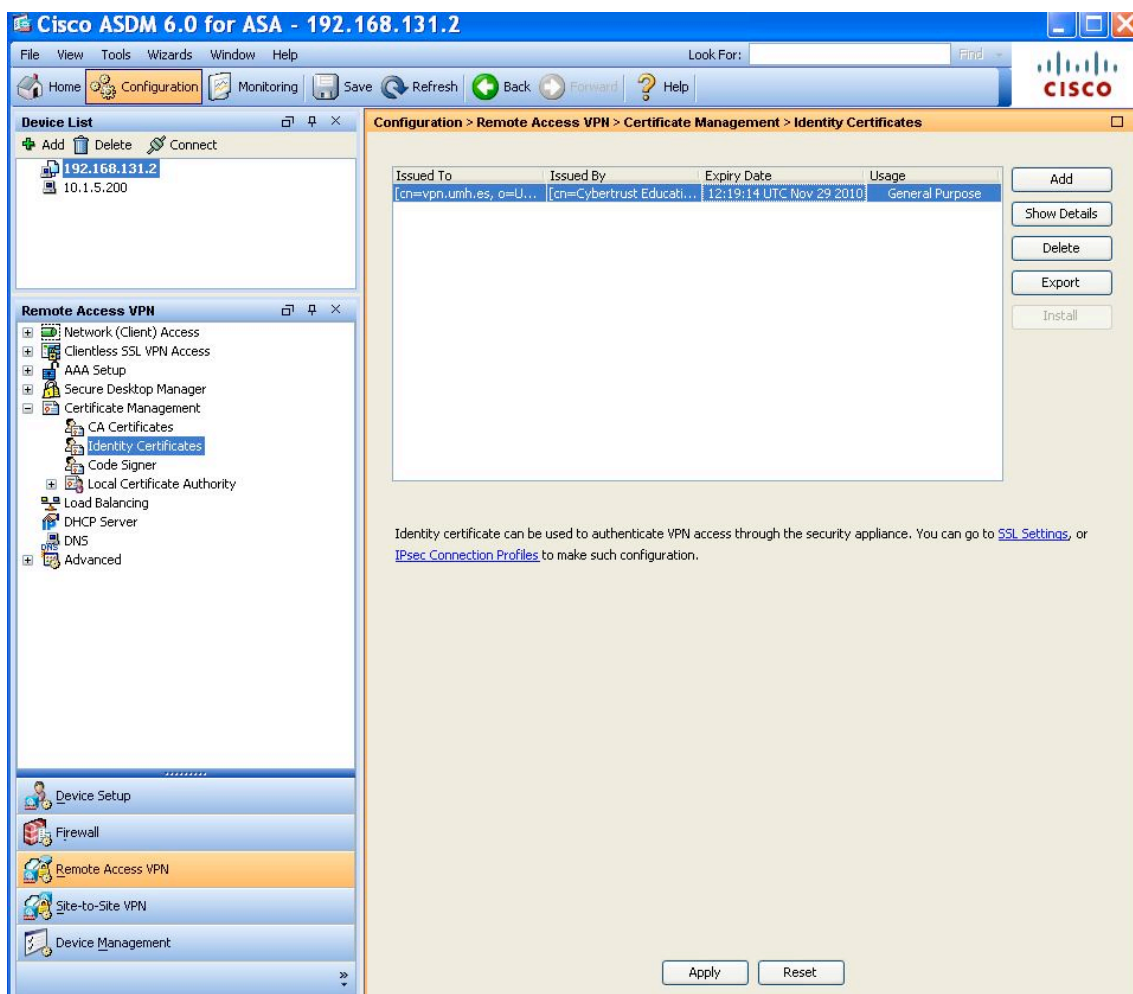


GUIA BÁSICA DE GENERACIÓN E INSTALACIÓN DE CERTIFICADOS PARA ASA 8.0

1.- Debemos utilizar la utilidad de administración ASDM, 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

Add Identity Certificate

Import the identity certificate from a file:

Decryption Passphrase:

File to Import From:

Add a new identity certificate:

Key Pair:

Certificate Subject DN:

Generate self-signed certificate

Act as local certificate authority and issue dynamic certificates to TLS-Proxy

Add Key Pair

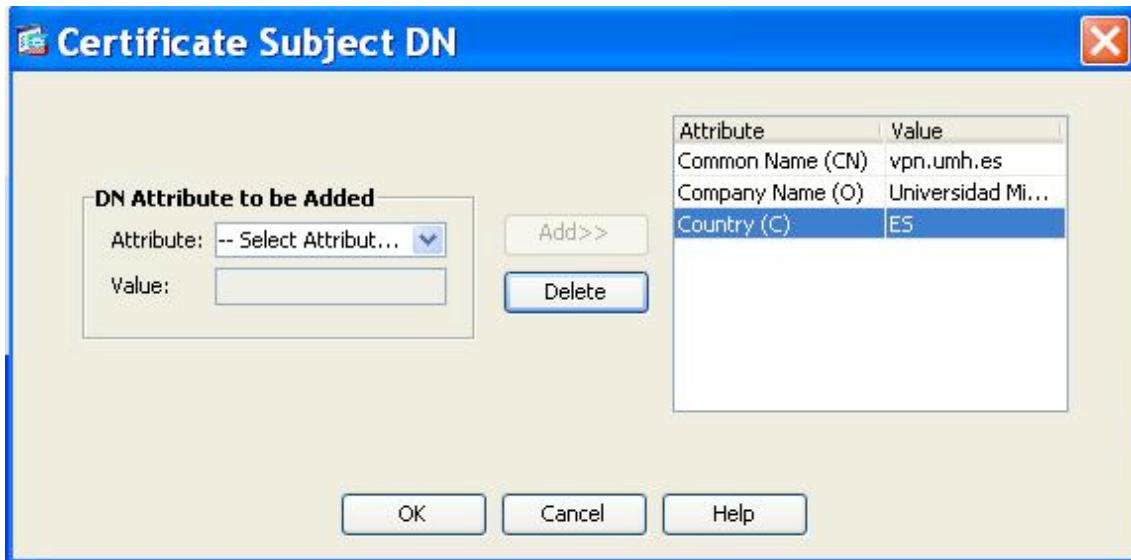
Name: Use default key pair name

Enter new key pair name:

Size:

Usage: General purpose Special

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



Add Identity Certificate

Import the identity certificate from a file:

Decryption Passphrase:

File to Import From:

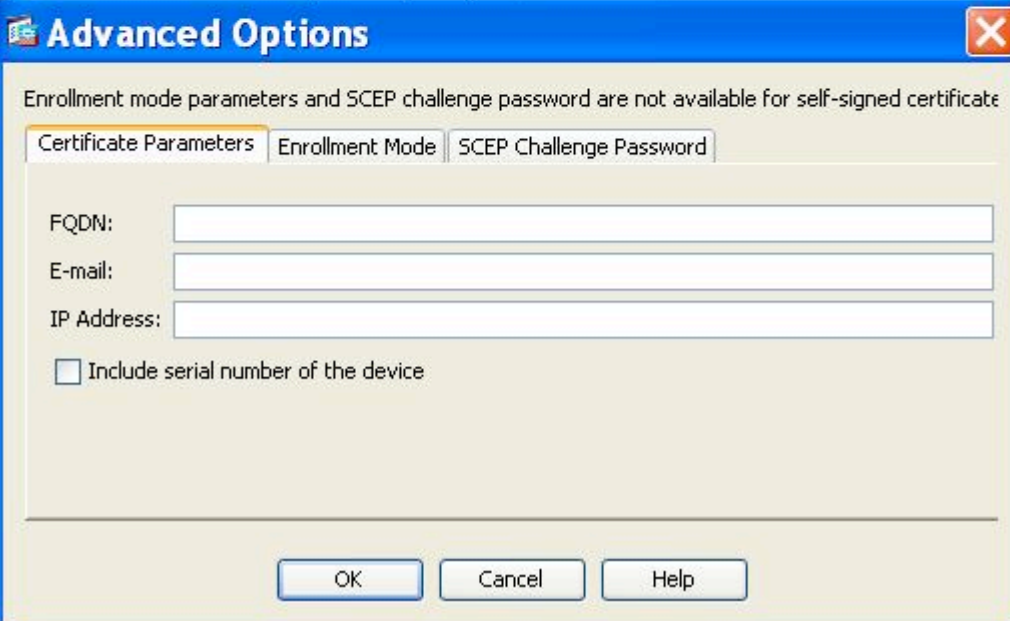
Add a new identity certificate:

Key Pair:

Certificate Subject DN:

Generate self-signed certificate

Act as local certificate authority and issue dynamic certificates to TLS-Proxy



Advanced Options

Enrollment mode parameters and SCEP challenge password are not available for self-signed certificate

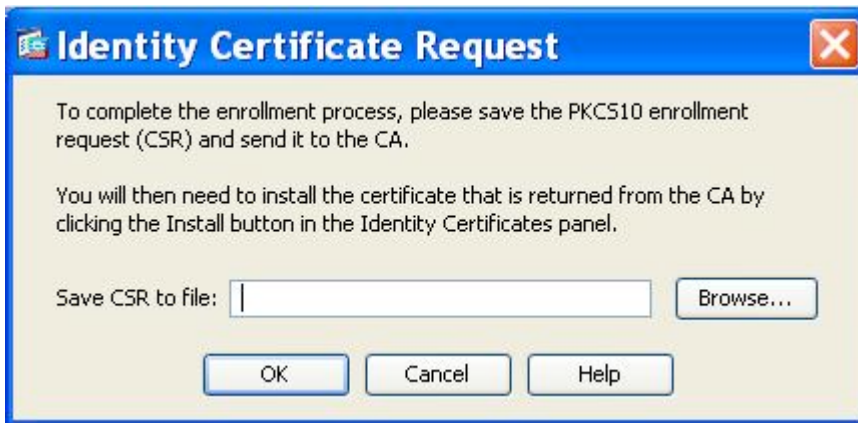
FQDN:

E-mail:

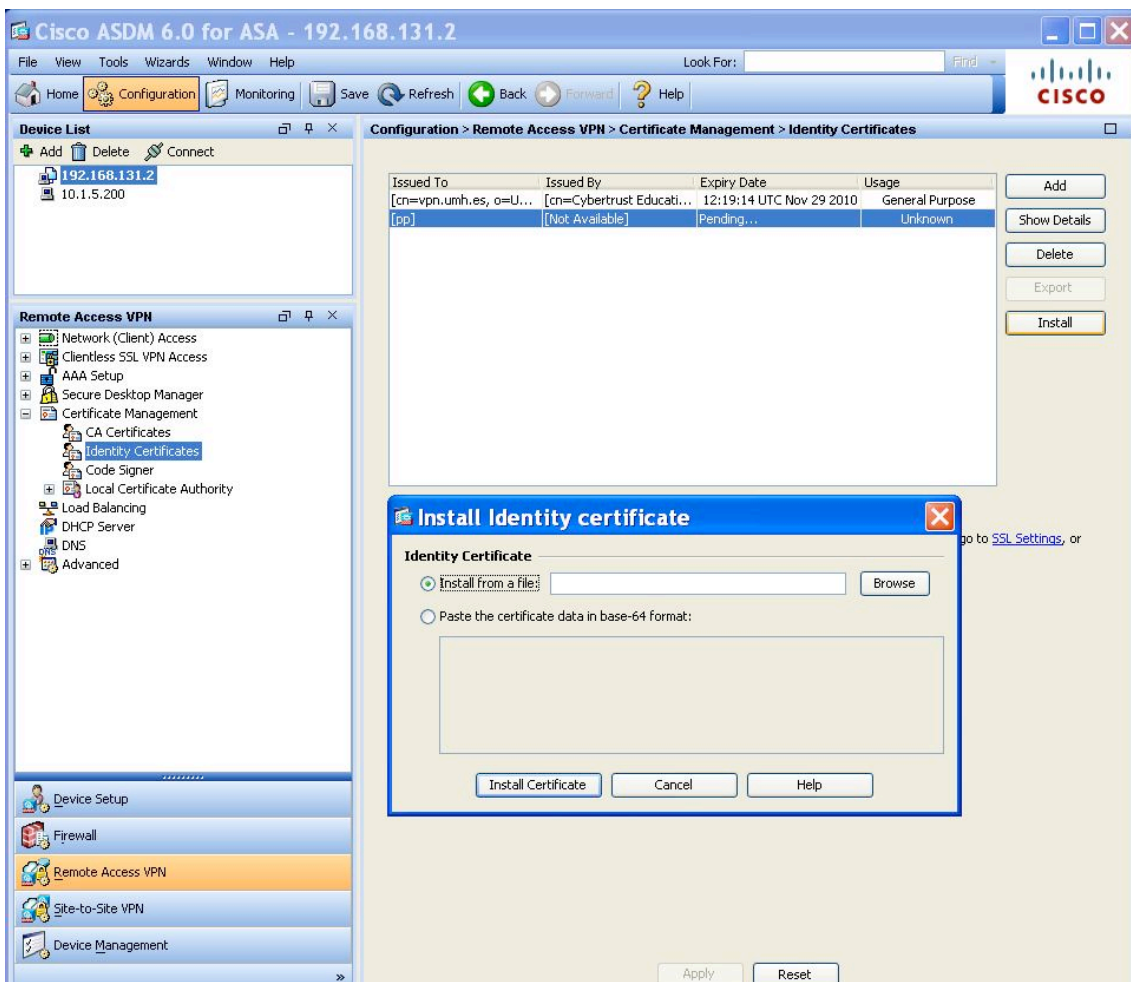
IP Address:

Include serial number of the device

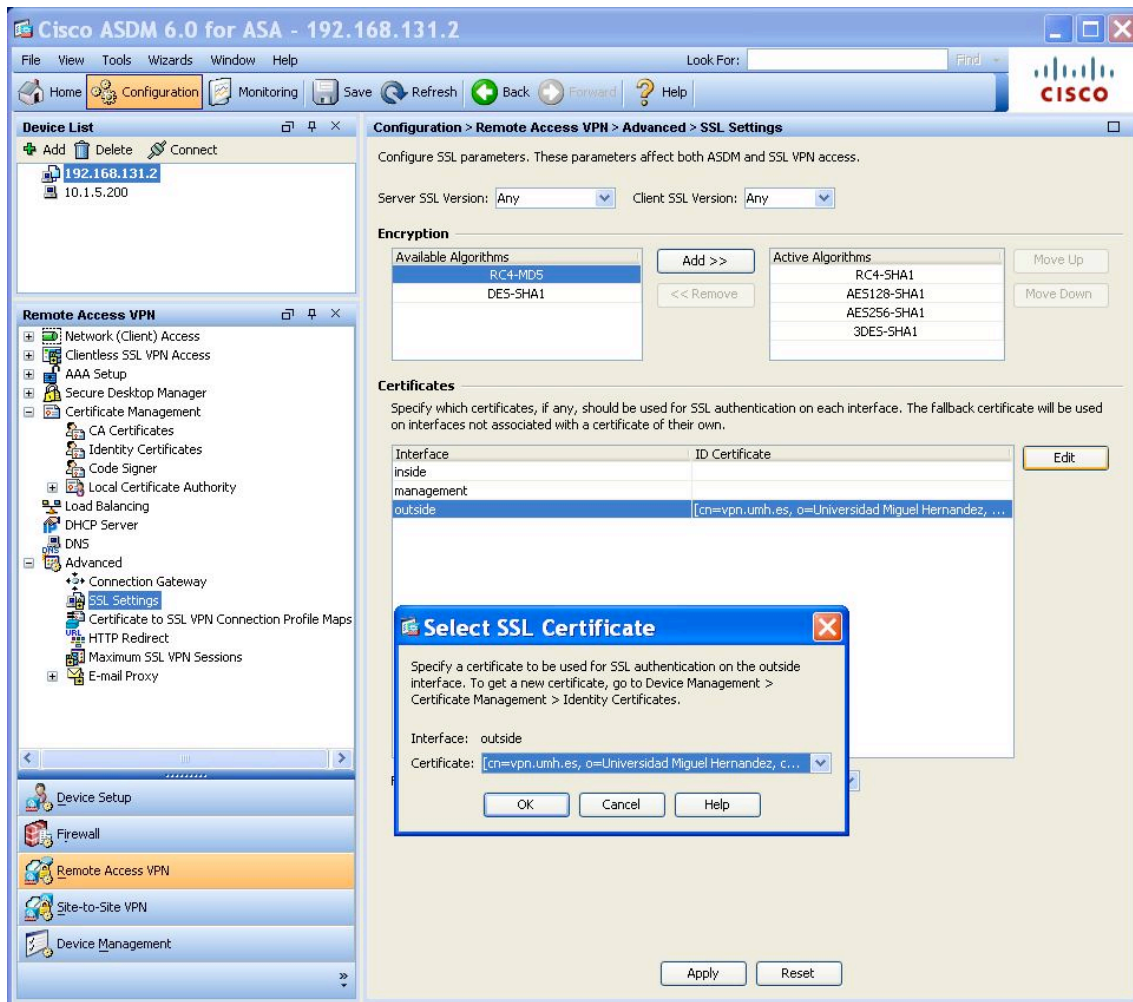
5.- Debemos añadir el certificado mediante la opción Add Certificate y a continuación se nos preguntará el nombre del fichero CSR que necesitamos para el proceso de registro en rediris.



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 envío 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 añadimos el certificado al interface



Listos para abrir sesiones SSL VPN.

José Ramón García Valdés

Universidad Miguel Hernández.