ASA 8.x: Renueve y instale el certificado SSL con el ASDM

Contenido

Introducción

El procedimiento en este documento es un ejemplo y se puede utilizar como guía de consulta con cualquier vendedor del certificado o su propio servidor del certificado raíz. Los requisitos especiales del parámetro del certificado son requeridos a veces por su vendedor del certificado, pero este documento se piensa para proporcionar los pasos generales requeridos renovar un certificado SSL y instalarlo en un ASA que utilice el software 8.0.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

Este procedimiento pertenece a las Versiones de ASA 8.x con la versión 6.0(2) o posterior del ASDM.

El procedimiento en este documento se basa en una configuración válida con un certificado instalado y usado para el acceso SSL VPN. Este procedimiento no afecta su red mientras el certificado actual no se borre. Este procedimiento es un proceso gradual en cómo publicar un nuevo CSR para un certificado actual con el mismo certificado raíz que publicó la original raíz CA.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Si la red está funcionando, asegúrese de haber comprendido el impacto

que puede tener cualquier comando.

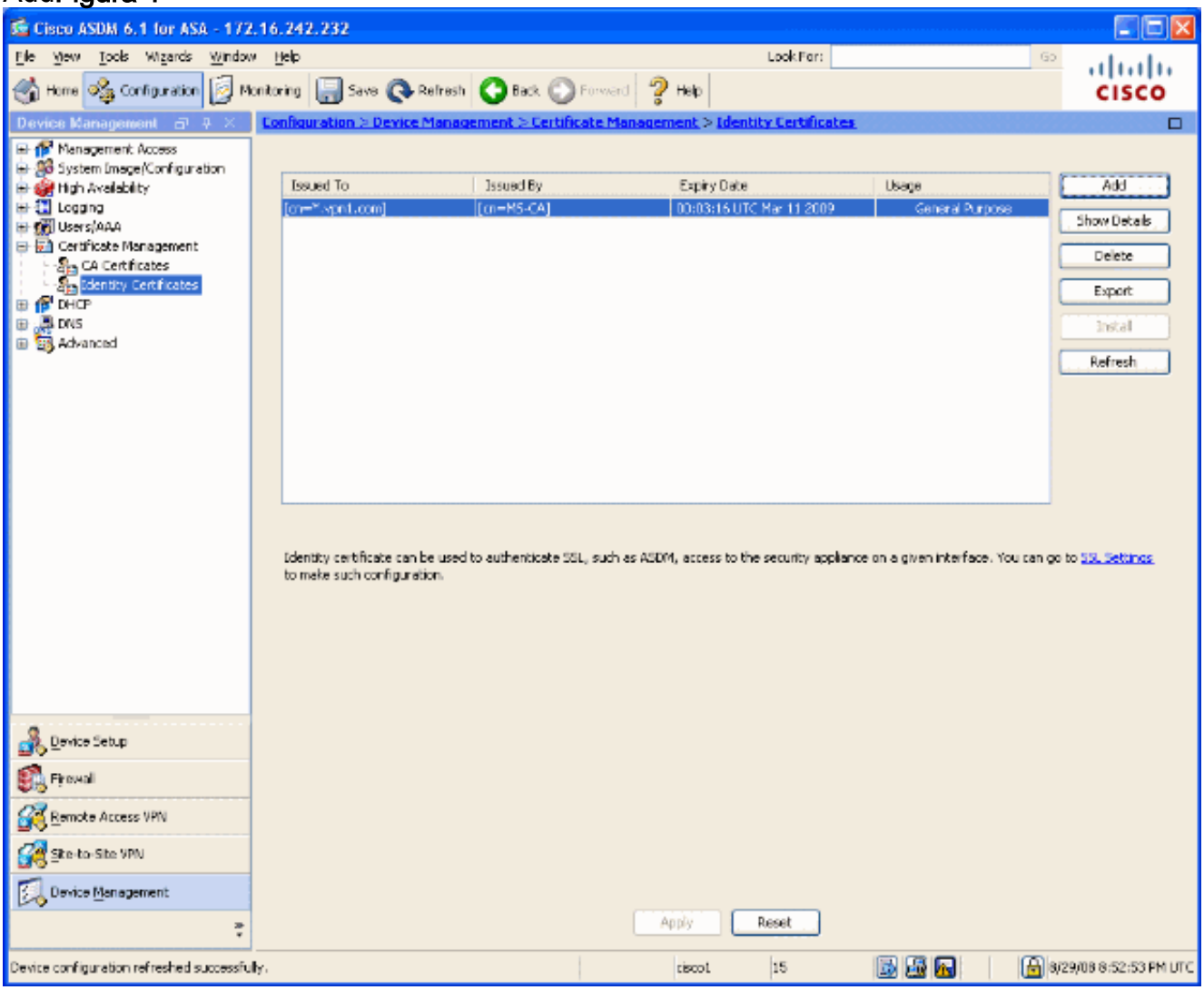
Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

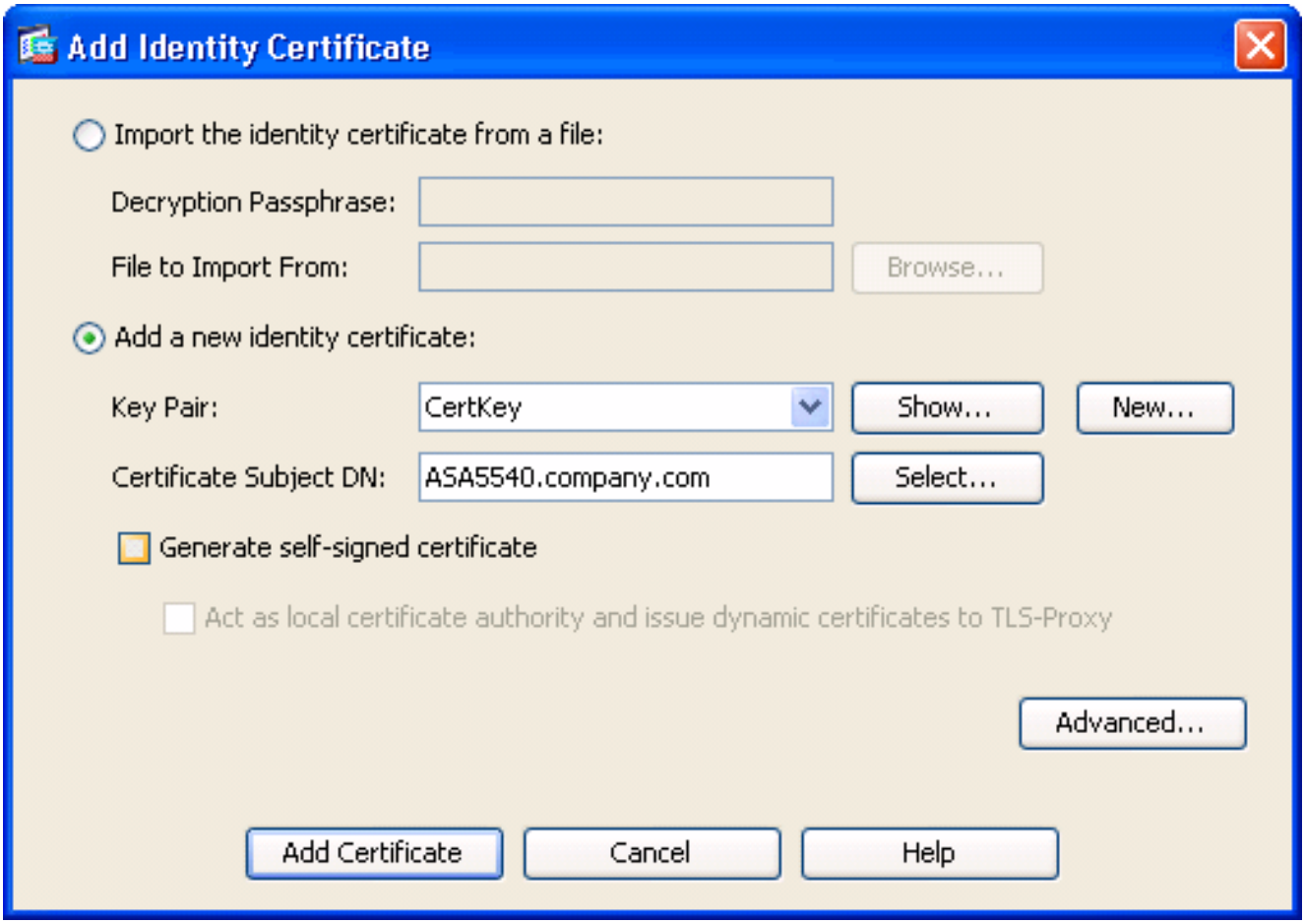
Procedimiento

Complete estos pasos:

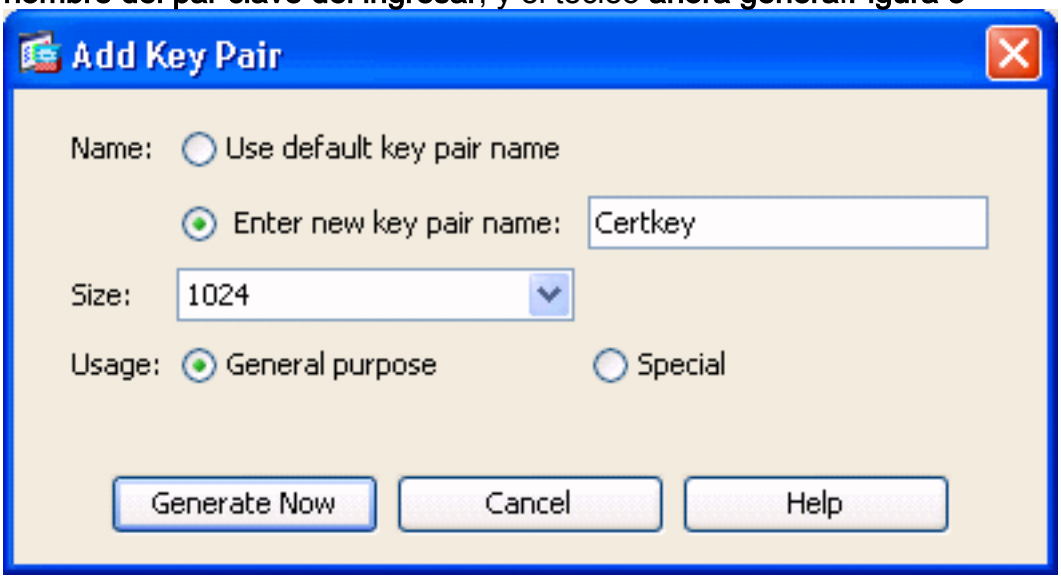
1. Seleccione el certificado que usted quiere renovar debajo de la configuración > de la Administración de dispositivos > de los certificados de identidad, y entonces el haga click en Add**Figura 1**



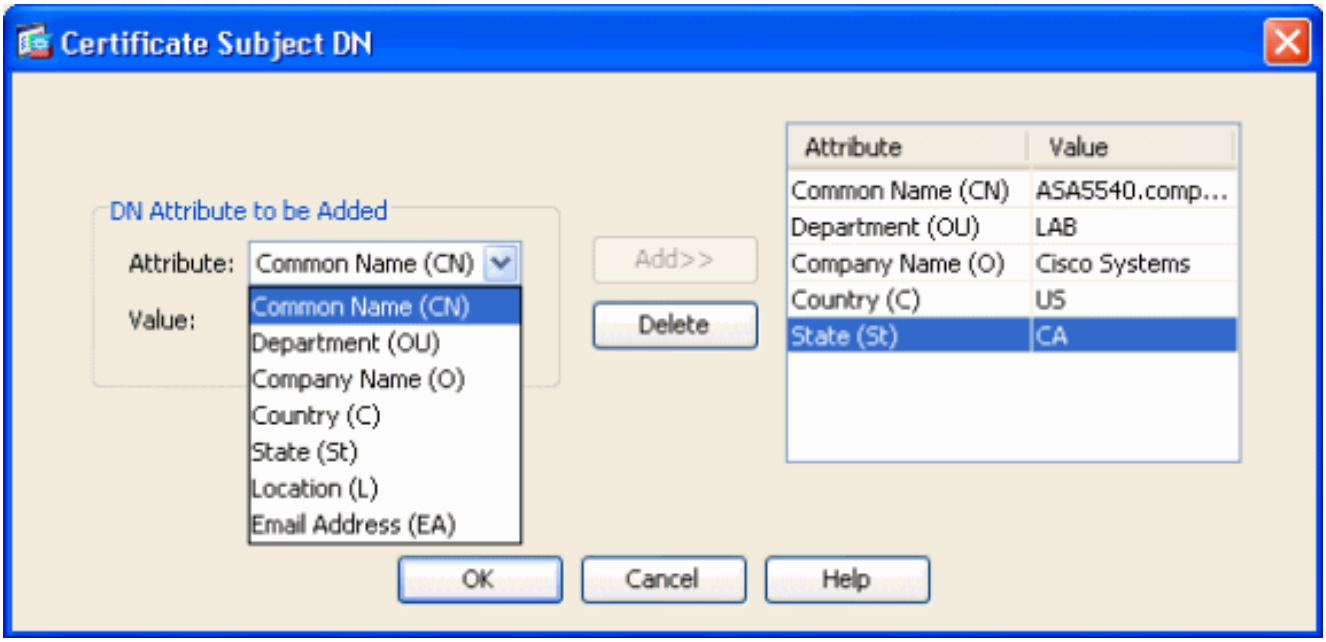
2. Bajo agregue el certificado de identidad, seleccione el **agregar un nuevo** botón de radio del **certificado de identidad**, y elija su par clave del menú desplegable.**Nota:** No se recomienda para utilizar el <Default-RSA-Key> porque si usted regenera su clave de SSH, usted invalida su certificado. Si usted no tiene una clave RSA, completa camina a y el B. Si no continúe al paso 3.**Figura 2**



(Opcional) complete estos pasos si usted no hace una clave RSA configurar todavía, si no salto al paso 3.Haga clic **nuevo....**Ingrese el nombre del par clave en el **nuevo campo de nombre del par clave del ingresar**, y el tecleo **ahora genera**.**Figura 3**



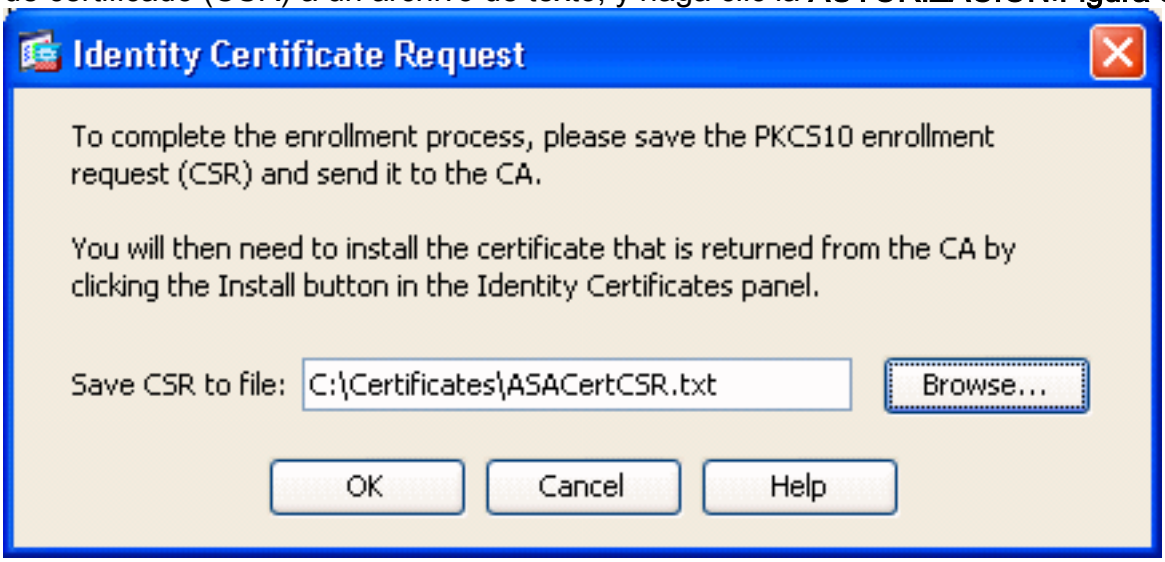
3. Tecleo **selecto**.
4. Ingrese los atributos apropiados del certificado tal y como se muestra en del cuadro 4. Una vez que está completado, haga clic la **AUTORIZACIÓN**. Entonces haga clic **agregan el certificado**.**'Figura 4'**



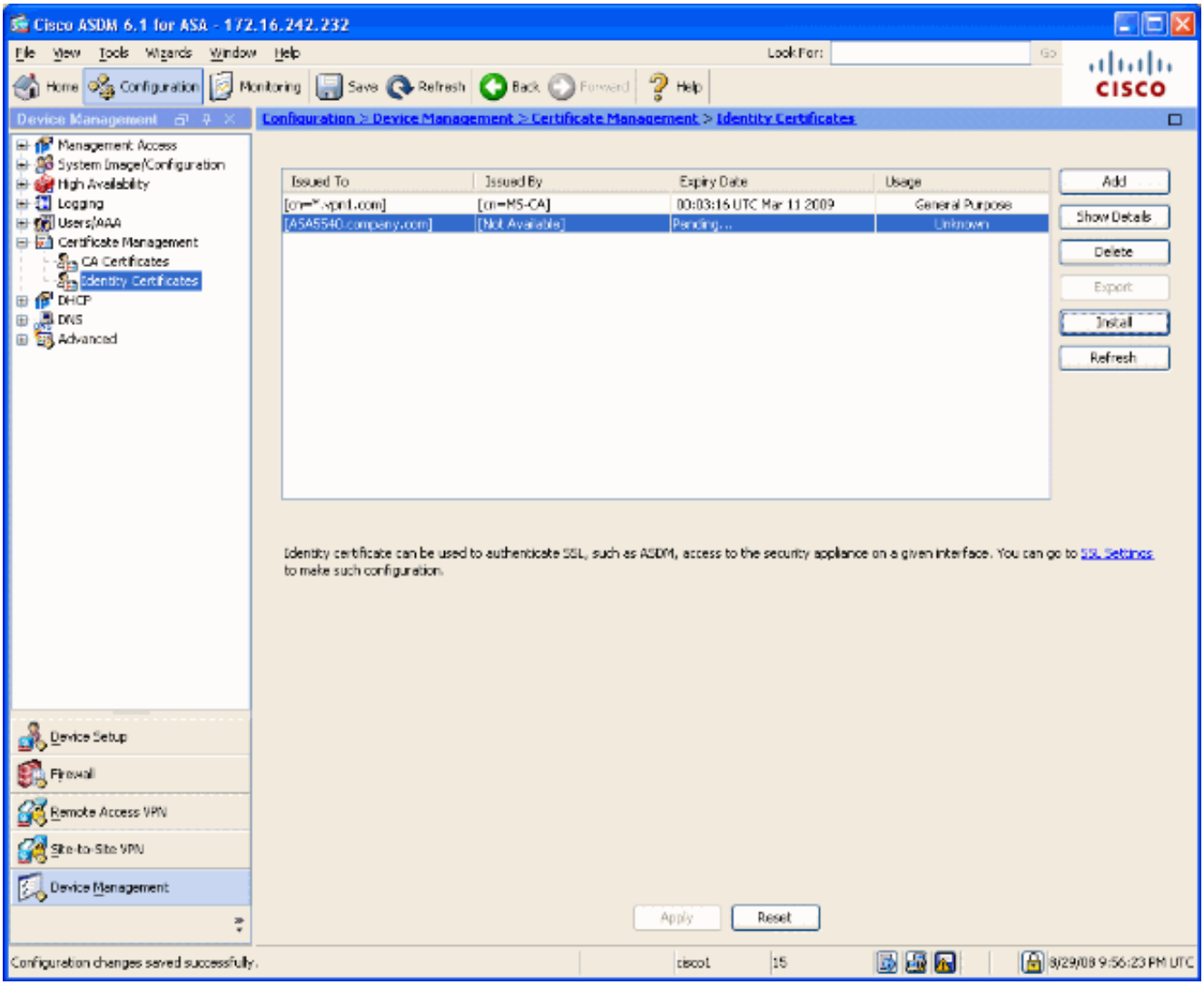
CLI hecho salir:

```
crypto ca trustpoint ASDM_TrustPoint0 keypair CertKey id-usage ssl-ipsec fqdn 5540-uwe
subject-name CN=ASA5540.company.com,OU=LAB,O=Cisco ystems,C=US,St=CA enrollment terminal
crypto ca enroll ASDM_TrustPoint0
```

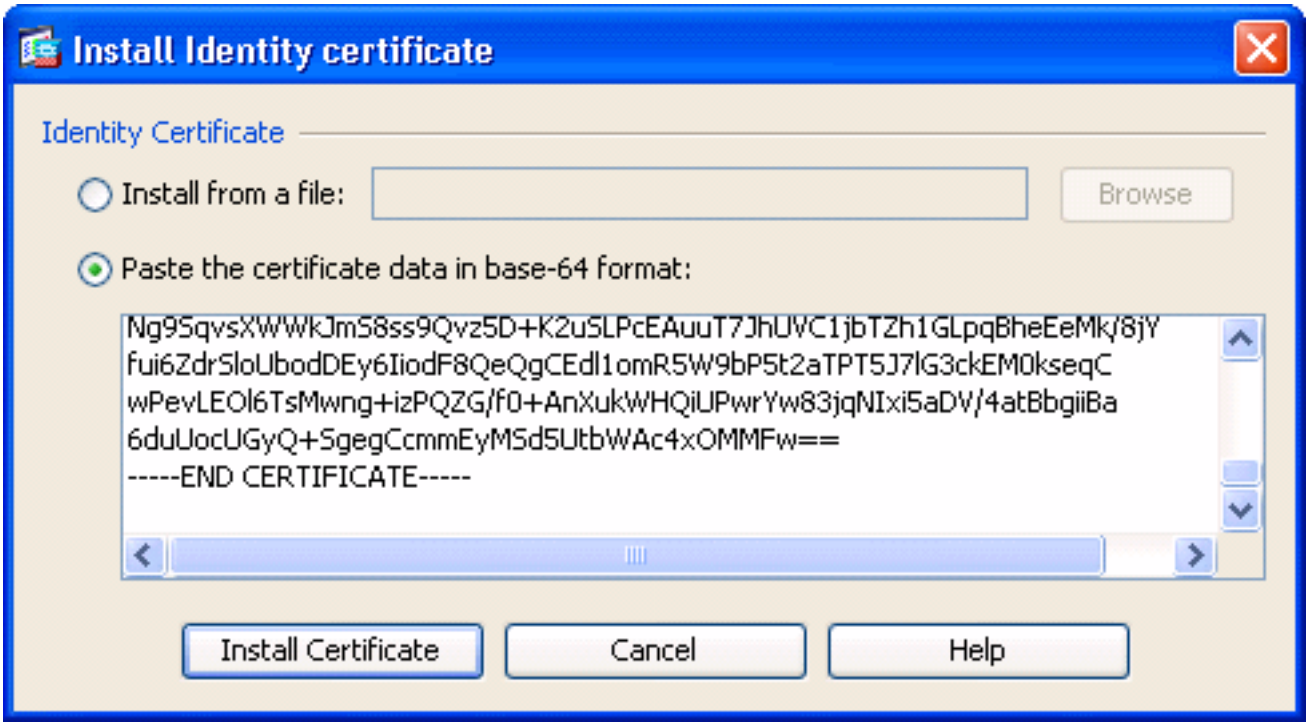
5. En la ventana emergente de la **petición del certificado de identidad**, salve su pedido de firma de certificado (CSR) a un archivo de texto, y haga clic la **AUTORIZACIÓN.Figura 5**



6. (Opcional) verifique en el ASDM que el CSR esté pendiente, tal y como se muestra en del cuadro 6.**'Figura 6'**



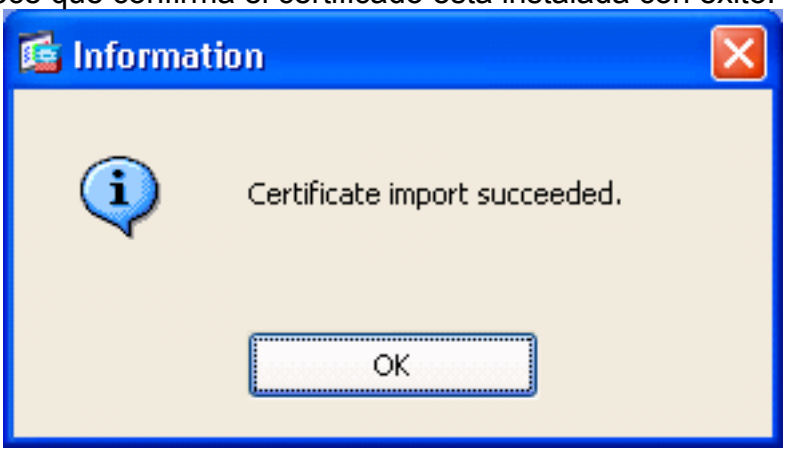
7. Presente el pedido de certificado al administrador del certificado, que publica el certificado en el servidor. Esto puede estar a través de una interfaz Web, email, o directamente raíz CA al servidor para el proceso del problema del certificado.
8. Complete estos pasos para instalar el certificado renovado.Seleccione el pedido de certificado pendiente conforme a la configuración > a la Administración de dispositivos > a los certificados de identidad, tal y como se muestra en del cuadro 6, y el tecleo **instala**.En la ventana del certificado de identidad del instalar, seleccione la **goma los datos del certificado en el** botón de radio del **formato del base 64**, y el tecleo **instala el certificado**.**Nota:** Alternativamente, si el certificado se publica en un archivo de .cer bastante entonces un archivo o un email basado texto, usted puede también seleccionar **instala de un archivo**, hojea al archivo apropiado en su PC, tecleo **instala el archivo de certificado ID** y después hace clic **instala el certificado**.**Figura 7**



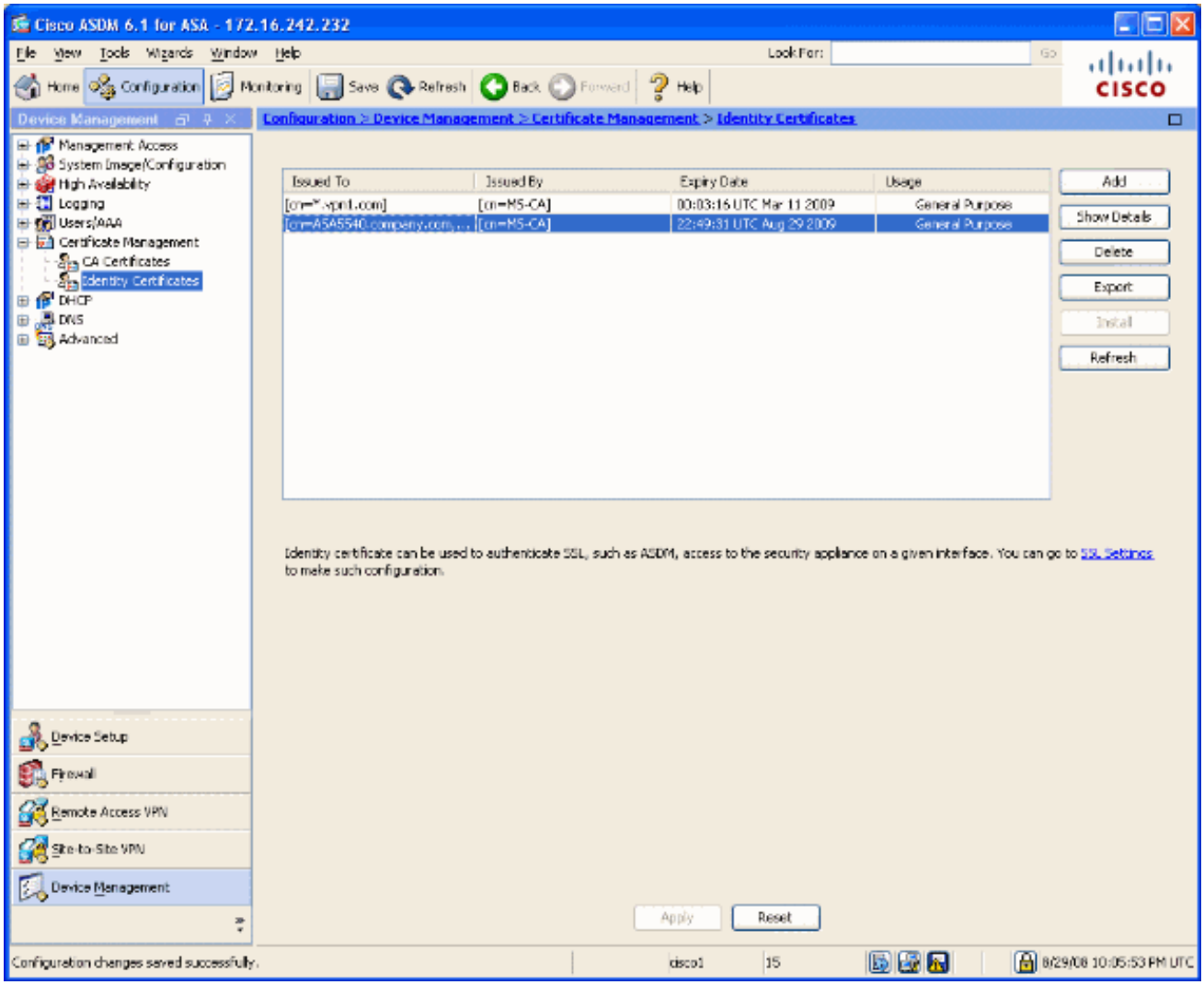
CLI hecho salir:

```
crypto ca import ASDM_TrustPoint0 certificate
WIID2DCCAsCgAwIBAgIKYb9wewAAAAAAJzANBgkqhkiG9w0BAQUFADAQMQ !--- output truncated
wPevLEOl6TsMwng+izPQZG/f0+AnXukWHQiUPwrYw83jqNIxi5aDV/4atBbgiiBa
6duUocUGyQ+SgegCcmmEyMSd5UtbWAc4xOMMFw== quit
```

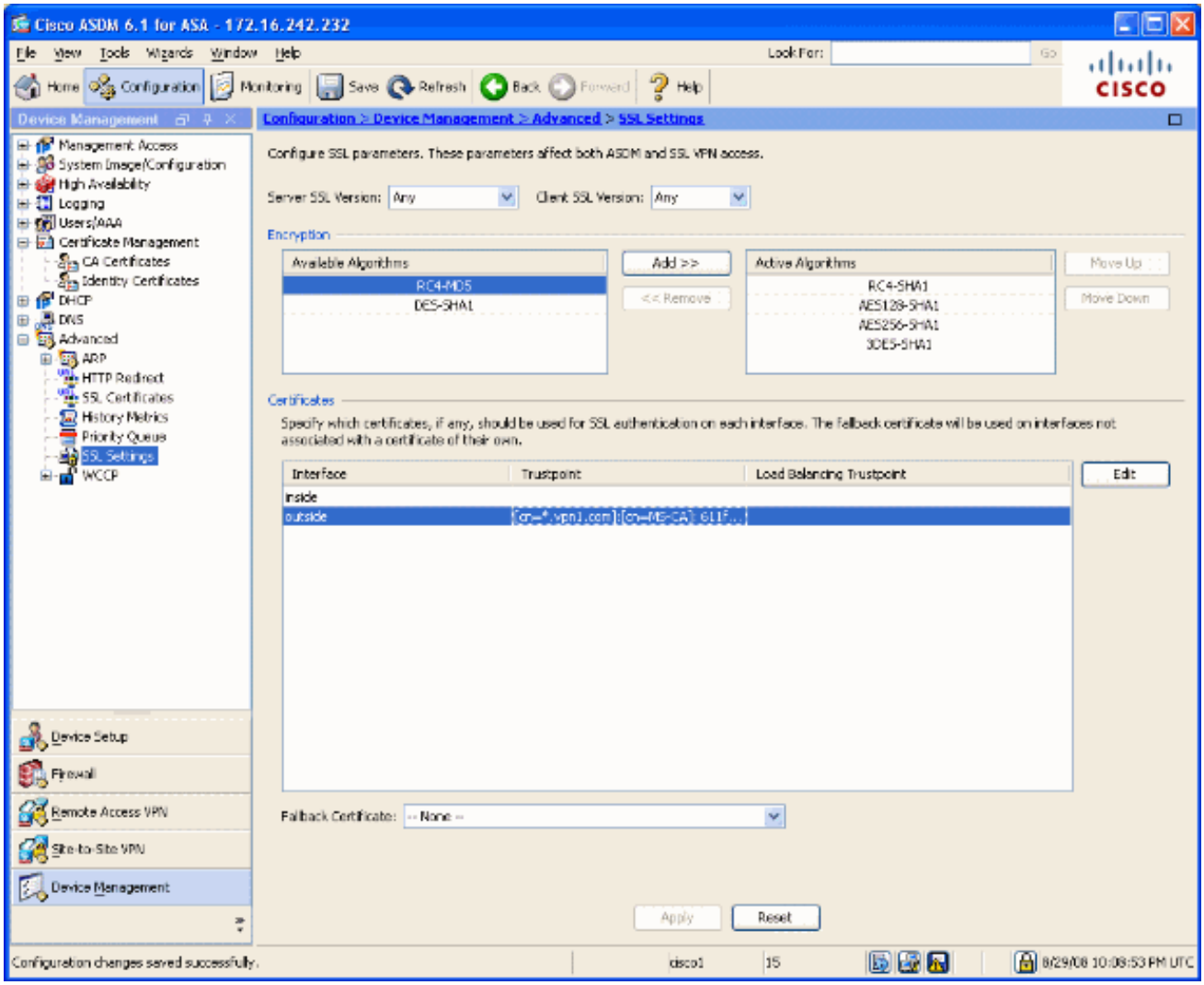
9. Una ventana aparece que confirma el certificado está instalada con éxito. “OK” del tecleo a confirmar.**Figura 8**



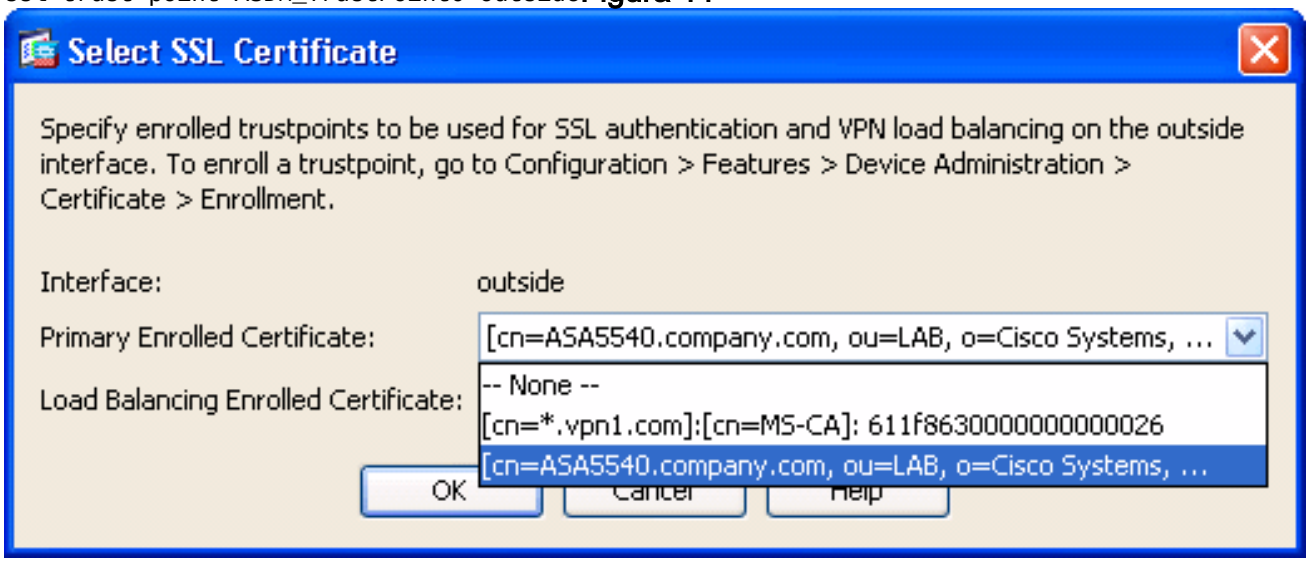
10. Asegúrese que su nuevo certificado aparezca bajo los certificados de identidad.**Figura 9**



11. Complete estos pasos para atar el nuevo certificado a la interfaz:Elija la **configuración > la Administración de dispositivos > avanzó > las configuraciones SSL**, tal y como se muestra en del cuadro 10.Seleccione su interfaz bajo los Certificados, y el tecleo **edita**.**Figura 10**



12. Elija su nuevo certificado del menú desplegable, haga clic la **AUTORIZACIÓN**, y el tecleo **se aplica**.`ssl encryption rc4-sha1 aes128-sha1 aes256-sha1 3des-sha1`
`ssl trust-point ASDM_TrustPoint0 outside`**Figura 11**



13. Salve su configuración en el ASDM o en el CLI.

Verificación

Usted puede utilizar la interfaz CLI para verificar que el nuevo certificado está instalado al ASA correctamente, tal y como se muestra en de esta salida de muestra:

```
ASA(config)#show crypto ca certificates Certificate Status: Available Certificate Serial Number:
61bf707b000000000027 Certificate Usage: General Purpose Public Key Type: RSA (1024 bits) Issuer
Name: cn=MS-CA Subject Name: cn=ASA5540.company.com !---new certificate ou=LAB o=Cisco Systems
st=CA c=US CRL Distribution Points: [1] http://win2k3-base1/CertEnroll/MS-CA.crl [2]
file://\\win2k3-base1\CertEnroll\MS-CA.crl Validity Date: start date: 22:39:31 UTC Aug 29 2008
end date: 22:49:31 UTC Aug 29 2009 Associated Trustpoints: ASDM_TrustPoint0 CA Certificate
Status: Available Certificate Serial Number: 211020a79cfd96b34ba93f3145d8e571 Certificate Usage:
Signature Public Key Type: RSA (2048 bits) Issuer Name: cn=MS-CA Subject Name: cn=MS-CA !---
'old' certificate CRL Distribution Points: [1] http://win2k3-base1/CertEnroll/MS-CA.crl [2]
file://\\win2k3-base1\CertEnroll\MS-CA.crl Validity Date: start date: 00:26:08 UTC Jun 8 2006
end date: 00:34:01 UTC Jun 8 2011 Associated Trustpoints: test Certificate Status: Available
Certificate Serial Number: 611f8630000000000026 Certificate Usage: General Purpose Public Key
Type: RSA (1024 bits) Issuer Name: cn=MS-CA Subject Name: cn=*.vpn1.com CRL Distribution Points:
[1] http://win2k3-base1/CertEnroll/MS-CA.crl [2] file://\\win2k3-base1\CertEnroll\MS-CA.crl
Validity Date: start date: 23:53:16 UTC Mar 10 2008 end date: 00:03:16 UTC Mar 11 2009
Associated Trustpoints: test ASA(config)#
```

Troubleshooting

(Opcional) verifique en el CLI que el certificado correcto esté aplicado a la interfaz:

```
ASA(config)#show running-config ssl ssl trust-point ASDM_TrustPoint0 outside !--- Shows that the
correct trustpoint is tied to the outside interface that terminates SSL VPN. ASA(config)#
```

Cómo copiar los Certificados SSL a partir de un ASA a otro

Esto puede ser hecha si usted había generado las claves exportables. Usted necesita exportar el certificado a un archivo PKCS. Esto incluye la exportación de todas las claves asociadas.

Utilice este comando de exportar su certificado vía el CLI:

```
ASA(config)#crypto ca export <trust-point-name> pkcs12 <passphrase>
```

Nota: Passphrase - usado para proteger el archivo del pkcs12.

Utilice este comando de importar su certificado vía el CLI:

```
SA(config)#crypto ca import <trust-point-name> pkcs12 <passphrase>
```

Nota: Este passphrase debe ser lo mismo según lo utilizado al exportar el archivo.

Esto se puede también hacer con el ASDM para un par de fallas ASA. Complete estos pasos para realizar esto:

1. Inicie sesión al ASA primario vía el ASDM y elija las **herramientas--> configuración de respaldo**.
2. Usted puede respaldo todo o apenas los Certificados.
3. En el espera, el ASDM abierto y elige las **herramientas --> configuración del Restore**.

Información Relacionada

- Página de soporte adaptante del dispositivo de seguridad de Cisco (ASA)
- El ASA 8.x instala manualmente los Certificados del vendedor de las de otras compañías para el uso con el ejemplo de configuración del WebVPN
- Soporte Técnico y Documentación - Cisco Systems