

# Re: Using EFS on a server shared drive

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2006-05/msg00105](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-05/msg00105)

---

- *From:* blankmonkey <[blankmonkey@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:blankmonkey@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Mon, 1 May 2006 17:48:02 -0700
- 

Yep, i read through this front to back, and it didn't help. I have gotten the system working as follows  
userA maps drive to server, creates and encrypts fileA  
userB maps drive to server, creates and encrypts fileB  
Then user A adds userB to the encrypt allow list, and it works.

BUT

the keys here, are on the server, so how does UserA or UserB export their private keys?  
Or are they supposed to be able to export this key through the certs mmc from the local workstation?  
I have imported a key at the local workstation, and it fails, because the key has to be on the server, so how can i import a key to the server cert lsit, WITHOUT logging on the the 'local machine', the server in this case.

"Jorge Silva" wrote:

Hi

Here it is a more complete article that covers most of the possible actions, please see if it helps:  
Encrypting File System in Windows XP and Windows Server 2003  
<http://www.microsoft.com/technet/prodtechnol/winxpro/deploy/cryptfs.mspx>

--

I hop that helps

Good Luck  
Jorge Silva  
MCSA  
Systems Administrator

Re: Using EFS on a server shared drive

"blankmonkey" <blankmonkey@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message  
news:6A2C41E4-EA7B-4106-8054-BC7C9461064E@xxxxxxxxxxxxxxxxxxxx

I am not so concerned about the revocation status of a cert, but more of  
backing one up. Since this is on the server, the user does nto have  
access  
to the "local machine" were the certs are stored, so how do you export  
them  
without logging onto the server as the user?

"Jorge Silva" wrote:

Hi

Windows XP performs revocation checking on all  
certificates for other  
users  
when they're added to an encrypted file. For performance  
reasons, users  
that  
hold a private key are not checked for revocation. However,  
certificates  
that do not contain a CDP (Certificate Revocation List  
Distribution  
Point)  
extension (such as those from some 3rd party CAs) will not  
be validated  
for  
revocation status.

Check for more info:

<http://www.microsoft.com/windowsxp/using/security/expert/sharefilesefs.mspx>

--

I hop that helps

Good Luck  
Jorge Silva  
MCSA  
Systems Administrator

"blankmonkey"  
<blankmonkey@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in

Re: Using EFS on a server shared drive

message

[news:4964C667-5D51-48C4-AD09-398737683BD6@xxxxxxxxxxxxxxxxxxxx](mailto:news:4964C667-5D51-48C4-AD09-398737683BD6@xxxxxxxxxxxxxxxxxxxx)

I want multiple users to share an encrypted file on a File server using W2k3. I can get this to work fine, but with one major problem. After the file is created, the person to be added has to log onto the server to export their key, so that others can add them to the allowed keys to un-encrypt. Obviously, i do not want my users logging into the server via RD or console, and there may be 100's of users. Is this the way it is supposed to function? how do i export my key that is on the server, from my workstation?