

# Re: Co-Administrator

---

*Source:*

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2007-12/msg02643.html>

---

- *From:* "tatat" <default@xxxxxxxxxx>
  - *Date:* Tue, 18 Dec 2007 14:35:46 -0800
- 

"kj [SBS MVP]" <KevinJ.SBS@xxxxxxxxxxxxxxxxxxxx> wrote in message <news:eNEFwGaQIHA.536@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

tatat wrote:

Using the built in Encrypting File System (EFS) it's possible to restrict access to the point that administrators cannot read the files without the proper account password. Learning curve is a bit steep. Practice on a workstation until you get the hang of it.

Leaks like a sieve. All the admin (or anyone else) needs is one of the encrypting certs or the recovery cert. Oh, and the admin is also the Certificate Authority Manager, so exporting any cert issued by it is trivial.

Not that it's not possible, just that using built in CA still has the Domain Admin still in control (by default).

Best practices for the Encrypting File System:

<http://support.microsoft.com/kb/223316>

"Charles" <Charles@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message <news:07ECA812-C39E-4A01-83B2-9A864524AB34@xxxxxxxxxxxxxxxxxxxx>

Hi,

I would like to grant admin rights with a young colleague so that he can help me with all the IT stuff. Problem: there are certain

Re: Co-Administrator

shared  
folder containing sensitive info that he cannot access now ---  
and I  
would like it to  
stay that way. Is there a simple way to give him enough  
rights to do  
the IT  
admin work, while keeping him from given shared folders?

So far this is what has kept me from granting him admin  
rights, so  
any help  
appreciated;

Charles

--  
/kj

Leaks like a sieve only if implemented incorrectly hence my comment about the learning curve. Documentation is readily available. A couple of necessary steps are the designation of a data recovery agent with the EFS certificate/key exported to a removable device, same with the EFS certificate/key of the administrator account. Then delete them from the server.

The EFS encrypted files are no longer readable by the Administrator or data recovery agent accounts until the certificate/key is re-imported (marked as not exportable for an extra layer of security, then deleted at the end of a recovery session)

If you know of a way to bypass the security built in to EFS when used as documented please post here. I would like to test it.