

Re: EFS recovery problem

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2003-05/0300.html

thiessendg_at_yahoo.com

Date: 05/02/03

Date: 2 May 2003 11:38:25 -0700

Roger,

Thanks for all the help so far. Obviously, I should have studied EFS before enabling it, but, I had been using it for a year with no problems. It only takes one time...

Anyway, I haven't checked, but, could this be an ownership issue also?

When I try to view the files encrypted with the thumbprint from the Dave User cert, I get "Access Denied". I assume that message is sent because of encryption, but, I got to wondering about ownership, especially now since my account name is Dave for some reason.

Here is my plan of attack, in case that doesn't work. Use the certificates mmc snap in, export the Dave User certificate (in *.p7b format??), log in to admin, create new account, import cert to that account, restore files from backup to that new account, try to decrypt.

Does that sound right?

One note, again, the password was set from the Computer Management Admin tool to the password it used to be, but, since there was no luck with that, I log into acct and try to use the Control Panel and set password from the account. It is not letting me though. Gives me the business about complexity, etc., however, there is no policy for complexity. ./

Seems this account is hosed, but, seems like I should still be able to decrypt those files since I still have a cert with that thumbprint.

Suggestions/Comments?

V/R,
Dave

"Roger Abell [MVP]" <mvpNOSPAM@asu.edu> wrote in message

news:<eMT7bdLEDHA.2384@TK2MSFTNGP12.phx.gbl>...

> *Renaming an account should not cause these issues,*
> *and when an account is renamed it is normal for the*
> *profile area on disk to retain the name that existed*
> *when the account was first logged into.*
>
> *I would focus on getting the data back first, and then*
> *on making the account function correctly. That you*
> *are seeing a second EFS cert created when you have*
> *deleted the new one and then try to use EFS is showing*
> *that the older certificate is not being recognized as*
> *usable (obviously!). I would first try, though doubt*
> *it will work, exporting the older certificate, using the*
> *Certificates snap-in when the account has the last*
> *known working (for EFS) password and it is the only*
> *certificate showing. If this works, I would then import*
> *that EFS certificate with key into a newly defined local*
> *account, and use that account to get the data stored in*
> *the clear without EFS encryption.*
> *If you are not able to export the certificate and key,*
> *then think very hard over the recent history, focusing*
> *on passwords. You have to have the account set to*
> *use the correct password for the cert/key to be accessible*
> *for EFS use.*
> *Before you go too much further you may want to make*
> *a backup using ntbackup.exe in which you include the*
> *EFS encrypted files, your account's profile from Doc*
> *and Settings, and the System State.*
>
> --
> *Roger*
>