Renovar certificado Exchange

jueves, 10 de mayo de 2018
9:45

Cómo solicitar un certificado en Exchange 2010

- 06/05/201418/07/2015
- Daniel Núñez Banega
- 2

De forma predeterminada al instalar el rol de *Client Access* de Exchange 2010 se crea un certificado auto firmado (*self signed*) que incluye el nombre de *host* y *FQDN* del servidor. Si bien este certificado nos puede ser útil para validar el funcionamiento general, este no es el ideal para un entorno productivo.
La recomendación es la utilización de un certificado público, es decir emitido por una entidad certificadora (*CA*) externa como por ejemplo *Godaddy* o *Digicert*. La ventaja principal de esto es que los clientes (*incluyendo dispositivos móviles*) normalmente ya confiarían en el certificado. Como alternativa se podría utilizar una *CA interna*, el tema acá es que si bien los equipos internos no tendrían problemas, los dispositivos móviles o equipos no unidos al dominio requerirían intervención adicional.
Independientemente del tipo de entidad certificadora, ya sea interna o externa, el proceso de instalación de un nuevo certificado en Exchange es el mismo:

1. *Crear una nueva solicitud de certificado*
2. *Procesar la solicitud con una entidad certificadora*
3. *Completar la solicitud pendiente en Exchange*

En este caso en particular vamos a procesar la solicitud con una *CA interna* instalada según se describe en una entrada anterior.
En cuanto a los nombres a utilizar en el ejemplo:

- *Webmail.contoso.com*
- *Autodiscover.contoso.com*
- *Autodiscover.adatum.com*

Si tienen dudas sobre que nombres solicitar les recomiendo ver el siguiente artículo.

Cómo generar la solicitud de nuevo certificado en Exchange 2010?

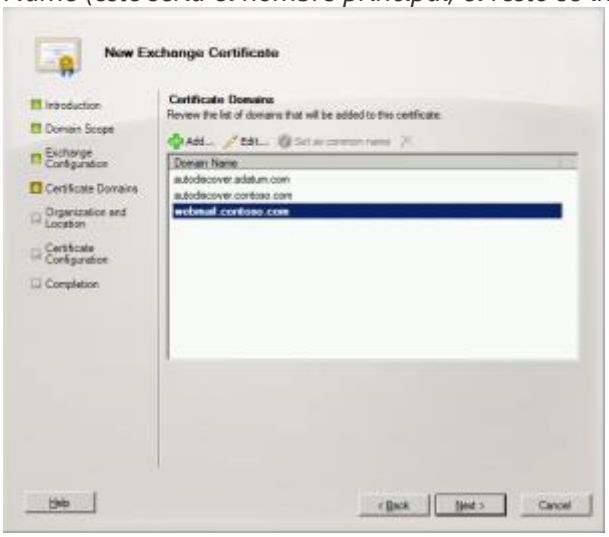
El procedimiento de solicitud de nuevo certificado es más sencillo utilizando el asistente por lo que vamos a abrir la *EMC (Exchange Management Console)*:

1. Dentro de la *EMC* seleccionar *Server Configuration -> Mail01* (*o el nombre del servidor con el rol de CAS que tengamos*)



2. Hacemos clic en *New Exchange Certificate*

3. Especificamos un nombre descriptivo, ej:"*Certificado Exchange*"
4. Si no precisamos un certificado de tipo *wildcard ("**")*, dejamos sin marcar la opción
5. El asistente nos va a solicitar un nombre para cada uno de los servicios diferenciando el caso interno del externo. En nuestro escenario vamos a utilizar únicamente servicios web (*OWA, OA, ActiveSync, OAB, EWS, Autodiscover*).
6. En la ventana de *Certificate Domains* marcar ***webmail.contoso.com*** como *Common Name (este sería el nombre principal, el resto se incluyen en el atributo de SAN)*

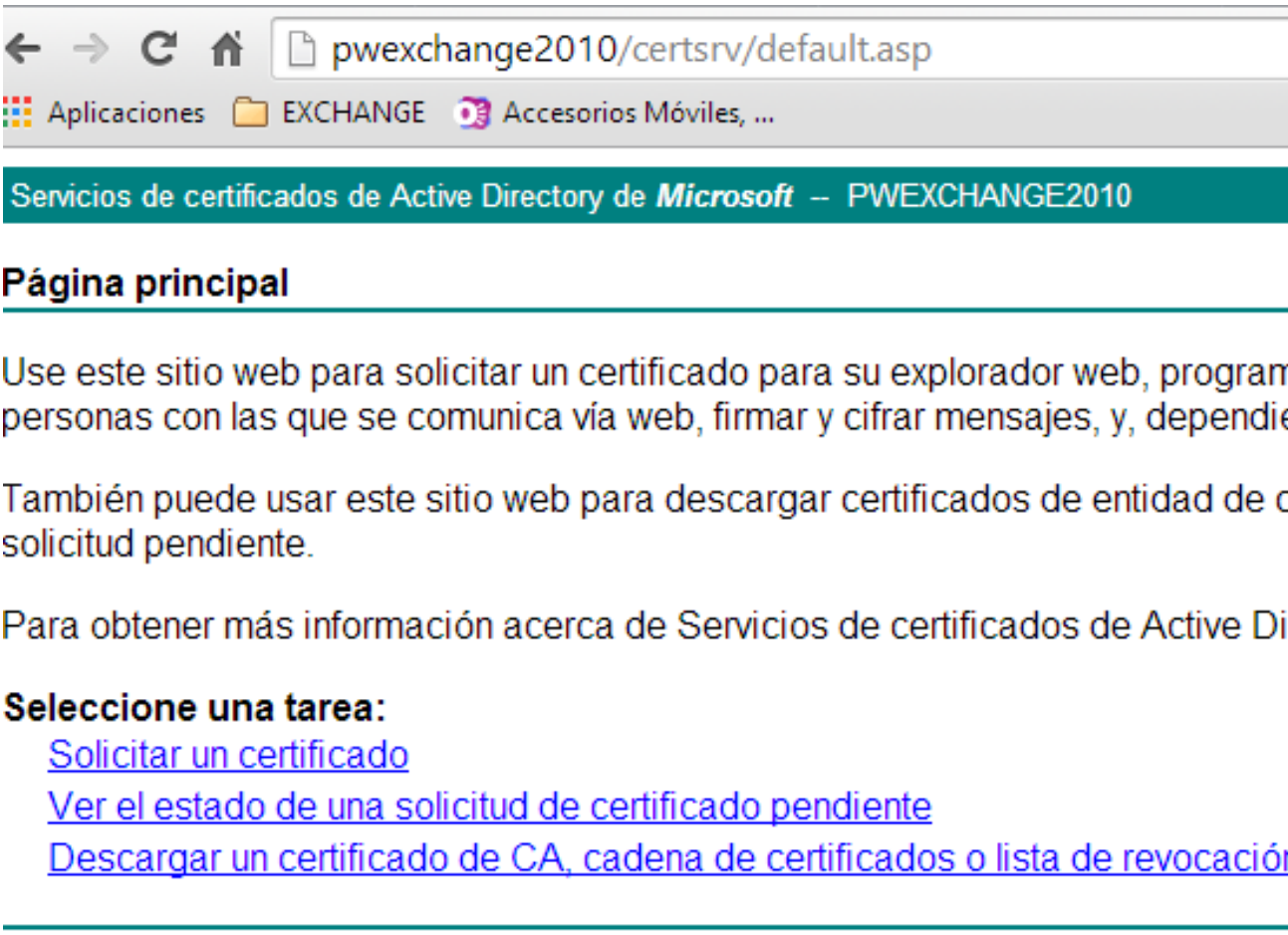


7. En caso de ser necesario, agregar nombres adicionales
8. Completar los datos de organización y hacer clic en *Browse* para guardar el archivo con la solicitud (*archivo.**req***).

Desde <https://aprendiendoexchange.com/como-solicitar-un-certificado-en-exchange-2010>

Cómo solicitar un certificado en Exchange 2010

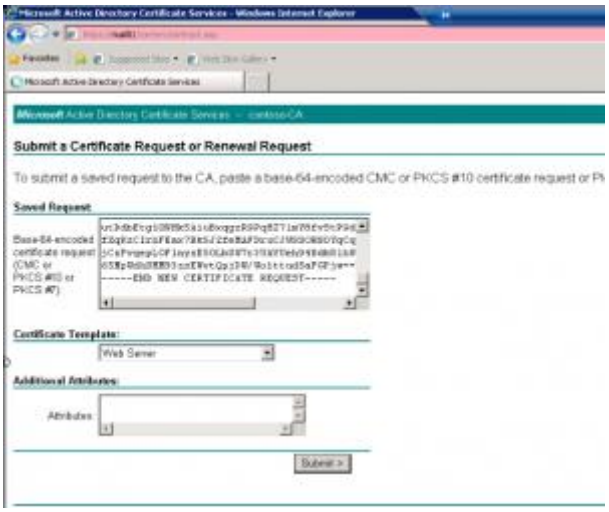
- 06/05/201418/07/2015
- Daniel Núñez Banega
- 2



Si utilizamos una entidad certificadora interna

Para procesar la solicitud con una *CA interna* debemos conectarnos al directorio virtual */certsrv* de la entidad certificadora:

9. Abrir *Internet Explorer* y escribir *https://servidor/certsrv*
10. En la ventana de bienvenido hacer clic en *Request a Certificate* y luego en *advanced certificate request*
11. Hacer clic en *Submit a certificate request by using a base-64-encoded CMC…*
12. Abrir con el bloc de notas el *archivo con extensión req* y copiamos todo el texto (*CSR*)
13. En la ventana de *Submit a Certificate Request*, en el cuadro de *Saved Request* pegamos el texto del ***req***
14. En *Certificate Template* seleccionamos *Web Server* y hacemos clic en *Submit*

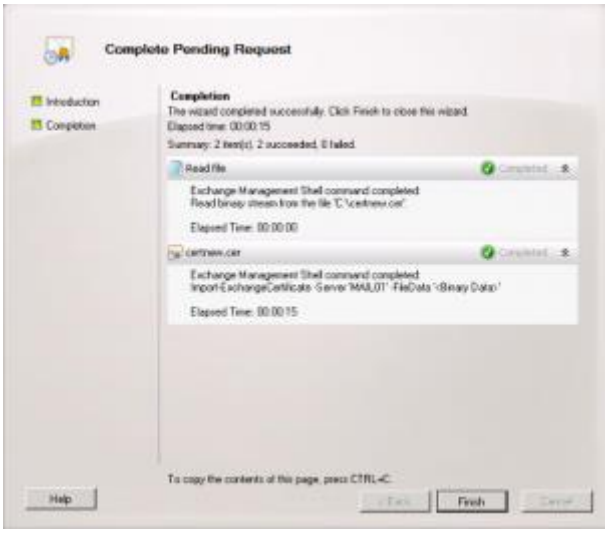


15. En *Certificate Issued* seleccionamos *Based 64 encoded y Download Certificate*
16. Guardar el archivo *.cer* obtenido

Completar la solicitud de certificado pendiente en Exchange

En general el archivo devuelto por la *CA* tiene extensión "*cer*". Una vez obtengamos el archivo estaríamos en condiciones para completar la solicitud pendiente en el servidor orígina.

17. Volver a la *EMC*, *Server Configuration* -> *Mail01* (o nombre de servidor)
18. Buscar la solicitud de certificado en el panel de abajo y hacer clic en *Complete Pending Request*
19. En *Browse* seleccionar el *archivo .cer* obtenido en el procedimiento anterior y seguir las instrucciones del asistente



20. Si todo fue exitoso el certificado tendría que figurar en la consola como *The Certificate is valid for Exchange usage*, de lo contrario tendríamos un problema.



Importante: *Usualmente el tipo de problemas que se puedan presentar tienen relación con que falte alguna raíz emisora, CA intermedia o que no se tenga acceso a la CRL (Certificate Revocation List), esto último depende de que el servidor tenga navegación directa hacia internet, si lo hace a través de un proxy requiere configuración adicional.*

En este punto el nuevo certificado se encuentra instalado pero los servicios continúan utilizando el predeterminado, para que Exchange comience a utilizar el nuevo certificado se debe correr el proceso de asignación.

Por último, ya sea para instalar el certificado en otro servidor o simplemente por respaldo es recomendable exportar el certificado junto a su llave privada.

Por información sobre renovación de certificados en Exchange 2010:

- *Cómo renovar un certificado en Exchange 2010*

Sobre Exchange 2013:

- *Certificados en Exchange 2013*

Desde <https://aprendiendoexchange.com/como-solicitar-un-certificado-en-exchange-2010/2>

Asignar servicios al certificado => IIS
Instalar el certificado en el servidor -> equipo -> personal
Y seleccionar el certificado en el IIS