

RE: Tired of fighting with Group Policy and Offline File Encryptio

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.group_policy/2006-06/msg00270.html

- *From:* Vbangia <Vbangia@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 27 Jun 2006 12:46:02 -0700
-

I was having this SAME EXACT issue. I just got off the phone w/ Microsoft. There is a hotfix available for this issue on XP post SP2. I just applied it to a few workstations and it FINALLY worked. The KB Article number is 810859. The file name is WindowsXP-KB810859-x86-ENU.exe.

"Engineer_Dell" wrote:

If my 1st post solution doesn't work then you may try these steps;

Modify the Active Directory Group Policy setting:

To modify the Active Directory Group Policy setting to reference the new Group Policy Client Side extension, use the new Client Side extension in an Active Directory Group Policy setting.

Note Update the System.adm file and the Group Policy object in Active Directory. Update the System.adm file first. To do this, follow these steps:1. Update the System.adm file to include the CLIENTTEXT line, as follows:POLICY!!Pol_EncryptOfflineFiles

```
#if version >= 4
SUPPORTED !!SUPPORTED_WindowsXP
#endif
VALUENAME "EncryptCache"
EXPLAIN !!Pol_EncryptOfflineFiles_Help
VALUEON NUMERIC 1
VALUEOFF NUMERIC 0
CLIENTTEXT {C631DF4C-088F-4156-B058-4375F0853CD8}
END POLICY
```

To find the System.adm location path for the Group Policy setting, follow these steps:a. Use the Active Directory Users and Computers tool to select a container where the Group Policy setting is applied.

b. Change the container to display the Group Policy setting GUID. An example of this GUID is {9F16DD40-9777-4AD9-870C-9B9F1E73203E}.

c. Use the Active Directory Service Interfaces (ADSI) Edit tool or the EnumProp tool to display the gPCFileSysPath attribute, as in the following

RE: Tired of fighting with Group Policy and Offline File Encryptio

exampe:

enumprop "LDAP://mydc/CN={3D6FF2C0-1DFC-41A9-AE72-D4502BDA81E8}.CN=Policies,CN=System,DC=mycompany,DC=com"

The following example shows the gPCFileSysPath attribute:

LDAP://machinedc/CN={3D6FF2C0-1DFC-41A9-AE72-D4502BDA81E8}.CN=Policies.CN=System,DC= mycompany,DC=com: 19 set properties.

gPCFileSysPath:

\\Test.net\SysVol\mycompany.com\Policies\{3D6FF2C0-1DFC-41A9-AE72-D4502BDA81E8}

Note The EnumProp tool is included in the Windows XP Resource Kit.

- Update the Active Directory Group Policy object to include the Client Side extension in the gPCMachineExtensionNames attribute. To do this automatically in the Group Policy Editor snap-in, follow these steps:
 - a. Use the Group Policy Editor snap-in to modify the Group Policy setting.
 - b. Modify the "Encrypt the Offline Files cache" Group Policy setting.

Note Because the "Encrypt the Offline Files cache" Group Policy setting is now linked to the new CLIENTTEXT line in the System.adm file, the Group Policy Editor will automatically update the gPCMachineExtensionNames Active Directory attribute to include the new Client Side extension GUID.

"Nivek R." wrote:

I'm trying to ensure that the Offline Files (client-side cache), on my client computers are encrypted. I tried applying the Group Policy: Computer Config \ Admin Templates \ Network \ Offline Files \ Encrypt the Offline Files Cache = Enabled, but that only served to grey out the "Encrypt offline files to secure data" box in the "Folder Options" ==> "Offline Files" Tab, but did not force a check mark into that box. Essentially, it took away the user's ability to encrypt the files, but it didn't actually encrypt them. The same issue was discussed, but not satisfactorily answered by the MS Tech at

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2006-04/msg005

This also led me to look into the hotfix suggested at MS KB810859 (<http://support.microsoft.com/default.aspx?scid=kb:en-us:810859>), but I wasn't getting the error that the hotfix applied to in my event logs, also, my test user is an admin on both machines, so I didn't think the hotfix should apply. The document was also vague about where the hotfix should be applied (client or dc?), and it looked as though my settings in the system.adm file in both locations was correct. I also read various Technet articles about EFS, and none seemed to have the answer I was looking for.

In an effort to get to the root of the problem, I've deployed a test lab with two clients using CSC. On these PCs, I've enabled offline files. I've checked the "Encrypt..." box on one, but not the other. When I apply the GP, the encrypt box stays checked or unchecked based upon how it was before

RE: Tired of fighting with Group Policy and Offline File Encryptio

applying the GP. However, when I checked the box on the one computer, the "encrypting" progress bar never appeared. When I browse to either computer's CSC directory from my admin computer over the network, no files appear in green (as they should when encrypted – all systems are running XP SP2). I tried first re-initializing the cache (CTRL + SHIFT + click "Delete"), but that didn't help, so I disabled offline files on both machines, deleted the "EncryptCache" registry value under the following keys:

HKLM \ Software \ MS \ Windows \ Current Ver \ NetCache (I think this one has precedence)

HKLM \ Software \ Policies \ Microsoft \ NetCache (Don't even know what this is for)

I then deleted all items out of the CSC folder on both machines and rebooted. Re-enabled offline files and encryption, but again, the "encrypting" progress bar never appeared. So I can't even get the files to encrypt correctly, let alone get the GPO to apply its encryption policy correctly. I'm trying to avoid going door-to-door to encrypt files on every client PC, and trying to make it so users can't decrypt files that have already been encrypted. Microsoft's documentation has really done nothing for me here, except maybe run me around in circles. I could run insert a ..reg file in a logon.bat, however I really don't want to give my users registry access, and I'm not confident that would even work, since nothing else seems to be actually encrypting the files.

Any help here would be GREATLY APPRECIATED. Thank you.

Pertinent info:

Both PCs are identical – XP SP2 Toshiba laptops, 256MB RAM, GPs are now set

to do nothing except allow the use of EFS – so nothing in GPs should be interfering with the encryption of files. Other GPs from the same test GPO were applying correctly when they were enabled. Nothing's compressed (which would prevent encryption from occurring). Files are on NTFS partitions. The test users that are trying to encrypt the files are local admins, also, I've tried applying settings using a Domain Admin as well.

Other pertinent docs I've read through and tried to apply practices from:

http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/csc_encrypt.msp

<http://www.microsoft.com/technet/prodtechnol/winxpro/reskit/c18621675.mspx>

<http://technet2.microsoft.com/WindowsServer/en/Library/b505401c-5ec8-4f0f-b82b-ea24b28bfbd1>

<http://technet2.microsoft.com/WindowsServer/en/Library/7161080d-270c-4a1c-8ce1-8d45dd6d7b59>

<http://technet2.microsoft.com/WindowsServer/en/Library/04122595-5d30-4b19-945a-b6e4bb33bd6>

RE: Tired of fighting with Group Policy and Offline File Encryptio

<http://thesource.ofallevil.com/technet/prodtechnol/winxpro/deploy/cryptfs.mspx>

<http://www.microsoft.com/technet/archive/community/columns/tips/inttips.mspx?mfr=true>