

Re: EFS/DRA

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2008-07/msg00243.html>

- *From:* "Brian Komar \ (MVP\)" <brian.komar@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 24 Jul 2008 23:37:14 -0500
-

If all you want to roam is credential information, then Credential Roaming is definitely the way to go. If you want to roam files as well (profile, desktop, My Documents), then you would be better to go with Roaming Profiles.

Both can be used, but as referenced in the Deploying CRS whitepaper, you need to set up exceptions to prevent the roaming of the credential information in roaming profiles.

If you do not have roaming profiles, and you want to roam EFS credentials, I would lean towards CRS, rather than roaming profiles.

Brian

"Steve" <Steve@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:E15464CC-7DD4-4C68-BB87-75D6A098B9D5@xxxxxxxxxxxxxxxxxxxx

I appreciate the assistance.

I have read about Roaming Profiles and Credential Roaming but I am still confused as to which one I should implement. Can you offer any advice?

Thanks,
— Steve

"Alun Jones" wrote:

"Steve" <Steve@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:B25710B1-0727-4067-AB9F-2EDCD098DD62@xxxxxxxxxxxxxxxxxxxx

> So either I'm missing something, or I completely misunderstand EFS.

>

> I have turned off the self-signed certificates on a few XP machines > (using

> the hotfix from MS and the Group Policy Option to not allow a user to

> create

> self-signed certs).

>

> Since then, when I create an EFS file on my XP machine, it uses a cert

> from

> my CA....Good. But when I try to add another user to the file, he is

> unable

> to open it. (In fact since installing the hotfix and adding the GP > option,

> he

Re: EFS/DRA

- > can't even create a new file on the encrypted share). I have NOT done
- > anything with credential roaming yet. Is that my problem?
- >
- > Bottom line, I want to encrypt a file on my machine (XP), add a user > with
- > the ability to decrypt it, and allow them to open it on their machine. > Is
- > this not possible?

It depends.

To make things easier, let's say that the file is stored on a "server", and needs to be fetched by a user on a "client".

The user's private key must be stored in his personal store on the server. If his key exists only on the client, he must export the certificate and key from the client, and import it onto the server. Because the key must be in his personal store, only the user can do this for himself.

Crazy though it may sound, EFS across a network share decrypts at the server, rather than at the client – the file is transferred across the network in plain text.

An alternative to having to export and import your private key on each server is to use a roaming profile, or credential roaming. Note that these two options are mutually exclusive per user.

Alun.

~~~~~

—

Texas Imperial Software | Web: <http://www.wftpd.com/>  
23921 57th Ave SE | Blog: <http://msmvps.com/alunj/>  
Woodinville WA 98072-8661 | WFTPD, WFTPD Pro are Windows FTP servers.  
Fax/Voice +1(425)807-1787 | Try our NEW client software, WFTPD Explorer.