

Re: EFS Certificates in AD 2003

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2006-06/msg00210.html>

- *From:* "BubBeard" <u23620@uwe>
 - *Date:* Fri, 30 Jun 2006 20:06:56 GMT
-

Thanks Steve. I believe the problem is that the servers do not know that the new CA is in the domain. I did not have a group policy created that assigned the CA certificate. I believe once this is done the servers will trust the Enterprise Trust CTL and use the XP certificate. I do not want to put private keys on all of our servers. The roaming issue is another issue I will have to attend to.

Steven L Umbach wrote:

Unless you are using a roaming profile the only way you can encrypt files on a computer is to have a user EFS certificate AND private key on that computer. Since one did not exist on the server it created one for you as apparently it did not have access to the CA. If you had imported your EFS certificate and private key into your user profile on the server using a password protected .pfx file that you exported from the computer that did contain your EFS certificate and private key then it would have been used. Otherwise if you logon to ten different computers using EFS you will have at least ten different EFS certificates/private keys. Yes this does make EFS confusing and challenging in environments where you want to have EFS files on more than one computer. Be sure to read the link below on EFS best practices if you have not seen it yet. It is not that hard for a user to lose permanent access to his own EFS files. --- Steve

<http://support.microsoft.com/default.aspx?scid=kb:EN-US:223316> --- PKI best practices.

I have an Enterprise 2003 CA that is issuing Basic EFS certificates. When I

[quoted text clipped – 15 lines]

don't
know how to remove it.