COGZ Technical Bulletin

File Corruption caused by Server Opportunistic Locking

When operating in a multi-user environment, correct server settings relating to file system operation are imperative. This is true whether using MS Windows Server, MS Windows Workstation or other platforms as your file Server. Opportunistic Locking (OpLocks) default settings cause data corruption. As such, **to avoid corrupt data files you need to update the default settings to Disable OpLocks.**

CAUTION: As registry changes involve a certain degree of risk, prior to making the changes be sure to follow best practices for Server and Registry Backup, as well as User considerations, etc., as a ***Server Restart is required to activate the registry changes.***

The registry changes need to be made on the server that has the actual COGZ ".TPS" data files. The following information is excerpted from Microsoft Document Q296264:

Note: If you are operating on MS Server 2008 with SMB2 (Server Message Block Version 2) Enabled, please see COGZ Technical Bulletin on SMB2 first.

*You must deny the granting of opportunistic locks by **setting the following registry entry to 0**:*

*HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters**

EnableOplocks REG_DWORD 0 <setting to zero disables oplocks>

*You may have to add this registry entry if not there.

Follow These Steps:

1. Set Registry Oplocks setting to 0.
2. Restart Server (Observe proper server restart protocol)
3. Check Registry Oplock setting to see if it retained Entry and setting of 0.
4. Run File Freshen on all COGZ data files for all properties.

Note: The EnableOplocks entry configures Windows-based servers to allow or to deny opportunistic locks on local files. These servers include workstations that share files.

COGZ has a utility available if you need assistance with these changes. Contact customer service for information.