

Re: About EFS and local certificate that I want to export in SBS

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2007-05/msg00837.html>

- *From:* "Dave Nickason [SBS MVP]" <gwdibble@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Fri, 4 May 2007 14:18:49 -0400
-

If that's the case, then you should install a certification authority on the SBS. It's probably not a good practice to let users encrypt data otherwise, since you risk someone maliciously encrypting data that you will then be unable to recover. It's a two-second thing to install the CA – on the SBS just go to CP Add/Remove → Add and remove Windows components. Add Certification Authority. From there, it should just work – users who encrypt files will automatically get a certificate from the CA.

I probably had a CA installed before I started supporting encryption.. I don't really remember, but I do use the CA to issue certs for wireless authentication, so it's been on my SBS for quite a while.

"Pascal" <pascal_t@xxxxxxxxxxxxxxxxxxxx> wrote in message <news:mn.24767d7563417b3d.70874@xxxxxxxxxxxxxxxxxxxxxxxx>

Hi Dave,

I am afraid that what you said is not true :D

Indeed, I just have to do what you say if I have a certificate authority but without I tried what you said but I always have the same problem.

The message is "No certificate appropriated for the selected user" (perhaps not exactly the same because it's a french translation ;))

If you have any other idea, do not hesitate !

Thank you

This is easier than you think. When you encrypt a file for the first time, the desktop PC gets a user certificate from the SBS. You should not have to configure this, it should happen automatically. You don't have to export certificates or anything like that – just the act of encrypting a file will cause the cert to be issued or installed on the workstation.

Re: About EFS and local certificate that I want to export in SBS

So Pascal logs in and encrypts a file on any workstation. The cert is installed. Isabelle does the same thing. Now Isabelle wants to give Pascal access to her encrypted file. She opens the properties of the file, clicks Advanced (General tab) -> Details. In the Encryption Details window, she will be able to add Pascal to the permissions, IF Pascal has already encrypted a file on that workstation so that his certificate is installed. Remind Isabelle about the NTFS permissions, too, because transparent access for encryption purposes still requires access from NTFS security.

The bad news is that I don't know how to add this access to more than one encrypted file at a time. As nearly as I can tell, it can't be done at the folder level. I haven't researched this and it seems like there would be a way to apply the settings to a whole encrypted folder at once - if you figure it out, please post back.

I strongly recommend that when anyone encrypts a file for the first time on any given PC, look in the Details and make sure that Administrator is listed as the EFS recovery agent. Recovery agent should be configured in Group Policy. It's in the Default Domain Policy under Computer Config -> Windows Settings -> Security Settings -> Public Key Policies -> Encrypting File System. Everything you need is on the r-click menu. In addition to making sure there is a recovery agent configured, make sure the agent certificate is not expired.

"Pascal" <pascal_t@xxxxxxxxxxxxxxxxxxxx> wrote in message news:mn.239b7d751bea3037.70874@xxxxxxxxxxxxxxxxxxxx

Hello,

I have test something but I am not sure that I am right !

I have two computers XP_A and XP_B member of an active directory domain with no certificate authority. There are two users : Pascal and Isabelle.

1. Pascal logs on XP_A and encrypt a file with EFS.
2. Pascal exports his certificate through Internet explorer (with or without the private key, the issue will be the same)
3. Now, on XP_B, an admin install the Pascal certificate on the computer (in the "Trusted People" store).
4. Isabelle logs on XP_B and encrypts a file with EFS, then she adds the Pascal certificate to authorize him to access this encrypted file.
5. Pascal is connected to XP_A and opens the encrypted files for which his certificate is attached on XP_B, but he still has an access

Re: About EFS and local certificate that I want to export in SBS

denied.

Question : Why Pascal is not able to access this file from the network ?

(From XP_A to XP_B)

More generally, if I export an EFS user certificate from one computer to another, can I access the encrypted file through the network.

With a certificate authority, I think there will be no problem but I would like to understand why like this it is not working.

Thank you !

— Pascal

—
Pascal