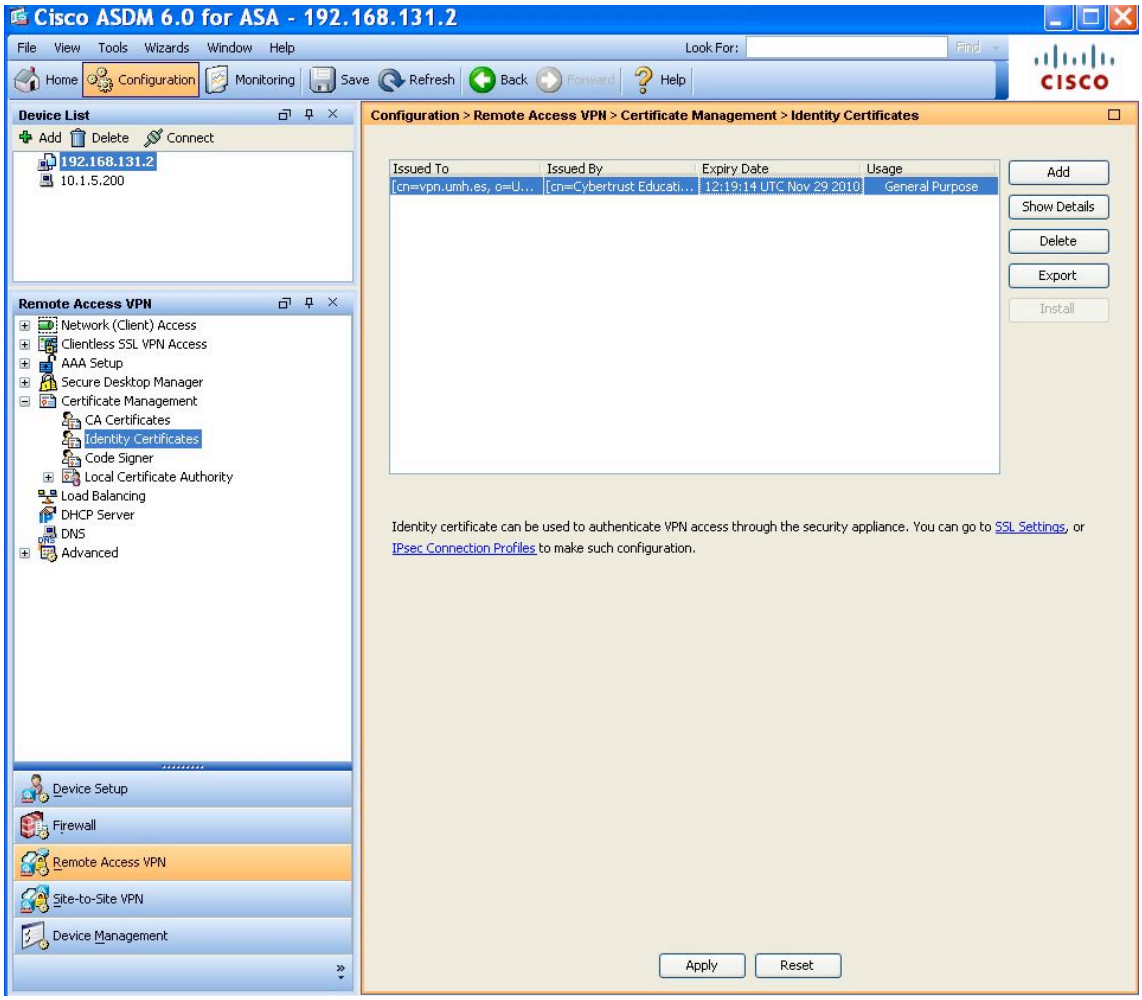
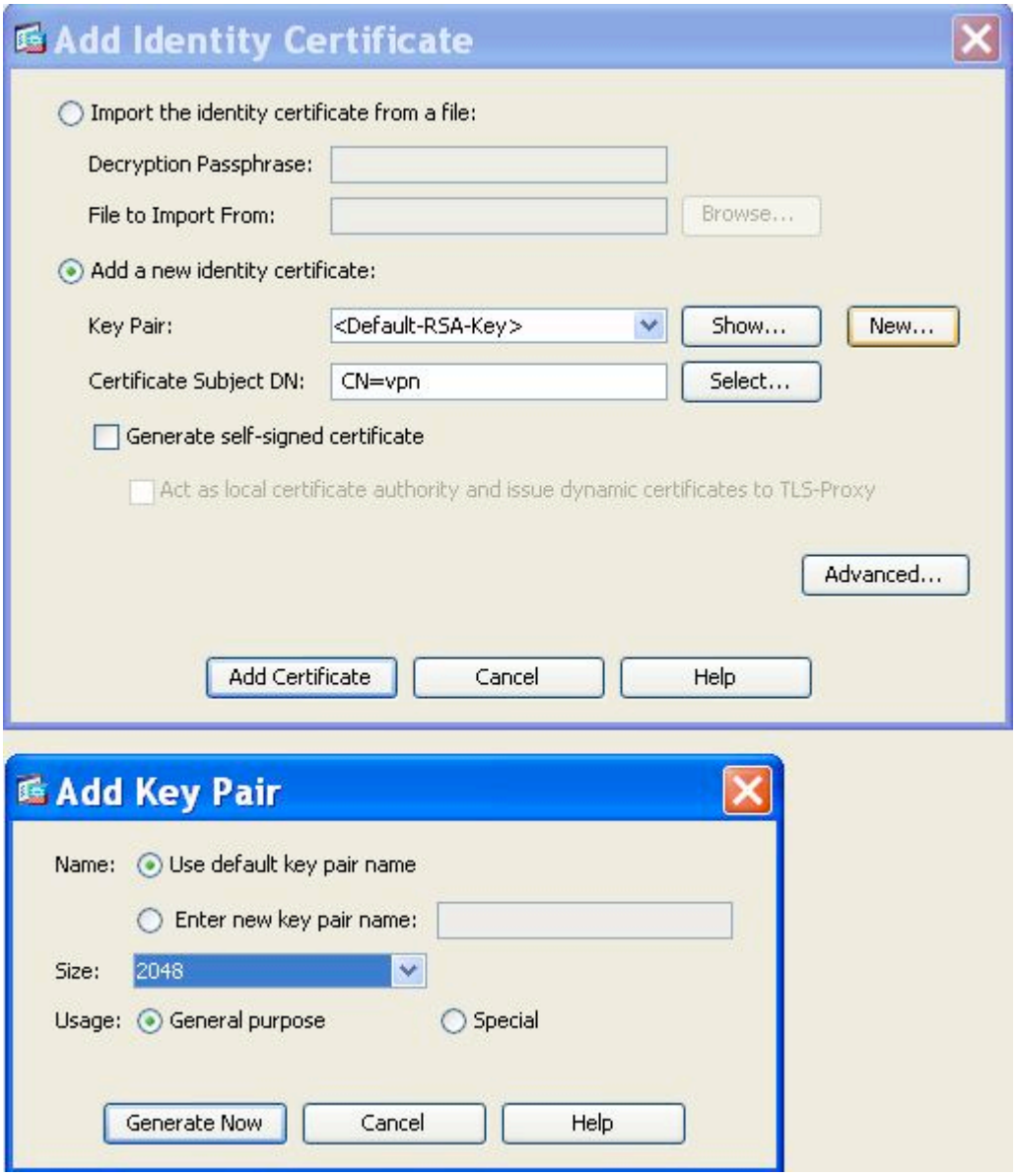
GUIA BÁSICA DE GENERACIÓN E INSTALACIÓN DE CERTIFICADOS PARA ASA 8.0

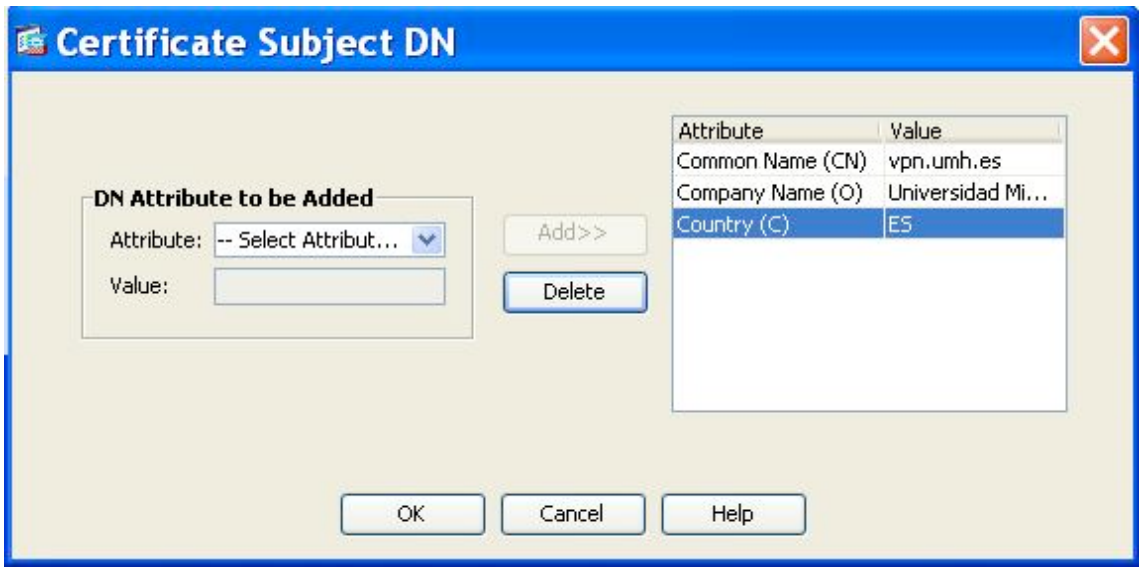
1.- Debemos utilizar la utilidad de administración ADSM, en este caso se ha utilizado la versión 6.0, una vez que hayamos entrado en la utilidad debemos seleccionar Configuration->Remote Access VPN->Identity Certificates



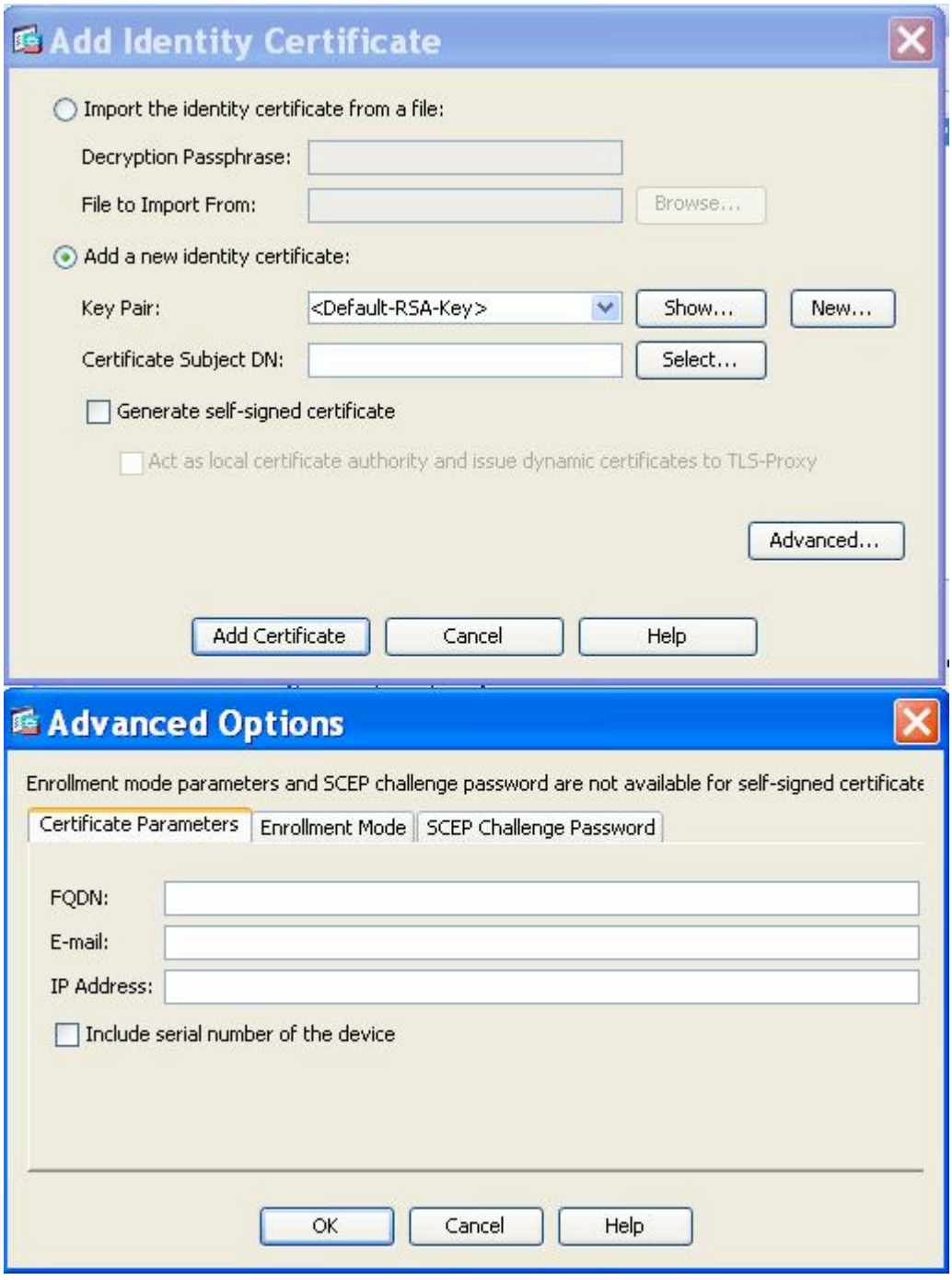
2.- Añadimos un nuevo certificado de identidad, para ello debemos previamente generar la clave pública y privada fijándonos que la clave sea de uso general y que el tamaño sea de 2048 bits



3.- A continuación debemos generar el Subject DN incluyendo los atributos CN,O y C para el servicio que proporciona redIris

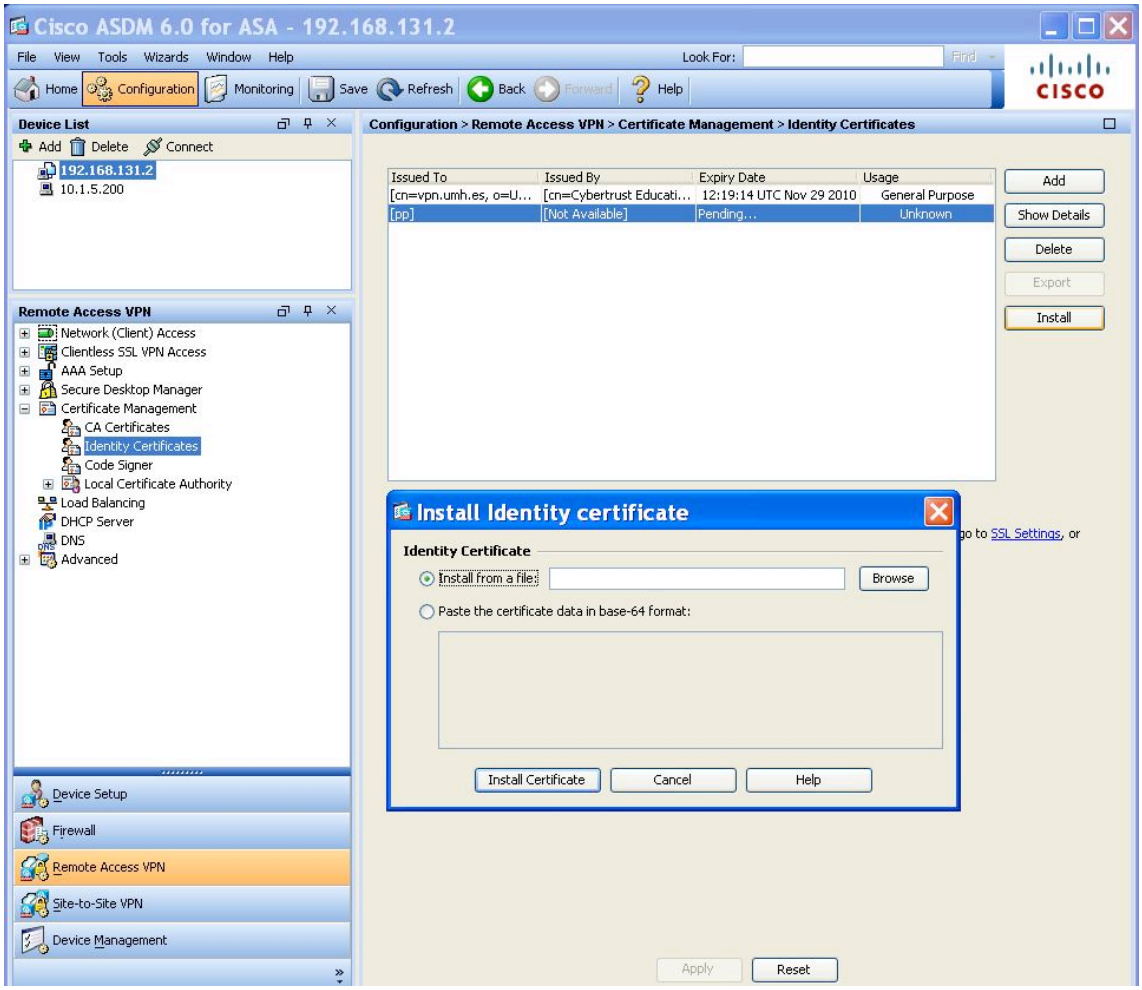


4.- Debemos seleccionar la opción Advanced puesto que si no se hace, por defecto se incluirá el campo FQDN en el CSR que se envía a redIris, para ello debemos borrar lo que aparezca en dicho campo y darle a OK

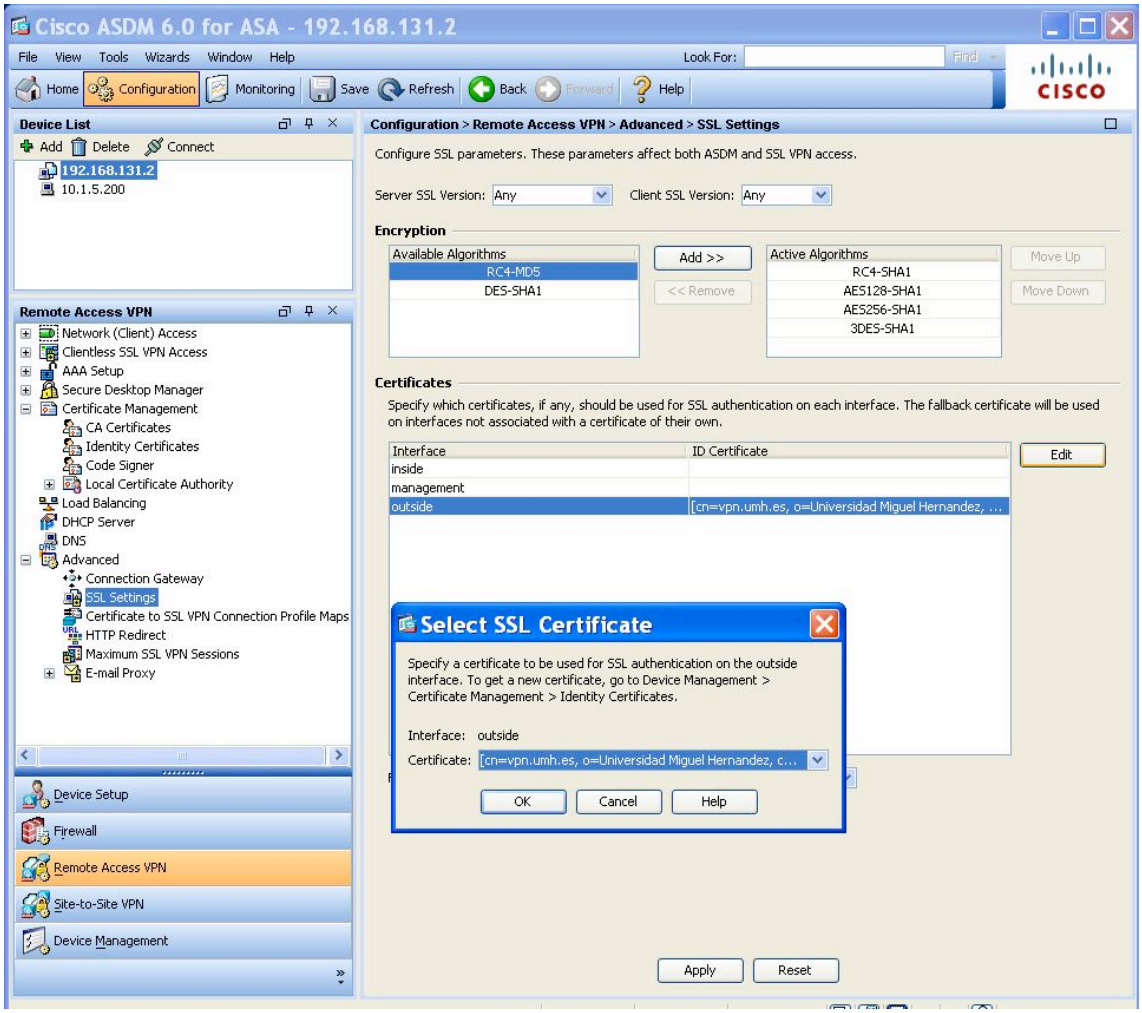


5.- Debemos añadir el certificado mediante la opción Add Certificate y a continuación se nos preguntará el nombre del fichero CSR que necesitamos para el proceso de registro en redIris.

6.- Cuando se termine el proceso de firmado del certificado, se nos envía un fichero .pem que deberemos instalar en el ASA mediante la opción Install, se nos pedirá que seleccionemos el fichero .pem que hemos recibido y si el proceso es correcto tendremos el certificado instalado emitido por Cybertrust con la fecha de caducidad correspondiente.



7.- Por último, para habilitar el envio de dicho certificado a aquellos clientes de SSL VPN debemos asignar dicho certificado al interface por donde se quiere establecer la VPN SSL, para ello seleccionamos bajo la opción Advanced -> SSL Settings y añadirmos el certificado al interface



Listos para abrir sesiones SSL VPN.

José Ramón García Valdés

Universidad Miguel Hernández.