**Workstation and Server Settings and Troubleshooting for Visual FoxPro Applications
Including: SBT/Accpac Pro Series and VisionPoint, and Sage Pro ERP 100/200 Systems**

 **Client Installation Notes**

Be sure to install the Pro client with Local Administrator rights. In Windows 7/Vista, it may be necessary to right-click the setup program and select “Run as Administrator.” Before installing the client, you should verify that you have the proper drive letter mapping to the Pro root. Pro will not run properly using “UNC” paths in its shortcut. Verify that the shortcut is installed correctly, by right-clicking it, and selecting Properties. ALL users of Pro must have full Administrator rights to the Pro root folder and subfolders.  If a user is not set as a local administrator on his/her workstation, be sure they have full rights to their own Windows user folder, and the Pro (SBTTMP) temp folder set in the user and/or system variables.

Wrong Paths (UNC)



Corrected Paths (Drive Letter)



**Windows Power-Saving**

All workstations and Servers must have standard power-saving disabled.  Machines must not be allowed to enter Sleep Mode, and hard drives must never be allowed to “sleep”.  If the workstation, or hard drive, goes into sleep mode while Pro is running from a network server, the file server will assume that the workstation has disconnected, and will remove the file handles corresponding to the Pro system and data files. Monitors can have power-saving enabled.  In WindowsXP, set the machines to Always On, and verify the hard drives are not allowed to power-down.

In WindowsXP, you can access the power management settings through the control panel, or through the screen-saver tab in the display properties (right click on desktop, select properties). Here is how it should be set (when found through the display properties):



In Windows 7, they have changed the power management system significantly. The screen capture below shows a Dell computer’s special power-saving plan. You need to click the arrow to the right of “Show Additional Plans” to choose the “High Performance Plan” 

Then, change to “High Performance” and save your settings. 

Then, go into Plan Settings and verify that “Put the computer to sleep” is set to “Never” (note: if this is greyed-out, it is being set by a network policy, as in the picture below. Otherwise, you can select or type “Never”): 

Be sure to save all changes to these settings before closing the windows.

Network Adapter Power Saving:  This **MUST** be disabled on all workstations and servers.  To access this new feature, you must go into the system hardware properties, Network Adapters - > Power Management tab.  Uncheck the top-level checkbox (“Allow the computer to turn off this device to save power”).

In **Windows 7**, there is a new System Properties Screen (access this through Control Panel or by right-clicking **Computer** on the desktop or Start menu – Note: from here you can access both the network card and environment variables). In Windows XP, you will skip to the System Properties screen directly from right clicking My Computer, and selecting properties, or from going into System from the Control Panel).

The following screen capture shows the new **Windows 7 System Screen**, along with the Device Manager (the Device Manager itself appears the same in all current versions of Windows):



Note that the Network Adapters has been expanded, and the adapter’s right-click menu is shown with the Properties bar selected. This takes us to the Network Adapter (Card) Properties. You may have to do this for more than one network adapter if your machine has multiple network cards, or an additional wireless adapter.

In Windows XP, you right-click on **My Computer**, found in either the desktop or Start menu  , and select **Properties** to take you to the following screen, which has the Hardware Tab with the button to launch the Device Manager (Note the Advanced tab - you will use this tab to locate the button for the Environment Variables):



On the next page,is the **Device Manager** with the Network **“Ethernet Adapter’s Properties”** window open. You need to select the Power Management tab, and make sure the top option to “Allow computer to turn off this device to save power” is **un-checked**. Note that in the example below that the power management features are enabled (Bad Setting!). This will often cause the computer (or server) to lose its connection to the Pro system and data tables **(“server file handles”)** during periods of inactivity. The usual symptom is that the user is in the middle of entering data, stops to do something else (i.e. lunch), and crashes when they try to continue working in Pro. Sometimes, this can occur when the workstation is busy working on a large temporary file stored locally, such as during processing shipments, closing the month, releasing to GL, etc. This can cause serious problems.



 *Further explanation: If the network card “goes to sleep,” which can happen when a user stops typing for a little while, or if Pro is busy doing an operation on a temporary table (more about the temp folder later), the network’s server will assume the workstation is no longer connected, and will disconnect the “file handles” to the Pro tables. The user will then get unusual errors about missing object references, or alias not found. The server may attempt to reconnect the files, but this will only generate more problems, and the user may be left with an incomplete transaction. I have also observed network servers with multiple network cards where the local card goes into sleep mode while working remotely, and the user loses connection to the Pro files, even though connected directly into the machine hosting them. This is a peculiarity with how Windows uses the network card’s drivers to access any shared drive or folder.*

This is how it should appear with the box unchecked:



Note that the power management tab for the network device properties (above) is pretty much the same between Windows XP, Windows 7/Vista, along with Windows Server. Depending upon the brand and type of network device, you may see more or less tabs and options. You can also get to the network card properties from the Network Properties -> Change Adapter Settings. If you are using a wireless connection (which is highly discouraged for operations such as shipping and receiving, along with any system manager functions other than clearing active users), or may have to use one periodically, you should make the same settings above for the wireless adapter. The wireless adapter’s power-saving can also be set (disabled) in Windows 7/Vista under the standard Power management, under the advanced plan properties. Even the best wireless connection is not nearly as fast, nor stable, as a 100Mb/s or 1Gb/s cabled connection. There may be situations where it is necessary to use wireless in the office (running reports for meetings may be a little slower than normal, but there is no risk to the data), but try to avoid using them for data entry or transaction processing. If you must use a wireless workstation, you can eliminate most complications and speed issues by using Remote Desktop (RDP) for connecting into a terminal server or file server to access Pro. That way, the actual work will be done on a wired connection to the server (in RDP, you are controlling a remote “virtual computer” or the actual server desktop), and if you lose your connection, or have poor connection issues, your RDP “session” should continue to work normally. Your IT department/service may have to adjust settings for remote users, so that their sessions remain active if they become disconnected, and they may want to lengthen time-out and screen-saver/locking settings depending upon usage/safety policies and user preferences.

Workstations/Terminal Server Users: Assign Temp Folder Variable Especially for Pro

Even SQL versions of Pro Series do a lot of the actual work in temporary Visual FoxPro files, which are stored in a temporary folder on the user’s local machine (or terminal server). This includes all report forms, and internal working files for Visual FoxPro. In VFP backend versions, almost all activity takes place on the workstation itself. Local settings specific to the user/workstation are also saved in this folder in newer versions. It is critical for some applications that the user has full rights to this folder. Add the variable SBTTMP.  Pro looks for certain variables when setting the local temp folder. The variable “SBTTMP” overrides all of the other variables, which is why I strongly recommend using it (“TEMP” and “TMP” are more likely to be assigned to a Windows restricted folder location. The value you enter for SBTTMP is a folder on the user’s local hard drive.  You must create the folder manually, and verify the user(s) have full rights.  I usually use “c:\sbttmp,” but you may change this as desired – on a Windows terminal server, each user can have their own SBT temp folder, or they can share one. Your network admin can setup a script using variables to create a folder for each user, set privileges and set the SBTTMP (and SBTUSERID) variable. It is imperative for smooth functioning to use a local drive. If you want/need to assign a drive letter to this location, use a SUBST command rather than a mapped path, to avoid passing data through the network drivers.  Also, never use the same physical drive for the temp folder (for terminal server users) as the system itself. The key thing for this folder is that the user has Full Privileges. Otherwise, certain operations in Pro may fail.  The Window’s default temp folder should not be used for Pro.  There are often restrictions on this folder.  In particular, Pro will take a temporary table, then modify its structure, which recreates the table under the same name.  For some reason, Windows security and certain AV scanners have been known to block this operation.  I recommend adding the variable to both the user and system sections.  Note that **user variables take effect immediately** (although, you do need to exit/restart Pro for Pro to recognize the new temp folder).  System variables become functional after a reboot, or a user logout/login.  If you want, you can add the variable “SBTUSERID” to automatically set the default user login name for Pro. The value should be the same as the user’s login ID for Pro. The screen shot below shows where the variable SBTTMP has been added.

Environmental Variables Screen, showing SBTTMP defined in both User and System variables. (Note the SBTUSERID variable)



Click the “New…” button. Enter the name and value:



**Do not forget to add the folder specified by the value (i.e. c:\sbttmp)!**

You can create the folder through a DOS command prompt with a “MD” command, or you can right click on, or in the C: drive (you may use an alternate drive/location if desired, but be sure to adjust the value of the SBTTMP variable to match). If you make a mistake in the variable, or forget to create the folder, you will get an error, along the lines of: “Temporary data directory is not accessible…the system directory will be used instead.” ***Tip: Always test Pro after completing the workstation setup to make sure you set it up correctly.***

To add the sbttmp folder to the C: drive, double-click Computer, then right click on the C: drive, select New…Folder.
Windows 7:



Click into the “New Folder” name you just created, and rename it “sbttmp.”





Once this folder has been created, right-click on it and go into security settings (if not on the right click menu below, choose Properties, then go to the Security tab), then edit, and be sure to assign Full Rights to all users (select user, click Full Rights, hi apply, select next user, repeat), and then save.





Antivirus/Anti-Malware (aka “AV”) General Settings

All workstations must be set to never scan the server hard drives. Otherwise, you will have locking contention issues, because AV programs temporarily lock files during scanning.  You should also exclude the Pro temp folder specified by the SBTTMP variable.  Also, the server’s AV software should be set to ignore the Pro root folder and subfolders.  On the workstations, if the AV software has “Heuristics” based scanning, which scans for unknown threats, or suspicious behavior, which most do, this is usually found under the advanced features. If it has a level-based setting, turn this to either its middle or lowest level, as the greater the heuristics scanning, the more the it slows down the computer. Also, some Pro file operations can cause the heuristics scanning to deem it as suspicious, and/or monitor every data operation, which may stop, or significantly slow down the system.  With early heuristics scanners, we often had to turn them completely off. If your heuristics scanner only has an on vs. off setting, you can try it both ways to see if it makes a noticeable difference.  **A SINGLE WORKSTATION WITH IMPROPER AV SETTINGS WILL AFFECT ALL OTHER USERS IN PRO!  (If you ever see a “Waiting for Lock…” message, most of the time, it’s because AV is causing a locking conflict, or the server has not been setup properly to block opportunistic locking/”Oplocks”).** You should also add the following VFP file extensions to be ignored: PRG, FXP, DBC, DCX, DCT, DBF, FPT, CDX, FRX, FRT, VCX, VCT, SCX, SCT, SPX, MNX, MNT, MPR, MPX,MEM, FLL (note if this is a version later than Pro7.4, you can let it scan the SCX and SCT extensions, as all forms (screens) should be housed in class libraries (\*.VCX/VCT). Versions prior to Pro6.5 do not have to exclude DBC, DCX, DCT files.

Sophos Anti-Virus Settings for Workstations
(Note: I believe your IT person was able to make the settings changes at the server level for all of the workstations. You should verify them, and add any that are missing, especially the exclusion for the local temporary folder for Pro: c:\sbttmp)Access the Sophos Control Panel, either by right-clicking its icon in the Systray, or by launching it from the Start menu Programs folder.

 

Select **Configure anti-virus and HIPS**



Select **On-Access Scanning.** Under the **Extensions tab,** Make sure **“Allow me to control exactly what is scanned”** is checked:



**On the Exclusions tab, add the following folders and extensions:**

* The root path for your system, or just the server hard drive (S:)
* The temporary data folder: (C:\sbttmp)

All of the following VFP file extensions:

* \*.PRG, \*.FXP, \*.DBC, \*.DCX, \*.DCT, \*.DBF, \*.FPT, \*.CDX, \*.FRX, \*.FRT, \*.VCX, \*.VCT, \*.SCX, \*.SCT, \*.SPX, \*.MNX, \*.MNT, \*.MPR, \*.MPX, \*.MEM, \*.FLL



Recommendations for Servers, Workstations and Switches

If you are still unable to track down random disconnects and data/index corruption, be sure that TCP Offloading and TCP chimney are disabled. While many servers have this enabled without problem, this can been determined to cause random corruption in VFP and SQL applications in some cases (see the following article for details: <http://blogs.msdn.com/b/psssql/archive/2010/02/21/tcp-offloading-again.aspx>). A general thought here: it always better to sacrifice a little performance for the sake of preventing corruption in a mission-critical application.

In general, **only SCSI or SAS drive systems should be used in file servers holding shared database systems** like Pro (the same goes for Act, Quickbooks, Peachtree, Access databases, etc.).   These allow for concurrent write and read operations, and are designed for multi-user systems.  Very small networks of 2-5 users might be able to get away with a server (or Windows workstation acting as a server) using non-SCSI/SAS drive systems, but even there, performance would be so poor, especially with the newer versions of Pro, which require much more server and workstation resources, that I would strongly recommend against it. (Note: on fileservers running on IDE/SATA drives, it is especially important to turn off write-caching on the hard drives holding the Pro system – data sitting in the hard drive’s cache memory may not be seen correctly by other users, and is much more likely to become corrupted).  If you have already purchased a server without an SAS drive controller built-in, and cannot afford to install a SAS controller and drive(s), you may be able to get significantly better performance by using a Solid State Drive (SSD). Only the shared database systems need to be stored on a fast drive. If Pro is your only shared flat database system (“ISAM”), you may only need a relatively small SAS or SCSI (or SSD) drive for the Pro system and its data, while you can run the fileserver’s system and shared storage locations from fast/high-capacity SATA drives (or a separate SSD drive for best server OS performance). Carefully research reviews, especially in regards to reliability before purchasing an SSD drive, and be sure to back it up daily (minimum). There is no way of recovering data from a failed SSD drive, and this is not an uncommon occurrence.

Having enough RAM is critical for good performance in Pro, especially in the workstations. In general, load your servers and workstations with as much RAM as possible. 32-bit systems can only utilize approximately 3.5GB of RAM, and Windows XP 32-bit functions best with 1-2GB. 32-Bit systems are generally much more stable with Pro and older applications than 64-bit computers. If you have a 32-bit Windows 7/Vista, or any Windows server, install 4GB of RAM (if possible), even though the machine might only be able to access the first 3.5GB. I recommend a minimum of 4GB for any 64-bit workstation. 64-bit Windows servers should have at least 8GB RAM. For Terminal/Citrix, Exchange and SQL servers, using the maximum allowable RAM (often 32MB), is strongly recommended. RAM has never been more inexpensive than it is now (and will no doubt continue to drop in price). Doubling your RAM will often produce better performance than doubling your processor speed, and at a fraction the cost. Unless your server specifically requires it, you should not have to pay for expensive proprietary RAM. You may find it less expensive to replace all your existing memory with new matching chips from another brand. There are many vendors, and websites with online memory configurators where you can find compatible or complete replacement RAM kits for specific machines (know your brand, model number, and/or motherboard model), often for a fraction of the price of your original RAM. Currently, you can purchase 8GB (as two matching memory sticks) of quality, name brand DDR3 1333MHz (or faster) RAM, for around $50. A year ago, the same two chips would have cost over $100, three years ago, around $500, and five years ago, if you had a machine with sockets for 8 RAM chips, buying eight 1GB DDR2 800Mhz chips would have run you well over $1200 (closer to $5000 for name-brand servers!). Since Pro and all “fat client” applications rely most heavily on the workstation for processing, investing in new workstations will produce more performance gains than upgrading servers.

With Pro7.4 and newer systems, it is strongly recommended to use Gigagbit network cards, switches, and routers (sometimes identified by “10/100/1000”). If wireless must be used, use a good quality Wireless-N router, along with extenders as necessary. Wireless cannot compete with the speed and stability of wired connections. Regardless of network hardware, the most important thing is to protect your network from power outages and fluctuations. Besides corrupting your index and/or data tables, surges, “brownouts,” and lightning strikes can cause both obvious and subtle damage to your computers and network equipment. **It is imperative to have battery backups on ALL pieces of network hardware, including: servers, workstations, routers, and especially network switches (hubs).** If Pro is to be run remotely by offsite users, DO NOT access the system directly via a VPN! You may use a VPN for enhanced security or access to network resources, but Pro users must use RDP or other remote control software to access a local terminal server or workstation. Do not attempt to “drag” Pro tables across the internet in real-time.

Copying and Backing-up Pro Installations

A little tip, if transferring a backup copy of Pro, use WinZip or other compression utility to shrink the system before sending. Expect a 70-80% reduction in system size when zipped. (That said, do not attempt to compress the live copy of Pro to save space – it cannot run this way). Lastly, I personally recommend every client purchase a copy of WinZip Pro for their fileserver. WinZip has the ability to zip files, even when they are in shared use. Since it can do this, you can create scripts to perform automated zipped backups of your system periodically during the day, and then have those zipfiles copied off to another server or device. If you ever experience a sudden server failure, a mid-day backup may save you a half-day’s worth of re-entering data. If you have a backup file server, you can simply unzip the backup, run a reindex, and database rebuild (in case any transactions were “in-process” during the zipping), remap the drive letter to the new server/location, reboot the workstations, and you’re back up, and running. Always have an emergency plan in place before you need it!

Windows 2008 R2/2011 Server, Windows 7/Vista (and older server versions) – Disable SMB2 and Oplocks

SMB2 and Oplocks absolutely MUST be disabled!  You can read about why here: <http://blogs.msdn.com/b/openspecification/archive/2009/05/22/client-caching-features-oplock-vs-lease.aspx>.

Oplocks are a long-known problem with shared table systems (this is true, even with Novell servers).  The only negative effect is on performance, and that should be negligible.  The alternative is random file locking and corruption problems (especially with index files). I have seen this firsthand with every single client running Windows 2008/2011 Server, or when using a Windows 7 or Vista machine as the Pro Series file server (not recommended).  If you do not implement these changes, the more users you have in Pro, the more frequent the corruption problems, and they can be both crippling to operations, and expensive to repair/re-enter the damaged data. Here are a summary of changes to make to all common versions of Windows server and workstations.  Note that if the registry keys do not already exist, they MUST be added manually. In each case, you are adding new keys and/or DWORD Values (except in the case of the **LanmanWorkstation** key, where you will remove **“Mrxsmb20”** from the list of **DependOnService** values) :

\*\*\*\*\*\* For NT Server - Windows 2000 Server - Windows 2003 Servers [HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters]

"EnableOpLocks"=dword:00000000

"EnableOpLockForceClose"=dword:00000001

"CachedOpenLimit"=dword:0000000

[HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\MRXSmb\Parameters]

"OplocksDisabled"=dword:00000001

\*\*\*\*\*\*\*\*\*\*\*\* For Windows 2008 Server

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters]

"EnableOpLocks"=dword:00000000

"EnableOpLockForceClose"=dword:00000001

"CachedOpenLimit"=dword:0000000

"SMB2"=dword:00000000

[HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\MRXSmb\Parameters]

"OplocksDisabled"=dword:00000001

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\DependOnService]

"MRxSmb20" -- REMOVE FROM LIST

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\MRxSmb20]

"Start"=dword:00000004

\*\*\*\*\*\* For Windows Vista and Windows 7 Workstations [HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters]

"EnableOpLocks"=dword:00000000

"EnableOpLockForceClose"=dword:00000001

"CachedOpenLimit"=dword:0000000

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\DependOnService]

"MRxSmb20" <-- **REMOVE THIS VALUE FROM THE LIST!**

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\MRxSmb20]

"Start"=dword:00000004

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters]

"SMB2"=dword:00000000

[HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\MRXSmb\Parameters]

"OplocksDisabled"=dword:00000001

**Note: If deploying on multiple machines, it is best to create .reg files which can easily be merged into the workstation or server registries. I have either provided these for you, or can upon request. If entering these changes manually, a backup of the registry or the specific keys that need to be altered should be done before applying changes. Your network admin may be able to automate the setting of the registry keys through system policies. To backup a key, launch Regedt32.exe (as the local Administrator). Expand the HKEY\_LOCAL\_MACHINE “hive” and then drill-down to System -> CurrentControlSet -> Services. Under this section, you will find the 4 keys that need to be altered. Before making changes, create a backup folder, then right-click each of the following keys, Select Export, and choose the backup folder you just created. You will need to type in a filename for each exported key, just use the same name as the key name. Here are the four keys to export:**

1. **LanmanWorkstation**
2. **LanmanServer**
3. **Mrxsmb**
4. **Mrxsmb20**

**If there is a problem with the changes, or you need to restore the original values, all you have to do is double-click each of the keys you backed-up, and the old keys will be restored (same process as applying the new keys). If, in the unlikely chance the computer will not reboot normally, reboot into safe mode by hitting the F8 key just before Windows starts loading. From Safe Mode, you should be able to restore the registry keys, and then reboot normally. Using Windows System Restore is another way to restore your registry. Instructions for Windows 7 are available at:** [**http://windows.microsoft.com/en-US/windows7/products/features/system-restore**](http://windows.microsoft.com/en-US/windows7/products/features/system-restore)**. You can find instructions for any current version of Windows through** [**http://support.microsoft.com**](http://support.microsoft.com)**.**