

Re: Password question

Source:

<http://www.tech-archive.net/Archive/Certification/microsoft.public.cert.exam.mcse/2004-03/0733.html>

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

Date: 03/09/04

Date: Tue, 09 Mar 2004 18:52:36 GMT

This change [versus W2K EFS] was done to improve confidentiality of EFS encrypted files. In W2K a recovery agent was required for EFS while it is not in XP Pro. In W2K it was very simple for someone with administrator credentials to access a users EFS files by simply resetting a users password and logging on as that user. That is why the change was implemented as that tactic will not work with XP Pro. Of course there could be a recovery agent configured in a domain that would also apply to XP computers that would allow any domain administrator with access to the recovery EFS private key to access the users files. A user can use efsinfo /r to see if a recovery agent is associated with their EFS files. The changes also make non domain XP Pro laptop computers using EFS more secure in that someone would need to know the password [which protects the EFS private key] for the user that encrypted the files, which can be obtained however by using a password program like LC4. Exporting and deleting the EFS private keys on an XP Pro computer that has no recovery agent would make it impossible for someone to access the EFS encrypted files if best practices are followed including encrypting only folders and may include the use of cipher /w or better yet a disk scrubber [such as East Tec Eraser] in very high security situations. See the link below for information on why password resets cause the behavior you describe. --- Steve

<http://support.microsoft.com/default.aspx?scid=kb:en-us:309408>

<http://support.microsoft.com/default.aspx?scid=kb:EN-US:223316> --- general EFS best practices.

"MikeF" <ctatraining@no-spamzapcomcast.net> wrote in message news:exoPCcXBEHA.1792@TK2MSFTNGP12.phx.gbl...

- > *There has to be an answer to this, but it has eluded me. Regarding 2K3 and*
- > *XP, Msft says:*
- >
- > *...after a user's password is reset, some types of information are no longer*
- > *accessible, including the following:*
- >
- > *E-mail that is encrypted with the user's public key*
- > *Internet passwords that are saved on the computer*
- > *Files that the user has encrypted*
- >
- > *To avoid such data loss, do not reset a user's password. When a new local*
- > *user account is created, have the user create a password reset disk. Then,*

microsoft.public.cert.exam.mcse: Re: Password question

- > *if the user forgets the password, the password reset disk can be used to*
- > *reset the password without data loss. If a user forgets the password to a*
- > *domain user account, the password must be reset manually.*
- >
- > *Unquote. That is, you, the admin, can't use the reset disk to reset the pw*
- > *on the domain account. However, on the reset domain account password page,*
- > *they give the same warning about data loss.*
- >
- > *So the user loses his keys and certificates if heshe forgets hisher AD*
- > *password? This is very unlike MSFT. Is the only way around this for the*
- > *admin to recover the users encrypted stuff, give it back to the user*
- > *unencrypted, & reset the password?*
- > *TIA*
- > *Mike*
- >
- >