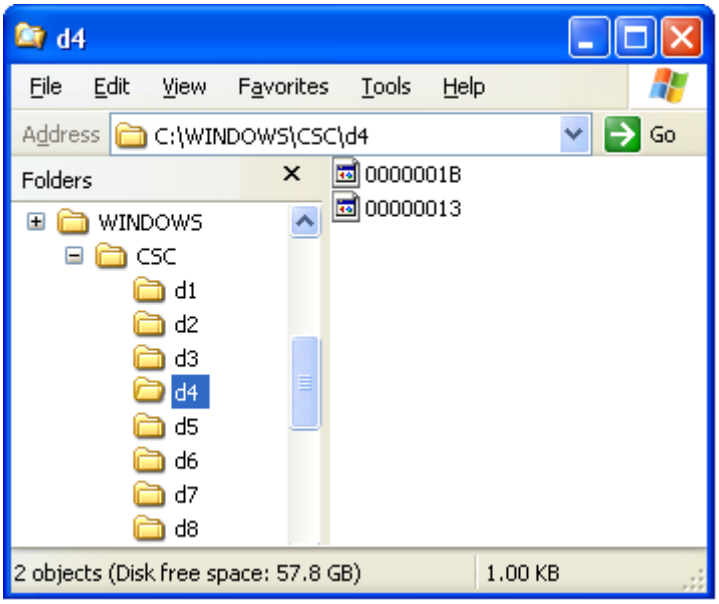
UNITEDLEX

Windows Offline Files

1. Description:

Windows Offline Files or Client Side Caching (CSC) allows files and folders stored on any Server Message Block (SMB) network share to be available offline. To further simplify, an SMB network share is basically any folder that is shared over a network. The Windows Offline Files allows those shared folders to be accessed when the user is offline or disconnected from the network. Offline Files can be enabled by either the user or via the domain if the computer belongs to one. Windows Servers 2003 allows My Documents redirect which Windows Server 2008 allows My Documents, Desktop and Favorites redirection. Offline Files operates by storing a copy of the network data in **%SystemRoot%\CSC** folder (Example: C:\Windows\CSC).

All of the data found in the CSC folder can be encrypted. The Windows XP CSC folder will have no recognizable structure, extensions or file names as seen below. Windows Vista and 7 will be completely accessable and recognizable.



Once enabled and configured, the Offline Files will be available and usable exactly as if online and connected to the SMB network share. When the computer is later reconnected any files modified, added or deleted in either location will be updated.

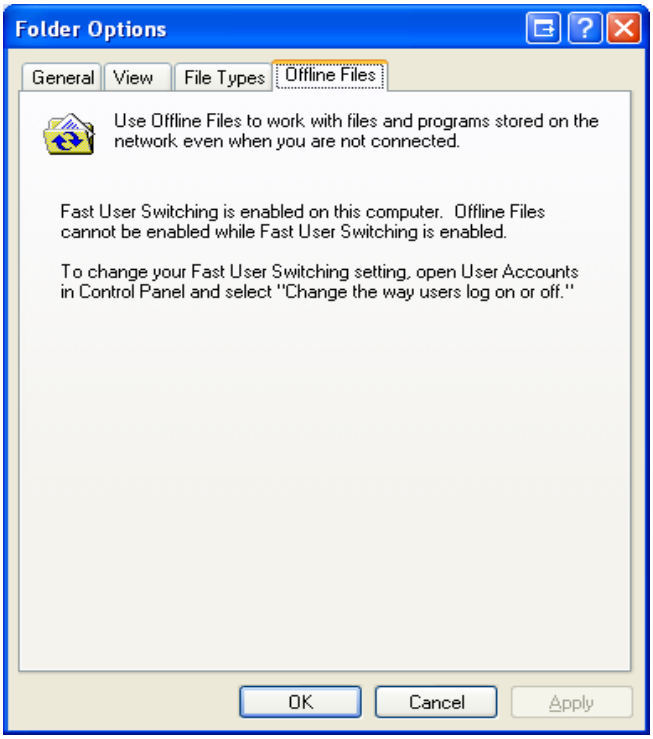
** Note it is also possible to use Offline Files with third party servers if they have SMB protocol installed. For example, UNIX or Netware servers can use a product, such as Samba, to setup SMB.

2. Requirements:

Offline Files require an SBM network share with one of the following versions of Windows:

- XP Professional
- Vista Business
- Vista Enterprise
- Vista Ultimate
- Windows 7 Professional
- Windows 7 Ultimate

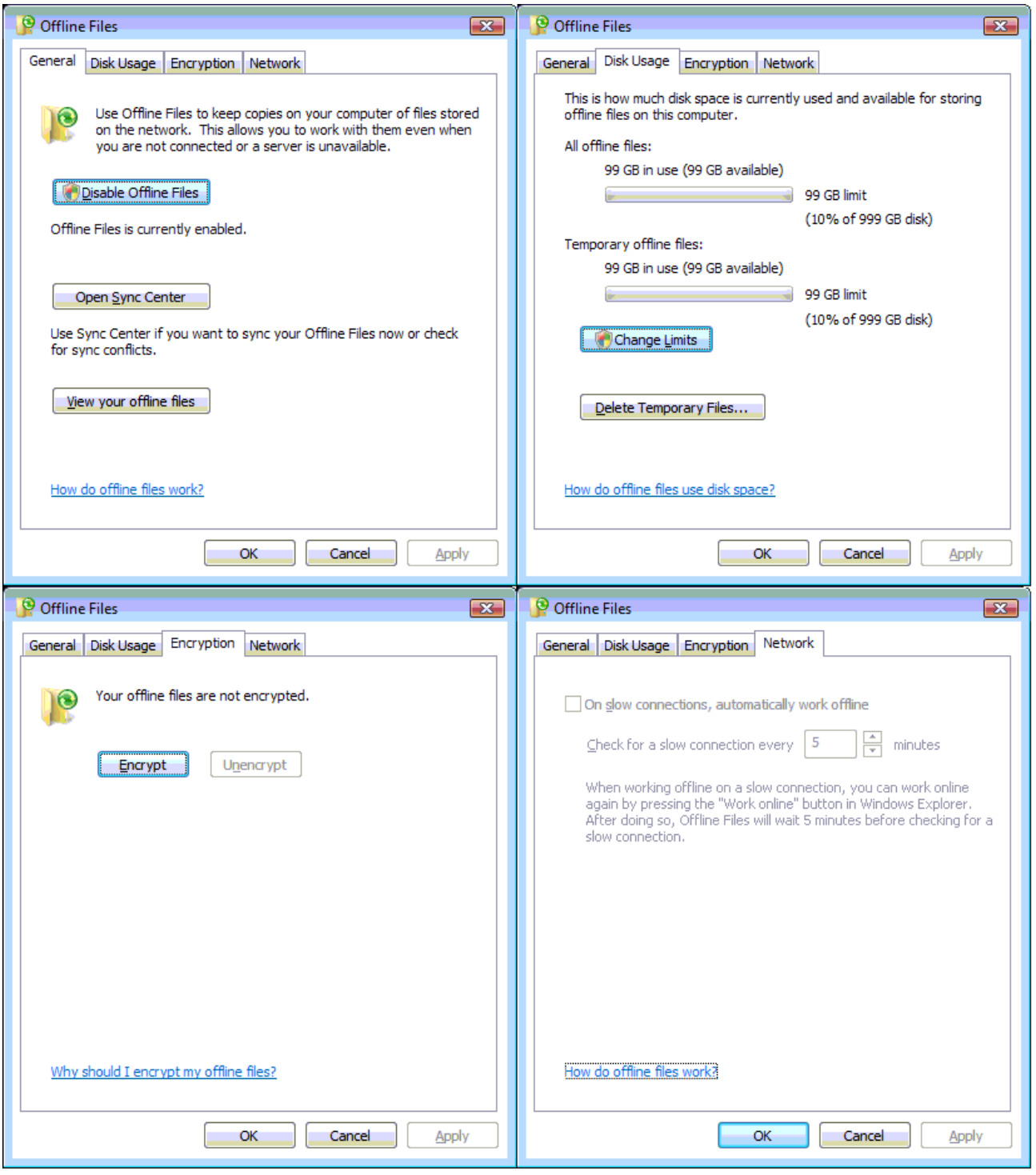
** NOTE: If Fast User Switching is enabled in Windows XP none of the options from the Offline Files tab will be available as seen below:



3. Enabling And Configuring Offline Files:

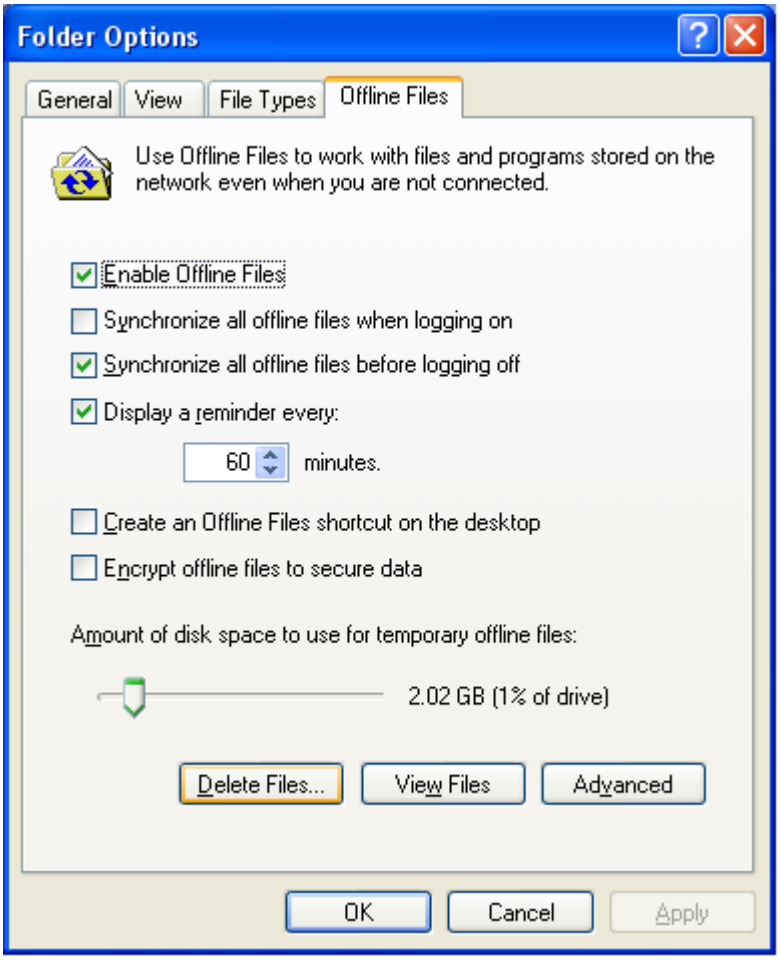
Windows Vista and 7:

1. Offline Files is enabled by default in every version of Windows Vista and 7 that supports it. The settings are accessible through the Offline Folders icon in the Control Panel. The default settings for Offline Files are displayed below:



Windows XP:

1. To enable Offline Files open **My Computer** or **Windows Explorer.**
2. On the **Tools** menu, click **Folder Options**.
3. Select the **Offline Files** tab.
4. Select the **Enable Offline Files** check box, and click **OK**. The default settings for Offline Files once enabled are displayed below:



** Note simply enabling Offline Files will automatically create the CSC directory and sub directories in Windows XP. When using Windows Vista and 7 the CSC folder exists by default.

4. Creating Offline Files:

Windows Vista and 7:

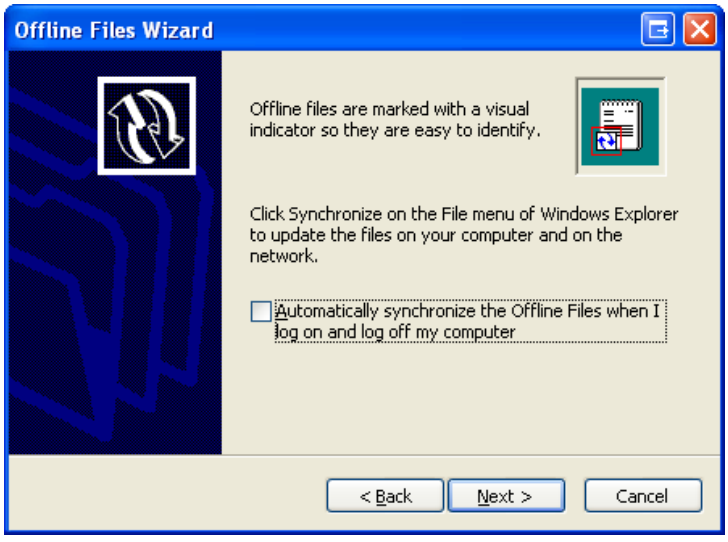
1. Right-click on any file or folder on an SMB network share and select **Always Available Offline.**

Windows XP:

1. Once Offline Files is enabled, right-click on any file or folder on an SMB network share and select **Make Available Offline**. The first time this is done the Offline Files Wizard will appear as seen below:

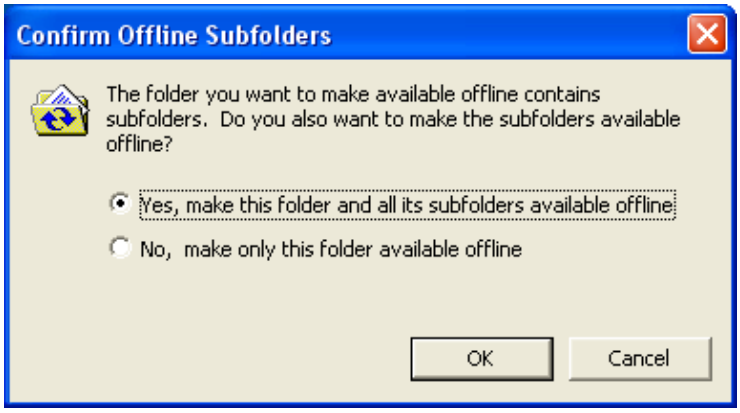
A.

B.



C.

D.



** Note the Offline Files Wizard will only be presented the first time and each consecutive time will show only step D.

5. Synchronization And Conflicts:

Synchronization is typically done automatically when the computer logs on or off but can be initialized manually by the user at anytime.

Because Offline Files will not synchronize files that have open handles they will not be automatically synchronized. Many of the files that have open handles when opened include *.slm, *.ldb, *.mdw, *.mde, *.db, *.mdb and *.pst.

A conflict in Offline Files will typically occur when changes are made to the same file in both locations. When this occurs, you are prompted to make decisions regarding what version of the file to save:

- Keep the workstation version.
- Keep the network version.
- Keep both versions (will require one to be renamed).

6. Encryption:

Offline Files offers the ability to encrypt the Client Side Cache (CSC) stored on the computer. Encryption is either enabled or disabled and cannot be set to specific files or folders. Offline Files in Windows XP offers encryption only within the context of the local system. Offline Files in Windows Vista offers enhanced security by encrypting each file in the local cache by using each user's local certificate. Encryption is disabled by default in all versions of Windows.

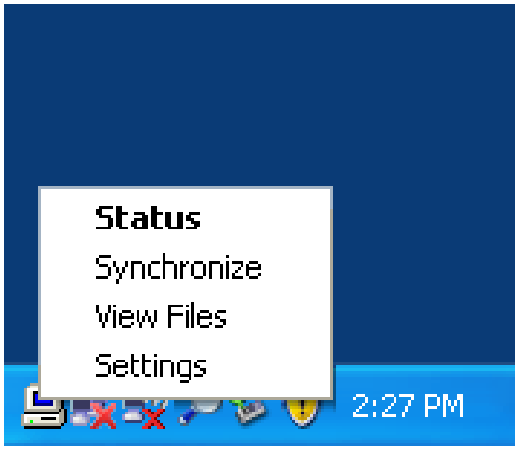
7. Identifying Offline Files:

Offline Files are identified by the icons below which will be found on every file and folder that is available offline. The icons will only be visible on the computer with Offline Files configured and not from any other workstation connected to the same share.

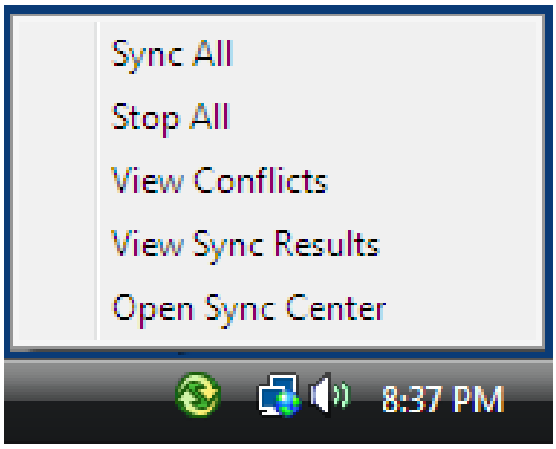
Windows XP

Windows Vista

Offline Files can also be identified on the taskbar with access to more options when clicked as seen below:



Windows XP



Windows Vista

8. Default Size And General Information:

Windows Vista has a default empty size of 68 bytes (3 files, 3 folders).

- The CSC folder has very limited access. Even a Windows Vista local administrator will not have permission to access this folder. Because of this file count and sizes will be unavailable. If the permissions are changed Offline Files will no longer function. This could be used as a method to prevent users from using Offline Files.
- If the CSC folder does not exist the computer is either not running the appropriate version of Vista or the user deleted the folder.
- If Offline Files had been used and later deleted with the **Delete Temporary Files…** button the size of the CSC folder will be larger then the default listed above.

Windows XP has a default empty size of 128 bytes (2 files, 8 folders).

- If the CSC folder does not exist, the computer is either running XP Home or Media Center, never configured for Offline Files or the user deleted the folder.
- If Offline Files had been used and later deleted with the **Delete Files…** button the size of the CSC folder will be larger then the default listed above.

** Note in all versions of Windows if Offline Files is disabled all files in the CSC folder will remain unless deleted manually or with the appropriate delete files button.

9. Restoring Offline Files In Windows XP:

The computer used to restore the files will be referred to as lab computer. The lab computer should be running a similar version of the operating system containing the Offline Files to restore which will be referred to as the evidence computer.

1. Disable Offline Files and delete everything in the CSC folder on the lab computer (a restart may be required).
2. Restore the CSC folder from the evidence computer into the CSC folder of the lab computer.
3. Download CSCCMD.EXE which is available in the Windows Server Resource Kit Tools or from http://www.richhoffman.com/csccmd_v1.1.zip
4. Unzip CSCCMD.EXE into **%SystemRoot%\System32** of the lab computer.
5. On the **Start** menu, select **Run** and type **CMD.**
6. Type **csccmd /enable** then hit **enter** on the keyboard**.**
7. Create a restore directory on the lab computer, example C:\Restore
8. Type **csccmd /extract /target:C:\Restore /recurse** then hit **enter** on the keyboard**.**

   ** Note Microsoft Article ID: 884739 contain more command-line options if needed.
9. When finished restoring it will display:

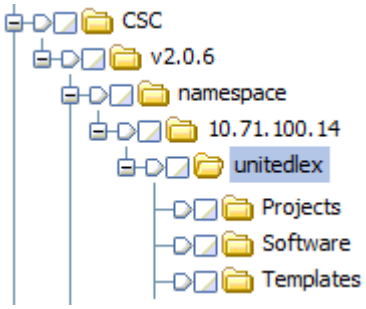
   Extracted # files

   The command has completed successfully.

   ** Note the file size of the CSC folder from the evidence computer should be around the same size as the restored data. The restored files last modified dates, locations and names will match that of the original data. The creation date will be when the data is restored.

10. Restoring Offline Files In Windows Vista and 7:

Restoring offline files in Windows Vista and 7 requires nothing but taking ownership or exporting from EnCase or AccessData FTK. The files and folders are displayed exactly as they are on the SMB network share including the computer name or IP address as seen below:



Please contact me if you find any additional information or misinformation so that I can distribute complete and accurate information.

Feel free to visit www.richhoffman.com for more articles or updated versions as they become available.

Thank You,

Rich Hoffman
UnitedLex
rich.hoffman@unitedlex.com
rich@richhoffman.com
(402) 541-4111