

Re: General help with XP, EFS, and Domain

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2008-05/msg00102.html

- *From:* "Steve Riley [MSFT]" <steve.riley@xxxxxxxxxxxxxx>
 - *Date:* Wed, 7 May 2008 20:50:21 -0700
-

How can I mitigate this risk?

Alas, it's the answer you don't want to hear: use an enterprise CA. Why do you not want to do this?

Steve Riley

steve.riley@xxxxxxxxxxxxxx

<http://blogs.technet.com/steriley>

<http://www.protectyourwindowsnetwork.com>

"AJ Harper" <andyjharper@xxxxxxxxxx> wrote in message

news:9c9543e9-fb59-4ff6-9232-99a83f369b8c@xx

Greetings,

Bear with me if this is a longer post. I have a need to allow XP machines in my domain to encrypt data via EFS but also allow the domain admins to recover the data in a emergency. We don't want to institute an Enterprise CA. So, I have created a cert and private key via the cipher command and imported that into my default domain policy. However, when a user encrypts his/her files it also looks like a key is created locally (unique to the user). This isn't an issue except I've seen software out there that claims it can break encryption as long as the local keys haven't been tampered with or the password/SAM file is available.

How can I mitigate this risk? If I export the local cert and private key and then select the option to remove the private key if successful, then they need to import it again to open the files. They can't do this every time. What is the best option for my scenario and at the same time make those EFS recovery products useless? Do I just use another product like TrueCrypt and develop a process that way? Thanks for any help anyone can provide.

Re: General help with XP, EFS, and Domain