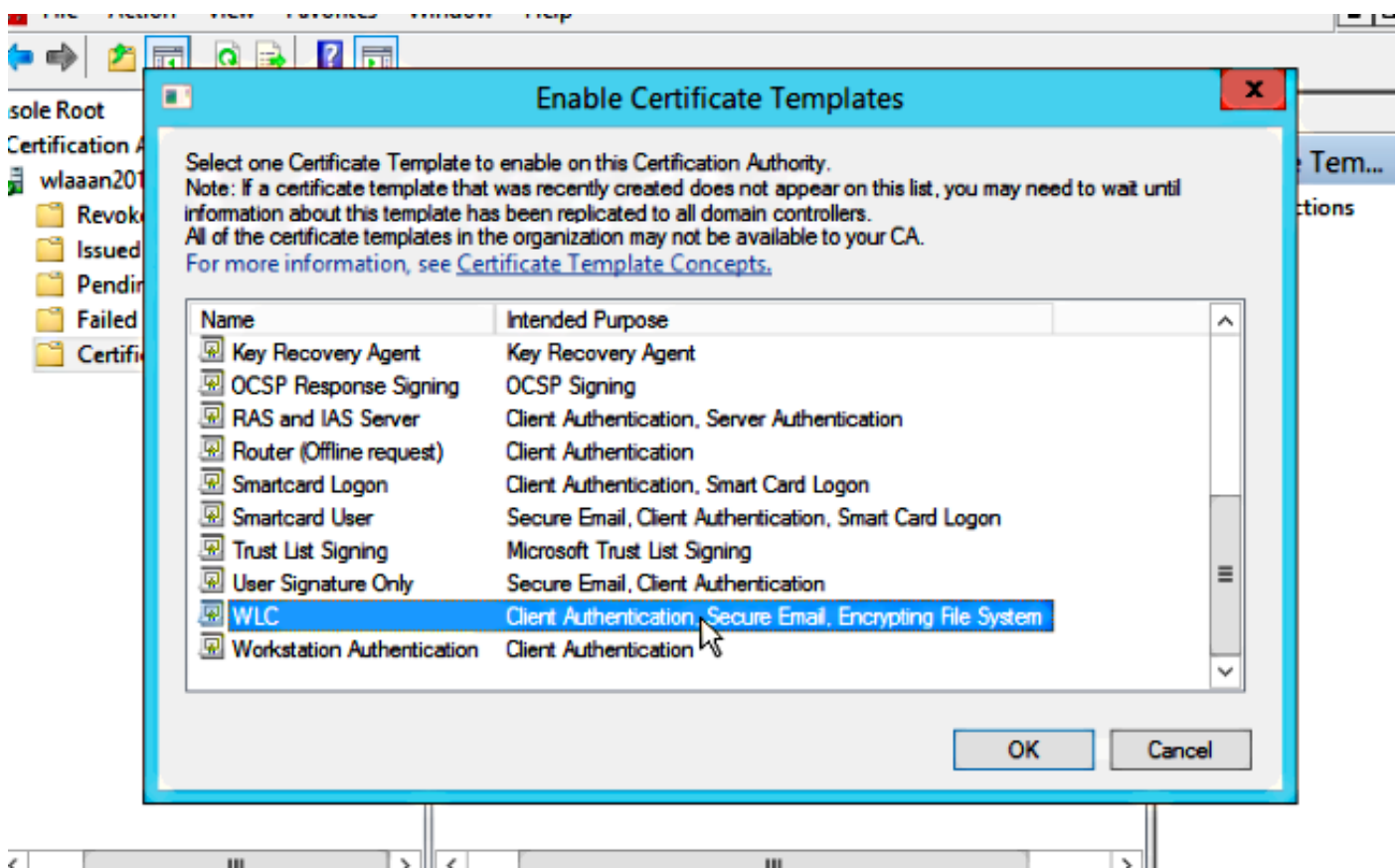
ステップ31:[Extensions]タブ、[Application Policies]、[Edit]の順にクリックします。[Add] をクリックして、[Client Authentication] がアプリケーション ポリシーとして追加されていることを確認します。[OK] をクリックします。



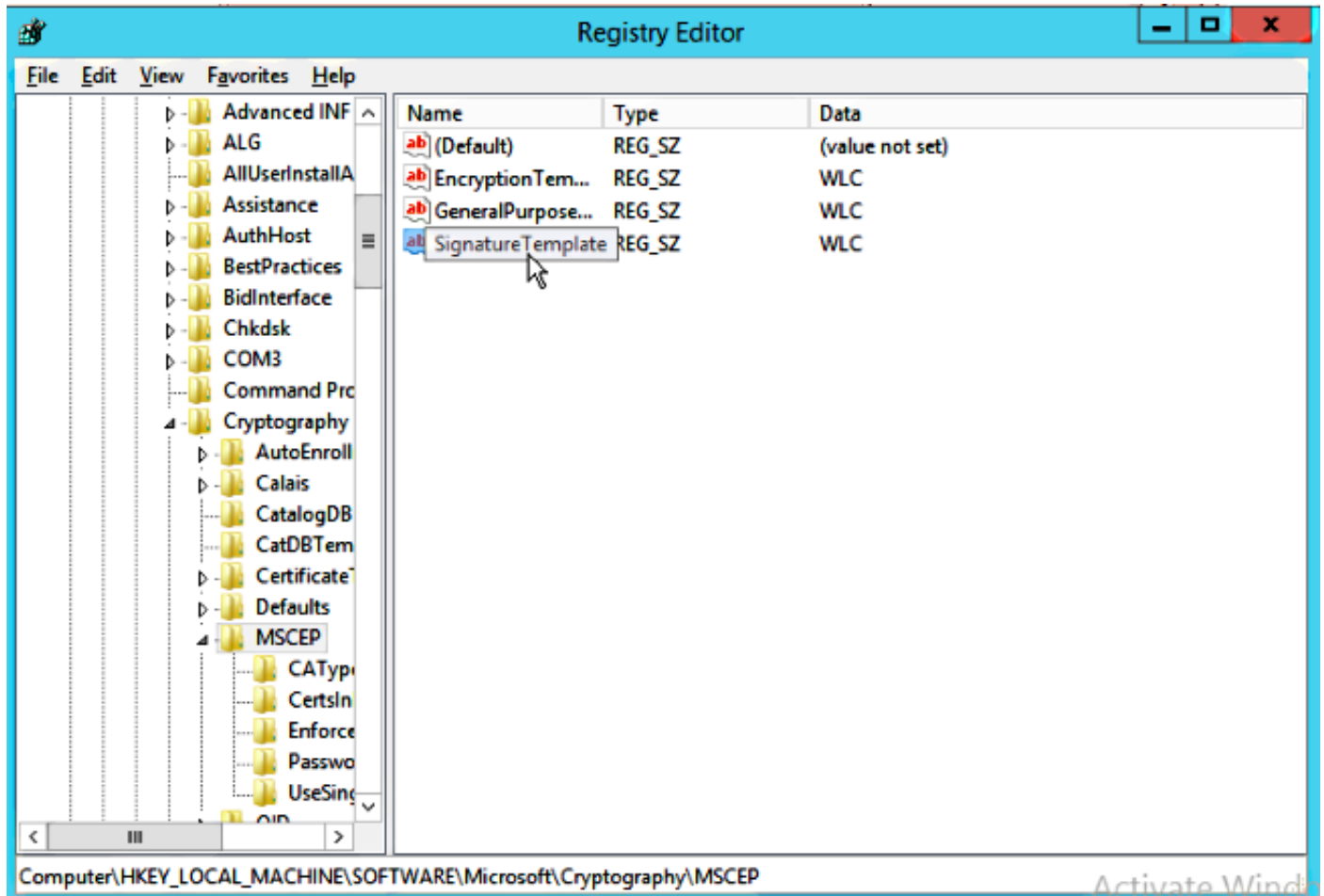
ステップ32:[セキュリティ]タブをクリックし、[追加...]をクリックします。.NDESサービスのインストールで定義されたSCEPサービスアカウントがテンプレートを完全に制御していることを確認し、[OK]をクリックします。



ステップ33: Certification Authority GUIインターフェイスに戻ります。Certificate Templatesディレクトリを右クリックします。[New] [Certificate Template to Issue] に移動します。以前に設定したWLCテンプレートを選択し、[OK]をクリックします。



ステップ34:[Computer] > [HKEY_LOCAL_MACHINE] > [SOFTWARE] > [Microsoft] > [Cryptography] > [MSCEP]の下のレジストリ設定で、デフォルトのSCEPテンプレートを変更します。EncryptionTemplate、GeneralPurposeTemplate、およびSignatureTemplateキーをIPsec (オフライン要求) から以前作成したWLCテンプレートに変更します。



ステップ35 : システムを再起動します。

WLC の設定

ステップ1:WLCで、[Security]メニューに移動します。[Certificates] > [LSC]をクリックします。

ステップ2:[Enable LSC on Controller]チェックボックスをオンにします。

ステップ3:Microsoft Windows Server 2012のURLを入力します。デフォルトでは、/certsrv/mscep/mscep.dllが付加されます。

ステップ4:「パラメータ」セクションに詳細を入力します。

ステップ5 : 変更を適用します。

Local Significant Certificates (LSC)

Apply

General

AP Provisioning

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

ステップ6：上のCA行の青い矢印をクリックし、[Add]を選択します。ステータスが[Not present]から[present]に変更されるようになっています。

ステップ7:[AP provisioning]タブをクリックします。

The screenshot shows the Cisco Security configuration interface for Local Significant Certificates (LSC). The left sidebar contains a navigation menu with categories like AAA, Local EAP, Priority Order, Certificate, Access Control Lists, Wireless Protection Policies, Web Auth, TrustSec SXP, and Advanced. The main content area is titled 'Local Significant Certificates (LSC)' and has two tabs: 'General' and 'AP Provisioning'. The 'AP Provisioning' tab is active, showing an 'Enable' checkbox that is checked, an 'Update' button, and a text input field for 'Number of attempts to LSC (0 to 255)' with the value '3'. Below this is a section for 'AP Ethernet MAC Addresses' with an empty text input field and an 'Add' button. The 'MAC Address' label is positioned below the input field.

ステップ8:[AP Provisioning]の下の[Enable]チェックボックスをオンにし、[Update]をクリックします。

ステップ9:アクセスポイントがリポートされていない場合は、リポートします。

確認

ここでは、設定が正常に機能しているかどうかを確認します。

アクセスポイントは、リポート後に再び参加し、[Wireless]メニューに証明書タイプとしてLSCが表示されます。

Wireless

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-CT5501I-2-K9	c8:9c:1d:6e:a3:cd	0 d, 00 h 35 m 21 s	Disabled	REG	1	Local	LSC
LAP1142I-1	AIR-LAP1142N-1-K9	ac:f2:c5:73:33:ce	0 d, 00 h 02 m 35 s	Enabled	REG	1	Local	LSC

Windows taskbar: ENG 6:41 PM, JIK 12/16/2014

注：8.3.112以降、MIC APはLSCが有効になると一度にまったく参加できません。したがって、「LSCへの試行」カウント機能は限られた使用になります。

トラブルシューティング

現在、この設定に関する特定のトラブルシューティング情報はありません。