

Re: EFS – Encryption and User Migration

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.general/2005-03/0853.html>

From: Steven L Umbach (n9rou_at_nospam-comcast.net)

Date: 03/10/05

Date: Wed, 9 Mar 2005 22:18:34 -0600

Hi Gerry.

I agree that EFS can be a real problem but it can be managed centrally. You can either disable it totally for all or select domain computers and you can also enforce that all or select domain computers use a central recovery agent. In this particular situation with a migration I agree that plain text backups is the best way to insure that data is not lost. --- Steve

"Gerry Hickman" <gerry666uk@yahoo.co.uk> wrote in message news:e0oNJ6OJFHA.3356@TK2MSFTNGP12.phx.gbl...

> *Hi Damon,*

>

> *It's probably not the answer you want, but my way of dealing with EFS is to ban all users from using it – end of story.*

>

> *In my view, it was badly thought to allow simply allow it to be enabled by a "tick box" in the GUI, making it user specifig and having no central control mechanism.*

>

> *One option with the laptops, would be to simply unencrypt EVERY file on the laptop, then do what you want to do, then re-encrypt if you want.*

>

> *I'd tell users of any such laptops to make sure everything they care about is backed up. If they don't have a backup system, they should not be allowed to have laptops in the first place.*

>

> *One thing I can help with, is finding encrypted files; this is great if you only have 30 rogue files among 20,000 on a laptop, but in your case it's pointless because you've already said ALL files are encrypted!*

>

> *Damon Birrell wrote:*

>

>> *Hi*

>>

>> *Apologies for the cross post, I believe these queries have relevance in several groups. I am working for a large Police organisation and we are planning a migration using ADMT2. Scenario is this:*

>>
>> 1) Two domains in same forest (intraforest migration)
>> 2) One domain is uplifted NT4 to W2K3 domain in W2k3 native mode, call it
>> SOURCE domain
>> 3) Other domain is W2K3 Domain in W2k3 native mode, call it TARGET domain
>> 4) SOURCE holds user accounts and groups
>> 5) TARGET holds machine accounts
>> 6) All workstations and servers have already joined TARGET domain
>> 7) Users login to the SOURCE domain
>> 8) All laptops have the logged on user's My Documents folder encrypted
>> using the CIPHER command upon logon either through a local machine script
>> or network login script depending upon their logonserver.
>> 9) We wish to migrate the user accounts to the TARGET domain with the
>> intention of decommissioning the SOURCE domain.
>>
>> My understanding is that Encyption will pose a problem, even with
>> SIDHistory and once I get the formal test environment running I expect to
>> observe that users who are migrated from SOURCE to TARGET will not be
>> able to access their previously encrypted files.
>>
>> QUESTION 1: Is this above statement correct?
>>
>> We are in a situation where we have a lot of users with laptops who may
>> or may not be connected at the network for long periods of time. We also
>> have a requirement to maintain security (i.e. encryption) until just
>> before the user is migrated. We are yet to determine the order in which
>> we are migrating users but I am confident that we will NOT be able to
>> determine which users are laptop users, and if they have logged onto
>> multiple laptops and encrypted data, we have no real way of knowing this.
>> Since users may not be on the network during the time we migrate them,
>> reversing the CIPHER command in the loogn scripts etc is not going to
>> catch all cases. e.g. one user who has logged onto multiple laptops.
>>
>> QUESTION 2: What is the best means of circumventing data loss in these
>> circumstances? I figured that we are probably going to have to perform
>> data recovery as the norm. I had several lines of thought a to how to
>> attack this problem, including a certificate export/import as part of an
>> automated script process. Will this approach actually work and if so,
>> what are the pre-requisites for allowing such a data recovery to take
>> place? (i.e. Domain recovery agent requirements, user certificate
>> requirements, etc). I expect that the following process may be a possible
>> solution, if it works:
>>
>> Rough Algorithm:
>>
>> If machine is a laptop
>> Determine if user has been migrated or not via central log
>> If Not Migrated
>> Export users certificate (CER/PFX) using CIPHER /r and store on
>> secured file share
>> Update a central log that user has not been migrated but cert has

>> *been backed up*
>> *Flag user to list of users who can be migrated*
>> *If migrated*
>> *Import users certificate (somehow, automatically without wizards*
>> *appearing or requiring user input)*
>> *End If*
>>
>> *I have scripted the "IF not migrated" part but struggled to get the*
>> *syntax using certutil, certmgr and rundll crypt.dll commands to automate*
>> *the import process of a certificate from a file. I guess I need to know*
>> *if it will even work before I continue...*
>>
>> *Anyone got any ideas?*
>>
>> *Regards,*
>> *Damon*
>>
>>
>>
>>
>>
>>
>
>
> --
> *Gerry Hickman (London UK)*