

## Re: EFS – Encryption and User Migration

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.windows.server.security/2005-03/0163.html>

---

**From:** Steven L Umbach (*n9rou\_at\_nospam-comcast.net*)

**Date:** 03/09/05

Date: Tue, 8 Mar 2005 23:03:57 -0600

I really don't know the answer to your dilemma but I will warn you that there is absolutely no room for error when it comes to EFS encrypted files. If it is done incorrectly or there is a glitch, that data can be lost forever. At a minimum you will have to make sure that all users that use EFS have exported their EFS certificate and private key to a password protected .pfx file and that all computers are configured to use a domain Recovery Agent. The safest way will be to have clear text backups of any files that are currently encrypted with EFS during the transition. I will not make any recommendation beyond that or use the phrase "this should work". — Steve

"Damon Birrell" <sophdamon.nospam@adsl.on.net> wrote in message news:ui88AfEJFHA.4028@tk2msftngp13.phx.gbl...

> *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 as 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*  
>  
> *II 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*  
>  
>  
>  
>  
>

microsoft.public.windows.server.security: Re: EFS – Encryption and User Migration

>