

Certificate Renewal Follies in IIS 7

Posted At : November 2, 2009 12:16 PM | Posted By : Mark Kruger

Related Categories: Hosting and Networking

I have a few Win2008 servers under management and I had to renew a cert for one of them today. Now I confess this is the first time I had to do this particular task so there was some head scratching involved. I learned a number of things that might be of some use to you if you are up against this task. In this case I was *renewing* a Verisign cert. Here's what I learned.

Quick Word on IIS 7

Now I don't have a beef with MS like a lot of folks. Indeed we have windows servers that perform really well and have a very low cost of ownership. What does bug me is how they have scrapped a perfectly serviceable tool like IIS 6 manager where everything is predictable and the idiom is familiar to anyone who has used any MS tools and turned it into something completely different. I spend as much time snooping around in IIS7 manager trying to figure out how to do simple tasks as I do actually doing the tasks. It doesn't help that my Windows Server "Bible" - the "mastering" series by Tech Guru Mark Minasi (Who's tech writing style does not have the sedative effect of other such ponderous books) has yet to publish the whole series for 2008 (all that is out is networking - which I have yet to purchase). Ok.. now on to what I learned.

"Renewal" Doesn't Work

The "Server Certificates" area is found in the main properties of the server (not in the properties of individual sites) - so that is the first tip I can give you. If you are hunting around in the site properties for the cert request stuff, go up to the main server settings (click on the server name above your sites in the snap in). You will see a list of certs in "feature" view. Right click on the cert and you will see some of the options you are looking for (renew, remove, create etc.).

As a second tip, you can't actually use the "renew" option if you are renewing a Verisign cert. I tried and VeriSign's signing application would not accept the renewal CSR. According to Verisign support IIS7 creates improperly formatted requests when using the renewal option. Instead you have to create a new CSR using the "create" option. This seemed to work and Verisign gave me back a new cert to process. I thought I was home free. I went back to the server certificates page and chose "Complete Request" from the context menu. I navigated to the file - but it gave me a syntax error. The list of certificates did not change. It still showed the old cert and the old renewal date. What gives?

After trying several approaches with different friendly names (thinking I needed to match something in the file), I navigated away from the server certificates properties and started poking around elsewhere to see if I had missed a step somewhere. Eventually I came back to the "server certificates page and immediately I noticed something odd. There was an additional cert installed without a friendly name. Hmmmm... My new cert had been processed and installed but not assigned to the domain presumably because it was not a renewal. So I had managed to get the cert into the cert store. Now I just needed to figure out how to assign it to the domain.

Assigning the Request to a Site

The basic problem here is that I created and installed a cert into the server, but because I did not follow the renewal process I could not complete the reassignment (sort of "overwriting" the existing cert). Instead I needed to "assign" the new cert to the domain. In IIS 6 this is done through the "Security" dialog box with an aptly named "assign" radio button and wizard. I couldn't find anything like that in IIS 7. Finally, I opened the "bindings" properties and found that, in the edit mode for SSL, I had a drop down of available certs that I could choose for the IP binding. I switched to the cert I had just installed and tested successfully.

Summary

Again this is for a *Verisign* cert when you are trying to *renew* using *IIS 7*.

- Don't use the "renewal" option - instead create a new cert request.
- When installing the approved cert make sure and refresh the list of installed certs. It does not appear to refresh on its own. Even if you get an error it may be related to assignment and not installation.
- To assign your cert to your domain use the "bindings" dialog in the site properties.

Perhaps this will help some of you struggling with the new IDE features of IIS 7.