Certificado localmente significativo (LSC) com exemplo de configuração de WLC e Windows Server 2012

Contents

Introduction

Este documento descreve como configurar o LSC (Locally Significant Certificate) com um WLC (Wireless LAN Controller) e um Microsoft Windows Server 2012 R2 instalado recentemente.

> **Note**: As implantações reais podem ser diferentes em muitos pontos e você deve ter controle total e conhecimento das configurações no Microsoft Windows Server 2012. Este exemplo de configuração é fornecido apenas como um modelo de referência para que os clientes da Cisco implementem e adaptem sua configuração do Microsoft Windows Server para fazer o LSC funcionar.

Prerequisites

Requirements

A Cisco recomenda que você compreenda todas as alterações feitas no Microsoft Windows Server e verifique a documentação relevante da Microsoft, se necessário.

> **Note**: O LSC na WLC não é suportado com CA intermediário, pois a CA raiz será perdida da WLC, já que a controladora recebe apenas a CA intermediária.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- WLC versão 7.6

- Microsoft Windows Server 2012 R2

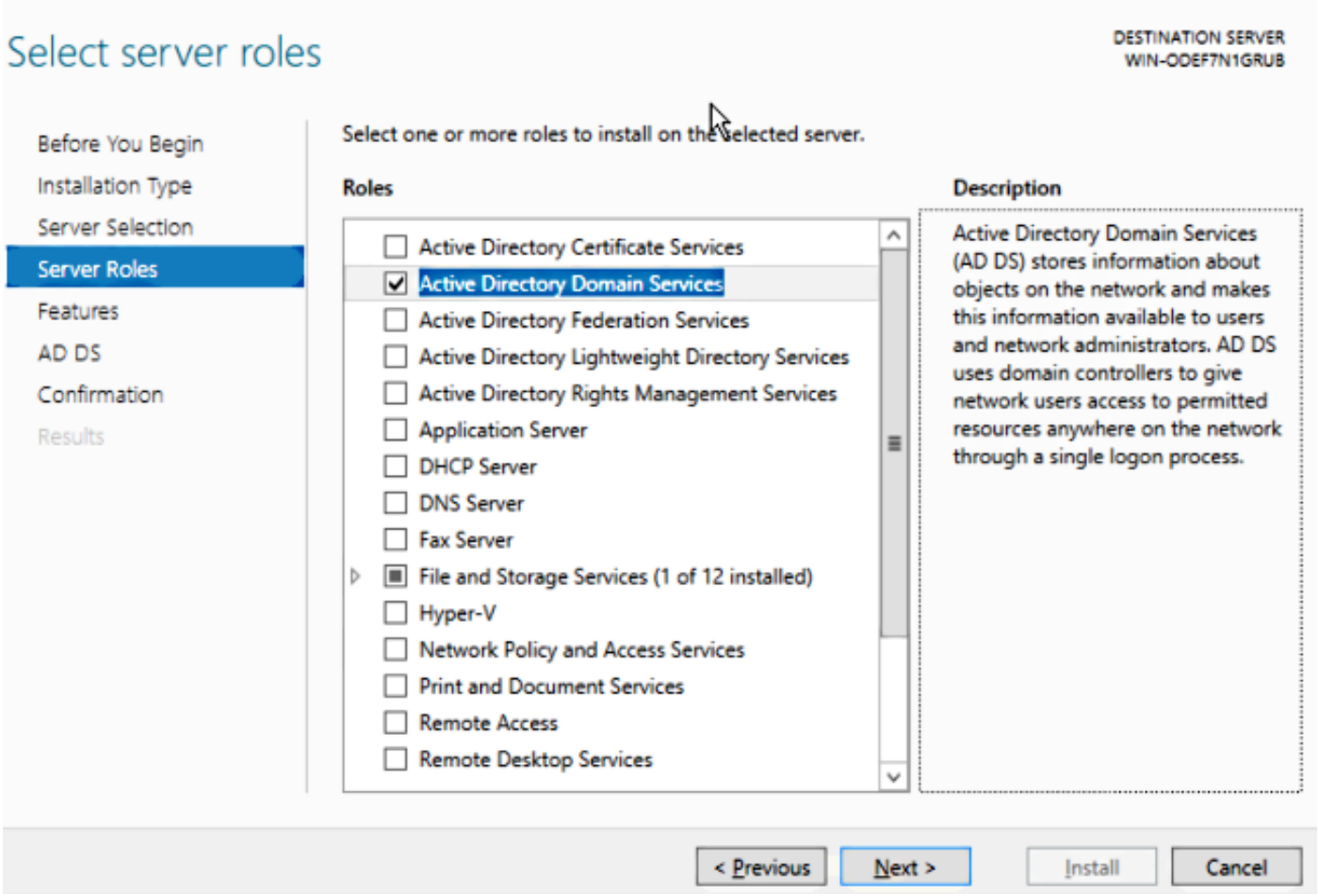
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurar

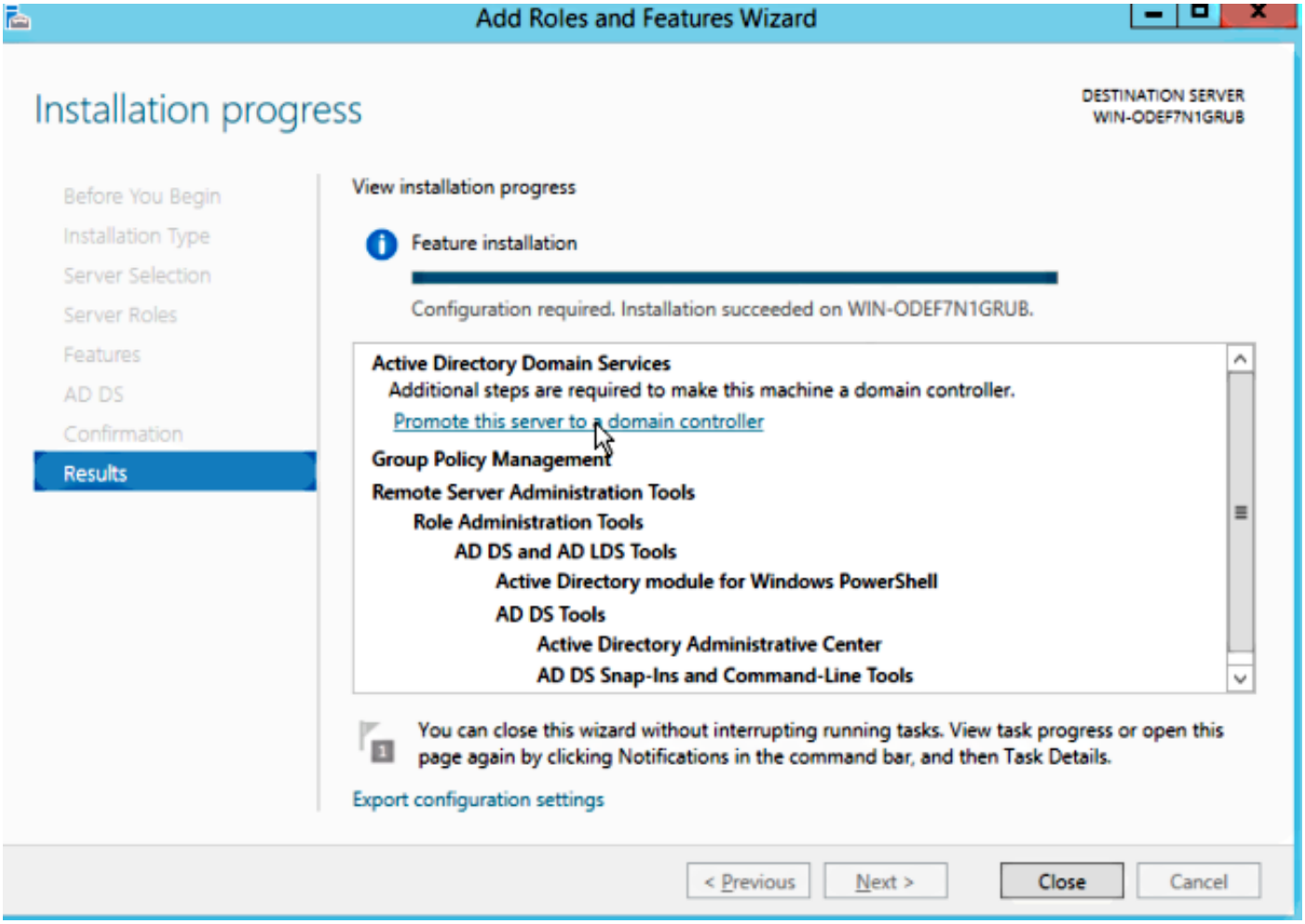
Configuração do Microsoft Windows Server

Esta configuração é mostrada como executada em um Microsoft Windows Server 2012 recém-instalado. Você deve adaptar as etapas ao seu domínio e à sua configuração.

Etapa 1. Instalar os Serviços de Domínio do Ative Diretory para o assistente de funções e recursos.

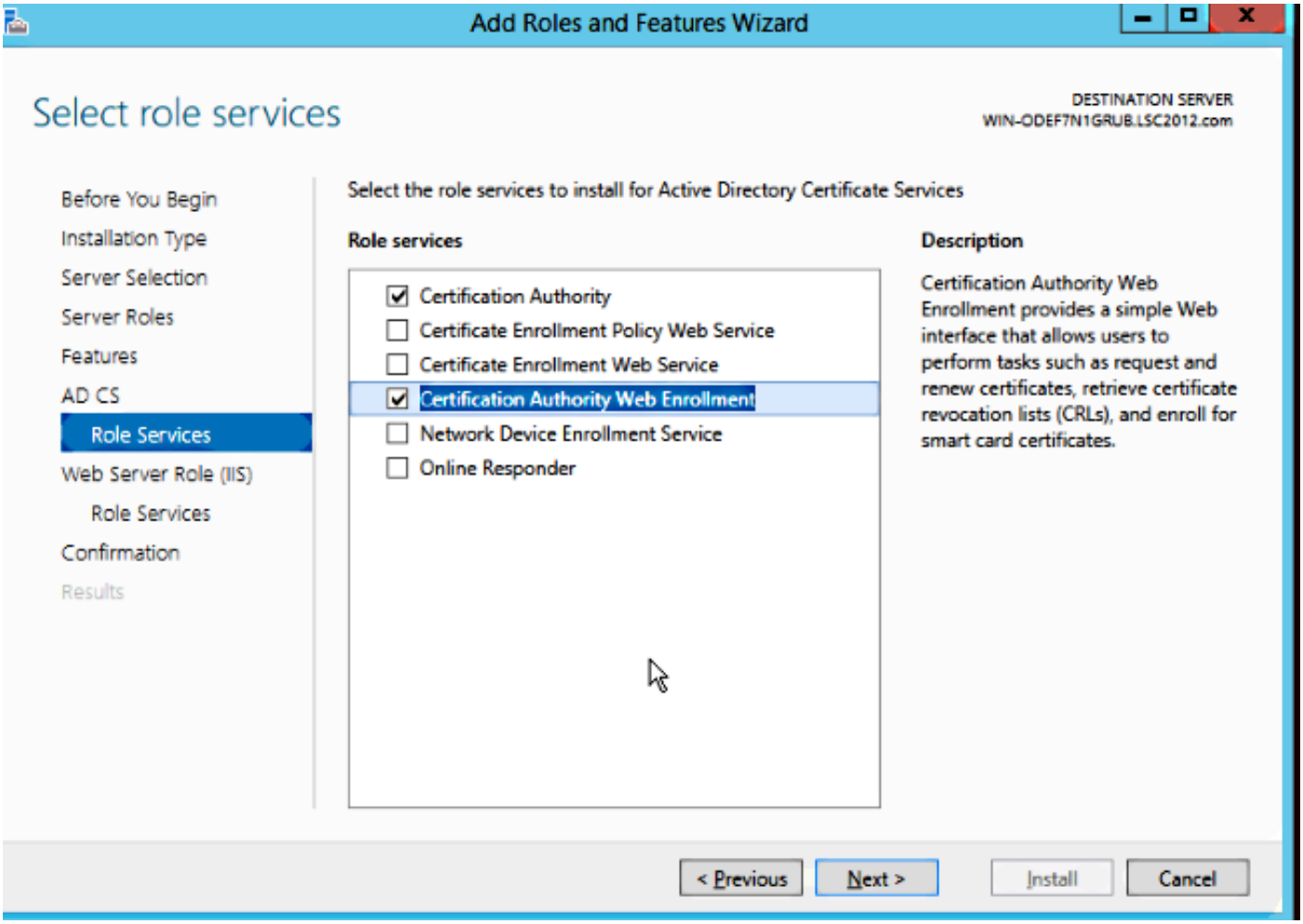


Etapa 2. Após a instalação, você deve promover o servidor para o controlador de domínio.

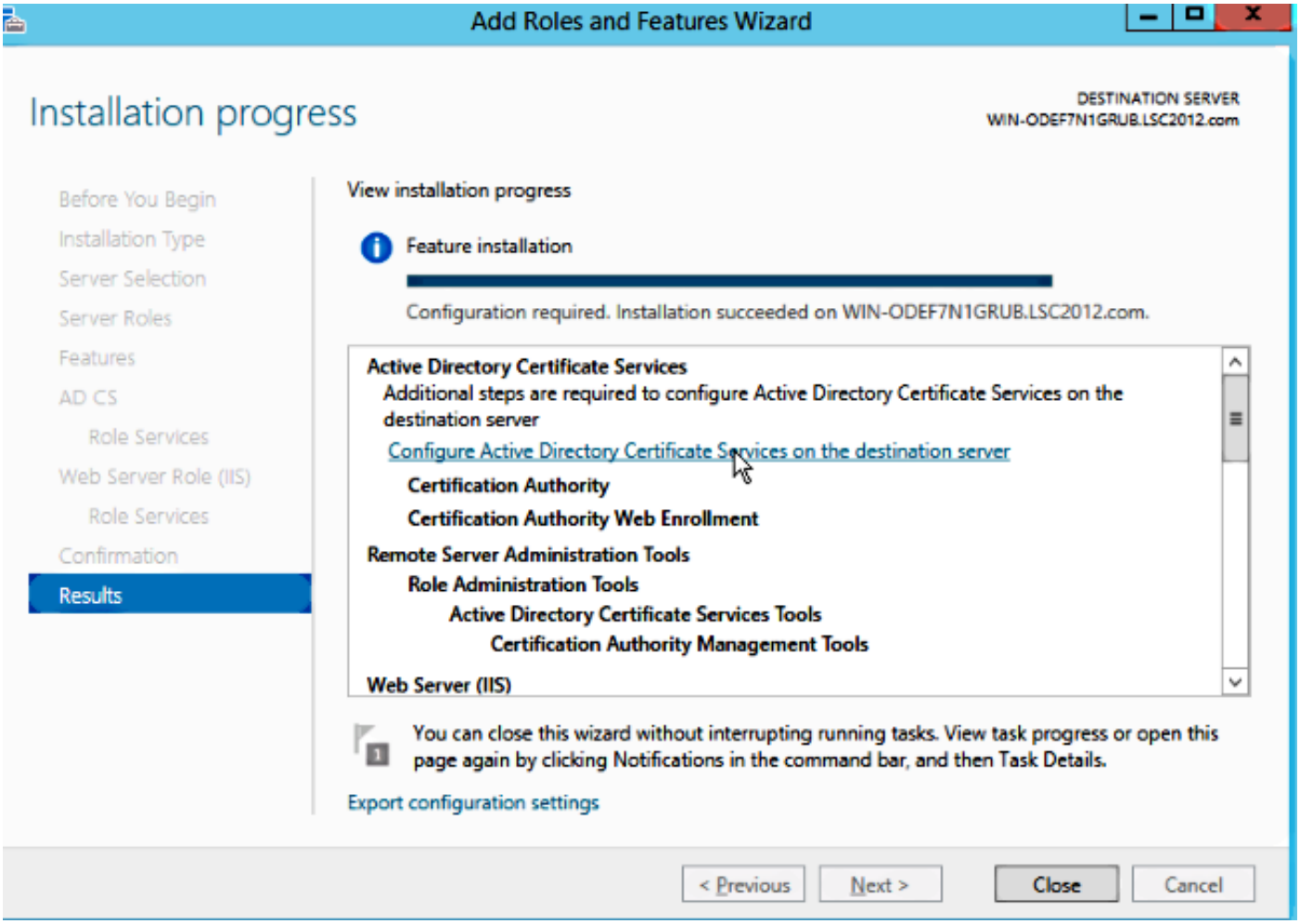


Etapa 3. Como esta é uma nova configuração, você configura uma nova floresta; mas normalmente em implantações existentes, basta configurar esses pontos em um controlador de domínio. Aqui, você escolhe o domínio **LSC2012.com**. Isso também ativa o recurso Servidor de Nomes de Domínio (DNS).

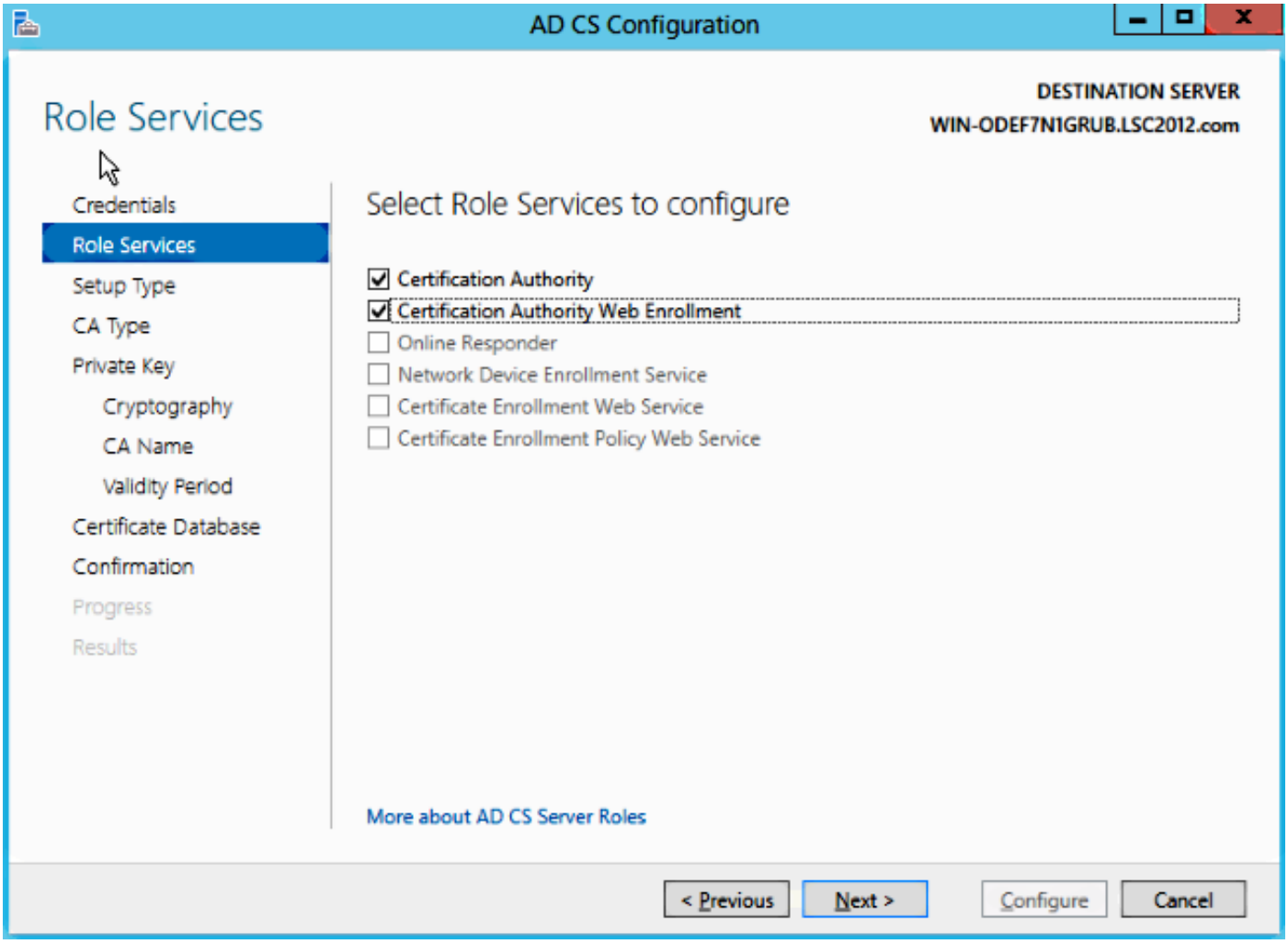
Etapa 4. Após uma reinicialização, instale o serviço Autoridade de Certificação (CA) e a inscrição na Web.



Etapa 5. Configure-os.



Etapa 6. Escolha AC empresarial e deixe tudo como padrão.

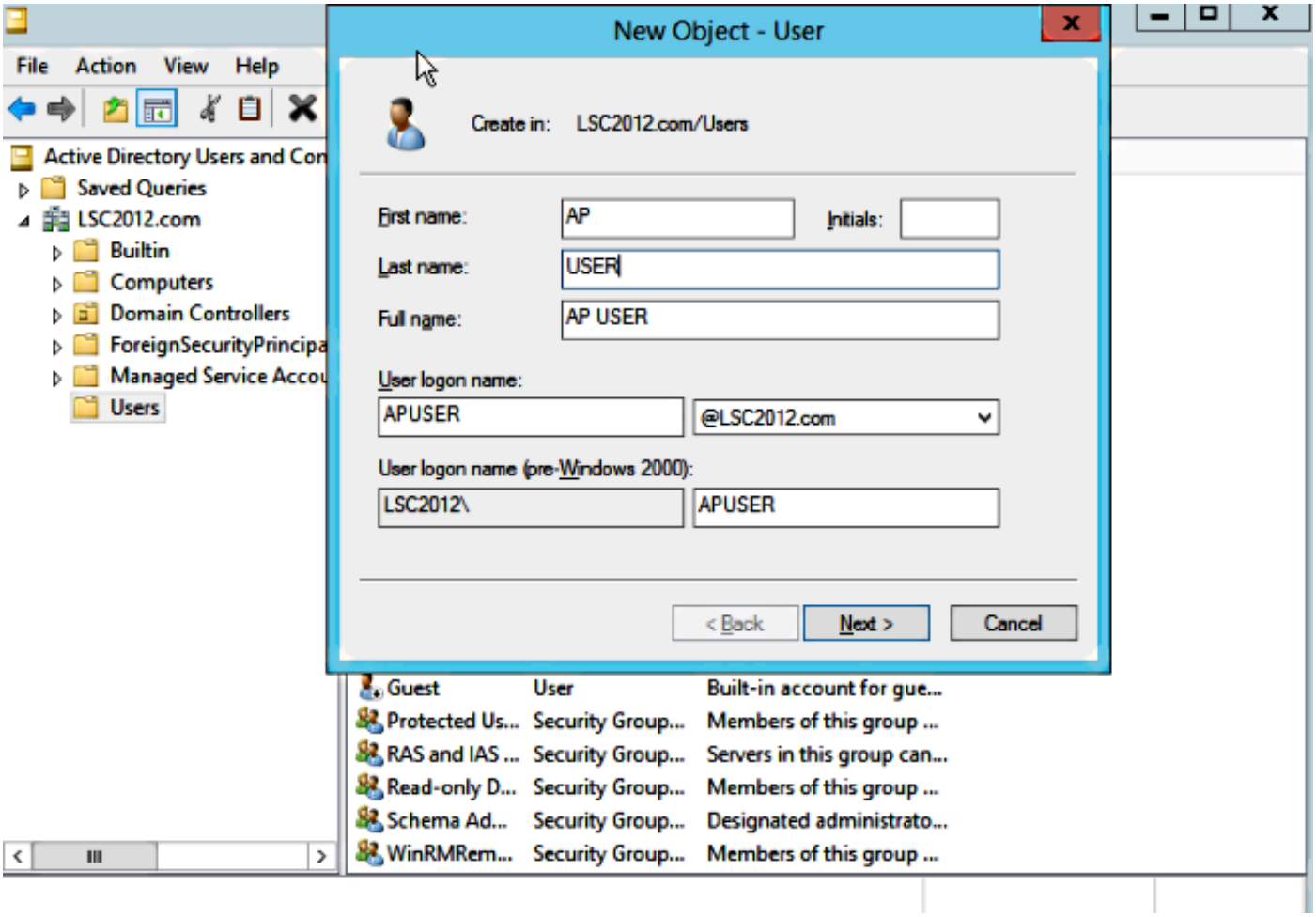


Passo 7. Clique no **menu Iniciar do Microsoft Windows**.

Etapa 8. Clique em **Ferramentas administrativas**.

Etapa 9. Clique em **Usuários e Computadores do Ative Diretory**.

Etapa 10. Expanda o domínio, clique com o botão direito do mouse na **pasta Usuários** e escolha **Novo objeto > Usuário**.



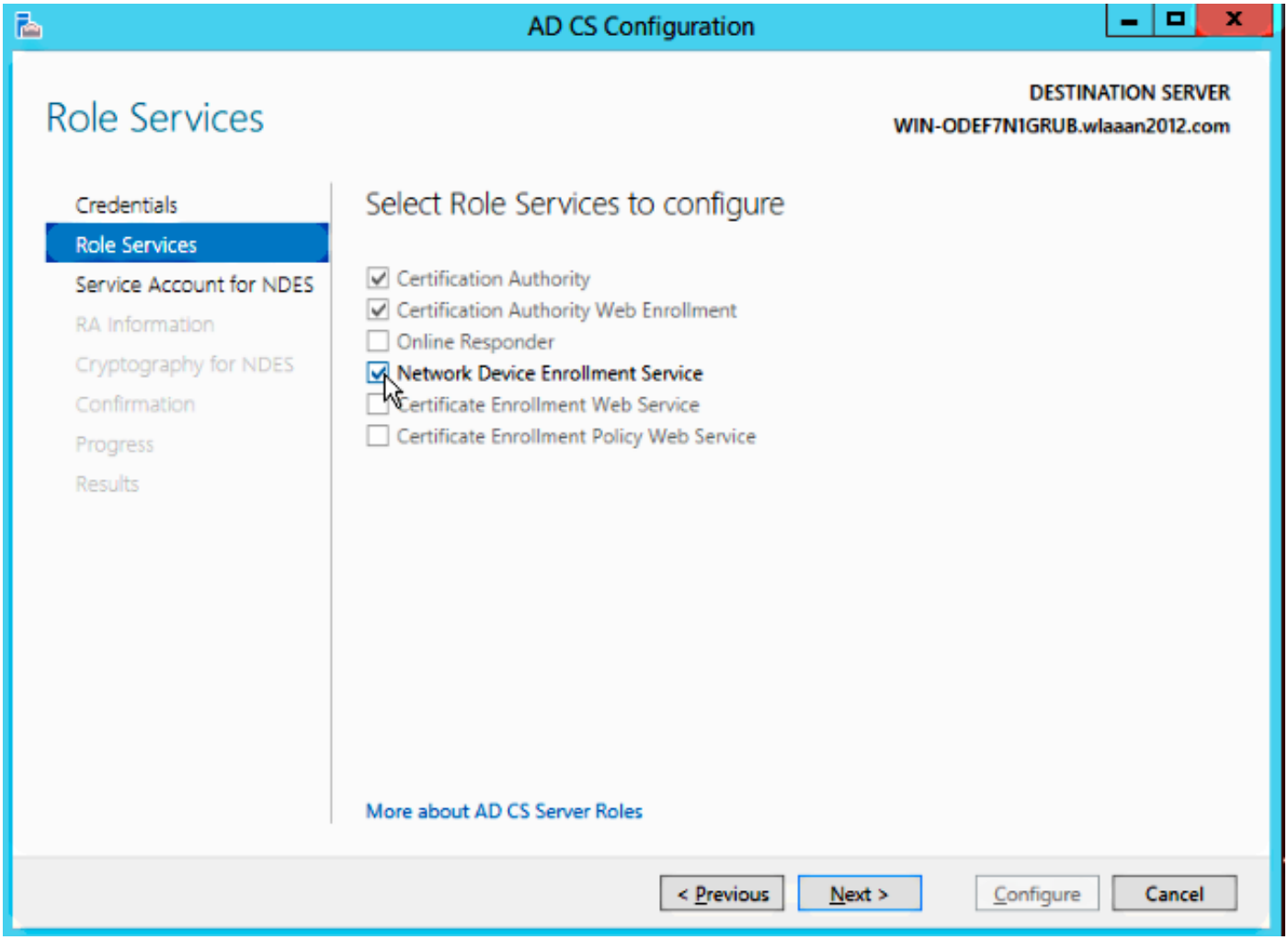
Etapa 11. Neste exemplo, ele é chamado **APUSER**. Depois de criado, você deve editar o usuário e clicar na **guia MemberOf** e torná-lo um membro do grupo IIS_IUSRS

As atribuições de direitos de usuário necessárias são:

- Permitir logon local

- Fazer logon como um serviço

Etapa 12. Instale o Network Device Enrollment Service (NDES).



- Escolha o membro da conta do grupo IIS_USRS, **APUSER** neste exemplo, como a conta de serviço para NDES.

Etapa 13. Navegue até Ferramentas administrativas.

Etapa 14. Clique em **Internet Information Services (IIS)**.

Etapa 15. Expanda **Server > Sites > Default web site > Cert Srv**.

Etapa 16. Para **mscep** e **mscep_admin**, clique em **authentication**. Verifique se a autenticação anônima está habilitada.

Etapa 17. Clique com o botão direito do mouse em **autenticação do Windows** e escolha **Provedores**. Certifique-se de que o NT LAN Manager (NTLM) esteja primeiro na lista.

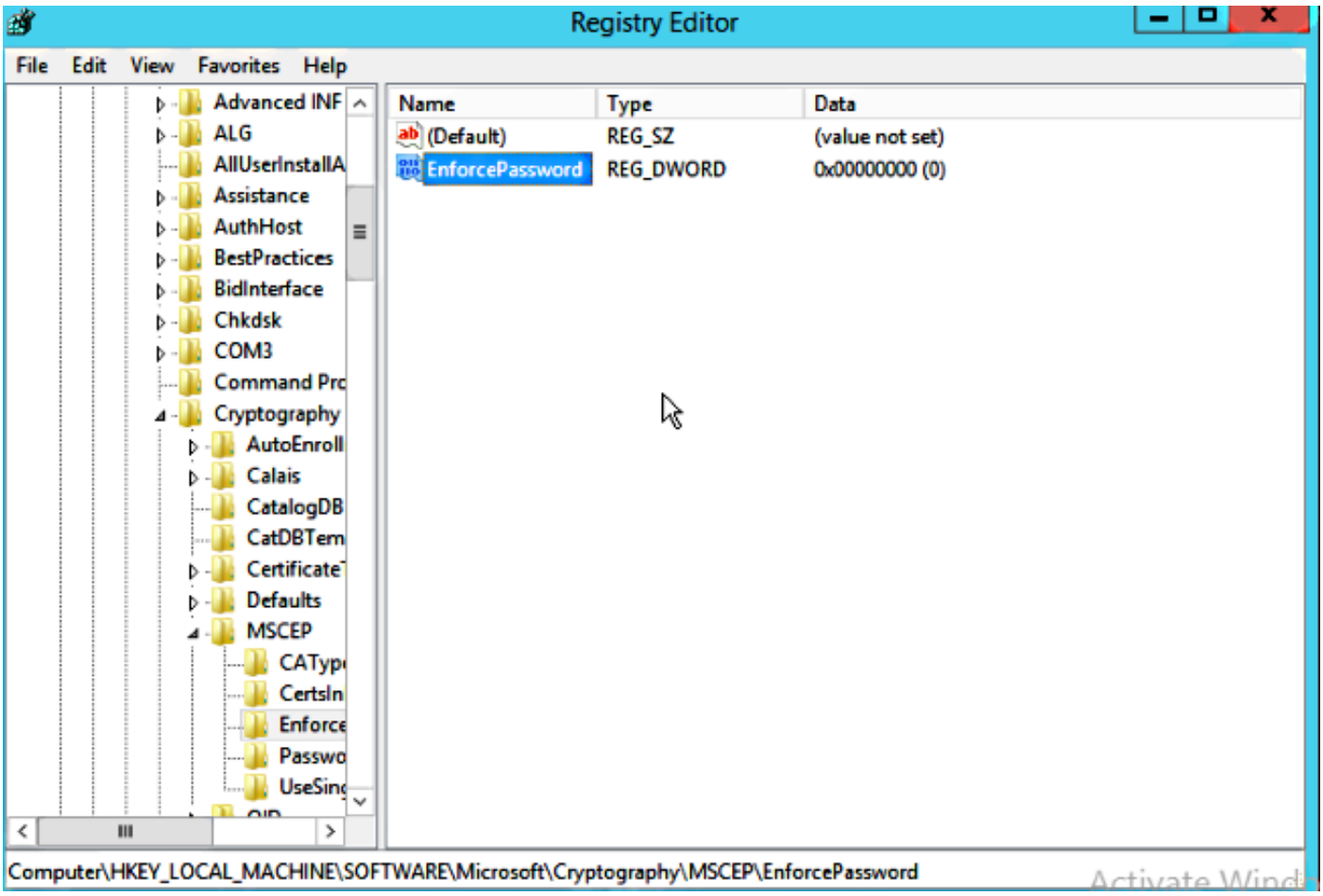
Etapa 18. Desative o desafio de autenticação nas configurações do registro, caso contrário, o protocolo SCEP (Simple Certificate Enrollment Protocol) espera a autenticação de senha de

desafio, que não é suportada pelo WLC.

Etapa 19. Abra o **aplicativo regedit**.

Etapa 20. Vá para **HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\Cryptography\MSCEP**.

Etapa 21. Defina EnforcePassword como **0**.



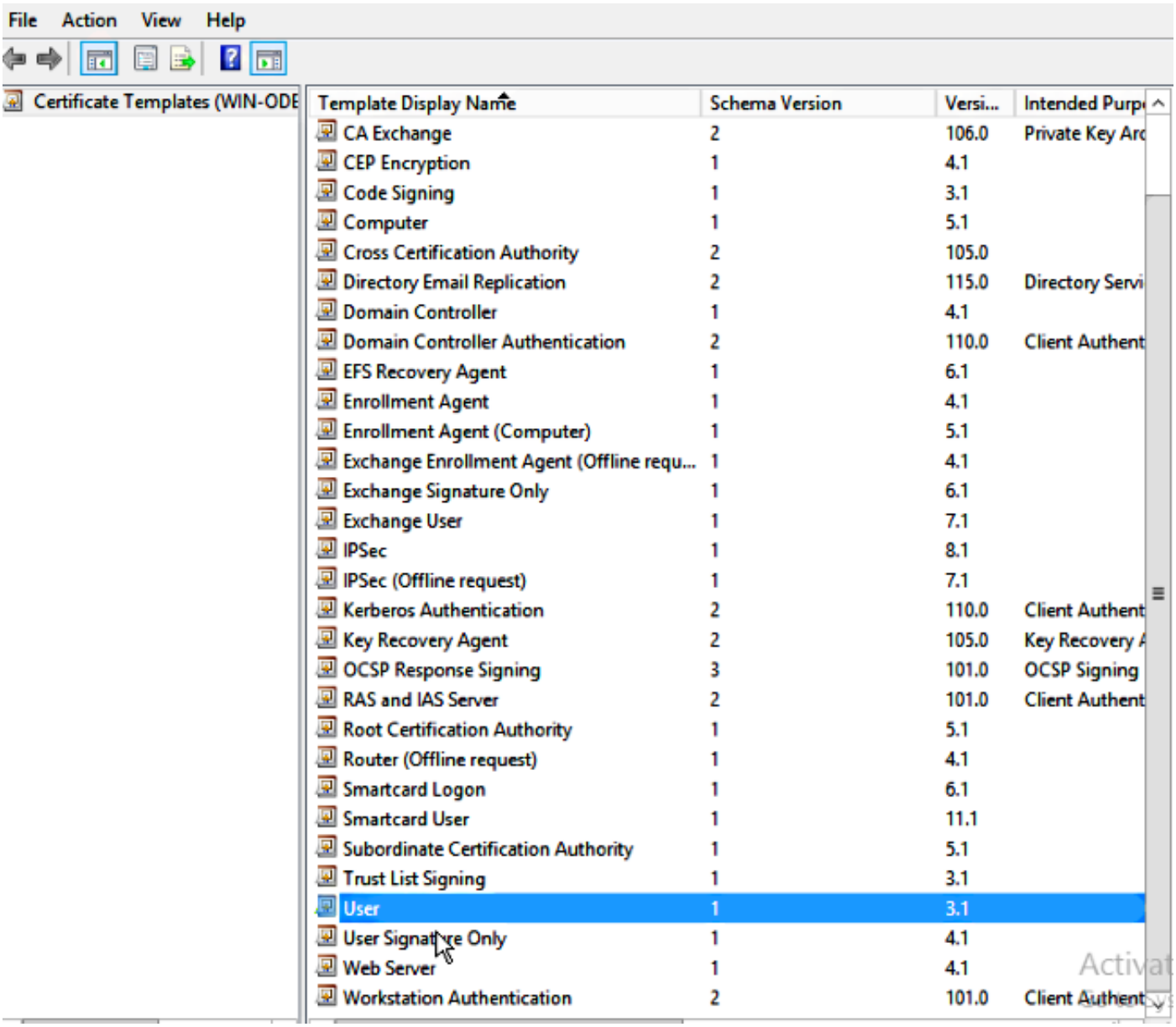
Etapa 22. Clique no **menu Iniciar do Microsoft Windows**.

Etapa 23. Digite **MMC**.

Etapa 24. No menu Arquivo, escolha **Adicionar/remover snap-in**. Escolha **Autoridade de Certificação**.

Etapa 25. Clique com o botão direito do mouse na **pasta Modelo de certificado** e clique em **Gerenciar**.

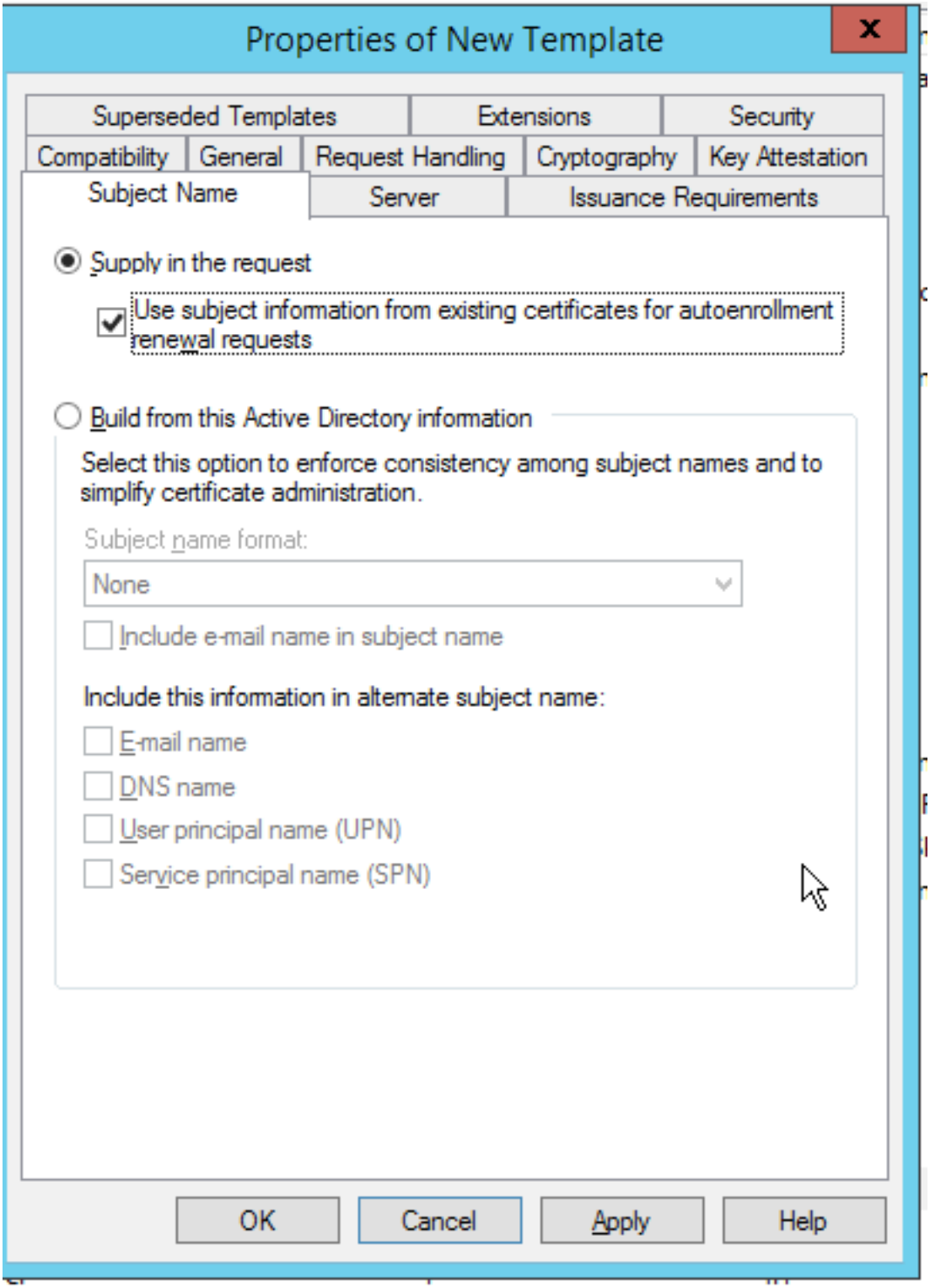
Etapa 26. Clique com o botão direito do mouse em um modelo existente, como Usuário, e escolha **Modelo duplicado**.



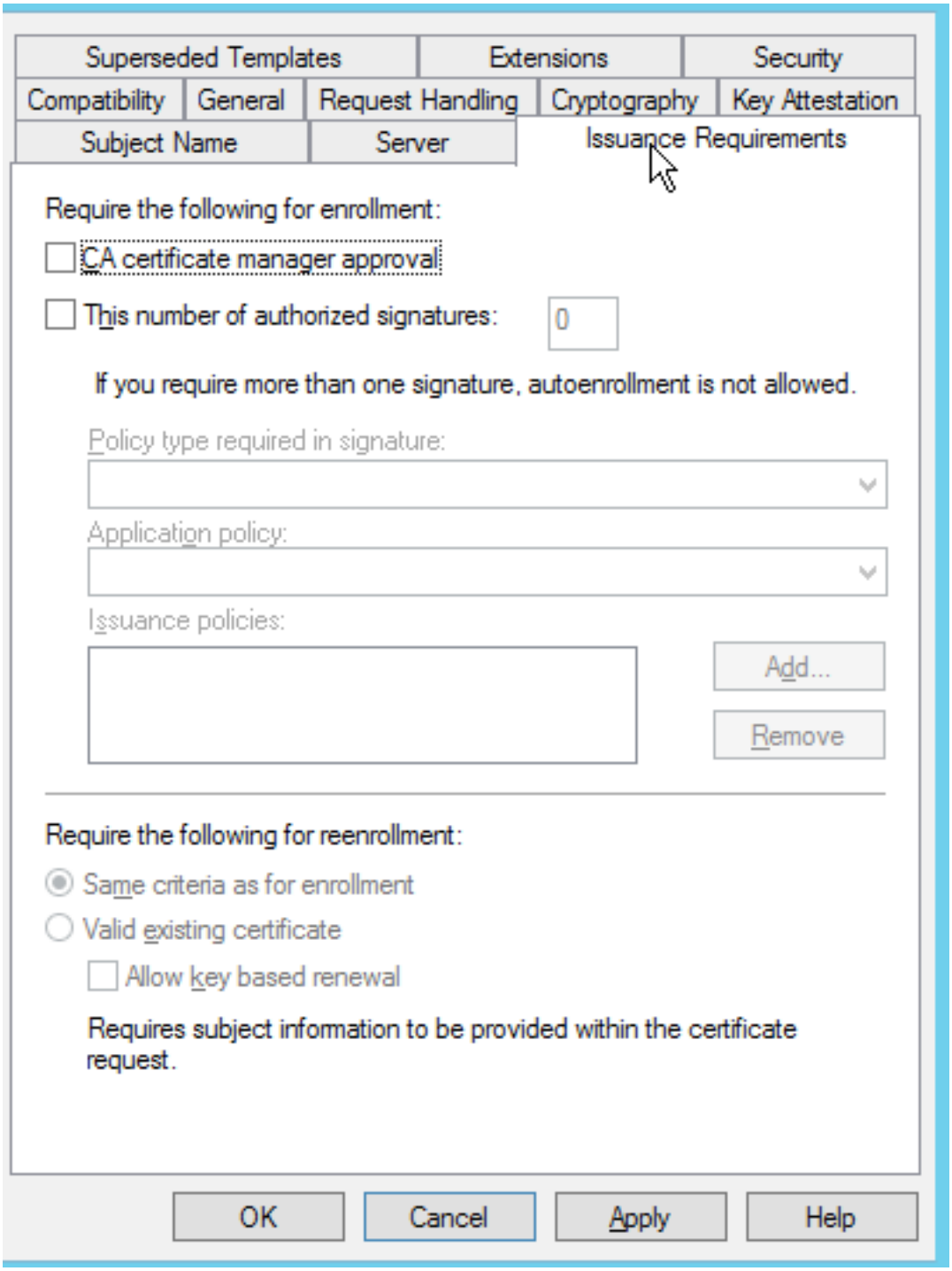
Etapa 27. Escolha a CA para o Microsoft Windows 2012 R2.

Etapa 28. Na guia Geral, adicione um nome de exibição, como WLC e um período de validade.

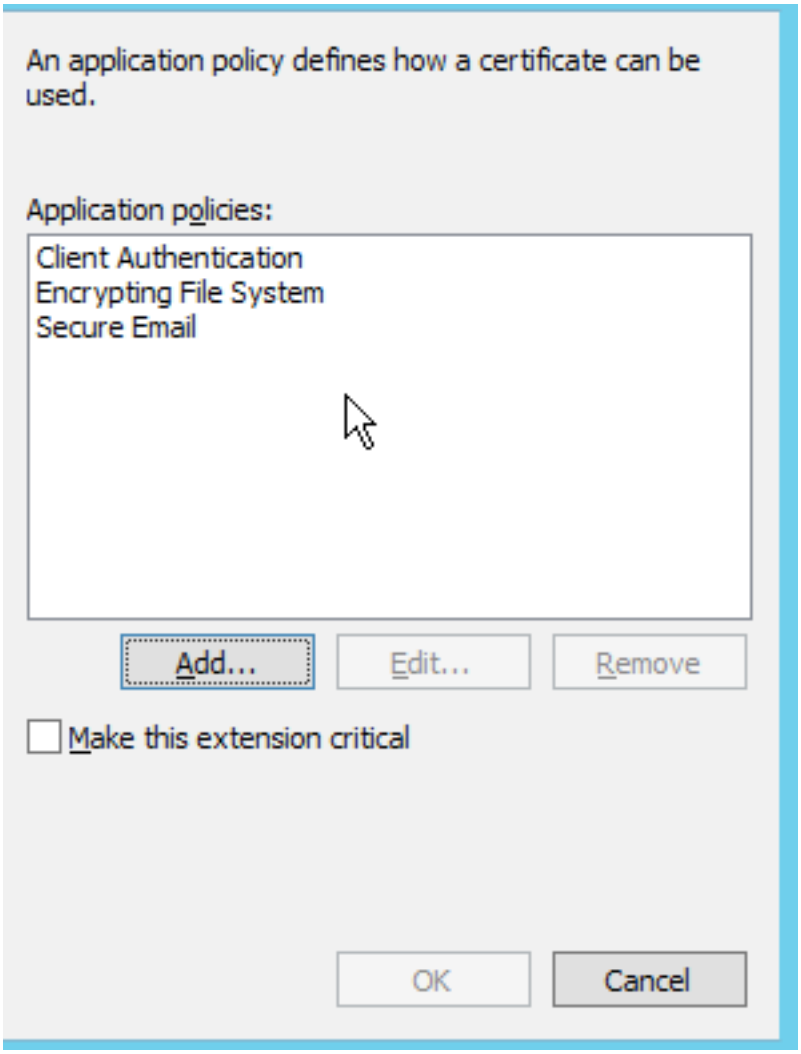
Etapa 29. Na guia Nome do assunto, confirme se **Suprimento na solicitação** está selecionado.



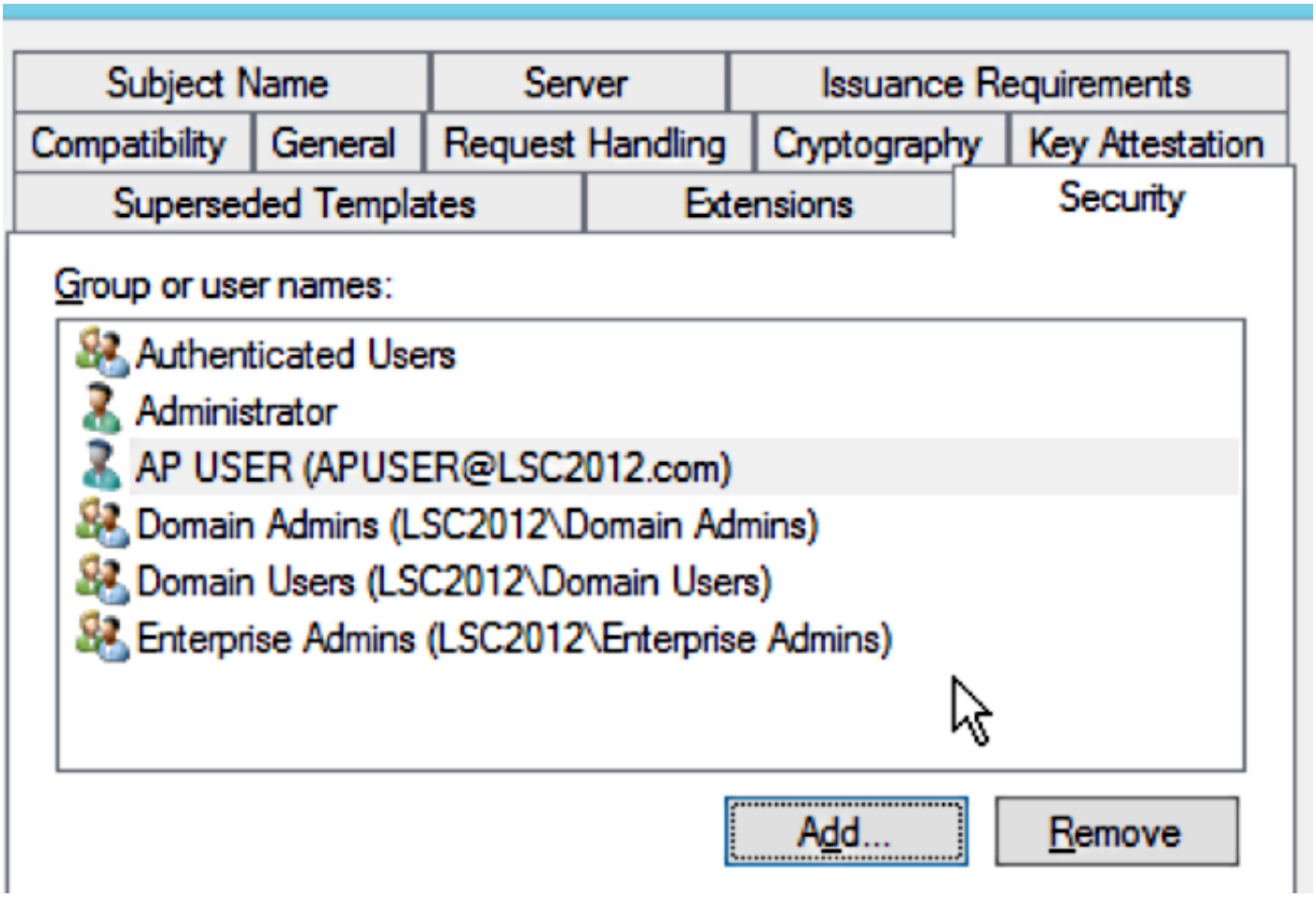
Etapa 30. Clique na guia **Issuance Requirements (Requisitos de problema)**. A Cisco recomenda que você deixe as políticas de emissão em branco em um ambiente de CA hierárquico típico:



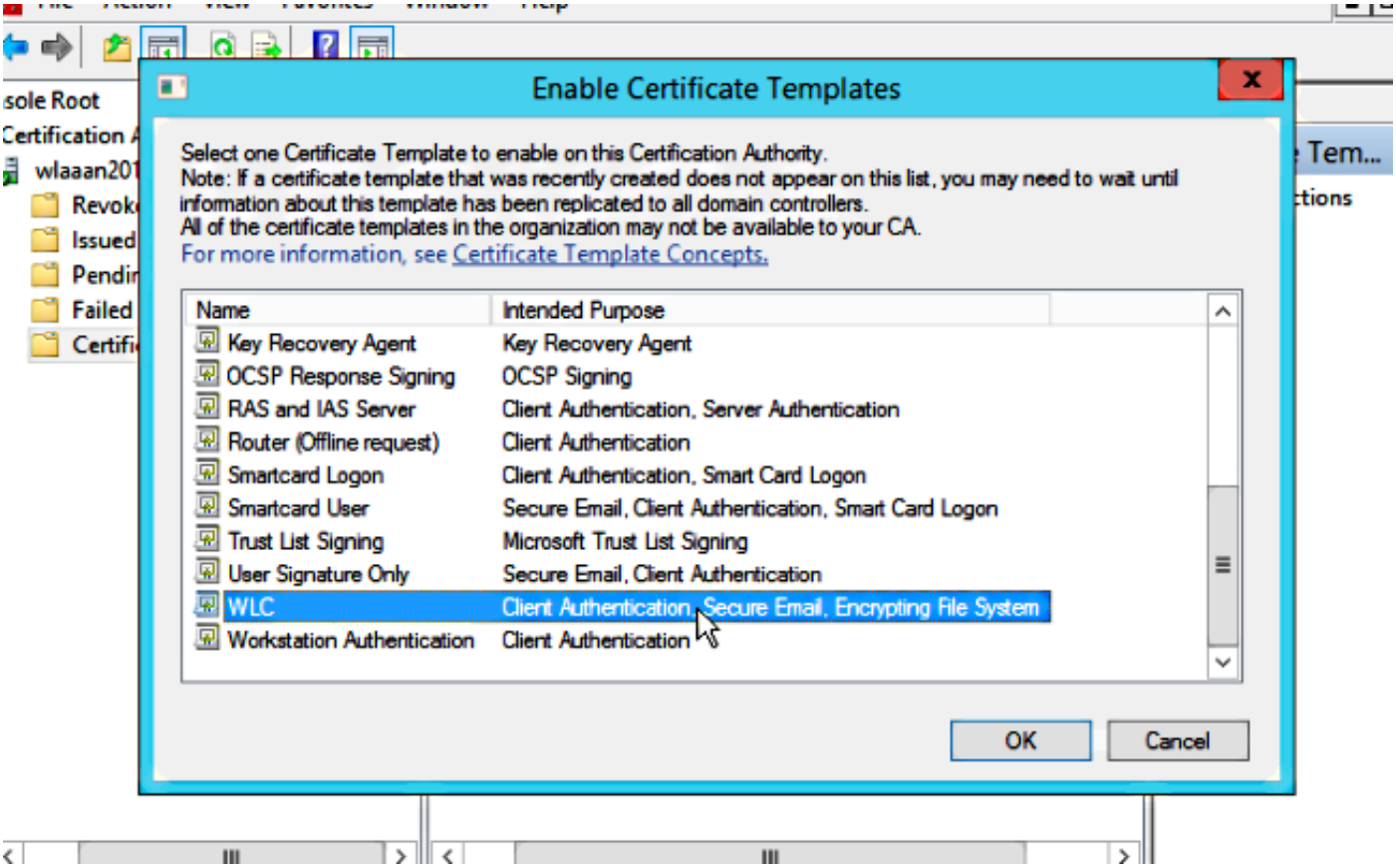
Etapa 31. Clique na **guia Extensions**, **Application Policies** e depois **Edit**. Clique em **Adicionar** e certifique-se de que a Autenticação do Cliente seja adicionada como uma política de aplicação. Click **OK**.



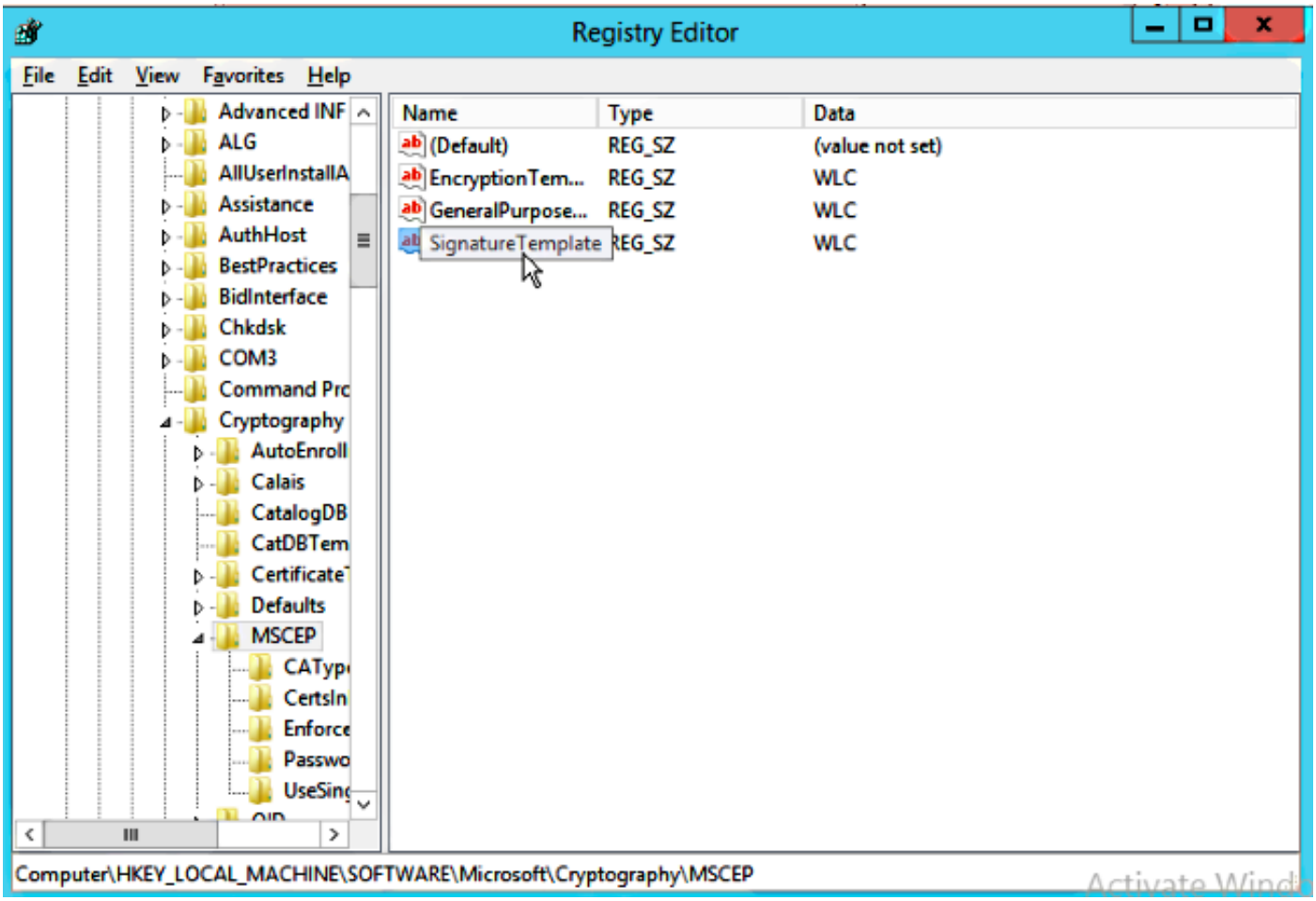
Etapa 32. Clique na **guia Segurança** e, em seguida, clique em **Adicionar...**. Certifique-se de que a conta de serviço SCEP definida na instalação do serviço NDES tem o controlo total do modelo e clique em **OK**.



Etapa 33. Retorne à interface GUI da autoridade de certificação. Clique com o botão direito do mouse no **diretório Modelos de certificado**. Navegue até **New > Certificate Template to Issue (Novo > Modelo de certificado a ser emitido)**. Selecione o modelo de WLC configurado anteriormente e clique em **OK.**



Etapa 34. Altere o modelo SCEP padrão nas configurações do Registro em **Computador > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Criptografia > MSCEP**. Altere as chaves EncryptionTemplate, GeneralPurposeTemplate e SignatureTemplate de IPsec (Solicitação Offline) para o modelo WLC criado anteriormente.



Etapa 35. Reinicialize o sistema.

Configurar o WLC

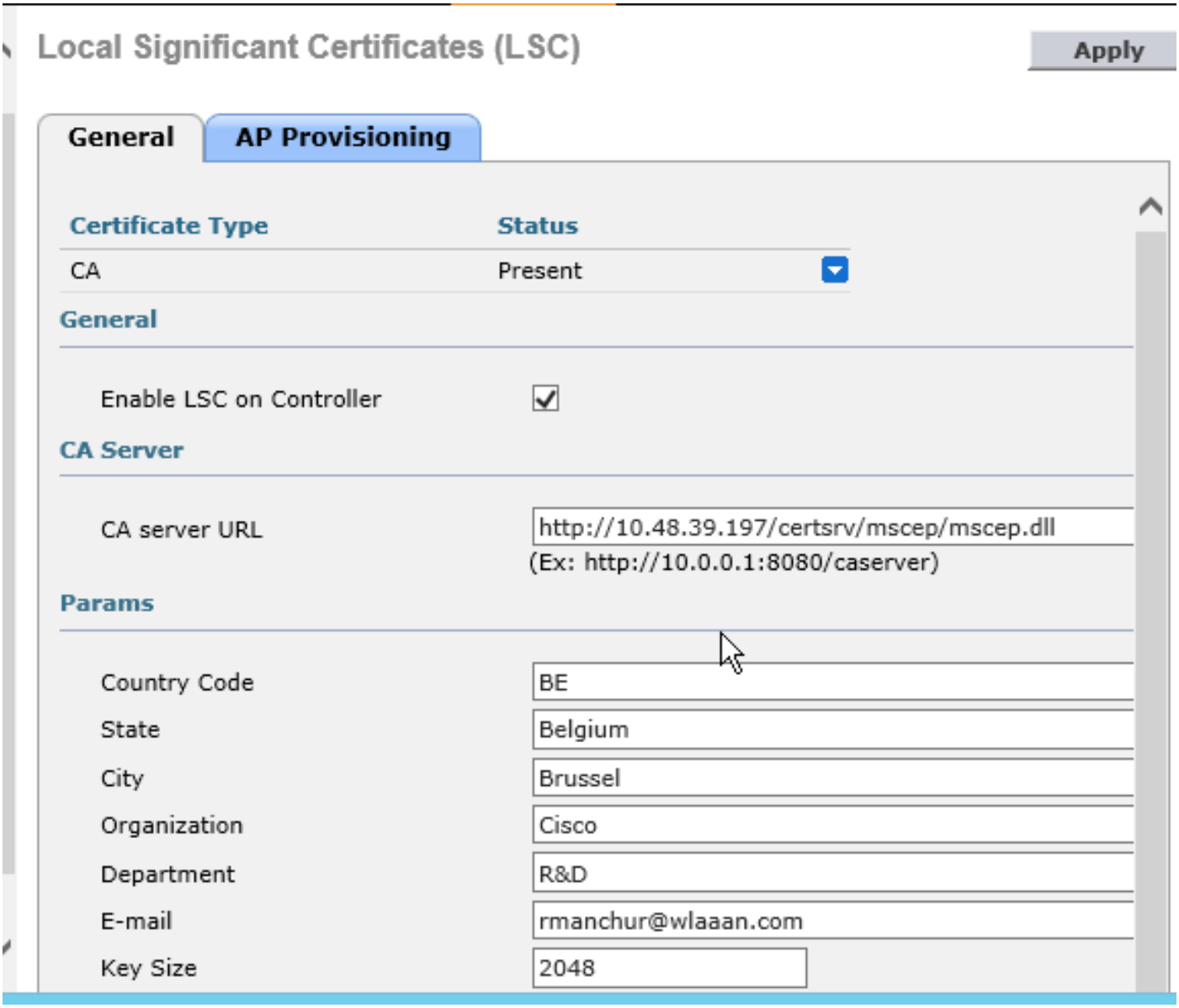
Etapa 1. Na WLC, navegue até o menu Security. Clique em **Certificados > LSC**.

Etapa 2. Marque a caixa de seleção **Enable LSC on Controller (Ativar LSC no controlador)**.

Etapa 3. Digite a URL do Microsoft Windows Server 2012. Por padrão, ele é anexado a **/certsrv/mscep/mscep.dll**.

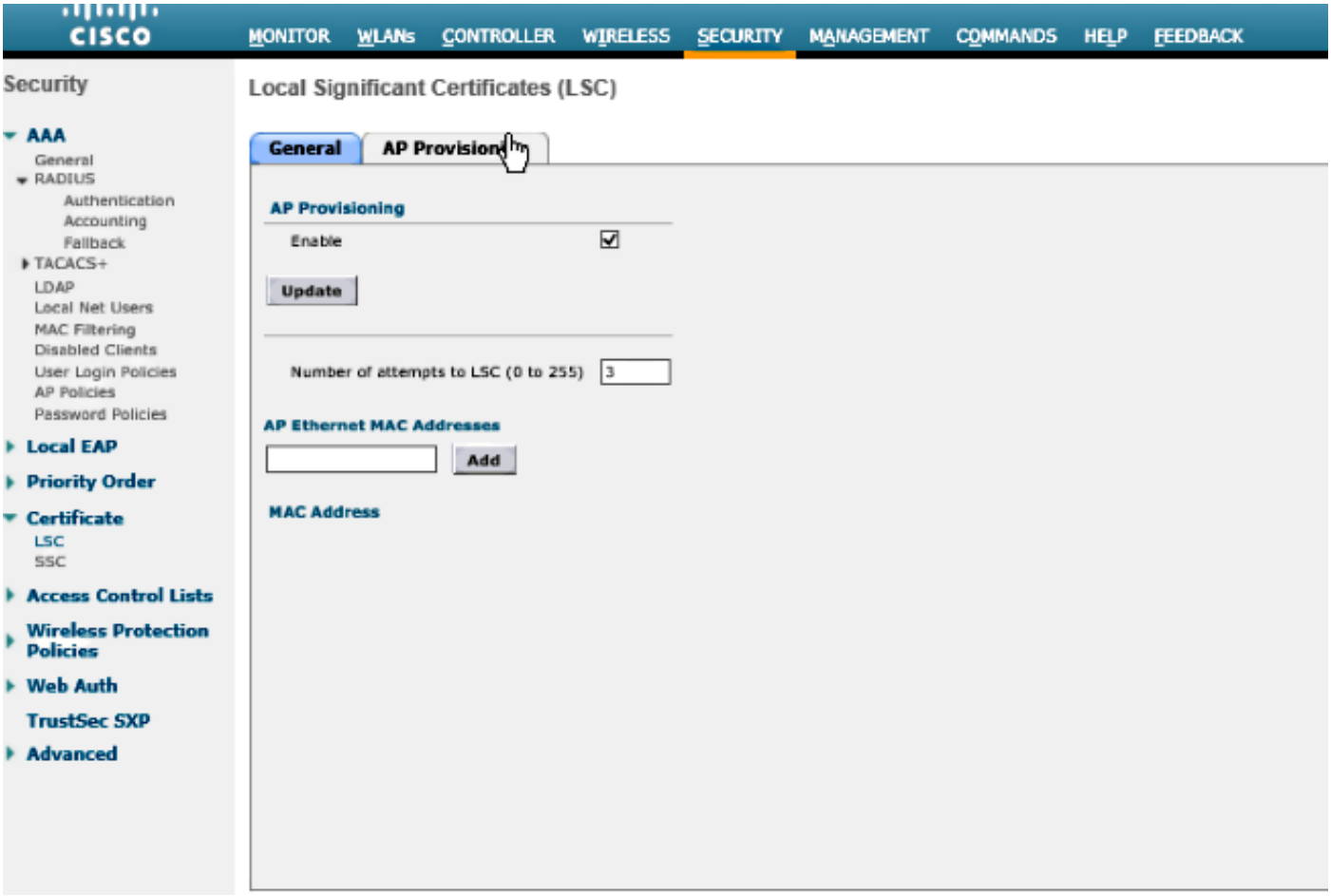
Etapa 4. Digite seus detalhes na seção **Params**.

Etapa 5. Aplique a alteração.



Etapa 6. Clique na seta azul na linha CA superior e escolha **Adicionar**. Ele deve alterar o status de **Não presente** para **presente**.

Passo 7. Clique na **guia Provisionamento de AP**.



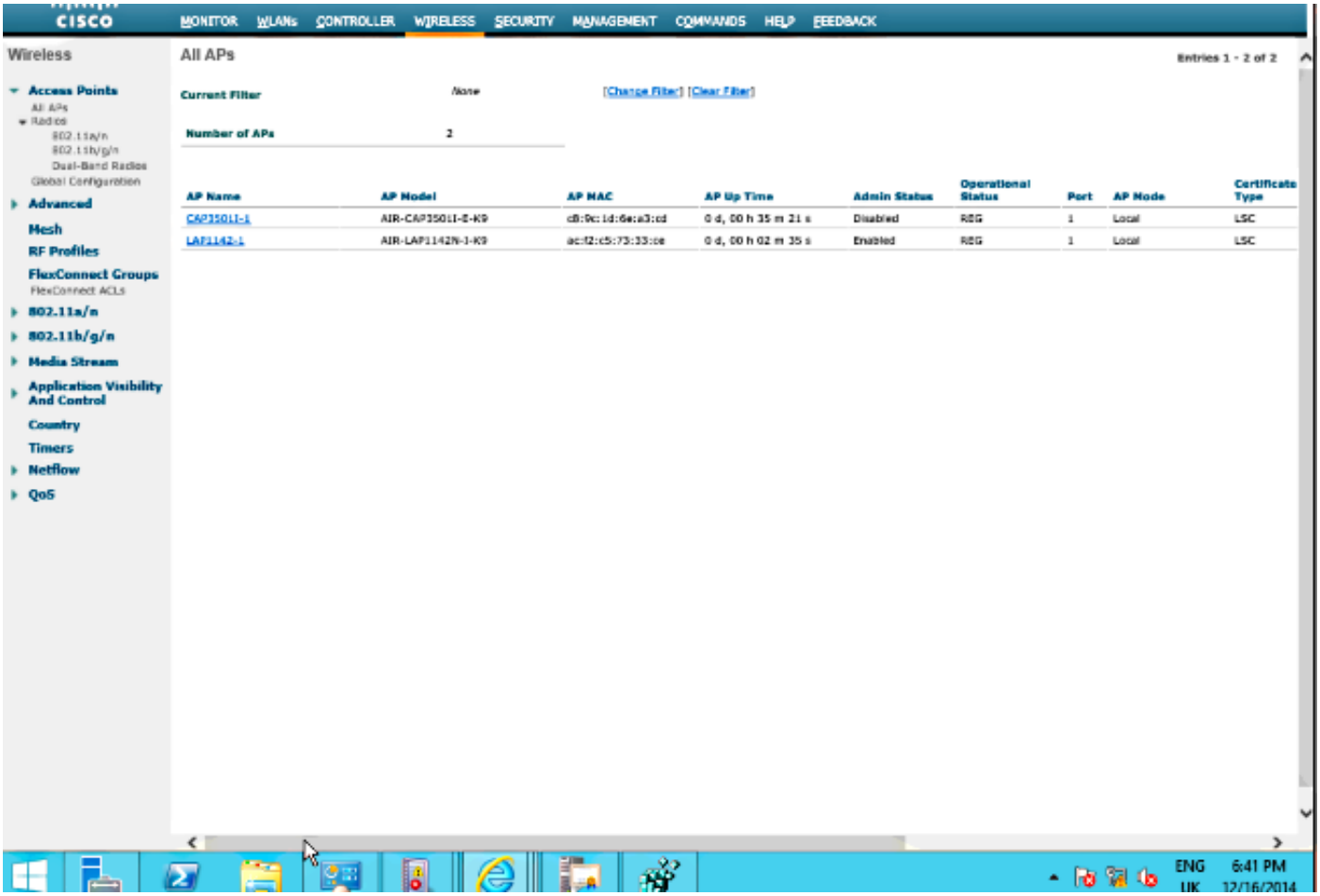
Etapa 8. Marque a caixa de seleção **Habilitar** em Provisionamento de AP e clique em **Atualizar**.

Etapa 9. Reinicialize seus pontos de acesso se eles não tiverem sido reinicializados.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

O ponto de acesso, após a reinicialização, se junta novamente e é exibido com o LSC como o tipo de certificado no menu Sem fio.



Note: Depois do 8.3.112, os APs MIC não podem se unir quando o LSC estiver ativado. Portanto, o recurso de contagem de "tentativas de LSC" torna-se de uso limitado.

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.