



Protecting Your Local Workspace

As everyone using Autodesk's Vault product line knows, your daily work is performed within the context of your local workspace. As you request data from the Vault, a copy is placed in your workspace for editing or review. When you are finished, that copy is placed back in the Vault for secure storage. But what happens to the work that requires a few days to complete? Simply put, it stays in your local workspace.

The question on everyone's mind is "What happens if my computer dies?" The Vault protects all of its data on the server, but any changes you have made since checking the file out to your local workspace could be lost. Also, any files that you have created but have not vaulted yet could be lost as well.

When your company works with ADRAFT to deploy any of the Vault products, we make sure your data is protected. Not just the server, we setup daily backups for the Vault, but for your local data as well. A handy tool from Microsoft called **Robocopy** does this.

Robocopy, or "Robust File Copy", is a command-line directory replication command. It was available as part of the Windows Resource Kit, and introduced as a standard feature of Windows Vista and Windows Server 2008. Robocopy is designed for reliable mirroring of directories or directory trees. It has features to ensure all NTFS attributes and properties are copied, and includes additional restart code for network connections subject to disruption.

Robocopy is notable for capabilities above and beyond the built-in Windows [copy](#) and [xcopy](#) commands, including the following:

Ability to tolerate network outages and resume copying where it previously left off (incomplete files are noted with a date stamp corresponding to 1980-01-01 and contain a recovery record so Robocopy knows from where to continue).

Persistence by default, with a programmable number of automatic retries if a file cannot be opened.

A "mirror" mode, which keeps trees in sync by optionally deleting files out of the destination that are no longer present in the source.

Ability to copy large numbers of files that would otherwise crash the built-in XCOPY utility.

Ability to copy long file and folder names exceeding 256 characters – up to a theoretical 32,000 characters – without errors.^[1]

Supports multithreaded copying (Windows 7 only).^[2]

There are two different ways that ADRAFT sets up the Robocopy backup routine. The first is run local on the user's PC. A BAT file is created with a simple call similar to the example below. This BAT file is then run as a scheduled task at a regular time.

```
ROBOCOPY C:\AOTCVault\VaultWorkingFolder P:\MAS\LocalWS_Backup /MIR
```

The line above creates a mirror of the local workspace folder

C:\AOTCVault\VaultWorkingFolder to the users share specified by

P:\MAS\LocalWS_Backup. The /MIR argument specifies "mirror" mode. This makes sure that local dir and the network dir are identical every time it's run.

The other method of running this is as a server based scheduled task. The theory is the same. Create a BAT file with the calls and schedule it to run on a nightly basis. This BAT routine is a little bit more complicated because we will want to make sure that we don't hang the program if a machine is inaccessible. The code might look something like this:

```
del C:\LWS_Backup_log2.txt
Rename c:\LWS_Backup_log1.txt LWS_Backup_log2.txt
robocopy \\<mach1>\c$\vault_workspace P:\Users\<User1>\LWSBackup /MIR /R:2 >>
C:\LWS_Backup_Log1.txt
robocopy \\<mach2>\c$\vault_workspace P:\Users\<User2>\LWSBackup /MIR /R:2 >>
C:\LWS_Backup_Log1.txt
robocopy \\<mach3>\c$\vault_workspace P:\Users\<User3>\LWSBackup /MIR /R:2 >>
C:\LWS_Backup_Log1.txt
robocopy \\<mach4>\c$\vault_workspace P:\Users\<User4>\LWSBackup /MIR /R:2 >>
C:\LWS_Backup_Log1.txt
```

This routine keeps a 2 day running log file of its work. You can add as many lines as you have users to backup. It does require some setup such as creating the user shares on the network and making sure that the server has access to the local machine. The specification C\$ is to access hidden shares on the local PC's. If you have publicly C drives then the C\$ can be replaced with your share name.

No matter what method you choose, your working data is protected and secure. Don't take chances with you workspace, backup it up. I have included some images of a local workspace and the network share after running this backup just to show how they look. Besides, an entire article with no pictures is even too nerdy for me.

