Ejemplo de Configuración de Certificados de Importancia Local (LSC) con WLC y Windows Server 2012

Contenido

Introducción

Este documento describe cómo configurar certificados de significación local (LSC) con un controlador de LAN inalámbrica (WLC) y un Microsoft Windows Server 2012 R2 recientemente instalado.

> **Nota:** Las implementaciones reales pueden diferir en muchos puntos y debería tener un control y un conocimiento completos de los ajustes de Microsoft Windows Server 2012. Este ejemplo de configuración sólo se proporciona como una plantilla de referencia para que los clientes de Cisco implementen y adapten su configuración de Microsoft Windows Server para que LSC funcione.

Prerequisites

Requirements

Cisco recomienda que comprenda todos los cambios realizados en Microsoft Windows Server y compruebe la documentación pertinente de Microsoft si es necesario.

> **Nota:** El LSC en el WLC no es soportado con el intermedio-CA, ya que la CA raíz se perderá del WLC ya que el controlador sólo obtiene la CA intermedia.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- WLC versión 7.6
- Microsoft Windows Server 2012 R2

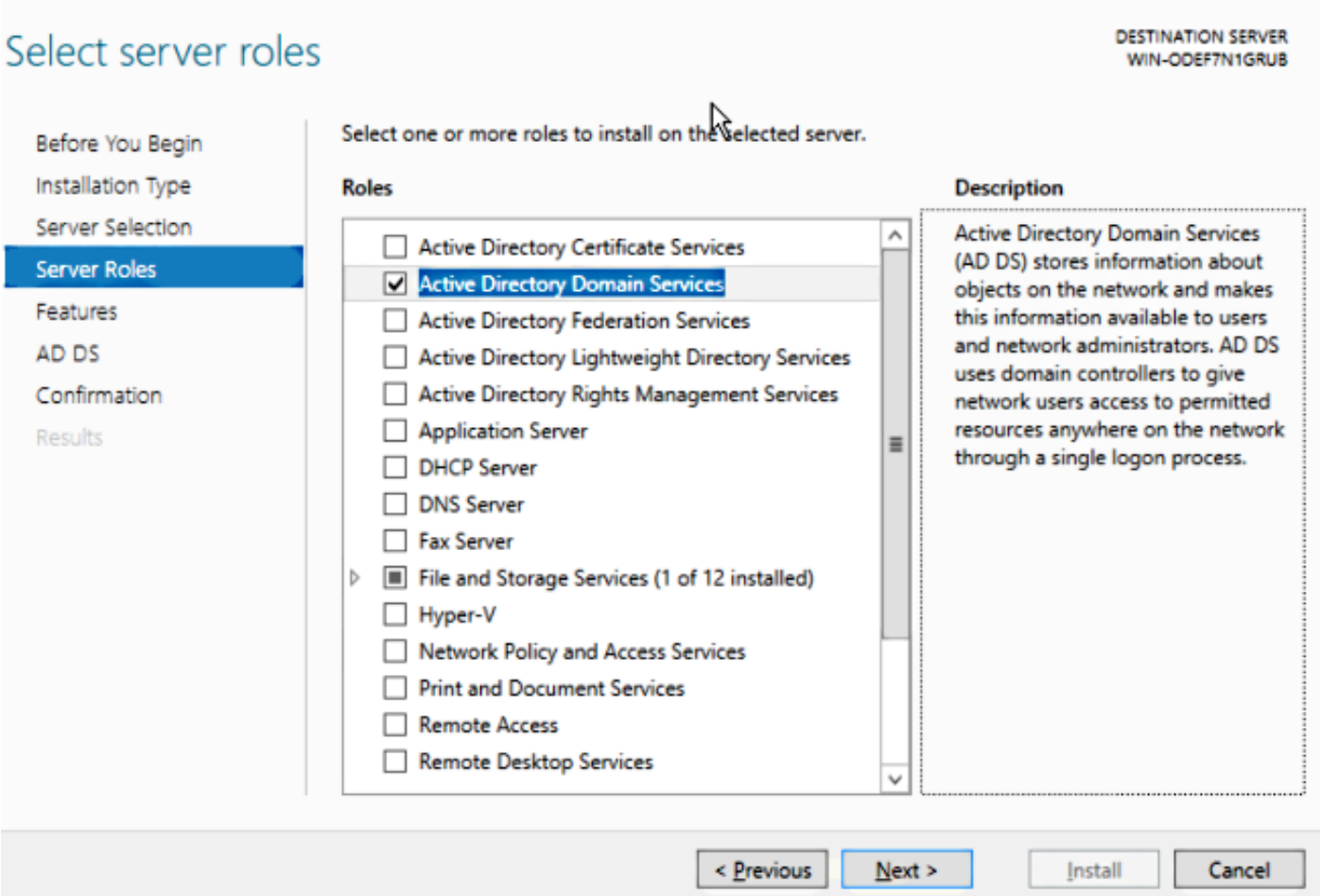
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurar

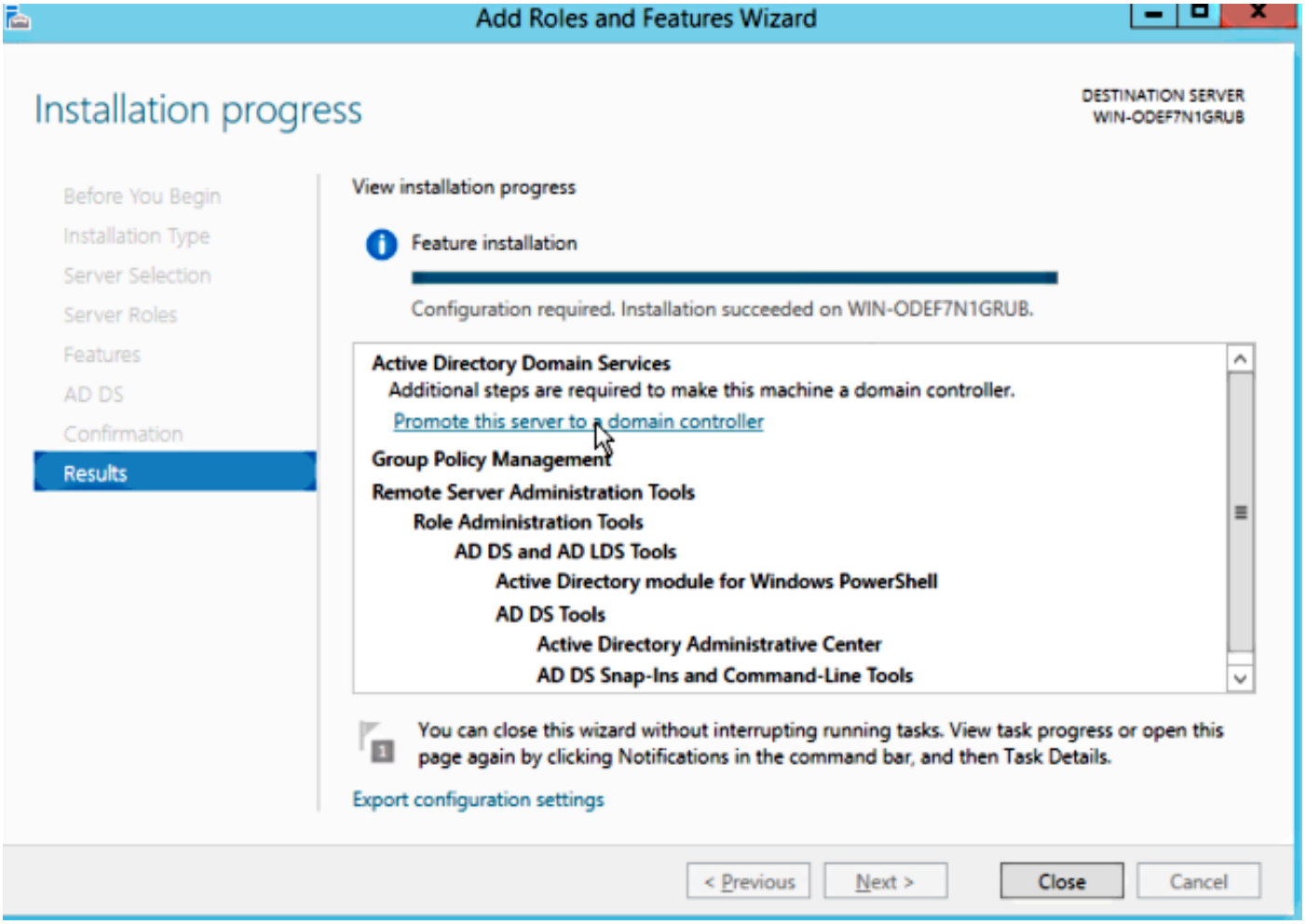
Configuración de Microsoft Windows Server

Esta configuración se muestra como realizada en un Microsoft Windows Server 2012 recientemente instalado. Debe adaptar los pasos a su dominio y a su configuración.

Paso 1. Instale los Servicios de dominio de Active Directory para el asistente de funciones y funciones.

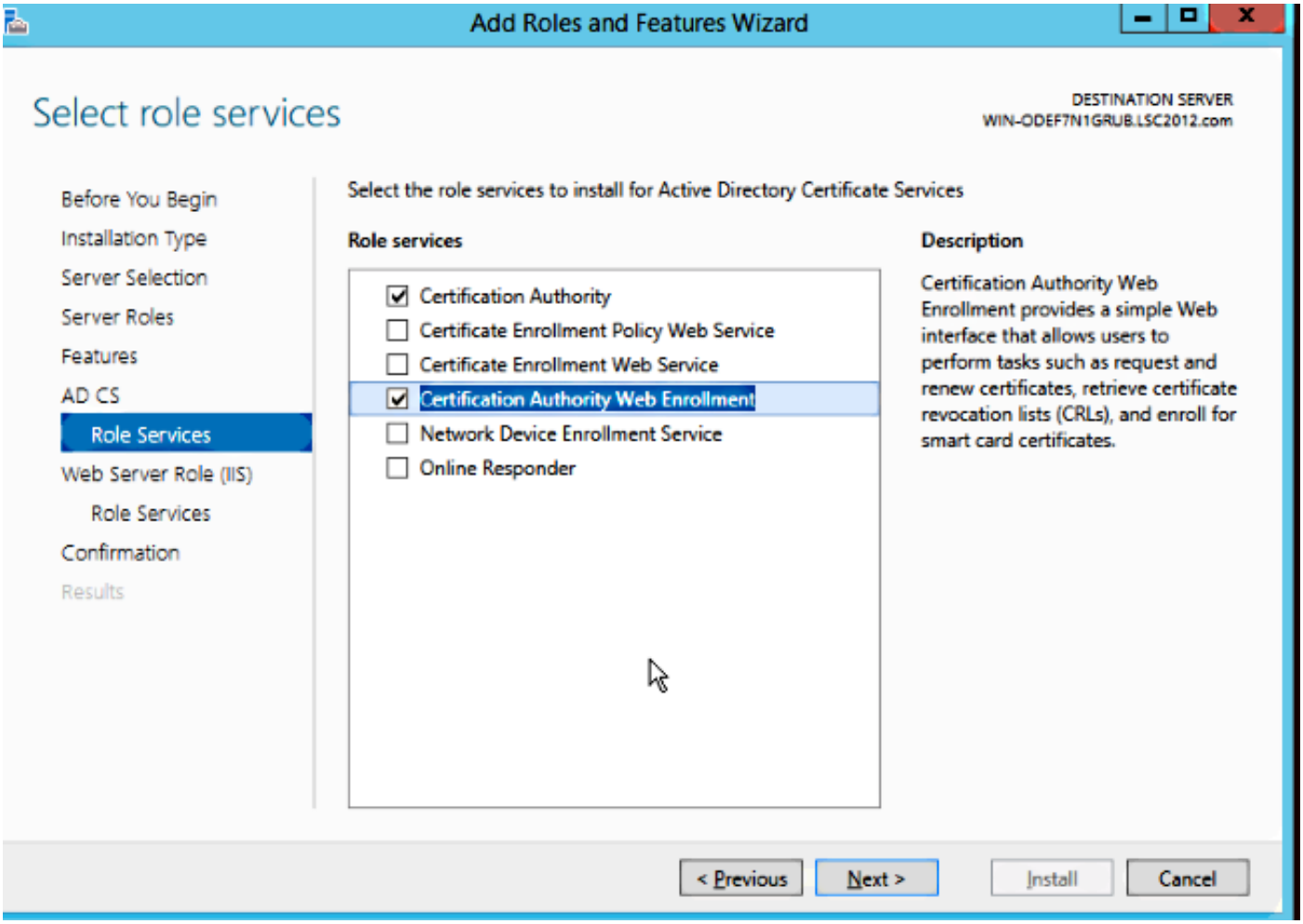


Paso 2. Después de la instalación, debe promocionar el servidor al controlador de dominio.

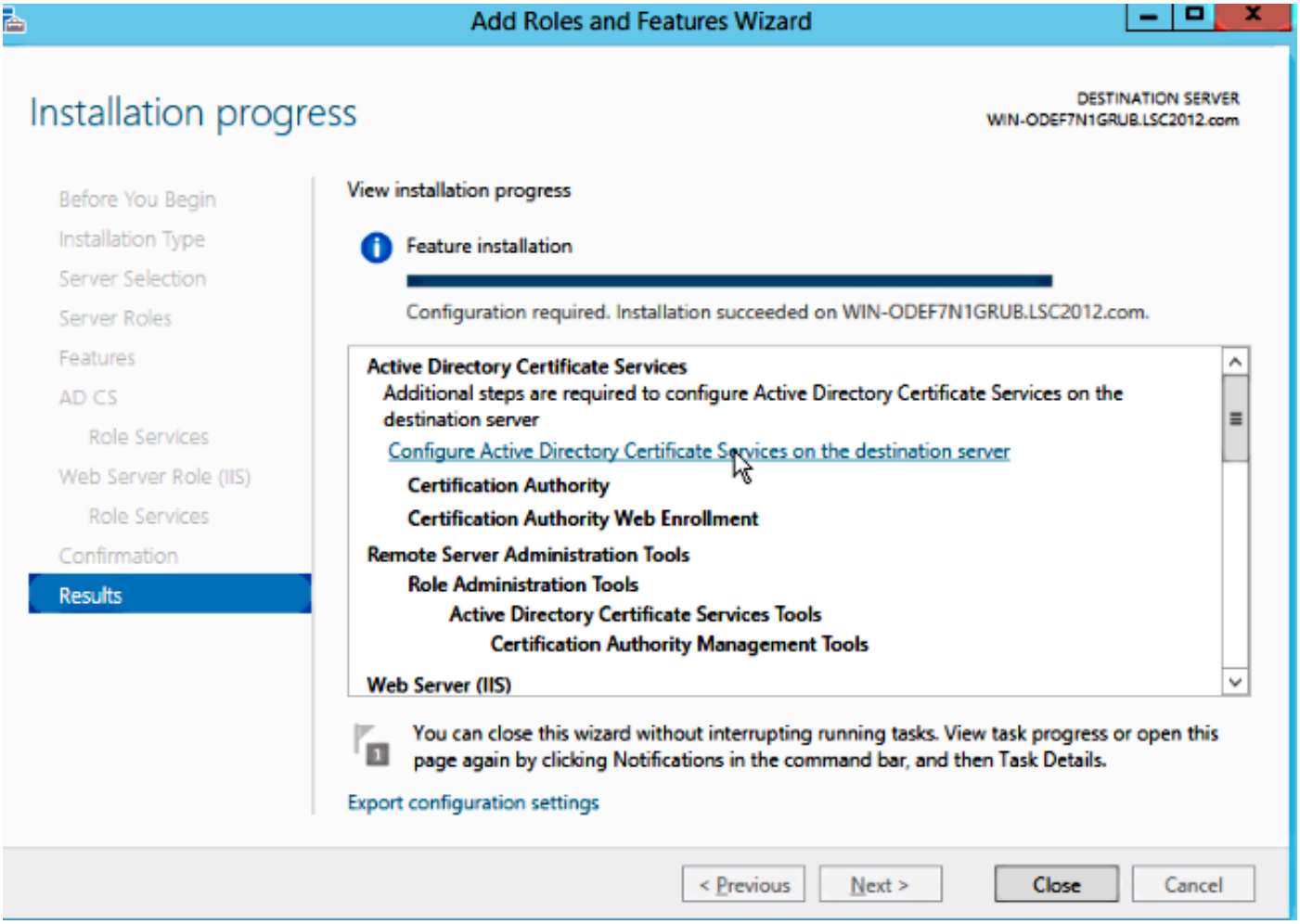


Paso 3. Dado que se trata de una nueva configuración, se configura un nuevo bosque; pero normalmente en implementaciones existentes, simplemente configure estos puntos en un controlador de dominio. Aquí, usted elige el dominio **LSC2012.com**. Esto también activa la función Servidor de nombres de dominio (DNS).

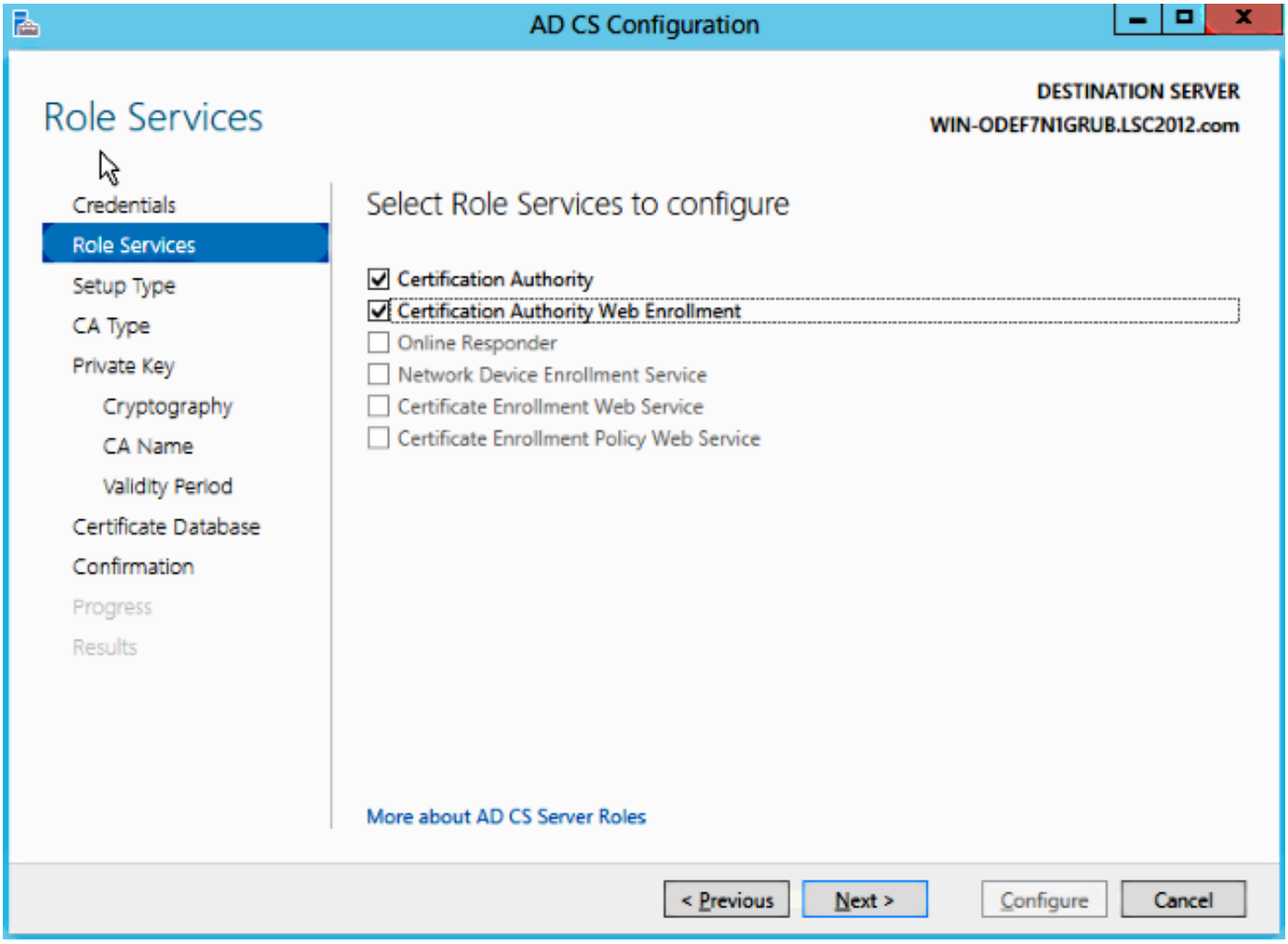
Paso 4. Después de reiniciar, instale el servicio de autoridad de certificados (CA) así como la inscripción en la Web.



Paso 5. Configure.



Paso 6. Elija Enterprise CA y deje todo como predeterminado.

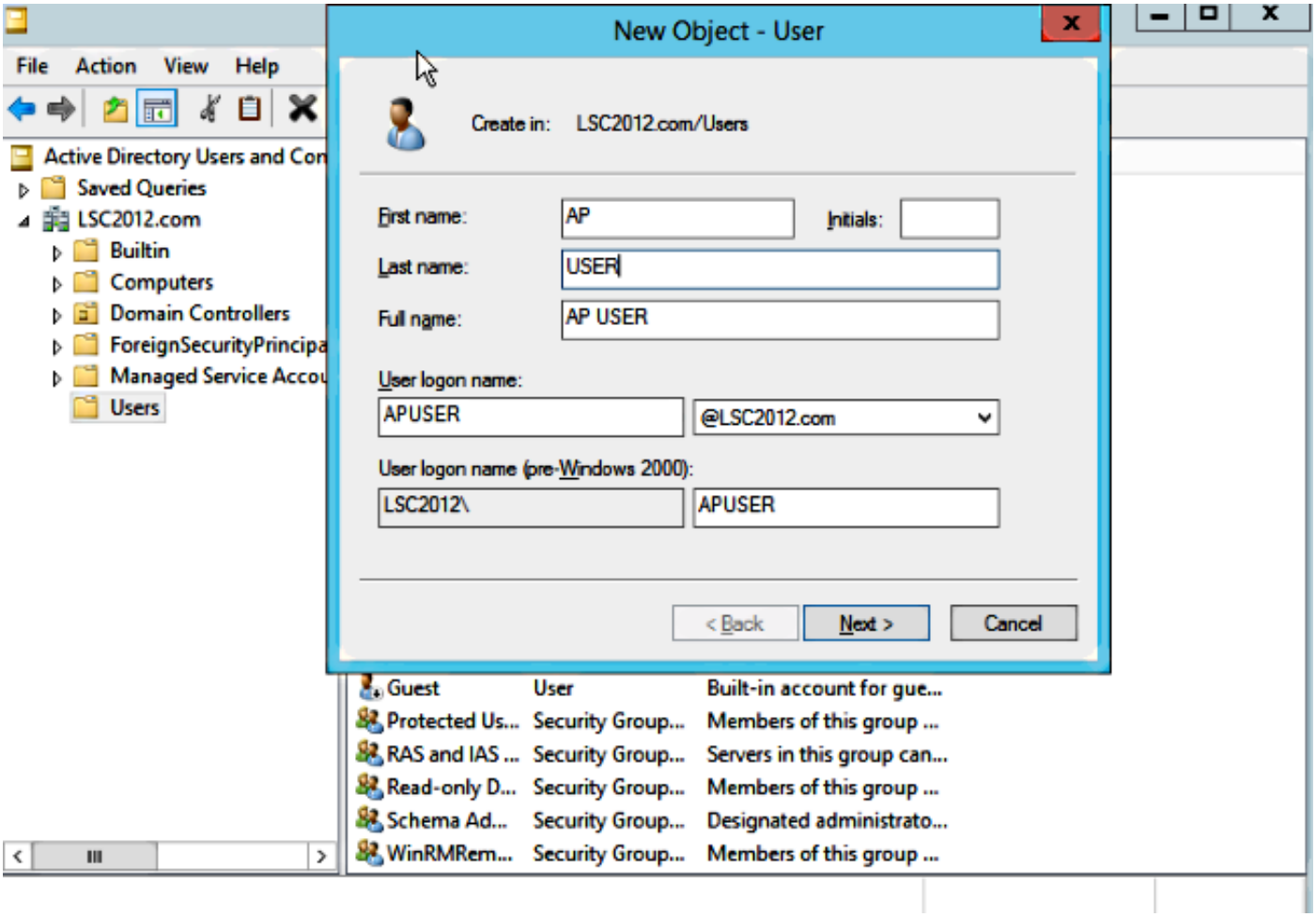


Paso 7. Haga clic en el **menú Microsoft Windows/Start**.

Paso 8. Haga clic en **Herramientas administrativas**.

Paso 9. Haga clic en Usuarios y equipos de Active Directory.

Paso 10. Expanda el dominio, haga clic con el botón derecho en la **carpeta Users** y elija **New Object > User**.



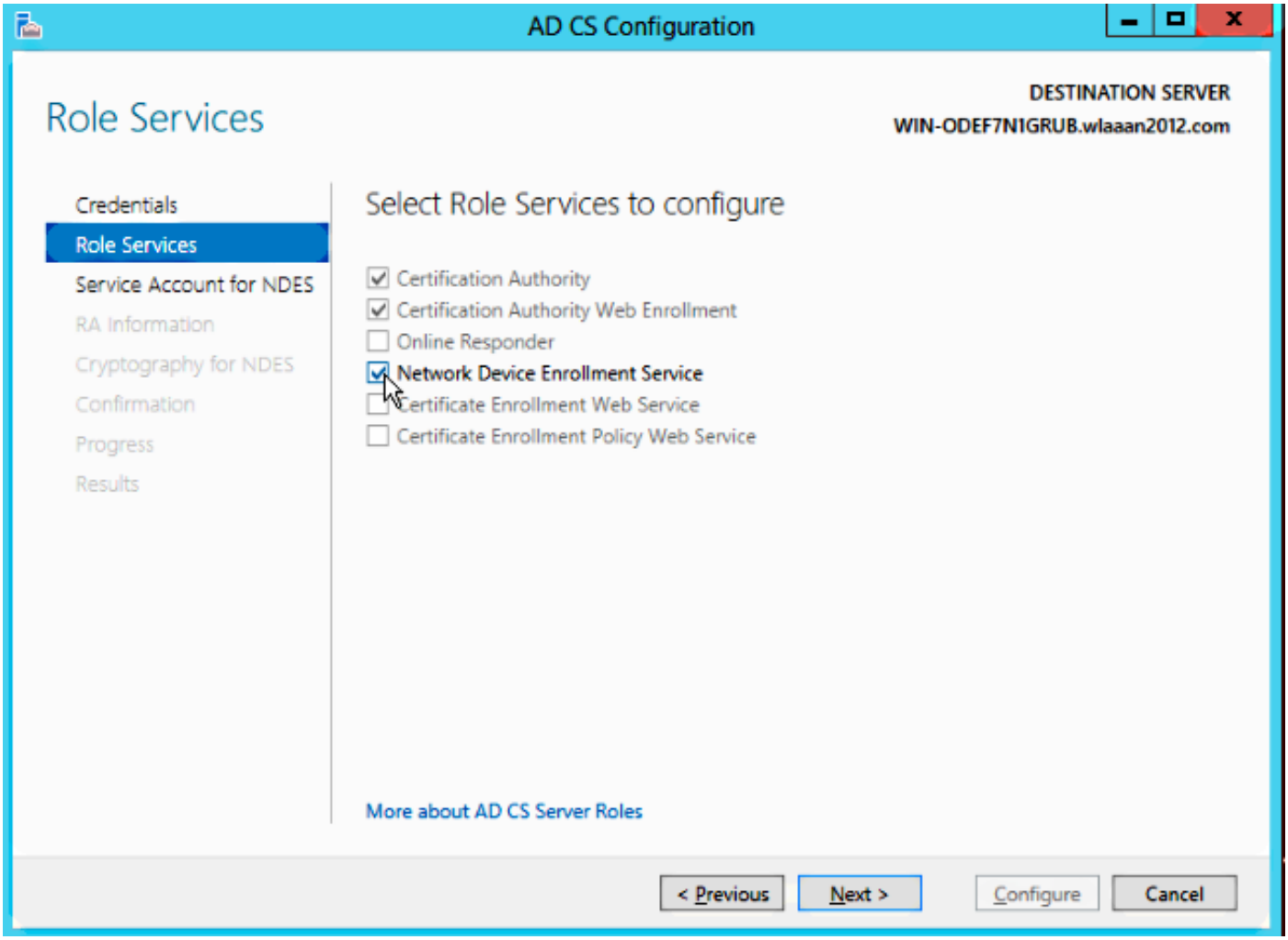
Paso 11. En este ejemplo, se denomina **APUSER**. Una vez creado, debe editar el usuario y hacer clic en la **ficha MemberOf**, y convertirlo en miembro del grupo IIS_IUSRS

Las asignaciones de derechos de usuario necesarias son:

- Permitir inicio de sesión localmente

- Inicie sesión como servicio

Paso 12. Instale el servicio de inscripción de dispositivos de red (NDES).



- Elija el miembro de cuenta del grupo IIS_USRS, **APUSER** en este ejemplo, como la cuenta de servicio para NDES.

Paso 13. Vaya a Administrative Tools (Herramientas administrativas).

Paso 14. Haga clic en **Servicios de Internet Information Server (IIS)**.

Paso 15. Expanda el **Servidor > Sitios > Sitio Web predeterminado > Cert Srv**.

Paso 16. Para mscep y **mscep_admin**, haga clic en **authentication**. Asegúrese de que la autenticación anónima esté habilitada.

Paso 17. Haga clic con el botón derecho del ratón en **autenticación de Windows** y elija **Proveedores**. Asegúrese de que NT LAN Manager (NTLM) sea el primero en la lista.

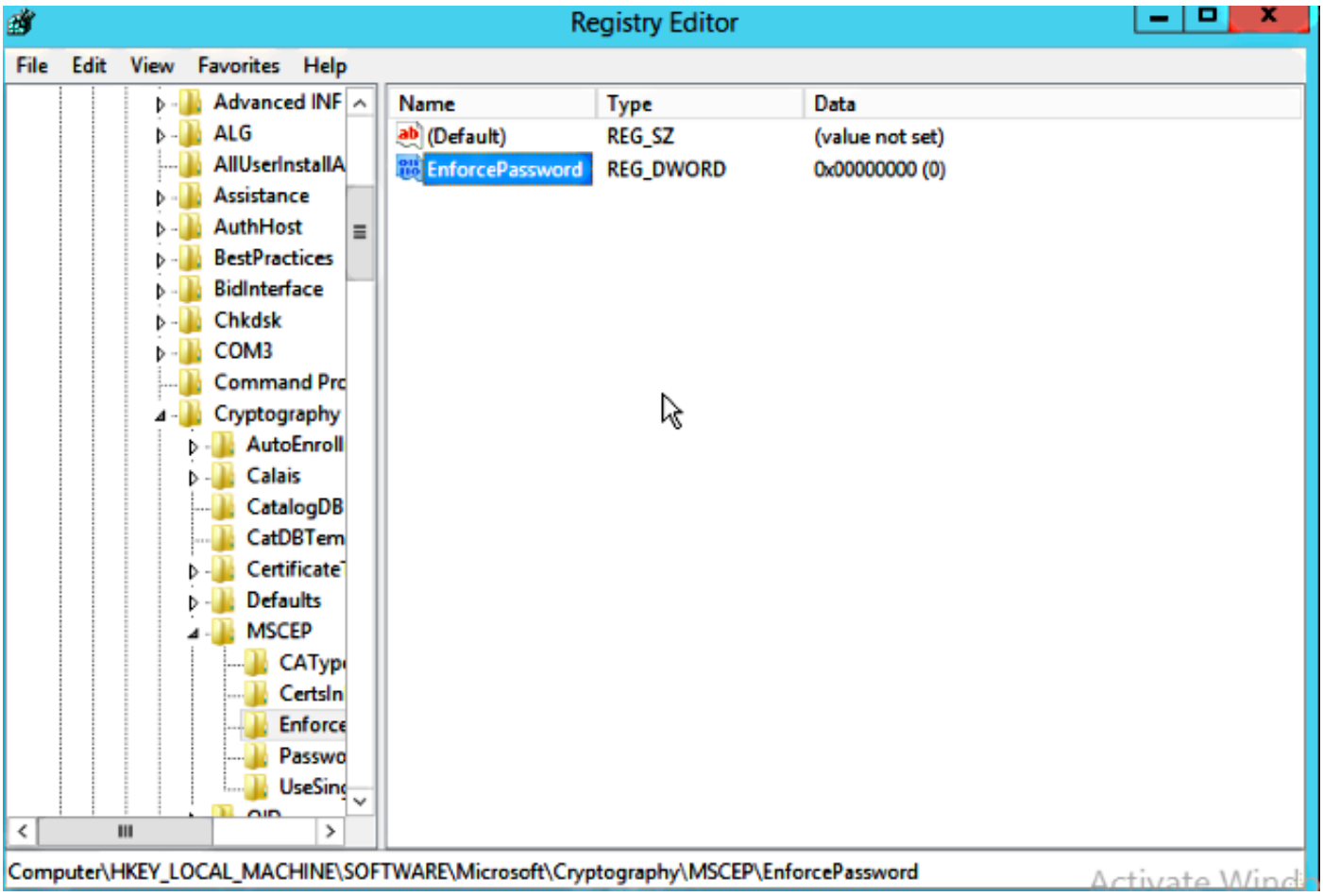
Paso 18. Inhabilite el desafío de autenticación en la configuración del Registro; de lo contrario, Simple Certificate Enrollment Protocol (SCEP) espera la autenticación de contraseña de desafío,

que no es compatible con el WLC.

Paso 19. Abra la **aplicación regedit**.

Paso 20. Vaya a **HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\Cryptography\MSCEP**.

Paso 21. Establezca EnforcePassword en **0**.



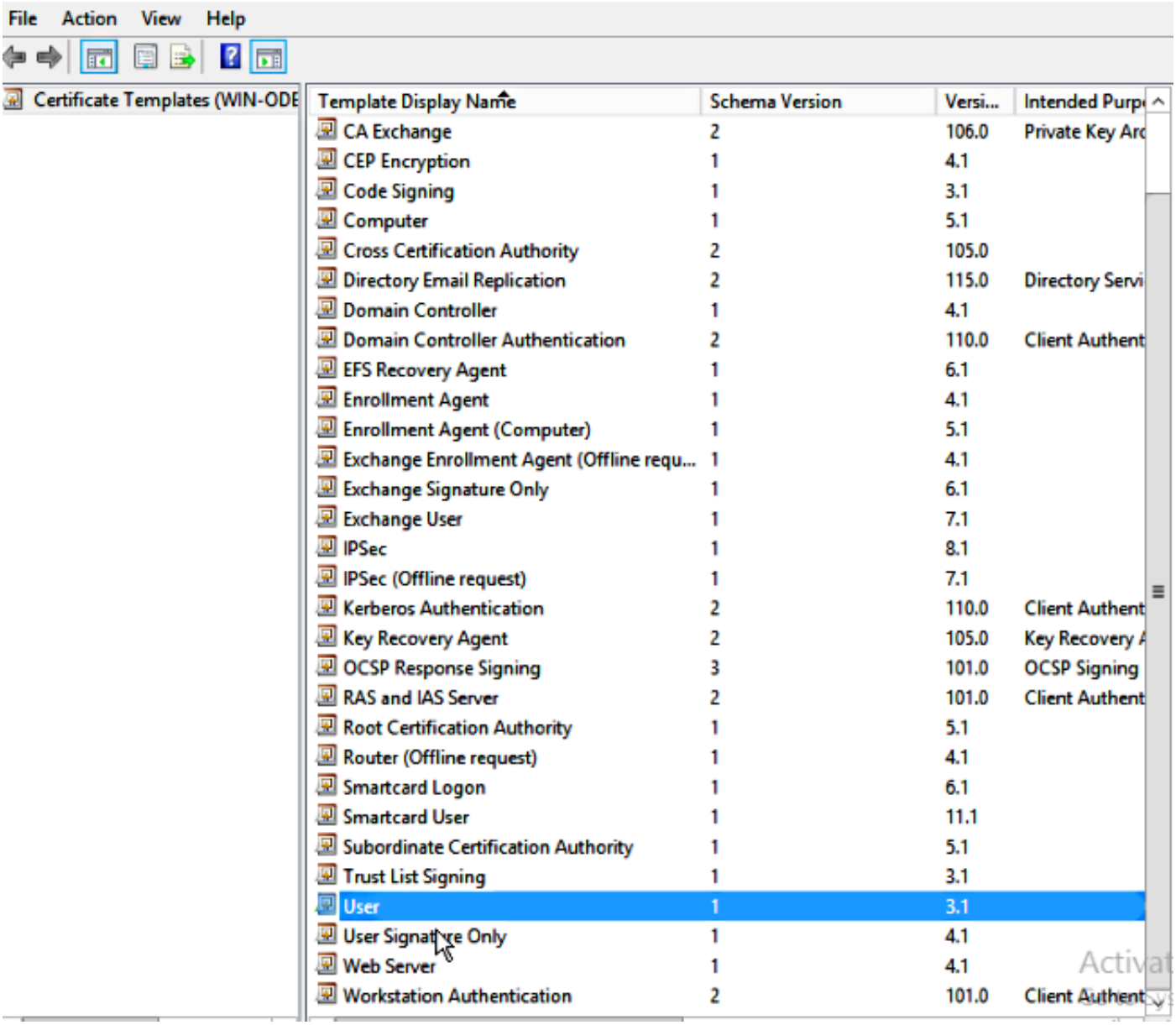
Paso 22. Haga clic en el **menú Microsoft Windows/Start**.

Paso 23. Escriba **MMC**.

Paso 24. En el menú Archivo, elija **Agregar o quitar complemento**. Elija **Autoridad de Certificación**.

Paso 25. Haga clic con el botón derecho en la **carpeta Plantilla de certificado** y haga clic en **Administrar**.

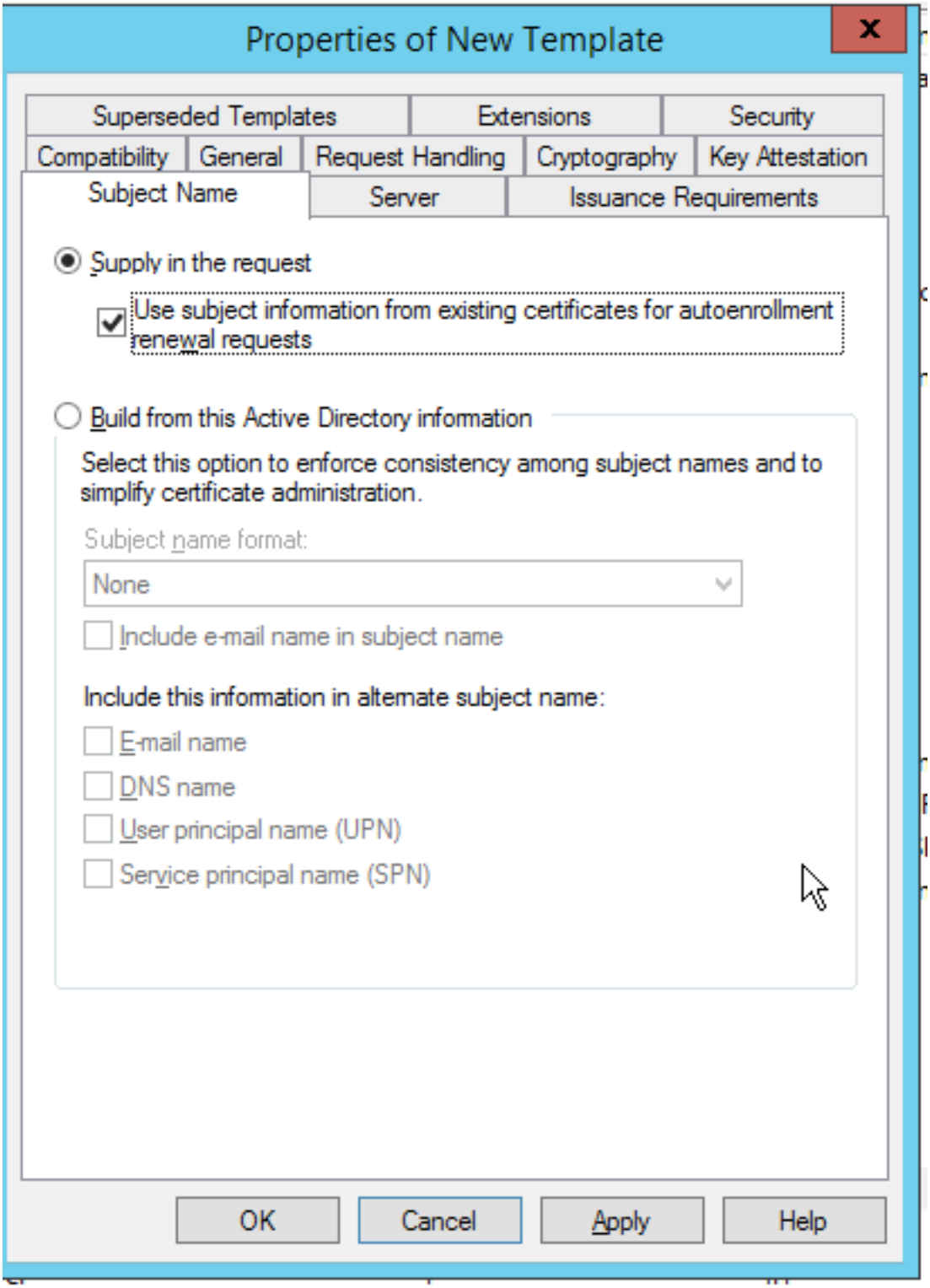
Paso 26. Haga clic con el botón derecho del ratón en una plantilla existente, como Usuario, y elija **Duplicar plantilla**.



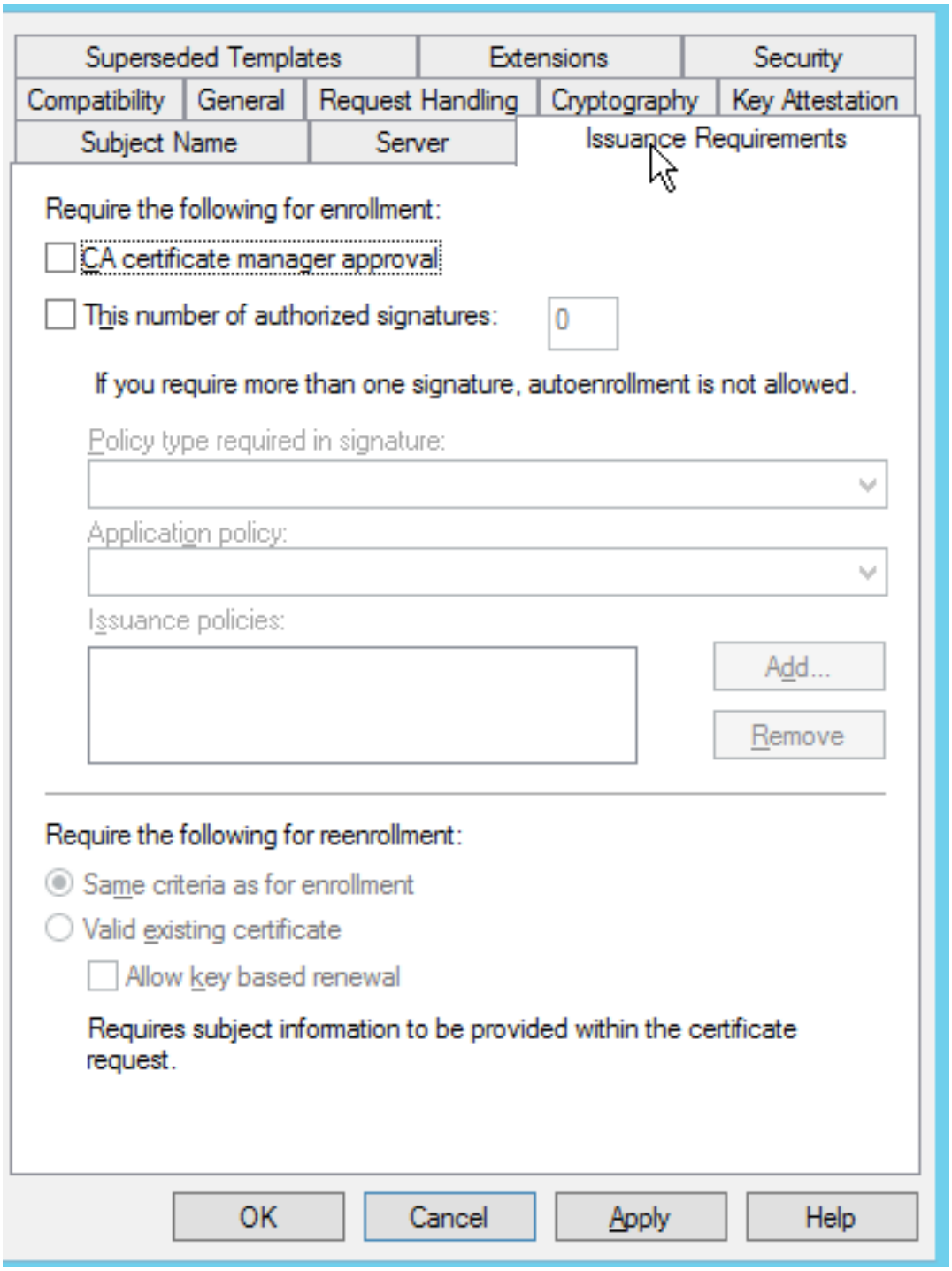
Paso 27. Elija la CA como Microsoft Windows 2012 R2.

Paso 28. En la ficha General, agregue un nombre de visualización como WLC y un período de validez.

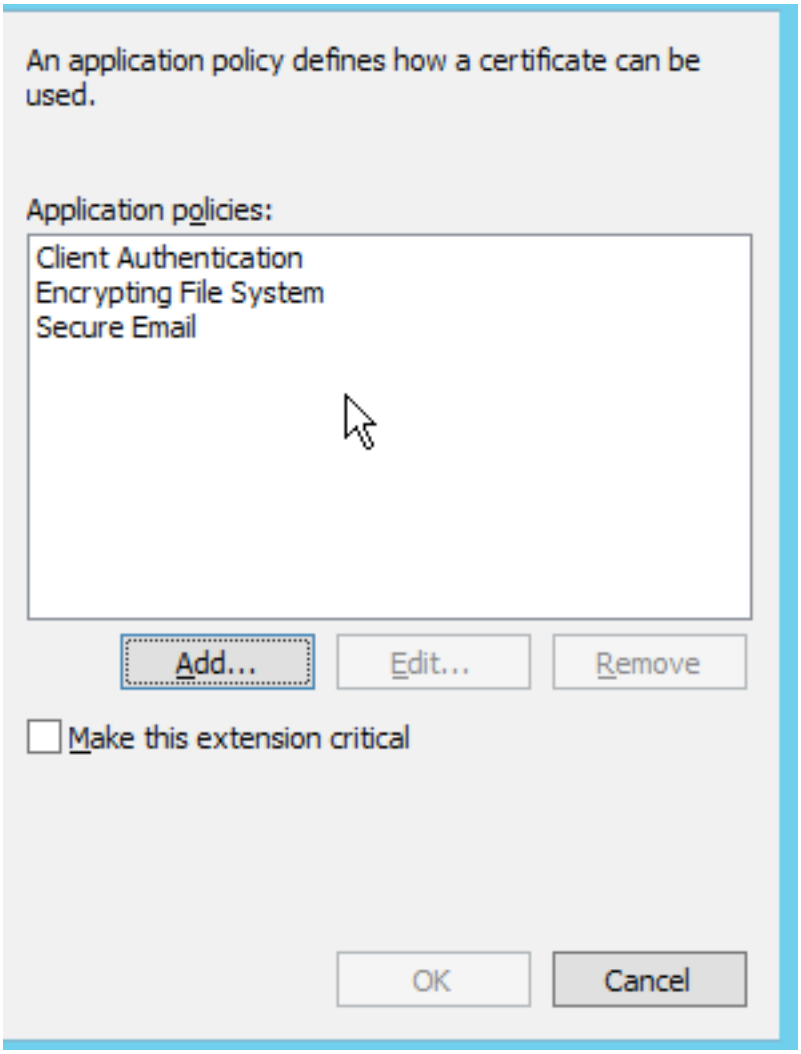
Paso 29. En la ficha Nombre del asunto, confirme que **se ha** seleccionado **Suministrar en la solicitud**.



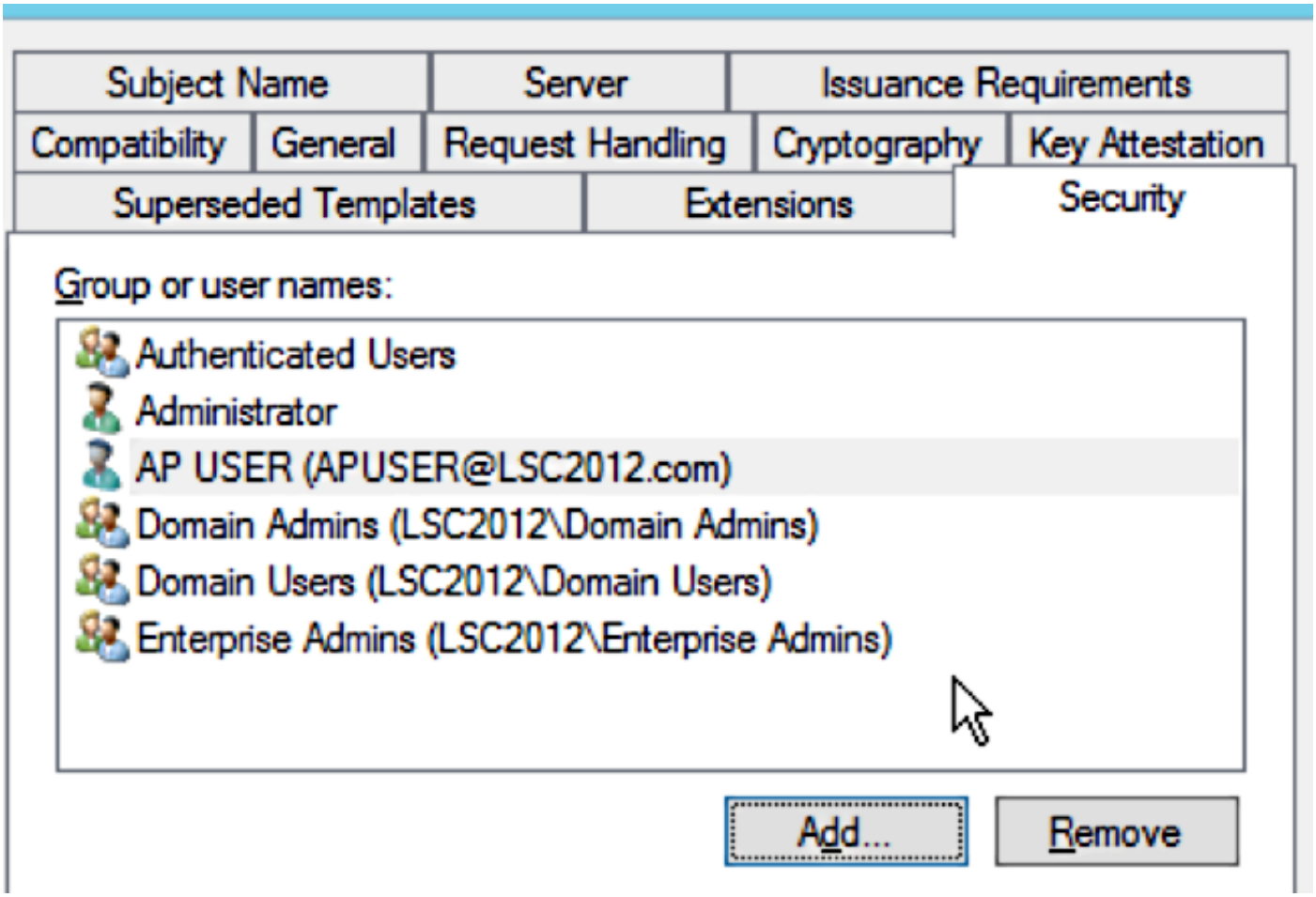
Paso 30. Haga clic en la pestaña **Requisitos de emisión**. Cisco recomienda dejar las políticas de emisión en blanco en un entorno de CA jerárquico típico:



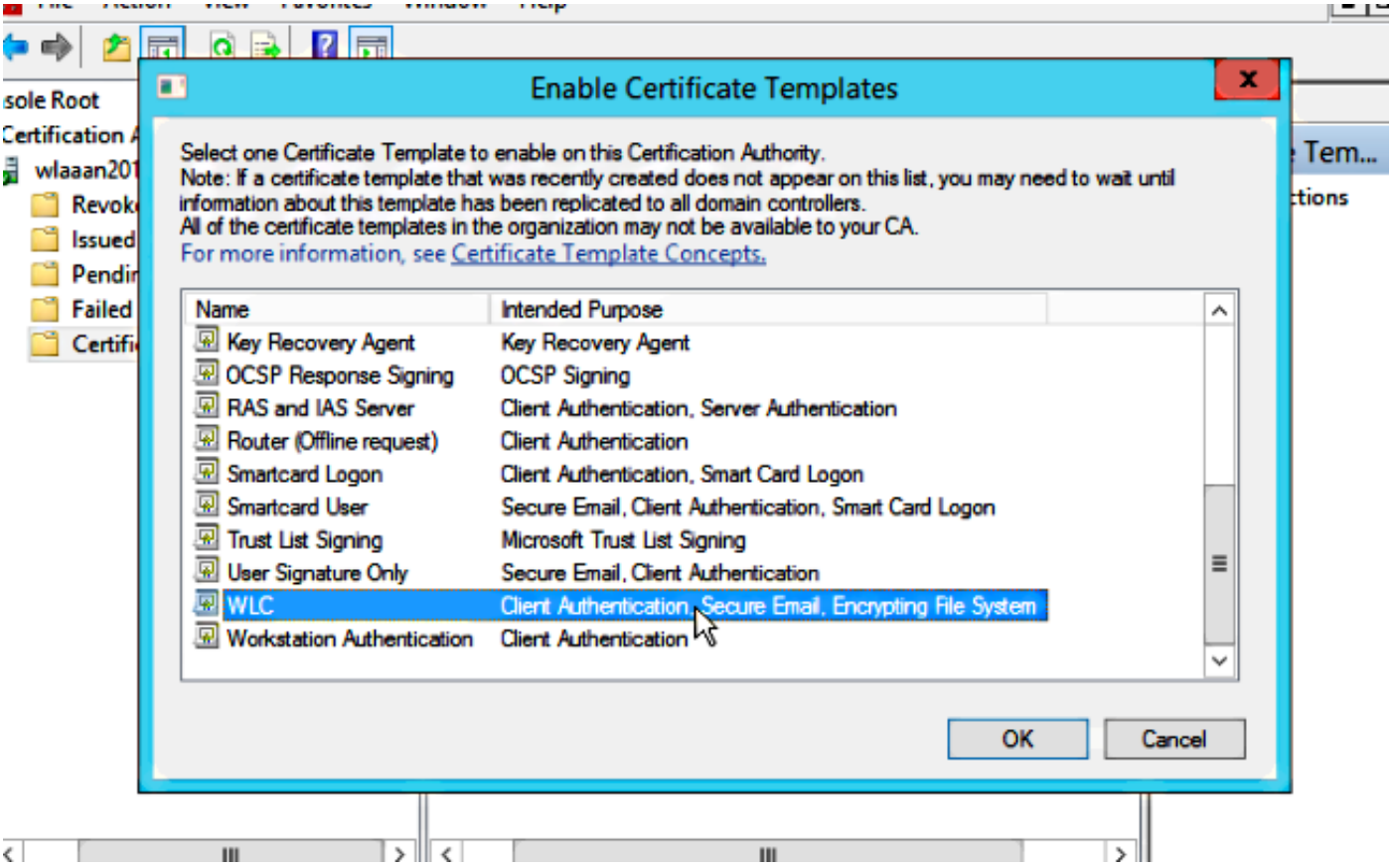
Paso 31. Haga clic en la ficha Extensiones, **Políticas de aplicación** y, a continuación, en **Editar**. Haga clic en **Agregar** y asegúrese de que la autenticación de cliente se agrega como política de aplicación. Click OK.



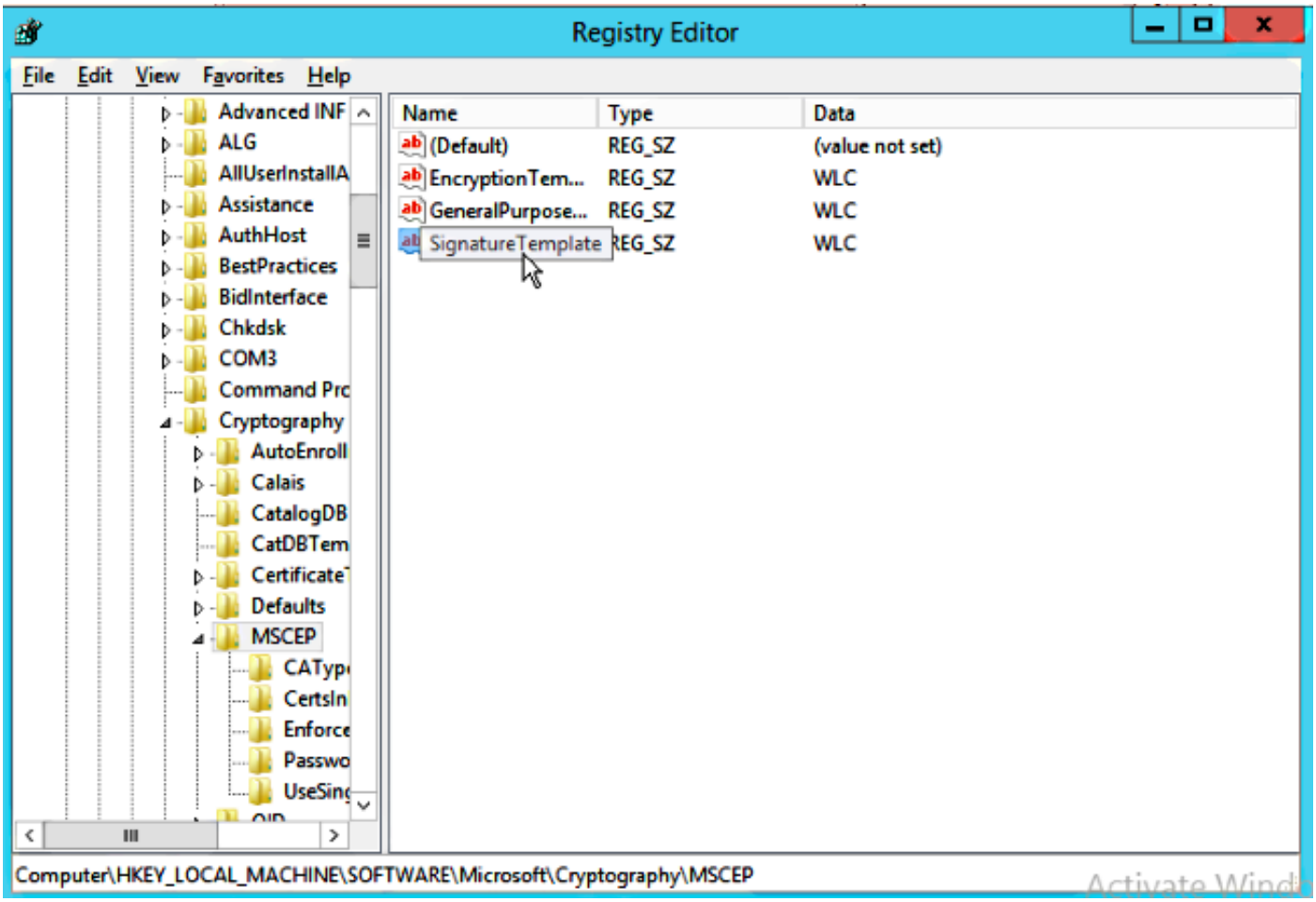
Paso 32. Haga clic en la **ficha Seguridad** y, a continuación, haga clic en **Agregar...**. Asegúrese de que la cuenta de servicio SCEP definida en la instalación del servicio NDES tenga control total de la plantilla y haga clic en **Aceptar**.



Paso 33. Vuelva a la interfaz gráfica de usuario de Certification Authority. Haga clic con el botón derecho del ratón en el **directorio Plantillas de certificado**. Vaya a **New > Certificate Template para emitir**. Seleccione la plantilla WLC configurada previamente y haga clic en **Aceptar.**



Paso 34. Cambie la plantilla SCEP predeterminada en la configuración del Registro en **Equipo > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Criptografía > MSCEP**. Cambie las claves EncryptionTemplate, GeneralPurposeTemplate y SignatureTemplate de IPsec (solicitud sin conexión) a la plantilla WLC creada anteriormente.



Paso 35. Reinicie el sistema.

Configurar la WLC

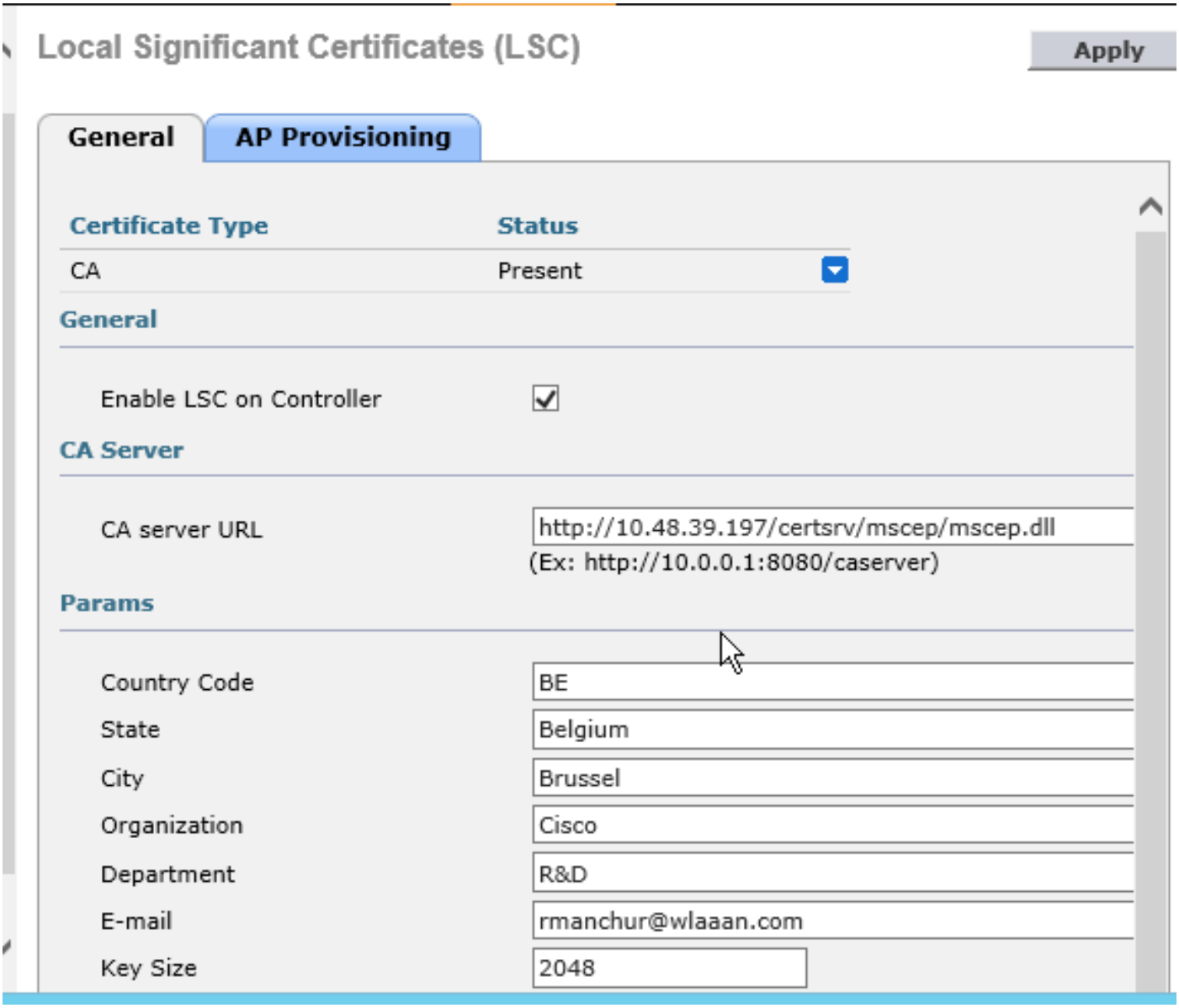
Paso 1. En el WLC, navegue al menú Security . Haga clic en **Certificados > LSC**.

Paso 2. Marque la casilla **Enable LSC on Controller**.

Paso 3. Introduzca la URL de Microsoft Windows Server 2012. De forma predeterminada, se agrega con **/certsrv/mscep/mscep.dll**.

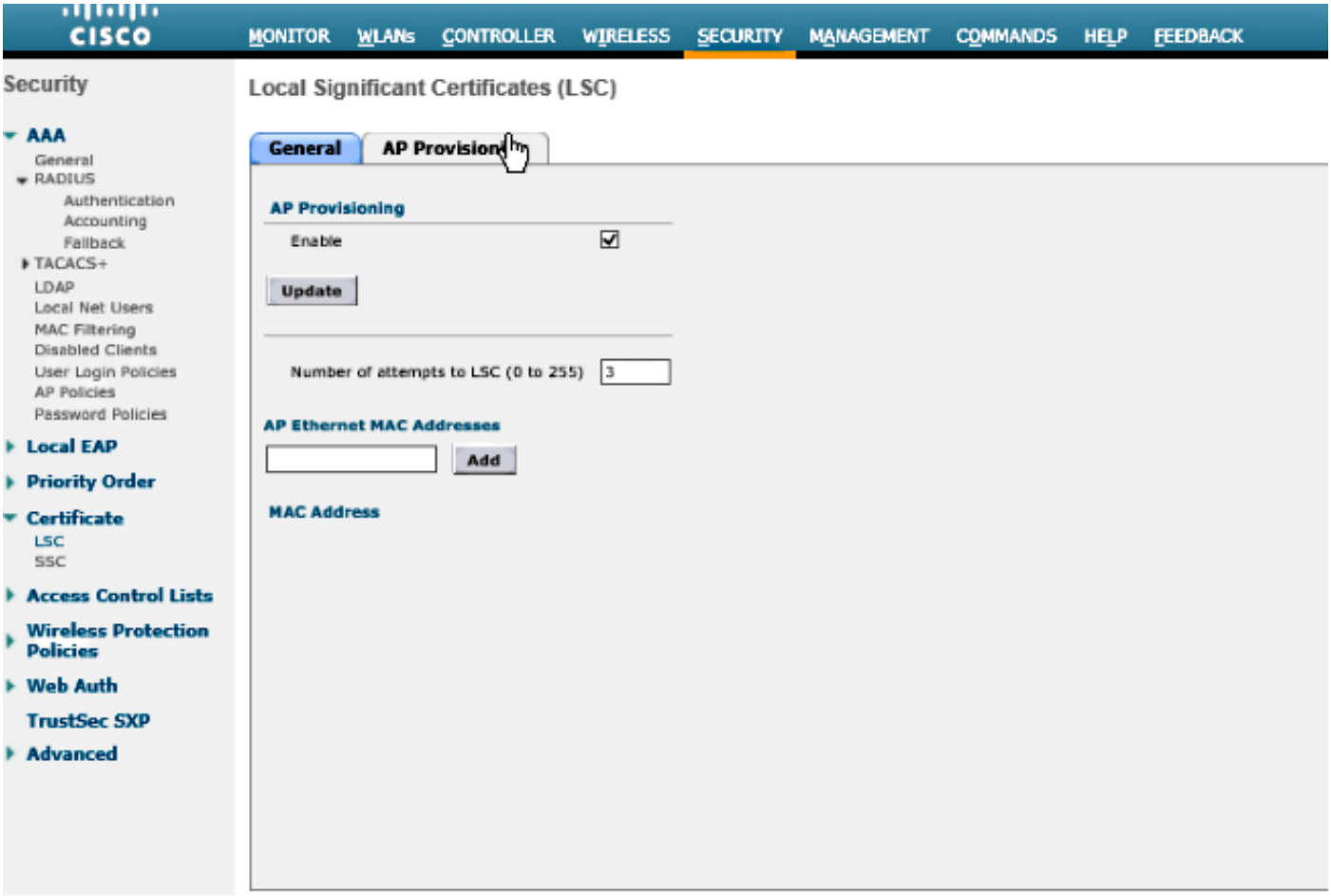
Paso 4. Introduzca sus detalles en la sección **Params**.

Paso 5. Aplique el cambio.



Paso 6. Haga clic en la flecha azul de la línea CA superior y elija **Agregar**. Debería cambiar el estado de **No presente** a **presente**.

Paso 7. Haga clic en la **pestaña AP provisioning**.



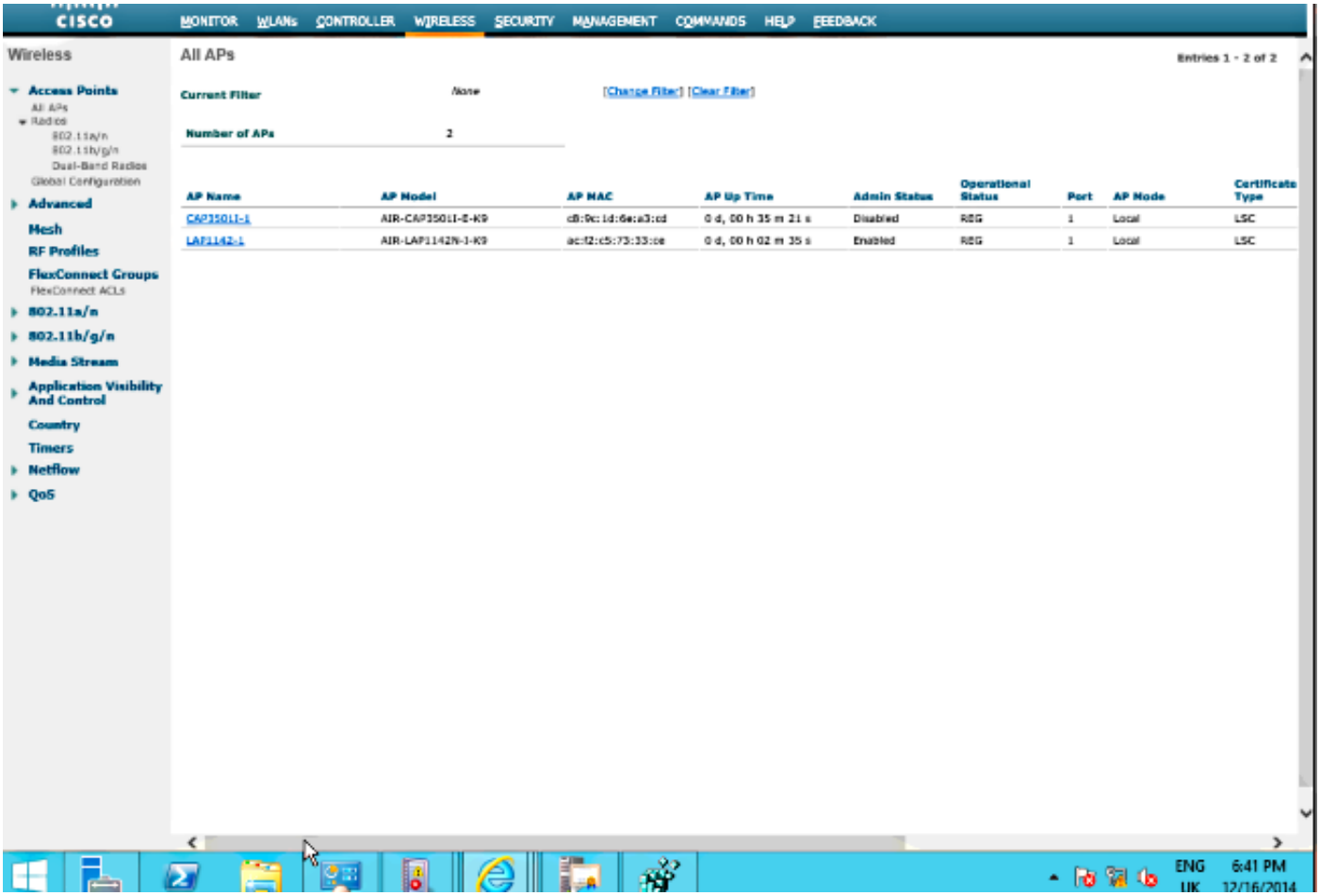
Paso 8. Marque la casilla de verificación **Enable** bajo AP Provisioning y haga clic en **Update**.

Paso 9. Reinicie los puntos de acceso si no se han reiniciado.

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

El punto de acceso, después de reiniciar, se une y se muestra con LSC como el tipo de certificado en el menú Inalámbrico.



Nota: Después de 8.3.112, los AP MIC no pueden unirse en absoluto una vez que LSC está habilitado. Por lo tanto, la función de recuento de "intentos de LSC" se vuelve de uso limitado.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.